PREFACE

NCRTCE-16 is the 1st National Conference on Recent Technologies in Computer Engineering. The aim of NCRTCE-16 is to provide a platform for world research leaders and practitioners, to discuss the full spectrum of current theoretical developments, emerging technologies, and innovative applications in Computing, Networking and emerging technologies. Computing and Networking is currently one of the most exciting research areas, and it is continuously demonstrating exceptional strength in solving complex problems. The main driving force of the conference is to further explore the fascinating potential of Computing and Networking.

NCRTCE-16 includes Keynote addresses. The time and effort of all the distinguished Keynote speakers, Program committee members and eminent persons from industry handling tutorials are greatly acknowledged.

Keynote speaker in NCRTCE-16 is Dr. T R Gopala Krishnan Nair (Rector, RRCE, Bengaluru).

All the accepted papers are reviewed by the panel of reviewers. On behalf of organizing committee, I express my sincere gratitude and appreciation to our sponsors. We would like thank members of Advisory committee, Technical committee, Review Committee and Organizing Committee for their time and efforts in organizing this conference

On behalf of NCRTCE-16, a special thanks to our Teaching and Non-teaching faculty, Research Scholars, Students of Department of Computer Science and Engineering and all others for their support throughout the conference. We thank all the authors for submitting their research work to NCRTCE-16. I would like to thank all the people involved in organizing this conference.

Dr. Usha. S
Organizing Secretary
ICICN – 16

ABSTRACT

Keynote on **"Frontiers of Internet Computing"-** Internet computing is a domain covering the computer technologies, communication technologies with methods and practices of creating services and disseminating them over the internet. The Internet, over a period of 3 decades have undergone very systematic revolution in an exponential scale. Today integrating more than a 3 billion users and delivering the pro-active services and deeper levels of information, it governs the culture of humanity.

The Internet technology has diversified by integrating most advanced computing systems and best of the communication systems with sophisticated searching, mining, extracting and presenting user defined information. Yet, there is a long way for the internet to trace and grow in the building knowledge in its multiple differentiated forms and morphisms.

Expectations of 21st century can never get quenched with the present structure and capabilities what the Internet possesses today. Revolutionary approaches are required to enable making to internet transform to a world of Internet of Things as well as Internet of Intelligence. It calls for revolutionary approaches in intelligent control of the current network cognitive capabilities building user termination point's mammoth capabilities of distributed information management in using knowledge networks that are getting formed.

Chairman's Message

"We cannot always build the future for our youth, but we can build our youth for the future."

I am very happy and proud that RajaRajeswari College of Engineering is hosting an National Conference of this stature and at the outset; I congratulate all those who have been a part of this conference. Such conferences give platform for Intellectual exchange wherein experts from the domain come and share their valuable expertise. I have absolutely no doubt that the students, faculties, participants will benefit immensely. Once again my heartiest wishes for all those who have been a part of this conference.

SHRI. A. C. SHANMUGAM

CHAIRMAN

Vice-Chairman's Message

My heartiest congratulations for the team of RRCE for pulling off this conference and hope that the students and the faculties shall be enriched by this experience.

SHRI. A. C. S. ARUN KUMAR

VICE-CHAIRMAN

Executive Director's Message

Greetings!!! Keeping up with today's evolving educational challenges, it requires out of the box approach to technical education as there are lot of technology breakthroughs happening in the educational field today. Professional Institutions need to redesign the training for the students as well as for the faculties. We believe that there has to be a continuous learning curve. Symposiums, workshops, seminars, conferences are the best medium for such scholarly exchanges.

I would like to take this opportunity to express my sincere happiness to all my team who have shown tremendous commitment and enthusiasm in making this happen .

I once again extend a very warm welcome to you all and assure you all a very productive and pleasant time at our institution. Thank you

SHRI. S. VIJAYANAND

Executive Director

Rector's Message

I am immensely happy on the occasion of the commencement of the 1st National Conference on Recent Technologies in Computer Engineering NCRTCE-16 to be held in RRCE, Bengaluru Soon. I understand that the conference emphasizes on Innovations happened in the recent past in the broad spectrum of computing and networking. As the main objective NCRTCE-16 is to provide an elegant platform for researchers to express their novel ideas and practices, this conference is going to be one of the very successful conglomerations of professionals, Encouraging and enriching the computing domain.

Conference received more than 75 papers and it was subjected to sufficient reviews resulting in a selection of 46 papers to be published in the name of the conference. This is a remarkable success. At this juncture, I would like to congratulate all the members of the conference team as well as the philanthropic management who had perceived and realized such an event in Bengaluru.

As the program chair I express my best wishes to all the delegates to a fruitful professional engagement during the period of conference.

Dr. T R Gopala Krishnan Nair

RECTOR

Principal's Message

"Creativity leads to thinking,

Thinking provides knowledge.

Knowledge makes you great"

I, on behalf the organizing committee, very much pleased to invite engineers, technocrats and the teaching faculty to contribute technical papers to International Conference On "1st National Conference on Recent Technologies in Computer Engineering **(**NCRTCE-16)", It is designed to attract as many experts from the Computer Science and Engineering from all over the nation to showcase their research and interact for the benefit of all academicians and the industry. I hope that each participant gets individually enriched in turn enriching every other participant. I am sure that this conference accords the right forum for interaction and benefits everyone concerned.

Join us and enjoy yourself at this great event and partake of our hospitality.

As Program Chairperson of the NCRTCE-16, I believe that this conference will help us in many directions to develop our country research potential.

Dr.R.Balakrishna

Principal

Vice Principal's Message

Proud to know that the department of Computer Science & Engineering of our Institution is conducting 2 days National Conference on 22,23 Sept 2016. The conference will probably chase for new innovations.

I am optimistic that, at the end of the day, many more innovative ideas on computing and networking could be place.

My congratulations to organizers and best wishes for the event.

Prof. Prabhakar M

Vice Principal

Organizing Secretary Message

The department of Computer Science & Engineering, RajaRajeswari College Of Engineering, Bengaluru proudly organizing our 1st National Conference "Recent Technologies in Computer Engineering **(**NCRTCE-16)" on 22,23 Sept 2016.

On behalf of the organizing committee NCRTCE-16, I proudly welcome all the speakers and delegates of different parts of the country and the world to present their innovative ideas on current trends in technology.

I would like to thank the keynote speaker. I will also place my gratitude to the management of RajaRajeswari group of Institutions. I would also like to thank all the members of different committees, who worked successively to make this event in much bigger way.

I wish a good luck for all the participants.

Dr. Usha S

Organizing Secretary

Convener Message

The conference is a meeting and information exchange between the end user, the event has attracted academicians, research scholars, students and industry experts. This conference will be exceptional in many ways, a strong accentuate is being prepared for a well-balanced and effective academic - industrial participation with High quality papers and presentations ; a momentous number of Keynotes, Invited talks and presentation sessions delivered by delegates from academic and industry communities.

I hope that this conference would surely induce modern ideas among the participants paving way for new inventions in the field of computer science

We are also very much thankful to the Management, Rector and Principal

I would like to pay thanks to all Authors and participant for their association.

Dr. Malathy M

Convener

Convener Message

It is a personal honor and pleasure for me to be the Convener of ICICN16. The technology today is developing at a rapid pace. In this era of globalization, the exchange of knowledge and skills has given a further fillip to the exponential growth in the field of technology. Such phenomenal advancements have revolutionized almost every sphere of human life today.

The objective of this conference is to provide a concrete platform which will encourage & support scholars, researchers & industry professionals to carry & accomplish their research targets.

Expecting a sound response from you all.

Prof. T Auntin Jose

Convener

CHIEF PATRON

Sri.A.C. Shanmugam
Chairman,
Moogambigai Charitable Educational Trust,
RajaRajeswari Group of Institutions, Bengaluru

PATRON

Sri. A. C. S. Arunkumar
Vice Chairman,
RajaRajeswari Group of Institutions, Bengaluru

GENERAL CHAIRS

Sri. S Vijayanand , Executive Director, RRGI
Sri. C. N. Seetharam, CEO, RRGI
Sri. Jeyabalan , Special Officer, RRGI
Dr. T R Gopalakrishnan Nair, Rector, RRGI

PROGRAMME CHAIR

Dr. R Balakrishna , Principal, RRCE

ORGANIZING SECRETARY

Dr. Usha S, Prof. & Head, CSE, RRCE

CONVENORS

Dr. Malathy M
Prof. Auntin Jose T

Co-CONVENORS

Prof. Vandana B
Prof. Shashidhar V
Prof. Nandini G

Technical ADVISORY COMMITTEE

Dr. V. Sridhar, Vice Chancellor (VTU)
Prof. M. Ramachandran, Leeds Becket University, UK
Mr. Aravind, Intel Corporation, USA
Mr. A M Padma Reddy, SVIT, Bengaluru
Dr. Vivek Deshpande, VIT, Pune
Prof. Dr. Lalit Mohan Patnaik, IISC, Banglore
Dr. Cyril Raj, Dr MGR University, Chennai
Dr. S Radha, SSNCE, Chennai
Dr. Shadaksharappa Bichagal SSEC, Bengaluru
Dr. Om.D Deshmukh, Xerox Research Center, Bengaluru
Dr. Guruprasad. N, NHCE, Bengaluru
Dr. C Nandini, DSATM,Bengaluru
Dr. Siddaraju.B, Dr AIT, Bengaluru
Dr. Madhu H Gowda, SVVIT,Bengaluru
Dr. Guruprasad. H S, BMSCE,Bengaluru
Dr. Arunachalam, RRCE,Bengaluru
Dr. G,T Raju, RNSIT,Bengaluru
Dr. M S Murali, ACSCE, Bengaluru
Mr. Ramesh, Cadence system
Prof. Prabhakar. M, RRCE, Bengaluru
Dr. Sheela T. SSEC, Chennai
Dr. J Anitha, DSATM, Bengaluru
Dr. Swarnajoythi, RRCE, Bengaluru
Dr. Shobha G, RVCE, Bengaluru
Dr. Mohan H S, SJBIT, Bengaluru

EDITORIAL COMMITTEE

Dr.T.R. Gopalakrishnan Nair
Dr. BalaKrishna R
Dr. Usha S
Dr. Malathy
Prof. Rajesh K S

COMMUNICATION AND ADVERTISEMENT COMMITTEE

Prof. Anitha K
Prof. Neelu L
Prof. Bharath J

Prof. Revathy S
Prof. Auntin Jose T

INAUGURATION AND VALEDICTORY COMMITTEE

Prof. Rajesh K S
Prof. Poonam Kumari
Prof. Malathy M
Prof. Shashidhar V
Prof. Swetha P
Prof. Srinivas R

SESSION COORDINATORS COMMITTEE

Prof. Rajesh K S
Dr. Malathy M
Dr. Janaki K
Dr. Subhashini K
Prof. Srinivas R
Prof. Neelu L

TRANSPORTATION COMMITTEE

Prof. Kamal Raj T
Prof. Bharath J
Prof. SarvanaPerumal.
Prof. Manigandan J

CERTIFICATE COMMITTEE

Prof. Poonam Kumari
Prof. Neelu L
Prof. M H Rehaman
Prof. Manigandan J

HOSPITALITY COMMITTEE

Prof. Rajesh K S
Prof. Poonam Kumari
Prof. SarvanaPerumal.
Prof. Kamal Raj T

Prof. Nandini G

RECEPTION COMMITTEE

Prof. Poonam Kumari
Prof. Swetha P
Prof. Anitha.K
Prof. Sreenivasa. B.R

REGISTRATION COMMITTEE

Prof. Swathipriya N
Prof. Revathy S
Prof. Shashidhar V

STAGE COMMITTEE

Prof. Sreenivasa. B.R
Prof. Revathy S
Prof. Prabhaharan J
Prof. Auntin Jose T
Prof. Srinivasa R

REFRESHMENT COMMITTEE

Prof. M H Rehaman
Prof. Manigandan J
Prof. Prabaharan J
Dr. Janaki M

JOURNALS AND PROCEEDINGS COMMITTEE

Prof. Shashidhar V
Prof. Sreenivasa. B.R
Prof. Nandini G
Prof. Auntin Jose T
Prof. Srinivasa R
Prof. Shashidhar V
Prof. M.Madhureka

FINANCE COMMITTEE

Prof. Nandini G
Prof. Vandana
Prof. M H Rehaman

WEBSITE COMMITTEE

Dr. Usha S
Prof. Swetha P

PURCHASE COMMITTEE

Prof. Sreenivasa.B.R
Prof. Bharath J
Prof. Saravana Perumal

BOARDING AND LODGING COMMITTEE

Prof. SarvanaPerumal. VM
Prof. Srinivas.R
Prof. Vandana B
Prof. Prabaharan J

INDEX

A Software-Defined Device-to-Device Communication Architecture for Public Safety Applications in 5G Networks

Poonam V Tijare[1], Rahul S Sreedhar[2]
[1]Asst. Professor, [2]UG Scholar, Dept. of CSE, CMR Institute of Technology, Bangalore-037
Email: poonam.v@cmrit.ac.in , rahuls.1234sreedhar@gmail.com

Abstract: In the near future beyond 4G, some of the major requirements that need to be addressed are increased capacity, improved data rate, decreased latency, and better quality of service. To meet these demands, drastic improvements need to be made in cellular network architecture. This paper presents the results of a detailed survey of the fifth generation (5G) cellular network architecture and some of the key emerging technologies that are helpful in improving the architecture and meeting the demands of users. In this paper, a general probable 5G cellular network architecture is proposed, which shows that D2D, small cell access points, network cloud, and the Internet of Things can be a part of 5G cellular network architecture.

Keywords – Channel Quality Information (CQI), Network Function Virtualization (NFV), Software Defined Networking (SDN), User Equipment (UE), Wireless Sensor Networks (WSNs)

1. INTRODUCTION

The drastic increase in the number of cellular devices and traffic volume in combination with the spectrum crunch represents the primary challenge for the fifth generation (5G) networks. Therefore 5G networks intend to combine radical solutions to assure high capacity, lower latency, and higher reliability. Such solutions include several emerging technologies such as Software Defined Networking (SDN), Network Function Virtualization (NFV), massive MIMO (Multiple Input Multiple Output) and Device-to-Device (D2D) communication. D2D communication represents one such technology that can potentially solve the capacity bottleneck problem of the current cellular systems.

This new concept enables direct interaction between nearby Long Term Evolution (LTE) based devices by minimizing the data transmissions in the radio access network. By doing so, it provides many benefits. First, direct communication can offload data from the treasured spectrum to out-of-band technologies improving spectral efficiency. Second, data rates and coverage can be increased by a very large extent for devices that lack direct access to the cellular infrastructure. Third, higher energy efficiency can be achieved due to the close proximity of devices requiring lower transmission powers. To fully realize these benefits in practice, the architecture for D2D communication should be flexible and powerful enough to meet the needs of commercial cellular scenarios as well as public safety applications. The convergence of public safety applications with the commercial cellular networks poses a major problem in defining the D2D communication architectures. This is due to more stringent requirements of public safety applications, like for example, high service reliability with ultra-low delays. Even when cellular infrastructure becomes overloaded or partially unavailable (e.g., in case of extraordinary events such as disasters or terrorist attacks), basic communication services should still be made available to public safety agencies such as police and paramedics. Furthermore, these networks should effectively incorporate mechanisms to seamlessly integrate with emerging technologies designed to further enhance public safety such as Wireless Sensor Networks (WSNs).

Here, we propose the SDN architecture for supporting D2D communication, which meets the above-mentioned requirements of public safety applications as well as commercial cellular scenarios. First, we exploit D2D communication to build mobile clouds, a powerful concept that enables diverse services for a wide range of applications such as proximity-based social networking (e.g., online gaming, video streaming), advertisements for by-passers, public safety (public safety devices provide at least local connectivity in the case of damage to the radio infrastructure), intelligent vehicle communication, and efficient content distribution. Second, we build our architecture on top of public safety enhancements for LTE standardized by the Third Generation Partnership Project (3GPP) as Proximity Services (ProSe) and Group Call System, assuring efficient inter-operability across different public safety applications.

The idea behind the proposed architecture is to associate a D2D controller application to a hierarchy of SDN controllers in the network, in such a way to couple the formation and management of the mobile clouds of devices with centralized control, resource allocation and routing features of SDN. To make our architecture scalable, we design it to be hierarchical in nature, placing SDN

controllers locally to the mobile cloud as well as globally in the core network. This choice makes the process of cloud formation scalable, energy efficient and robust to cellular infrastructure failure.

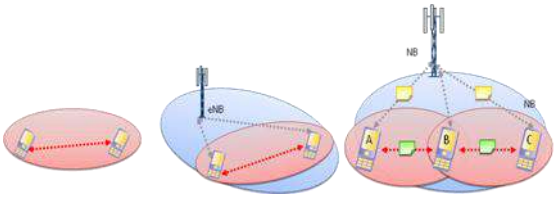


Figure 1: Basic concept of Device to Device Communication. [1]

The cloud formation process is divided into two phases. In the first phase, a UE (User Equipment) initiates formation of mobile cloud by broadcasting a request to the nearby devices by using an out-of-band technology e.g., Wi-Fi Direct, Bluetooth etc. Based on the information received from the responding UEs, a mobile cloud is formed and it is registered at a global SDN controller. In the second phase, the central SDN controller will have a global view of all served clouds with the services that they offer. At this point, the global controller can setup the clouds upon several users' requests. The SDN controller has also a visibility of link qualities between UEs/CHs and residual batteries, which it can use to compute routing paths between the CHs.

2. LITERATURE SURVEY

In literature, various architectures are proposed for D2D communication in cellular networks. The mobile cloud coverage area is divided into clusters (logical regions) of UEs and comprises of a Primary Cluster Head (PCH), a Secondary Cluster Head (SCH) and standard UEs. PCH and SCH, which are chosen based on the residual energy and SINR (Signal-to-interference-plus-noise ratio) of the UEs, multicast information to the UEs of their respective clusters [3]. The architecture provides an energy efficient solution for a single eNodeB or base station. However, it does not allow extension of coverage area beyond a single cell, making it less ideal for public safety applications. Further studies show that a mobile cloud system that implements device discovery based on the audio data obtained from the user environment [4]. This centrally controlled cloud system follows client-server architecture, where clients (UEs) send synchronized time series recordings to the server that runs a clustering algorithm on the time series in order to group them based on their audio similarity. Such a complex algorithm is neither energy-efficient nor scalable, as all clients have to be continuously synchronized with a single server through the cellular interface. Some of the ideas proposed in the literature can also be used in the proposed architecture [5]. There are cloudlets to describe resource-rich computing environment located at the edge of the network and in the proximity of mobile users. The UEs can use this environment to offload computations and execute virtualized tasks. The FlashLinQ, a synchronous OFDM-based system, to perform device discovery, channel allocation and link scheduling in the licensed spectrum [6]. The distributed channel allocation in licensed spectrum is claimed to provide significant gain over conventional IEEE 802.11 systems. Our mobile cloud-based architecture provides several **advantages** over the conventional solutions:

2.1 Scalability

The mobile clouds and hierarchical controllers make our architecture very scalable. The cloud heads control the nearby UEs and transmit their aggregated information to the central controller, reducing the number of LTE links and improving scalability.

2.2 Energy and spectral efficiency

The UEs communicate with each other using Wi-Fi links and the cloud heads transmit their aggregated information to the SDN controller. This improves the overall energy and spectral efficiencies of the network.

2.3 Robustness

In the case of disaster and traffic hotspot situation, the UEs are still able to communicate with partial support from cellular infrastructure, making the architecture reliable and robust. UEs outside the cellular coverage are served by UEs inside the cellular coverage.

2.4 Interference reduction

The central controller has the global view of the network by managing multiple eNodeBs. Such global view enables the interference reduction between neighboring eNodeBs and allows UEs to participate in multiple clouds.

3. THE SOFTWARE DEFINED D2D ARCHITECTURE

This is the schematic diagram of our D2D architecture for public safety applications. Each UE runs a D2D application, using a hierarchical approach to create a mobile cloud on demand. The central D2D/SDN controller that resides on the Internet has a global view of all mobile clouds in its range, while the local controllers (cloud heads) are aware of UEs only in their neighborhood. Each SDN controller serves a number of eNodeBs depending on the deployment. Our architecture also enables a UE to participate in multiple mobile clouds providing different resources/services. This raises two important issues that need to be considered:

1) The operations belonging to different mobile clouds should be isolated from each other with no ability to affect each other, a primary goal for virtualization.

2) Given heterogeneity across different applications requiring different Quality of Service (QoS), SDN controller should be able to dynamically allocate resources. For example, let us consider that one of the mobile clouds provide services for file transfer and the other one for video conferencing. In such situations, we need to deploy a dynamic resource allocation scheme that improves the spectrum efficiency and /or throughput of the network.

3.1 Signaling for Cloud Formation

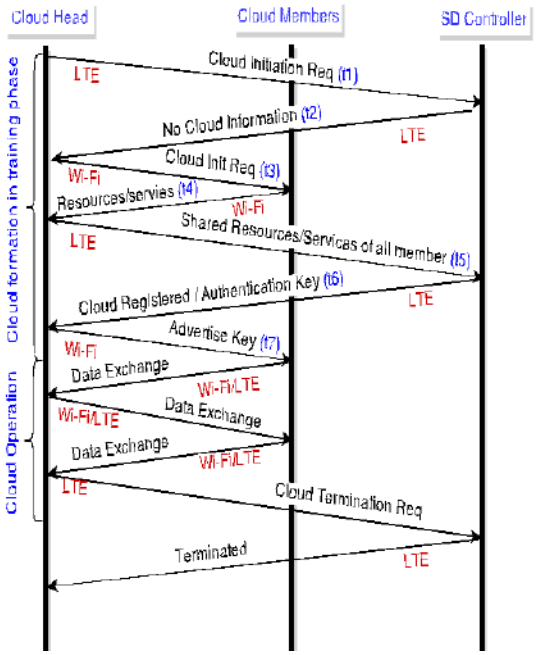


Figure 2: Description of signaling for cloud formation [4].

The above figure describes the formation and the operation of the mobile clouds. The initiator broadcasts a request of cloud formation over the Wi-Fi interface. The mobile devices in the vicinity, interested in sharing such service, respond with their resources/services. The SDN application in each mobile device maintains a database of all services and resources that a mobile user is willing to share. Once a cloud formation request is received from an initiating UE, all interested UEs share the complete database with the initiator. The initiator shares this database with the central SDN controller. The SDN controller registers the mobile cloud and assigns an authentication key to the cloud. The initiator then unicasts the authentication key to each UE, securing it from any malicious attack. Once the cloud is formed, devices can communicate during the rest of their operation, unless the cloud head sends a termination request.

3.2 Energy and Spectral Efficiency

The SDN controller maintains a database of all mobile clouds, saving identities of individual UEs and their sharable services. In the case of resource sharing services, the details of resources are also stored in the SDN database.

Once the database is fully populated, the central controller can form clouds without involving local controllers and save energy.

Using outband D2D links in mobile clouds improves the spectral efficiency of the network. Moreover, any service change of a UE is updated to the SDN controller over the LTE interface. [9]

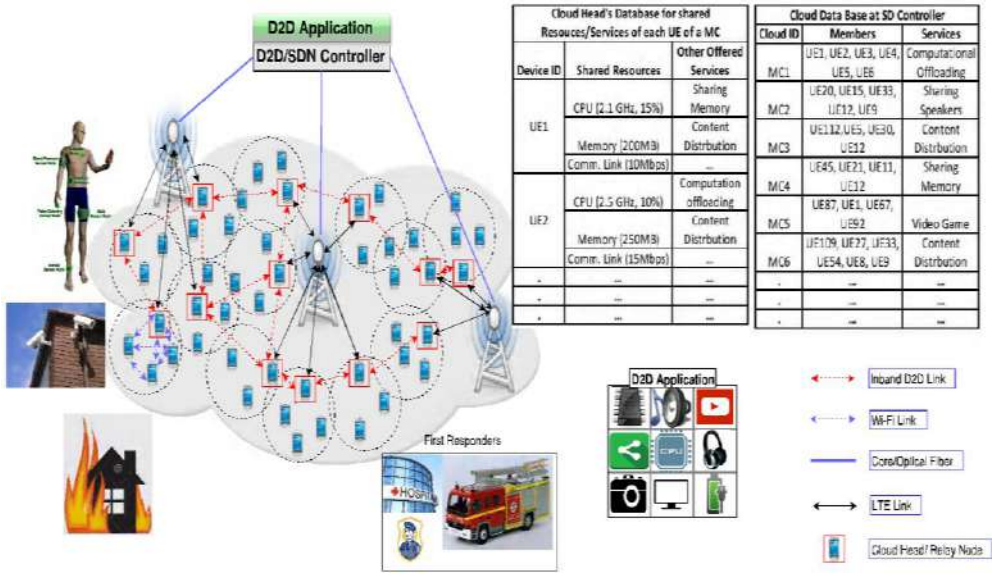


Figure 3: The proposed Software-Defined D2D communication architecture for public safety applications. [3]

3.3 Scalability

There are several studies concerning the design and implementation of controllers (e.g., centralized, distributed, hierarchical, etc.), where each has its own advantages and disadvantages. However, the hierarchal architecture better fits our needs in a way that it helps to address the problems of scalability and efficient resource utilization by lowering the communication load with the central controller. The distribution of different functionalities to different levels of the controllers (i.e., local and central/SDN controller) reduces unnecessary communication with the higher-level controllers, which use the scarce radio resources (i.e., LTE spectrum). For example, the local controller (initiator/cloud head) can independently enable and or disable clouds without involving central controller. In addition, the hierarchical architecture is very convenient for scalability. The number of devices participating in a cloud can increase as long as the processing capacity of the Cloud Head (CH) is not reached. The Channel Quality Information (CQI) of the UE determines the selection of the CH, i.e., the UE should be in better signal condition. Moreover, the flexibility of having local decisions carried out by local controller enables each cloud to work in a distributed manner. Based on the above contributions (i.e., saving resources in terms of spectrum), our architecture is applicable to a wide range of applications that are an integral part of 5G networks, e.g., in public safety. [10]

3.4 Coverage and Interoperability

Proximity services include features to discover devices in physical proximity and enable an optimized communication between them. Proximity services offer two functions: the network-assisted discovery of users in a close proximity and the facilitation of direct communication between such users with or without supervision from the network (see Fig. 3). Proximity services also extend normal network coverage area. If a User Equipment is outside the cellular coverage, it can, through another UE, relay its traffic to a base station (eNodeB) or to a different UE.

The former is termed as User Equipment to Network Relay feature, while the later is called User Equipment to User Equipment Relay feature. Notably, in User Equipment to User Equipment Relay feature, the traffic does not even traverse the cellular network and yet it can reach the intended destination or at least a location closer to it. In addition to the extended network coverage provided by ProSe, public safety devices need to communicate in groups. Therefore, the LTE Group Call System provides and optimizes concurrent communication between multiple groups. In addition, it describes appropriate group management and control facilities.

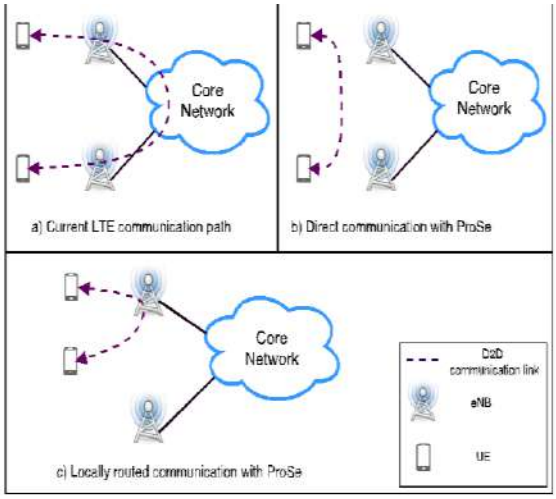


Figure 4: Examples of Proximity Services. [4]

4. ROUTE COMPUTATION

The figure below shows the possible signaling that could be performed for delivering the information from the source to destination in the cases that were discussed.

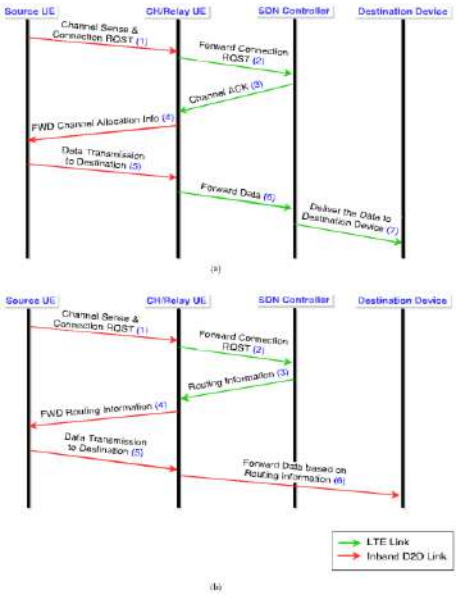


Figure 5: Signaling for multi-hop routing between cloud heads. (a) Adequate resource available in eNB. (b) The eNB is fully loaded, computes a route information. [4]

The signaling is shown in Fig. 5(a) is for the case when the target eNodeB has an adequate radio of resources to entertain the incoming resource requests, and

allocates cellular radio resources to the transmission, as shown in the signaling number [(1)-(7)]. Fig. 5(b) shows the signaling when the cellular network radio resource is completely depleted. In this case, the central SDN controller computes a route from the source (i.e., Relay UE) to the destination device using the inband D2D communication links between CHs and forwards the routing information to the Relay UE (i.e., as depicted by the signaling number (4)). The computation of the routing information could be done using different routing algorithms, such as the Dijkstra's routing algorithm. Dijkstra's algorithm finds the shortest paths between nodes (source and destination) in a graph traversing through the smallest link cost paths.

The link cost function could be defined as a function of device battery life, computational power, and channel quality indicator (CQI) (i.e., contributes to the physical data rate of the channel). Each of these parameters has direct proportionality with respect to the probability of selection of the link, as in (1), as the shortest path. That means, if the battery life of the device is high then the probability of this node being selected as the next hop of the route is higher.

$$\mathbf{P_n \alpha f (P_{comp}, L_{batt}, CQI);} \qquad (1)$$

where P_n is the probability of selecting a link as the shortest path to the next hop (node), P_{comp} is the computational power of the device and CQI (a function of the received signal strength indicator) is directly related to the signal-to-noise (SNR) of the channel resulting a direct insight on the channel capacity of the link. Actually, the link cost is defined as the inverse of P_n. From (1) we can further describe P_{comp} and L_{batt} in details respectively as shown below:

$$\mathbf{P_{comp} = vf^2;} \qquad (2)$$

where *v* is the voltage (in volts) input to the processor of the device and *f* is the number of instructions executed per second.

$$\mathbf{L_{batt} = \frac{Battery\ capacity\ [mAh]}{Load\ current\ [mA]};} \qquad (3)$$

The choice of the cost function depends on a predefined *priority*, where the device battery life (L_{batt}) is assumed to have the highest priority, then the channel link quality, and finally the computational power (P_{comp}) of the device. Based on these priorities, a link cost is assigned to each link of a UE connecting it with the next hop to facilitate end-to-end route computation.

In Figure 6, have two options, though UE 2 or UE 3. Relying on the priority of the cost functions that we defined earlier, the battery life of UE 2 is better than UE 3. Thus Link 1 is selected instead of Link 2. On the other hand, if both UEs (i.e., UE 2 and UE 3) have equal battery life, then the next parameter to be considered is the computational power (i.e., CPU voltage and CPU frequency) of the devices, assuming same link quality for both links.

Figure 6: Example of route selection for different cost functions.[5]

5. CONCLUSION

In future smart cities, there will be a dense deployment of WSNs ranging from water reservation to public safety and the seamless integration of these WSNs with future 5G networks is an open issue. A novel hybrid D2D communication architecture that is applicable to a wide range of applications is the proposed concept. The mobile clouds in our architecture meet the needs of processing and storage demands of WSNs, where raw data from sensors can be processed and sent to first responders to decide their rescue plan. Currently, research is being done for simulating the above-mentioned scenario using the NS3 simulator to analyze the computational load incurred by the cloud heads.

REFERENCES

[1]P. Demestichas et al., *"5G on the horizon: Key challenges for the radio-access network,"* IEEE Veh. Technol. Mag., vol. 8, no. 3, pp. 4753, Jul. 2013.

[2]F. Granelli et al., *"Software defined and virtualized wireless access in future wireless networks: Scenarios and standards,"* IEEE Commun. Mag., vol. 53, no. 6, pp. 2634, Jun. 2015.

[3]S. Tamoor-ul-Hassan, M. I. Ashraf, and M. D. Katz, *"Mobile cloud based architecture for device-to-device (D2D) communication underlying cellular network,"* in Proc. IFIP Wireless Days (WD), Valencia, Spain, Nov. 2013, pp. 13.

[4]J. Mass, S. N. Srirama, H. Flores, and C. Chang, *"Proximal and socialaware device-to-device communication via audio detection on cloud,"* in Proc. 13th Int. Conf. Mobile Ubiquitous Multimedia, Melbourne, VIC, Australia, Nov. 2014, pp. 143150.

[5]M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, *"The case for VM-based cloudlets in mobile computing,"* IEEE Pervasive Comput., vol. 8, no. 4, pp. 1423, Oct./Dec. 2009.

[6]X. Wu et al., *"FlashLinQ: A synchronous distributed scheduler for peer-to-peer ad hoc networks,"* in Proc. 48th Annu. Allerton Conf. Commun., Control, Comput., Allerton, IL, USA, Sep./Oct. 2010, pp. 514521.

[7]The 3rd Generation Partnership Project (3GPP). Public Safety. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1455-Public- Safety, accessed Jul. 15, 2015.

[8]Z. Xiao, H. Wen, A. Markham, and N. Trigoni, *"Lightweight map matching for indoor localization using conditional random elds,"* in Proc. 13th Int. Symp. Inf. Process. Sensor Netw. (IPSN), 2014, pp. 131142.

[9]*Data communication and Networking*, 4th Edition, Beherouz A Forouzan

[10]Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Muhammad Inayatullah Babar, "An Efficient Network Monitoring and Management System", *International Journal of Information and Electronics Engineering*, Vol. 3, No. 1, January 2013

Analysis of Miscategorization Fraud Detection in Electronic Mails Using Data Mining Techniques (002)

[1]Bhavana Gowda D M, [2]Pushwitha K, [3]Prakruthi C, [4]Sindhu G

[1]ASST.PROF,[2,3,4]UG Scholar, Dept. of CSE, VKIT, Bangalore.

bgowdadm@gmail.com , pushwitha@gmail.com

Abstract-This paper provides the classification of the filtered data. The main purpose of this analysis is to reduce the error rate of the data and to improve the accuracy. In this analysis the problem of miscategorization is reduced. The work is presented by this research is the classification techniques. Therefore, it is a good solution for filtering. This will improve the system performance and also some improvements on the previous algorithm. This will give the better results than the previous one.

Keywords-- Email, Filtering, Bayesian filters, Spam, Decision tree

I. INTRODUCTION

Email is an electronic device. It is method of exchanging digital message or information from source to destination. The abbreviation of email is electronic mail. Email message can be text files, images, sound and so on. Email server accept, forward, deliver and store messages. Originally an ASCII text, only-communication medium, internet email was extended by multipurpose internet mail extension. When one user send the message to the specified address then one can also send the same message to the several users and this is called broad casting. Emails are fast and language used in emails is simple can be formal or informal. There is no paper work while using email. It contains friendly environment and can also have pictures, audio files, video files etc. There are also auto responders in email. Products can be advertised, so that companies can reach a lot of people and can advertise their product in a very short time. But having all these advantages emails have some disadvantages too like emails can carry viruses. Unknown and unwanted people can also send messages called spams. Through emails ones systems can get crashed. Mailbox may get flooded with emails after a certain time so one have to empty it from time to time.Their messages are modules which are added in the working of the email system. In the processing of the email, SMTP is also used. In shorts, the steps are:

- Message is sent by email client.
- Email server contacted to the recipients email server.
- Username's validity is checked by the email server.
- If valid username is typed, email is sent to the email server of the address.
- When the recipient sings in to his mailing account, he finds his email.

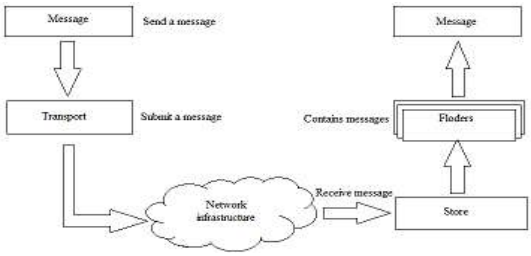


Fig1: Working of email server

II. PROBLEM EXPLANATION

Our research is for the less error prone classification by reducing the misclassification. Misclassification is defined as when justified emails are categorized as junk emails or vice versa. Cost of misclassifying justified emails as junk is much higher than the cost of junk mails as justified mails. Remedies can be found using the following steps: Classification scheme which will provide probability for its classification decisions.

The above concepts are implemented in the following algorithms for classification. These algorithms are:

- Naïve Bayes Classifier.
- Decision tree.

In case of Linear Discriminant Analysis, there are training data and sample data. The observations with known class labels are known as training data. There are sample data on which we will be using the training data sets. Then we will be computing the resubstitution error which is the misclassification error (the proportion of misclassified observations) on the training set. We will also compute the confusion matrix on the training set. A confusion matrix contains information about known class labels and predicted class labels. Generally speaking, the (i,j) element in the confusion matrix is the number of samples whose known class label is class i and whose predicted class is j. The diagonal elements which would be represented in graph will be correctly classified

observations. For some data sets, the regions for the various classes are not well separated by lines. When that is the case, linear discriminant analysis is not appropriate. Instead, you can try quadratic discriminant analysis (QDA) for our data. In our base paper , it has been declared that random forest algorithm is the best to classify spam and non-spam mails. But there are some advantages of decision tree over random forest.
These are as follows:

- Decision tree is easy to explain and interpret.
- Decision tree takes less time to be executed than random forest. So it is time efficient too.

These are the reasons why we are implementing decision tree rather than random forest. Except that, the dataset is already filtered, and as random forest is used when there are some complex dataset, there is no need to implement the random forest again. Decision trees can handle both categorical and numerical data. For the decision tree algorithm, the cross-validation error estimate is significantly larger than the resubstitution error. This shows that the generated tree over fits the training set. In other words, this is a tree that classifies the original training set well, but the structure of the tree is sensitive to this particular training set so that its performance on new data is likely to degrade. It is often possible to find a simpler tree that performs better than a more complex tree on new data.

Objective-The objective of our work is to minimize the classification error by reducing misclassification. As the base of our research is Naïve Bay's algorithm, so we will be implementing the Naïve Bay's algorithm at first. Our proposed method is based on decision tree, so we will be implementing the standard decision tree algorithm and the algorithm with least error will be chosen as the best way to filter emails. The steps are:

- Accessing and categorizing the UCI repository on email filtering.
- Implement Naive Bay's Algorithm.
- Implement decision tree algorithm.
- Finding out the misclassification error.

III. RESULTS

The dataset for the implementation is taken from the machine learning dataset website "UCI" Repository". The software used for the development of the classification system Weka 3.6 (for the visualization of the dataset) and MATLAB 8 (R2012a). The numeric data is imported to the dataset variable and the class labels are stored in mail group variable.

Table 1. Dataset information of spam mails from UCI repository

Data Characteristics	Multivariate	Number of instances	4601
Attribute Characteristics	Integer, real	Number of attributes	57

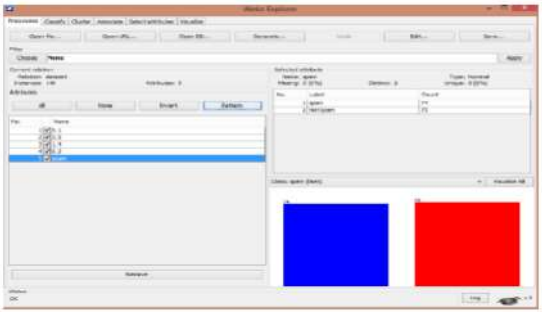


Fig 2: Weka visualization of the data

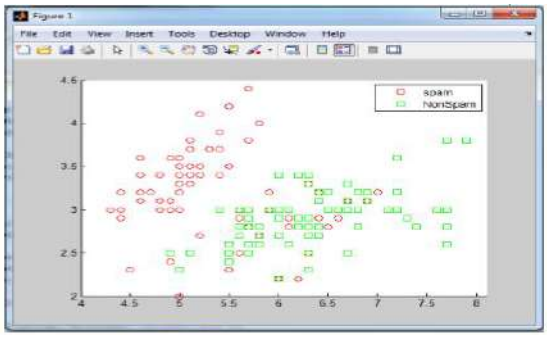


Fig 3: Scattering of the dataset on the basis of the class labels spam and non spam

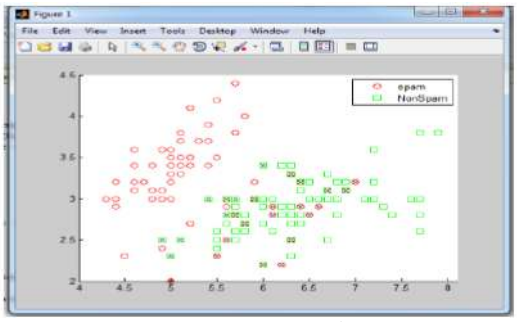


Fig 4: Misclassification

Fig 5: Classification using linear distribution

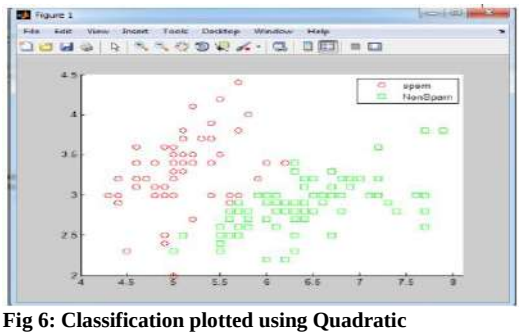


Fig 6: Classification plotted using Quadratic distribution

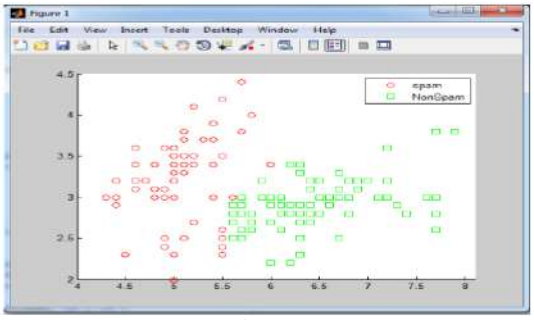


Fig 7: Classification using Naive Bayes Gaussian distribution

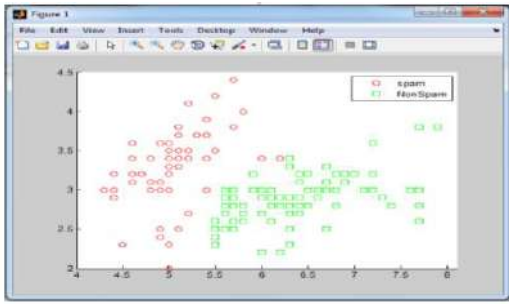


Fig 8: Classification plotted using Naive Bayes Kernel distribution

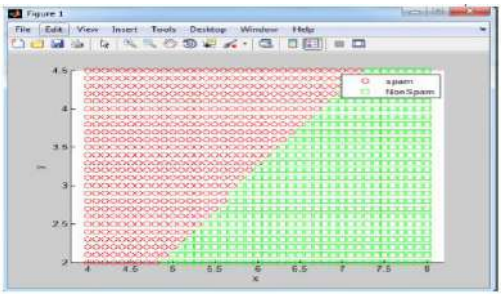


Fig 9: Scattering of mesh grid for x and y axis

Fig 10: Scattering of decision tree based evaluation

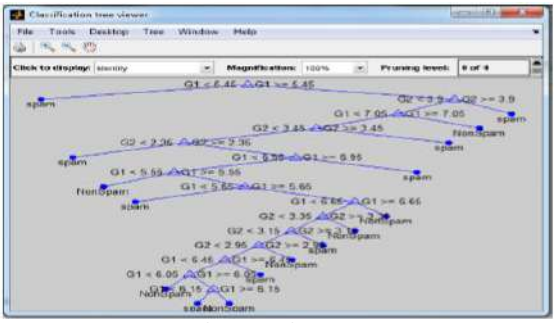


Fig 11: General classification of the email dataset.

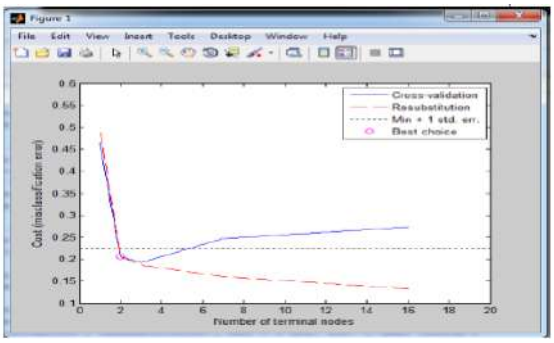


Fig 12: Plotting the best choice

Table2.Calculation of cost and secost of nodes

Cost	Secost
0.2733	0.0362
0.2467	0.0347
0.1933	0.0305
0.2067	0.0305
0.4667	0.0407

Table3.Calculation of n term nodes and resubcost of nodes

Ntermnodes	Resubcost
16	0.1333
7	0.1600
3	0.1867
2	0.2067
1	0.5000

Best Level=3

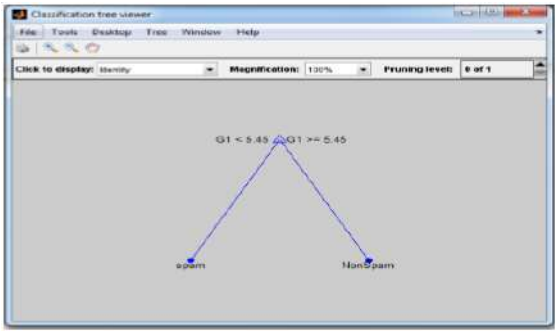


Fig 13: Best Level using Decision Tree Classification

Therefore the final cost of the bestlevel = cost(bestlevel+1) = 0.2067

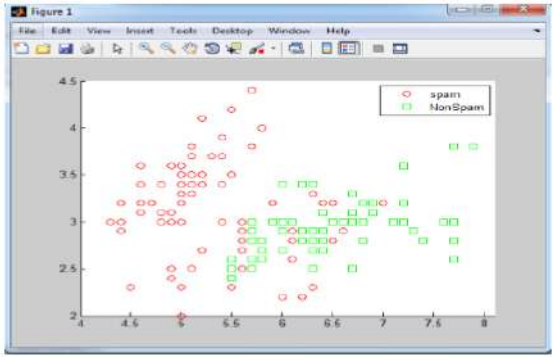


Fig 14: Classification plotted using decision tree Classifier

Table 4.Comparision of data mining techniques

Classification	Misclassification	Error
Linear Resubstitution error	28	0.1867
Quadractic Resubstitution error	25	0.1667
Naïve Bayes	**Misclassification**	**Error**
Gaussian Resubstitution error	30	0.2000
Gaussian cross validation Resubstitution error	30	0.2000
Kernel distribution	28	0.1867

Resubstitution error		
Kernel distribution cross validation Resubstitution error	28	0.1933
Decision tree	**Misclassification**	**Error**
Resubsitution error	20	0.1333
Crossvalidation error	20	0.2533

Above calculations and comparison proves that decision tree provides the best results for the classification.

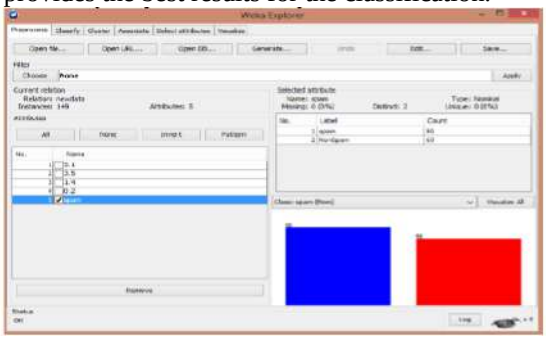


Fig 15: Visualization of the classified dataset using Weka

IV. Conclusions And Future Scope

In this paper the filtered mails are further filtered to measure the misclassification using different data mining techniques. This paper shows that the decision tree is the best classifier. It is easy to interpret and explain the executives. In comparison to random forests are time efficient. Decision tree requires relatively less effort from users for data preparation. For proper visualization and calculation, weka tool and MATLAB has been used.As a future work of our research, we can tune the parameters of our research with neural network. We can also expand the limit of our dataset while using neural network to extract more accuracy from our results.

V. References

[1] Androutsopoulos, I., Paliouras, G., Karkaletsis, V., Sakkis, G., Spyropoulos, C. D., & Stamatopoulos, P. (2000). Learning to filter spam e-mail: A comparison of a naive bayesian and a memory-based approach. arXiv preprint cs/0009009.

[2] Basavaraju, M., & Prabhakar, R. (2010). A novel method of spam mail detection using text based clustering approach. International Journal of Computer Applications, 5(4).

[3] Hovold, Johan. (2005, July). Naive bayes spam filtering using word-position-based attributes. In Proceedings of the 2nd Conference on Email and Anti-Spam (CEAS 2005).

[4] Jin, X., Wang, L., Lu, Y., & Shi, C. (2003). MC-tree: Dynamic index structure for partially clustered multidimensional database. Tsinghua Science and Technology, 8(2), 174-180.

[5] Liu, P. Y., Zhang, L. W., & Zhu, Z. F. (2009). Research on e-mail filtering based on improved Bayesian. Journal of Computers, 4(3), 271-275.

[6] Rajput, Arjun., & Toshniwal, D. Adaptive Spam Filtering based on Bayesian Algorithm.

[7] Rennie, J. (2000, August). ifile: An application of machine learning to e-mail filtering. In Proc. KDD 2000 Workshop on Text Mining, Boston, MA.

[8] Sahami, M., Dumais, S., Heckerman, D., & Horvitz, E. (1998, July). A Bayesian approach to filtering junk email. In Learning for Text Categorization: Papers from the 1998 workshop (Vol. 62, pp. 98-105).

[9] Song, Y., Kołcz, A., & Giles, C. L. (2009). Better Naive Bayes classification for high-precision spam detection. Software: Practice and Experience, 39(11), 1003-1024.

[10] Prajwala T R(2015).A comparative study on decision tree and random forest using R tool.International journal of advanced research in computer and communication engineering.(vol.4 196-1)

[11] Christina V et al(2010).Problems associated with spam and spam filtering methods.

[12]Konstantious V. Chandrinos,Constantine D.spyropoulos(2000).To detect the spam Naïve Bayesian is trained automatically.

[13] Xiaoming JIN,Yuchang LU et al (2003).Indexing problem in dataset composed of partially clustered data.

[14] Rachna mishra,Ramjeevan Singh Thakur et al (2014).An efficient approach for supervised learning algorithms using different data mining tools for spam categorization.Journal IEEE.

[15] Jehad Ali,Rehanullah khan,Nasir Ahmad,Imran Maqsood(Sep 2012).Random Forests and Decision trees .Journal IJCSI.

Analysis of Healthcare in Data Mining

[1] Lakshmi K, [2]Megha R , [3]Abhilasha B K

[1]Asst.Prof, [2,3] UG Scholar, [1,2,3]Dept.CSE, VKIT, Bangalore,

lakshmikumesh@gmail.com , megharanganth459@gmail.com , abk1619@gmail.com

Abstract- Data Mining is the area of research which means digging of useful information or knowledge from previous data. There are different techniques used for the data mining in different fields. One of the rapid growing fields is health care industries. The medical industries have great amount of data set collections about diagnosis, patient details and medications. To turn these data into useful pattern and to predict forthcoming trends, data mining approaches are used. In this paper the diagnosis of heart disease with reduced number of attributes are involved. Analysis of Dengue fever causes, symptoms and prevention of the disease is discussed. The disease recognition and classification approaches are specific to human organ and image type. One of such disease class includes detection of retinal disease such as glaucoma detection. This paper also contains the information of glaucoma disease.

Keywords-Data Mining, Healthcare

I. INTRODUCTION

Data Mining is one of the most vital and motivating area of research with the objective of finding meaningful information from huge data sets. In present era Data Mining becoming popular in healthcare field because there is a need of efficient analytical methodology for detecting unknown and valuable information in health data. In health industry, Data Mining provides several benefits such as detection of the fraud in health insurance, availability of medical solution to the patients at lower cost, detection of causes of diseases and identification of medical treatment methods. It also helps the healthcare researchers for making efficient healthcare policies, constructing drug recommendation systems, developing health profiles of individuals *etc*.This paper explains the analysis of some diseases in healthcare.

II. DATA MINING

Data Mining appeared as a powerful tool that is suitable for fetching previously unknown pattern and useful information from huge dataset. Various studies highlighted that Data Mining techniques help the data holder to analyze and discover unsuspected relationship among their data which in turn helpful for making decision. In general, Data Mining and Knowledge Discovery in Databases (KDD) are related terms and are used interchangeably but many researchers assume that both terms are different as Data Mining is one of the most important stages of the KDD process. The knowledge discovery process are structured in various stages whereas the first stage is data selection where data is collected from various sources, the second stage is pre - processing of the selected data, the third stage is the transformation of the data into appropriate format for further processing, the fourth stage is Data Mining where suitable Data Mining technique is applied in the data for extracting valuable information and evaluation is the last stage as shown in fig 1.

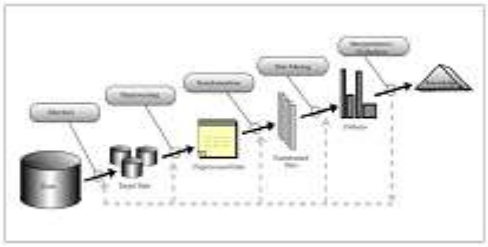


Fig 1: Stages of knowledge discovery process

The Knowledge Discovery in Databases process comprises of a few steps leading from raw data collections to some form of new knowledge. The iterative process consists of the following steps:

Data cleaning: also known as data cleansing, it is a phase in which noise data and irrelevant data are removed from the collection.

Data integration: at this stage, multiple data sources, often heterogeneous, may be combined in a common source.

Data selection: at this step, the data relevant to the analysis is decided on and retrieved from the data collection. Data transformation: also known as data consolidation, it is a phase in which the selected data is transformed into forms appropriate for the mining procedure.

Data mining: it is the crucial step in which clever techniques are applied to extract patterns potentially useful.

Pattern evaluation: in this step, strictly interesting patterns representing knowledge are identified based on given measures.

Knowledge representation: is the final phase in which the discovered knowledge is visually represented to the user. This essential step uses visualization techniques to help users understand and interpret the data mining results.

III. HEALTHCARE

There will be many advantages of the Data Mining in Healthcare e.g. it may provide benefits of grouping the patients having similar type of diseases or health issues so that they can be provided with effective treatments, check or provide availability of medical solution to the patients at lower cost, safe healthcare treatment, reducing the time for medical treatment, providing detection of causes of diseases and identification of medical treatment methods and efficient use of other resources etc. It also helps the Healthcare organizations and experts in making efficient healthcare policies. Some of the healthcare issues we have analyzed are mentioned below.

A. Heart Diseases

Now a day's Heart or Cardiovascular diseases are the very hot issue in Healthcare industry globally. In April 2011, World Health Organization (WHO) published the latest data. According to that, Coronary Heart Disease deaths reached 15.36% of total deaths in one of the country and according to World Health Organization by the year 2030 more than 23 million people will die annually from heart diseases.

Human's life fully depends upon the efficient working heart without any break or pause. The term heart or cardio disease refers to such disease that related to the heart and its blood circulatory system. It is a general name for a wide variety of diseases and disorders that affect the heart and sometimes the blood vessels as well. These are caused by disorder of heart and its pumping system. That may results illness, disability or may be death.

- **Factors Leads To Heart Diseases And Treatments To Avoid Them**

There are number of factors that increase the risk of heart disease. These factors are, Family history, Hyper Tension, Blood Pressure, Cholesterol, Smoking or Tobacco, Poor or Unhealthy Diet, Physical Inactivity etc.

In early stages, many Heart Diseases can be avoided by the patients itself from some preventive measures which includes regular exercise, healthy and well balanced diet, avoid smoking, maintaining the normal healthy weight etc. Risk factors such as diabetes, cholesterol, hyper-tension etc can also be controlled or prevented through regular medicine care and by changing life style. Critical type of heart disease such as heart attack, heart failure or stroke require hospitalization, and the treatment for these diseases include supplement amount of oxygen that is deliver to the heart tissues. It also includes monitoring of vital signs and advance life support measures.

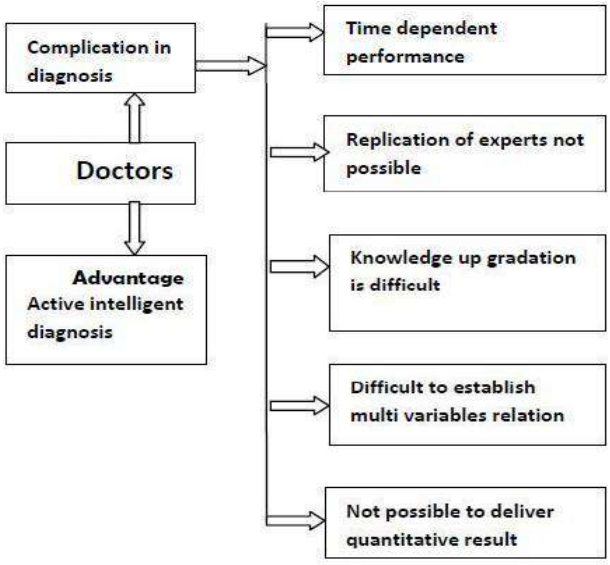


Fig 2: Traditional ways of making decisions

Clinical decisions are often made based on doctor's instinct and experience rather than on the knowledge, rich data hidden in the database. This practice leads to unwanted biases, errors and excessive medical costs which affects the quality of service provided to patients. Wu, et al proposed that integration of clinical decision support with computer-based patient records could reduce medical errors, enhance patient safety, decrease unwanted practice variation, and improve patient outcome. This suggestion is promising as data modeling and analysis tools, e.g., data mining, have the potential to generate a knowledge-rich environment which can help to significantly improve the quality of clinical decisions.

- **DATA SET**

We have taken 14 attributes from medical data. These fourteen attributes are listed in fig 3. For simplicity, categorical attributes were used for all models. The number of attributes is reduced to six using Genetic Search are listed in fig 4. The reduced data set is fed to the three classification models.

S.N.	Attribute Name	Description
1	Age	Age in years
2	Sex	Male=1.Female=0
3	Cp	Chest pain type
4	Rbp	Resting Blood pressure upon hospital admission
5	Cholesterol	Serum Cholesterol in mg/dl
6	Fasting blood sugar	Fasting blood sugar>120 mg/dl true=1 and false=0
7	Resting ECG	Resting electrocardiographic Results
8	Thalach	Maximum Heart Rate
9	Induced Angina	Does the patient experience angina as a result of exercise (value 1: yes, value 0: no)
10	Old peak	ST depression induced by exercise relative to rest
11	Slope	Slope of the peak exercise ST segment
12	Thal	Value 3:Normal ,value 6:fixed defect, value 7: reversible defect
13	CA	Number of major vessels colored by fluoroscopy(value 0-3)
14	Concept class	Angiographic disease status

Fig 3: Attribute of Heart Disease Data Set

S.N.	Attribute Name	Description
1	Rbp	Resting Blood pressure
2	Oldpk	Old peak
3	Type	Chest pain type
4	Vsl	Number of major vessels colored
5	Eia	Exercise induced angina
6	Thal	Maximum heart rate achieved

Fig 4: Reduced Attribute List

B. Dengue Fever

Dengue fever is disease transmitted by mosquitoes and causing sudden high fever and pains in the joints. Also known as break bone fever. The first case was detected in the Philippines in 1953, the disease is identified as one of the most dangerous disease in the humans. Accurate prediction of this disease is possible only after several tests of laboratory and clinical symptoms.

A multi variant model was constructed for predicting Dengue by testing hemoglobin using predictors i.e., they have used various attributes such as vomiting sensation, weight, sex and other factors. These techniques are used only after two to twelve days from the day of illness. The world health organization is made classification for identifying affected individual persons based on the laboratory and clinical symptoms. The models developed for the diagnosis of dengue fever is affected by missing values and influential features. This may be due to incorrect data entry or not collected properly at the time of data collection.

In order to avoid incorrect prediction, we follow a procedure as below

1) A manual missing value imputation method is used.

This reduces the false value entry. So that our results will

improve marginally.

2) For selecting the most influential attributes that predict

The dengue fever we took expert doctors opinion and Internet survey. This process reduces collecting unnecessary attributes during data collection. This helps in accurate prediction of dengue fever.

3) After preprocessing the data we use neural networks for predicting dengue fever. This will be implemented by

using MATLAB 2013a. So as we are expected this method gave accurate results as explained in the implementation section.

System Architecture:

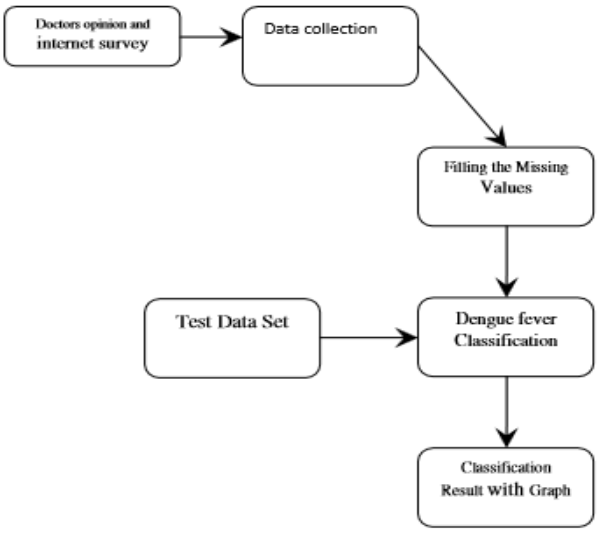


Fig 5: System Architecture

IV. IMPLEMENTATION:

Data collected is tabulated and missing values are filled manually with appropriate normal values. This makes to get the prediction values more accurate. The data collected is of mixed data. That is it includes categorical data and numerical data. So for the data to be used in MATLAB it should numerical data for neural networks. The dengue fever dataset collected can be used to predict the new dengue fever case.

a. Retinal Diseases

Retinal Disease detection locates and segments Retinal Disease regions from cluttered images, either obtained from video or still image. It has numerous applications in areas like surveillance and security control systems, content based image retrieval, video conferencing and intelligent human computer interface. Most of the current Retinal Disease recognition systems presume that retinal disease is readily available for processing. However, we do not typically get images with just Retinal Disease.

Retinal Disease detection remains an open problem. Many researchers have proposed different methods addressing the problem of Retinal Disease detection. In a recent survey Retinal Disease detection technique is classified into feature based and image based.

Medical image processing and analysis is a technique and science to detect degenerated tissue. The main advantage of medical imaging is to make diagnosis as possible as noninvasive way in the treatment planning and clinically diagnosis. There are various types of medical imaging technologies based on noninvasive approach like Computed Tomography (CT), Magnetic Resonance Imaging (MRI) and X-Ray etc. The disease recognition and classification approaches are specific to human organ and image type. One of such disease class includes detection of retinal disease such as glaucoma detection or diabetic detection.

- **Glaucoma Disease**

Glaucoma is a progressive degeneration of retinal ganglion cells (RGC) and their axons, resulting in a distinct appearance to the optic nerve head (ONH), often called „cupping". Glaucoma leads to visual disability. This damage also leads to improper functioning of drainage system of eye leading to increased intra-ocular pressure. Glaucoma is the third leading cause of blindness.

The below method is about the detection of retinal Glaucoma disease in optical retinal images.

This methodology includes following steps:

- Data Acquisition
- Preprocessing
- Processing
- Classification or Segmentation

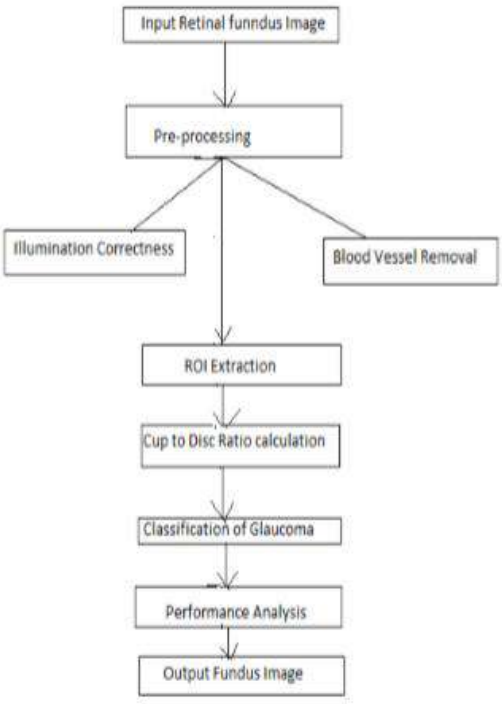


Fig 6: Methodology for detection of glaucoma disease

IV.CONCLUSION

In this paper the various data mining application in the healthcare domains are analyzed to discover new range of pattern information. There is a variety of data mining tools and techniques available for health care diagnosis systems that are defined in this paper. This data mining based prediction systems reduces the human effects and cost effective one. Large amounts of heterogeneous medical data have become available in various healthcare organizations. The rate of electronic health record (EHR) adoption continues to climb in both inpatient and outpatient aspects. Analyzing the massive amount of healthcare information that is newly available in digital format should enable advanced detection of powerful treatment, better clinical decision support and accurate predictions of who is likely to get sick. This requires high performance computing platforms and algorithms. In this paper some techniques of Data mining are compared for predicting Heart Disease with reduced number of attributes. Inconsistencies and missing values were resolved before model construction but in real time, that is not the case. Also, the intensity of the disease based on the results was unpredictable. Heart disease is a fatal disease which may cause life threatening complications such as death. We use online available heart patient's data from UCI repository. This study shows that the data mining can be used to predict about heart disease efficiently and effectively.

A multi variant model constructed for predicting Dengue by testing hemoglobin using predictors. The models developed for the diagnosis of dengue fever is affected by missing values and influential features. This may be due to incorrect data entry or not collected properly at the time of data collection is discussed. The paper has defined the basic filtration model to improve the image features so that effective disease recognition will be done. Paper also described the work on disease recognition and classification approaches.

V. REFERENCES

[1] Muhamad Hariz Muhamad Adnan, Wahidah Husain,Nur'Aini Abdul Rashid, *"Data Mining for Medical Systems: A Review*".

[2] Hian Chye Koh and Gerald Tan." *Data Mining Applications in Healthcare*".

[3] M. Durairaj, V. Ranjani*," Data Mining Applications in Healthcare Sector: A Study"*, International Journal of Scientific & Technology Research Volume 2, Issue 10, October 2013.

[4] Chaitrali, S., D. Sulabha and S. Apte, "Improved study of heart disease prediction system using data mining classification techniques"

[5] Jawei Han and Micheline Kamber, "Data Mining: Concepts and Techniques," Morgan Kaufmann Publishers Inc.,

[6] Soni, J., U. Ansari, D. Sharma and S. Soni, "Predictive data mining for medical diagnosis: An overview of heart disease prediction," Int. J. Comput. Applic. 17: 43-48.

[7] Obenshain, M.K: "Application of Data Mining Techniques to Healthcare Data", Infection Control and Hospital Epidemiology, 25(8), 690–695, 2004.

[8] R. B. Rao, S. Krishan, and R. S. Niculescu(2006), "Data mining for improved cardiac care," ACM SIGKDD Explorations Newsletter., vol. 8, no. 1, pp. 3–10.

[9] Greg Rogers and Ellen Joyner, "MINING YOUR DATA FOR HEALTH CARE QUALITY IMPROVEMENT", SAS Institute, Inc.,
Cary, NC, January 1, 2009.

[10] Two Crows Corporation,"Introduction to Data Mining and Knowledge Discovery. Third Edition." Two Crows Corporation. 10500 Falls Road, Potomac, USA, 2005.

[11] KEITH P. THOMPSON," Therapeutic and Diagnostic Application of Lasers in Ophthalmology", 00189219/92@1992 IEEE [12] Jim Beach," Spectral Reflectance Technique for Retinal Blood Oxygen Evaluation in Humans", Proceedings of the 31st Applied Imagery Pattern Recognition Workshop (AIPR.02) 0-7695-1863-X/02 © 2002 IEEE

Empirical Study of Internet Usage in Health Care Informatics

Kumuda.S[1], Manu.M[2] , Govindraju.A[3],Bhavana Gowda D M[4]
[1,2,3] UG Scholar, [4] Asst. Prof.
Dept. of CSE, VKIT, Bangalore.
rajugowda1996@gmail.com

***Abstract*—In order to achieve the change, health care organizations are reorganizing their processes. The main aim of this organisation is to reduce costs, be more competitive, and provide better and more personalized customer care. The business strategies of this organisation includes Internet applications, enterprise systems, and mobile technologies in order to achieve their desired business changes. This article gives a brief description about the conceptual model for implementing new information systems, integrating internal data, and linking suppliers and patients.**

***Index Terms*—Bioinformatics, data mining, enterprise systems, health informatics, information warehouse, mobile technology, patient relationship management, telemedicine.**

I. INTRODUCTION

This paper provides a model for health care organizations to utilize the different information system technologies that can be employed to streamline business processes, reduce administrative costs, make organizations more competitive, and ultimately provide better care to patients. Specifically, this study focuses on using the Internet as the backbone to connect suppliers, enterprise systems, physicians, and patients to one value added supply chain. Fig.1. depicts that health care organizations can use the Internet to link not only their own operations, but also the operations of suppliers and physicians, and needs of patients. The diagram shows that the Internet facilitates two-way communication between all entities in the supply chain. In addition to general communication and data exchange through the Internet, suppliers, including insurance providers and pharmaceutical companies, can access part of a health care organization's enterprise systems via secure extranets. The model also shows that internal company data can be accessed by physicians and specialists via intranets. Internet is meant to enhance physician-patient relationship by making both physicians and patients better informed.

II. INTERNET APPLICATIONS

Internet can serve as the backbone for implementing supply chain solutions to add value to health care providers, their suppliers, and their patients. Even though health care information systems in some hospitals and clinics have been linked together with a local area network or a wide area network, network based health care systems have not been popular until the advent of the Internet. The three primary Internet applications that the healthcare industry uses, to varying degrees, are the Internet, intranets, and extranets.

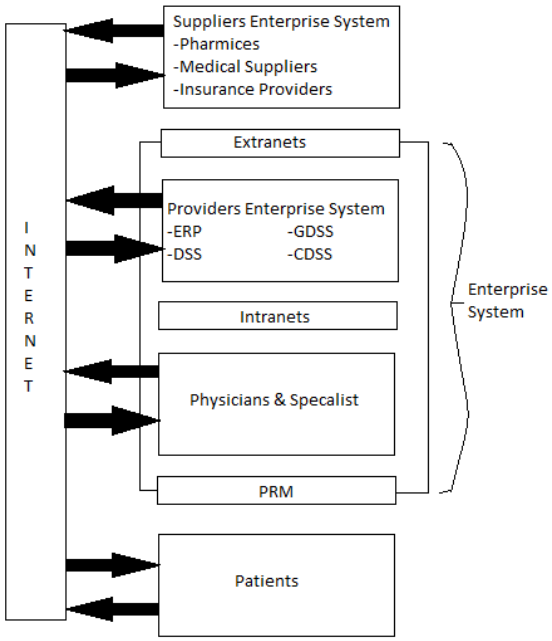


Fig.1. Health care supply chain.

A. The Internet

The use of the Internet by health care providers, and certainly their patients, has seen dramatic increases in the past few years. For example, one study shows that 60 million adults sought out health care information on the Web in 1998, and 91% of them found what they were looking for. The estimated 60 million in 1999 has since sky rocketed; a Harris poll in August of 2000 shows that 98 million adults have used the Web to find health information. Based on the results of another study done by the Health Information Management Systems Society, 87% of its members were using the Internet. Another survey

noted that most researchers, patients, and doctors had access to medical information systems through the Internet. There are many reasons for this explosive growth, including faster connections, and greater trust in Internet security, as well as the added convenience of the Web.

The dramatic increase in the popularity of the Internet means tha16t health care providers are left with the decision to either capitalize on the new e-world, or being left behind. The key benefits include allowing physicians and specialists from across the globe to share vital health care information. Also, the Internet has the capability of allowing patients to self-select themselves to view information on the Internet, and apply their own disease management and prevention. A third primary benefit that the Internet has to offer the health care industry is its unique ability to enable telemedicine, which brings health care to an entire new level.

1) The Internet as a Physician Tool: Internet technology can facilitate the distribution of important medical information and knowledge to the medical community. This includes use by health practitioners to locate useful medical information on the Web. Online services, browsers, and query languages, allow physicians access to immediate information without having to sift through piles of outdated health care journals. This serves to reduce the amount of time that providers need to spend researching clinical information, and will allow them more time to spend with their patients. The Internet allows quick and seamless information exchange between providers from across the globe. This is already taking hold as a 1999 survey showed that 63% of physicians used e-mail on a daily basis. This percentage is also likely to be much higher now, as many more physicians have adopted Internet technology in the last two years. This communication is enabled by the Internet's open architecture and connectivity. Ruffin claimed that the Internet provided the technical design necessary for standardized, vendor-independent, computer-based patient records to flourish. Thus, with the expanding capability, and quicker connection and transmission speeds, physicians are able to communicate with each other about the best and proper treatment for patients with specific symptoms. This type of collaboration will allow more knowledge transfer, and will ultimately lead to more satisfied customers, as appropriate care decisions are made.

Doctors can use the Internet to do more than download information and communicate with other providers; it can also be used to send complex medical files across the Web. One specific application of this technology is being applied in the Boston area, where neurosurgeons and trauma physicians receive encrypted radiological image files in their homes and offices via a high-speed cable modem. Applying this technology makes use of a virtual private network (VPN), in which private information is encrypted and sent across a public network, thus providing the communication capability of a public network but with the security of a private network. If this technology proves to be successful, it will save doctors' time, because hospital visits can be reduced, and decisions can be made from a remote location. This will provide physicians with more up-to-date information and will free up more of their time to focus on patient care, rather than performing administrative tasks.

2) The Internet as a Patient Tool: The second major benefit to utilizing e-health care initiatives is that online access allows patients to be better informed about how exactly they can manage their own health, as well as prevent diseases. The Internet allows customers to gain up-to-date information so that they no longer have to rely on outdated or irrelevant general health data. Rather, they have immediate access to health information when they need it. For example, one online health site, WebMD.com, gives patients tools such as access to important health care records, diet and fitness journal, doctor searches, as well as immunization and pregnancy planners. Web sites like WebMD allow a large and growing group of consumers to use the Internet as their primary resource on health and medical matters. This creates an additional benefit for the health information provider, because people seeking out the provider's Web site are "self-selected." Unlike mass advertising campaigns, where information is delivered to everyone regardless of their interest, the provider can be sure that the consumer who accesses the site wants specific information.

The Internet's global access allows patients in remote areas who may be suffering from very rare diseases to interact with one another via e-mail and chat rooms. This can be very beneficial to patients because they no longer have to feel like they are in the struggle alone, but rather they have others to share ideas and treatment plans with. These support groups are generally comprised of very skilled e-patients. E-patients are a new breed of patients who are using the Internet to gain specific knowledge about their symptoms and treatments, as well as using the Web to track down nearly every lead they can find on the best type of new treatment. Some patients have even gone as far as starting their own Web sites to give support, information, and advice to other patients suffering from similar afflictions. For example, one patient suffering from lung cancer started her own Web-site which offers access to detailed information about lung cancer, listings of specialists, and clinical trial information, as well as support groups and survivors' stories. Local health care providers

need to be aware of the impact of the Internet, and use the Internet to their advantage by providing their own interactive sites, and not allowing their patients to slip away to other providers who reacted more quickly to the e-revolution.

3) The Internet and Telemedicine: Telemedicine is one of the hottest trends currently engaging the health care industry. One survey found that in 1998, 139 interactive telemedicine programs were found in the U.S., which was an increase from three in 1993. The idea behind telemedicine is to provide more convenient and more customized care to patients, using such technologies as Web TV, smart phones, and wireless devices to interact with patients in their homes. While this type of technology is currently in its infancy, many health care professionals are seeing the potential benefits of telemedicine. Possible telemedicine services range anywhere from scheduling appointments online, to performing remote surgical procedures directed by a surgeon to a nonsurgeon via high bandwidth technologies and video cameras. These services will allow patients to bring up appointment books online, schedule appointments online,receive custom designed messages on their PDA or cell-phone reminding them of their appointments, and reminders to refill prescriptions. This interaction allows patients to take a more active role in their health care.

B. Intranets

The second major Internet application that promises to affect the health care industry is the intranet. An intranet is a collection of inter-connected networks within an organization, usually based on Internet technologies. Intranets are important technological tools that can be used by health care organizations to provide efficient and more effective service to their patients. These benefits come from allowing physicians access to comprehensive internal enterprise systems that can store detailed information about possible treatments and patient records. Hospitals are rapidly adopting intranet technology. The growth in medical intranets can be attributed to its various advantages including: 1) low-cost connectivity; 2) ease of rapid deployment of the technology; 3) use of cross-industry communications standards; 4) user-friendliness; 5) short training times; 6) reduced network administration costs; 7) the ability to extend the value of legacy systems; and 8) the ease of development of strategic links between healthcare organizations and outpatient providers including physicians.

As a pioneering effort in connecting different systems by using Internet technology, a number of medical intranets have been developed and implemented for different purposes. For members of the health care community, offering health care information and sharing data have many benefits. First, physicians can search internal patient medical records that have been stored by the specific organization, use clinical decision support systems, and research specific topics that have been stored by internal enterprise systems. Administrative employees can access the database to deal with billing and insurance. To date, intranet applications have been widely used as a tool of knowledge diffusion within the medical community rather than for patient care. Specific medical intranets have been used mostly to improve knowledge diffusion via the Web. MEDLINE, controlled by the National Library of Medicine, maintains medical literature from the past 30 years. Another example is CliniWeb. CliniWeb is an index of clinical information, which is designed for retrieving specific clinical topics on the Web. It provides an index of clinical information for health care students, providers, and researchers via the Web. CliniWeb is an exclusive intranet that furnishes only clinical information by organizing clinical resources with a specific topic, so that only specified users can access the information.

C. Extranets

The third and newest Internet application to be used by the health care industry is the extranet. Simply put, extranets are networks, again usually based on Internet technologies, built between a core business and the other members of its value chain, on both the supply and demand sides. Extranets are not currently widely used in the health care industry. An InternetWeek study revealed that while 92% of health care respondents host informational sites, only 20% are currently participating in extranets or supply chain networks. Extranets offer a way to link services in a more timely and efficient manner. Extranets are less cumbersome and restrictive than an electronic data interchange (EDI) system. Extranets can also be used to streamline transactions between providers and their suppliers to the benefit of both.

Extranets offer another unique capability to the health care industry—secured connectivity. Consequently, heath care providers, including physicians, hospitals, pharmacists, lab researchers, and dentists, would be able to utilize those patient records and information to the betterment of the health care community. Extranets are the key for this integration to occur, because they reduce the need for a centralized database, that would undoubtedly be too large to manage. Using extranets, key patient and clinical data are available on the Web, but accessible only through a secure connection.

In order for data repositories to be implemented, computerized patient records must be developed before anything else. A universal electronic patient record could be defined as electronically stored health information about one individual recognized by a unique identifier. Efforts are already underway to build a universal computerized patient record by the Computer-based Patient Record Institute in Schaumburg, IL. However, because of several obstacles, including costs, lack of network standards, and difficulty of transferring data to systems from charts, no universal method is currently available.

On an administrative and inventory control basis alone, extranets should benefit the health care supply chain. With the advent of computerized patients records, extranets can be used to link health care providers together to provide better clinical care. Extranets also play an important role in integrating the supply chain, because they allow different organizations to access a part of each other's internal data via Internet connections.

III. ENTERPRISE SYSTEMS

Enterprise systems include a company's internal applications, such as enterprise resource planning (ERP) systems, customer relationship management (CRM) systems, data mining and data warehousing programs, as well as the various models of decision support tools that can be used in the health care industry. These different software tools can be used in a powerful way in the health care industry to not only integrate enterprise data, but also to provide important information and forecasting data to provide improved patient care.

A.ERP

ERP technology has made a tremendous impact on the business world in the past few years. What these packages promise is the full integration of an organization's information, from payroll and human resources to accounting and finance; with each functional business unit being represented and supported by an ERP module. Utilizing ERP systems in the health care industry offers several advantages. One of the primary benefits of ERP systems to the health care industry isits integrated database. This means that all of the organization's information is encapsulated in one place, which makes it possible to reduce administrative costs by eliminating some of the manual processes. This can help to solve the problem of overrunning physician's desks with paper, and will free them up to focus more upon patient care. Having the systems integrated also streamlines data entry, which saves office workers' time, and ensures that everyone in the organization is working with the same information. Another administrative benefit of ERP systems to the health care industry is that one system can be used to track inventory, order information, and delivery requirements. This means that health care organizations can better plan and organize for receipt of inventory goods, as well as always have access to a real time inventory status. In addition, ERP systems can be used to determine equipment usage and maintenance schedules. ERP systems allow information to be stored in a shared database, so that information on maintenance schedules can automatically retrieved, and crossed with other information such as number of beds in use, to determine when and where demand is greatest for a specific piece of equipment. In addition to reducing administrative tasks, and streamlining processes, ERP systems can also be used on the clinical side of the business to store useful patient education information. ERP systems allow doctors to store common disease management techniques inside the system, so that this information can be easily accessed and disseminated to patients. This will not only save the physician time, but will also allow for better patient care. An additional piece of an organization's enterprise systems that can be used in the health care industry are decision support systems (DSSs).

B. DSSs

Unlike the earlier healthcare DSSs that focused on financial and scheduling domains, current decision systems can be used for diagnostic situations in health care specialties including pharmacy, emergency, and nursing practices. DSSs can be used to store standard diagnostic techniques for disease management, and can be used as a cross check against a patient's records, in order for a physician to apply the appropriate individualized care for the given patient. For example, clinical decision support systems (CDSS) can be used to send alerts and reminders to patients about preventive care. In this way, CDSS can be used in telemedicine to communicate critical information with patients about their care. For instance, a patient may use the Internet to log-on to their health care provider's Web site and place their current blood pressure readings, as well as diet information, and a CDSS can be used to analyze that information and send information alerts to patients who may be at risk of heart problems. In addition to its own ability to store and analyze current medical information and patient records,

DSSs can also be utilized on a group basis. Recently, group DSSs (GDSSs) have been developed in many non-health care organizations to assist in the decision making process of group members by broadening the quantity, quality, and structure of data exchange. Since all of patients information can be stored in one place, and all of that information can be accessed via secure channels, several physicians will be

able to view the information, and advise the primary physician of proper treatment techniques. This puts the old adage of "two heads are better than one" into play, in which each physician can analyse his own experience and contribute ideas to the care of the given patient.

C. Patient Relationship Management (PRM)

Patient relationship management (PRM), or more commonly known as customer relationship management (CRM). PRM is a software tool that places an organization's primary focus on determining and meeting patient needs. PRM involves tracking patient information from diet and exercise data, to past diagnosis information, to family history, and allergy information. By storing all of this information, health care providers will be able to send e-mails to patients about newly published health care studies that may be of interest to the patient, or offer specialized prescriptions that may fit a certain patient profile. This information could also be used to automate certain call center operations, in which routine advice for certain ailments can be made available at the call center without having to distract nurses or physicians from their primary care duties. The general guideline in the business world is that customer emails requesting information should be answered within two to four hours. This type of online support will provide better care, because patients will be able to ask questions of their providers whenever they need to, and providers will have time to review pertinent health information and patient records to supply adequate answers. Another important feature of PRM is that it will help to build loyalty between patients and providers. This is possible because in a PRM strategy the health care organization has taken the time to learn about the patient, and the patient has taken the time to give information, therefore with the nature of the time investment and the personalized care, patients are more likely to stick with the health care provider that knows them and their preferences

The bottom line is that an increased understanding of patients needs and wants will help health care organizations to provide better care. This is essential for providers trying to manage and prevent disease, because information can be disseminated much easier without having to mass market all information on a particular disease to all the people accessing a Web site or receiving newsletters. This personalized touch will become a critical success factor in the health care industry, and serves as one more option for health care providers to use information systems to improve the care they provide.

C. Information Warehousing Tool

An information warehouse is a collection of integrated, subject-oriented databases designed to support decisionmaking. Information warehouse is seeing new applications on the clinical side of patient care. For instance, pharmaceutical makers are using information warehousing for marketing purposes and health care providers are using information warehousing for diagnosis and treatment of patients. One example in the pharmaceutical industry is Glaxo Wellcome in
London, who has implemented information warehousing for the analysis of drug demands. Also, Pfizer Incorporated, a pharmaceutical firm based in New York, has implemented information warehousing that supports 2700 sales representatives in furnishing doctors with detailed and specific drug information regarding the effectiveness of drugs, side effects, and costs.

In addition to using information warehousing for pharmaceutical purposes, information warehouse tools can be used for patient data and care. For instance, Kaiser Permanente, the largest and oldest HMO in the United States, has employed information warehousing containing diabetic data for accurate and proper treatment of diabetics. Taking this initiative a step farther is Patient Infosystems, which uses personal computers, Internet applications, and telephones to allow diabetic patients to enter their glucose levels into an online application that can be monitored by qualified physicians. This information can then be backlogged into an information warehouse, which can be used as an information store for future clinical use by physicians. This represents an exciting new avenue because the information stored in the information warehouse can be stored, mined, and analyzed to provide better and more accurate care to patients.

D. Data Mining Tools

Applying data mining techniques to information warehousing in the health care industry is becoming more and more common. Data mining permits health care providers to save costs, provide better care, and save lives. Sentara Health System at Norfolk introduced a data mining concept to improve the quality and the treatment of pneumonia patients. Growth in the use of data mining techniques in the health care industry will provide more information to physicians, so that better care decisions can be made.

IV. FUTURE TECHNOLOGY—MOBILE HEALTH CARE SYSTEMS

Mobile communications offer two distinct advantages to the health care world. First, mobile technologies are important for telemedicine success. While certain media that are

already in place, such as televisions and telephones, offer avenues for telemedicine deployment, mobile communication offers another avenue that can also be used in conjunction with telemedicine. Personal digital assistants can be used by physicians to send instant messages to patients reminding them when they need to take their medication. This will serve to eliminate certain administrative and insurance costs that are associated with hospitalizations that result from not taking the prescribed medication at the correct time. This is important because a study done by the National Council of Patient Information and Education, revealed that 50% of patients are either not taking their medications at all, or not taking it according to schedule, which correlates to an average of 10% of hospital visits that are caused simply because medications were not taken at the prescribed time.

Second, mobile devices and the wireless Internet allow physicians to access information anywhere at any time. This is an important benefit for providers, because real-time information is essential for physicians and hospitals, and mobile devices provide that capability. Although, this functionality is still not completely developed, Oracle, PeopleSoft, and SAP all have releases that will support a portion of their enterprise software on hand-held devices.

V. DISCUSSION AND CONCLUSIONS

Three basic sets of tools can be applied to health care industry: 1) Internet applications; 2) enterprise systems; and 3) mobile technologies. These various tools can be used by health care organizations to store internal organizational information based upon its different business modules, including finance and accounting, human resources, payroll information, etc. Also, health care organizations can use these numerous technologies to provide better patient care, by not only obtaining more information from patients, but also giving more information on self-care and disease management to patients. Better care can also be provided using such enterprise applications as decision support tools, PRM applications, information warehousing and mining, as well as Internet applications such as telemedicine, which can be used to personalize care and make care more convenient for patients who can access information from anywhere. Mobile technology will also make physicians' jobs easier, because information will be available on smaller communication devices, such as mobile phones and PDA's. Not only will this help physicians to work from anywhere, and collaborate with other physicians and specialists online, it will also save them administrative time, which will translate into more value added time for the health care provider and ultimately the patient. These tools also promise to link the supply chain, giving suppliers the access to internal information will result in reduced inventory costs, and faster delivery of medicines and other health care devices.

While these technologies do offer health care organizations options to provide better care and reduce costs, none of the technological devices discussed in this research are meant to replace the physician–patient relationship. Instead they seek to enhance that relationship by reducing administrative time and costs, providing more accurate patient record information, allowing for shared decision making, and offering more timely patient care.

REFERENCES

[1] C. Clark, "Healthcare information systems," in *e-Healthcare*, D. E. Goldstein, Ed. Gaithersburg, MD: Aspen, 2000, (1995), 679, pp. 300– 301.

[2] A. Maitra, *Building a Corporate Internet Strategy: The IT Manager's Guide*. New York: Van Nostrand, 1996.

[3] T. Wilson. (2000, Oct. 30) The focus is care, not the business: Web data and diagnostics, physician collaboration take precedence over supply chain. *InternetWeek* [Online]. Available:http://www.internetweek.com/transformation2000/industry/healthcare.htm

[4] D. Howcroft and N. Mitev, "An empirical study of Internet usage and difficulties among medical practice management in the UK," *Internet Res.*, vol. 10, no. 2, pp. 170–181, 2000.

[5] D. E. Goldstein, *e-Healthcare: Harness the Power of Internet eCommerce& e-Care.* Gaithersburg, MD: Aspen, 2000.

[6] J. Anderson, "Clearing the way for physicians' use of clinical information systems," *Communications of the ACM*, vol. 40, no. 8, pp. 83–90, Aug. 1997.

[7] (1999, May 6) Research shows 42% growth in physician use of the Internet in the last three months. *Healtheon Corp. Internet Survey Med.* [Online]. Available: AOLNews@aol.com

[8] L. Nicholoson, *The Internet and Healthcare*. Chicago, IL: Health Administration Press, 1999.

[9] H. Taylor, "Explosive growth of a new breed of cyberchondriacs," *Harris Poll*, vol. 11, 1999.

[10] PeopleSoft and A. Anderson, "Intranet: Powerful new tools for healthcare organizations,", White Paper, pp. 1–14, March 1998.

[11] J. Cimino, S. Socratous, and P. Clayton, "Internet as clinical information system: Application development using the World Wide Web," *J. Amer. Med. Informat. Assoc.*, vol. 2, no. 5, pp. 273–284, Sept.–Oct. 1995.

[12] M. Ruffin. The World Wide Web is coming soon to an organization near you. *Medical Intranet Forum* [Online]. Available: http://www.misforum.org/news/ruffin_soon.html/

Comparison between Arduino and Raspberry Pi in the applications of IoT

Rohit Mulay[1], Rohini T[2]

[1]UG Scholar, [2]Assistant Professor,Dept of CSE, NHCE, Bengaluru

E-Mail: rohitmulay96@gmail.com , rohini.antharmuki@gmail.com

Abstract*—The introduction of the greatest breakthrough in technology, The Internet of things (IoT) which is now an emerging topic of technical, social, and economic significance. The Internet of Things (IoT) has generated a large amount of research interest across a wide variety of technical areas. These include the physical devices themselves, communications among them, and relationships between them. When embarking on IoT projects, you have to choose the best platform to build your application. The perplexity of which platforms to be use for what kinds of projects is now a common issue as there are so many ways to solve one particular problem. It depends on what the goals and plans are for the IoT project. In this paper, we will discuss features of Arduino and Raspberry Pi, when it is most suitable to use Arduino and when to use Raspberry Pi and also talk about why is Raspberry Pi better than Arduino in the applications on IoT.

I. INTRODUCTION

Internet of Things (IoT) can define as internetworking between people, animal or object that ability to exchange data over network without involving human-to-human or human-to-computer interaction. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "the infrastructure of the information society."[1] This is an ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems like connected security systems, thermostats, cars, electronic appliances, lights in household and commercial environments, alarm clocks, speaker systems, vending machines and more.

A. Arduino

Arduino is an open-source prototyping platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing [12]. It doesn't have an operating system, or a file system. The processor on these devices is quite simple and cannot multitask between several applications. The Arduino is entirely focused on executing a specific task even if that task involves reading multiple sensors or controlling multiple components via output pins. The typical Arduino device has a very small amount of RAM, about 2KB, and 32KB of flash memory for your application storage. For data values that might change during the execution of your application, but need to be preserved, there is also 1KB of EEPROM storage. With this relatively low amount of computing power available it's easy to see why only small, highly focused applications can run on an Arduino [2]. There are many Arduino boards like Arduino UNO, Arduino PRO, Arduino MEGA, Arduino DUE etc.

Figure.1: Arduino Logo [10]

B. Raspberry Pi

The Raspberry Pi is a low cost, small and **portable size of computer board**. This series of credit card-sized single-board computers is developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and developing countries. All its models feature a Broadcom system on a chip (SoC), which includes an ARM compatible central processing unit (CPU) and an on chip graphics processing unit (GPU, a VideoCore IV). CPU speed ranges from 700 MHz to 1.2 GHz for the Pi 3 and on board memory range from 256 MB to 1 GB RAM. Secure Digital SD cards are used to store the operating system and program memory in either the SDHC or MicroSDHC sizes. Most boards have between one and four USB slots, HDMI and composite video output, and a

3.5 mm phone jack for audio. Lower level output is provided by a number of GPIO pins which support common protocols like I²C. The B-models have an 8P8C Ethernet port and the Pi 3 has on board Wi-Fi 802.11n and Bluetooth. The Foundation provides Raspbian, a Debian based Linux distribution for download, as well as third party Ubuntu, Windows 10 IOT Core, RISC OS, and specialised media center distributions. It promotes Python and Scratch as the main programming language, with support for many other languages. [3] It has several models and revisions like Raspberry Pi, Raspberry Pi 2, and Raspberry Pi Model B+ etc.

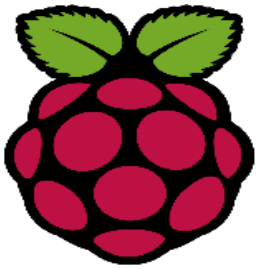


Figure.2: Raspberry Pi Logo [11]

II. MAJOR APPLICATIONS OF INTERNET OF THINGS (IOT)

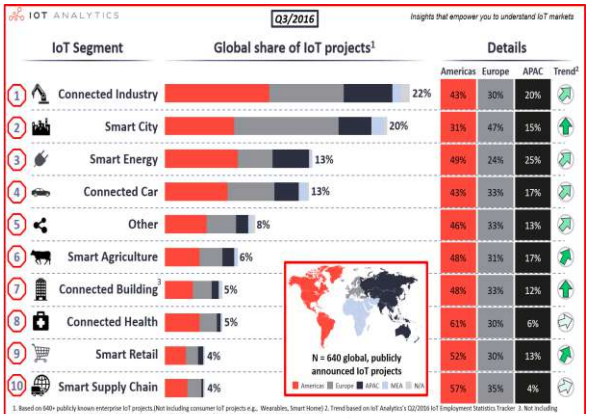


Figure.3: Global share of IoT projects [5]

Most IoT projects in connected industry Most of the IoT projects we identified are in industrial settings (141 projects), followed by Smart City (128) and Smart Energy IoT projects. The Americas make up most of those projects (44%), followed by Europe (34%). There are large differences when looking at individual IoT segments and regions. The Americas and particularly Northern America is strong in Connected Health (61%) and Smart Retail (52%), while the majority of Smart City projects are located in Europe (47%). The Asia / Pacific region is particularly strong in the area of Smart Energy projects (25%).

A. Connected Industry: Strong IoT project footprint in oil & gas and in factory environments.Connected industry is the largest IoT segment in terms of number of IoT projects. This segment covers a wide range of connected "things" such as printing equipment, shop floor machinery, cranes or entire mines. One of the largest sub-industries is Oil & Gas. The ability to remotely monitor and optimize heavy assets has resulted in a number of projects. An example is RasGas´ LNG equipment monitoring in Ras Laffan, Qatar, allowing the LNG producer to perform predictive maintenance on its assets. Manufacturing shop floors are another area of major importance for IoT. For example, German food producer Seeberger knows exactly where specific goods are at any stage of the production process allowing for complete food traceability.

B. Smart City: Traffic management and utilities driving Smart City IoT use cases

20% of all identified IoT projects are Smart City related. On top of that, the IoT Employment Statistics Tracker shows a strong upward trend on the back of hundreds of recent Smart City initiatives started by governments around the world. Prominent examples include the City of Barcelona and the City of London. The most popular Smart City application is Smart Traffic (e.g. Intel and Siemens´ Smart Parking solution in the City of Berlin) followed by Smart Utilities (e.g. Dublin´s smart bins). Other Smart City initiatives evolve around city safety. A notable (European) safety monitoring IoT project is the CityPulse IoT project in Eindhoven where the information on noise levels is matched with social media messages in order to detect and manage incidents and adjust the street lighting accordingly.

C. Smart Energy: Strong push in the US and other parts of the Americas

Both North and South America appear to be strong adopters of Smart Energy projects with nearly half of all identified Smart Energy IoT projects taking place there. The majority of Smart Energy projects can be classified as Smart Grid initiatives, an example being the American City of Fort Collins Utilities´ Smart Grid initiative. Another extensive Smart Energy project is the smart grid demonstration project on Jeju Island, South Korea, which incorporates both distributed renewable generation and advanced metering infrastructure. While typically these projects focus on increasing the efficiency and reliability of the grid, IoT technology can also be used to avoid energy theft as showcased in a project in Tucumán, Argentina.

D. Connected Cars: Largest segment making use of M2M technology Connected cars is one of the more mature IoT segments in which M2M/Cellular type of IoT connectivity has been employed for quite some time. Most Connected Car IoT Projects focus on vehicle diagnostics and monitoring. Two out of three projects can be classified as Fleet Management initiatives, an example

being Telefonica´s fleet management solution for ISS. On top of that, there are a number of usage-based car insurance projects, e.g. Unipol Sai´s black box solution. Other types of projects include real time decision support for Honda´s racing team or Daimler´s Car2Go car sharing service.

III. ARDUINO VS RASPBERRY PI

Arduino and Raspberry Pi are the most popular boards among the students, hobbyists and professionals. Experienced and professionals know the utility and differences between the two. But beginners and students often get confused between them, like which board to use for their project or which board is easy to learn or why should they use Arduino over Pi and vice versa. So here in this paper we are covering mostly all the aspects which make them easy to take the decision over the choice of Arduino vs. Raspberry Pi.

A. Advantages of Arduino overRaspberry Pi

Simplicity:
It's very easy to interface analog sensors, motors and other electronic components with Arduino, with just few lines of code. While in Raspberry pi, there is much overhead for simply reading those sensors, we need to install some libraries and software for interfacing these sensors and components. And the coding in Arduino is simpler, while one needs to have knowledge of Linux and its commands for using the Raspberry pi.

Robustness:
Raspberry Pi runs on a OS so it must be properly shut down before turning OFF the power, otherwise OS & applications may get corrupt and Pi can be damaged. While Arduino is just a plug and play device which can be turned ON and OFF at any point of time, without any risk of damage. It can start running the code again on resuming the power.

Power Consumption:

Pi is a powerful hardware, it needs continuous 5v power supply and it is difficult to run it on Batteries, while Arduino needs less power can easily be powered using a battery pack.

Price:
Obviously Arduino is cheaper than Raspberry Pi, Arduino costs around □ 600-1200 depending on the version, while price of Raspberry is around □ 2500-3000. [4]

Figure.4: Arduino UNO [8]

B. Advantages of Raspberry Pi over Arduino:

One can think that Arduino is the best, after reading its merits over Raspberry Pi, but wait, it's completely depends on your project that which platform should be used. Raspberry Pi's power and its easiness is the main attraction of it, over Arduino. Below we will discuss some of its advantages over Arduino:

Powerfulness:
This is the main advantage of Raspberry Pi. Pi is capable of doing multiple tasks at a time like a computer. If anyone wants to build a complex project like an advanced robot or the project where things need to be controlled from a web page over internet then Pi is the best choice. Pi can be converted into a webserver, VPN server, print server, database server etc. Arduino is good if you just want to blink a LED but if you have hundreds of LEDs needs to be controlled over web page, then Pi is the best suited.

Raspberry Pi is 40 times faster than Arduino, with PI, you can send mails, listen music, play videos, run internet etc. Also as we have stated earlier that it has memory, processor, USB ports, Ethernet port etc. and it doesn't require external hardware for most of the functions. It can be accessed via SSH and file can be easily transferred over FTP.

Networking:
Raspberry Pi has the built in Ethernet port, through which you can directly connect to the networks. Even Internet can easily be run on Pi using some USB Wi-Fi dongles. While in Arduino, it's very difficult to connect to network. External hardware need to be connected and properly addressed using code, to run network using Arduino. External Boards called "Shields" needs to be plugged in, to make Arduino, as functional as Pi, with a proper coding to handle them.

Don't need deep electronics knowledge

For Arduino you definitively need an electronic background, and need to know about embedded programming languages. But to start with Pi you don't need to dive into the coding languages and a small knowledge of electronics and its components is enough.

Besides those advantages, one advantage is that OS can be easily switched on the single Raspberry Pi board. Pi uses SD card as flash memory to install the OS, so just by swapping the memory card you can switch the operating system easily. [4]

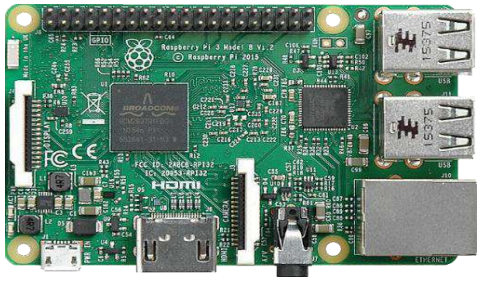


Figure.5: Raspberry Pi Model B [9]

C. You should choose Arduino if:

- You are from electronics background or if you are a beginner and really want to learn about electronics and its components.
- Your project is simple, especially networking is not involved.
- Your project is more like an electronics project where software applications are not involved, like Burglar alarm, voice controlled light.
- You are not a computer geek who is not much interested in software and Linux.

D. You should choose Raspberry Pi If:

- Your project is complex and networking is involved.
- Your project is more like a software application, like a VPN server or Web server
- Don't have good knowledge of electronics.
- Have good knowledge about Linux and software.

Although they both have their own pros and cons, but they can also be used together to make the best out of them. Like Pi can collect the data over the network and take decisions, and command the Arduino to take the proper action like rotate a motor. [4]

IV. FUTURE OF IOT:

The acceleration of IoT from lofty concept to reality is predicated on the projected exponential growth of smart devices and the confluence of low-cost infrastructure, connectivity and data. Declining device costs, widespread and pervasive connectivity, and an ever-increasing focus on operational efficiency and productivity is leading to wide deployment of IoT solutions. This rapid growth is based on expectations that the IoT will bring tangible benefits to businesses and consumers. Those benefits can take different forms for citizens, for businesses and for governments.

Consumers can get more personal product or service offers, based on what they actually do or where they are. They can travel more efficiently by avoiding traffic jams when their connected car suggests an alternative route, based on traffic reported by other vehicles. They can save money by reducing energy usage or by paying lower car insurance premiums based on verified safe driving practices. They can be healthier, safer and more independent due to wearable devices that provide feedback on health or that monitor the elderly in the home.

Businesses can provide better products and services by studying how customers behave; they can also discover needs for new products or services. They can protect buildings via remote security; secure assets like cars and machinery with location trackers and remote locking devices; and ensure that sensitive products (e.g. pharmaceuticals) are consistently stored in correct conditions. They can become more efficient, as in the case of utilities using smart meters to eliminate waste or loss, or in the case of equipment sellers providing just-in-time preventive maintenance. Farmers can be more productive with smart irrigation that provides water just where and when needed. New business models based on selling final outcomes rather than just equipment may boost business revenues.

Governments and public authorities can also benefit from the IoT. For example, health and long-term care costs can be reduced with better remote support for the elderly in their own homes. Road safety can be improved based on data from thousands of drivers. The efficiency of street lighting can be improved by dimming lights on empty roads. As governments work to deliver quality services in increasingly complex environments, devices that have already begun to make life easier and more efficient for companies and consumers can also help create greater public value. [6]

CONCLUSION

There is no simple answer to which one to use Arduino or Raspberry Pi. It really depends on the requirements of your project. The table (Table.1) below shows the summary of some of the decision points. The IoT device market is quite strong right now and new boards appear on the market frequently. New entrants, like the Raspberry Pi Zero, may shift your decision point in the months to come. One thing is for certain, this is an exciting and dynamic market.

Table.1 [7]

Category	Arduino	Raspberry Pi
Horsepower	Single-task	Multiple-task
Development Languages	C/C++ with Arduino IDE	C, PHP, Java, Python, NodeJS, .NET
Sensor Connectivity	Digital and Analog	Digital only. Analog with additional circuitry.
Network Connectivity	None without shields	Ethernet. Low cost WiFi dongle
Power Requirements	7V to 12V - flexible, low amperage	5V - very specific, higher current draw
Cost	Low	Medium*

* Raspberry Pi Zero changes this at it's new $5 price point

Many people find benefit in incorporating both devices into their projects. The network and processor capabilities of the Raspberry Pi make it ideal to serve a

web user interface for your project or communicate with cloud-based IoT services which often have IoT client libraries that are too large to fit in the memory of an Arduino device [2].

The Internet of Things is closer to being implemented than the average person would think. Most of the necessary technological advances needed for it have already been made, and some manufacturers and agencies have already begun implementing a small-scale version of it. The main reasons why it has not truly been implemented is the impact it will have on the legal, ethical, security and social fields. Workers could potentially abuse it, hackers could potentially access it, corporations may not want to share their data, and individual people may not like the complete absence of privacy. For these reasons, the Internet of Things may very well be pushed back longer than it truly needs to be.

The development of the Internet of Things will occur within a new ecosystem that will be driven by a number of key players (Figure 6). These players have to operate within a constantly evolving economic and legal system, which establishes a framework for their endeavours. Nevertheless, the human being should remain at the core of the overall vision, as his or her needs will be pivotal to future innovation in this area. Indeed, technology and markets cannot exist independently from the over-arching principles of a social and ethical system. The Internet of Things will have a broad impact on many of the processes that characterize our daily lives, influencing our behaviour and even our values. [7]

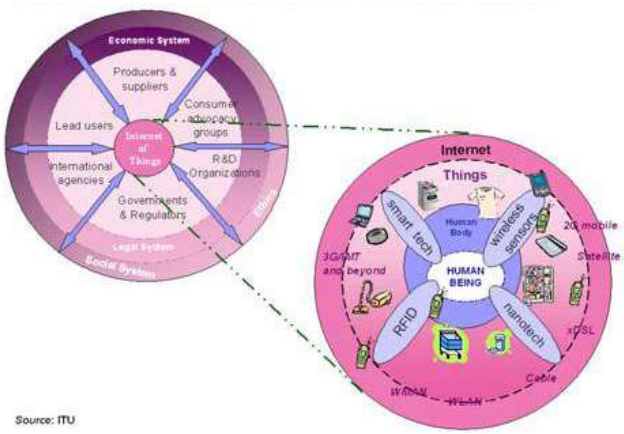


Figure.6: The Ecosystem of IoT [7]

REFERENCES

[1] http://www.itu.int/en/ITUT/gsi/iot/Pages/default.aspx ITU.
[2] http://www.universalmind.com/blog/technology/raspberry-pi-vs-arduino-when-to-use-which/ Universal Mind Blog.
[3] https://en.wikipedia.org/wiki/Raspberry_Pi Wikipedia.
[4] http://circuitdigest.com/article/arduino-vs-raspberryp-pi-difference-between-the-two Circuit Digest.
[5] https://iot-analytics.com/wp/wp-content/uploads/2016/08/List-of-640-IoT-projects-min.png
[6] Ms. Yogita Pundir, Ms. Nancy Sharma, Dr. Yaduvir Singh, "Internet of Things (IoT): Challenges and Future Directions" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016.
[7] ITU Internet Reports 2005: The Internet of Things (Executive Summary), November 2005.
[8] https://cdn.sparkfun.com/assets/9/1/e/4/8/515b4656ce395f8a38000000.png
[9] https://upload.wikimedia.org/wikipedia/commons/b/b4/Raspberry_Pi_3_Model_B.png
[10] https://upload.wikimedia.org/wikipedia/commons/thumb/8/87/Arduino_Logo.svg/1280px-Arduino_Logo.svg.pnghttps://upload.wikimedia.org/wikipedia/en/thumb/c/cb/Raspberry_Pi_Logo.svg/810px-Raspberry_Pi_Logo.svg.png
[11] https://www.arduino.cc/en/Guide/Introduction Arduino official site.

OTHER PUBLICATIONS:

[1] "Near Field Communication: A Survey", International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 6, June 2016).

Analysis of Audio Transmission using FSO at an altitude of 15.25m

J. Niranjan Samuel[1] T. Pasupathi[2], and J. Arputha Vijaya Selvi[3]

[1] Lab in-charge-R&D, [2] Assistant Professor, [3] Professor
Dept. of E&CE, Kings College of Engineering, Punalkulam, Tamil Nadu
E-Mail: niranjansamuelvimalan@gmail.com

***Abstract*—Laser as a communication medium provides a good alternate for the present day communication systems as there is no electromagnet interference and high deal of secrecy is achieved. Instead of RF signals, light from a laser source is used as carrier. In this paper capable to transmitting sound signals through a laser beam is described. From the analysis, it is found that the data transmission using laser light is superior in many aspects such higher bandwidth (Gbps), no licensing, easy deployment and etc., compared to the conventional communication system.**

Keywords—FPGA; Free Space Optical Communication;

I. INTRODUCTION

Free Space Optical Communication (FSOC) is a Line of Sight (LoS) communication in which modulated laser beam (visible/ infrared) is used to transfer information wirelessly through the atmospheric channel. Terrestrial FSOC now proven to be a viable technology in addressing the present-day communication challenges, most especially the bandwidth/ high data rate requirements of end users at an affordable cost. Performance of FSOC is degraded by the significant optical signal losses due to the atmospheric particles absorption and scattering of the propagating optical and infrared waves, since their wavelengths are very close to the wavelengths of these frequencies [1]. However, during clear weather condition, theoretical and experimental studies have proved that scintillation can severely degrade the reliability and connectivity of FSOC links. In FSOC, the transmitters and receivers are placed on high-rise buildings as shown in Fig.1.

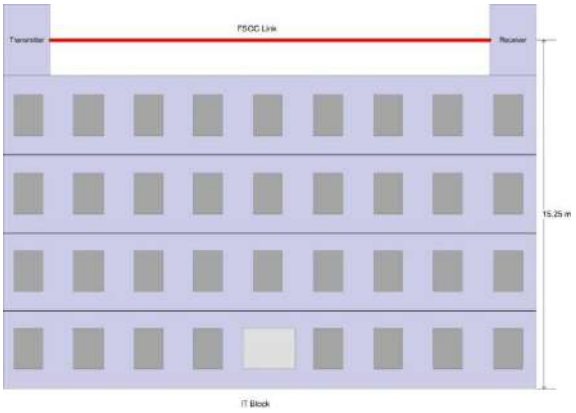


Fig. 1. A schematic of FSOC channel

III. CHALLENGES IN FSOC

FSOC uses atmosphere as propagating medium whose properties vary randomly as a function of space and time. FSO communication is dependent on various factors like clouds, snow, fog, rain, haze, etc, cause strong attenuation in the optical signal and limit the link range. Terrestrial links include communication between building-to-building, mountain-to-

FSOC systems with unlicensed modulation bandwidth capability have attracted a great deal of interest from a number of sources including academia, industry, telecommunication and standardization bodies. This huge bandwidth represents high potentials in terms of capacity and flexibility thus making FSOC technology particularly an attractive candidate for multi-gigabit wireless applications including audio, video streaming and file transferring for last mile access network [1].

II. BACKGROUND AND RELATED WORKS

Mohammed Kamal Khwaja & Vishakh B V 2015, described the development of laser based audio communication system. From their studies, they concluded that laser communication has certain limitations such as beam dispersion, atmospheric absorption, and attenuation due to rain, fog, interference from background light sources etc [2]. A. Arockia Bazil Raj et.al 2010, described the development of a Position Sensing Detector (PSD) and Stochastic Parallel Gradient Descent Algorithm (SPGDA) based control system using FPGA in a Closed Loop to improve the performance of the FSOC by Aligning, Tracking and Positioning (ATP) the laser beam [3]. Md. Kayesar Ahmmed et.al 2013, discussed about the design of a low cost voice transmission system using an LDR and Laser torch. It given that it almost 86% cheaper than the lowest cost voice transmission system is achievable [4]. A. Arockia Bazil Raj et.al 2010, described the design and development of an Adaptive Fuzzy Logic Controller (AFLC) in FPGA. The performance of the system is tested in real time and statistical analyses of the experimental data are also presented [5].

A. Arockia Bazil Raj et.al 2011, described the beam steering technique of a propagating laser beam, which is essential for Free-Space Optical Communication (FSOC) and FSOC to Single Mode Fiber (SMF) coupling. Performance of the developed steering system is tested in the real time FSOC link [6]. T. Pasupathi et.al 2016, presented practical implementation of adaptive optics system at 850 nm based on a wave-front sensorless architecture with reduced cost and setup complexity. Sensorless Adaptive Optics provides fast and effective wave-front correction, compared to the conventional AO systems. This technique eliminates the requirement of high cost wavefront sensor [7].

mountain or horizontal link between two ground stations. The various losses that degrade the optical signal strength when propagating through the atmospheric channel are Absorption, scattering, Fog, Rain and snow.

IV. EXPERIMENTAL TEST-BED AND ITS DESCRIPTIONS

The transmitter and receiver experimental test-beds are established at an altitude of 15.25 m above ground level. Fig.2 shows experimental set-up and descriptions. The transmitter laboratory consists of (i) Audio generator, (ii) Modulator (iii) Laser source and (iv) Beam expander, (v) FPGA and (vi) PC. Audio signal is applied as input applied to the 850 nm, 10mW laser source. On-Off keying (OOK) Modulation Technique is used. After modulation, the laser beam is passed into the primary side of the beam expander that expands the beam diameter from 3mm to 9mm. This device is used to increase the output beam diameter that significantly decreases/limits the beam divergence at the aperture of the receiving telescope. At the transmitter, transmitted audio signals are acquired using suitable HDL and logged in a PC through RS 232 ports using MATLAB environment for performance monitoring. At the receiver, the modulated laser beam is collected by the telescope with a diameter of 330mm. It is designed such a way to collect almost all the optical energy.

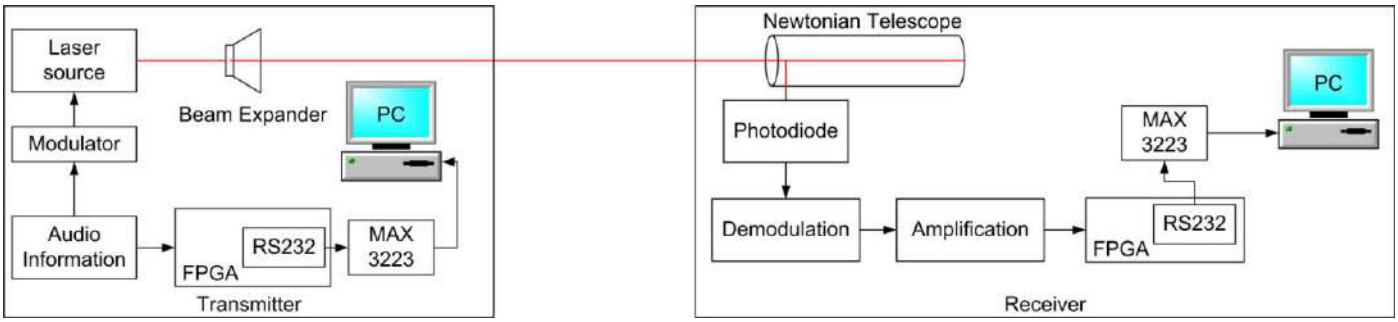


Fig. 2. Architecture of FSOC Transceiver

The receiver laboratory mainly consists of (i) receiving telescope, (ii) photodiode, (iii) demodulator, (iv) amplifier, (v) ADC, (vi) FPGA and (vii) PC. The received data corresponding are transferred to computer through the DB9-Serial port.

V. RESULTS

Fig. 3 shows the averaged beam profile at the transmitter laboratory. From Fig. 3, it is clear that transmitter voltage is maintained uniformly throughout the period.

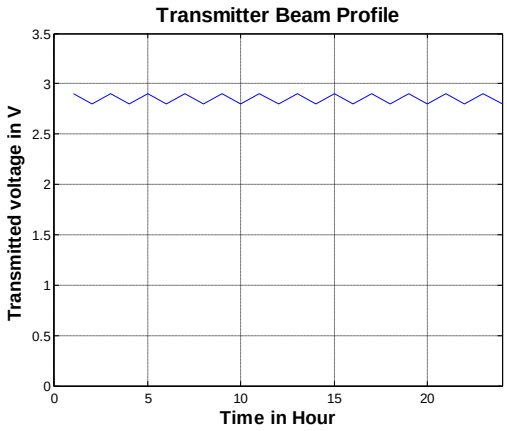
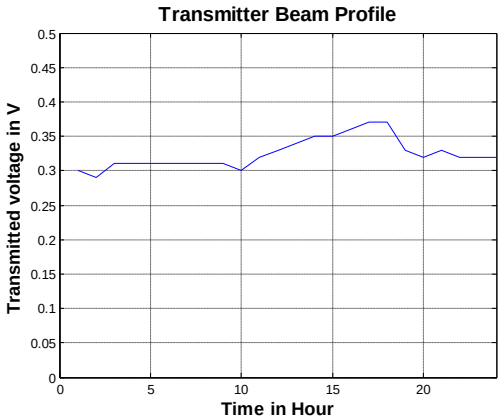


Fig. 3. Transmitted Beam Profile

Fig. 4 shows the averaged beam profile at the receiver laboratory. From Fig. 4, it is observed that some of the transmitted, is lost due to the various factors such scattering, absorption, rain, fog, visibility, distance and bandwidth.



Received Beam Profile

VI. CONCLUSION

The performance analysis of audio transmission in free space communication link is achieved and it is performed during normal daytime and night.

REFERENCES

[1] A. Arockia Bazil Raj. *Free Space Optical Communication. System Design, Modeling, Characterization and Dealing with Turbulence*, De Gruyter Oldenbourg, Boston. 2015.

[2] Mohammed Kamal Khwaja & Vishakh B V, Laser Based Audio Communication System, International Journal of Engineering Sciences & Research Technology, vol. 4, Iss.5, pp.284-288.

[3] A. A. B. Raj, J. A. V. Selvi and S. Raghavan, "Terrestrial free space line of sight optical communication (TFSLSOC) using adaptive control steering system with laser beam Tracking, Aligning and Positioning (ATP)," *Wireless Communication and Sensor Computing, 2010. ICWCSC 2010. International Conference on*, Chennai, 2010, pp. 1-5.

[4] Md. Kayesar Ahmmed, Anmona Shabnam Pranti and Arif Md. Shahed Iqubal, Low Cost Voice Communication Device Design using Ordinary Laser Torch and LDR Available in Bangladesh, International Journal of Electronics and Electrical Engineering, Vol.1, No. 4, 2013, pp. 223-229.

[5] A. A. B. Raj and J. A. V. Selvi, "Lower-order adaptive beam steering system in terrestrial free space point-to-point laser communication using fine tracking sensor," *Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on*, Thuckafay, 2011, pp. 699-704.

[6] A. A. B. Raj, J. A. V. Selvi, R. Sathiya, A. Shanthi, M. Sharmila and L. K. Soumya, "Low cost beam steering system for FSOC to SMF coupling," *Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on*, Nagapattinam, Tamil Nadu, 2012, pp. 49-54.

[7] T.Pasupathi, J. Arputha Vijaya Selvi, J.Niranjan Samuel, "Mitigation of low-order atmospheric turbulent effects using Sensorless Adaptive Optics in Terrestrial Free Space Optical Communication," *Emerging Trends in Engineering, Technology and Science* (ICETETS-2016), 2016 *International Conference*, Punalkulam, Tamil Nadu, 2016, pp.

Impact of Motivational Techniques in E-learning/Web learning Environment

K.Raja[1], M.Nirajana[2], B.Ramaya[3]
[1]K. Raja., Research Scholar , Dept.of CSE, Sudashran College of Arts & Science, Pudukottai
[2.3.] Assistant Professor, Dept.of CSE, Annai College of Arts & Science, Kumbakonam

Abstract-This paper focuses on the motivational aspects of a virtual learning environment. The majority of student teams work entirely in virtual space and they have no face to face contact, and the team members are initiated by the instructor or facilitator of the team and the instructor should promote a change of mind set and help the learners to break out of their stereotypical roles of information receivers to information seekers. This change in the mind set is brought out by interaction and motivation of the instructor. This paper analyses the virtual motivational strategies of practise and aims in finding out the impact of it on the study group.

I. INTRODUCTION

Computer Mediated communication is characterized by a highly interactive multi way synchronous or asynchronous communication. Asynchronous and synchronous tools provide opportunities for active input from all members of the online class room and support learner centred learning environments. Interaction plays a key role in the information exchange. The instructor in the learning group arranges for the setting of the frames the rules and nourishes the conversation. The need for the instructor to act as the host of the VLC is rapidly increasing and he should cut off the inappropriate behaviour of the learners. The facilitator contacts the members frequently and increases the skills and their ability by providing various notification aspects.

II. MOTIVATION

Motivation has been defined by Maslow as a psychological process where behaviour towards a goal based on individual needs. It is one of the most important components of learning in an E-learning environment. It is important for the instruction in a virtual study group to consider the motivation level of the learners the most important factor in successful instruction. Motivation mediates learning and it is the result of learning also. Motivation brings successfulness to the students while comparing the others and so the motivation and successfulness very dependent on each other. Motivation also links itself with learning n the way it resides with the pupil who learn well. The above really the fact the motivation is the clear component to instruction and learning. Using killer's Attention, relevance, confidence and satisfaction ARCS motivational aspects, the role of online instruction between students, their peers and instruction and how these instructions influence to learner's motivation will be explored. This knowledge will contribute to understanding the online modality of education and therefore help educators select the most appropriate technological and motivational methods to improve learning.

III. WAYS OF MOTIVATING IN SG

Motivating students are not a magical one. There are many factors that affect the motivation of the students in a study group to work with it. Few of them in that list are Interest in the subject matter, perception of its usefulness, General desire to achieve, Self confidence and self esteem and patience and persistence. There exist various situations for the students to get motivated same by the approval of others and same by over coming challenges.

Instruction in the study group plays the role of master of the community. This facilitates to shape his role on the basics of nature of the individual but there are some pin points the instruction posses to encourage and motivate successful community instructions.

The instructions do the following (lowman (1984), lucas (1990)) to encourage the students to become self motivated independent learners.

1. Give frequent, early, positive feedback that supports student's beliefs that they can do well.
2. Assign topics that are neither too easy nor too difficult. Then only the student can expect the opportunity of success.
3. Help students find personal meaning and value in the material.
4. Create an atmosphere that is open and positive.
5. Make the students to recognize their position and to realize their importance in the community.

Research has shown that good everyday teaching practices can do more to counter student apathy than special efforts to attack motivation directly. The level of motivation depends on the instructor of the community. In a well organised course taught by an enthusiastic instructor in the level of motivation is high. Because the instructor has a genuine interest in students and what they learn and the student's response to that course will be high.

A simple logic exists there is that the activities that are taken to promote learning will increase students motivation.

IV. MOTIVATIONAL STRATEGIES OF PRACTICE

1. Capitalise on Students needs.

The learner behaviour depends mainly on the satisfaction of their own motives for enrolling in the course. Te needs

of the students to join the group may vary, need to learn the same thing in order to complete a particular task or activity, the need to seek new experiences, the need to prove their perfect skills, their need to overcome the challenge, the need to become competent, the need to succeed and do well, the need to get interacted with other people. Satisfying such needs is rewarding in it self and such records sustain learning more effectively than do grades.

2. Active participation in learning

The process of learning is accompanied by doing, making, writing, designing, creating and solving passive participation dampens student motivation and curiosity. Frequent posting of questions encourages the students to suggest approaches to a problem. Collaborative learning focuses mainly on the learner and instructor interaction to be very high.

3. Get frequent feedback

Collect the feedback from the student of the learner group that whether they are motivated positively or negatively by the activities of the instructor. Ask the students to prepare a list of specific aspects that influences their level of motivation. Some of the major contributors of student motivation are The instructor should enthusiastic one There should be one sort of influence in their conversation between instructor and the learner.

The course should be organised properly with several modules in it.

- Students should be made to participate actively in the group.
- Rapport between the instructor and the learner.
- The technique used by the instructor for solving the puzzles
- Difficult /ease of the course.

V. THE IMPACT OF INSTRUCTION STRATEGY ON MOTIVATION

The role of expectations

The expectation of the instructor plays a major role in motivating the students positively throughout the course. It is the duty of the facilitator / instructor to expect the participants to be motivated hard working and interested in the course, they are more likely to be so. The instructor should set realistic expectation for students when they are given assignments, presentations, while conducting discussions and grade examinations.

Realistic means that standards are high enough to motivate students to do their best work but not so high that students will inevitably be frustrated in trying to meet the expectations. There is a need for the ins to provide the early opportunities for success.

1. Facilitate setting of goals.

Failure to attain unrealistic goals can disappoint and frustrate the students. Encourage students to focus on their continued improvement. The students should be encouraged to critique their own work, analyse their strengths and their weakness.

2. Supply with materials for getting success.

The steps to get succeed should be given clearly to students by the instructor. Ask them to work out many examples of problem which increases their problem solving skill paves the way for success.

3. Strengthen the self motivation

The facilitator should not command or impose the conditions on the learners in turn they should clearly utter the words that increases the self motivation of learners.

4. The competitive nature should be withdrawn.

Completion produces anxiety, which can interface with learning. The instructor should be very careful in a virtual community to check whether competition is involved in that virtual community. It was found previously that students are more attentive, display better comprehension, produce more work and more favourably to the teaching method when they work cooperatively inn groups rather than compete as individuals.

5. Increase enthusiasm in the subject.

The enthusiasm plays a major role in the student motivation. The behaviour of the instructor in the virtual community is reflected among the learner participants also. The instructor should challenge himself to device the most exciting way to present the material.

VI. THE IMPACT OF COURSE STRUCTURE ON MOTIVATION

Find out strength and interests

The instructor has to identify the aim of the student enrolled in the course, their expectations about the subject matter. The course initiator ha to device examples, case assignments that relate the course contents to student's interest and examples. The explanation about how the content and objectives of the course will help the participants achieve their educational, professional or personal goals.

Choice based system

The participants should be allowed to have their options on term papers or other assignments.

The teaching method should be varied

Variety reawakens student's involvement in the course and their motivation. The instructor has to break the routine by incorporating a variety of teaching activities and methods in the course, role playing, debates, brainstorming discussion, demonstrations, case studies, audio visual presentation, guest speakers or small group.

VII. THE IMPACT OF GRADES ON MOTIVATION

Emphasize mastery and learning rather than grades

Researchers recommend de-emphasizing grading by eliminating complex systems of credit points.

Avoid using grades as threats

The threat of low grades may prompt students to work hard but other students may resort to academic dishonesty, excuses for late work and their counter productive behaviour.

VIII.The Impact of Response on Motivation

Feedback

The participants should be given some indication of how well they have done and how to improve. Reward should be given to student's response as such it is good.

Reward success

Research consistency indicates that students are most affected by positive feedback and success. Praise builds students self confidence, competence and self esteem. The ins has to make the participant believe that she can improve and succeed over time.

Discussing the good work done by their peers

Share the ideas, Knowledge and accomplishments to individual participants in the course registered.

- Circulation of the list of research topics chosen by the students to others to know about the interest of others.
- The topics of the bet papers should be made available for others.
- The research paper experience should be shared among the participants.

Careful about Negative feedback

Negative feedback is very powerful and can lead to a negative class atmosphere.

Avoid Demeaning Comment

Many participants in the work group may be anxious about the performance and abilities. The instructor has to be sensitive to phrase his comments and avoid offhand remarks that might prick their feelings of inadequacy.

Motivate the students to do the reading.

1. The participants should be given ample time to prepare and try to pick their curiosity about the reading.
2. Students should be asked to choose a single word that summarizes the reading and then write a page or less explaining or justifying their word choice.

IX. The Sample Model for Motivation

The ARCS model is a method for systematically designing motivational strategies into instructional material. It comprises three parts a set of four categories for concepts of human motivation, a set of strategies for enhancing motivation under the assumption that the learners will be motivated if they feel they can be successful and there is a value in their learning. ARCS summarizes into four categories of motivation. They are i) Attention ii) Relevance iii) Confidence and iv) Satisfaction.

X. Outcomes

The level of engagement in the online environment is evident in student's responses. The online interaction enriched their engagement in the learning process. The students consider this discussion board is very helpful simply because it shows different answers form different perspectives. The learner's satisfaction with an online environment is related to the amount of interaction with other learners. The learners are primarily motivated by active colleagues.

Creation of safe learning environment through positive social relationships can support online interactions. New mode of delivery in an e-learning environment motivated the learners a lot. Accessibility and convenience are also included as important motivational factor in an online environment. Facilitator s feedback also motivates learners.

CONCLUSION

In this paper we have discussed some concepts of motivation. But there are still many unknown elements about this. It is clear that self -efficacy is at the heart of motivation. When designing learning experiences one should take this to consideration and make every effort to increase the student's self-efficacy. When designing a new course the initiator should take special care, such it is designed with relevant and authentic experiences for learners. It also includes features such as feedback and navigation systems. Feedback mechanisms are meaningful and adaptive. It also emphasize that a simple, consistent and easily understood navigation system should be incorporated in to the materials. These factors that have influenced motivation for learning in the part with the new factors that have arisen due to the nature of e-learning delivery media must be addressed for the enhancement of student learning in today's virtual learning environment

REFERENCES

1. Collis, B. & Moonen, J. (2001). Flexible learning in a digital world: Experiences and expectations. London: Kogan Page.
2. Coppola, N.W., Hiltz, S.R., and Rotter, N.G. (2002). Becoming a virtual professor: pedagogical roles and asynchronous learning networks. Journal of Management Information Systems, Spring, Volume 18, Number 4, pp. 169-189.
3. Hara, N., Bonk, J. & Angeli, C., (1998). Content analysis of online discussion in an applied educational psychology. CRLT Technical Report No.2-98.

4. Hillman, D.C.A., Willis, D.J., & Gunwardena, C.N. (1994). Learner-interface interaction in distance education: An extension of contemporary models and strategies for practitioners. American journal of distance education, 8(2), 30-40.
5. Hiltz, S.R. (1994). 'The virtual classroom: Learning without limits via computer networks.' Human-Computer Interaction Series. Norwood, NJ: Ablex in Järvelä, S. & Häkkinen, P. (2002) Web-based Cases in Teaching and Learning – the Quality of Discussions and a Stage of Perspective Taking in Asynchronous Communication. Interactive Learning Environments Vol. 10 No. 1 pp. 1 – 22.
6. Kaye, AR. (1991) Learning together apart, in Kaye, AR. (1991) (ed) Collaborative learning through computer conferencing: the Najaden papers, Milton Keynes, Open University, pp 1 – 24
7. Keegan, D.(1988). Problems in defining the field of distance education. The American Journal of Distance Education, 2(2),4-11.
8. Keller, J (1987). Development and use of the ARCS model of instructional design. Journal of Instructional Development, 10(3), 2-10.
9. Keller, J. M. (1999a). Motivation in cyber learning environment. International Journal of Educational Technology, (1), 7-30.

Software Development Using Effort Estimation Technique

Manohar K. Kodmelwar[1], Dr. Shashank D. Joshi[2], Dr. V. Khanna[3]

[1]*Research Scholar,*[2,3]*Professor*

[1] *Bharath Institute Of Higher Education And Research,Chennai,*[2] *Bharati Vidyapeth College of Engineering,Pune Higher Education And Research,*[3] *Bharath Institute Of Higher Education And Research,Chennai*

E-Mail: kodmelwarmk@gmail.com, *sdj@live.in*, drvkannan62@yahoo.com

Abstract: ***The estimation of software in terms of effort & cost is still the challenging problem for the developers. The prior estimation before development is always useful for avoiding the delay. Various methods are developed for effort estimation .Some techniques use the Function point analysis, Usecase method, Lines of code, Fuzzy logic etc. The estimation of considering all points can provide good results. This paper presents various method available for software cost & effort estimation.***

Keywords:- EAF (Efforts Adjustment Factors) Cost Drivers, FP (Function Point), COCOMO (it is one of the approach of efforts estimation),EF (Experience Factor). TCP (Technical Complexity Factors),UCP (Use Case Point).

I. INTRODUCTION

Estimation of software is at most important factor for the project development. The correctly selected model for estimation will result in time bound output. The seventy five percent of project fails due to the incorrectly used software estimation model. New techniques developed for the good result. The research is still going on in the filed of software development. The incorrectly selected model will result in the reputation of company , loss of money & loss of resources. The customer satisfaction should be given the priority.

The various model like Constrictive Cost Model, Usecase point , Function point Analysis & fuzzy logic are available for estimation. In these method various points are applied & the effort are calculated.

II. ESTIMATION TECHNIQUES

Some of the estimation techniques are discussed into non algorithmic & algorithmic based. In non algorithmic based estimation techniques[1][2][3]

1.Expert based judgment : This method mainly take the decision by arranging the discussion among the experts. The views are gathered and finally the decision is taken. The experts are experienced. The Delphi technique is used for understanding. Where the group of expert opinion is taken by giving the forms.

2. Estimating by analogy: This method mainly consider the past similar type of project. The comparisons are done on the basis of current requirement & decision is taken.

3. Top Down Approach:- In this the from the estimation are done on the basis of the global properties & then it is divided into the small component

4. Bottom up approach:- In this method the cost of each component is estimated & then results are combined to get the overall estimation..

To understand the top –down & bottom –up approach the example of climate adaption policy is as follows in fig1

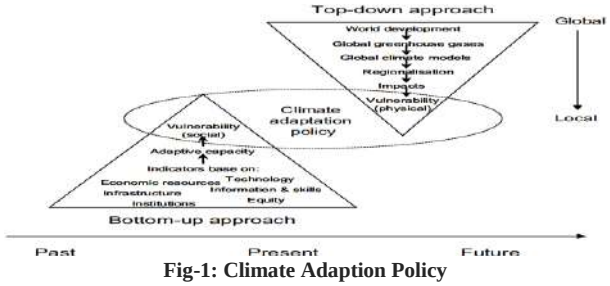


Fig-1: Climate Adaption Policy

The second estimation using algorithm based estimation is considered where some mathematical formulas are used and calculated the effort. These mathematical equations are based on research and

historical data and use inputs such as Source Lines of Code (SLOC), number of functions to perform, and other cost drivers such as language, design methodology, skill-levels, risk assessments, etc. The algorithmic methods have been largely studied and many models have been developed, such as COCOMO models, Putnam model, and function points based models [17] .

1. COCOMO Model:- This model proposed by Barry Boehm (Boehm, 1981), is the most popular method which is categorized in algorithmic methods. [4][3][16]

B. Simple COCOMO : It was the first model suggested by Barry Boehm, which follows following formula:

$$\text{Effort} = a * (\text{K LOC})b.$$

C. Intermediate COCOMO Model : In this method the effort adjustment factor is used in the simple COCOMO effort formula.

$$\text{Effort} = a * (\text{K LOC})b * \text{EAF}$$

D..COCOMO-II model new Scale factors added for estimation

1.Precedentedness (PREC)

2.Development flexibility (FLEX)

3.Architecture/ risk resolution (RESL)

4.Team cohesion (TEAM)

5. Process maturity (PMAT, derived from SEI CMM)

NOMINAL PERSON-MONTHS = A*(SIZE)^B

B = 0.91 + 0.01 ∑(SCALE FACTOR RATINGS)

Where KLOC are the code size, a & b are the complexity functions in the code.

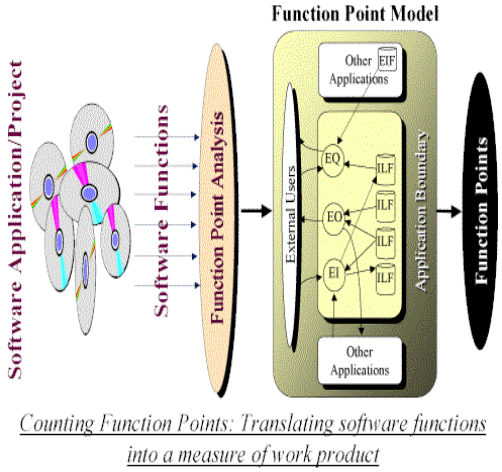
2. PUTNAM Model:- In Putnam model for calculating the estimate for a software task the software equation is solved for effort:

$$\text{Effort} = \left[\frac{\text{Size}}{\text{Productivity} \cdot \text{Time}^{4/3}}\right]^3 \cdot B$$

B= It is a scaling factor and is a function of the project size

3.FUNCTION POINT ANALYSIS:- FP defined by Allan Albrecht at IBM in 1979, is a unit of measurement to express the amount software functionality In this how much functionality is given o user on the basis of that the size & complexity of software is calculated.[6][8][18]

It is independent of programming language . The Function Point Model in the fig 2.It calculate by using five parameters are external inputs, external outputs, external inquiries, logic internal files, and external interfaces, each at one of three complexity levels: simple, average or complex.



Fg-2 Function Point Model

3. Bayesian Belief Network : This model framework is based on the four basic sub-models, which are used to model quality, effort and schedule information[13].[19]

4.USE CASE Point The UCP technique was developed by Gustav Karner in 1993 while employed at what was known at the time as Objectory Systems, which later merged into Rational Software and then IBM. The method for determining the size estimate to develop a system is based on a calculation with the following elements:[15]

- Unadjusted Use Case Weight (UUCW) – the pint size of the software that accounts for the number and complexity of use cases.
- Unadjusted Actor Weight (UAW) – the point size of the software that accounts for the number and complexity of actors.
- Technical Complexity Factor (TCF) – factor that is used to adjust the size based on technical considerations.
- Environmental Complexity Factor (ECF) – factor that is used to adjust the size based on environmental considerations.

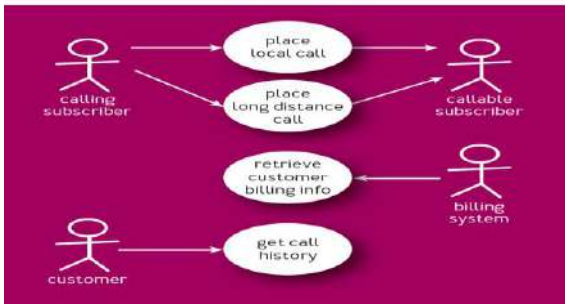


Fig 3: Usecase diagram for telephone system

The use case diagram fig. 3 for simple telephone system for understanding.

5. Fuzzy logic:- The fuzzy logic based approach will divide the data in small, very small, large, very large &medium categories. Establish the subcategories & categories find the closet among them.

CONCLUSION

The estimation of software cost & effort is critical issue. This paper gives the brief idea about the estimating techniques available. The choosing of estimation techniques is depending on the application to developed.The paper will gives idea about the factors affect on the estimation by various point. These consideration are important otherwise the delay in schedule & cost can increase.

ACKNOWLEDGMENT

I wish to express my sincere thanks to Dr. M. Sundararajan, Dean Research**,** Bharath Institute of Higher Education & Research for providing all necessary facilities.
I wish to place my sincere thanks to Dr. Shashank D. Joshi, guiding me during the paper preparation.
I place on record my sincere gratitude to Dr. V. Khanna, Professor, Bharath Institute of Higher Education & Research for continuous encouragement.
I am also thankful to my parents for unending support.
I am also thankful to friends & all those who directly or indirectly helped me.

REFERENCES

[1]Y. F. Li, M. Xie, T. N. Goh, ”A Study of Genetic Algorithm for Project Selection for Analogy Based Software Cost Estimation, IEEE, 2007.
[2]Khaled Hamdan, Hazem El Khatib, Khaled Shuaib,” Practical Software Project Total Cost Estimation Methods”, MCIT 10, IEEE, 2010.
[3]Chetan Nagar, ”Software efforts estimation using Use Case Point approach by increasing technical complexity and experience factors”, IJCSE, ISSN:0975-3397, Vol.3 No.10 , Pg No 3337-3345,October 2011.
[4]Chetan Nagar, Anurag Dixit, ”Software efforts and cost estimation with systematic approach”, IJETCIS, ISSN:2079-8407, Vol.2 No.7, July 2011.
[5]Chen Qingzhang, Fang Shuojin, Wang Wenfu, ”Development of the Decision Support System for Software Project Cost Estimation”, World Congress on Software Engineering,IEEE, 2009.
[6]Yinhuan Zheng, Yilong Zheng, Beizhan Wang, Liang Shi, ”Esti- mation of software projects effort based on function point”, 4th International Conference on Computer Science and Education, 2009.
[7]Jairus Hihn, Hamid Habib-agahi, ”Cost Estimation of Software Intensive Projects:A Survey of Current Practices”, IEEE, 2011.
[8]Yunsik Ahn, Jungseok Suh, Seungryeol Kim, Hyunsoo Kim, ”The software maintenance project effort estimation model based on function points”, Journal of software maintenance and evoloution, 2003.
[9]Jin Yongqin, Li Jun, Lin Jianming, Chen Qingzhang, ”Software Project Cost Estimation Based On Groupware”, World Congress on Software Engineering, IEEE, 2009.
[10]Pichai Jodpimai, Peraphon Sophatsathit, and Chidchanok Lursin- sap, ”Analysis of Effort Estimation based on Software Project Models”, IEEE, 2009.
[11]Nancy Merlo Schett, ”Seminar on software cost estimation”, University of Zurich,Switzerland, 2003.
[12]Hao Wang, Fei Peng, Chao Zhang, Andrej Pietschker, ”Software Project Level Estimation Model Framework based on Bayesian Belief Networks”, Sixth International Conference on Quality Software (QSIC’06), IEEE, 2006.
[13]angyang Yu, Charlottesville, ”A BBN Approach to Certifying the Reliability of COTS Software Systems”, annual reliability and maintainability symposium, IEEE, 2003.
[14]Ying Wang, Michael Smith, ”Release Date Prediction for Telecommunication Software Using Bayesian Belief Networks”, E Canadian Conference on Electrical and Computer Engineer- ing, IEEE, 2002.
[15] Suresh Nageswaran, ”Test Effort Estimation Using Use Case

Points", Quality Week , San Francisco, California, USA, June 2001
[16]Kusuma Kumari B.M " Software Cost Estimation Techniques, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-4)
[18]Jyoti G. Borade , Vikas R. Khalkar " Software Project Effort and Cost Estimation Techniques" International Journal of Advanced Research in Computer Science and Software Engineering 3(8), August - 2013, pp. 730-739
[19]http://www.agenarisk.com/newsletters/NS5Articles/Siemens_BNs_software_project_estimation.pdf

The Solar Energy: An EcoFriendly Energy Source for Various Applications

Namratha R[1], Triveni G[2],Tanmayee V [3], JaiPriya[4] , Nandini G[5]

[1,2,3,4] UG Scholar, [5]Asst. Professor Student, Dept. Of CSE, RRCE, Bengaluru,

E-mail: nammuanu15@gmail.com , trivenig03@gmail.com ,tanmayee.tanu14@Qgmail.com ,prasinahans@gmail.com nanduamma@gmail.com

***Abstract:** The Sun light is a non-vanishing renewable source of energy which is free from environmental pollution and noise. Large number of improvement steps took place in the fabrication of solar cells from one generation to another. Solar chargers are the simple and ready to use device which can be used everywhere specially in remote areas. Using solar energy we can solve more than one problem from reducing carbon emission and dependence on fuels. Using solar as a source of energy we can reduce energy crisis. This project aims at making a simple solar charger from which multiple devices can be charged. Regulated voltage cannot be supplied from solar panel; hence an adapter is used to have the desired constant voltage. Instead of an adapter, diode switches can be used to ensure charging is cut off at the right saturation point.*

***Keywords:** Renewable resources, Solar cells, solar energy, solar panels..*

I INTRODUCTION

Those days are gone when we were looking at the sun and cursing for being out on a hot sunny day. Take pride. Very soon you will become a walking energy station and people will ask to charge their devices with your clothes!. This is not scene from a science-fiction movie. It's a simple application of solar cell. This is the only way we can convert sunlight directly into electricity and day by day it's improving and it's getting better, smaller and cheaper.

When it comes to radiating energy, nothing can dare challenge the sun. The energy available from the sun per hour is more than what humans require for an entire year. It is limitless source of energy which is available without cost. Petrol, diesel and all these fossil fuels are the sun's energy which are concentrated over years together. Solar energy is not something new. People have used this to dry and preserve things. According to Indian Vedic literature, flying machines were powered using sun.

Solar panels are the cells lined up together in series and parallel so as to get sufficient voltage. Solar cells are p-n junction semiconductor devices with pure silicon doped with 'n' type phosphorous on the top and 'p' type boron on the base.

When the PV cell is placed in the sun, **photons** will strike the electrons in the p-n junction and energize them, hence knocking them free of their atoms. These electrons get attracted to the positive charge in the n-type silicon and they get repelled by the negative charge in the p-type silicon. Connecting wires across the junction we can generate power. Efficiency of solar cell has increased from 6% to 30% when it comes to thin film solar panel. Today, they are selling solar panels like hot cakes.

Fig 1.1 Solar cell

We must understand the solar panel in order to understand their applications. We have different types of solar panel namely mono crystalline, polycrystalline and amorphous thin film panels. Amorphous thin film panels are layers of silicon on surface of a glass. They are least expensive. Hence, they are used widely.

Solar panels are really useful in broad day light. But we even need energy when the sun is not shinning. That is why we need this solar charger to store energy in rechargeable batteries.

Fig-1.2 Solar panels

15% efficient solar panels are installed across the world's wastelands and it can produce enough clean energy to sustain mankind for a year. Yet new technologies are

continuously being developed though solar energy generation is still in its infancy. The concept of SOLAR FRAMING is new technology developed. Cutting down on our carbon emissions and reducing dependence on fossil fuels are the most important aspects of solar energy. Another crucial point is that it can make any country especially tropical country like India, self sufficient in energy.

II GENERATIONS OF SOLAR CELLS

- **First Generation Solar Cells**

Traditional solar cells are made from silicon. At present the most efficient solar cells available for residential use and account for about 80+ percent of all the solar panels sold around the world. Generally silicon based solar cells are more resourceful and longer lasting than non silicon based cells. However, they are more at risk to lose some of their competence at higher temperatures (hot sunny days), than thin-film solar cells.

Fig2.1- First generation solar cell

There are currently four types of silicon based cells used in the manufacture of solar panels for residential use. The types are based on the type of silicon used, namely:

1. Mono crystalline Silicon Cells

The oldest solar cell technology and still the largely popular and efficient are solar cells made from skinny wafers of silicon. These are called Môn crystalline solar cells because the cells are slices of large single crystals that have been painstakingly grown under carefully guarded conditions. Typically, the cells are a few inches across, and some amount of cells is laid out in a network to create a panel.

Relative to the other types of cells, they have an advanced efficiency (up to 24.2%), meaning you will attain more electricity from a given area of panel. This is useful if you only have a partial area for mounting your panels, or want to keep the installation small for artistic reasons. However, growing large crystals of pure silicon is hard and very energy-intensive process, so the production costs for this type of panel have historically is the highest of all the solar panel types.

Production methods have improved though, and prices for raw silicon as well as to construct panels from Mono crystalline solar cells have fallen a huge deal over the years, partly driven by competition as other types of panel have been formed.

Another issue to keep in mind about panels made from Môn crystalline silicon cells is that they lose their efficiency as the warmth increases about 25˚C, so they need to be installed in such a way as to permit the air to circulate over and below the panels to improve their efficiency.

Fig 2.2- Mono crystalline Silicon Cell

2. Polycrystalline Silicon Cells

It is cheaper to produce silicon wafers in moulds from multiple silicon crystals moderately than from a single crystal as the circumstances for growth do not need to be as tightly forced. In this form, a number of interlock of silicon crystals grows together. Panels based on these cells are cheaper per unit part than mono crystalline panels - but they are also slightly less efficient (up to 19.3%).

Fig 2.3- Polycrystalline Silicon Cell

Note: Many of the leading firms make together mono crystalline and polycrystalline solar cells for their panels.

3. Amorphous Silicon Cells: You perhaps never thought about it before, but most solar cells used in calculators and lots of small electronic devices are made from amorphous silicon cells.

Instead of growing silicon crystals as is done in making the two earlier types of solar cells, silicon is deposited in a very thin layer on to a backing substrate – such as metal, glass or even plastic. Sometimes numerous layers of silicon, doped in slightly different ways to respond to diverse wavelengths of light, are laid on top of one another to improve the efficiency. The production methods are compound, but less energy intensive than crystalline panels, and prices have been coming down as panels are mass-produced using this process.

One advantage of using very slim layers of silicon is that the panels can be made flexible. The disadvantage of amorphous panels is that they are much less efficient per unit area (up to 10%) and are generally not suitable for roof installations you would typically need nearly double the panel area for the same power output. Having said that, for a given power rating, they do perform better at low light levels than crystalline panels - which are worth having on a dismal winter's day, and are less likely to lose their efficiency as the temperature climbs.

However, there flexibility makes them an brilliant choice for use in making building incorporated PV (e.g., roofing shingles), for use on curled surfaces, or even attached to a flexible backing sheet so that they can even be rolled up and used when going backpacking, or put away when they are not needed!

4. Hybrid Silicon Cells

One recent drift in the industry is the emergence of hybrid silicon cells and several companies are now exploring ways of combined different materials to make solar cells with better efficiency, longer life, and at reduced costs.

Recently, Sanyo introduced a HIT hybrid cell whereby a layer of amorphous silicon is deposited on top of single crystal wafers. The effect is an efficient solar cell that performs well in terms of indirect light and is much less likely to lose efficiency as the temperature climbs.

Fig 2.4- Hybrid Silicon Cells

- **Second Generation Solar Cells**

Second-generations cells are typically called thin-film solar cells because when compared to crystalline silicon based cells they are prepared from layers of semiconductor materials only a few micrometers thick. The combination of using less material and low cost manufacturing processes permit the manufacturers of solar panels made from this type of technology to create and sell panels at a much lesser cost.

There are basically three types of solar cells that are measured in this category, amorphous silicon and two that are made from non-silicon materials specifically are cadmium telluride and copper indium gallium dieseline. Together they accounted for around 16.8% of the panels sold in 2009.

First Solar, the number of producer and seller of solar panels in the world currently makes their solar cells using cadmium telluride. The big appeal of these types of solar cells is that they are inexpensive (currently below $1.00 / watt to produce and going towards $0.70 / watt). However, as we discuss in the accompanying articles about cadmium telluride (CdTe) and first there are some concerns about this technology.

Venture capitalists love CIGS solar cells (or at least used to as they have invest over $2.3 billion into companies developing these cells but have yet to see them be a commercial victory) as they have been able to reach efficiency levels of 20% in the laboratory. Regrettably it has turned out to be much more difficult to produce CIGS solar cells in mass quantities at competitive prices with wherever near than efficiency level, so the jury is still out on this technology.

Fig 2.5- Second Generation Solar Cell

Third Generation Solar Cells

At present there is a lot of solar research going on in what is being referred to in the industry as Third-generation solar cells. In actual fact according to the number of patents filed last year in the United States solar research ranks second only to research in the region of fuel cells.

This new generation of solar cells are being made from variety of new materials besides silicon, as well as nanotubes, silicon wires, solar inks using conventional printing press technology, organic dyes, and conductive plastics many more. The aim of course is to improve on the solar cells already commercially available – by making solar energy more capable over a larger band of solar energy (e.g., infrared), less expensive so it can be used by more and more people, and to develop more and different uses.

Currently, most of the work on third generation solar cells is being done in the laboratory and being developed by new companies and for the most part is not commercially available.

Fig 2.6- Third Generation Solar Cell

III LITREATURE REVIEW

People at present are using electricity to charge their phones. Many other ways are also there to charge a phone like the power bank, batteries etc.

But now we do not regular power supplies because of frequent power cuts and many other problems. The batteries too contain harmful chemicals which are hazardous and can cause pollution.

Fuels are non-renewable sources of energy. Once these get depleted it takes lot of time for them to replenish back. When these fuels (in batteries) are consumed, firstly they do cause pollution and secondly they get depleted. Many people at present use portable power banks too. But the disadvantages of using them is

- They drain your battery very fast. Plugging smart phones to the power banks for a prolonged time makes the battery life of phones run shorter than it already did.
- They are highly expensive.
- There are power banks that are heavy and bulky. If they are not conveniently shaped they might be awkward to bring around. Moreover these power banks themselves need to be charged first.

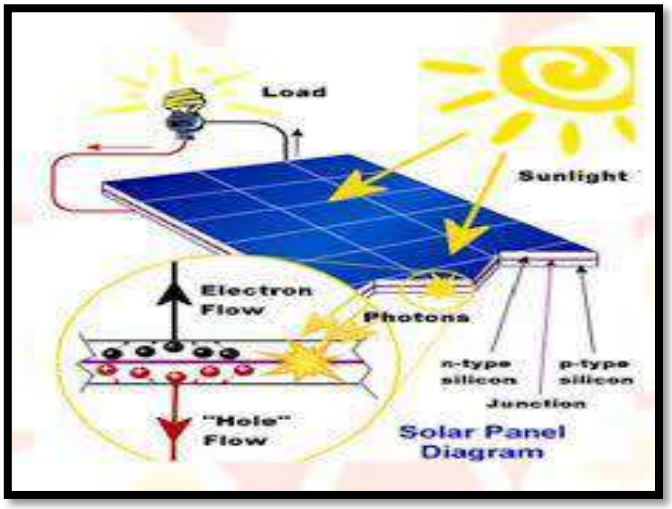
Why struggle with all these problems when the best and safe solution is right above us-THE SUN. Using this renewable source all these disadvantages can be cut-off and also eco-friendly!!

Bangladesh is a developing country with full courage to be developed by 2021. But the main factor of development i.e. electricity has not reached its daily demand yet. The present power scenario in Bangladesh is that they greatly rely on fossil fuels for its energy. Here coal is still the major fuel for power generation. Solar energy is a great source for solving power crisis in Bangladesh. Not only in Bangladesh but in other countries too. They get a lot of sunlight each day throughout the year. Till now, the national capacity of renewable energy based on solar power is 1MW. There is a lot of achievement in solar home system, water pumping system etc. Even the government has taken initiatives for utilization of renewable energy sources for electricity generation.

Fig 3.1- Solar panels on roof tops

IV PROPOSED SYSTEM

In this paper, we propose the system of charging a phone using solar power. Using this solar cells, harmful emissions, dependence of fuels and energy crisis can be solved. Instead of mobile phones, a rechargeable battery (like lithium batteries) can be used to store the energy which can be used for future purpose. All the drawbacks stated above can be easily solved utilizing this solar energy using solar cells. Seriously this is the best way to charge a phone. We just don't want to wait until the power comes or anything, if the battery is low then just connect the phone to the simple circuit design and lay back and can carry on with other works.

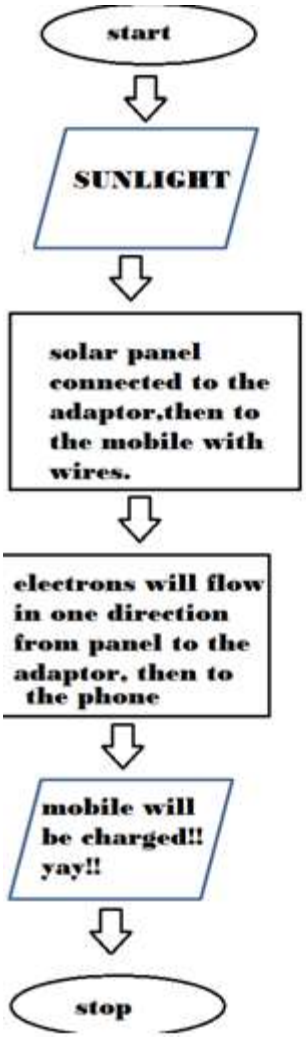


4.1 Architecture of proposed System.

Solar cells basically convert solar energy into electricity. Whether they're embellishing the calculator or orbiting the planets on satellites, they depend on the photoelectric effect: the ability of matter to emit electrons when a light is shone on it.

A solar cell consists of a semi-conductor material: silicon which is the key ingredient to these cells. Sunlight which is radiated from the sun consists of photons. When these hit the silicon atoms they transfer their energy to lose electrons, knocking them off the atoms.

Freeing up electrons is however only half the work of solar cells. These electrons are attracted to the positive charge in the n-type silicon and repelled by the negative charge in the p-type silicon. This creates electric field across the cell. This field drives them along in an orderly manner which provides electric current. Connecting wires across the junction will have a current in them.



4.2 Flowchart of the proposed system.

V ADVANTAGES

1."solar energy is renewable", this the very first benefit of using this technology, 100% eco-friendly.

2. In this technology, green house gases, harmful agents, volatile material and carbon dioxide are released into the environment.

3. It is the most useful technology for the users in remote areas.

4. Solar panels are reliable and highly durable. Since they do not have any moving parts, replacement is not required.

5. The solar cell technology can be used to generate thousands of hours of electricity with minimum maintenance.

6. The energy is extracted from sun without any noise. So, these solar cells are totally silent.

7. Although solar panels are expensive, it is one time investment. We do not have to pay for energy from sun.

8. We can lower our monthly electricity bills.

9. High intensity in summer season.

VI APPLICATIONS

These solar panels which contain solar cells can be placed anywhere like on rooftops, cars, laptops, cell phones, etc. It's cheap and is durable. Soon this will be the source of electricity. It is a onetime investment. Solar cells/solar panels have so many applications in domestic fields, telecommunication, charging devices, etc; solar pumps are used for water supply. In telecommunication field, for example, radio transceivers on mountain tops, even telephone boxes can be solar powered. The satellites in the space get electrical power because of these solar cells itself. In ocean navigation aids- many lighthouses get power supply from solar cells. We can charge multiple devices by using these solar cells simultaneously.

Fig 10.1.Solar keyboard

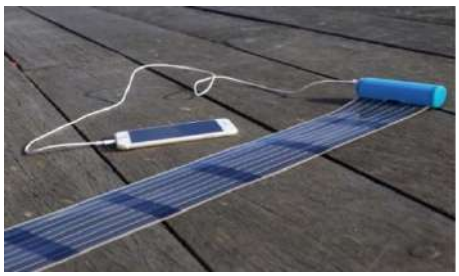


Fig 10.2.Charging a mobile

Fig 10.2- Other applications

CONCLUSION

Energy must be conserved and used efficiently. It's also up to all of us who create new energy technologies in future. All energy sources have an impact on the environment. Solar energy has the biggest impact so we can utilize it as much as possible. Battery life is more as high voltage are not developed. Versatility of solar mobile charging using panel is very high. Life of battery is very high.

Conserving the world is one of the people's responsibilities and so we hope that this solar cell will be widely used soon so as to provide another clean and cheap energy source. Argument that sun provides power only during the day is negated by the fact that 70% of energy demand is during daytime hours. At night, traditional methods can be used to generate electricity. The main intension is to reduce the dependence on fossil fuels.

REFERENCES

[1] http://www.scirp.org/journal/msa

[2] http://dx.doi.org/10.4236/msa.2015.612113

[3] http://dx.doi.org/10.4236/msa.2015.612113

[4] www.main.org/polycosmos/glxywest/vimanas.html

[5] http://en.wikipedia.org/wiki/solar_cell

[6]http://www.planetarypower.com.au/solar_panels.html
[7]http://www.earthtimes.org/energy/solar-cells-future/1403

[8] www.howstuffworks.com

[9]vwww.solarcell.net.in

[10] Aldus, Scott. "How Solar Cells Work." How Stuff Works. 22May2005.

GPS Locator: Dynamic location device

Hemanko Baidya[1], Dr.S Usha S[2]
[1]UG Scholar, [2]Professor ,Dept of CSE, RRCE, Bengaluru
E-Mail: hemanko@gmail.com, ushasakthivel@gmail.com

Abstract: ***This document depicts the working and implementation along with the bushiness class and possible future enhancements for a dynamic GPS locator System.***

Keywords—GPS, LI-FI, IRNSS, IDE, IoT , UAV, Zigbee, GAGAN, NAVIK.

I. INTRODUCTION

In today's era the matter of security is a big concern, whether it be in office or school or transport. For this reason the device is made to locate the precise location of the target body. A GPS locator unit is a device, normally carried by a moving vehicle or person, that uses the Global Positioning System to determine and track its precise location, and hence that of its carrier, at intervals. The recorder location data can be stored within the tracking unit, or it may be transmitted to a central location database, or it may be transmitted to a central location database or internet connected computer, using a cellular (GPRS), radio, or satellite modem embedded in the unit. This allows the access location to be displayed against a map backdrop either in real time or when analyzing the track later, using GPS tracking software. Data tracking software is available for smart phones with GPS capability. A GPS navigation device and a mobile phone sit side-by-side in the same box, powered by the same battery. At regular intervals, the phone sends a text message via SMS or GPRS, containing the data form the GPS receiver.

The results can be translated into ASCII values for human readability using simple programs or it can be kept as it is for direct machine implementation. Section II discuss about the existing system. Sec III discusses about the implementation section IV discusses about the problems in present system. Sec V talks about the proposed system. Sec VI contains the Requirements specifications. Sec VII gives the conclusion. and finally followed by references.

II. EXISTING SYSTEM

The device is designed in a 2 module system where one module serves as the transmitter and the other serves as a receiver. This is based on the GPS architecture and works with a Bstar BS_280 GPS module. The entire system is controlled by an arduino mega microcontroller and the communication is established by a pair of Zigbee modules. The entire programming process took place in the Arduino IDE and the setup of the Zigbee module is done on the XCTU software. the gathered information is displayed in the form of NMEA codes those are long strings of data gathered in different formats according to the need of the user by the GPS module.

- The existing system loses functionality in heavily cloudy weather.

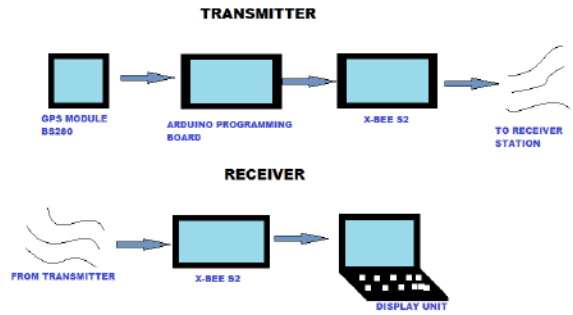


Fig 1: NMEA block diagram

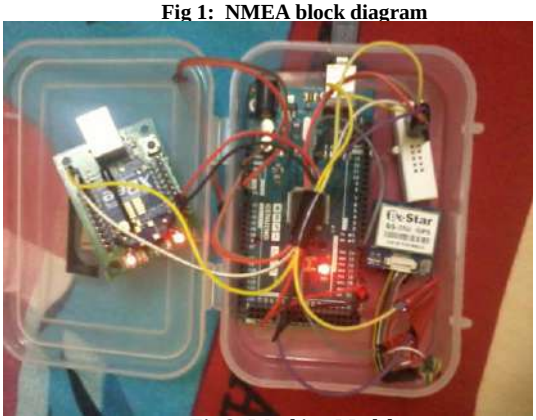


Fig 2: Working Model.

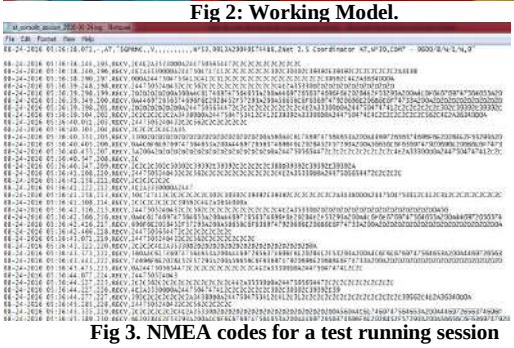


Fig 3. NMEA codes for a test running session

III. IMPLEMENTATION

There is endless implementation of this device. Basically every field where the knowledge of location and motion is necessary, this device can prove its worthiness. From security applications to simple monitoring everything can be accomplished using the dynamic GPS locator. Unlike the built in GPS of the mobile devices this can be utilized with any device or products.

It's also cheaper than the readily available independent GPS modules and helps program the output according to the will and need of the user. Situations such as disaster management and UAV navigation are the ideal situations for the application of this project.

IV. PROBLEMS WITH EXISTING SYSTEM

- The radio modules are prone to damage on long run and takes up a lot of power.

- The retrieval of data requires another set of programs

V. PROPOSED SYSTEM

With the rise in technological advances in IoT and India's advances in satellite navigation systems there can be immense enhancements in the modular aspects of the device. The major of them are replacing the GPS module with GAGAN or NAVIK to make it indigenous and more accurate.

With the recent completion of the 7 satellite navigation system by the Indian space research organization (ISRO), the transition from the GPS to IRNSS will be very simple as soon as the front end chips are released for the public. Apart from that, the Zigbee modules can be accompanied by LI-FI Trans-receivers that will enable the module with under water communication and Hence enhancing its margin of applications.

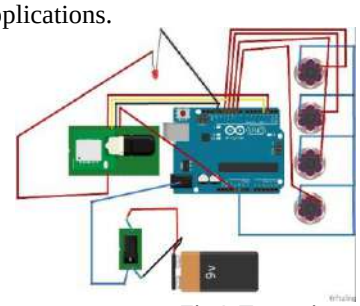


Fig 4: Transmitter diagram

VI. REQUIREMENTS

Software Requirements:

1. ARDUINO IDE
2. XCTU
3. COOLTERM

for each and every different application.

Hardware requirements

1. ARDUINO MEGA BOARD
2. GPS LOCATOR

3. ZigBee module

CONCLUSION

In the recent years the accessibility to sensors and ease of programming has motivated the development of many personalize, portable and compact devices that facilitates the day-to-day activities, GPS locating which was recently limited to only the industry and to the most financially sophisticated divisions of the society is now accessible at a very affordable price that increases its accessibility to the common people through this project.

REFERENCES

[1]G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)

[2]J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[3]I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[4]K. Elissa, "Title of paper if known," unpublished.

[5]R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6]Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7]M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

CONCEPTS OF FIREWALL TECHNOLOGY IN NETWORK SECURITY

AasthaMishra[1] , Meghana R Salagundi[2],Anitha K[3]

[1,2] UG Scholar, [3] Asst.Professor, Dept. of CSE ,RRCE, Bengaluru

E-mail:aasthamishra1406@gmail.com , meghanasalagundi@gmail.com

***Abstract*-Computer security, also known as cybersecurity or IT security is the protection of information systems from theft or damage to hardware, the software and to the information on them as well as from disruption or misdirection of the services they provide. In computer security a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall is most effective and important first step you can take to protect your network. The firewall monitors all the information traffic to allow 'good data' in, but block 'bad data' from entering your computer. It blocks illegal access to an organization networks. They can be implemented on software or hardware or combination of both. They prevent illegal internet users, especially intranets. It detects source of viruses and other problems that affect the network. In general there are two main technologies, according to which firewall can be categorized: packet filtering and application layer filtering. Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like WWW(World Wide Web) or FTP(File Transfer Protocol). This paper gives a brief description about firewall technology, its working, its types, problems faced while using firewall technology and their solutions and future scopes**.

Keywords*: *network security, firewall technology, firewall technology overview, filter, protocol, traffic

I. INTRODUCTION

Shwetambari G. Pundkaret..al[1].The world is becoming more interconnected by the whole of the advent of the internet and new networking technology. There are currently two fundamental different networks, data networks and synchronous network. The internet is considered as a data network. The synchronous network that consists of switches does not buffer data and thus are not threatened by attackers. Hence security is emphasized in data networks, like the internet and various networks that link to the internet.

The vast topic of network security is analyzed by researching the following

1) History of security in networks.

2) Internet architecture and vulnerable security aspects of the internet.

3) Types of internet attacks and security methods.

4) Security for networks with internet access.

5) Current development in network security hardware and software.

The future of network security is forecasted, based on this research. In order to understand where network security is heading, new trends that are emerging will also be considered.

Over the last few years, there is a pick up in threats to companies and has changed significantly so have the defences. There is a large amount of personal, commercial, military and government information on networking infrastructure world wide. Network security is becoming of considerable importance for intellectual property that can be plainly acquired over the internet. Computer security is a problem that is unbreakable and so is the security on networked computers. But if the machine is connected to the network it is practically harder. The network security is in the network information security. To trim the vulnerability of the computer to the network there are large amount products available. These tools are encryption, authentication mechanism, intrusion-detection, security management and firewalls.

Usually firewall installed before 2005 are often not the best matched for existing threats and cannot defend against a number of newer threats. A firewall is a hardware or software system that prevents unauthorized access to or from a network. Firewalls are computer security systems that protects your office/ home PCs on your network from intruders, hackers and malicious code. Firewalls are software programs or hardware devices that filter the traffic that flow into your PC or your network through an internet connection. Firewalls make it possible to filter the incoming and outgoing traffic that flows to the system. It can use one or more set of "rules" to inspect network packets as they come in or go out of network connections and either allows the traffic through or blocks it. The rules of firewall can inspect one or more characteristics of the packet such as the protocol type, source or destination host address, and source or destination port. It can improve the security of the network. They can also be used to do the following. Guard and padding is the applications, services and machines of an interior network from unwanted traffic of data from the

public internet. Limit or disable access from host of the internal network to services of the public internet. Support network address translation which allows an internal network to use private IP addresses and share a single connection to a public internet using either single IP address or shared pool of automatically assigned public address.Fig 1. Shows a brief description about how firewall manages the traffic.

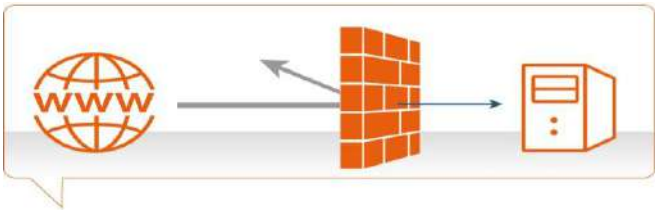


Fig.1. Firewall managing traffic

Firewall manages the traffic using FILTERS. These filters are basically set of rules which are defined in the order of priority. If the packet matched the criteria of the rule then actions of the rule are been applied and if they are not matched then next no action is taken and next set of rules are been checked. There are three most common outcome of the action ALLOW,DENY and LOG out of which most of the actions are ALLOW.

II. WORKING OF FIREWALL IN OUR PCs

Shwetambari G. Pundkaret.al[1].Firewallsuse different methods to filter out data, and some are used in combination. These methods work at dissimilar layers of a network, and this determines how specific the filtering options can be used. To add protection to your home or business, firewalls can be used in a number of ways. In order to secure their networks large organization or corporations often have very complex firewalls in place. Firewalls can also be configured to avoid employees from sending certain types of mails or transmitting confidence data outside of the network. On the inbound side, to stop access to certain websites like social networking sites, firewalls can be programmed. Moreover, outside computers can be prevented from accessing computers inside the network using firewalls. A company chooses to select a single computer on the network for file sharing and all other computers could be controlled. Using firewall there are no limits to the variety of configurations that are possible.

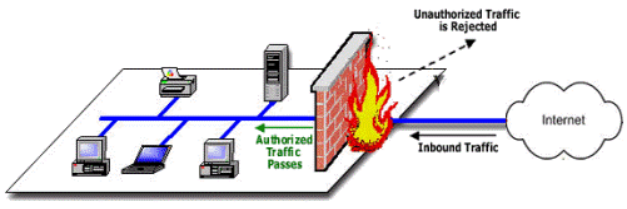


Fig.2. Working of Firewall

Fig. 2. Working of Firewall or residence use, firewalls work much more basically, protecting your personal computer and private network from various threats, is the main goal of firewalls present in the standalone systems. Malware, malicious software, are the main threats to your home computer. The first type of malware that comes to the mindare 'viruses'. Emails or the internet can be the source for the viruses to be transmitted to the systems and injure your files. There are two ways a Firewall can prevent this from occurring. It allows all the interchanges to pass through except data that meets a preset set of criteria. Firewall makes use of the later way to prevent malware from installing onto your computer. This free software firewall, from a global security solutions provider and certification power, uses the patent pending "Clean PC Mode" to disallow any applications from being installed on your computer unless it meets one of two criteria. Those criteria are as follow a) the user gives authorization for the installation and b) the application is on a widespread list of standard applications provided by this firewall. With these features, your awareness is not necessary about the unauthorized programs installing on your computer, and so this firewall is top rated and suggested for both basic and complex users. It has a number of exclusive features including "Defense +," a complex Host interruption Prevention System which is also known as HIPS, which prevents changes to critical system resources. In order for you to regulate this software to your exact needs this software is greatly customizable. To secure millions of computers around the world this Internet Security Suite combines the firewall with a controlling antivirus.

A**.** Firewall technology overview:

Shwetambari G. Pundkaret.al[1].The selection that is less suitable for a router to do, is done by a firewall. A firewalls primary role is filtering, whereas a router primary employment is addressing. Auditing can besides be done by firewalls. Even more significant, router is worried only with source and destination MAC and IP addresses whereas firewall can recognize at an entire packet's contents, including the word area. Three dominating types of firewalls are in common use today: packet filters, application gateways and stateful inspection firewalls.

*1) Packet Filters:*Packet filters are the simplest form of firewall. Any IP packet that attempts to knock the firewall at variance with its access control list will be evaluated by this packet filter firewall. It is once sent from first to last if the packet is certified. If not, the packet filter can either send back an ICMP fault response or drop the packet. Packet filters only watch at five things: the source and destination ports, source and destination IP addresses and the protocol such as UDP, TCP/IP, and so on.

*2) Application Gateways:*An application gateway goes a step on top of everything than packet filters. It typically looks at the application layer data, rather of barely checking

the IP parameters, Single application gateways are regularly called proxies, such as an SMTP (Simple Mail Transfer Protocol) proxy which understands the SMTP protocol. The data that is being sent is checked by these and authenticate to visualize whether that particular protocol is being used perfectly.

*3)Stateful Inspection:*In computing, the stateful inspection firewall keeps track of the state of network associations (such as TCP streams, UDP communication) travelling contrary to it. For diverse types of connections,the firewall is programmed to differentiate legal packets. Onlythose packets which are much the same is an active connection and will be allowed by the firewall; others will be unwelcome in inspection, furthermore referred to as Dynamic Packet Filtering, which is a security feature.

III. PROBLEMS FACED BY FIREWALL TECHNOLOGY

1) Cost: The charge of adding firewall "brains" to the inner of the network is substantial, particularly compare to the continued cost reduction of standard networking switches and routers.

2) *Performance:*Firewalls have proven themselves on Internet-speed links, but approximately enterprises have significantly higher hover rates within the join than towards the Internet. Common tasks a well known as claim sharing and backups would draw a firewall designed for Internet speeds to its knees on a 100 Mbps Ethernet link.

*3) Management:*Most firewall vendors have bottom it challenging to infer management in many-to-many relationships. Generally, the three-legged firewall (outside, inner, DMZ) is roughly as detailed as they gain, and having infinite firewalls in a hit configuration has been a difficult lag to deny elegantly. While small number vendors forthwith cleanly evaluate dozens of ports, touching this to thousands and managing access control dynamically contrary across to hundreds of network elements is a challenge.

*4) Policy***:** Network managers face it agile to figure it to save thing as it relates to the Internet, yet clash it for all practical purposes more deep to represent what are permitted and denied flows within the university itself. If you can't infer practice, previously you can't study a firewall to bring about that policy.

*5) Authentication:*Users on the network have traditionally not authenticated themselves at layers 2 and 3; they connect to applications and underwrite at that level. However, for network-layer security, authentication of "who is on the wrong track there" intend be tightly skip to the user.

*6) Binding:*As packets flow through a network, it's spiritual to assign security policies anywhere yet at the undue edge. The part and parcel of unit of access got a handle on something is continually the junkie, but packets aren't dump to a contrasting user. Making a solid binding during a user-based policy and a mint that has a temporary IP study is a moratorium for which there's no standards-based solution.

IV. FIREWALL MANAGEMENT

5 CHALLENGES EVERY COMPANY MUST ADDRESS

- *Business Challenge #1:*Assessing the risk of the firewall policy
- *Business Challenge #2:* Managing firewall changes
- *Business Challenge #3:* Maintaining optimized firewall rulesets
- *Business Challenge #4:* Keeping up with rules and regulations
- Business Challenge #5: Proving where things stand

A. Assessing the risk of the firewall policy:

David L. Drakeet.al[12].As networks are becoming greater complex and firewall rulesets restore to surge in length, it is moderately difficult to notice and quantify the spin of the roulette wheel that is instructed by misconfigured or overly tolerant firewall rules. The profession contributor to firewall practice risks is call for of the pertinent understanding of doubtless what firewall is doing at any time. Serious IT and network security professionals are regularly thinking about the choices they're making today, and the resulting risks those choices gave a pink slip create against forward. Everything you and your set do familiar to your firewall policies moves your network as a substitute towards outstrip security or added risks. Even the most gifted firewall administrators gave a pink slip make above suspicion mistakes. You'll never be sure of what place things quit until you have the consistent visibility.

B. The Solution:

The best approach for minimizing firewall procedure risks is to assure you—and management—understand what there is to lose. Use capable network and firewall architectures to your advantage and then lean on automated management tools to aid find and remedy the security risks before they grow out of control. Solid automated management tools can employ widely-accepted firewall best practices and analyze your current environment to highlight gaps and weaknesses. Some tools can also aid tighten overly tolerant rules by pinpointing the traffic that is actually flowing through any supposing rule.Combining manual policy analysis with the right tools allows you to be proactive with firewall security rather than finding out roughly the risks once it's too late.

C. Managing firewall changes:

E. Al-Shaer et.al[13].In IT, things are regularly in a state of flux. Managing all the changes is one of the biggest problems that businesses face. As mutually most things in IT, there's not a easily done solution for managing changes

by default—especially when it comes to firewalls. Still, not smoothly managing changes can conduct to serious business risks, from issues as benign as legitimate traffic being blocked, for the most part the way to the entire business network going offline and businesses being hacked.Many factors contribute to problems with firewall change management, anyhow the prevalent culprits are:

*1) Lack of reserved policies:*In the frame of reference of firewalls, rulesets—or policies—are often confused with formal information security policies.

*2)Loose processes that aren't taken seriously:*Its one capacity to have a policy stating "this is what we must do," but quite another to have a formal set of steps for carrying out and enforcing that policy. Firewall change management requires perfected and concise steps that everyone must inherit when changes are needed.

*3) Poor air mail amid IT staff:*Another real barrier to network security expansion is poor communication bounded by those responsible for keeping the firewall environment in check.

*4) Not breadth of view the associated job risks:*It's essential to get what the business is up against from the point of view of threats and vulnerabilities. What's constantly overlooked, however, is the impact poorly-managed firewall changes have on the business

*5) Network complexity:*The sheer complexity of any supposing network can conduct to a lot of mistakes, specifically when it comes to multiple firewalls with complex rulesets. Complexity is the rival of security, and you need to do and all it takes to simplify your firewall environment and management processes.

*6)Not breadth of view the strength of firewall changes:*Not analyzing and thinking over how ultimately the smallest firewall changes are going to impact the network environment can have dangerous effects. Without thoughtful analysis you might not visualize things such as:

- Which applications and connections your changes may break.
- Which new security vulnerabilities are going to be introduced.
- How performance and visibility are going to be affected.

D. The Solution:

If you can manage firewall changes consistently over time, formerly you've already won half the battle. You'll not only have a more secure network environment, but you will manage IT to show its final cause by approximately facilitating business rather than getting in the way. To manage firewall changes closely, you crave to act by the whole of regard to a useful set of tools in the right ways. To set up your team for well-being, it's urgent to have well-documented and low-cost policies and procedures, combined with technical controls that boost with enforcement and oversight. The right automated tools can:

• Create and bring about workflows for the divergent processes of security policy changes.

• Leverage topology awareness to regard the firewalls that are affected by a proposed change.

• Simulate the critical point to proactively detect risk or compliance implications before the critical point is implemented.

• Reconcile change requests with the actual changes performed, to identify any changes that were performed "out of process."

E.Maintaining optimized firewallrulesets:

Errin W. Fulpet.al[14].Maintaining a clean set of firewall rules is one of the most important firewall management functions, yet many businesses resume to struggle by the whole of it. Unwieldy rulesets are not just a technical nuisance—they further create business risks, including open ports and unneeded VPN tunnels, conflicting rules that create backdoor entry points, and an tremendous amount of trivial complexity. In addition, bloated rulesets significantly complicate the auditing behavior, which regularly involves a review of each rule and its devoted business justification. This creates inappropriate costs for the business and wastes precious IT time. Examples of firewall rules that can create problems include: Unused rules, Shadowed rules, Expired rules, Unattached objects, Rules that are not ordered optimally.

Another humorous problem occurs when absorb administrators and warranty managers are committed and imitate of their consolidate diagram. Quite regularly there is in turn no bar chart, or the bar chart is absolutely outdated. Firewall rulesets are no different.This express, combined mutually network entanglement and IT governance, cause mismanaged firewall rulesets and their associated business risks.

F. The Solution

Just as firewall change management is a formal process where people are held accountable, firewall ruleset maintenance needs to adopt formalized as well. Proactive and occasional checks can help wipe out rulebase oversights, and allow you to maintain a firewall environment that facilitates security rather than exposes weaknesses. To effectively manage your firewall rulesets, you prefer the right tools. The suited firewall management tools will grant you with the visibility needed to instruct which rules can be eliminated or optimized, and furthermore see the implications of removing or changing a rule. They can further automate the process, eliminating the

need for time-consuming and inaccurate manual checks.You furthermore require to secure that you're managing the rulesets on all of your firewalls. Picking and choosing certain firewalls is like limiting the degree of a security assessment to only part of your network. Your results will be limited, creating a serious false sense of security. It's fine to intensify on your virtually critical firewalls initially, nonetheless you need to address the rulesets across all firewalls eventually**.**

G. Keeping up with rules and regulations:

Keeping up with the various compliance regulations, as well as business partners, client and internal policy requirements, can be quite a challenge. You have to consider things a well known as: What's approximately needed for each regulation or policy. What specific terms management and legal counsel have agreed to in contracts and SLAs. How your current firewall configurations and management practices impact what the business has committed to, or is entitled to.

In reality, if you glare at all of the information security regulations one as PCI-DSS, GLBA and HIPAA, their gist is to bind oneself the confidentiality and morality of sensitive information, and secure the availability of the network and application environment. These are nothing greater than best practices we've known— and implemented—for years**.**

G. The Solution

Given the complexities and nuances of information security regulations, policies and contracts, businesses can't allow to omit what's required and what's at stake. Appoint yourself or someone to stay on top of the regulations affecting your business. If your business doesn't have an official compliance manager, that's generally the greater reason for you to stay connected by the whole of what your business must grip to. Ideally, you crave a formal information security committee consisting of other decision-makers from HR, legal, operations, IT and internal audit. Having the right people on board will ingrain information security responsibility contrary to the organization. It will also aid ensure that for the most part the regulations, policies and contracts anywhere the business is held accountable are accurately communicated.

Keep in mind that the regulations your business is up against are no greater than security best practices that you've likely had in place, in some capacity, before now. Plus, the distinctive regulations are not all told that divergent from one another. By addressing compliance from the bias of higher-level information spin of the roulette wheel management, you can cut back security risks and last to all the regulations across the board. Utilize automated tools that are both network aware (e.g., they recognize which network subnets are intact PCI zones) and security aware (e.g., observant of unwavering PCI requirements or your custom corporate policy). Such tools can assess your firewall policies at variance with compliance regulations and flag exceptions that crave attention.

H. Proving where things stand

Keeping up A sharps and flat aspect of network security is insight: having the significant visibility facing your network and being qualified to prove your security or compliance position at any given time. The need to prove your current security position ties directly into firewall management, rulebase maintenance and so on. We've been proving where things stand by the whole of firewalls for decades. The problem is that we haven't been doing it all that well. There are large amount scenarios in which you wish to comprehend where things stand within your firewall environment, a well known as:

• An IT auditor needs to assess your existing controls.

• Management is approaching better recognize network security.

• You suspect your network is under attack.

• A forensics investigator is analyzing a network breach that has already occurred.

I. The Solution

Being able to prove your current firewall security or compliance situation requires the discipline controls, accurately implemented. This includes technical controls a well known as audit logging and alerts off the rack into your firewalls. Practically all firewall has these controls out-of-the-box, anyhow in large amount cases network administrators and security managers aren't taking advantage of them.The problem with stock solutions is that they can be acquire unwieldy when you have greater than a only a few of firewalls to manage. When you have an enterprise scale deployment that includes sum of firewall vendors, third-party firewall management applications can help take the pain away and enable greater insight into your firewall environment. Such tools can ultimately generate out-of-the-box reports that instantly demonstrate compliance with industry regulations and corporate policies, thus saving valuable audit preparation time.

J. A Case Study in Firewall Mismanagement

A recent incident at an e-commerce company, in which firewall changes went awry, provides helpful insight into how a few mistaken choices can keep up to a monumental failure.The company was a core provider of ecommerce services tobusinesses in the U.S. One day, all e-commerce transactions in and out of their network ceased. The entire business was taken offline for a number of hours. It ended up as a few members of the firewall team who had made some out-of-band (and untested) changes to a core firewall that broke thecommunication between the ecommerce

application and the rest of the Internet. Because of the incident, executive management got engaged and the blamable IT staff members were reprimanded. Hundreds of thousands of dollars eventually, the root cause of the outage was revealed: IT staff chose not to test their firewall changes—bypassing their "burdensome" ITIL-based change management procedures—and unanswered the consequences.

K. Moving Forward

Firewall management is regularly out of sight and out of mind. However, what may seem inconsequential or unimportant with firewalls can have a huge impact on the business if something goes awry. Never neglect that IT is there for the business. Do what it takes to set up yourself, your network administrators and your business for success. Looking further, the bits and bytes to instruct the business tie-ins that network security and firewall management have. Ensure you're using the right tools and have reasonable processes in place that support you to make informed network security decisions and provide value with little to no impact on the business.You must be efficient to get insight directed toward your network, and then manage it commonly on an continuous basis. Without the significant tools and processes, it will be difficult to claim that you have a secure and stable firewall environment that's ready to take on whatever comes your way.

B. NEXT GENERATION FIREWALLS

As we have seen so far compared to the features provided by previous generation of firewalls the next generation firewalls promise to provide us with better, faster and more intelligent solutions. Deeper packet analysis, built in intrusion, application-aware capabilities and integrated anti-virus technologies are just some of the features that these next generation firewall promise will better secure our networks.

CONCLUSION

Computer security is a complicated issue, involving many aspects of computer technology, network management, network usage and maintenance. In order to increase computer security, we should mix various types of applications for protection measures. It is necessary to develop more effective security solving measures, thereby to improve the computer network security. Now a day, the firewall furthermore has its own limitation, which does not go through firewall's process; the firewall is helpless, if it is secure in the network through SLIP and the PPP way directly and is mutually the relationship of internal user, will then creates the solid hidden danger. The protection that firewalls extend is as profitable as the rule they are configured to execute. The study of real organization data shows that corporate firewalls are constantly enforce rule sets that abuse well established security plan. Finally, by analysing the paper we can say that firewall strategies are user-friendly to the network security

ACKNOWLEDGEMENT

The author gratefully acknowledges the support of management and Dr.Balakrishna R, Principal, RajaRajeshwari College of Engineering, Bengaluru, Dr.UshaSakthivel, Professor, Head of Computer Science Department, RRCE, Bengaluru and my teachers and friends for their invaluable support and encouragement.

REFERENCES

[1]Miss. Shwetambari G. Pundkar, Prof. Dr. G. R. Bamnote, "ANALYSIS OF FIREWALL TECHNOLOGY IN COMPUTER NETWORK SECURITY", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 4, April 2014, pg.841 – 846, ISSN 2320–088X

[2]Wool, "A quantitative study of firewall configuration errors," Computer, vol. no. 6,2004.

[3]Yu Qiu, "Internet network security and firewall technology discussion", Mianyang Normal school journal ,2004.

[4]Rui Wang. Haibo Lin, Network security and firewall technology, Tsinghua university publishing house, in 2000

[5] Kuang Chu, "Network security and firewall technology", Chongqing university publishing house,2005

[6] Tushar Wason and Anubhav Chandra, "Firewall technology in network security" Student, Department of Information Technology Dronacharya College of Engineering, Gurgaon, Hr, India, © 2014 IJIRT | Volume 1 Issue 5 | ISSN : 2349-6002

[7]Jie Shan, "Analysis and research of computer network security", Journal of Chemical and Pharmaceutical Research, 2014, 6(7):874-877, Binzhou Polytechnic, Binzhou, Shandong, China, ISSN : 0975-7384 CODEN(USA) : JCPRC5

[8] W. R. Cheswick and S. M. Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker", Addison-Wesley Publishing Company, 1994

[9]Amandeep Kumar and Harmandeep Singh, "Network Security: A Literature overview", SLIET, Longowal, India, October 2014,International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-10)

[10]William R. Cheswick and Steven M. Bellovin, "Firewalls and Internet Security: Repelling the Wiky Hacker", Addison Wesley Publishing Company, ISBN 0-201-Bell Laboratories. 63357-4, 0 1994 AT&T

[11]Hiral B.Patel, Ravi S.Patel, Amit V.Patel, " To study the Risk or Issues of Firewall: Solution with different approach", Acharya Motibhai Patel Institute of Computer Studies, Ganpat University,Kherava, International Journal of P2P Network Trends and Technology- Volume1Issue3- 2011

[12]David L. Drake, Katherine L. Morse, "APPLYING THE EIGHT-STAGE RISK ASSESSMENT METHODOLOGY TO FIREWALLS", ScienceApplications International Corporation 10770 Wateridge Circle San Diego, CA 92121 © 1996 SAIC

[13]E. Al-Shaer and Hamed, " Modelling and Management of Firewall Policies". IEEE Transactions on Network and Service Management, 1(1),2004.

[14]Errin W. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Department of Computer Science, Wake Forest University, Winston-Salem, NC,USA 27109

[15]http://www.algosec.com/wpcontent/uploads/2016/03/Firewall-Management-5-Challenges-Every-Company-Must-Address-WEB.pdf

A STUDY ON SECURITY AND AUTHENTICATION OF QR CODES

Shrivatsa D Perur[1], Vaishnavi N[2]
[1]Asst. Professor, [2]PG Scholar, [1]Dept of CSE, GIT, Belgaum,[2]Dept of CSE, AMCEC, Bengaluru.
E-Mail: perur35@gmail.com, cellociya@gmail.com

Abstract— QR code is network standardized matrix, which was intended for industry of automotives in Japan. The QR Code framework has ended up appreciated outside the car business because of its quick meaningfulness and more noteworthy storage limit contrasted with standard UPC scanner matrix. This paper make note of QR codes fundamentals, its ongoing application in everyday life and examination zones related. With the innovation of cell telephones always developing, particularly in the zone of portable web access, QR codes appear to be a sufficient instrument to rapidly and productively speak URLs to clients. This additionally permits disconnected from the net media, for example, magazines, daily papers, business cards, open transport vehicles, signs, shirts and whatever other medium that can grasp the print of a QR code to be utilized as bearers for commercials for online items. QR code being so adaptable in view of its basic adaptability that it prompts such a large number of assorted field for exploration, for example, expanding information limit, security applications, for example, various types of watermarking and steganography too. Some tests have likewise been done for better acknowledgment of the QR code picture that incorporates scratch evacuation methods. Along these lines, this paper is an endeavor to highlight some of the ideas while considering QR codes.

Keywords— QR code, Universal Product Code (UPC)

I. INTRODUCTION

QR (Quick Response) Codes, are 2D(dimensional) bar codes that encode text strings and were introduced by the Japanese corporation Denso Wave Incorporated [1]. QR codes are considered as the evolution of the one dimensional barcodes. They are able to encode information in both vertical and horizontal direction, thus able to encode several times more information than the one dimensional barcodes. QR codes consist of black and white modules which represent the encoded data. In order to access the encoded data in a QR code, a built-in smartphone camera is used to capture an image of the QR code and then decode it using QR code reader software. There are 40 different versions of QR codes with different data capacities. Version 1 consists of 21 X 21 modules from which 133 can be used for storing the encoded data. Version 40, which is the largest QR code, has 23,648 modules which can be used for storing data. This practically means that it can hold up to 4296 alphanumeric characters.

II. RELATED WORK

In 2002, Clarke et al. were probably one of the first to suggest the usage of camera-based devices as an alternative, more secured authentication method for critical transactions, such as banking operations, and most particularly when connecting from untrusted computers [1]. The amount of camera equipped smart phones around us is increasing so rapidly that mobile based authentication might become a popular method to authenticate in a short time.

In traditional Barcode data capacity is around the only 16 digit.

QR Code Data Capacity:

Numeric Code = 7,089 characters max.

Alphanumeric code = 4,296 characters max.

Fig 1: Comparisons of QR and Barcode

QR codes (Quick Response codes) were introduced in 1994 by Denso-Wave [2], a Japanese company subsidiary of Toyota. Initially, these codes where conceived as a quick way to keep track of vehicle parts, being nowadays extremely popular in Asian countries like Japan, South Korea, China or Taiwan and becoming more and more popular in western countries by the day.

The enhanced version of one dimensional barcode is the QR code. Roughly QR code (Two dimensional) contains 350 times more amount of information than the one dimensional barcode. QR code is matrix form or 2D because it contains the rows and columns for storing the information in two directions. Countries like Japan use the QR code for storing QR code. It is popular over the worldwide that will use for future uses.

As we can see the use of QR code is really just the beginning. At this point, we can implement the authentication using the QR code for all platforms such as PC, tablet and mobile phones. We get the idea from the paper, related to our project and we use multi factor

authentication. Also by using this project we can replace the demand draft and cheque by Cash Card.

III. SYSTEM FEATURES

Following system features will be facilitated:

A. Sign up

1) User information:

User must enter his naming details, address and valid mobile and valid email. The valid mobile and valid email is mandatory for user.

2) System Generated information:

After entering the naming details by the user according to the system will generate automatically unique QR code and OTP to the mobile and email. After the reentering the OTP the registration is successful.

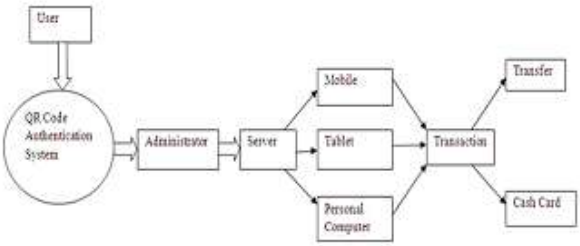


Fig 2: System Architecture

B. Authentication

In order to provide same level of security as a web application, the system shall provide login screen on the user's hardware device. The login entered by the user shall be user ID, password and scan his unique QR code. After matching the user ID, password and QR code OTP will be sent on user's correspondence number and then OTP was reentered by user. The values shall be verified by the system prior the user having access to the system.

C. Transaction

The sensitive information. Nowadays United States also use the QR code. It is popular over the worldwide that will use for future uses. As we can see the use of QR code is really just the beginning. At this point, we can implement the authentication using the QR code for all platforms such as PC, tablet and mobile phones. We get the idea from the paper, related to our project and we use multi factor authentication. Also by using this project we can replace the demand draft and cheque by Cash Card.

Case 1: Online mode authentication: If the phone detects an active Internet connexion, the steps below are followed (refer to Fig.2):

• The encrypted string plus the username are sent to the web server via POST through a secured channel (https). This means that the IMEI and random number are encrypted twice, and the username once.

• The server decrypts the string using the user public key and verifies that a row exists in the transactions table with our random number, updating the row with the IMEI of the user.

• The server checks then that the IMEI is correct and assigned to an user as per the users table.

• In case of success, the transaction row will be deleted and the user authenticated.

• A PHP session is created for the user, being destroyed when the user logs off or when the browser is closed.

Case 2: Offline mode authentication: If the phone detects that the Internet cannot be accessed, the steps below are followed (refer to Fig. 3):

• Using an internal algorithm, a unique six-digit number is derived from the encrypted string. This number is the pincode that the user will need to input in the authentication screen within the web application, along with her username. The pincode is entered through a screen keyboard, in order to avoid keyloggers.

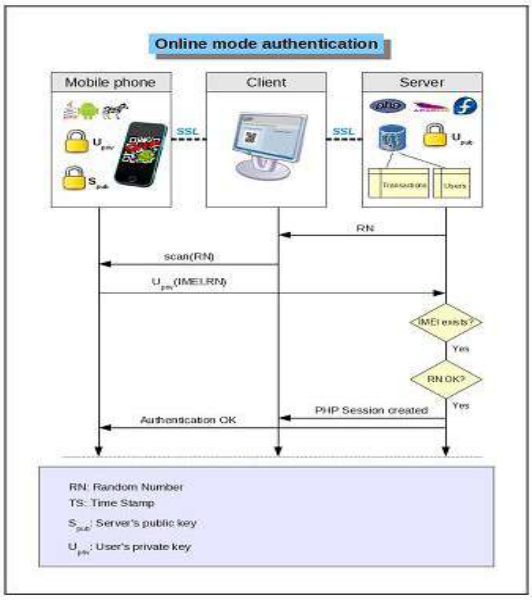


Fig 3: Online mode authentication

• The server receives the username and pincode, recreates the pincode using the user's private key, the random number shown and the user's IMEI, the last stored in the users table.

• The timestamp is also checked, rejecting the authentication if the random number was generated more than 5 minutes ago.

• If the pincode matches, the transaction row is deleted and the user authenticated.

• Once again, a PHP session is created for the user.

IV. ADVANTAGES

***1) Portable*:**

Portability is one of the most noticeable benefits of QR code. As our system is support to all hardware platform devices. Mobiles are Handy and

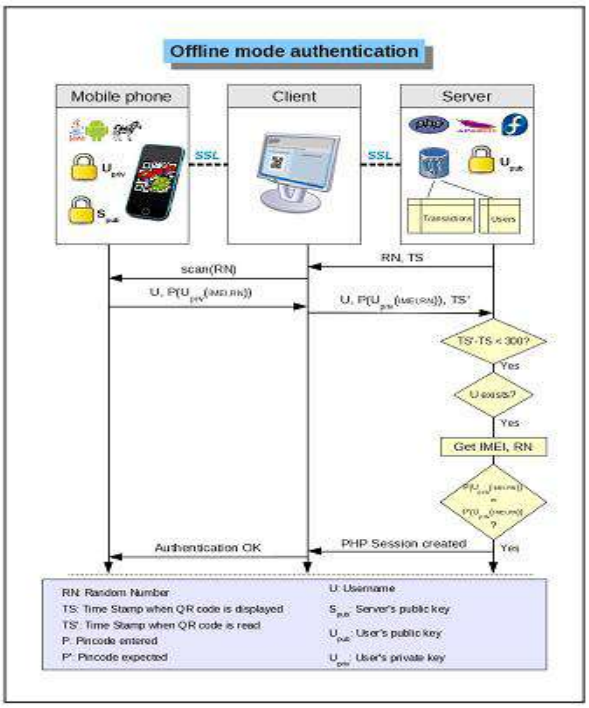


Fig 4: Offline mode authentication

Tablets, Laptops, PCs can be carried anywhere easily.

***2) Real Time*:**

This application System provides real time data about the users interested in QR code.

***3) Low Cost*:**

As QR code can be scanned on any hardware device, it requires low cost and maintenance. All that is maintenance is cell phones with internet access.

***4) Easy to carry*:**

QR code is easy to carry as it can be scan from anywhere to get our authentication and transaction successful.

5) Great deal Resistance to damage:

If the QR code is partially damage then it can also readable.

V. LIMITATIONS

The only disadvantage of QR code based authentication is that it can easily copy, but we provide other supportive activity.

VI. APPLICATIONS

***1) Can replace Smart Card*:**

It requires the separate scanner to scan the smart card. Smart card has less storage as compare to QR code.

***2) Can replace Swipe Card*:**

Swipe card can be cloned, but QR code can't be cloned. Swipe Card has no memory compared to QR code.

***3) Secure way of transaction*:**

QR code is scanned through camera equipped with hardware device therefore our system provides the more secure transaction.

***4) Cash Card*:**

Transfer can be also done using Cash Card which is replicable to Demand Draft and Cheque. System will generate Cash Card with QR code providing secure authentication.

CONCLUSION

This paper gives a brief outline on the security and authentication of the QR codes. Firstly we speak about the system features of the QR codes and then the authentication methods used for the security purposes. Later we discuss about the advantages and the disadvantages of the QR codes. We discuss about the QR code authentication in two cases i.e. online mode and offline mode.

REFERENCES

[1]DENSO Wave Incorporated. What is a QR Code?, 2013. http://www.qrcode. com/en/. Accessed 10 Feb 2013.
[2]QRStuff. What's a QR Code?, 2011. http://www.qrstuff.com/qr_codes.html. Accessed 25 Jan 2013.
[3]Steeman, J. QR code data capacity, 2004. QR4 QR Codes blog: http://blog.qr4. nl/page/QR-Code-Data-Capacity.aspx. Accessed 3 Feb 2013.
[4]A. Sankara Narayanan, QR Codes and Security Solutions :International Journal of computer Science and Telecommunications [Volume 3, Issue 7, July 2012]
[5]Dipika Sonawane, Madhuri Upadhye, Priyanka Bhogade, Prof. Sanchika Bajpai, QR Based Advanced Authentication for all Hardware Platforms International Journal of Scientific and Research Publications, Volume 4, Issue 1, January 2014 International standard ISO/IEC 18004, ―Information technology Automatic identification and data capture techniques Bar code symbology QR Code‖, Reference number - ISO/IEC 18004:2000(E), First edition 2000-06-15
[6]A. Sankara Narayanan, ―QR codes and security solutions‖, International Journal of Computer Science and Telecommunication,Volume 3, Issue 7, July 2012.
[7]Henryk Blasinski, ―per-colorant- channel color barcodes for

mobileapplications: an interference cancellation framework‖,IEEE Transactions on Image Processing, vol. 22, no. 4, April 2013.

[8] Kamon Homkajorn, Mahasak Ketcham, and Sartid Vongpradhip, ―technique to remove scratches from QR code images‖, International Conference on Computer and Communication Technologies (ICCCT'2012), May 26-27, 2012.

[9]Kuan-Chieh Liao, ―a novel user authentication scheme based on QR-code‖, Journal of networks, vol. 5, no. 8, august 2010

[10]Suppat Rungraungsilp, Mahasak Ketcham, Virutt Kosolvijak, and Sartid Vongpradhip, ‖data hiding method for QR code based on watermark by compare DCT with DFT domain‖, International Conference on Computer and Communication Technologies (ICCCT'2012), May 26-27, 2012.

ANTI-JAMMER FOR EMP SIGNALS

Akash R Mannari[1], Usha S[2]
[1]UG Scholar, [2]Professor, Dept of CSE, RRCE, BENGALURU
E-Mail- aakashmannari@gmail.com, ushasakthivel@gmail.com

Abstract - Nowadays the important aspect of an individual is 'Network'. As we are living in the era of Wireless Sensor Networks, the major threats will be its security - suspected to enormous types of attacks. These can be categorized into many categories – Denial Of Service attack (DOS attack). Signal Jammer is one such threat which can be considered as DOS attack. Basic function of this signal jammer is jamming the legitimate nodes at the physical layer which are used to produce signals. This results in decrease of its network performance. As an antidote for this Signal Jamming the concept of Anti-Jamming is being introduced. By this technique it can be assured that the proper signal (network signal) is regained. The Anti-Jamming device is being built in order to destroy the Electro-Magnetic Pulse jammer signals (EMP Jamming signal). It is usually a challenging job to find out whether there is a breakdown in a network or cross connection in the physical layer design. Almost all the signal generating devices use the chargeable battery for their operations at which the pattern can be predicted intervals in the case of EMP Jammers. Hence, in this paper, an instrument is being introduced, named as 'Anti-Jammer'. For the sensor networks (EMP jammers) this mechanism is time-synchronized and modified in such a way that with higher frequencies the patterns gets detached resulting in proper working of the jammed device. Through analysis, simulation and experimentation this paper demonstrates that the Anti-Jammer device's efficiency of any EMP jammer which has the lowest censorship-to-link utilization ratio.

Keywords- Anti-Jammer, EMP Jammer, Wireless networking, DOS attack, ARM7, RTC

I. INTRODUCTION

Initially jamming devices were developed for military purposes. In addition to this, mobile phone is being used individually which uses Electro Magnetic Pulse signals. There are many organizations like Indian Space Research Organization (ISRO), Nuclear Power plant and many other where the mobile phones are prohibited; hence to avoid these they use "EMP JAMMERS", which is basically the electronic countermeasure device (EMC device).

Usually the mobile network transmits a Radio Frequency signal in the frequency range are reserved for particular signals. For example: 2G network uses the bandwidth range from 900MHz – 1200MHz. This results in "no network available" in the mobile phone display. Entire radius of the jamming device – the devices using these signals will be jammed and silenced. Therefore, in this paper, the Antidote for the EMP JAMMER is being explained. This device jams the jammer and breaks down it. This method is called as "ANTI-JAMMER". Mentioning that cell phone jammers are illegal devices in most countries, this report is solely done for educational purposes [1].

II. RELATED WORKS

A. MOBILE PHONE JAMMER

An instrument used to prevent the cellular phones from acquiring signals through the base station is basically called as mobile phone jammer. Jammers can be used practically in any location for its own use but usually exploited in locations where the radio signals of any mobile phones has to be jam-packed. Basic idea of the jammer is to block the radio signals either to send or receive the signals from mobile or signal towers. This device acts as the signal obstacle between the mobile phone signal and the signal receiver tower by producing more frequency than that of the frequency produced by cellular phone. To the highest degree signals utilizes assorted bands to transmit and get into communication from a tower (frequency division duplexing, FDD). Small ranged signals ranging from 800 MHz-1200 MHz (for 2G) within a purview of 30-40 foot depending on its frequency power capacity[2][3].

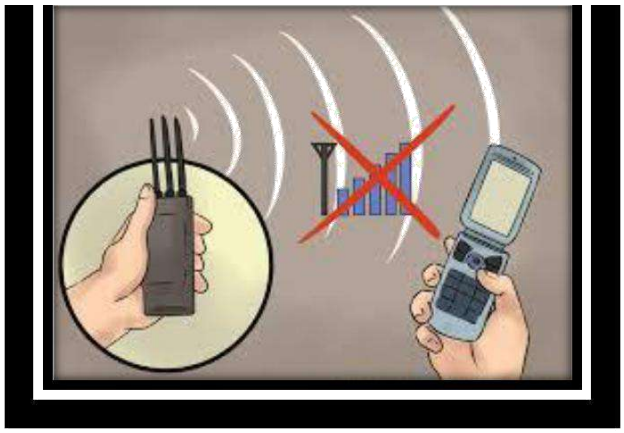


Figure 1: Basic Concept of Jamming device

Earlier the EMP jammers were undermanned on working of only mobile phones which used either digital mobile signals or analog signals defined for cellular phones. Parvenu models (like double and triple band jammers) will block wide range of devices just as CDMA- Code Division Multiple Access, GSM- The Global System for Mobile Communication are even very trenchant against parvenu models which leap to different frequencies[4][7].

B. SPOOFING

EMP jammer steamrolls the cellular phones to switch off the signals automatically. This kind of technique is nasty to be implemented, as the jammers first instantiate all the mobile phone signals in that surrounding rather than selecting the particular signal. Sometimes the cellular phones receive the message to user indicating to switch

the mobile into silent mode. These are the ethical way of spoofing the jammers [11].

C. SHIELDING ATTACK

Electromagnetic field shielding (EMF shielding) or the TEMPEST are basically known as the two types of shielding attacks. Shielding attacks requires a stoppered circumference within a faraday range so that the device generating the electronic signals in this range will not be able to communicate between the signals.

D. DENIAL OF SERVICE

Denial of service usually referred to as DOS attacks, transmits a noise signals at the correspondent operating frequency of the mobile ranging signals. This drops off the Signal-to-noise Ratio (SNR) of the mobile phone signals with its minimal value [5]. This method of is of the following type; Mobile jammer circuit including IF section, RF section, Antenna and power supply. Jammers can impose on any frequencies usually are effective on Aviation Mission Planning System (AMPS), Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), The Global System for Mobile Communication (GSM), Personal Communication Services (PCS), DCS systems.

III. PROPOSED SYSTEM

Any disease erupted will get an antidote, for any problem occurred the solution will be found out. Similarly this paper gives the solution for jammer devices used as non ethicals. Basically ANTI-JAMMER acts as an antidote for the JAMMER device. Meaning by using the proposed device jams the jammer itself. Firstly, the ANTI-JAMMER device uses the reverse engineering concept of the Jammer device. This device creates more frequency than that of the frequency created by the jammer resulting in breakdown of the signals, and the actual signals are recovered.

Basic idea of this device is to shut the capacitors down used in Jammer device, so that it cannot be regained. Anti-Jamming techniques for all the four types of attacks are explained below;

ANTI-JAMMING TECHNIQUES

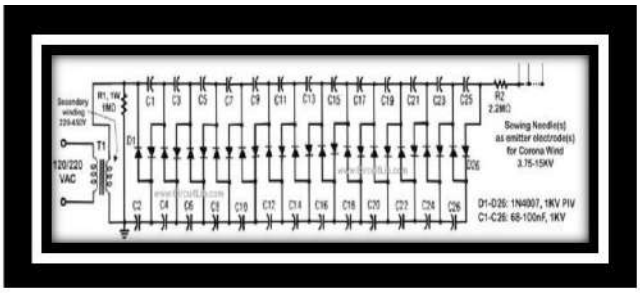


Figure 2: Circuit Diagram of Air Ionizer

A. Anti-Jammer foregathers the jammed signal and crushes the jammer circuit internally. The frequency should range more than 2500MHz – 3000MHz. This device uses Air ionizer connected to the igniter. As and when the ignition is more than the frequency increases as desired to block the signals. This just blocks the capacitor without any destruction. The transistor and capacitor are connected in series in order to produce higher desired frequency [9] [10].

B. The cross section of the Anti-Jammer is shown below. In order to destroy the capacitor in the Jammer device the high voltage converter is used. High voltage converter blocks the capacitance of the capacitor by the virtual connection. These are connected to an Ion-Lithium battery for a better performance.

Figure 3: Cross-section of Anti Jammer

C. Anti-Spoofing technology can be used when a cellular signal is jammed with taking a more time to target the cellular phones and process it. Any major organization having any kinds of threats of getting their devices jammed will be having a building system control at different place. The control system recognizes the circumference where its bee jammed and this technology of Anti-Jamming is brought into that circumference and operated in order to recover the original signals. Figure 4 justifies the block diagram of working of the Anti-Jammer. Firstly the power source from the battery will produce required amount the power to the IF-section to the 12V Air Ionizer which is then sent to the RF-Section to high voltage convertor[6][8].

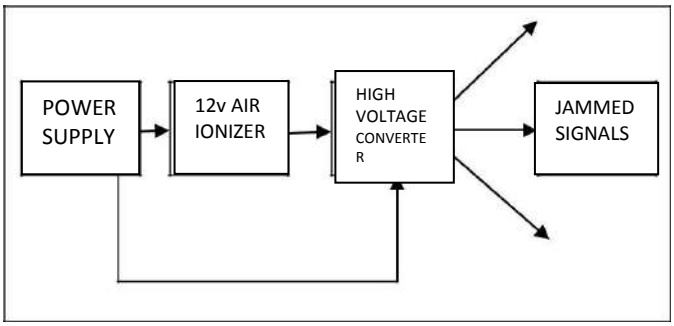


Figure 4: Flow Chart of Anti-Jammer

D. In the design, the frequency of jamming should be same or more than that of the downlink frequency. This is to be done because it needs lower power than the uplink range. As the frequency increases the base station itself gets damaged. The design will be as followed:

GSM 900MHz → 960 MHz – 1500 MHz

GSM 1800MHz → 1885 MHz – 1965 MHz

E. Sometimes there will be a requirement of keypad connected in the device in order to select the signals which to be blocked. These are programmed into the device if desired [9].

Table 1: Operating Signal bandwidths

	UPLINK (Handset Transmit)	**DOWNLINK** (Handset Receive)
GSM 900	890-915 MHz	935-960 MHz
DCS 1800	1710-1785 MHz	1805-1880 MHz

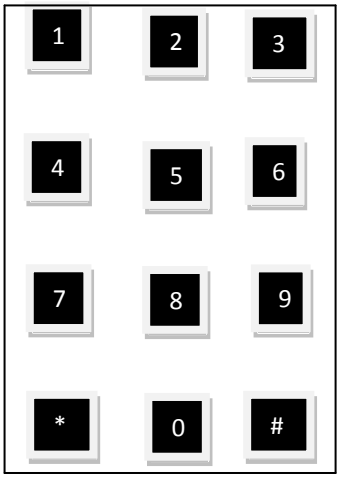


Figure 5: Keypad

IV. RESULT ANALYSIS

Figure 6: Hardware Design / Deactivation of Jammer and activation of Anti-Jammer

Figure 6 shows the hardware design of the mobile jammer with pre-scheduled time duration. It includes the Jammer, Anti-Jammer, ARM 7, keypad and relay. When the time schedule arrives in RTC the jammer will be activated with the help of relay and disrupt the communication system. This will be shown in fig6.

CONCLUSION

This paper is successfully completed using Mobile jammer, Anti-Jammer, and ARM7. By this system, we can deactivate all the jammed signals at any location. This device can be applied in many places like;

- If the military Database is Jammed.
- In the War field, if the Radio signals are Jammed.
- In any of the organization where the signals might be jammed.

The design device works within the small range, with the proper installation and equipment; this can be transformed into a bigger device with a wider distance.

ACKNOWLEDGEMENT

The author gratefully acknowledges the support of management and Dr. Balakrishna R, Principal, RajaRajeshwari College of Engineering, Bengaluru, Dr.Usha Sakthivel, Professor, Head of Computer Science Department, RRCE, Bengaluru and my teachers, friends and family for their invaluable support and encouragement.

REFERENCES

[1] www.HowStuffWork.com
[2] En.wikipedia.org/wiki/Mobile_phone_jammer
[3] Multitopic conference2008.INMIC 2008.*IEEE* International
[4] "Zone of silence [cell phone jammer]," *Spectrum, IEEE, vol.42, no.5, 18,*May 2005
[5] Sami Azzam, Ahmad Hijazi, Ali Mahmoudy. "Smart Jammer for mobile phone systems"
[6] Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, "Use of jammer and disabler Devices for blocking PCS,Cellular & Related Services"
[7]Ahmed Jisrawi, "GSM 900 Mobile Jammer", undergrad project, JUST,2006.
[8]John Scourias Overview of the global system for Mobile communications,http://ccnga.uwaterloo.ca/~jscouria/GSM/gsm re port.html#1
[9] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, (2002) "A survey on sensor networks", IEEE Communication. Mag., pp. 102-114.
[10]Cagalj M; Capkun S; Hubaux J.P; (2007) "Wormhole-Base Antijamming Techniques in Sensor Networks," Mobile Computing, IEEE Transactions on, vol.6, no.1, pp.100-114.
[11] P.Naresh, P. Raveendra Babu, K.Satyaswathi; Dept of ECE, CMR College of Engineering&Technology Hyderabad, AP-India. "International Journal of Science, Engineering and Technology Research (IJSETR)" Mobile Phone Signal Jammer for GSM, CDMA with Pre-scheduled Time Duration using ARM7.

Survey on Virtual Grid-Based Dynamic Routes Adjustment (VGDRA) for Mobile Sink-Based Wireless Sensor Networks

Shruti B Karki[1] , Anitha K[2]

[1]PG Scholar, [2]Asst. Professor. Dept. of CSE, RRCE, Bengaluru.

shruthikarki@gmail.com ,anithakrishna14@gmail.com

Abstract-Exploiting the sink mobility has been considered as a good strategy to balance the nodes energy dissipation in wireless sensor networks. The data dissemination to the mobile sink is a challenging task for the resource constrained sensor nodes due to the dynamic network topology caused by the sink mobility. The nodes need to reconstruct their routes toward the latest location of the mobile sink, which undermines the energy conservation goal. This results in the efficient data delivery. In this paper, we present a virtual grid based dynamic routes adjustment (VGDRA) scheme that aims to minimize the routes reconstruction cost of the sensor nodes. This maintains nearly optimal routes to the latest location of the mobile sink. We propose a set of communication rules that governs the routes reconstruction process which requires only a limited number of nodes to readjust their data delivery routes toward the mobile sink. Simulation results demonstrate reduced routes reconstruction cost and improved network lifetime of the VGDRA scheme when compared with existing work.

Index Terms-Routes reconstruction, energy efficiency, mobile sink, wireless sensor networks.

I. INTRODUCTION

WIRELESS Sensor Network (WSN) is a self-organized network of tiny computing and communication devices (nodes) that has been widely used in several un-attended and dangerous environments. In a typical deployment of WSN, nodes are battery operated. Here they cooperatively monitor and report some phenomenon of interest to a central node called sink or base-station for further processing and analysis. Traditional static nodes deployment where nodes exhibit n-to-1 communication in reporting their observed data to a single static sink, gives rise to energy-hole phenomenon in the vicinity of sink. Sink mobility introduced i not only helps to balance the node's energy dissipation but can also link isolated network segments in problematic areas. In addition, several application environments naturally require sink mobility in the sensor field. For example in a disaster management system, a rescuer equipped with a PDA can move around the disaster area to look for any survivor. Same way, in a battlefield environment, a commander can obtain real time information about any intrusion of enemies, scale of attack, suspicious activities etc via field sensors while on the move. In an Intelligent Transport System (ITS), sensor nodes deployed at various points of interest - junctions, car parks, areas susceptible to falling rocks, can provide early warnings to drivers (mobile sink) well ahead of their physical approach.

Exploiting the sink's mobility helps to prolong the network lifetime thereby alleviating energy-hole problem. However, it brings new challenges for the data dissemination process.

Unlike static sink scenarios, the network topology becomes dynamic as the sink keeps on changing its location. Nodes need to keep track of the latest location of the mobile sink for efficient data delivery. This is to cope with the dynamic network topology. Some data dissemination protocols propose periodic flooding of sink's topological updates in the entire sensor field which gives rise to more collisions and thus more retransmissions. Frequent propagation of sink's mobility updates should be avoided as it greatly undermines the energy conservation goal. In this regard, to enable sensor nodes to maintain fresh routes towards the mobile sink while incurring minimal communication cost, overlaying based virtual infrastructure over the physical network is considered as an efficient approach. In the virtual infrastructure based data dissemination schemes, only a set of designated nodes scattered in the sensor field are responsible to keep track of sink's location. Such designated nodes gather the observed data from the nodes in their vicinity during the absence of the sink and then proactively or reactively report data to the mobile sink.

In this paper, a novel scheme called Virtual Grid based Dynamic Routes Adjustment (VGDRA) is proposed for periodic data collection from WSN compared to the existing solutions . This improves data delivery performance either by employing multiple mobile sinks or by deploying super nodes at strategically important points in the sensor field. The proposed scheme does not impose any such constraints. It aims to optimize the trade-off between nodes energy consumption and data delivery performance using a single mobile sink while adhering to the low-cost theme of WSN.

The proposed scheme enables sensor nodes to maintain nearly optimal routes to the latest location of a mobile sink with minimal network overhead. It partitions the sensor field into a virtual grid of K equal sized cells and constructs a virtual backbone network comprised of all the cell-headers. Nodes close to the centre of the cells are appointed as cell-headers, which are responsible for data collection from member nodes within the cell and

delivering the data to the mobile sink using the virtual backbone network. The goal behind such virtual structure construction is to minimize the routes re-adjustment cost due to sink mobility so that the observed data is delivered to the mobile sink in an energy efficient way. In addition, VGDRA also sets up communication routes such that the end-to-end delay and energy cost is minimized in the data delivery phase to the mobile sink.

The mobile sink moves along the periphery of the sensor field and communicates with the border cell-headers for data collection. The routes re-adjustment process is governed by a set of rules to dynamically cope with the sink mobility. Using VGDRA, only a subset of the cell headers needs to take part in re-adjusting their routes to the latest location of the mobile sink thereby reducing the communication cost. Simulation results reveal decreased energy consumption and faster convergence of VGDRA compared to other state-of-the art.

II. RELATED WORK

Several virtual infrastructure based data dissemination protocols have been proposed for mobile sink based WSN in the last decade. The data collection or dissemination schemes can be classified into controlled and uncontrolled sink mobility schemes based on the mobility pattern exhibited by the sink in the sensor field. In controlled sink mobility schemes [7]-[10], the mobility (speed and/or direction) of the sink is manipulated and controlled either by an external observer or in accordance with the network dynamics. The uncontrolled sink mobility based schemes are characterized by the fact that the sink makes its next move autonomously in terms of speed and direction. This paper considers the uncontrolled sink mobility environments and in the following lines, we briefly describe the related works in this context including their methodology and the relative strengths and weaknesses.

Chen et al. [1] presented a converge-cast tree algorithm called Virtual Circle Combined Straight Routing (VCCSR) that constructs a virtual structure comprised of virtual circles and straight lines. A set of nodes are appointed as clusterheads along these virtual circles and straight lines. Together the set of cluster-heads form a virtual backbone network. The sink circulates the sensor field and maintains communication with the border cluster-heads for data collection. The clusterheads in VCCSR follow a set of communication rules to minimize the routes re-adjustment cost in propagating the sink's latest location information. VCCSR scheme although reduces the routes reconstruction cost in handling the sink Mobility. However, the cluster-head at the centre of the sensor field being the focal point in routes re-adjustment process, depletes its energy much earlier.

Hexagonal cell-based Data Dissemination (HexDD) proposed in [2] constructs a hexagonal grid structure to address real-time data delivery while taking into consideration the dynamic conditions of multiple mobile sinks and event sources. Based on the six directions of a hexagon, HexDD defines query and data rendezvous lines to avoid redundant propagation of sink's data queries. Nodes send their data to nearest border line which is then propagated towards the centre cell. Nodes along the border line store and replicate the data. Sink's data queries are forwarded towards the centre cell and as soon as it approaches a border line node with the relevant data stored, data delivery to the mobile sink starts using the reverse path. To cope with sink mobility, whenever the sink moves from one cell to another, it informs the centre nodes as well as the border nodes along the route about the new cell where the sink is currently stationed. This results in high energy consumption especially at higher sink's speeds. Nodes along the border line cells and especially at the centre cell are vulnerable to high energy consumption thereby causing early hot-spot problem.

Oh et al. proposed a data dissemination scheme called Backbone-based Virtual Infrastructure (BVI) in [3] that makes use of single-level multi-hop clustering. It aims to minimize the total number of clusters and thus the scale of network overhead associated with informing all the CH nodes about the sink's location information. For clustering it employs HEED [4] where priority is given to residual energy level of nodes in electing the CH nodes. To keep track of sink location information, it assumes that the network operator appoints a certain CH node as root of the tree. Whenever, the mobile sink joins the sensor field, it registers itself with the closest CH via an agent node. The host CH node accordingly updates other CH nodes along the route to the root CH about the sink's location information. Furthermore, when a mobile sink moves within a cluster, the respective CH node only takes care of connection with the sink within the cluster and avoids propagation of sink location updates to the root. However, when the sink joins another cluster, it selects another agent node and registers itself to the new CH node which accordingly shares this information with the root and the other CH nodes along the BVI segment to the root. The multi-hop clustering although appears a good strategy to minimize the number of clusters and thus the network control overhead, however, the root node being the focal point in routes adjustments triggers early energy depletion and thus reduces the network lifetime.

Multiple Enhanced Specified-deployed Sub-sinks (MESS) in [5], creates a virtual strip in the middle of sensor field thereby placing enhanced wireless nodes (sub-sinks) having more storage capacity at equal distances. The set of sub-sink nodes along the accessible path serve as rendezvous points for the mobile sink and collect and store data from sensor nodes. In data delivery phase, mobile sink floods the query along the virtual strip till it reaches to the sub sink node owning the data. Upon receiving the query from mobile sink, the sub-sinks route their deposited data to the mobile sink using geographical forwarding approach. A similar approach has also been proposed in Line-Based Data Dissemination (LBDD) [6] which constructs a vertical line by dividing the sensor

field into two equal sized blocks. Yet another similar approach can be found in [7], which places a virtual rail (called RailRoad) in the middle of the sensor field where nodes inside the virtual rail's premises serve as rendezvous points. The main limitation of MESS, LBDD, and RailRoad is the early energy depletion of nodes close to the virtual structure as the same nodes are repeatedly chosen as relays for the farther nodes. In addition, MESS also imposes placement of enhanced nodes along the virtual strip which limits its applicability.

III. THE VGDRA SCHEME

In this section, we give detailed description of our VGDRA scheme, including how to construct the virtual infrastructure and how to maintain fresh routes towards the latest location of the mobile sink. We design a virtual infrastructure by partitioning the sensor field into a virtual grid of uniform sized cells where the total number of cells is a function of the number of sensor nodes. A set of nodes close to centre of the cells are appointed as cell headers which are responsible for keeping track of the latest location of the mobile sink and relieve the rest of member nodes from taking part in routes re-adjustment. Nodes other than the cell-headers associate themselves with the closest cell-headers and report the observed data to their cell-headers. Adjacent cell-headers communicate with each other via gateway nodes. The set of cell-headers nodes together with the gateway nodes constructs the virtual backbone structure.

A. Network Characteristics

It is worthwhile to highlight the various assumptions of the sensor networks before describing the methodology of VGDRA scheme. We assume the following network characteristics:

• Nodes are randomly deployed and they remain Static throughout.

• All the nodes are of homogeneous architecture and know their location information.

• Nodes adapt their transmission power based on the distance to the destination nodes.

• The mobile sink does not have any resources constraints.

• The mobile sink performs periodic data collection from sensor nodes while moving along the periphery of the sensor field and maintains communication with the closest border-line cell-headers for data collection.

B. The Virtual Structure Construction

The VGDRA scheme constructs the virtual grid structure by first partitioning the sensor field into several uniform sized cells based on the number of nodes in the sensor field. The rationale behind such portioning is to uniformly distribute the work-load on part of cell header nodes which consequently results in prolonged network lifetime.

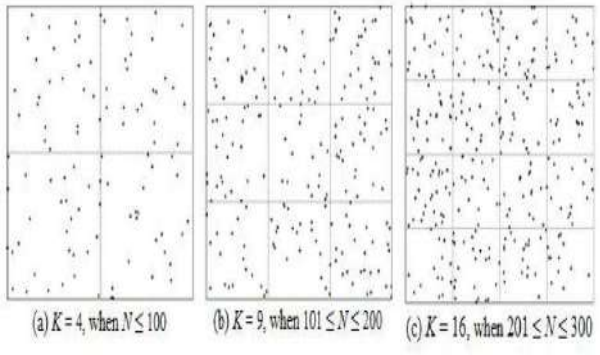


Fig.1. Example of different virtual grid based structures for different number of nodes.

To determine the optimal number of cells and thus the cluster-heads, we adopt the heuristics used in LEACH, TEEN , and APTEEN which consider 5% of the total number of sensor nodes. Given N number of nodes, the VGDRA scheme partitions the sensor field into K uniform sized cells using Equation 1, where K is a squared number. Fig. 1 (a), (b) and (c) shows network partitioning into various uniform sized cells for N = 100, 200, 300 respectively.

$$K=\begin{cases} 4 & N \times 0.05 \leq 6 \\ 9 & 6 < N \times 0.05 \leq 12 \\ 16 & 12 < N \times 0.05 \leq 20 \end{cases} \quad (1)$$

After the network partitioning, next VGDRA scheme appoints a set of nodes as cell-headers. Initially in every cell, the node closest to the mid-point of the cell is elected as the cell-header. Nodes using the knowledge of sensor field's dimension and the total number of nodes compute the midpoints of all the cells. In order to reduce the communication cost in the cell-header election, only those nodes take part in the election whose distance to the mid-point of the cell is less than a certain threshold. The threshold distance to the mid-point is gradually increased if no node can be found within the threshold distance around the mid-point of the cell. This threshold based cell-header election strategy not only helps in energy conservation but also elects the cell-header at the most appropriate position within the cell. After the initial cell-header election, each cell-header notifies its status not only to the surrounding nodes within its cell but also to the nodes which are slightly beyond the cell boundary. Nodes might receive cell-header notifications from more than one cell-header and associate themselves to the closest one. Nodes that receive notifications from multiple cell-headers also share the information of the secondary cell-header with their primary cell-header. In this way, each cell-header form adjacencies with neighbouring cell-headers using gateway nodes. The maximum number of adjacent cell-headers for a borderline cell-header is 3 whereas for an inside cell-header is 4. The set of cell-header nodes together with the

gateway nodes constructs a chain like virtual backbone structure as shown in Fig. 2.

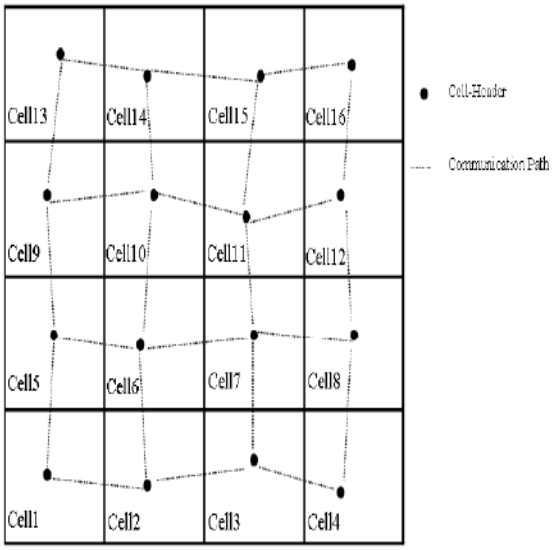


Fig. 2.An example of virtual backbone structure after establishing adjacencies.

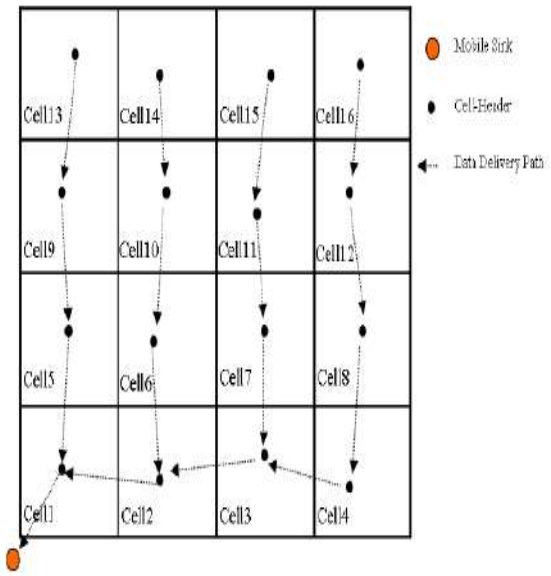


Fig. 3. An example of virtual backbone structure after initial routes setup.

After the cell-header election and establishing the adjacencies, communication routes are setup considering the mobile sink is located at coordinates (0, 0). As a result of the initial routes setup, all the cell-headers adjust their routes to the initial position of the mobile sink. Fig. 3 shows the virtual backbone structure after the initial routes setup when the sensor field is partitioned into 16 cells.

C. Dynamic Routes Adjustment

In order to cope with dynamic network topology caused by sink mobility, nodes need to setup their data delivery routes in accordance with the latest location of the mobile sink. Flooding the sink's latest location to the entire sensor field is the most naive approach in this regard but greatly undermines the energy conservation goal and is therefore avoided. Using our VGDRA scheme, only the set of cell-headers that constitute the virtual backbone structure are responsible for maintaining fresh routes to the latest location of mobile sink. For periodic data collection from the sensor field, the mobile sink moves around the sensor field and collects data via the closest border-line cell-header. The closest border-line cellheader (originating cell-header) upon discovering the sink's presence, shares this information with the rest of the cell headers in a controlled manner.

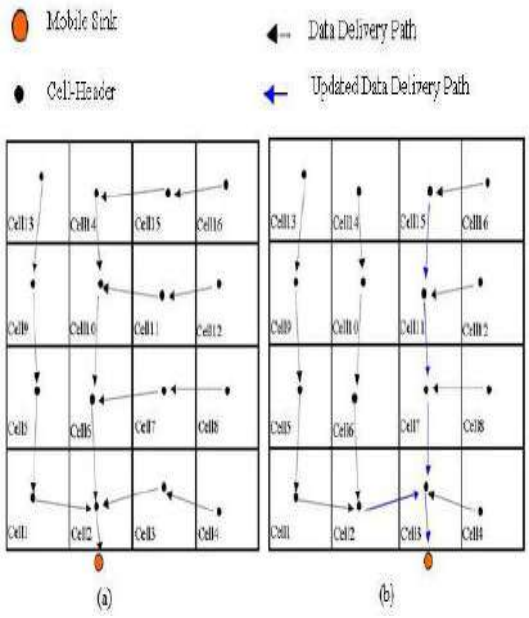


Fig. 4. An example of routes re-adjustments when sink moves from cell 2 to cell 3.

The VGDRA scheme defines a set of propagation rules so that only those cell-headers take part in the routes re-adjustment process that really require to adjust their routes. The propagation rules are described as follows:

Rule 1: The originating cell-header upon sink discovery first verifies whether its next-hop is already set to the mobile sink or not. If the mobile sink was previously being setup as its next-hop, the originating cell-header does not propagate sink's location update. However, if the next-hop entry of the originating cell-header is other than the mobile sink, it exercises rule 2.

Rule 2:

The originating cell-header being one-hop from the mobile sink sets the mobile sink as its next-hop and shares this information with the previous originating cell-header and its downstream adjacent cell-header.

Rule 3:

The previous originating cell-header upon receiving the sink's location update from the current originating cell header, adjusts its data delivery route by setting the current originating cell-header as its next-hop towards the sink.

Rule 4:

The downstream cell-header upon receiving the sink's location update checks whether the sender cell-header is the same as its previous next-hop or different. If it is the same, the downstream cell-header drops the sink's location update packet and does not propagate it further to the next downstream cell-header. In the case when it is different, the downstream cell-header updates its next-hop entry to the new sender cell-header and further propagates the sink's location update to the next downstream cell-header. This procedure is repeated till all the downstream cell-headers adjust their data delivery routes towards the latest location of the mobile sink.

Fig. 4(a) shows an example of the data delivery paths when the sink is located in the cell 2 premises.When the mobile sink moves from cell 2 to cell 3, the cell-header at cell 3 exercises rule 2 and rule 3 to update the cell-header at cell 2, followed by rule 4 to update its downstream cell-headers i.e., 7, 11 and 15 as shown in Fig. 4(b). In this way, only a limited number of cell-headers take part in the routes re-adjustment process thereby reducing the overall routes re-adjustment cost of the network.

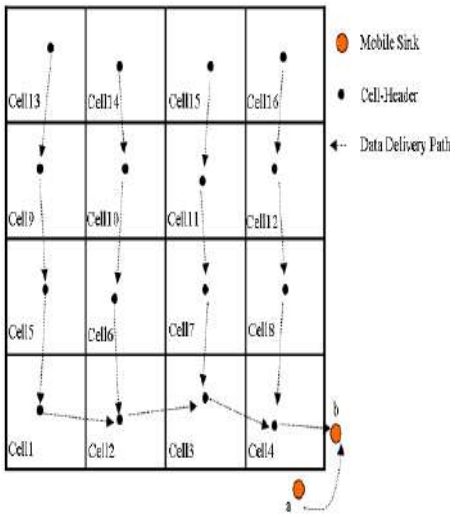


Fig. 5. An example of preventing the undesired propagation of sink location updates.

Similarly, Fig. 5 demonstrates when the mobile sink moves from position *a* to *b* within the same cell, the cell-header at cell 4 exercises rule 1 and refrains itself from propagating sink's location information. This strategy helps to minimize the routes reconstruction cost to a great extent and thus improves the network lifetime.

Algorithm 1 Routes Re-Adjustment Using VGDRA Scheme

1. Mobile Sink (MS) updates its location to the closest Cell-Header (CH).

2. The closest CH becomes Originating Cell-Header (OCH).

3. **if** the previous Next_Hop of OCH is not the MS

4. {

5. set Next_Hop of OCH ← MS

6. OCH sends route update packet to the previous OCH

7. set Next_Hop of previous OCH ← OCH

8. OCH sends route update packet to its immediate downstream CH

9. **for** each downstreamCHreceives route update packet

10. {

11. **if** the previous Next_Hop of CH is not the current sender

12. {

13. set Next_Hop of CH ← current sender

14. **if** next downstream CH is not **NULL**

15. {

16. set sender ← current CH

17. Current CH sends route update packet to its immediate downstream CH

18. }

19. **else**

20. drop the packet

21. }

22. **else**

23. drop the packet

24. }

25. }

26. **else**

27. drop the packet

The VGDRA algorithm that governs the routes adjustment process along the sink mobility is described in detail as above.

D. Cell-Header Rotation

An integral part of the proposed VGDRA scheme is rotating the role of the cell-header in every cell. The cell-header being the local data collector is vulnerable to high energy dissipation and therefore to prolong the network lifetime, the cell-header role needs to be distributed among the nodes within the cell. In order to achieve uniform energy dissipation, the VGDRA scheme keeps track of the residual energy level of the current cell-header, where if it gets below a certain threshold, the new cell-header election is initiated by the current cell-header. In the re-election process, the node that is relatively more close to the mid-point of the cell and has a higher energy level compared to other candidates is elected as the new cell-header. Also in the re-election process, the search zone around the mid-point in every cell is slightly

increased or the energy threshold level is decreased progressively if no suitable

node can be found. In order to preserve the virtual backbone structure, the current cell-header before stepping down, shares the information of the new cell-header not only with all its member nodes but also with the adjacent cell-headers in its neighbourhood.

IV. SIMULATION AND RESULTS

In this section, we present the simulation results using NS-2. We varied the total number of sensor nodes from 100 to 400 which are randomly deployed in a sensor field of 200 × 200 dimension. A mobile sink moves around the sensor field counterclockwise and periodically broadcasts hello packets. Initially all the sensor nodes have uniform energy reserve of 1 mJ. We considered the energy model being used in [27] and assumed free space radio propagation model ($d2$, d is the distance between sender and receiver). Furthermore, we considered nodes energy consumption in transmission (Tx) and receiving (Rx) modes only which are computed using Equation 2 and 3 respectively.

$T_X = (E_{elect} \times K) + (E_{amp} \times K \times d^2)$ (2)

$R_X = E_{elect} \times K$ (3)

In Equation 2 and 3, K is the message length, E_{elect} is the node's energy dissipation in order to run its radio electronic circuitry and E_{amp} is the energy dissipation by the transmitter amplifier to suppress the channel noise. In our experiment, we took E_{elect} = 50 nJ, and E_{amp} = 10 nJ/bit/m2 and K = 8 bits. We considered the nodes communication cost in adjusting the data delivery routes only. We compared our VGDRA scheme with VCCSR, HexDD, and BVI where a common feature among them is the use of a virtual infrastructure for network operation. We used four different criteria to evaluate the performance of the VGDRA against the other schemes under the same network dynamics: virtual backbone structure construction cost, per round routes reconstruction cost, average network lifetime, and network convergence time.

A. The Virtual Backbone Structure Construction Cost

The virtual structure construction cost is an estimate of the nodes energy consumption in electing the cell-headers and then forming the virtual backbone network. Fig. 6 compares the average nodes' energy consumption of our VGDRA scheme with the other schemes in constructing the virtual backbone network for different network sizes.

As demonstrated in Fig. 6, nodes using VGDRA scheme incur least cost compared to other schemes in constructing the virtual structure. The VCCSR considers fixed number of cluster-head nodes irrespective of the network size e.g., it considers 81 cluster-head nodes under the considered network dynamics and thus as a result, a high population of the sensor nodes take part in the cluster-head election. Similarly, the BVI incurs considerable communication cost in clustering the network where all the nodes exchange residual energy level information.

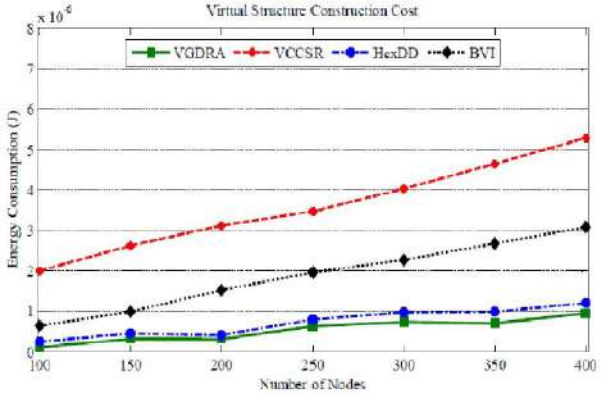


Fig. 6. Comparing the virtual structure construction cost for different network sizes.

Compared to VCCSR and BVI, nodes using HexDD perform local processing thereby causing less communication overhead. On contrary, using our VGDRA scheme, the total number of cells and thus the cell-headers is a function of the total number of nodes e.g., the number of cell-headers varies from 4 to 16 when N varies from 100 to 400 nodes. In addition,

only the nodes within short distance to the mid-point of the cell take part in cell-header election thereby reducing the communication cost.

B. The Per Round Routes Reconstruction Cost

The per round routes reconstruction cost represents the nodes energy expenditure in re-adjusting the data delivery routes as the sink moves around the sensor field and completes one round of the sensor field.

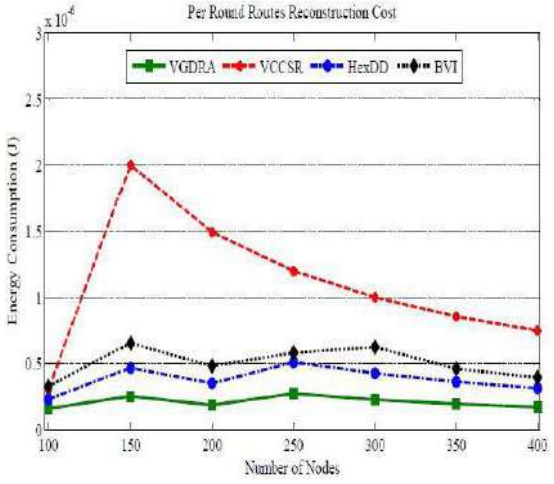


Fig. 7. Comparing the per round routes reconstruction cost for different network sizes.

As shown in Fig. 7, using the VGDRA scheme, the average nodes' energy consumption in reconstructing the data delivery routes to the latest location of the mobile sink is significantly less compared to the other schemes. This is mainly attributed to the least propagation of sink's location updates by following the set of communication rules of the VGDRA while preserving nearly optimal routes towards the latest location of the mobile sink. Using our VGDRA scheme, only a partial sub-set of cell-header nodes takes part in the routes reconstruction process thereby reducing the overall routes reconstruction cost as the mobile sink completes one round of the sensor field.

C. The Network Lifetime

The network lifetime is defined as the time elapsed since the nodes deployment till the first node dies due to energy depletion. In our experiments, we estimated the network lifetime in terms of the number of rounds of the mobile sink around the sensor field till the first node in the network dies due to energy depletion.

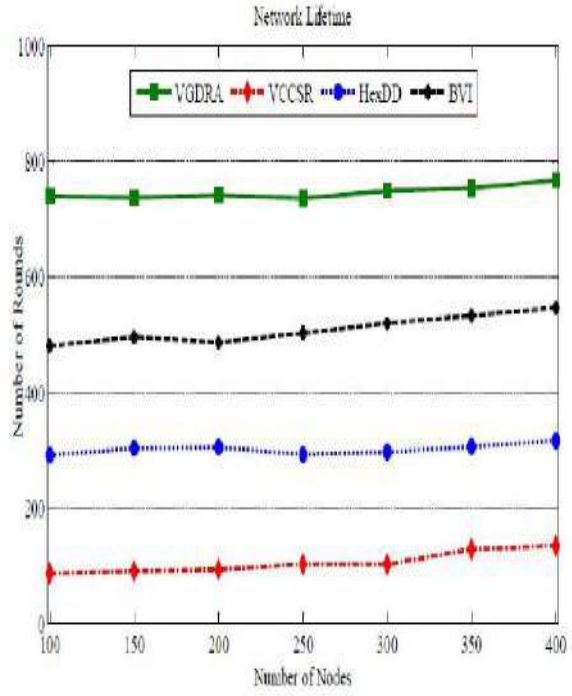


Fig. 8. Comparing the network lifetime in terms of number of rounds around the sensor field.

As presented in Fig. 8, our VGDRA scheme outperforms the other schemes in terms of network lifetime at different network sizes. In VCCSR, the cluster-head at the central-point of the sensor field suffers from more work-load for taking part in every single reconstruction phase and thus depletes its energy much earlier compared to others. Similar behaviour is exhibited by the centre and border nodes in HexDD thereby decreasing the overall network lifetime. Unlike the VCCSR and HexDD, the proposed VGDRA and BVI schemes keep track of the residual energy of cell-header nodes and progressively elect new header nodes thereby prolonging the network lifetime. Furthermore, compared to BVI, the proposed VGDRA scheme incurs least network control overhead. The results presented in Fig. 8 also demonstrates nearly uniform network lifetime at different network sizes using our VGDRA scheme which justifies our approach of partitioning the sensor field into different number of cells on the basis of the total number of nodes.

D. The Network Convergence Time

The network convergence time is an indirect reflection of the data delivery efficiency as the more promptly the nodes come to know about the latest location of a mobile sink, the more efficient routes they can select in disseminating the sensed data.

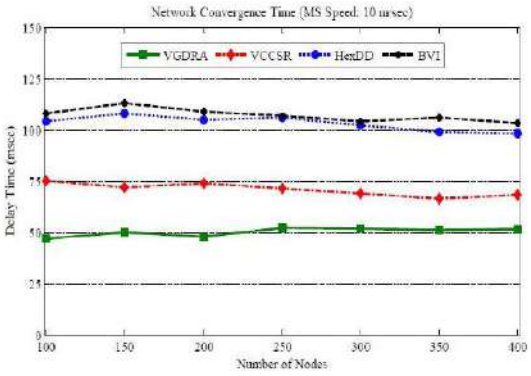


Fig. 9. Comparing the network convergence time for different network sizes.

It is an estimation of the elapsed time that a significant position change of the mobile sink is recorded by the nodes constituting the virtual infrastructure. In terms of convergence time, the faster the nodes converge to latest location of a mobile sink, the better they perform in data dissemination phase. As shown in Fig. 9, the convergence time of the proposed VGDRA scheme is very fast compared to VCCSR, HexDD, and BVI when the sink is moving at a speed of 10 m/sec. Using the set of communication rules, our VGDRA scheme intelligently picks a small subset of cellheaders in the routes re-adjustment process and then greedily shares the latest location information of the mobile sink with them. This partial re-adjustment greatly reduces the network overhead and leads to faster convergence of nodes to the latest location of the mobile sink.

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed a novel Virtual Grid based Dynamic Routes Adjustment (VGDRA) scheme that incurs least communication cost while maintaining nearly optimal routes to the latest location of the mobile sink. Our VGDRA scheme partitions the sensor field into a virtual grid and constructs a virtual backbone structure comprised of the cell header nodes. A mobile sink while moving around the sensor field keeps on changing its location and interacts with the closest border-line cell-header for data collection. Using a set of communication rules, only a limited number of the cell headers take part in the routes reconstruction process thereby reducing the

overall communication cost. In terms of nodes energy consumption, the simulation results reveal improved performance of our VGDRA scheme for different network sizes.

Considering the scope of this paper, we have not included the actual data delivery model. In future work, we will analyze the performance of our VGDRA scheme at different sink's speeds and different data generation rates of the sensor nodes. The proposed VGDRA scheme though offers a light weight solution and does not impose many constraints on part of the resource constrained sensor motes, yet its practical implementation on real hardware needs to be confirmed. We also aim to develop a small test bed for the practical implementation of the proposed VGDRA scheme on real hardware (motes) and evaluate its results.

REFERENCES

[1] T.-S. Chen, H.-W. Tsai, Y.-H. Chang, and T.-C. Chen, "Geographic convergecast using mobile sink in wireless sensor networks," *Comput. Commun.*, vol. 36, no. 4, pp. 445–458, Feb. 2013.

[2] S. R. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, "Energy efficient schemes for wireless sensor networks with multiple mobile base stations," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, vol. 1. Dec. 2003, pp. 377–381.

[3] A. W. Khan, A. H. Abdullah, M. H. Anisi, and J. I. Bangash, "A comprehensive study of data collection schemes using mobile sinks in wireless sensor networks," *Sensors*, vol. 14, no. 2, pp. 2510–2548, 2014.

[4] M. Di Francesco, S. K. Das, and G. Anastasi, "Data collection in wireless sensor networks with mobile elements," *ACM Trans. Sensor Netw.*, vol. 8, no. 1, pp. 1–31, Aug. 2011.

[5] I. Chalermek, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proc. ACM SIGMOBILE Int. Conf. Mobile Comput. Netw. (MOBICOM)*, 2000, pp. 56–67.

[6] E. B. Hamida and G. Chelius, "Strategies for data dissemination to mobile sinks in wireless sensor networks," *IEEE Wireless Commun.*, vol. 15, no. 6, pp. 31–37, Dec. 2008.

[7] A. Kinalis, S. Nikoletseas, D. Patroumpa, and J. Rolim, "Biased sink mobility with adaptive stop times for low latency data collection in sensor networks," *Inf. Fusion*, vol. 15, pp. 56–63, Jan. 2014.

Identification and Elimination of Cracks in Digitized Painting

Kusuma.N[1], Harshitha.N[2], Saravana Perumal.V.M[3]

[1]UG Scholar, [2]Asst. Professor , Dept. of CSE, RRCE, Bengaluru

kusumanmurthy@gmail.com, coolpurpleh@gmail.com , saran4umohan@gmail.com

Abstract: A united methodology for the detection and elimination of cracks on digitized paintings is presented in this project. The cracks are identified by threshold the output of the morphological top-hat transform. Later, the thin dark brush strokes which have been misunderstood as cracks are removed using either a median radial basis function neural network on hue and saturation data or a partially automatic procedure based on region growing. At last, crack filling using order statistics filters or controlled anisotropic scattering is performed. The methodology is shown to perform well on digitized paintings suffering from cracks.

Keywords: PDEs,CLR,MRBS

I. INTRODUCTION

Most of the paintings, especiallythe old images, suffer from breakages in the substratum, the paint, or the varnish. These patterns are usually called cracks or breakagesand can occur due to aging, drying, and mechanical factors. Age cracks can result to non-uniform contraction in the canvas or wood-panel support of the painting, which stresses out the layers of the painting. Drying cracks are usually caused by the evaporation of volatilepaint components and the consequent contraction of the paint. Finally, mechanical cracks result to the painting deformations due to external effects. For example: vibrations and impacts.

The presence of cracks on paintings suppresses the image quality of a picture. However, we can use digital image processing techniques to identify and eliminate the cracks on digitized paintings. Such a "virtual" restoration can provide clues to art historians, museum curators and the public on how the painting would look like in its initial state, i.e., without the breakages. Eventually, it can be used as a constructive tool to plan the actual restoration. A system is capable to track and interpolate cracks.The user should select a point on every crack to be restored. A method for the identification of cracks using multioriented Gabor filters. Crack detection and elimination bears certain similarities with methods proposed for the detection and removal of scratches and other artifacts from motion picture films.However, those methods depend on information obtained over many adjacent frames for both artifact identification and filling and, thus, are indirectly applicable in the case of painting cracks. Other research areas that are nearly related to crack elimination include image inpainting which deals with the restoration of missing or corrupted image areas by filling the information from the neighboring areas, and dis-occlusion, i.e., recovery of object parts that are hid behind other objects within a picture. Methods implemented in these areas assume that the regions where data has to be filled in are known. Unique approaches for interpolating information in organizedand textured image areas have been constructed. The former are usually based upon partial differential equations (PDEs) and on the calculus of variations whereas the latter depend on texture synthesis principles. A technique that decomposes the image to textured and organized areas and uses suitable interpolation techniques depending on the area where the information is missing. The results achieved by these techniques are good. A procedure for the restoration of cracks on digitized paintings, which adapts and summation of a number of image processing and analysis tools is presented in this paper. The methodology is an extended version of the crack removal framework. The technique comprises of the following steps:

- Crack identification;
- Separation of the thin dark brush strokes, which have been misunderstood as cracks;
- Crack filling (interpolation).

A certain part of user interaction, mostly notable in the crack-identification stage, is required for accurate results. User interaction is rather accepted since the large differences observed in the typology of breaks would lead any impartial automatic algorithm to failure. However, all processing stages can be executed in real time, and, thus, the user can immediately observe the effect of parameter making a changeover the image under study and choose in an intuitive route the values that achieve the accurate visual result. Needless to say, only subjective accuracy criteria can be used in this case since no ground truth information is available. The opinion of restoration experts is that the virtually inspected restored images are

positive. Two methods for the separation of the brush strokes which have been wrongly detected as cracks.

OVERVIEW OF THE PROPOSED FRAMEWORK:

At present, in the case like paintings, especially ancient ones, suffer from cracks in the substratum, the paint, or the varnish. Such a breaks are usually called cracks and can occur due to aging, drying, and mechanical factors. Drying cracks are almost caused due to evaporation of volatile paint components and the shrinkage of the paint. The cracks caused due to aging is known as aging cracks, cracks formed due to evaporation is known as drying crack and cracks due to any other external factors is known as mechanical cracks. To identifyand eliminate cracks, this project uses the digital image processing technique to regain the image for processing. Image is processed in top – hat transform and the characteristic of image are processed to identify the crack. After identifying the cracks that part alone can be deleted and image filling activity can be done and finally gets combined with the remaining part of image.

DESCRIPTION OF PROBLEM:

Existing System

The present methods for digital processing of images are there which actually deal with enhancing the picture quality, brightness, color etc. These factors can be suppressed due to aging process. Such image processing technique algorithm concentrates on developing factor alone. They are not designed to analyze and enhance the cracks region. The cracks elimination is to be rectified in different manner. The principle applied to enhance image color, brightness and other characteristic can't be used for crack identification and elimination. This project highlights the digital image processing algorithm that deals only with crack identification and elimination.

Proposed System

The suggested system deals with digital image processing technique which identifies and remove the cracks in pictures. A system is capable of tracking and fixing cracks. The user should choose a point on every crack to be restored. A method for the detection of cracks using multioriented Gabor filters. Crack identification and elimination bears certain similarities with methods suggested for the identification and eliminating the scratches and other artifacts from motion picture films.However, such methods depend on information achieved over many adjacent frames for both artifact identification and filling and, thus, are indirectly applicable in the case of painting cracks. Other research areas that are nearly related to crack elimination includes image inpainting which deals with the reconstruction of missing or corrupted image areas by filling the information from the neighboring areas, and dis-occlusion, i.e., recovery of object parts that are hid behind other objects within a picture. Methods constructed in these areas assume that the regions where information has to be filled in are known. Unique approaches for filling information in structured and textured image areas have been developed. The former are almost based on partial differential equations (PDEs) and on the calculus of variations whereas the latter depend on texture synthesis principles. A technique that decomposes the image to textured and organized areas and uses suitable interpolating techniques depending on the area where the information is missing. The results obtained by these techniques are good. A methodology for the restoration of cracks on digitized paintings, which adapts and sum of a number of image processing and analysis tools is shown in this paper. The methodology is an extension of the crack removal framework. The technique comprises of the following steps:

- There should be few methods through which crack region in the digital image can be identified;
- Segregation of the thin dark brush strokes, which have been misunderstood as cracks;
- Crack filling or interpolation.

A certain region of user interaction, mostly notable in the crack-detection step, is required for accurate results.

System Environment

Front end used: Microsoft Visual Basic.Net is used as front end tool. The reason behind selecting Visual Basic .Net as front end tool is as follows:

- Visual Basic .Net is flexible, allows one or more language to operate internally to provide the result. This language allows to do project at a faster rate.
- Visual Basic .Net has CLR(Common Language Runtime), which allows the components to intersect into one intermediate format and then can interact.
- Visual Basic .Net provides a very good security when the application is executed.
- Visual Basic .Net is flexible, which allows us to configure the working environment to suit individual style. We can make a choice between a single and multiple document interfaces, and size can be adjusted and various IDE elements can be positioned.

- Visual Basic .Net has excellent feature that makesthe coding easy and also active which helps to provide less coding time.
- The working environment in Visual Basic .Net is often referred to as Integrated Development Environment because it summatesdifferent functions such as designing, editing, compiling and debugging within the sameenvironment. In most customary development tools, each of segregated program, each with unique interface.
- The Visual Basic .Net language is powerful –we can imagine a programming workand achieve using it.
- After preparing a Visual Basic .Net application, if we wish to distribute it, we can freely distribute to anyone who uses Microsoft windows. We can distribute it through other resources.
  - Toolbars provide quick access to usually used commands in the programming environment.
  - Most of the parts of Visual Basic are context sensitive which means we can get help on these regions directly without going to help menu.
  - Visual Basic assumes the code as we enter it, catching and indicating most syntax or spelling errors on the fly.

II. SYSTEM ANALYSIS

It can be defined, as a method to determine the use of resources and machines in the best manner and operate on tasks to get the data needs of an organization.

System Description

It is also a management method which helps in developing a new system or enhancing a present system. The system development life cycle consists of four basic components as follows:

- System Analysis
- Requirement of System
- Developing
- To Code
- To Check
- Sustain

DETECTION OF CRACKS

Cracks usually glow less brightly, hence, it can be considered as local intensity minima with rather organized characteristics that is extensive. Therefore, a crack identifier can be applied on the luminance object of an image and should be able to identify such minima. A crack-identification procedure is mainly based on the top-hat transform which is suggested in this paper. The top-hat transform is a grayscale morphological filter defined as follows:

$$Y(x) = f(x) – fnB(x) \quad (1)$$

WherefnB(x) is the opening of the function f(x) (in our case, the luminance component of the picture under study) with the organizing set , which is defined as

$$nB = B \Phi B \Phi \ldots\ldots\ldots \Phi B \text{ (n times)} \quad (2)$$

In the last equation, Φ denotes the dilation function. A circle ora square that can be used as organizing element B. The final organizing set nB is evaluated only once using and is used subsequently in the opening operation of (1). The opening fnBof a function is a low-pass nonlinear filter that erases all peaks (local maxima) in which the structuring element nBcannot fit. Thus, the image f – fnB contains only those peaks and no background at all. Since cracks are local minima rather than local maxima, the top-hat transform should be applied on the negated luminance image. Alternatively, one can detect cracks by performing closing on the original image f(x) with the structuring set nB and then subtracting from the result of closingfnB(x)

$$Y(x) = fnB(x) -- f(x) \quad \text{-------- (3)}$$

It can be easily shown that the result of (3) is identical to that of applying (1) on the negated image. Use of (3) does not require negation of f(x) which grands it a small but not negligible computational advantage over (1).

In situations where the crack-like artifacts are of high luminance, as in the case of scratches on photographs, negation of the luminance component prior to the crack detection is not required, i.e., the crack detection procedure can be applied directlyon the luminance image. The user can control the result of the crack-detection procedure by choosing appropriate values for the following parameters:

- The type of the structuring element B ;
- The size of the structuring element B and the number n of dilations in (2).

These parameters affect the size of the “final” structuring element nB and must be chosen according to the thickness of the cracks to be detected. It should be noted, however, that these parameters are not very critical for the algorithm performance due to the thresholding operation that will be described in the next paragraph and also due to the existence of the brush-stroke/crack separation procedure, which is able to remove crack-like brush strokes that have been erroneously identified as

cracks. The fact that all the results presented in this paper have been obtained with the same top-hat transform parameters comes as a clear indication that the above statement is indeed true. These parameters were the following:

- Structuring element type: square;
- Structuring element size: 3 X 3;
- Number n of dilations in (2) : 2.

The top-hat transform generates a grayscale output image t(k,l) where pixels with a large grey value are potential crack or crack-like elements. Therefore, a thresholding operation on t(k,l) is required to separate cracks from the rest of the image. The threshold can be chosen by a trial and error procedure, i.e., by inspecting its effect on the resulting crack map. The low computational complexity of the thresholding operation enables the user to view the crack-detection results in real time while changing the threshold value, e.g., by moving a slider. This fact makes interactive threshold selection very effective and intuitive. Alternatively, threshold selection can be done by inspecting the histogram of for a lobe close to the maximum intensity value (which will most probably correspond to crack or crack-like pixels), and assigning it a value that separates this lobe from the rest of the intensities. The result of the thresholding is a binary image marking the possible crack locations. Instead of this global thersholding technique, more complex thresholding schemes, which use a spatially varying threshold can be used. Obviously, as the threshold value increases the number of image pixels that are identified as cracks decreases. Thus, certain cracks, especially in dark image areas where the local minimum condition may not be satisfied, can remain undetected. In principle, it is more preferable to select the threshold so that some cracks remain undetected than to choose a threshold that would result in the detection of all cracks but will also falsely identify as cracks, and subsequently modify, other image structures. The thresholded (binary) output of then top-hat transform on the luminance component of an image containing cracks (Fig. 1) can be seen in Fig. 2.

SEPARATION OF THE BRUSH STROKES FROM THE CRACKS

In few paintings, some areas exist where brush strokes have almost the same thickness and luminance features as cracks. Therefore, the top-hat transform might misunderstand these dark brush strokes as cracks. Thus, in order to ignore any undesirable to the actual changes al image, it is important to segregate these brush strokes from the actual cracks, before theimplementation of the crack filling process. Two methods to achieve this goal are described in the following subdivisions. An interactive approach towards the separation of cracks from brush strokes is to apply an area growing algorithm on the threshold output of the top-hat transform, starting from pixels (seeds) on the real cracks. The pixels are chosenby the userin an interactive mode. At least one seed per connected crack element should be chosen. Alternatively, the user can choose to apply the technique on the brush strokes, if this is more easy. The growth mechanism that was once used implements thewell-known algorithm that checks repeatedly for unclassified pixels with value 1 in the 8-neighborhood of every crack pixel. At the end of this procedure, the pixels in the binary image, which corresponds to brush, strokes that are not 8-connectedto cracks will be eliminated. The above procedure can be used either in a stand-alone mode or applied on the output of the MRBF segregation procedure described in the upcoming section to eliminate any remaining brush strokes

Fig.1

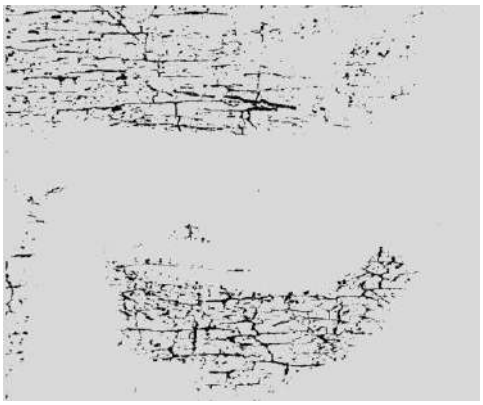


Fig.2

In our implementation, a MRBF (Mean Round Before Failure) network with two outputs was used. The very first output represents the group of cracks while the second one the group of brush strokes. Input vectorswere two-dimensional and comprised of the hue and saturation valuesof pixels identified as cracks by the top-hat transform. The number of clusters (hidden units) chosen for each group depends on the overlap between the populations of cracks and brush strokes. If there is a substantial overlap, the number will be increased, to reduce the classification error. In our implementation three hidden units have been incorporated.

Training was carried out by presenting the network with hue and saturation values for pixels corresponding to cracks and crack like brushstrokes. Data from 24 digitized portable religious icons from the Byzantine era were used for this purpose. The system is trained by this specific training set can be considered to be optimized for paintings of this style and its use on paintings of other style might result in somewhat suboptimal results. However, suitably selected training sets can be used to train up the system to separate cracks from brush strokes on paintings of different artistic styles or content. In order to choose pixels corresponding to cracks and crack-like brush strokes the crack detection algorithm presented was applied on the pictures. Results were subsequently postprocessed by an expert by the partially-automatic approach presented in Section III-A.

The aim of this postprocessing stage was twofold: to remove pixels that are neither cracks nor crack-like brush strokes and also to separate cracks and crack-like brush strokes for the supervised step of the training procedure. In the supervised training stage, the network was proposed with these labelled inputs, that ispairs of hue-saturation values that corresponds to the image pixels that have been identified as belonging to cracks and crack-like brush strokes. After the training session, the MRBF (Mean Round Before Failure) neural network was able to classify pixels identified as cracks by the top-hat transform to cracks or brush strokes. Naturally, the performance of the cracks or brush-stroke separation methodology was judged only in a subjective manner (by visual inspection of the results), as ground truth data (brush stroke-free crack images) is not available. Due to this reason, two restoration experts were asked to do inspection on several crack images before and after the application of the segregation system and finalised that in the processed crack images the majority of the brush strokes has been eliminated successfully. A thresholdtop-hat transform output comprising many brush strokes. A greater part of these brush strokes is separated.

CRACK-FILLING METHODS

After identifying cracks and segregating misunderstood brush strokes, the final job is to restore the image using local image information (information from neighbouring pixels) to interpolate the cracks. Two divisions of methodology, using order statistics filtering and anisotropic diffusion are suggested for this purpose. Both are implemented on each RGB channel independently and affect only on those pixels which belongs to crack. Therefore, the identified crack pixels are indeed crack pixels, the filling procedure does not affect the “useful” content of the image. Image inpainting methodology like the ones stated in Section I can also be used for crack filling.

SYSTEM DESIGN

It is concerned with detecting software elements specifying connections among elements. Specifying software structure and to provide blue print for the document phase.

Modularity is one of the expectable properties of abundant systems. It implies that the system is classified into several areas.

Design will explain software elements in detailed manner. It helps with the implementing system. This will guide the further changes to satisfy the further requirements in the system.

Form design

Form is a message tool; it represents the physical carrier of data or information.

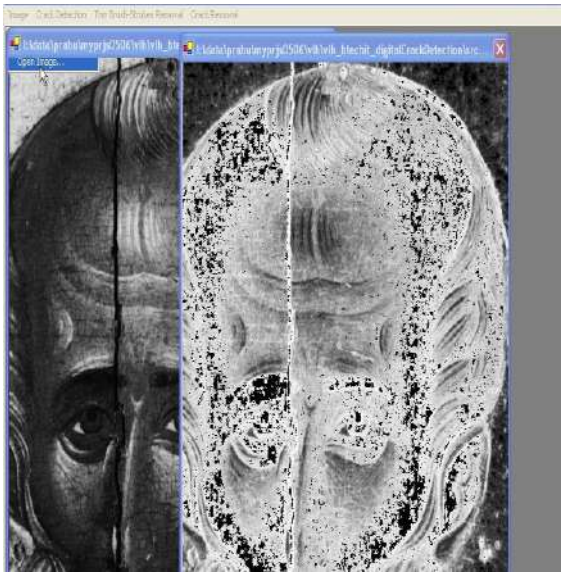


Fig.3

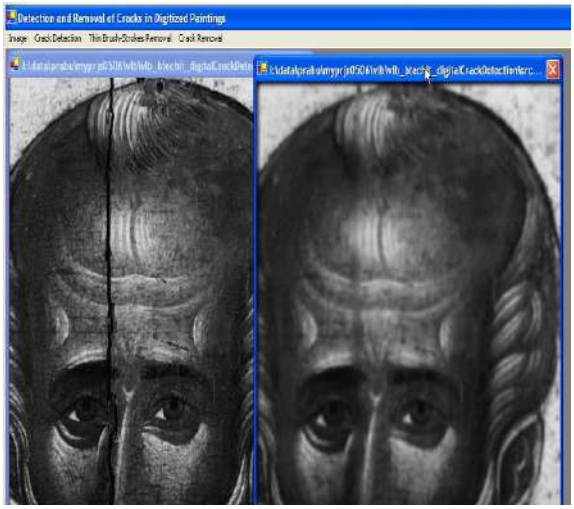


Fig.4

Input design

Mistaken input data is the mostly found errors in processing of data. Input design controls the errors made by data entry. Input design is the process by which the user-originated inputs get converted to a computer-based format.

Module Design

Processing of image: It is to understand how images are theirfile formats are stored, and to operate basic operations like read, write and drawinga picture.

Crack Detection: the basic characteristics of cracks are that they containextensive organized distinguishing feature. It is performed using top-hat transform which is an operation that extracts small elements and details from given images.

Removal of misunderstood cracks: apply starting point from the rest of the image to separate cracks. This section requires the manual interaction. A binary image will be created showing only using the crack regions.

Crack removal: Removal of cracks is done by trimmed mean filter. That is, we are placing thresholder binary image over result of top-hat transformed image, to detect cracks and smoothen the crack region of original picture using the pixels from the portion around the breaks.

Software Testing

After the source code is generated, software should be tested to correct the errors before delivering to the customer. The goal is to generate a test case series that have a resemblance of finding errors.

Software Testing is the process of assuring the ability and correctness of software by running it. It is usually performed by any one of the following reasons:

1) Detecting the defect

2) Reliability estimation.

The problem for defect detection is that software will only recommend the presence of defect, not their absence. The problem for reliability estimation is that the input distribution used for selecting test cases may be defected. In both of the above cases, the process used to determine whether output is correct. Clearly the benefit of the entire process is dependent on many different pieces. If any of these parts is not adequate, the entire process is compromised.

Software is now a physical process where inputs are received and outputs are produced. Most physical systems cease in a fixed set of ways. By distinguish, software can fail in many appearance ways.

The key to software testing is trying to find the multitude of failure modes. For most of the programs, this is reckoning infeasible. It is commonplace to attempt to test as many of the syntactic features of the code as possible are called white box software testing technique. Techniques that do not consider the code's rule when test cases are chosen are called black box technique.

Functional testing is a testing process which is black box in nature. The aim of this is to examine the complete functionality of the product.

Final step of the testing process must be System Testing. This test involvesthe examination of the whole system, all the software and hardware components and any interfaces.

The whole computer based system is checked not only for validity but also to satisfy the objectives.

III. IMPLEMENTATION

It includes all the activities that takes place to transfer from the old to the new system. The new one may be fully new, restoring an existing system or it may be major alteration to the system presently put into use. This system "Identification and Elimination of Cracks in Digitized Painting" is a new system. Implementation as a complete involves all the tasks that we do for successfully restoring the existing or introduce new software to meet the requirement.

CONCLUSION

In this paper, we have suggestedan united strategy for identification and elimination of cracks in digitized paintings. Cracks are identifiedusing top-hat transform, the thin dark brush strokes, which are misunderstood as cracks, are differentiated either by an automatic method (MRBF networks) or by partially automatic approach. Crack filling is operated by suitably modified order statistics filters or controlled anisotropicdiffusion. The technique has been applied for the virtual reconstruction of images and was found effective by restoration experts. There are a few aspects of the suggested technique that can be further improved. For example, the crack-detection step is not efficient in identifying cracks situated on very dark image areas, since in these areas the intensity of crack pixels is close to the intensity of the surrounding area. A possible solution to this shortcoming would be to apply the crack-identification algorithm on this area and choose a low threshold value. Another situation where the system (more particularly, the crack filling stage) does not performas efficiently as we expect is in the case of cracks that cross the border between regions of different color. In such situations, it might be the case that part of the crack in one area is filled with color from the other region, resulting in small spurs of color in the border between the two regions.However, this process is rather rare and, furthermore, the extent of these filled areas is very small (2–3 pixels maximum). A solution would be to operate edge identification or segmentation on the image and confine the filling of cracks that cross edges or areas or borders to pixels from the corresponding region.

BIBLIOGRAPHY

1.Steven Holzner , “Visual Basic .Net Programming “ Black Book - Dream Tech Press, New Delhi

2. Visual Basic Programmer’s Cook Book

3. Software Engineering By Roger Pressman

4. Lee “ Introduction to System Analysis and Design”

5.Galgotia Book Source Publications, Garg, Shruti, and G. Sahoo. "A Comparative Study of Classification Methods for Cracks in Old Digital Paintings." Proc. of Int. Conf. on Emerging Trends in Engineering and Technology DOI :03. AETS .2013.3.253 © Association of Computer Electronics and Electrical Engineers, (2013).

6.IoannisGiakoumis, Nikos Nikolaidis, Member, IEEE, and Ioannis Pitas, Senior Member, IEEE “ , Digital Image Processing Techniques for the Detection and Removal of Cracks in Digitized Paintings” , IEEE TRANSACTIONS ON I MAGE PROCESSING, VOL. 15, NO. 1, JANUARY 2006 .

7.Deepika Pagrotra, Navneet Kaur, “ A Review Paper On Crack Detection and Restoration of Old Painting”, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

8.B. Cornelis , T. Ruzˇic´, E. Gezelsd, A. Dooms , A. Pizˇurica , L. Platiˇsa, J. Cornelis, M. Martens, M. De Meye, I. Daubechies “Crack detection and inpainting for virtual restoration of paintings: The case of the Ghent Altarpiece “Signal Processing, Volume 93, Issue 3, March 2013, Pages 605–619

9.M. KirbieDramdahl “Morphological Operations Applied to Digital Art Restoration ”, Scholarly Horizons: University of Minnesota, Morris Undergraduate Journal Volume 1 | Issue 2 Article 6,2014

10.Pratap Kumar Dakua, Dr.S.S.Nayak and Sunila Kumar Swain “DETECTION AND REMOVAL OF CRACKS IN DIGITIZED PAINTINGS”, Asian Journal of Science and Technology Vol. 5, Issue 12,pp.828-832, December, 2014 11.G SchirripaSpagnolo, F Somma “Virtual restoration of cracks in digitized image of paintings” , International Conference on Defects in Insulating Materials IOP Publishing Journal of Physics: Conference Series 249 (2010) 012 doi:10.1088/1742-6596/249/1/012059

12.Khyati T. Vaghela, Narendra M. Patel,” Automatic Crack Detection and Inpainting”, International Journal of Computer Science Engineering (IJCSE), ISSN : 2319-7323 Vol. 3 No.06 Nov 2014,p271-275

13.Sukhjeet Kaur, Amanpeert Kaur,” Restoration of Historical Wall Paintings Using Improved Nearest Neighbour Algorithm” , International Journal Of Engineering And Computer Science ISSN:2319- 7242 Volume 3 Issue 12 December 2014, Page No. 9581-9586. 14.Rousopoulos, P., Arabadjis, D., Panagopoulos, M., Papaodysseus, C., &Papazoglou, E., “Determination of the method of drawing of prehistoric wall-paintings via original methods of pattern recognition and image analysis” IEEE International Conference on Image Processing ,pp. 65-68,2009.

SMART BIN IMPLEMENTATION IN METROPOLITAN AREAS

Akshatha G.S[1], Amrutha V[2], Deekshitha B[3], Noor Saba[4] , Janaki K
[1,2,3,4] UG Scholar, Associate Professor, Dept of CSE, RajaRajeswari College of Engineering,Bangalore-74
E-Mail: akshatagsawant@gmail.com , karur.janaki@gmail.com

Abstract: **In the present day scenario, there is a vast growth in the rate of urbanization and thus there is a need of bearable non-rural development plans. Now using current technology and deliberate approach, the conception of metropolitan cities is coming up all around the world. A metropolitan city is imperfect without a smart waste management system. This paper narrates the usage of "smart bins" in waste management system of metropolitan cities. This model is based on microcontroller 8051, wireless module GSM sim300 which is used to send the message to the respective authority, an ultrasonic sensor which is used to measure the distance of the garbage filled and an LCD which displays the threshold value of the bin.**

Keywords: **Microcontroller, GSM Sim300, Ultrasonic Sensor, Threshold Value**

I. INTRODUCTION

There is one notable problem as the world is in a phase of up gradation to manage with garbage. In our daily life we see that the garbage bins placed at the public places are overflowing. Thispromotes number of disorders as large number of insects and mosquitoes breed on it. A huge task in the metropolitan cities is waste management not only in India but almost in all the countries in the world. Hence, such a system has to be enhanced which can suppress this complication or to some extent. The project provides us one of the most systematic ways to retain our environment clean and green. The smart city notion is still unfamiliar in India, although it has undergone a lot of recognition in past few years when our present prime minister came up with an idea of establishing 100 smart cities all over India. The basic requirement of a smart lifestyle begins with hygiene and hygiene begins with garbagebin. A society will get its garbage settled properly only if the garbagebins are placed well and composed well. The main difficulty in the current garbage management system in most of the Indian cities is the unhealthy condition of dustbins. In this paper we have tried to improve the insignificant but essential component of the urban garbage management system, i.e. garbagebin. Now with the arise of technology it is high time that we should use technology for garbage management systems. As we have observed that technology with analysis has made the world a better place to live by its petition in the field of genetics, insurance, marketing, engineering, banking etc. in past many years. So, in this paper we have united analytics and electronics in order to bring out optimal changes in the typical methodology of garbage collection with the huge amount of data that is being produced by the smart bin networks.

II. PROPOSED SYSTEM

The block diagram of the proposed system "Smart bin implementation in metropolitan areas" is shown in the Fig.1.

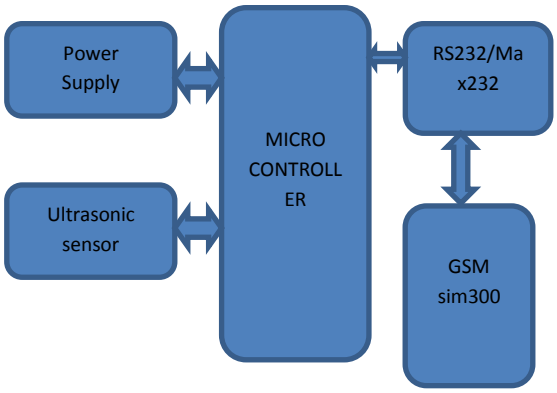


Fig.1. Block diagram of Proposed system

System design is the process of specifying the architecture, parts, modules, interfaces and data for a system to please specified requirements. Systems design could be seen as the application of systems theory to product enhancement. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering .If the immense topic of product enhancement "combines the perspective of marketing, design, and manufacturing into a single approach to product enhancement", then

design is the move of receiving the marketing information and producing the design of the product to be manufactured. Systems design is therefore the process of explaining and developing systems to please the specified requirements of the user. The main components of the system are Microcontroller, Power supply, GSM sim300, Ultrasonic sensor. Two software mainly used in this system. The first one is the keiluv4 development tools which are proposed for the professional software developer, however programmers of all levels can use them to get almost out of the embedded microcontroller architectures that are supported. The second one is embedded C which is a set of language augmentation for the C programming language by the C standards committee to label commonality problems that exists between C augmentation for different embedded systems.In-System Programming(ISP) is the ability of some programmable microcontrollers, logic devices and other embedded devices to be programmed while installed in a complete system, rather than demanding the chip to be programmed prior to installing it into the system.The hardware setup and complete model of proposed system is shown in the Fig.2 and Fig.3 respectively.

A .Microcontroller

The Intel 8051 microcontroller is one of the accepted popular general purpose microcontrollers which is in use today. The Intel 8051 is an 8-bit microcontroller which means that most available operations are restricted to 8 bits. Some of the features that have made the 8051 are Chip program memory-4KB,Chip data memory(RAM)- 128 bytes,4 register banks, User defined software flags-128,Data bus-8 bits, Address bus-16 bits,16 bit timers (usually 2, but may have more, or less), 2 external and 3 internal interrupts.

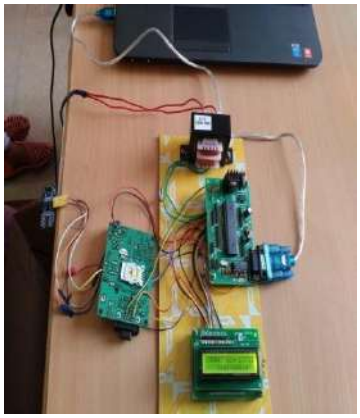


Fig.2.Hardware setup of the proposed system

- Bit as well as byte addressable RAM area of 16 bytes is available.
- Four 8-bit ports are available (short models have two 8-bit ports).
- 16-bit data pointer and program counter..

B. GSM/GPRS Module

GSM/GPRS module is used to build communication between a computer and a GSM-GPRS system**.** Global System for Mobile communication (GSM) is an architecture which is used for the mobile communication in most of the countries. Global Packet Radio Service (GPRS) is an extension of GSM that validates higher data transmission rate. GSM/GPRS moduleconsists of a GSM/GPRS modem gathered together the with power supply circuit and communication interfaces (like RS-232, USB, etc) for computer. The MODEM is the spirit of such modules.

C. Ultrasonic Sensor

Ultrasonic sensors are devices which are used for electrical–mechanical energy transformation. Here the mechanical energy will be in the form of ultrasonic waves and these waves are used to determine the distance from the sensor to the target object. Ultrasonic waves are longitudinal mechanical waves which travels as compressions and also rarefactions along the direction of wave propagation through the agency. Any sound wave which is above the human auditory range of 20,000 Hz is called ultrasound.

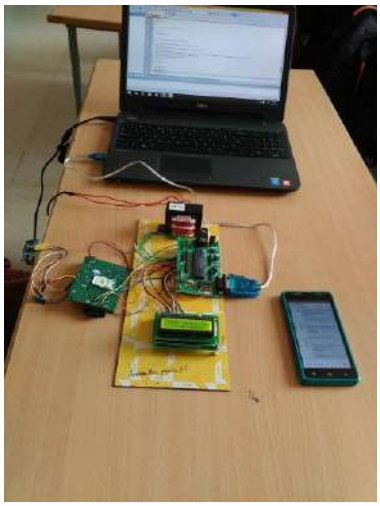


Fig.3.Complete model of proposed system

D. Rs-232 Communications

RS-232 is a standard used by two serial devices in order to communicate within 50 feet with transmission voltages between –15V and +15V, transmission of characters (of 7 bits of length).One salient aspect of RS-232 is that it is an asynchronous type of communication. Asynchronous communication is very important because it is systematically efficient; if the data is not sent, the connection is "idle." No additional CPU overhead is required for an idle serial line.

E. Power Supply

A power supply is just an electronic device that donates electric energy to an electrical load. The key function of a power supply is to transform one form of electrical energy to another and, as a result, power supplies are sometimes known as the electric power converters. Some power supplies are distinct, stand-alone devices, whereas others are constructed into larger devices along with their loads. Examples of the latter include power supplies found in desktop computers and customer electronics devices.

III. RESULTS AND DISCUSSION

The ultrasonic sensor is fixed at the top edge of the bin. So whenever the garbage exceeds the threshold value, the ultrasonic sensor senses it and alert message "smart bin is filled please replace as soon as possible" is sent to the respective person or authority as shown in Fig.4. On receiving the message the bin shall be replaced.

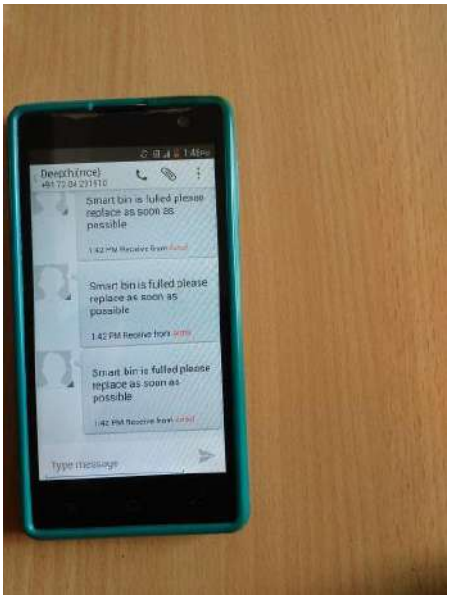


Fig.4. Real time smart bin status

IV .ADVANTAGES

It uses for waste Level detection inside the dustbin .it transmits the information wirelessly to concerned authority.It avoids the overflows of Dustbins .This embedded based waste managementsystem is very useful for smart cities in different aspects. There are different dustbins located in the different areas and dustbins get over flown many times and the concerned people do not get information about this. The concerned authority can access the information from anywhere and anytime to get the details. Accordingly they can take the decision on this immediately.

V. CONCLUSION

Urbanization is at an expeditious growth stage around the world, as more number of people desire to live in the city lights with more opportunities for growth and success. By employing the concept of wireless technology, we are able to create our communication more economical, rapid with greater efficiency. With advancement of technology things are becoming faster and easier for us. Automation is the use of control systems and information technologies to reduce the need for human work. Moreover, owner can control waste bin automatically by mobile using GSM technology from anywhere. The project is small but efficient step towards cleanliness and believes that this paper would encourage people. Overall this project discusses the analysis, design and implementation of city automation.

REFERENCES

[1] Narayan Sharma,NirmanSingha and TanmoyDutta," Smart Bin Implementation for Smart Cities", International Journal of Scientific & Engineering Research(ISSN 2229-5518), Volume 6, Issue 9, September-2015

[2] KanchanMahajan, "Waste Bin Monitoring System UsingIntegrated Technologies", International Journal of Innovative Research in Science,Engineering and Technology, Issue 3 ,Issue 7 , July 2014.

[3] M. Al-Maaded, N. K. Madi, RamazanKahraman, A. Hodzic, N. G. Ozerkan , An Overview of Solid Waste Management and PlasticRecycling in Qatar, Springer Journal of Polymers and the Environment, March 2012, Volume 20, Issue 1, pp 186-194. '

[4] Islam, M.S. Arebey, M. ; Hannan, M.A. ; Basri, H,"Overview for solid waste bin monitoring and collection system" Innovation Managementand Technology Research (ICIMTR), 2012 International Conference , Malacca, 258 – 262

[5] Raghumani Singh, C. Dey, M. Solid waste management of Thoubal Municipality, Manipur- a case study Green

Technology andEnvironmental Conservation (GTEC 2011), 2011 International Conference Chennai 21 – 24

[6] Vikrant Bhor, "Smart Garbage management System International Journal of Engineering Research & Technology (IJERT),Vol. 4 Issue 03, March-20152000. [6] Narayan Sharma,, "Smart Bin Implemented for Smart City",International Journal of Scientific & Engineering Research, Volume 6, Issue 9, September-2015

[7] Michael Alexander, John Walkenbach, "Microsoft Excel Dashboards & Reports", Wiley; Second edition, 28 June 2013. (Book style)

[8] YannGlouche, Paul Couderc. A Smart Waste Management with SelfDescribing objects. Leister, Wolfgang and Jeung, Hoyoung and Koskelainen, Petri.The Second International Conference on Smart Systems, Devices and Technologies (SMART'13), Jun 2013, Rome, Italy. 2013.

[9] FodayPinkaSankoh, Xiangbin Yan, Quangyen Tran on "Environmental and Health Impact of Solid Waste Disposal in Developing Cities: A CaseStudy of Granville Brook Dumpsite, Freetown, Sierra Leone," on Journal of Environmental Protection, 2013, 4, 665-670. (Journal or magazine citation

DIGITAL MODEL APPROACH TO WATER SUPPLY MANAGEMENT USING IOT

Kavya H R[1], Prajwal R[2], Bhagyashree G[3], Sarvanan Perumal[4]
[1,2, 3] UG Scholar ,[4]Asst. Professor, Dept. Of CSE , RRCE, Bengaluru.
kavyarammurthy353@gmail.com, prajwalrjain@gmail.com, bhagyashreegangaraju@gmail.com

ABSTRACT: Water is the most precious and valuable since it is an essential need for all human beings but, these days Water Supply Management are facing difficulties in real time scenario because of inadequate amount of water due to less rain fall. With rapid raise in Population, urban residential areas have increased. Due to these reasons water has become a major problem which affects the problem of water distribution, interrupted water supply, water conservation, water consumption and also the water quality so, to prevail over these problems and make system efficient there is need of proper monitoring and controlling system.. Here every user is provided with a web based mobile application having many choices like recording the water flow rate using level sensors and sensors for checking water quality and send the same to remote monitoring station using iot and it is also provided with solenoid valves for supply purpose. The on/off of valves are controlled by Raspberry pi, which stops the flow whenever the rate exceeds pre-defined limit. Using different kinds of sensors with controller and raspberry pi as Minicomputer for monitoring data and also controlling operation with efficient client server communication.

KEYWORDS: Raspberry pi,Water level sensor,Flow sensor, Turbidity sensor, Solenoid valves, motors, Relays.

I. INTRODUCTION

The recent survey on water supply reports about scarcity of water due to less rain fall and rapid growth in population. Many cities are facing inadequate supply of water for their daily needs and this is due to lack of monitoring and control over supply. The monitoring of water resource for enterprises can put a stop to the occurrence of theft and leakage water successfully. There is imbalanced supply of water as some areas in city get water but the other areas doesn't and other problems are excessive consumption, run over of tanks, outflow in pipeline ,broken up water supply ; in order to overcome these issues continuous monitoring, water supply scheduling and proper distribution has to be done.. Water is fundamental for each one and it is very much important to save water, but many a times due to lack of monitoring, overflow of tanks occur and plenty of water gets wasted, the other factors like overflow in pipelines with more pressure results in pipeline damage and leakage detection. By focusing on harms in traditional methods our system design and develop a low cost embedded device for synchronized monitoring of water distribution using Internet of things (IOT). IOT is a globe where billions of objects sense, communicate and share information, all are interconnected based on public or private Internet Protocol (IP) networks. These interrelated objects have data regularly collected, analyzed and used to initiate action, providing riches of intelligence for planning, managing and decision making.

II. PROPOSED SYSTEM

The anticipated system is developed on embedded based remote water controlling and theft avoidance system by recording the rate of flow at the consumer/user end. For the implementation of proposed system, every consumer end should be provided witha web based mobile application which has many choices like recordingthe rateof flow byusing a level sensor and to send the same to a remote monitoring station using IOT and in addition an electrically operated solenoid valve is provided to supply water to the consumers. With the swift development of universal system Internet infrastructure and information, communication technology in the past few years has made the communication dependable for transmitting and receiving information resourcefully. So the concept of IoT is used for efficient communication purpose.

Block Diagram: Interaction Of Components With Raspberry Pi Using Iot

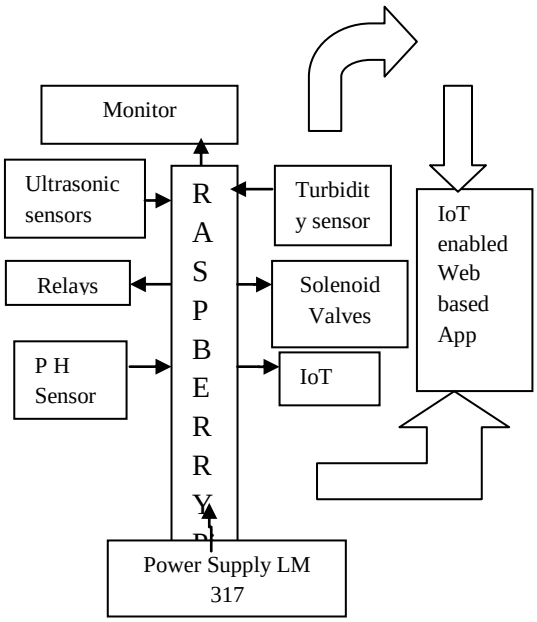


Fig1.Working Principle Of Proposed System

The proposed project supports usage of Anti-theft control system for drinking water supply. By implementing this anticipated system in a real time; certainly it is possible to manage the drinking water larceny in the domestic areas. Supply of water in urban areas to residence and commercial establishments are provided at a fixed rate of flow. There are cases of surplus water drawing by certain customers/users by linking motor-pump sets to the water lines which is referred as water theft.

The proposed system is used to develop an embedded based remote water monitoring and theft prevention system by recording the rate of flow at consumer/user end. To implement the proposed water supply system, each consumer end should be provided given a web based mobile application having many options for the user like to record the rate of flow using a level sensor and to transmit the recorded value to a remote monitoring station using IOT and in addition with an electrically operated solenoid valve for supplying water to consumers.

The valve turns on/off using Raspberry Pi which is the central processing unit used for supplying water for a limited time period. In addition the system is provided with an electrically operated solenoid valve to terminate the water supplyeach time the flow rate exceeds a predefined limit. Using TRAIC switch the processor will switch ON/OFF the solenoid valve and in use of IOT for wireless communication, using this information can be passed between consumer and service provider.

III. REQUIREMENTS OF HARDWARE AND SOFTWARE

HARDWARE: Raspberry pi

Fig2: Raspberry Pi Board

Raspberry pi is a low cost small and portable size of computer board it has a high performance powerful processor its main core language is raspbian OS can alsodevelop script or program using python language. Raspberry pi 2 has CPU 900 MHz BCM2836 quad-core ARM Cortex-

A7 Memory,1GB RAM, It has a 40 pin GPIO connector, micro SD. Purpose of using raspberry pi is an IOT. Raspberry is compatible with IOT.

PROCESSOR

The system on a chip(SoC) worn in the first generation Raspberry Pi to some extent is equivalent to the chip used in older Smartphone's(such as iPhone, 3G, 3GS). The Raspberry Pi is based on the BroadcomBCM2835 SoC,which includes an 700MHz ARM1176JZF-S processor, Vide core IV graphics processing unit(GPU),and RAM. It has aLevel 1 cacheof 16KBand a Level 2 cache of 128KB. The Level 2 cache is used primarily by the GPU. The SoC is stakeunderneath the RAM chip, so only its edge is visible.

PYTHON (PROGRAMMING LANGUAGE)

Python is a widely used advanced, general-purpose, vibrant programming language. Its design viewpoint stresses on code readability, and its syntax permits programmers to put across concepts in smaller amount of code which is not possible in other object oriented languages for instance C++ or Java. The language supports constructs intended to enable clear programs on both a small and large range. Python supports manifoldencoding standards, including object-oriented, fundamental and functional programming or methodological styles. It features a dynamic sort of system and mechanical memory management and has a huge wide-ranging standard library.

FEATURES OF PYTHON

The core philosophy of the language includes:

- Beautiful is better than ugly
- Explicit is better than implicit
- Simple is better than complex
- Complex is better than complicated
- Readability counts

WATER SOLENOID VALVES

Fig3: Water Solenoid Valve

Operating Voltage: 12V DC.

Current: 500mA.

Pressure: 0.2 ~ 10 Bar.

Pipe Diameter 1/2"

Application: To control Water Flow.

RELAY

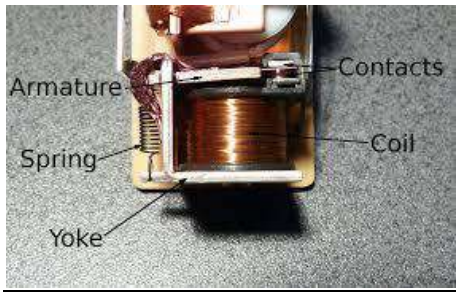


Fig: 3 Relay

ThisBoardcanbeusedtoControl Solenoids,Motorsetc.

•InputLogic-5vlevelfromMUC.

•Interfacedwith Transistor 547.

•InputPinconnectedtoBurgstick.

ULTRASONIC SENSORS

.

Fig: 4 Ultrasonic Sensors

Ultrasonic sensors are devices which are used for electrical–mechanical energy transformation. Here the mechanical energy will be in the form of ultrasonic waves and thesewaves are usedtodetermine the distance from the sensor to the target object. Ultrasonic waves are longitudinal mechanical waves which travel as compressions and also rarefactions along the direction of wave propagation through the agency. Any sound wave which is above the human auditory range of 20,000 Hz is called ultrasound.

ADVANTAGES

- ✓ **Economical**: The proposed system is inexpensive and low budget.
- ✓ **Portable**: The proposed system is mobile and transferable.
- ✓ **Reduced Man Power:** The basic aim of concept is to reduce the man power & to increase the accuracy of the system. So we can able to achieve the same with our own built concept.

TECHNICAL SPECIFICATIONS

1. Operating voltage of embedded circuitry is 3.3vdc
2. Current consumption of device in active mode 200mill amp
3. Operating frequency of device is 10MHZ to 60MHZ.

APPLICATIONS

1. It can be used in Fuel supply system in underground tunnels.
2. The concept can be used in electricity management system.

CONCLUSION

Using proposed system secure and continuous monitoring is possible. There is no need for field monitoring which means manual work has been reduced and hence it makes the system more resourceful, reliable, low cost and accurate. Data is monitored from anywhere controlling is possible from a remote server it is economical in development.

REFERENCES

[1] Gouthaman.J, Bharathwajanprabhu.R&Srikanth.A "Automated urban drinking water supply control and water theft identification system" Proceeding of the 2011 IEEE Students' Technology Symposium, IIT Kharagpur pp.87-91, 2011.

[2] S.Leirens, C. Zamora, R.R. Negenborn, and B. De Schutter "Coordination in urban water supply networks using distributed model predictive control" Proceedings of the 2010 American Control Conference, Baltimore, Maryland, pp. 3957–3962, 2010.

[3] Shicheng Dong, Hao Jin "Design of wireless monitoring system for urban water supply based on embedded technology" International Conference on Measurement, Information and Control (MIC), pp.348-351, 2012

[4] Lingjuan Wu, Jennifer Trezzo, DibaMirza, Paul Roberts, Jules Jaffe, Yangyuan Wang, Fellow and Ryan Kastner IEEE Members."Designing an Adaptive Acoustic Modem for Underwater Sensor Networks".

[5] Peng Jiang , Hongbo Xia , Zhiye He and Zheming Wang "Design of a Water Environment Monitoring System Based on Wireless Sensor Networks" Sensors, ,pp. 6411-6434, 2009.

[6] H.G.Rodney Tan, C.H.Lee and V.H.Mok, "Automatic Power Meter Reading System Using GSM Network", 8th International Power Engineering Conference (IPEC),pp-465-469, 2007. [7] Ma Ming, "Design of embedded system application platform based on ARM", Manufacturing Automation, vol.34, pp 15-16, 2012.

[8] Hen Hui, Zhou Wenchao and so on, "Design of the embedded remote meter reading system based on Ethernet", Electronic Design Engineering, vol. 20 pp. 184-186, 2012.

[9] Stancil, Stoian and Kovacs, "Urban water supply distributed system", vol.3, pp.316-321, 2008.

Comparisons of Data Mining methods for Customer churn Prediction

Swetha P[1], Dr.Usha S[2]
[1]Research Scholar, [2]Professor, RRCE, Bengaluru.
Shwetha6600@gmail.com ,Sakthivelusha@gmail.com

Abstract-In the current competitive mobile world, it has become obvious for all the service providers to survive by attracting new customers to their network and it also has become obvious for them to retain the existing customers. This acquiring and retention of customers will increase the revenue for the company. Thus, for any service provider it becomes the important task to identify their customers who are likely to churn in future. This paper shows the different mining methods comparison to identify the true churners for the benefit of the company.

Keywords: Customer relationship Management (CMR), ANN,

I . INTRODUCTION

Since there is a high influence on customer relationship management in recent years, churn prediction has gained attention.This customer churn prediction has major role in the telecommunication industry. Churnprediction is the process of identifying those customers who leaves the current service provider due to the dissatisfaction of the current services and/or due to the better services they got from the new service provider. These customers may contribute in the loss of profit to the company. Hence the companies use new state of art of applications and technologies to identify and retain those customers.

Today in the competitive telecommunication industry, retaining the customers should happen to increase in the company profit.For retention of customers we need to first identify those customers who likely to churn in future. To identify the customers we aim at studying the Customer relationship Management (CMR) which in turn helps to identify few data mining techniques to predict the churners.Thus the paper is organized into two sections where the section1 consists of concepts of CMR and its basics followed by comparisons of existing data mining techniques in churning.

II. CUSTOMER RELATIONSHIP MANAGEMENT

With the new advent of technologies in the market, the term CMR is widely used.The term CMR has gained a lot of importance in recent years due to the high competitive world. CMR helps in acquiring knowledge about customers. Customer relationship management is a two way process in which it uses the knowledge about the customers to maintain relationship with the customers [1].Thus CMR provides a strategy and process of acquiring and retaining the selective customers to make an increase in the value of an company and customer. It also involves integrating marketing, sales, supply chains, customer service functions of a company [2].

Benefits of CRM include the following:

- CRM helps in accumulating, storing and distributing the customer data.
- CRM along with the information technology helps in acquiring the more personal interaction of customer data.
- CRM helps to judge the customer loyalty and profitability to the company based on the customer behavior recorded.
- CMR helps in increased customer retention and profit to the company.

1.1 Customer Attributes

CRM helps in acquiring the enormous information about the customers. This acquired information may have the data which may not help in churn prediction.

Thus, the customer information can be grouped into following categories [3]:

- Customer service details
- Customer personal details
- Customer credit score
- Bill and payment details
- Customer usage pattern
- Customer value added services

The study of the customers behavior based on above categories will help us in predicting the churn customers. As only these information are not sufficient for predicting, we have different data mining models which assist in obtaining the better prediction.

III. Data Mining Process

In the last few years there is a huge increase in the volume of data that the companies need to maintain.The data received will be of raw and needs many mining process to be done on that data to retrieve the useful information. Thus, data mining models provides a better solution[4].

The term data mining also known as Knowledge Discovery process can be defined as the process of searching the large datasets, repositories for the required patterns, associations and trends[5].Data mining process involves data collection, data storage, data preprocessing and data preparation[6]:

1. Data Collection

In this stage, the data for mining process is collected from different sources. Data can be present in different large repositories, databases, etc..All these data are collected and can be represented in the form of chart which includes many customer attributes like customer number, call minutes used in different times of the day, call charges,etc..

2. Data Preprocessing

Since the collected data will have many noise, outliers and all these should be removed and our data should be preprocessed before using it for mining.Thus the unwanted data and attributes which are empty in the dataset should be ignored.

For example, the missing values in call_date, call_time, call_duaration attributes can be ignored.

3. Data Preparation

Once the data is preprocessed, now we can set the threshold value to the dataset and we can also search for the required pattern of data in the data set. Once the required data pattern matches with the existing data, then that data pattern can be mined and can be stored for future reference. Then the different decision making models can be applied on this to predict the true churners.

IV. Data Mining Methods

Many research is going in this field by applying various different data mining algorithms based on classification and prediction models. In this paper we mainly concentrate on comparing two models: Decision tree and Neural Network.

- **Decision Tree**

A decision tree is a decision support tool, which has tree like structure. Decision trees are the most common method used in classifying and evaluating the true churners. Decision trees use the concept of divide and Conquer. Each internal node represents a test on an attribute and the branch shows the outcome of the test. Each leaf node holds the class label and the initial node in a tree will be called as a root node. These decision trees can be easily converted into classification rules and hence they are widely used[7].

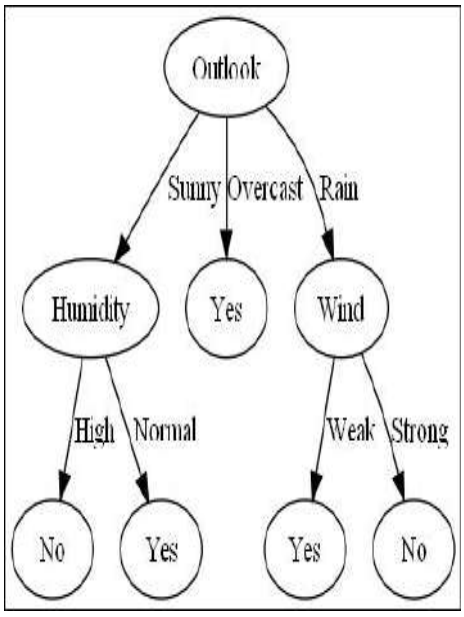


Fig1 : A simplified example of decision tree

The customer's dataset can be evaluated by developing a decision tree and by altering a tree until a leaf node is attained.

Decision trees are not suitable for complex and non-linear relationship between attributes. Hence more advanced algorithms like CART, C4.0, ID3 are used.

Neural Network

Artificial Neural Networks (ANN) are the statistical group of algorithms derived by biological neural networks. It can be accessibleas an interconnected neurons which can calculate values from inputs and helps in machine learning. This method has the capability of learning from errors[4].

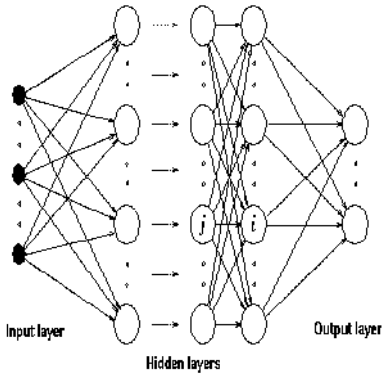


Fig2: Activation Functions of Neural Networks

The idea behind the neural networks is that each attribute is associated with a weight. During the learning the weights are constantly updated and based on the

predictor variables the neural network calculates a combination of the inputs and to output the probability of a customer being a churner [8].

V. Decision Tree Vs Neural network

Comparison of two data mining algorithms used for churn prediction is summarized in the following table[9]:

Table1: Comparision of two data mining techniques.

Classifier	Parameters	Pros	Cons
Decision trees	Set of Candidate attributes and an attribute selection method	Domain Knowledge is not required for tree construction. High dimensional data can be handled easily. Both numeric and categorical data can represented easily and understandable.	Output limited to one attribute. Decision trees algorithms are unstable. Trees of numeric data can be complex.
Artificial neural Network		Requires less statistical training. High tolerance to noisy data. Availability of multiple training algorithms.	More computational burden. Proneness to overfitting.

CONCLUSION

As customer relationship management is an important task for the company to have long retention of customers. Maintaining the customer behaviour and which inturn helps in predicting the churners will make the company increase in their revenue. Thus, prediciting the true churners with different data mining algorithms and comparing their results and accuracy will be my future work.

REFERENCES

1. "Impact of Customer Relationship management on Customer Relation in Telecom Industry of Pakistan"; Industrial Engineering Letters (IISTE), Vol 4, 2014.
2. Ali Tamaddon ,Jahromi; "Predicting customer churn in Telecommunication Service providers"; Lulea university of technology.
3. V Umayaparvathi, K iyakutti; "A survey on Customer Churn Prediction in Telecommunication industry:Datasets, Methods & Metrics"; International Research Journal of Engineering & Technology (IRJET), Vol 3, Issue 4, April 2016.
4. Kiran dahiya, Kanikatalwar; "Customer Churn Prediction in Telecommunication industries using Data mining Techniques-A review"; International Journal of advanced research in computer science & software engineering, Vol 5, Issue 4,2015.
5. DrMamtamadan, drMeenu Dave, Vani Kappor; "A Review on data mining for telecom customer churn management"; International Journal of advanced research in computer science 7 software engineering, Vol 5, Issue 9,2015.
6. Aishwaryachuri, MayuriDivekar; "Analysis of customer churn in Mobile industry using data mining"; International journal of emerging technology and advanced engineering, Vol 5, Issue 3, March 2015.
7. Amal M Almana, Mehmet SabihAksoy; " A survey on data minig techniques in customer churn analysis for telecom industry"; International Journal of engineering research and applications, Vol 4, Issue 5, May 2014.
8. VladislavLazarov, Marius Capota ; "Churn Prediction"; www.researchpapers.com.
9. Nisha Saini, Monika; " Churn prediction in Telecommunication using classification techniques based on data mining: A Survey" ; International Journal of advanced research in computer science & software engineering.

Literature Survey of Image Compression Techniques

ChaithraVS[1], PoojaR[2], Janaki K[3]
[1,2]UG Scholar, [3]Associate Professor, Dept. of CSE, RRCE, Bengaluru
chaithra1684@gmail.com , karur.janaki@gmail.com

Abstract: Image compression addresses the problem to reduce the size of graphical file and also reduce the storage requirement area to represent an image. Image compression provides larger bandwidth as well as makes the faster transmission process and also affords security for the data transmission. In storage and transmission, the raw images need large amounts of disk space seems to be a big disadvantage. In this research work, a literature review was conducted to measure the progress made in the field of image compression. This paper summarizes the different compression methods based on different transformation techniques and it has been analyzed that wavelet transform have superior overall performance over other transforms in terms of compression ratio. On the basis of analyzing the various image compression techniques this paper presents a survey of existing research paper.

Keywords: Bandwidth, Compression ratio, Wavelet transform

I. INTRODUCTION

Image compression is a method with the persistence of reducing the quantity of data required to symbolize a digital image by eliminating the redundant data. It is also be used to decrease the size in bytes of a graphics filedevoid of corrupting the rate of the illustration to an intolerable level. The decrease in file size allows extra images to be stored in memory. Images are compressed for different reasons like storing the images in a lesser memory like mobile devices or low volume devices, for transmitting the large data over network, or storing large number of images in files for research purpose. This is essential due to the reason that compressed images can be transmitted faster due to its small size or it occupy minimum amount of memory space. Due to this reason, the properties of image compression on face recognition started getting importance and have become one of the important areas of research work in other biometric methods as well as iris recognition and fingerprint recognition. Most recent contribution were made in iris recognition and fingerprint recognition. In addition to giving importance to standard compression methods in recognition, researchers have concentrated in evolving special purpose compression algorithms, e.g. a recent low bit-rate compression of face images.

One of the major drawbacks in the face recognition using compressed images is, the image has to in the decompressed mode. The task of reconstructing a compressed image for the purpose of face recognition is computationally costly and the face recognition systems would advantage if full decompression could somehow be removed. In other words, while the images are in compressed mode, the face recognition is carried out and it would additionally increase overall performance of a face recognition system and computation speed. The most popular compression techniques are JPEG and their related transformations are Discrete Wavelet Transform and Discrete Cosine Transform.

II. PRINCIPLE OF IMAGE OFCOMPRESSION AND TECHNIQUES

The purpose of image compression is to decrease the size of digital images to protect storage space or transmission time. The image with size 512*512*3 = 786,431 pixels needs only 41,909 bytes when compressed in JPEG format. The space can be saved while maintaining most of the content during compression. The ratio of sizes expresses us about the efficiency of the image. The term describing this is known as the compression ratio.
Compression ratio:
Size of the compressed image/Size of an original image

A. Differential pulse-code modulation(DPCM)

DPCM is a signal encoder that adds some functionalities based on the prediction of the samples of the signalusing the baseline of pulse-code modulation (PCM). The input can be an a digital signal or analog signal. A discrete time signal is the input to the DPCM encoder when the input is a continuous time analog signal, it requires to be sampled first. Option 1 is to take the values of two successive samples. if they are analog samples it is to be quantized and the difference between the first one and the next is to be calculated. It can be additionally entropy coded. Option 2 is instead of taking a difference relative to previous input sample, the difference relative to the outcome of a local model of the decoder process is taken. The difference can be quantized, which allows a good way of including a controlled loss in encoding. Applying one of these two processes, short-term redundancy of the signal is removed. Compression ratios on the order of 2-4 can be achieved if differences are consequently entropy coded, because of the entropy of the difference signal is much lesser than that of the original discrete signal treated as independent samples.

B. Super resolution

Super resolution is a technique that alters the resolution of an image. The technique translates low resolution images to

high resolution which in turn growths the high frequency components and eliminates the blurriness produced by low resolution camera. So, this technique is used to reestablish the actual image with the high resolution image given a set of perceived images at lower resolution.

C. Normal matrices

Image compression are provided using normal matrices. For this purpose, the matrix representing the image is transformed into the memory of normal matrices. The properties of its eigen value decomposition are used, and someless important image data are removed. By returning to the original memory, the compressed image can be reconstructed.

D. Compressive sensing and lifting scheme

The concept of compressive sensing (CS) is to obtain significant information directly without first sampling of thesignal in the traditional logic. It is shown that if the signal is "sparse" or compressible,then the attained information is adequate to reconstruct the original signal with a highprobability.Sparsity can be defined with respect to an appropriate basis, such as WT or DCT for that signal. The theory of CS is also developed measurements of the signal through a

method that is incoherent with the signal. In CS, a sensing technique should provide aenough numberof CS measurements in a non-adaptive manner, so that it enables near perfect reconstruction.

E. Huffman coding

Huffman code is a particular kind of optimal prefix code which is commonly used for lossless data compression. The procedure of finding and using such a code progress by means of Huffman coding, algorithm developed byDavid A. Huffman and published in the year 1952 "A Method for the Construction of the Minimum Redundancy Codes". The termination from Huffman's algorithm can also be viewed as variable length code of the table for encoding a source symbol (such as character in a file). The algorithm has derived this table from the estimated probability or from the frequency of occurrence (*weight*) for each probable value of the source symbol. As in other entropy encoding methods, more commonly used symbols are generally represented using fewer bits than less commonly used symbols. Huffman's method can be efficiently implemented, finding code in the linear time for the number of input weights if these weights are sorted. Although optimal among methods encoding symbols individually, Huffman coding is not constantly optimal among all compression methods.

III. LITERATURE SURVEY

Mohamed Abo-Zahhadet al (2015) "Huffman Image Compression Incorporating DPCM and DWT",presented a image compression method consisting of the connection of the DPCM, the DWT and the Huffman coding. In this technique, the image is passed through the DPCM transformation, then the wavelet transformation is applied to the DPCM output, and lastly by Huffman coding the wavelet coefficients are encoded. The wavelet transformation reduces the spatial reputation in the image data and redundancy, by making the compression more efficient. Simulation results has revealed that the proposed DPCM-DWT-Huffman outperforms the Huffman methods, DPCM-Huffman and DWT-Huffman. These four methods provide CR of 6.48, 4.32, 2.27 and 1.2 respectively.

Zhang Ning et al (2015)"Study On Image Compression And Fusion Bases The Wavelet Transform Technology", presented the paper on wavelet analysis and its application in the image compression coding on the proposed improved SPIHT algorithm. The standard SPIHT algorithm is the quantization of wavelet coefficients, the standard SPIHT algorithm adopted quantitative two into interval fixed, without considering the features of energy distribution of wavelet coefficients, sometimes this is not the best method. This paper gives a new method based on this. The SPIHT algorithm is the algorithm than the standard decoding and encoding times greatly reduce thePSNR and time consumption and the SPIHT algorithm is quite. Lastly, using MATLAB to attain reasonable procedures shows the improved algorithm. This paper,proposes a new adaptive multiplicative noise elimination algorithm based on variation method. By analysis the fault of Euler-Lagrange equation, its found that these traditional variation models are not fitted for the multiplicative noise very well. The amount of the multiplicative noise is relative with pixel value.

Sudeepti Dayal et al(2015)"Image compression based on Super-Resolution Technique: A Review",reviewed image compression based on the super resolution technique, principle and need. Is also focus on various imaging file formats and lossless image compression and compression techniques of lossy. Thereby concluding that the super resolution technique is the most proficient technique of the image compression as it combines the multiple low resolution image to form a high resolution image. The advantage of using super resolution technique is that it costs less and existing low resolution image can still be utilized. The method can be applied in the areas of medical imaging, video imaging and satellite imaging.

HarpreetKauret al (2015) "Review of the Various Techniques for Medical Image Compression",stated Image compression refers to compression of the significant bits of an image so that the quality of the image does not gets affected. In this paper brief overview of lossy compression technique along with various techniques for lossless compression of medical images has been presented. Lossless image compression is widely used in many of the applications as this leads to minimum loss of data. It is an

efficient method to be used in the hospitals for diagnosing of several disorders. Auto Shape-R.Huffscheme for lossless compression is efficient as it provides greater compression ratio.

K. Mounika et al(2015)"SVD Based Image Compression", detailed the Singular Value Decomposition (SVD) which is a simple, reliable and robust technique. This SVD technique provides effective and stable method to splitting the image matrix to a set of linearly independent matrices. SVD provides good quality compression ratio and also practical solution to image compression problem. The results of this paper clearly displays the compressed output for different r values. Thus, the selection of the value plays a crucial role in this SVD based image compression technique.

Rahul Shukla and Narender Kumar Gupta(2015) "Image Compression by Huffman Coding Technique and DCT", specified that objective of the research is achieved by following observation. It concludes that Image Compression is an important technique in digital image processing. There are different methods of compression techniques but Huffman Coding technique is a good compression technique in the lossless image compression. Huffman compression is the variable length type of compression technique. By Huffman, coding redundancy can be eliminated when assigned the codes in better way. Discrete Cosine Transform with the Huffman codes is used in the proposed algorithm and good quality of the compressed image with high MSE value and PSNR has been achieved with high compression rate.

Sheikh Md. Rabiul Islam et al(2015)"Image Compression Based On The Compressive Sensing Using Wavelet Lifting", projected that the image compression is based on compressive image sensing using the wavelet lifting scheme framework that address the preservation of high frequency details in medical images and best compressed image components. This method is also compared with three different matrix, i.e., Bernoulli,Gaussian and random orthogonal measurement matrix. Image reconstruction by convex optimization technique for reforming of the image via l1-norm which is called as greedy pursuit such as Orthogonal Matching Pursuit algorithm andBasis Pursuit. Experimental results exhibit that the proposed sparse CDF9/7 wavelet transform are better compressed images than sparse DCT or DWT with Basis Pursuit (BP) or OMP algorithm in proposed framework with CS.

Anitha. S (2015) "Lossless Image Decompression And Compression Using Huffman Coding", proposed image compression method which well suited for gray scale bit map image. Huffman coding suffers from the fact that uncompress or need have some information of the probabilities of the symbols in the compressed file, this can need more bits for encoding the file. This work may be extended for the better compression rather than other compression techniques. The performance of this proposed compression technique using human coding and hashing is performed on TIFF, GIF formats. This technique can be applied on chrominance and luminance of the color images for getting better compression.

Rime Raj Singh Tomar and Kapil Jain(2015) "Lossless Image Compression using Differential Pulse Code Modulation",paper proposed the method of compression that is based on Huffman entropy and EDT encoding. Compression ratio of the proposed method is most powerful than few previous methods. This method is suitable for thereal Time applications. Comparison was based on compression efficiency which is computational complexity and compression ratio. To understand the efficiency of this method for medical compression and real time application of medical imaging such as online diagnosis and telemedicine, test this method on medical test cases. So, it can be efficient for lossless compression and implementation on near-lossless or lossless medical image compression. Further, compare this method with previous JPEG standards such as lossless JPEG2000 and JPEG. As it is illustrated and proved by simulations, the new compression method causes good compression ratio and improve older method. The compression ratio improvement helps the real time process and helps transmission systems to work faster. It is a low complex method in spite of the compression ability.

E. Kokabifaret al(2015) "A new approach for image compression using normal matrices", stated eigenvalue decomposition of skew-symmetric and symmetric matrices, as two important kinds of normal matrices, and the properties applied to obtain image compression scheme. Thismethod is uncomplicated and straightforward ones requiring fewer and clear computations as compared to some of the exiting methods. This image compression method is the first one introduced and concerns with the symmetric part of an image, which is also applicable in the case of the skew-symmetric part of the images. The technique is capable of keeping halfof the image unchanged, and this feature may be of some usage. This experimental study shows, just half of the original image can be changed, which causes the compressed images to lose its reliability. This makes the technique different from other image compression techniques. The second image compression scheme using both skew-symmetric and symmetric parts of the original image was proposed. Experimental results show the high reliability of this method. Finally, the proposed method can be used to devise block-based compression techniques.

IV. CONCLUSION

The observation from literature survey exposed superior performance of wavelet transform
over other transforms in terms of compression ratio and PSNR. There is a greater overall performance of wavelet transform based compression against other compression algorithms at higher compression ratios. wavelets offer a

much richer set of directions and shapes, and thus they are more effective in capturing geometric structures in images especially in medical images. Compression of images using wavelet transform can be extended to real time application for video compression in medical images.

REFERENCES

[1] S.Srikanth, SukadevMeher,"Compression Efficiency for Combining Different Embedded Image Compression Techniques with Huffman Encoding" IEEE, 2013.

[2] Bhonde, Nilesh, Shindesachin, NagmodePradip and D.B.Rane "Image compression using discrete wavelet transform" in A national level conference held at Prava engineering college,Maharashtra.

[3]]Suresh Yerva, Smita Nair and Krishnan Kutty, Lossless Image Compression based on Data Folding, IEEE, pp. 999-1004, 2011.

[4] Joan Puate, Fred Jordan "Using fractal compression scheme to embed a digital signature in to an image "in signal processing laboratoryr4, Switzerland.

[5] AshutoshDwivedi, N Subhash Chandra Bose, AshiwaniKumar."A Novel Hybrid Image Compression Technique": Wavelet-MFOCPN, 2012.

[6] FirasA.Jassim and Hind E.Qassim," Five Modulus Method for Image Compression", Vol.3, 2012.

[7] K. Rajakumar and T. Arivoli "Implementation of Multiwavelet Transform coding for lossless image compression," IEEE, pp. 634- 637, 2013.

[8] Firas A. Jassim and Hind E. Qassim, "Five Modulus Method for Image Compression", SIPIJ Vol.3, No.5, pp. 19-28, 2012.

[9] S. Sahami and M.G. Shayesteh,"Bi-level image compression technique using neural networks" IET Image Process, Vol. 6, Issue 5, pp. 496–506, 2012.

[10] G.M.Padmaja,P.Nirpuma "Analysis of various image compression techniques" APRN journal of science and technology VOL.2, NO.4,May 2012

[11] RichaGoyal "A review of various image compression techniques" International journal of advanced research and software engineering Volume 4 issue 7, July 2014

SELF REGULATED TRAFFIC COMMAND CONTROL SYSTEM USING IoT

Abhijit K S[1], Divyashree J[2], Anitha K[3]

[1,2]UG Scholar, 3Asst.Professor, Dept. of CSE, RRCE, Bengaluru

E-mail:abhijitsn1001@gmail.com , divyajayashankar3@gmail.com ,anithakrishna14@gmail.com

Abstract-In this rapidly developing world, transportation contributed a major part. In recent years, the number of vehicles has been increased like a wildfire. This increase in number of vehicles leads to many problems such as traffic congestion, accidents, violation of traffic rules etc. In metropolitan cities, it is very difficult for the commuters to reach their working places or their residence in time. We cannot reduce the vehicles density instead we can think of better traffic management systems. At present all traffic signals are operating manually i.e. the traffic police has to switch the signals for each lane. Or else he can set a time interval for each lane. But the problem in this is waiting at each traffic signal. And also accidents are becoming more and more and more traffic rule violations. Actually, this is the current problem in metropolitan cities. So, present signal management concept fails to give the solution for this problem. Using RFID somehow we can manage the traffic, but it has disadvantages too. Implementation is expensive and also the maintenance. For emergency service vehicles, it has to be worked manually. And also weather problems. Nowadays, technology is developing rapidly. Why can't we use this modern technology to overcome this problem? This paper aims in providing a better solution to this problem using Internet of Things- IoT. Here we make the signals intelligent and make them to communicate with the central control unit. So, at every time intervals the signals send the current scenario at their places to the central control unit through GPS. Later the data is send to the central control unit. Then it analyses the data and intimates the signal control unit to switch ON/OFF. By using this information about the traffic we can extend the application to a higher level. At present, there are signage boards at every traffic signal to give directions to different places. We can mount digital signage at every traffic signal. So, by using the information provided by the GPS, we can display the directions to the different places along with approximate time duration to reach those places from that traffic signal. It mainly helps vehicles which do not have GPS navigation. This provides a smooth traffic control.

Keywords— ***Wireless sensor network, traffic enforcement camera, GPS, network powered switches,* RFID**

I. INTRODUCTION

In recent years the transport system has been developed rapidly. The main contributor for this problematic development is the private vehicles. Increase in the number of vehicles lead to traffic congestion.

Some of the major causes for traffic congestion are:

*Violation of traffic rules

*Careless driving/riding

* Roads are characterized by private vehicles, trucks, buses, two-wheelers, three-wheelers, carts and pedestrians. So this gives rise to problems for managing traffic and leads to slow moving traffic or even traffic jam.

* Metro construction, damaged roads, all contributes to traffic congestion in the city.

To limit this, the traffic management system must be developed. For this problem, Internet of Things gives the better solution. [1]

The internet of things is the internetworking of physical devices, vehicles and other things which are extended with software, electronics, sensors, actuators and network connectivity that allows these objects for the collection and exchange of data.The Internet of Things helps in sensing the objects and it controls remotely the present network infrastructure, which leads to the opportunities for creating the physical world into computer-based systems, which further leads in improving accuracy, efficiency and economic benefit. [2]

When Internet of Things is extended with sensors and actuators, the technology can do multiple works of similar type, which further becomes solutions for smart homes, transportation and cities. Each thing is separately identified using its embedded computing system. It is also able to interoperate within the current Internet infrastructure.

Internet of Things relates the real world to the virtual world which enables whenever, wherever connectivity for a thing that has an ON/OFF switch. It comprises physical objects and living beings, and also virtual data and environments, which communicate with each other. Large amount of data is generated as a large number of devices are connected to the internet.

II. RELATED WORKS

A number of researchers have been carried out related to the traffic monitoring and controlling. And the outcomes of these researches led to several different approaches. Few among them are traffic flow prediction mechanism which is based on a fuzzy neural network model, using sensors and radio frequency identification (RFID) tags for

the vehicles, applied agent-based fuzzy logic technology for controlling traffic situations which involves vehicle movements multiple approaches. Recently researchers started concentrating on revolutionizing paradigm of the Internet of Things. These led to the construction of a more convenient environment comprised of different intelligent systems in different fields like intelligence business inventories, smart metering, health care, smart home, retail, supply chain logistics, monitoring electrical equipment, smart agriculture etc

III. PROPOSED SYSTEM

The basic principle of the proposed system is the intercommunication between the traffic signals. It means a traffic signal should communicate with its neighboring traffic signals with the help of wireless mesh sensor network about the current traffic level. The traffic density can be determined by the traffic enforcement camera. Based on that information the signal should be set to green to the respective lane. In the given time the vehicles which have crossed that signal should cover a certain number of upcoming signals without stopping. And also for emergency service vehicles like ambulance, fire brigade, police etc a separate sensor is fixed which activates when the siren is on. The traffic signals will have siren detectors which sense the siren from these vehicles and makes a way for them to pass through.

A. Wireless Mesh Sensor Network

The building blocks of wireless mesh sensor network (WSN) are nodes. [3] There can be thousands of nodes which are interconnected through sensors as shown in fig 1. These networks are reliable which can withstand harsh environmental conditions.Their communication medium is either by LAN or WAN through a gateway. This gateway is act as a link between the WSN and other networks. So it enables the devices to store and processes data with more resources.

Using this concept, we can interconnect all signals using mesh topology. There will be a point-to-point connection. So each signal can communicate with its neighboring signals. These WSN are controlled by a control unit which is placed at a particular area and these are accessed by a remote administrator.

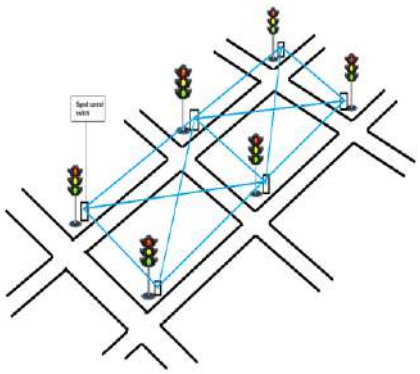


Fig 1: Interconnection of traffic signals

B. Video Analysis

Traffic enforcement camera

These cameras can be installed at the traffic signals. These cameras are of different types. It does multiple works based on its type such as traffic rule violation, speed limit crossing, traffic congestion etc. Here we require its traffic congestion analyzing property. [4]

These cams can share the data with the GPS since it is a GPS enabled device. So by capturing the current scenario, it analyses the traffic density at each lane and shares this data with GPS [5].GPS then utilizes this data to give approximate time to reach the places which are displayed on the digital direction board at the traffic signal. And also it sends the data to the control unit. Then control unit switches ON/OFF the signals for the respective lane as shown in fig2

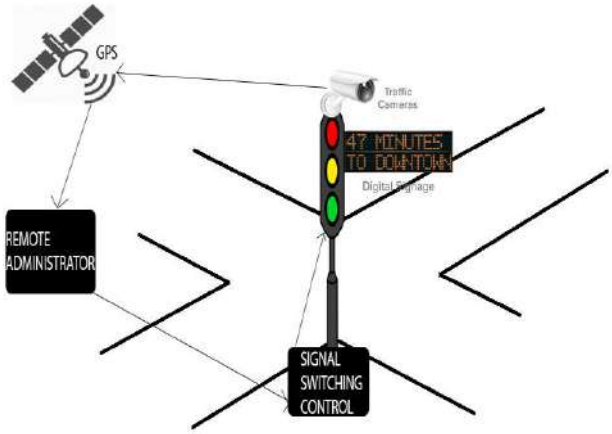


Fig 2: Traffic data Analysis

C. Control Unit

It additionally comprises of network based power switches, sensors.

Network Based Power Switches

It plays a vital role in the network administration. It provides a secure, reliable means for control of the system. It also provides services such as rebooting and power switching functions at remote network places automatically. An example for this is NPS-31F5 PDU. [6] As shown in fig 3.

When this is installed in toll booths or signal control unit, the administrators will be able to communicate with the unit via a primary network or out of band. And also it can intimate the unit to reboot or to ON/OFF the switch for troubleshooting some minor problems such as unresponsive units offline.

This helps in controlling the signals. Based on the data provided by the GPS it switches ON/OFF the respective signals. Basically it relays the traffic signal one after the other for longer roads.

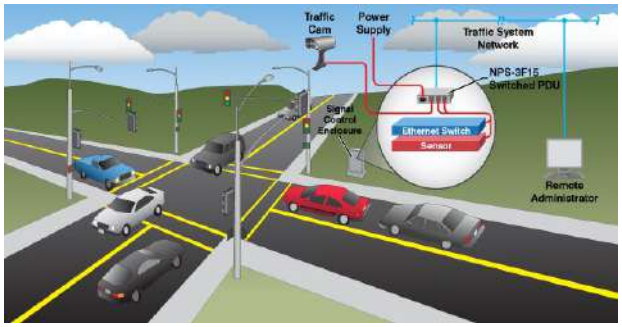


Fig 3: Control unit

The remote administrator is the main controller of the whole system.[7] The main intelligence part is the administrator. It can be referred as Data Centre. It can works manually . All traffic signal controllers are controlled by the administrator. On analyzing the data received from the GPS, it intimate the signal control unit to switch ON/OFF as shown in fig 4

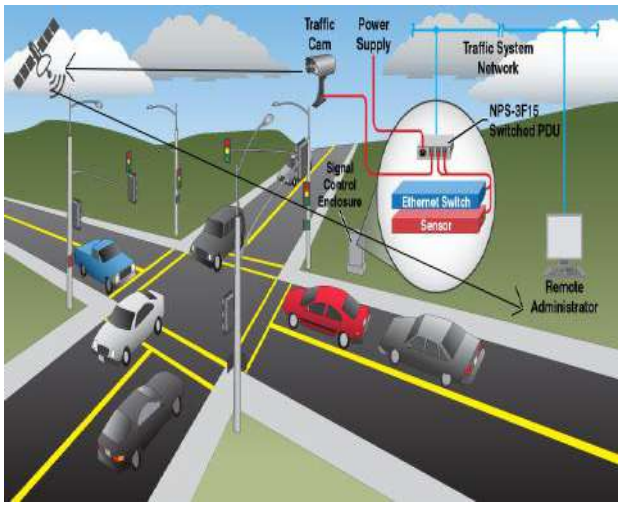


Fig 4: The overall process

CONCLUSION

This paper provides a better solution for the increased traffic congestion. From this, there will be a decrease in accidents, theft of vehicles, noise pollution, traffic rule violation etc .The real time monitoring of traffic density can be utilized in many ways such as determining the traffic density at a particular area, pollution level etc.This works more efficiently when everyone should follow the traffic rules and regulations.

ACKNOWLEDGEMENT

The author gratefully acknowledges the support of management and Dr.Balakrishna R, Principal, RajaRajeshwari College of Engineering, Bengaluru, Dr.Usha Sakthivel, Professor, Head of Computer Science Department, RRCE, Bengaluru and my teachers, family and friends for their invaluable support and encouragement.

REFERRENCES

[1]. *www.wikipedia.com*

[2]. Hasan Omar Al-Sakran, "Intelligent Traffic Information System Based on Integration of Internet of Things and Agent Technology", *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 2, 2015.*

[3].Smart IoT Technologies for Adaptive Traffic Management Using a Wireless Mesh Sensor Network posted by Advantech B+B smart worx.

[4]. Ninad Lanke and Sheetal Koul, "Smart Traffic Management System",*International Journal of Computer Applications (0975 – 8887) Volume 75– No.7, August 2013*

[5]. Dr. Khalifa A. Salim, Ibrahim Mohammed Idrees, "Design and Implementation of Web-Based GPS-GPRS Vehicle Tracking System", Khalifa A. Salim et al | IJCSET | December 2013 | Vol 3, Issue 12, 443-448

[6]. www.wti.com, "NPS-4HS15-1 Network Power Switch PDU"

[7]. www.wti.com, "Reboot Remote Network Elements in Traffic and Transportation Applications"

Digital Image Watermarking Technique for Colour Images Based On DWT-DCT-SVD

Rebecca A[1] , Dr. Usha Sakthivel [2]
[1]PG Scholar , [2] Professor,Dept.of CSE,RRCE, Bengaluru.

Abstract— This paper displays a powerful and visually impaired advanced digital image watermarking technique to accomplish copyright security. The copyright image is embedded into a cover image(colour image) by using the DWT-DCT-SVD technique then transferred to the client over the internet. Now the client will extract the watermark image. Suppose during the transfer of the watermarked image, if it is subjected to various attacks. And while extracting the watermark image, the watermark image must be less affected by the attacks when compared to the initial watermark image.

Keywords: Digital image watermarking, DWT and SVD, Key-based cryptographic, MSE and PSNR value.

I . INTRODUCTION

With a specific end goal to protect copyright material from illicit duplication, different advances have been created, similar to cryptography based strategy, computerized watermarking and so forth. In computerized watermarking, a mark or patent message is furtively implanted in the picture by abuse partner degree algorithmic system. In this endeavor to execute that calculation of computerized watermarking by consolidating DWT, DCT and SVD procedures. At first, deteriorate the first (cover) picture to 4 sub-groups abuse 2D DWT, and after that affect the SVD on every group by adjusting their solitary qualities. In the wake of applying the watermarked picture to various assaults like obscuring, including pixilation, revolution of image, rescaling, contrast conformity, gamma revision, histogram accomplishment, trimming, honing, misfortune pressure and so forth, extricate the initially embedded watermark picture from the entire the groups and think about them on the premise of their MSE and PSNR standards.

In the event that perform change in all frequencies, then it will make the watermarked picture extra invulnerable to an extensive shift of picture procedure assaults (counting basic geometric assaults), that is, it will recuperate the watermark from some of the 4 sub-groups with proficiency.

The execution of the watermarks can be assessed on the possibility of modest arrangement of properties like heartiness, devotion, and intangibility and so forth. Watermarking plans can be partitioned into 2 principle classes in venture with the implanting area: reflection and rebuild space. In the spatial space, the concealing data is installed into particular pixels of the cover picture. In change area, the cover picture be initially revamped to recurrence space and afterward concealing data is embedded into recurrence coefficients. Since, high frequencies may be lost by pressure or by scaling, the watermark sign is connected to the poorer frequencies, or superior nonetheless, connected adaptively to frequencies that enclose imperative data of the first picture.

Along these lines, in DWT based watermarking methods, the DWT coefficients are changed to watermark data. Due to contention amongst heartiness also straightforwardness, the alteration is typically take place in gonadotropin, HL and HH sub-groups for keeping up higher picture quality as HH band contains better points of interest and supply irrelevantly towards signal vitality. Thus, concealing data installing in here district won't influence the never-ending devotion of the blanket picture

Computerized watermark is an arrangement {of data of data of knowledge} containing the proprietors copyright for the sight and sound framework information. It is embedded noticeably or imperceptibly into another picture so it will be separated later as a proof of real proprietor. Utilization of computerized picture watermarking strategy has become extensively to guard the copyright ownership of advanced interactive media framework data since it is unimaginably plentiful powerless against unlawful and unapproved replication, generation and control.

II. LITERATURE SURVEY

Ingemar Cox *et al* (2009): Computerized watermarking development is Associate in Nursing edges investigation field Associate in Nursing it serves a vital half in learning security. As demonstrated by the examination of the clarity and essential characteristics of cutting edge concealing development, the structural model of modernized watermarking is given. The system includes 2 modules that a watermark putting in module and watermark disclosure and extraction module. In context of the centrality of cutting edge pictures exclusive rights security, in light of the examination of the essential automated watermarking figurings, the electronic watermarking development will be associated with the picture copyright protection. The two measuring separate roundabout capacity correction is encoded on the Windows stage by using Visual C++ program non-standard discourse. On examination results show that mechanized watermark is non-distinguishable; the watermark learning will be evacuated in spite of the chance that it's been manhandled, and the typical effect are frequently expert.

Dattatherya *et al*. (2013): Outlining negligible exertion Associate in Nursing quick check answer for electronic footage is dependably an enticing change of examination in picture making prepared. As of late in light of no matter how you look at it use of web and framework advancement,

thought of learning transport has been closed up inclination as basic unique case in everyday life. In same viewpoints challenges encased with scattering of approve information has been widened manifolds. In this paper a total up picture affirmation system has anticipated by crossbreeding of shading bar diagram and associated starting four genuine minutes to finish the objectives of littlest exertion and fast. Proposed procedure will apply for every dull and shading footage having any size and any setup. Plan makes a little acceptance code while barely lifting a finger implies that that is use to analyze the characteristics of got picture from settling reason for read [5].

Dr. M. Mohamed Sathik, S. S. Sujatha (2012): Watermarking frameworks which are fragile to intentional changes though generous to simultaneous or coincidental controls are implied as Semi-sensitive. In this paper, a semi-fragile watermarking methodology which introduces watermark signal into the host picture remembering the completion objective to approve it. The watermark is laid out so the uprightness is in contestable if the substance of the picture has not been changed and beneath some gentle taking care of on the picture. The watermark is made as a parallel case from the component of the host picture and is embedded inside the exceptional yield sub band inside the moving edge house. Top Signal to Noise greatness connection (PSNR) and Similarity extent connection (SR) are enrolled to gage picture quality. Entertainment results exhibit that this strategy still jam high picture quality once the embeddings plan and is vigorous against aground of the simultaneous picture taking care of operations though demonstrating the extortion if the picture is to a great degree prepared [7].

III TECHNOLOGIES

A. Disceret Wavelet Transform

Discrete moving edge revamp (DWT) is a scientific apparatus for progressively disintegrating a photo. It is helpful for procedure of non-stationary signs. The change is construct for the most part in light of small waves, called wavelets, of differing recurrence and confined period. Wavelet revamp gives every recurrence related reflection portrayal of a picture. Not at all like run of the mill Fourier revamp, worldly data is protected in this change technique. Wavelets are made by interpretations and enlargements of a mounted work known as mother moving edge.

This segment examinations appropriateness of DWT for picture watermarking and offers endowments of abuse DWT as against option changes. For 2Dimensional pictures, applying the DWT compares to preparing the picture by 2Dimension channels in every measurement. The channels partition the information picture into four non-covering multi-determination sub-groups LL1,LH1, HL1 and HH1. The sub-band LL1 speaks to the coarse-scale DWT coefficients even as the sub-groups LH1, HL1and HH1 speak to the fine-size of DWT coefficients.

Implanting the watermark in the more elevated amount sub groups builds the toughness of the watermark. Be that as it may, the picture visual devotion might be lost, which will be measured by PSNR. With the DWT, the edges and surface will be effortlessly known inside the high waveband .Therefore it's challenging to intensely mindful that golf stroke the watermarking signal into the gigantic plentifulness steady of high-recurrence band of the picture DWT rebuilt.

B. Discrete Cosine Transform

The discrete expense rebuild (DCT) isolates the picture into ghastly it changes a sign or picture from the deliberation space to the recurrence area. The transform (DCT) turn over the picture periphery to make the picture revised into the state of even perform. It's one of the chief regular straight changes in computerized signal procedure innovation. The 2D-DCT can not exclusively think the most information of unique picture into the tiniest low-recurrence steady, yet conjointly it will bring about the picture obstruction result being the littlest, which will comprehend the immense trade off between the information centripetal and hence the processing inconvenience. So it acquires the wide spreading application in the pressure mystery composing.

The principal the truth is that a great deal of the sign vitality is in low-frequencies sub-band that has the preeminent fundamental visual segments of the picture. The second truth is that high recurrence parts of the picture are ordinarily expelled by pressure and commotion assaults.

The watermarking picture will be unmistakable expense renovated primly. Since these DCT transform modulus contain the low recurrence data of watermarking picture, the length of these data don't lose or lost almost no then the watermarking picture might be restored well. This improves the strength and camouflage. The cover picture I is decayed through DWT revamp, then pick the acknowledge undulating modulus in the high recurrence level.

The watermarking data square measure inserting in the relating position. Transform the entire picture IDWT changed and gain the watermarked picture I′. The watermarking refining is an incredible opposite.

C. Singular Value Decomposition

The solitary worth deterioration (SVD), one of the first valuable devices of variable based math, is a factorization and guess method that viably lessens any grid into a littler invertible and framework. One extraordinary elements of SVD is that it will be performed on any genuine m×n grid. an essential utilization of Singular value Decomposition (SVD) to picture procedure is that the clarity of the picture relies on upon what number particular values square measure wont to reproduce it conjointly SVD is utilized to constrict the scale required to store a photo. Mat lab gives us the capacity to perform (SVD) on bigger grids. So Mat lab is horribly helpful to attempt to work with any size of

lattices and its offers the outcome as fast as potential. The particular quality disintegration (SVD) of m×n genuine esteemed lattice A also m nine n, performs orthogonal line and segment process on An in a manner that the resulting grid is inclining and corner to corner costs (solitary qualities) square measure composed in diminishing esteem and agree with the foundation of the Eigen estimations of ATA.

IV. DESCRIPTION AND APPROACH FOLLOWED

Security of copyright material from unlawful duplication abuse advanced watermarking by joining DWT-DCT-SVD methods for shading pictures. Computerized picture watermarking system to accomplish copyright insurance. Keeping in mind the end goal to monitor copyright material from illicit duplication, different advances have been created, similar to key-based cryptographic system, computerized watermarking and so forth. In advanced watermarking, a mark or copyright message is furtively installed into the picture by abuse Associate in nursing recipe.

On performing adjustment in all frequencies, then it will make the watermarked picture extra invulnerable to a huge shift of picture procedure assaults (counting basic geometric assaults), that is, it will recuperate the watermark data from any of the four sub-groups quickly. The DWT-SVD procedure is utilized to install watermark picture into primary or cowl picture that is solid to various very assaults.

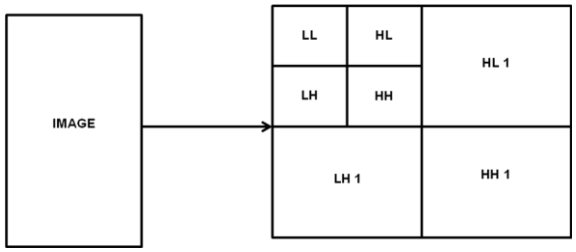


Fig 1: Two level DWT

V. Watermark Embedding

To conceal individual information into cowl picture in perceptually noticeable way is that the fundamental motivation behind anticipated paper. A scientific apparatus discrete undulating rebuild is understood this article. The wavelet of daubecheis is utilized for watermarking. Wavelet area watermarking is utilized as an aftereffect of it decreases the peril of any contortions like pressure and low pass separating that progressions the high recurrence parts of a photo anyway it can't avoid assaults that devastate the complete watermarked picture like editing. In this first we tend to take cowl picture and spoiled it into four sections i.e. low recurrence estimation, high recurrence corner to corner, low recurrence flat, low recurrence vertical segments misuse second DWT. The same strategy is connected on the watermark picture which is to be implanted into cowl picture.

In this first, apply dwt to every sub-band and watermark picture to get spoiled parts that zone unit more expanded by a chose scaling issue and region unit esteem included. It is not easy to embed the watermark specifically into cowl picture undulating coefficients; it tends to embed undulating coefficients of watermark picture into cowl picture as an aftereffect of estimate undulating coefficients contain extra information of unique watermark picture.

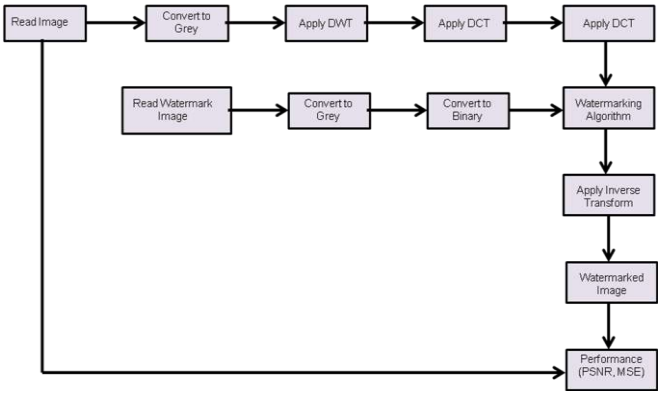


Fig 2: Watermark Embedding

VI. Watermark Extraction

In this watermarked picture and covering picture every range unit spoiled into their sub groups by applying DWT to both pictures. Presently, to utilize cowl picture to remove the watermark picture misuse non-blind watermarking. At that point alpha mixing ignite is connected to recoup the watermark picture structure watermarked picture. Here low recurrence estimate part of cowl picture is first expanded by a chose scaling issue thus subtracted from watermarked picture steady. To produce a definitive watermark separated picture, backwards discrete redesign is connected to watermark picture steady.

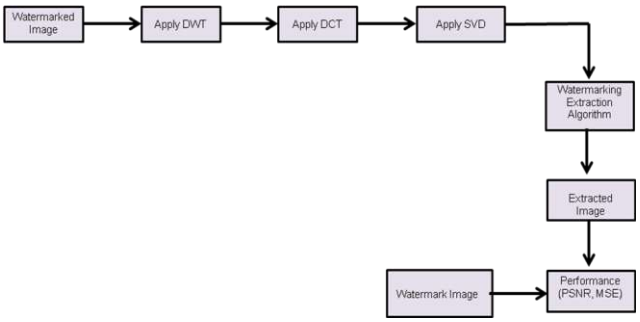


Fig 3: Watermark Extraction

VII. Experimental Results.

The executed plan depends on supplanting particular estimations of the HH band with the solitary estimations of watermark. In table I, most extreme and least particular estimations of all sub-groups of unique picture Lena are given. The wavelet coefficients are found to have biggest worth in LL band and most minimal for HH band.

Fig 4: Cover image

Fig 5: Watermark Image

Fig 6: Watermarked image

We, test the watermarking by embedding the watermark image into a cover image(colour) as shown in the above figure.The end goal is, inspite of the various image modification operations done on the watermarked image, while extracting the watermark image from the watermarked image(i.e, Embedded image) the extracted watermark image must be clear as much as it was before embedding.

Test Cases:

Firstly, we subject the watermarked image by adding a bluring effect, then extract the watermark image. Now comparing the extracted watermark image with the initial watermark image based on the PSNR and MSE values.

Now, we subject the watermarked image by adding a rotational effect(e.g, 10 degree), then extract the watermark image. Now comparing the extracted watermark image with the initial watermark image based on the PSNR and MSE values.

CONCLUSION

The realized DWT-DCT-SVD set up has incontestable an abnormal state of wholeheartedness against lion's offer of ambushes also asthuslid geometric strikes and additionally composing and totally distinctive sorts of sign gaining strength so on get ready attacks which may be acknowledged the watermark from some of the sub-band, which demonstrates that adjustment house is extra healthy than spatial space. Henceforth, the given system can be with achievement utilized for copyright security of visual information. All around, LL band is not balanced as any style of changes in it will be viably seen by human eyes. However, in DWT-DCT-SVD approach, there no such possible issue.

REFERENCES

[1].http://booksite.elsevier.com/9780123725851/casestudies/02~Chapter_1.pdf

[2] Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker. “Importance of Digital Watermarking”, Digital Watermarking and Steganography, USA: Morgan Kaufmann, 2009, ch.1, sec.1.4, pp.11-12.

[3]Dattatherya S, Venkata Chalam and Manoj Kumar Singh, “A Generalized Image Authentication based on Statistical Moments of Color Histogram," International Journal on Recent Trends in Engineering and Technology, Vol. 8, No-1, Jan. 2013.

[4]M. Mohamed Sathik and S. S. Sujatha, “Authentication of Digital Images by using a Semi-Fragile Watermarking Technique,” International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Vol. 2, issue. 11, pp. 39-44.

[5]Ramkumar M and Akansu N, “A Robust Protocol for Providing Ownership of Multimedia content”, IEEE trans on Multimedia, 2004, Vol.6, pp.469-478.

[6]Asna Furqan and Munish Kumar, “Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB”. IEEE International Conference on Computational Intelligence & Communication Technology, 2015.

[7]Navnidhi Chaturvedi and S .J. Basha, “Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR”, International Journal of Innovative Research in Science, Engineering and Technology, 2012.

[8]P. Meerwald and A Ubi, "A survey of wavelet-domain watermarking algorithms", Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III, 2000, vo1.4314, San Jose, CA, pp.SOS-SI6.

[9]Rowayda A. Sadek, “SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges”, International Journal of Advanced Computer Science and Applications, 2012.

Development of Surveillance Robot With Remote Control

T S Dhanalakshmi[1], Pooja M[2], Rohini R[3], VM.SaravanaPerumal[4]
[1,2],[3]UG Scholar, [4] Asst.Professor, Dept. of CSE ,RRCE, Bengaluru
ambekarlakshmie@gmail.com , muralipooja1@gmail.com, rohh1995@gmail.com, saran4umohan@gmail.com

Abstract: **Now a day's wireless technology is a very big technology were we are able to communicate with everyone very easily and the main concept of the wireless communication in this robot will be a data transfer from the robot side to the user side the existing system is very costly when compared to the proposed project. The proposed project can be able to detect the live environment by sensing the temperature, toxic gases, and obstacle's in front of the robot and also at the back of the robots, and also this uses a pir sensor for human detection. The human detection sensor senses the people for rescue operation. Disasters can be of two kinds- natural and human-induced. Natural disasters are not under the control of human beings. The main aim of the project is to implement a Wireless Multipurpose Robot which can be controlled Through PC or mobile phone using Zigbee interfaces and can navigate around the disaster areas to find the Humans who are in need of help.**

Keywords**: Arduino Uno Controller, PIR Sensor, IR sensor, Temperature sensor, wireless Camera, Zigbee.**

I. INTRODUCTION

The robot can be reprogrammed, and it can be Multifunctional manipulator designed and programmed to move Materials or specific modules through variable programmed motions for the Performance of a variety of tasks. Basically a robot consists of a civilian structure, such as a wheeled platform, arm, or other construction, which is Capable of sensing and monitoring with its environment. Sensors to sense the surroundings and give useful data back to the device. System to process sensory Input in the context of the current situation in order to instruct the device to perform actions in response to the situation.

The robot is designed to recognize and detect motion automatically around a robotic Environment. The design of the robot is separated into sensor, control, and planning systems. Robotic surveillance modules like camera's are built on a moving Platform of robot designed for surveillance and human tracking Tasks.

The robot can be operated in remotely monitoring "Or" automatic trips" in form of modes. It means that it can be steered remotely by a human watchman as Moving surveillance camera or it can drive autonomously along an unknown route, detecting. All Inconsistencies in the video input. Secret of Surveillance is tightly constrained areas is demanded in many military and indoor hostage rescue operations and the terrorists attacks

NEED FOR ROBOTS

Robots are used in order to do the work which an human cannot accomplish and the human needs like food and water is decreased, were these robots can be used in the place of humans by replacing them and the Robot can be used because they are faster than people at carrying out goals. This is because the robot is an mechanical equipment and the are faster when compared to human's and these advanced robots can do such operations like picking up the materials and firing in borderlines also.

The part of robotics wide when compared to the technologies were they can overcome all types of the terrains most commonly the robust always prefer in order to spying or in order to sense the surroundings of the area, for this purpose an Arduino microcontroller can be implemented but the wireless communication only on the zigbee modules were the transfer limit of the data is shortened for spying purposes.

However, this method is limited by the processing power of the computer, a problem that is addressed by robot side performing all imaging processing operations on a different monitor's, after transmitting the camera output and data. The project is either unique in the sense that it is a low-cost solution, that gives the ability to remotely control the robot with an limited range (by using the zigbee), while also offering video feedback. There is no any extra processing since everything is done far away remotely.

II. EXISTING SYSTEM

In the existing robotic system the robotics field is suffering like the rescue operations are less and there is noisy reception when compared to the proposed system etc. The proposed system will be able to solve all the below mentioned problems.

1. Home Security (Surveillance) Robot: this robotics is different from the traditional robotic system were the human cannot patrol always and the security cameras cannot move from one place to another and The existing security system have proved to be not that much effective and it could be easily fooled by the trespassers. Wherever human is employed for security purposes, there is a great risk of human life being at risk. Hence, the employment of an intelligent robot which has control of the entire area

would mi the harm caused by Intrusion/theft and strengthen the security.

2. Hazardous/Dangerous Environments: Robotics can be used hence they can Work in places where a human would be in danger. Example, robots are designed to withstand larger amounts of Heat, Radiation and Chemical Fumes, than humans could. Existing systems
   - Fire Detection Robot.
   - Bomb detection robot.
   - Obstacle avoidance robot.

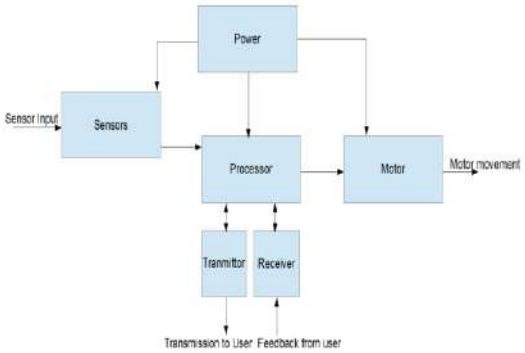
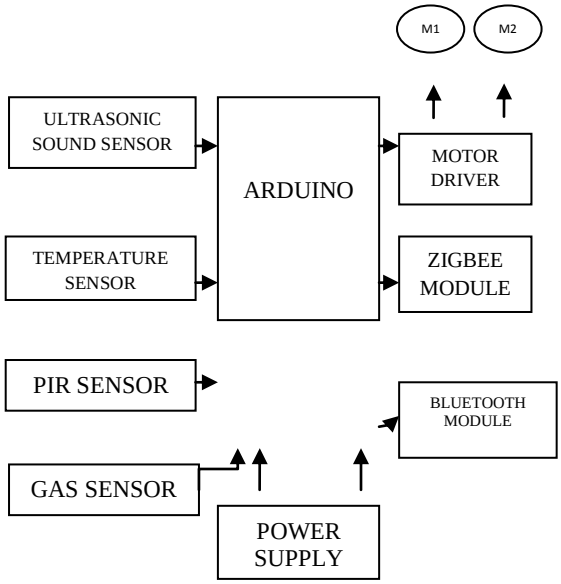


Fig 1: **Block Diagram**

III. PROPOSED ROBOTIC SYSTEM



IV. EXPLANATION OF COMPONENTS

A. Zigbee Technology

Fig 2: Zigbee

Zigbee is a specification for a suite of High level communication protocols used to create secure area networks by the AT and API commands built from small, low-power Digital radios. Zigbee is based on Standards of IEEE 805.1. Zigbee devices often transmit data over longer distances by passing Data through intermediate devices to reach large distant ones, creating a new loop network; i.e., a Network with no centralized control or high-power Transmitter/receiver able to reach all of the Networked devices.

B.SENSORS

A sensor (also called detector) is a Converter that measures a physical quantity and Converts it into a signal which can be read by an Observer or by an (today mostly electronic) Instrument.

1. PIR SENSOR

Fig 3: PIR sensor

It is passive Infrared sensor which detects the motion with the Variation of infrared Radiation. A passive infrared Sensor (PIR sensor) is an Electronic sensor that Measures infrared (IR) light radiating from objects in its field of view. They are most often used in PIR-based motion detectors.

Features
1) High reliability
2) High radiant intensity
3) Peak wavelength λ=940nm
4) 2.54mm Lead spacing
5) Low forward voltage.

2. TEMPERATURE SENSOR

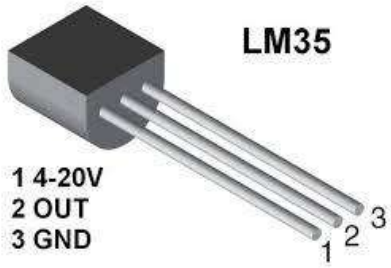


Fig 4: Temperature Sensor

There are so many kinds of sensors. Sensors Applications covers all major fields of Applications. In this paper we are controlling Temperature (physical parameters), for this purpose LM35 temperature sensor used to measure the Temperature.

3. **ULTRASONIC SOUND SENSOR**

Fig 5: Ultrasonic sound sensor

Position feedback of the robot in its physical location will be achieved using ultrasonic ping sensors. A total of 4 ping sensors will be used to ping the distance of the robot from the front, back, and side walls. The ping sensors will ping the distance of the robot and send the distance data to the microcontroller where it will be compared with expected values.

The wheels will adjust their speeds based on the data from the ping sensors. For example, if the distance from the left wall is detected to be higher than expected, the left wheel will slow down and the right wheel will speed up until the next sample. The same feedback and compensation scheme is employed for the front, back and sides.

4. **CARBON MONOXIDE SENSOR**

Fig 6: Toxic gas sensor

The figure above is a picture of the gas sensor that will be used for detection of both carbon monoxide and flammable gases. The sensor is composed of a micro AL2O3 ceramic tube, a Tin Dioxide (SnO2) sensitive layer, a measuring electrode and a heater. The housing for the sensor components is made of stainless steel. The heater provides necessary work conditions for work of sensitive components. When CO concentration in the surrounding space is changed, the sensitive Tin Dioxide layer will change in resistance. The output circuit will respond to changes in this surface resistance.

C. LITHIUM BATTERY PACK (12V LI ION BATTERIES)

:

Fig 7: Lithium battery

The power supply used to power the Motor Drive circuit above is two 12V 18650 Lithium ion battery packs. The batteries are placed in series and are connected to terminals B- and B+. B- Connects to the negative side of the battery B+ connects to the positive side of the battery. Figure n3 below shows a picture of the battery been used.

D. MOTORS

Fig 8: 12v dc motor

The Drive sizing is intended to give an idea of the type of drive motor required for your specific robot by taking known values and calculating values required when searching for a motor. The table below lists the motor characteristics. This motor has a small torque of about 20 kg-cm.

E. L293D MOTOR SHIELD

Double H driver module uses L293D dual full-bridge motor driver, an integrated monolithic circuit in a 15-lead Multi watt package. It is a high current dual full-bridge driver, high voltage designed to accept standard TTL logic levels and drive inductive loads such as DC, stepping motors and relays. Two enable inputs are provided to enable or disable the device independently of the input signals. The emitters of the lower transistor of each individual bridge are connected together and the corresponding external terminal can be used for the connection of an external sensing resistor. An additional supply input is given so that the logic works at a lower voltage.

Fig 9:L293 Motor Shield

F. CAMERA

Fig 10: Camera

The Camera is a security camera with remote viewing capability and built in video recording ability. The

camera will act as a standalone unit on the security robot and will activate upon specific alarm conditions. When an alarm condition is detected, power to the camera will be supplied the reason the camera should not be turned on at all times is because the camera has a very large current draw at 2A.

G. ARDUINO IMPLEMENTATION

Fig 11: Arduino Uno

In this system, we have used an Arduino Uno is a microcontroller board based on the ATmega328. The Arduino project provides an integrated development environment (IDE) based on Processing, and programming is done using a language based on Wiring, which is very similar to C++. The Arduino microcontroller is configured to receive serial input from the app running on the zigbee, and subsequently control four DC motors (2 fronts and 2 rears). Upon receiving the hexadecimal codes from the zigbee, the Arduino generates two control signals per DC motor. For e.g., on receiving 0x00 to indicate a forward motion, the code on the Arduino sends one HIGH and one LOW on each pair of control signals. A backward motion would involve inverting of the same, and so on. Since the Arduino cannot directly power a DC motor due to insufficient current, motor drivers, with their own power supply are used. Each motor driver is capable of controlling 2 DC motors

Fig 12: Working Robot

ADVANTAGES

1. Wireless Robot controlling.
2. Video surveillance monitoring.
3. Low power consumption.
4. Fast response.
5. Hyper terminal developing with wireless network.
6. Usage of Arduino Uno and USB camera.
7. Live video monitoring with wireless communication.
8. Usage of duplex communication of zigbee network.

DISADVANTAGES

1. Periodic monitoring of Robot with battery interfacing.
2. Interfacing of I/O devices to ARDUINO is sensitive.

APPLICATIONS

1. It's a domestic purpose robot.
2. Can be used every field like banking and where ever security is required.
3. Military purpose.
4. Traffic monitoring.
5. Home security and so on.

V. OUTCOME OF THE PROJECT

Sensors	Environment no.1	Environment no.2	Environment no.3
Uss1 sensor	300	120	13
Uss2 sensor	480	600	150
PIR sensor	HIGH	HIGH	LOW
Temperature sensor	29.5*C	32*C	30.2*C
Mq5 toxic gas sensor	59PPM	30PPM	25PPM

FUTURE SCOPE

The interest in the robot and making a active device without any external supply made us think differently and make a successful project up on surveillance robot. If the sun light can produce the charge means it can absorb the charge too. Then making a simple digital robot to charge automatically can also be done in future.

REFERENCES

1. S. Pratheepa and P. Srinivasan, Surveillance Robot for Tracking multiple targets, International Journal of

Scientific and Engineering Research, vol.2, issue 3, pp. 1-4,2011.
2. T. Hellström, "On the moral responsibility of military robots". Ethics and Information Technology, 15 (2): 99–107, 2013.
3. K. Brannen, "Army kills off MULE unmanned vehicle", Military Times, 15 August 2011.
4. Robotics.org, accessed on May 10th 2014.
5. Parallax.com
6. C. Gerald, "Mobile Robot: Navigation, Control and remote Sensing", Wiley Publisher, 2011
7. W. Budiharto, et al, "A New Obstacle Avoidance Method for Service Robots in Indoor Environments", Journal of Engineering and Technological Science, Vol. 44, No. 2, pp.148-167, 2012. DOI Number : 10.5614/itbj.eng.sci.2012.44.2.4
8. O. Khatib, , Real-time Obstacle Avoidance for Manipulator and Mobile Robots, International Journal of Robotics Research 5(1), pp.90-98, 1986.
9. E. Masehian and Y. Katebi, Robot Motion Planning in Dynamic Environments with Moving Obstacles and Target, Int. Journal of Mechanical Systems Science and Engineering, 1(1), pp. 20-25, 2007.

An investigation on diabetic skin images by different imaging modalities For diabetes diagnosis

Dr. Punal M Arabi[1], Gayatri Joshi[2],Tejaswi Bhat

[1]Professor, [2]Asst.Professor ,[3]UG Scholar ,Dept. of BME, ACSCE, Bangalore

Email: Arabi.punal@gmail.com , gayitrijoshi@gmail.com , tbhat1995@gmail.com

Abstract:Diabetic patients suffer from diseases like diabetic retinopathy, diabetic neuropathy, diabetic foot. Their quality of life is affected to a great extent. About half of all people with diabetes have some form of nerve damage. Near-infrared imaging (NIR) is a quickly developing method for the in-vivo imaging of biological tissues. Near Infrared Spectroscopy and imaging uses near infrared light between 650 and 950 nm. This paper investigates the suitability of point & shoots camera, NIR camera images for analyzing skin texture of non diabetic and diabetic images. Point &shoot and NIR images of non diabetic and diabetic are taken for analysis. GLCM (Gray level co-occurrence matrix) parameters are used to investigate the suitability of the imaging modalities namely point & shoot camera imaging and NIR imaging. The results obtained show that images taken by using NIR modality are giving better performance in analyzing the skin texture of diabetic, non diabetic sample images than compared to the point & shoot camera imaging modality.

Key words: Analysis-Skin texture-diabetic-non diabetic-Near Infrared Imager –point & shoot camera imaging-GLCM parameters.

I. INTRODUCTION

Imaging modalities and image processing play a vital role in disease diagnosis, treatment planning and monitoring. Human perception is limited to the visible spectral range that is defined by the luminous efficiency functions ranging between wavelengths of $\lambda = 380$ nm and $\lambda = 780$ nm [1]. Near infrared imaging and spectroscopy is an emerging technology concerned with monitoring the changes in the state of biological tissues using light in the range of 600 to 900 nm [2].

Andras szentkut.etal[3], provided an overview of the technological advantages, opportunities of infrared imaging. They reviewed short history of thermograph, overview on the clinical and biomedical research. Muhammad Nadeem Ashraf .etal[4] focused on the analysis of texture micro-patterns of the regions of interest (ROIs), which are suspicious regions in a fundus image, for the detection of Haemorrhages and Micro aneurysms. Carla Agurto.etal[5], presented characterization of diabetic peripheral neuropathy(DPN)subjects using an infrared imaging device and independent component analysis (ICA). Infrared video sequences are captured after cold provocation of the plantar foot. After the video frames are pre processed and registered, ICA is performed. The objective of using ICA is to separate the temporal and spatial components that may represent thermo regulatory differences in response to a cold provocation between normal controls and patients with DPN.

This paper investigates the suitability of point & shoot, NIR images for analyzing skin texture of non diabetic and diabetic images.

II. METHODOLOGY

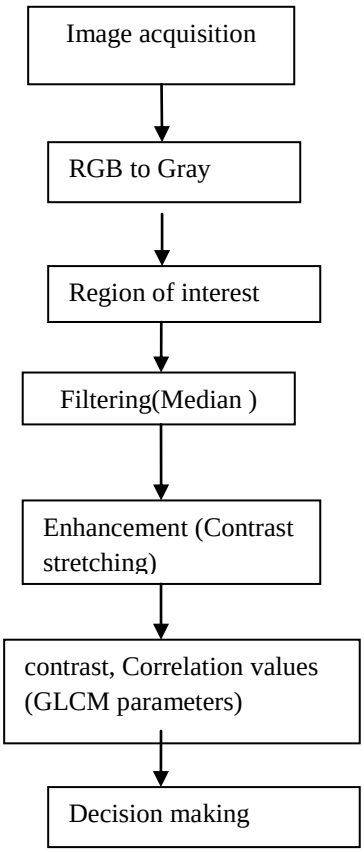


Fig1: Block diagram

The figure1 shows the flow chart of the proposed method. Images of dorsal skin of Diabetic person, non-diabetic

person are obtained using Point and shoot camera, near infrared imager are taken for investigation to find out the suitable imaging modality Point &shoot camera used here has focal length: 4.3 – 43.0 mm (35 mm equivalent: 24 – 240 mm); resolution of near infrared camera is VAG(640*480) ,CIF(320*40) and the wavelength is 0.75–1.4 µm. The images obtained are converted to gray. The region of interest (ROI) is then selected. The ROI must have at least 600 to 1200 pixels to get reliable results. Selected ROI of images are filtered using median filter, enhanced using contrast starching and GLCM parameters namely contrast correlation of the point & shoot camera images, Near Infrared images are calculated. The calculated contrast, correlation values are compared to analyze the performance of point & shoot and near infrared imaging modalities for analyzing the skin texture of non diabetic and diabetic persons to diagnose diabetes.

The formulae of GLCM Parameters are as follows:

Contrast $= \sum(i,j) = |i-j|2p(i,j)$

Where p=image, i,j=coordinates, p(i.j)=Intensity value at i,j ,

Correlation = $\sum(i,j) = \frac{(i-\mu i)(j-\mu j)p(i,j)}{\sigma_i \sigma_j}$

Where p=image, i,j=coordinates, p(i,j)=Intensity value at i,j.

Median filter:

$y(m,n)=\text{median}\{x[i,j],(i,j)\ \varepsilon\ w\}$

where w represents a neighbourhood defined by the user, centered around location [m,n] in the image

Decision rule:The average contrast value is taken as refernce. The image of interest is to be identified as a diabetic or non diabetic, if the contrast value of the image of interest is greater than the reference value then it is identified as diabetic skin. If this value is lesser than the reference value then it is identified as non diabetic skin.

III. RESULTS

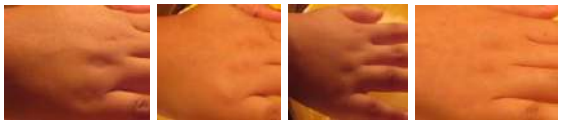


Fig 2: Non diabetic images of side and upper illumination using point & shoot camera

Fig 3: Non diabetic images of side and upper illumination using Near infrared camera

Fig 4: Diabetic images of side and upper illumination using point & shoot camera

Fig 5: Non diabetic images of side and upper illumination using Near infrared camera

Figure 2 shows the non diabetic images of side and upper illumination using point & shoot camera; figure 3 shows the non diabetic images of side and upper illumination using near infrared camera. Figure 4 shows the diabetic images of side and upper illumination using point & shoot camera; figure 5 shows the diabetic images of side and upper illumination using near infrared camera.

Table1 shows the contrast, correlation values of the non diabetic and diabetic images using point & shoot camera. Table 2 shows the contrast, correlation values of non diabetic and diabetic images using near infrared camera.

Table1: Contrast and correlation parameters for non diabetic, diabetic skin images taken by point and shoot camera.

S.NO	Illumination	Images	Non diabetic sample image		Diabetic sample image	
			Contrast	Correlation	Contrast	Correlation
1	Side illumination	Sample1	0.1185	0.9808	0.1750	0.9624
		Sample2	0.3315	0.9440	0.3415	0.9315
2	Upper illumination	Sample1	0.2130	0.9519	0.2619	0.9445
		Sample2	0.4115	0.7519	0.4644	0.6415
Average(Threshold)			0.2686			

Table 2: Contrast and correlation of NIR image for non-diabetic and diabetic

persons

S.NO	Illumination	Images	Non diabetic sample image		Diabetic sample image	
			Contrast	Correlation	Contrast	Correlation
1	Side illumination	Sample 1	0.0575	0.9930	0.0789	0.9859
		Sample 2	0.0602	0.9892	0.088	0.9819
2	Upper illumination	Sample 1	0.0860	0.9854	0.0777	0.9845
		Sample 2	0.0562	0.8532	0.0500	0.9952
Average(threshold)			0.0645			

1V. DISCUSSION

Non diabetic and diabetic dorsal skin images obtained point and shoot camera and Near Infrared imager are taken for experimentation. A region of interest is identified for each sample and GLCM parameters like contrast, correlation are calculated for this region of interest.

From table-1 it could be seen that, of the four non diabetic skin sample images (two side illumination skin sample images and two upper illumination skin sample images) two images are having higher contrast value where as other two are having lower contrast value when compared to the average value which is the threshold value here (average contrast value is 0.2686). Similarly, out of the four diabetic sample images two are having higher contrast values and other two are having lower value when compared to the threshold value. Out of these eight sample images (four diabetic and four non diabetic skin images) only 50% of the images are rightly diagnosed as diabetic or non diabetic. The decision rule says that if the image of interest has a contrast value lower than the threshold value it is non diabetic; if the contrast value of the image is greater than threshold value then it is diabetic.

From table-2 it could be seen out of the four non diabetic skin sample images (two side illumination skin sample images and two upper illumination skin sample images) three images have lower contrast value where as one image has higher contrast value when compared to the average value which is the threshold value here (the average contrast value is 0.0645).

Similarly, out of the four diabetic sample images three have lower contrast values and other one has higher value when compared to the threshold value. Out of these eight sample images (four diabetic and four non diabetic skin images) 75% of the images are rightly diagnosed as diabetic or non diabetic. By comparing the accuracy percentage of diabetic and non diabetic skin sample images taken by using point & shoot camera and Near infrared camera, the images taken by near infrared imaging modality has higher accuracy compared to the images taken by point &shoot camera imaging modality for detecting the diabetic or non-diabetic skin image.

CONCLUSION

The proposed method is tested on the non diabetic and diabetic dorsal skin sample images taken by the point and shoot camera, Near Infrared imager. Eight samples are taken from four samples are tested. The results obtained show that the accuracy of the proposed method is more for near infrared images compared with the images taken by point & shoot camera. For a number of eight images the accuracy is 75% for near infrared imaging modality where as it is 50 % for images taken by point & shoot camera imaging modality. This result shows that near infrared imaging modality is better suited than Point & shoot camera imaging modality for diabetic diagnosis by skin texture analysis. However, more number of samples are to be analysed and clinical trials are to be done to confirm the accuracy of the proposed method.

ACKNOWLEDGMENT

The authors thank the Management and Principal of ACS College of engineering, Mysore road, Bangalore for permitting and supporting us to carrying out this research work.

REFERENCES

[1] Klaus Mangold, Joseph A Shaw and Michael Vollmer," European journal of physics",vol. 34 (2013), S51–S71, doi:10.1088/0143-0807/34/6/S51

[2] Il-young son, birsen yazıc," Near infrared imaging and Spectroscopy for brain activity Monitoring", Advances in Sensing with Security Applications,Volume2 of the series NATO Security Through Science Series pp 341-372,2006.

[3]Andras szentkuti1 hana skala kavanagh2 simeon grazio," Infrared thermography and image analysis for biomedical use", PERIODICUM BIOLOGORUM UDC 57:61 VOL. 113, No 4, 385–392, 2011.

[4]Muhammad Nadeem Ashraf , Zulfiqar Habib, Muhammad Hussain." Texture Feature Analysis of Digital Fundus Images for Early Detection of Diabetic Retinopathy", 978-1-4799-5720-0/14 2014 IEEE,DOI 10.1109/CGiV.2014.293

[5]Carla agurto, simon barriga, mark burge,petersoliz."characterization of diabetic peripheral neuropathy in infrared video sequences using independent component analysis", 2015 ieee international workshop on machine learning for signal processing, Sept. 17–20, 2015.

[6]Fredembach,Clément, Barbuscia,Nathalie,Süsstrunk, Sabine," Combining visible and near-infrared images for realistic skin smoothing", Proc. IS&T;/SID 17th Color Imaging Conference (CIC)
2009.

OVERVIEW OF 5G WIRELESS TECHNOLOGIES

Hiya Choudhary[1], Manu R[2], Swetha P[3]
[1]UG Scholar, [2]UG Scholar, [3]Asst. Professor,*Dept. Of CSE,RRCE ,Bengaluru*
E-MAIL:02anu97choudhary@gmail.com ,mrmanur@gmail.com,shwetha6600@gmail.com

Abstract: 5G indicates 5th generation mobile technology .As a user becomes more aware of the mobile phones technology, he/she will seek for an appropriate package altogether, including all the advanced features a cellular phone can have. Hence, the search for new technology is always the main intention of prime cell phone giants to innovate their competitors. From generation 1G to2.5G and from 3G to 5G ,the world of telecommunication has seen a number of improvements along with improved performance with every spanning day.5G is the standard released beyond 4G in progress by standardization bodies, such as GPP, WiMAX forum or ITU-R but now it is not in use since the 4th generation is still under way. Fifth generation will throw a light on VOIP (Voice OverIP) enabled devices such that user will experience a high levels of call volume & data transmission. This paper presents the knowledge of usage of modernized technology in 5G.Once the 4G module would present its entire widespread use then the goals of 5G based telecommunication network would challenge the present 4G technology.5G technology is on the way to change the process by which most of the users Handel there headsets and is a step ahead with improved and accessible connectivity around the world.

Keywords: 5G(Fifth Generation)

I. INTRODUCTION

We have seen a lot of changes in the world of communication. Today, landlines are no more used. Apple has an ever shining remark by putting forth its latest I phone 4G that has taken the market by storm, hence shivering the entire electronic world .This forthcoming revolution of our mobile technology is the 5G that is 5th generation mobile network . With 5G technology we can connect our mobile phone to our laptop for broadband internet access.5G is going to be packed based network.5G is a packet switched wireless system with wide area coverage and high accessibility .The features of it and usability are much beyond our expectations. It is potential enough to change the meaning of cellphone usability because of its ultra-high speed. The new advanced features make it the most powerful and the highly demanded technology in future.

Fig 1: Wireless Communication System

5th generation is based on 4G technologies. This real wireless word is supported by LAS-CDMA(Large area synchronized–Code–Division Multiple access),OFDM(orthogonal frequency –division multiplexing),MCCDMA(Multi-carrier code division multiple access),UWB(Ultra-wideband),Network-LMDS(Local multipoint distribution service),and IPv6.5G technologies use CDMA and BDMA and millimeter wireless that enables the speed greater than 100Mbps at full mobility and at low mobility it would be higher than 1Gbps. It offers unrestricted call volumes, tremendous data capabilities and infinite data broadcast together within latest mobile operating system. This should be able to connect the entire world without limits with more intelligent technology over 4G.This generation are to be released around 2020.

II. EVOLUTION OF 5G

Wireless communication came into existence in early 1970's .This communication started its journey from the 1G-first generation,2G-second generation,3G-third generation, then the recently organized 4G-fourth generation which lead to the origin of 5G-the fifth generation.

A. First Generation System (1g)

The advanced mobile phone services (ANPS) technology created an environment of 1st generation in the early 1980's, during that time analog systems were widely used using the frequency modulation technique for radio transmission using frequency division multiple access (FDMA) with channel capacity of 30 KHz and frequency bandwidth of 824-894MHz.

B. Second Generation Systems (2g)

The second generation was developed in later 1990's this mobile communication system is a digital system which

is widely used in different paths of the world. It is mainly used for voice communication with a speed of 64kbps and additional services such as SMS and e-mail[2] .The second generation uses two modulation schemes; one is time division multiple access (TDMA) and the other is code division multiple [1] with the frequency band of 850-1900MHz.In 2G ,GSM technology uses 8 channels per carrier with a cross data rate of 22.8kbps in a frame of 4.6millseconds(ms) duration in the full rate channel .The other generation of this includes 2G,2.5Gand 2.75G.

C. Third Generation Systems (3g)

Third generation services combine high speed mobile access with Internet Protocol(IP) –based services which includes wireless web base access, multimedia services ,e-mail and videoconferencing. Packet switching technology is used for data transmission which operates at a range of 2100MHz and has a bandwidth of 15-20MHz used for video chatting and high speed internet services [2].The data rate of 144kbps is used in satellite and rural outdoor, 384kpbs for urban outdoor and 2Mbps in outdoor and low range outdoor [4].

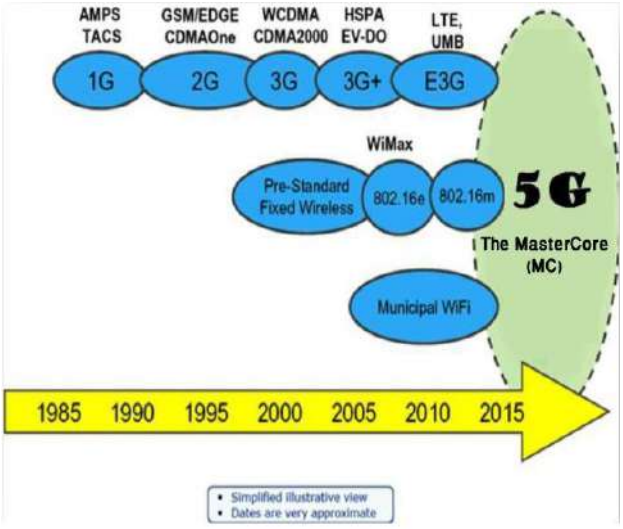


Fig 2: Evolution Of Mobile Technologies

D. Fourth Generation Systems (4g)

4G is the updated version of 2G and 3G. LTE (long term evolution) is considered as 4g technology. It offers the downloading speed of 100Mbps .A 4G system is expected to provide facilities such as voice, streamed multimedia and data will be provided to users on an "anytime, anywhere" basis and at much higher data rates compare to previous generations . It supports wireless broadband access multimedia messaging service (MMS),video chat mobile TV, HDTV content and Digital Video Broadcasting (DVB). 4G provides same features as 3G including few additional services like Multimedia news papers and sends data much faster [2].

III. 5G ARCHITECTURE

Fifth generation systems model is all IP based which fulfills increasing demands of the cellular communication markets and is a common platform for all radio access technologies[4].Terminals and network components are dynamically upgraded to new situation .AIPN(All-IP network)uses packet switching and its continuous evolution provides efficient performance and cost. The fifth generation architecture consists of a user terminal and a number of independent autonomous radio access techniques (RAT). The various IP based mobile applications and services such as Mobile portals, Mobile commerce, Mobile health care, are offered by Cloud Computing Resource(CCR) in 5G network architecture. Cloud computing allows consumers to use applications without installation and access their personal data at any computer with internet access.CCR links the reconfigurable multi technology core (RMTC) with remote configuration data from RRD attached to reconfiguration data models(RDM). RMTC is connected to different radio access technologies ranging from 2G/GERAN to 3G/UTRAN and 4G/EUTRAN in addition to 802.11x WLAN and 802.16x WMAN [4].

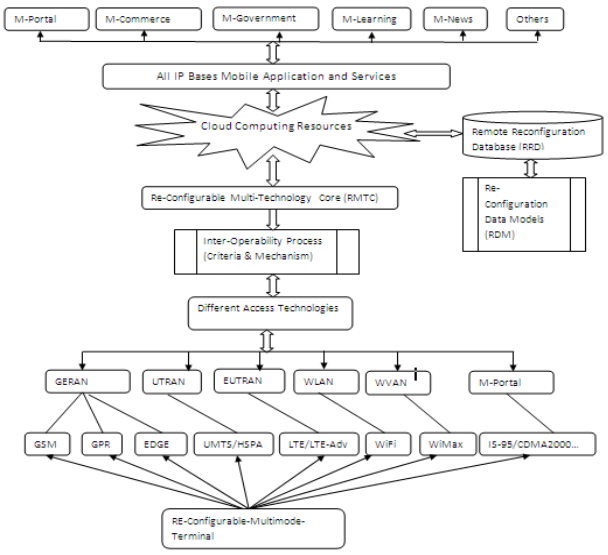


Fig 3: 5G Network Architecture

The 5G Nanocore is combinations of the following technologies .These technologies have an immense impact on existing wireless network which makes them into 5G [3].

- Nanotechnology
- Cloud computing
- All IP platforms

The following describes each in brief:

- **Nanotechnology**

Nanotechnology is the application of nano science to control process on nano meter scale between 0.1 and 100 nanometer. Nanotechnology is also referred to as molecular nanotechnology (MNT). The term nanotechnology was proposed by Nori Taniguchi in 1974 at the Tokyo international conference on production engineering. MNT is the process which controls the structure of matter based on atom-by-atom and molecule by molecule engineering. It is the next industrial revolution in the telecommunication industries which will be drastically transformed in a few years. Thus this technology has shown its effect on both mobile as well as the core network [3]

- **Cloud computing**

"Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resource that can be rapidly provisioned and released with minimal management effort or services provider interaction" .In 5G networks this central remote server cloud is a content provider. It allows consumers and business to use applications without installation [2]. The cloud computing has three main segments which are as follows:

1. Application– it is based on demands software services.

2. Platform- it refers to products that are used to deploy internet net suite, Amazon, Google, Microsoft have developed platforms that allow users to access application from centralized servers.

3. Infrastructure– It is the backbone of the entire concept. Infrastructure provides environment such as Google gears which allow users to build applications example Amazon's S3

All these above segments make the 5G nano core, to efficiently satisfy the consumer demands. This concept of cloud computing will decrease the CAPEX of 5G network deployment.

- **IP Platform**

Last but not the least. It is an evolution of the 3GPP system to meet the increase in demands of the mobile telecommunications market .The key benefits of flat IP architecture are:

1. Lower cost
2. Universal seamless access
3. Reduced system latency
4. Decoupled radio access and core network evolution.

Within a few years, more than 10 billion fixed and mobile devices through the internet are to satisfy more than one billion already connected [3].

IV. COMPARISION OF MOBILE TECHNOLOGIES

The following table describes the comparison of different mobile technologies. Their pricing scheme and how the software is delivered to the end users .

Table 1: Comparison of different technologies

ECHNOLOGY→ FEATURES↓	1G	2G	3G	4G	5G
Start/Deployment	1970-1980	1990-2004	2004-2010	At present	2020
Data band width	2kbps	64kpbs	2Mbps	1Gbps	Higher than 1Gbps
Technology	Analog cellular technology	Digital cellular technology	CDMA 2000(1xRTT,EVDO) UMTS,EDGE	WiMax LTE Wi-Fi	WWWW(to be promoted)
Services	Mobile telephony(voice)	Digital voice,SMS,higher capacity packetized data	Integrated high quality audio,video and data	Dynamic information access	Dynamic information access, wearable devices with AI capabilities
Multiplexing	FDMA	TDMA,CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit, packet	packet	All packet	All packet
Core network	PSTN	PSTN	PacketN\W	Internet	Internet

V. FEATURES OF 5G

As user point of view the major difference between current generations and expected 5G techniques must be accompanied with increased maximum. The essential features of 5G technology are as follows:

- Very high speed, high capacity and low cost per bit.

- Improved and innovative data coding and modulation techniques , which includes filter bank multicarrier way in schemes
- It supports interactive multimedia, voice, video ,internet, and other broadband services , more attractive, and have bidirectional ,accurate traffic statics , offers global access and service portability
- Lower batteries consumption and high data rates available at cell edge
- It is providing large broadcasting capacity up to gigabit which supports almost 65,000 connections at a time
- More secure; better cognitive radio/SDR security
- The uploading and downloading speed of 5G technology is very high. 5G technology offers high resolution for crazy cell phone user and bidirectional large bandwidth shaping
- Not harmful to human health
- 5G technology used remote management that user can get better and fast solution
- Cheaper traffic fees due to low infrastructure deployment cost
- Smart beam antenna systems.

This new 5G technology will provide all the possible applications by using only one universal device and interconnecting most of the already existing communication infrastructures .The 5G mobile networks will focus on the development of the user terminals where the terminal will be accessed by different wireless technologies simultaneously.

CONCLUSION

In this paper we have discussed the existing and future wireless mobile communication generation and cellular system focusing on four main contents: switching schemes, bandwidth, data rates and radio access. The 5G mobile technology will be hopefully implemented by the end of the current decade. We expect that this paper helps in organizing stronger links between people working in different fields creating future concepts of mobile communication , internet services, cloud computing , quality of services all IP network , nano technologies and the concept of master core . The upcoming 5G technology will be available in the market to fulfill user demands in affordable rates, bright and high peak as well as exceptional application.

REFERENCES

[1]"5G Wireless communications systems by Saddam Hossain, American Journal of Engineering Research(AJER) 2013 Department of Electronics and telecommunication Engineering, the peoples university of Bangladesh (PUB) in Bangladesh.

[2]"5G wireless technology" by Ganesh.R.patilet al; International Journal of computer science and Mobile computing, Vol.3 issue.10,octomber-2014,pg-203 to 207.

[3]"A Review on 5G technology" from International Journal of Engineering and Innovative Technology(IJEIT) Volume 1, Issue 1, January 2012 by SwarnaPatil ,Vipinpatil,PallviBhat.

[4]"5G Mobile technology" form internal Journal of Advanced Research in Computer Engineering and technology(IJARCET) Volume 2,Issue 2, February 2013 by Ms. Reshma .S.Sapakal, Ms. Sonali.S.Kadam.

Overview: Biological Computers

Harshitha T N[1], Devaraj K S[2], Swetha P[3]

[1,2,]UG Scholar,[3]Asst. Professor,Dept. of CSE,RRCE,Bengaluru

E-Mail:harshithatnnandeesh@gmail.com, devarajks47@gmail.com, shwetha6600@gmail.com

Abstract: Biological computers are special type of microcomputers which are mainly designed for medical applications. Bio computers work like a powerful computer but they are not robots or any spiritual beings.CPU acts as brain and DNA acts as a software of biological computers. This biological computer can be inserted into human body, by using this kind of microcomputers the doctors or surgeons can carry out the target specified operations effectively. It has its main application in genetics and forescenic science.

I. INTRODUCTION

Biological computers are a special kind of biosensors that have arrived as a interdisciplinary field which includes molecular biology, chemistry, computer science and mathematics. These are mainly used for monitoring body's activities by inducing therapeutic effects at molecular and cellular levels. This bio computing is one of the new field in research that relates to computer science and biology but not exactly fits to both, there were million possible solutions to a computational problem among those solution 'DNA Computers' gave a approximate answers at the earliest . This biological computers are flexible in nature, Flexible in the sense, they solve the problems in their own way, the only work we have to do is to direct them towards the answer with the help of neurons.This method of approach is mainly applicable for pattern recognizing tasks such as reading hand writing .The normal computers takes enormous amount of power to performthe same task. It uses system of biologically derived molecules such as DNA and Proteins to perform computational calculations involving storing, retrieving and processing data .The development of bio-computers has been made possible by the expanding new science of nano biotechnology. The term nano biotechnology can be defined in many ways .In more general form, it can be defined as a type of technology that uses both nanoscale material and biologically based materials.The term "biological computation" refers to the approach of living organisms which themselves perform computations and more over that the abstract ideas of information and computations may be key to understand biology in more confined manner. Biological computation is distinct from the field of biologically-inspired computing.

II. BIOCOMPUTING

Human uses variety of electronic devices without knowing how the devices could be working on a code which is already stored and initialize in mother board.Living organisms also carry out complex physical processes under the direction of digital data[1] .Computers and software are no exception in this constrast[2].DNA has the ability to store billions of data and hence biological computing can be done .Human genome project[3] is an effort at an international level. Themost important thing is we have tounderstand molecular genetics [4] to understand this project and to know how frequently different forms of two variable traits are inherited together i.e., not separated by recombination during meiosisGenetics[5] have used a technique called linkage analysis, there is a large difference between DNA and silicon chip[6] when the concept ' storage capacity' comes into picture i.e., single grams of DNA can store as much information as 1trillion audio CD's[7] .Since we are living in the age of computers, biological computing is slowly gaining its importance. DNA has acquired the place of CPU in the system .The cell is nothing but as computational system and the program will be stored in DNA .The 1st major step in computation is to know how state is to represented physically .There are many ways to represent for example pebbles, by triangular marks pressed into a clay tablet.

Fig 1: Biological Computers installed on human brain

III. TECHNOLOGY USED

Biological computer is implanted inside a patient's body. The information about the patient's body is called blueprint[8] by using which the biological computer would be manufactured .once the genetic blueprint is provided, by using the body's natural biological processes and the cells found in the body the human body will start to build on its own[9]. All types of cellular activity can be easily identified by using biological computer through Boolean logic equations, and we can determine its

harmfulness [10].The biological computer can also detect the cellular activities that include mutated genes and also other activities of the genes found in the cells. The biological computer works with an output and an input signal similar to conventional computers. Body's proteins, RNA and other specific chemicals that are present in the human cytoplasm [11]is the main inputs of biological computers the output can be detected by using laboratory equipment's.

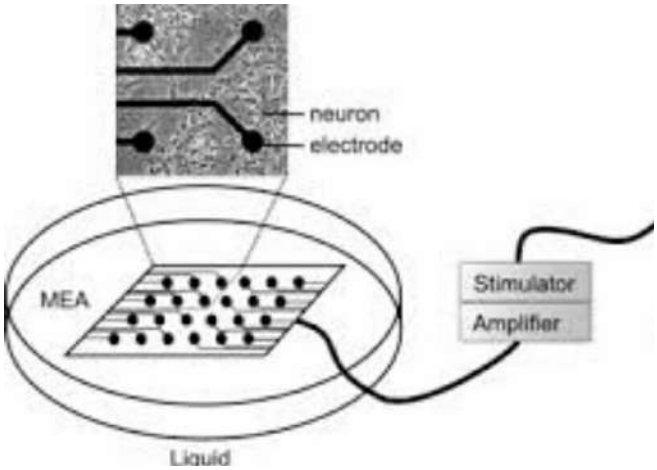


Fig 2: Technology used in Biological computers

IV. APPLICATIONS

A biological computer is a human implementable device which can be used in various medical applications [12,13]. Which requires intercellular evaluation and treatment [14]? It is mainly useful in handling intercellular activity including mutation[15-17] of genes by using biological computers. A doctor can focus on or find and treat only damaged or diseased cell and cell can be selected for the treatment.We can even produce bio fuels from cells by using bio computers made of RNA strands.

Fig 3: Biological Computers with DNA

In 2004, a group in Israel have created a device called "DNA Automation" which can detected and diagnose symptoms of cancer and guides a therapy.It senses messenger RNA and can detect the abnormal mRNA's produced by genes involved in certain types of lung and prostate cancer. In case abnormal mRNA is found an anticancer drug is released.DNA computers which can also be called as computational genes that can be integrated into the genetic material which is already present in patient's cell.

V. ETHICS

The following section describes the ethics we required to impart biological computers:

Computer taking over

- Biocomputers has capacity of solving problems with their own without the help of humans
- This can be known as takeover by a terminator type creation

Are you ready to give your life in the hands of computer?

- We can't trust the computer all the times
- Doctor illegal practises

Formation of superior race (cyborg)

- Capacity to use bio computers to enhance certain abilities
- Intelligence
- Physical abilities
- Age

These users outperform have nots who cannot purchase the technology can be used like steroids (without the side effects)

Terrorism and Government Control

- Destroys complete organ, if nanobots fail inside a body
- It has capacity to release harmful virus to computers in the internal bodies which is more harmfull
- OVER POPULATION :
- This technology has made people to live longer by creating more demand on resources
- User friendly(cheaper)
- Utilizes low power to be in its normal state
- Has got much capacity to solve toughestproblems in the issue of weeks
- Light weight
- 1 Ib of DNA has much computing capacity than all electronic computers ever made
- It processes several operations at meanwhile Efficient for parallel computing
- large amounts of working memory can be used
- A gram of DNA has capacity to hold 1*10^14Mb of data* Or 145 trillion CDs where one CD is 800Mb

VI. DISADVANTAGES

- Imperfections in molecular operations
- large amount of error involves in DNA computing
- as the amount of problems increases, probability of receiving wrong answers eventually increases, more than the probability of receiving correct answers
- there exist DNA strand errors while pairing
- electronic computers solve problems in faster way

VI. CONCLUSION

Biological computing system has a bright life in future. It is the only computing system which extracts computing power from the large collections of biological molecules. Biological computers use the immense variety of feedback loops that are characteristics of biological chemical reactions, in order to achieve computational functionality. CPU being replaced by biological molecules remains in the far future, biological computer is a massively parallel machine where processor consists of only single biological macromolecule. Some part of system can be made by biological and other parts of system made by using existing or new hardware that are available. this type of combined part application would give us the combined benefit of both the systems. Actual biological organism provides some useful insight into the statements, of the form of biological computers can't do. Biological organisms always convert macroscopic world gathered data into a form that influences molecular level biology. In order to get solution to particular problem it is better to look into a real biological system.A computational micro architecture which is based on membrane gives or justifies the name biological which is opposed to nearly molecular computing.

REFERENCES

[1]http://www.CS.virginia.edu/¬robins/Bringing_DNA_Computers_to_life.pdf.

[2] http://arxiv.org/ftp/arxiv/papers/0911.1672.pdf.

[3] ebomoyi EW(2011) Establishing Genome sequencing Centers, the Thematic units in the Devloping nations and the Potential Medical,Public health and Economics Implications. J Drug MetabolToxicol 2:108

[4] Shi Huang (2008) the Genetic EquidistantResult of Molecular Evolution In Independent of Mutation Rates.JComputSciSystBiol 1:92-102.

[5] http://www.bscs.org/pdf/computers .pdf.

[6]lien TTN,VietNX,Chikea M, Ukita Y, Takamurar Y(2011) Development of Label-Free Impedimetric HCG-Immunosensor Using Screen-Printed Electrode. J BiosenseBioelectron 2: 107.

[7]http://courses.umass.edu/physics890b-parsegia/pdf_files/kamenetskii-dna.pdf.

[8]BuchkoGW(2011) Structural Genomics-A Goldmine of blueprints for Structure –Based Drug Designe. Metabolomics 1: 104e.

[9]Ewing GW,Ewing EN(2009) Does an Improved Understanding of the Nature and Structure of Physiological Systems Lead to Better Understanding of theTherapeutic Scope of Complementary &Conventional Medicine?. J Com put SciSystBiol 2: 174-179.

[10]Sarvestani AS (2011)On the Effect of Substrate Compliance on Cellular Motility. J BiosenseBioelectron 2: 103.

[11]Shirotake S, Nakamura J, Kaneko A, Anabuki E, Shimizu N(2009) Screening Bactericidal Action of Cytoplasm Extract from KumazasaBomboo(Sasaveitchii) Leaf against Antibiotics-Resistant Pathogens such as MRSA and VRE Strains. J BioequivAvailab 1: 80-85.

[12]AljofanM,LoMK,Rota PA, Michalski WP,Mungall BA(2010) Off Label Antiviral Therapeutics for Henipaviruses: New Light Through Old Windows. J AntivirAntiretrovir 1: 1-10

[13]Mzayek F, ResnikD(2010) International Biomedical Research and Research Ethics Training in Developing Countries. J Clinic Res Bioeth 1: 103

[14]Sinnathamby G, Zerfass J, Hafner J, Block P, Nickens Z, et al. (2011) EDDR1 is a Potential Immunotherapeutic Antigen in Ovarian, Brest, and Prostate Cancer. J Clin Cell Immunol 2: 106.

[15]C Li, Luo Q, Li XM, Zhang XB, Han CL, et al.(2010) Filaggrin Mutations are Associated with Ichthyosis Vulgaris in the Southern Chinese Population. J ClinExpDermatol Res 1: 102.

[16]Tmanna A, Asad UK (2008) Identification of a Point Mutation Causing Splitting of Antigenic Domine in M1 Protein of H5n1 Strain from 2006 Outbreak in India . J Proteomics bioinform 1: 302-306.

[17]Berdeli A, Nalbantoglu S, Mir S, OzsanFM, Cam SF, et al. (2010) Novel Nonsense p. C522X Mutation in SLC5A2 Gene of a Turkish Family with Familial Renal Glocosuria: A Molecular Case Report. J CytolHistol 1: 104.

Data Analysis Software Tool for Radar Computers for Ground Based Radar

K. S Rajesh[1], Srinivasa R[2] , Sreenivasa B R[3]

[1,2]Assoc. Prof, [3]Asst.Professor CSE, RRCE, Bengaluru

E-Mail: rajeshks_hrr@yahoo.com , sirnivasa.r@rediffmail.com , br.sreenu@gmail.com

Abstract -RADAR is an active device that uses its own controlled illumination to detect the target and probe the target characteristics. The main functionality of the radar system is target tracking. In this project, first we discuss about radar, its working mechanism and its application and various scenarios i.e., building of Data Analysis Tool. Data Analysis system generates the offline error analysis report of the online logged data in radar. This tool is required to generate a detection report which states information about all possible detection of target of interest. It gives details of detection tracked successfully and the duration of the track and the reason for loss of track subsequently. It checks whether the search and track dwells were scheduled at correct time with correct parameter it is also required to carry out efficient accurate and fast completion of data analysis.

I. INTRODUCTION

Radar is acronym for Radar Detection and Ranging. Radar is an electromagnetic system for detection and location for reflecting objects. Radar can also be used to detect stationary objects buried underground. In some cases, Radar can identify as well. For example, it can identify the type of the aircraft it has detected. It operates by radiating energy into space and detecting the eco signal reflected from an object or target. The radar makes use of radio waves that are electromagnetic in nature which gets reflected when they encounter some object in their path. The time taken by the radio waves to go from the transmitter to the objects and in coming back to the receiver is recorded by Radar, which is used to determine the distance of objects from the Radar the existing system, the data retrieved for the radar is stored in various files by the logger which is later extracted by the extractor. The analysis currently done is a manual process where as automating the process would be more advantageous such as use of data analysis software tool. The activities for initiating the process were not done by menu driven method. Hence it was associated with disadvantages like time consuming, manual data handling, information loss.

In proposed system used an effective graphic user interface is designed to retrieve the files generated by the extractor which is then analyzed using Data Analysis Tool which automates the process. The analysis includes providing state information about all possible detection of target of interest, successful track detection and duration of the track. The main objectives are check whether the search and track dwell were scheduled at correct time with correct parameter and carry out efficient, accurate and fast completion of data analysis.

II. SYSTEM ARCHITECTURE

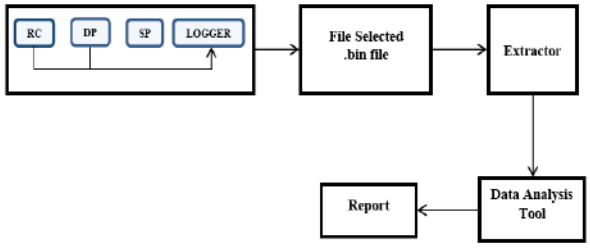


Figure1: System Architecture

Data Processing Module is an interface between the system and the radar. It mainly receives range, elevation and azimuth along with other information. These processed data is later sent to the logger.

Radar control is a method of providing air traffic control services with the use of radar and Automatic Dependent Surveillance (ADS-B). Signal Processing includes frequency filtering in the detection process. The space between each transmit pulse is divided into range cells or range gates. Each cell is filtered independently much like the process to produce the display showing different frequencies. These information are used to perform the detection process. Logger mainly receives the data from data processor and radar controller software module and transfers it into the file which is later extracted in various detailed files by extractor.

Data Extraction is the act or process of retrieving data out of (usually unstructured or poorly structured) data sources for further data processing or data storage (data migration). The import into the intermediate extracting system is thus usually followed by data analysis and possibly the addition of metadata prior to export to another stage in the data workflow.Extractor generates files which would be examined by the other modules. Analysis of data is a process of inspecting, cleaning, transforming, and modeling data with the goal of discovering useful information, suggesting conclusions, and supporting decision-making. Data generated by the

extractor is analyzed in this module in offline mode. Then tool generates the report for each of the target request made.

The user with the help of the graphic user interface searches for a desired file from apop-up dialog box. The selected input filei.e., the search data undergoes search analysis. Search analysis involves checking of dwell count misses, checking the scheduling time of each fence, error analysis and overall scheduling time. Once all the required conditions are satisfied final search report is generated. In track analysis involves checking for target re-look report, init beams report. Once all the required conditions are satisfied final track report is generated.

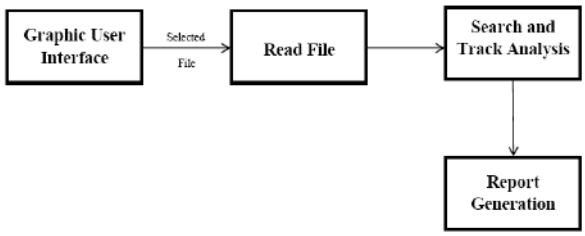


Figure 2: Data Analysis Tool

Algorithm for Search Analysis

Step 1: Start
Step 2: open file dialog to select file
Step 3:open selected file i.e., search data
Step 4: If first line verified,
Then, Read all parameters and initiates first frame time.
Else,
Report error.
Step 5: If errors in scheduling process,
If 1st fence is scheduled in 6 seconds,
If 1st fence visited twice,
If 2nd to 14th fence visited in 9 seconds,
If 2nd to 14th fence having any misses in dwell count,
Then, generate search report.
Else, Error
Step 6: Stop

In Search analysis module, data is searched for first line for the verification of correctness of data and if found correct, it is sent to the next module where all the parameters are read and first frame time is initialized. Next the data is checked for any errors in scheduling process. If yes, then error is reported to the user else, it next checks for scheduling time of fence 1 to be 6sec. Fence is usually visited twice and other fences i.e., 2nd to 14th fence are visited once during Radar rotation hence we check if the fence 1 is visited twice and also the scheduling time of 2nd to 14th fence to be 9sec. Then the tool check for misses in dwell count after which final search report is generated.

Algorithm for Track Analysis

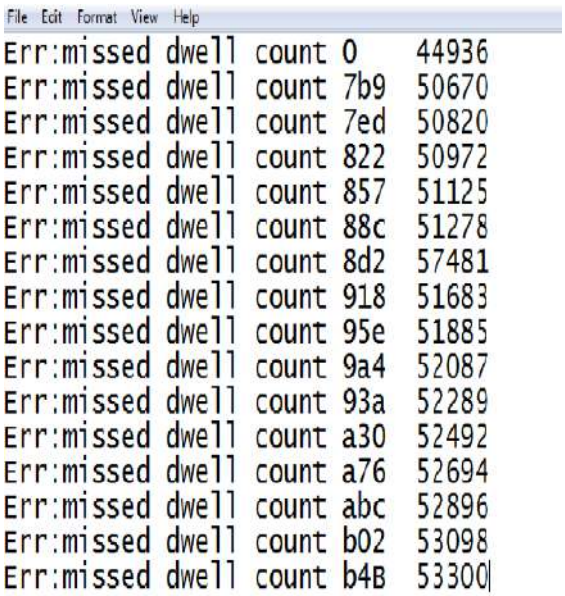
1: Start.
2: open file dialog to select file.
3: open selected file i.e., search data.
4: If target found,
Then, initiate re-look request and generate relook report.
Else if,
Null
Then, report null values.
Else,
Place 3-init beams and generate corresponding init beams report.
5: If null, Then, report null values.
Else,
Initiates track request and generates corresponding track report.
Step 6: Stop.

During track analysis, tool reads the retrieve search data and looks for the target. If target found it further initiates the re-look request else returns null values. Successful re-look request generates a corresponding re-look request which is fed as an input in placing 3-init beams for which another report is generated. These reports are later checked for null values, thereafter they are fed as an input to track request for which corresponding track report is generated.

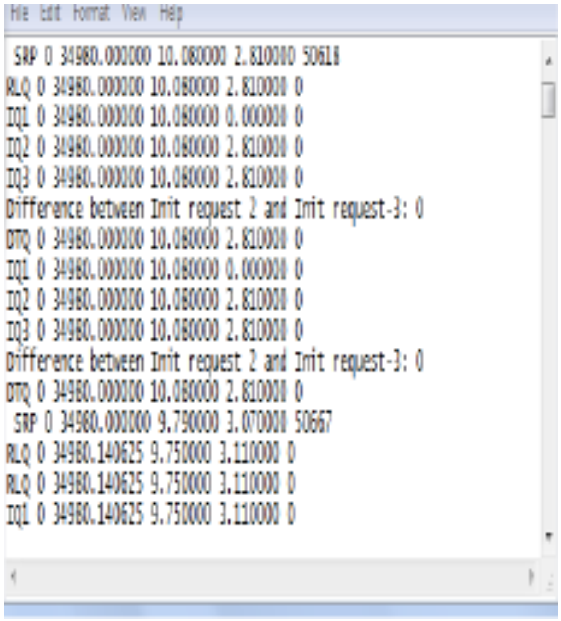
The Search and Track analysis module runs parallel and provides the user the final organized report.

III. RESULTS

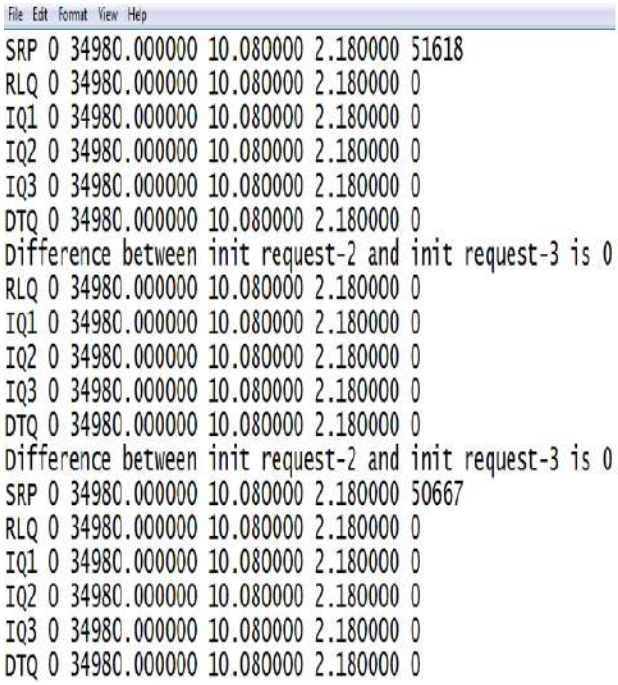
The selected input file after the user selects the desired input file for analysis of search data. Then find file that output file containing the error information about misses in dwell count and time



Selecting Track File



Computational Output



The output file for the track process containing the search request, relook request, 3 init beams delete target and difference between 2nd and 3rdinit beams of one of the target objects of different frames.

CONCLUSION

Data analysis tool generates the offline error analysis report of the online logged data in radar. This tool is required to generate detection report which states information about all possible detection of target of interest. It gives details of the detection tracked successfully and duration of the track and reason for loss of track subsequently. It checks whether the search and track were scheduled at correct time with a correct parameter. This tool is required to carry out efficient, accurate and fast completion of data analysis.

REFERENCES

[1] Merril.I.Skolnik, Introduction to Radar system,Third Edition, 2001
[2] YashvanthKanetkar, Lets us C, Third Edition, 1999
[3] Ivor Horton, Beginning with visual c++ 6,Third Edition, 2002
[4] Bruce Eckel,Thinking in C++, Second Edition,2002
[5] Ian Somerville, Software Engineering, Sixth Edition, 2004
[6]http://www.softpedia.com/get/programming/Components-Libraries/Microsoft-Visual-CRedistributable -Package.shtml
[6]http://www.softpedia.com/get/Programming/Components-Libraries/Microsoft-Visual-C- Redistributable- Package.shtml
[7] Colin Mayer, PanosTzanos, Gerry McCartorand Steven D. Thompson, Estimating Radar Azimuth Jitter ThroughAnalysisof Targets of Opportunity Data, IEEE Trans. Nov 2011

SECURE DATA AGGREGATION TECHNIQUE FOR WIRELESS SENSOR NETWORK IN THE PRESENCE OF COLLUSION ATTACK

Arpitha J[1],Varsha K[2],Naveen Gowda A K[3] , Mahantesh Matapathi[4]
UG Scholar,Asst. professor,Dept.of CSE,ACSCE,Bengaluru
E-Mail: arpitha.j14@gmail.com, varshak568@gmail.com, navidon.k143@gmail.com,manteshkrishna@gmail.com

Abstract—Sensor nodes in wireless sensor network have very limited energy resources.Using simple averaging method data aggregation from multiple sensor nodes is done by aggrgating node.But in such aggregation node are at high risk for compromising attacks.Iterative filtering algorithm hold great promise to make sure trustworthiness of data and reputation of sensor nodesmaking WSN less risk of attack.In this algorithm data are assigned weight factors that can help in simultaneous data aggregation from many sources and provide trust assessment.Here we propose enhanced iterative algorithm to address security issue.

I. INTRODUCTION

Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. This cannot be remedied by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus, better, more sophisticated algorithms are needed for data aggregation in the future WSN. Such an algorithm should have two features.

1. In the presence of stochastic errors such algorithm should produce estimates which are close to the optimal ones in information theoretic sense. However, such estimation should be achieved without supplying to the algorithm the variances of the sensors, unavailable in practice.

2. The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data, such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node.

A trustworthiness assessment at any given moment represents an aggregate of the behavior of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behavior. There are a number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation can severely impair the performance of such a system . The main target of malicious attackers is aggregation algorithms of trust and reputation systems.

Sensors deployed in hostile environments may be subject to node compromising attacks by adversaries who intend to inject false data into the system. In this context, assessing the trustworthiness of the collected data becomes a challenging task. WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms; an example is the recent emergence of multi-core and multi-processor systems in sensor nodes. Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems—data aggregation and data trustworthiness assessment—using a single iterative procedure. Such trustworthiness estimate of each sensor is based on the distance of the readings of such a sensor from the estimate of the correct values, obtained in the previous round of iteration by some form of aggregation of the readings of all sensors. Such aggregation is usually a weighted average; sensors whose readings significantly differ from such estimate are assigned less trustworthiness and consequently in the aggregation process in the present round of iteration their readings are given a lower weight. In recent years, there has been an increasing amount of literature on IF algorithms for trust and reputation systems. The performance of IF algorithms in the presence of different types of faults and simple false data injection attacks has been studied, for example in where it was applied to compressive sensing data in WSNs. In the past literature it was found that these algorithms exhibit better robustness compared to the simple averaging techniques; however, the past research did not take into account more sophisticated collusion attack scenarios. If the attackers have a high level of knowledge about the aggregation algorithm and its

parameters, they can conduct sophisticated attacks on WSNs by exploiting false data injection through a number of compromised nodes. This paper presents a new sophisticated collusion attack scenario against a number of existing IF algorithms based on the false data injection. In such an attack scenario, colluders attempt to skew the aggregate value by forcing such IF algorithms to converge to skewed values provided by one of the attackers. Although such proposed attack is applicable to a broad range of distributed systems, it is particularly dangerous once launched against WSNs for two reasons. First, trust and reputation systems play critical role in WSNs as a method of resolving a number of important problems, such as secure routing, fault tolerance, false data detection, compromised node detection, secure data aggregation, cluster head election, outlier detection, etc., .

Second, sensors which are deployed in hostile and unattended environments are highly susceptible to node compromising attacks . While offering better protection than the simple averaging, our simulation results demonstrate that indeed current IF algorithms are vulnerable to such new attack strategy. In this paper, we propose a solution for such vulnerability by providing an initial trust estimate which is based on a robust estimation of errors of individual sensors. When the nature of errors is stochastic, such errors essentially represent an approximation of the error parameters of sensor nodes in WSN such as bias and variance. However, such estimates also prove to be robust in cases when the error is not stochastic but due to coordinated malicious activities. Such initial estimation makes IF algorithms robust against described sophisticated collusion attack, and, we believe, also more robust under significantly more general circumstances; for example, it is also effective in the presence of a complete failure of some of the sensor nodes. This is in contrast with the traditional non iterative statistical sample estimation methods which are not robust against false data injection by a number of compromised nodes [18] and which can be severely skewed in the presence of a complete sensor failure. Since readings keep streaming into aggregator nodes in WSNs, and since attacks can be very dynamic (such as orchestrated attacks [4]), in order to obtain trustworthiness of nodes as well as to identify compromised nodes we apply our framework on consecutive batches of consecutive readings. Sensors are deemed compromised only relative to a particular batch; this allows our framework to handle on-off type of attacks (called orchestrated attacks in [4]). Our simulation results illustrate that our robust aggregation technique is effective in terms of robustness against our novel sophisticated attack scenario as well as efficient in terms of the computational cost. Our contributions can be summarized as follows:

1. Identification of a new sophisticated collusion attack against IF based reputation systems which reveals a severe vulnerability of IF algorithms

2. A novel method for estimation of sensors' errors which is effective in a wide range of sensor faults and not susceptible to the described attack

3.Design of an efficient and robust aggregation method inspired by the MLE, which utilises an estimate of the noise parameters obtained using contribution 2 above.

4. Enhanced IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs from contributions 2 and 3 above.

II. BACKGROUND, ASSUMPTIONS THREAT MODEL AND PROBLEM STATEMENT

In this section, we present our assumptions, discuss IF algorithms, describe a collusion attack scenario against IF algorithms, and state the problems that we address in this paper.

A. Network Model

For the sensor network topology, we consider the abstract model proposed by Wagner in [20]. Fig. 1 shows our assumption for network model in WSN. The sensor nodes are divided into disjoint clusters, and each cluster has a cluster head which acts as an aggregator. Data are periodically collected and aggregated by the aggregator. In this paper we assume that the aggregator itself is not compromised and concentrate on algorithms which make aggregation secure when the individual sensor nodes might be compromised and might be sending false data to the aggregator. We assume that each data aggregator has enough computational power to run an IF algorithm for data aggregation.

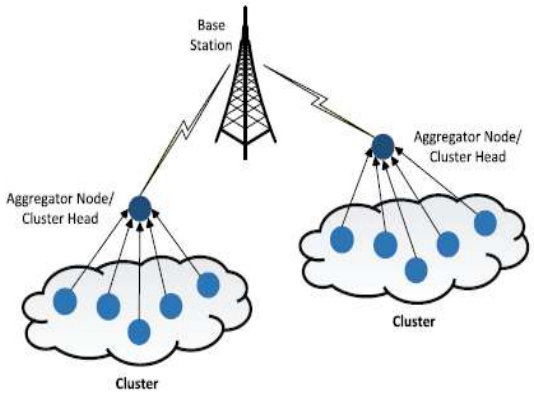


Fig.1. Network model of WSN.

B. *Iterative Filtering in Reputation Systems*

Kerchove and Van Dooren proposed in [8] an IF algorithm for computing reputation of objects and raters in a rating system. We briefly describe the algorithm in the context of data aggregation in WSN and explain the vulnerability of the algorithm for a possible collusion attack. We note that our improvement is applicable to other IF algorithms as well. We consider a WSN with n sensors Si, i = 1;..;n. We assume that the aggregator works on one block of readings at a time, each block comprising of readings at mconsecutive instants. Therefore, a block of readings is represented by a matrix X={x1,x2.....xn} where xi=[x1,x2….xm] represents the ithm -dimensional reading reported by sensor node Si. Let r=[r1 r2 ... rm]^T denote the aggregate values for instants t = 1,...m, which authors of [8] call a reputation vector,2 computed iteratively and simultaneously with a sequence of weights w=[w1,w2….wn]^T reflecting the trustworthiness of sensors. We denote by $r^{(1)}$,$w^{(1)}$ the approximations of r; w obtained at lth round of iteration (l>=0). The iterative procedure starts with giving equal credibility to all sensors, i.e., with an initial value $w^{(0)}$= 1. The value of the reputation vector $r^{(l+1)}$ in round of iteration l+1 is obtained from the weights of the sensors obtained in the round of iteration l as $r^{(l+1)} = X.w^{(l)} / w(i)$: Algorithm 1 illustrates the iterative computation of the reputation vector based on the above formulas.

ALGORITHM 1: iterative filtering algorithm.

INPUT: X,n,m

OUTPUT: The reputation vector r

l←0;

$w^{(0)}$ ←1;

REPEAT:

Compute $r^{(l+1)}$;Type equation here.

Compute d;

Compute $w^{(l+1)}$;

l←l+1;

Until reputation has converged;

C. *Adversary Model*

In this paper, we use a Byzantine attack model, where the adversary can compromise a set of sensor nodes and inject any false data through the compromised nodes . We assume that sensors are deployed in a hostile unattended environment. Consequently, some nodes can be physically compromised. We assume that when a sensor node is compromised, all the information which is inside the node becomes accessible by the adversary. Thus, we cannot rely on cryptographic methods for preventing the attacks, since the adversary may extract cryptographic keys from the compromised nodes. We assume that through the compromised sensor nodes the adversary can send false data to the aggregator with a purpose of distorting the aggregate values. We also assume that all compromised nodes can be under control of a single adversary or a colluding group of adversaries, enabling them to launch a sophisticated attack. We also consider that the adversary has enough knowledge about the aggregation algorithm and its parameters. Finally, we assume that the base station and aggregator nodes cannot be compromised in this adversary model; there is an extensive literature proposing how to deal with the problem of compromised aggregators; in this paper we limit our attention to the lower layer problem of false data

being sent to the aggregator by compromised individual sensor nodes, which has received much less attention in the existing literature.

D. *Collusion Attack Scenario*

Most of the IF algorithms employ simple assumptions about the initial values of weights for sensors. In case of our adversary model, an attacker is able to mislead the aggregation system through careful selection of reported data values. We use visualization techniques from to present our attack scenario.

Assume that 10 sensors report the values of temperature which are aggregated using the IF algorithm proposed in with the reciprocal discriminant function. We consider three possible scenarios;

In scenario 1, all sensors are reliable and the result of the IF algorithm is close to the actual value.

In scenario 2, an adversary compromises two sensor nodes, and alters the readings of these values such that the simple average of all sensor readings is skewed towards a lower value. As these two sensor nodes report a lower value, IF algorithm penalizes them and assigns to them lower weights, because their values are far from the values of other sensors. In other words, the algorithm is robust against false data injection in this scenario because the compromised nodes individually falsify the readings without any knowledge about the aggregation algorithm.

In scenario 3, an adversary employs three compromised nodes in order to launch a collusion attack. It listens to the reports of sensors in the network and instructs the two compromised sensor nodes to report values far from the true value of the measured quantity. It then computes the skewed value of the simple average of all sensor readings

and commands the third compromised sensor to report such skewed.

II. ROBUST DATA AGGREGATION

In this section, we present our robust data aggregation method.

E. Framework Overview

In order to improve the performance of IF algorithms

against the aforementioned attack scenario, we provide arobust initial estimation of the trustworthiness of sensornodes to be used in the first iteration of the IF algorithm. Most of the traditional statistical estimation methods for variance involve use of the sample mean. For this reason, proposing a robust variance estimation method in the case of skewed sample mean is an essential part of our methodology. In the remainder of this paper, we assume that the stochastic components of sensor errors are independent random variables with a Gaussian distribution; however, our experiments show that our method works quite well for other types of errors without any modification. Moreover, if error distribution of sensors is either known or estimated, our algorithms can be adapted to other distributions to achieve an optimal performance. Fig. 2 illustrates the stages of our robust aggregation framework and the interconnections. As we have mentioned,our aggregation method operates on batches of consecutive readings of sensors, proceeding in several stages.In the first stage we provide an initial estimate of two noiseparameters for sensor nodes, bias and variance.Based on such an estimation of the bias and variance ofeach sensor, the bias estimate is subtracted from sensorsreadings and in the next phase of the proposed framework, we provide an initial estimate of the reputation vector calculatedusing the MLE. In the third stage of the proposed framework, the initialreputation vector provided in the second stage is used toestimate the trustworthiness of each sensor based on thedistance of sensor readings to such initial reputation vector.

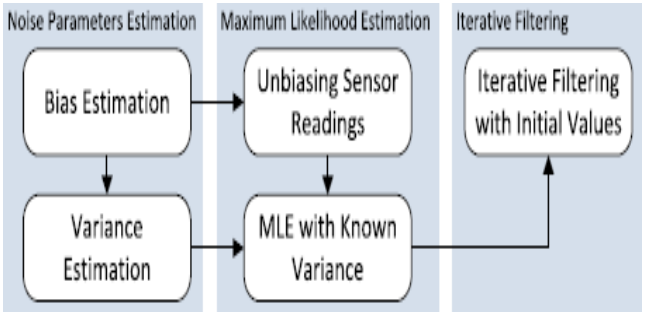


Fig.2. Our robust data aggregation framework.

F. Enhanced Iterative Filtering

According to the proposed attack scenario, the attacker exploits the vulnerability of the IF algorithms which originates from a wrong assumption about the initial trustworthiness of sensors. Our contribution to address this shortcomings is to employ the results of the proposed robust data aggregation technique as the initial reputation for these algorithms. Moreover, the initial weights for all sensor nodes can be computed based on the distance of sensors readings to such an initial reputation. Our experimental results illustrate that this idea not only consolidates the IF algorithms against the proposed attack scenario, but using this initial reputation improves the efficiency of the IF algorithms by reducing the number of iterations needed to approach a stationary point within the prescribed tolerance.

III. ACCURACY WITH COLLUSION ATTACK

In order to illustrate the robustness of the proposed dataaggregation method in the presence of sophisticated attacks, we synthetically generate several data sets by injecting the proposed collusion attacks. Therefore, we assume that the adversary employs c ($c < n$) compromised sensor nodes to launch the sophisticated attack scenario proposed in Section 2.4. The attacker uses the first c - 1 compromised nodes to generate outlier readings in order to skew the simple average of all sensor readings. The adversary then falsifies the last sensor readings by injecting the values very close tosuch skewed average. This collusion attack scenario makes the IF algorithm to converge to a wrong stationary point. In order to investigate the accuracy of the IF algorithms with this collusion attack scenario, we synthetically generate several data sets with different values for sensors variances as well as various number of compromised nodes (c). the collusion attack scenariocan circumvent all the IF algorithms . Moreover, the accuracy of the algorithms dramatically decreases byincreasing the number of compromised nodes participated in the attack scenario. As explained before, the algorithms converge to the readings of one of the compromised nodes, namely, to the readings of the node which reports values very close to the skewed mean. This demonstrates that an attacker with enough knowledge about the aggregation algorithm employed can launch a sophisticated collusion attack scenario which defeats IF aggregation systems.

IV. ACCURACY WITH SIMPLE ATTACK SCENARIO

An attack scenario against traditionalstatistical aggregation approaches. We described thescenario in Section 2.4 and the second round of Fig. 2 as asimple

attack scenario using a number of compromisednode for skewing the simple average of sensors readings. Inthis section, we investigate the behavior of IF algorithmsagainst the simple attack scenario. Note that the objective ofthis attack scenario is to skew the sample mean of sensorsreadings through reporting outlier readings by the compromisednodes.

In order to evaluate the accuracy of the IF algorithms against the simple attack scenario, we assume that the attacker compromises c(c < n) sensor nodes and reportsoutlier readings by these nodes. We generate syntheticallydata sets for this attack scenario by taking into account differentvalues of variance for sensors errors as well asemploying various number of compromised nodes. Moreover, We generate biased readings for all sensor nodes withbias provided by a random variable with a distribution$N(0, \alpha^2_b)\alpha^2_b$ with the variance of bias chosen to be α^2_b.=4

V. CONCLUSIONS

In this paper, we introduced a novel collusion attack scenario against a number of existing IF algorithms. Moreover, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging. In future work, We will investigate whether our approach can protect against compromised aggregators. we also plan to implement our approach in a deployed sensor network.

REFERENCES

[1] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," *Comput. Netw.*, vol. 53, no. 12, pp. 2022–2037, Aug. 2009.
[2] L. Wasserman, All of Statistics : A Concise Course in Statistical Inference.New York, NY, USA: Springer,.
[3] A. Jøsang and J. Golbeck, "*Challenges for robust trust and reputation systems," in Proc. 5th Int. Workshop Security Trust Manage.*,Saint Malo, France, 2009, pp. 253–262.
[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surveys, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.
[5] R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, "Trust and reputation systems for wireless sensor networks," in Security and Privacy in Mobile and Wireless Networking, S. Gritzalis, T. arygiannis, and C. Skianis, eds.,Leicester, U.K.:Troubador Publishing Ltd, 2009 pp. 105–128,.
[6] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.
[7] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN," in Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput., 2011, pp. 1–4.
[8] C. de Kerchove and P. Van Dooren, "*Iterative filtering in reputation systems*," SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.
[9] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," Europhys. Lett., vol. 94, p. 48002, 2011.
[10] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information filtering via iterative refinement," Europhys. Lett., vol. 75, pp. 1006–1012, Sep. 2006.
[11] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding information from noisy, redundant, and intentionally distorted sources," Physica A: Statist. Mech. Appl., vol. 371, pp. 732–744, Nov. 2006.
[12] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputation based ranking on bipartite rating networks," in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.

A SURVEY ON DIFFERNT SYBIL ATTACKS AND DEFENCE MECHANISMS

Nandini L N Gowda[1], Pavithra T N[2], Lakshmi Priya P[3], Kavita K Patil[4]
[1,2,3]UG Scholar, [4]Asst. Professor, Dept of CSE, ACSCE, Bengaluru
E-Mail: nandinilakshminarayan@gmail.com, pavithratngowda@gmail.com, lakshmipriya825@gmail.com, kavitakpatil@yahoo.com

Abstract: Sybil attacks are a fundamental threat to the security of distributed systems. Recently, there has been a growing interest in leveraging social networks to mitigate Sybil attacks.Sybil attacks in which an adversary forges a potentially no limits of identities are a danger to distributed systems and online social networks. The goal ofSybil defense is to accurately identify Sybil identities. Sybil defense schemes can be divided into two categories: Sybil detection and Sybil tolerance.Sybil detection schemes are application-independent , while Sybil tolerance schemes rely on application-specific information. The defense mechanism takes nodes over a social network which consists a small set of known benign nodes and a small set of known Sybilas input. Moreover, SybilBelief performs better Sybil classification mechanisms and Sybil ranking mechanisms. For instance the emerging Internet-of-Things (IOT) are vulnerableto Sybil attacks where attackers can manipulate fake identitiesor abuse pseudoidentities to compromise the effectiveness of theIOT. There are three types of Sybil attacks: SA-1, SA-2 and SA-3 according to theSybil attacker's capabilities. We then present some Sybil defenseschemes, including social graph-based Sybil detection (SGSD),behavior classification-based Sybil detection (BCSD).

I. INTRODUCTION

Sybil attacks, where a single entity emulates the behaviorof multiple users, form a fundamental threat to the securityof distributed systems[5] Examples include systems include peer-to-peernetworks, email, reputation systems, and online socialnetworks[6].Sybil accounts in online social networksare used for criminal activities such as spreading spam or malware.Stealing other users private information.Traditionally, Sybil defenses require users to present trustedidentities issued by certification authorities but this approaches violate the open nature that underlies the success of these distributed systems. Although an attacker can create arbitrary Sybil users and social connections among themselves, he or shecan only establish a limited number of social connections tobenign users. As a result, Sybil users tend to form a communitystructure among themselves, which enables a large number ofSybil users to integrate into the system.The existing structure-based approaches suffer fromone or more of the following drawbacks: They can bootstrap from either only known benign or known Sybilnodes and limiting their detection accuracy. They cannot tolerate noise in their prior knowledge aboutknown benign or Sybil nodes and they are notscalable.To overcome these drawbacks, we recast the problem offinding Sybil users as a semi-supervised learning problem,where the goal is to propagate reputations from a small setof known benign and/or Sybil users to other users alongthe social connections betweenthem. More specifically, wefirst associate a binary random variable with each user in thesystem; such random variable represents the label (i.e., benignor Sybil) of the user. Second, we model the social networkbetween users in the system as a pair wise Markov RandomField, which defines a joint probability distribution for thesebinary random variables. Third, given a set of known benignand/or Sybil users, we infer the posterior probability of a userbeing benign, which is treated as the reputation of the user. Forefficient inference of the posterior probability, we couple ourframework with Loopy Belief Propagation, an iterativealgorithm for inference on probabilistic graphical models.We extensively evaluate the influence of various factors including parameter settings in the Sybil-belief, the numberof labels, and label noises on the performance of Sybil-Belief.For instance, we find that SybilBelief is relatively robust toparameter settings, Sybil-Belief requires one label per community.In addition, we compare SybilBelief with Sybil classification and ranking approaches on realworldsocial network typologies[4]

The Sybil attacks pose a fundamentalproblem in web-based and distributed systems. In a Sybilattack, a malicious user creates multiple (Sybil) identities andtakes advantage of the combined privileges associated withthese identities to attack the system. For example, in onlineaction systems like eBay, a fraudulent user can continue touse the system by creating a new user account whenever herexisting accounts have acquired a bad reputation.

In this paper, we focus on the design of such social network-based Sybil defense schemes.

There are two categories of social network-based Sybildefense schemes. The first category, called Sybil detectionschemes, operate by detecting identities that are likely to beSybil.[10]. In contrast, the second category, called Sybiltolerance schemes, do not attempt to label identities as Sybil ornon-Sybil. Instead, they try to bound the leverage an attackercan gain by using multiple Sybil identities.[7],[9].

The emerging IOT is vulnerable to Sybil attackswhere attackers can manipulate fake identities orabuse pseudoidentities to compromise the effectiveness of thesystems. In the presence of Sybil attacks, the IOT

systems maygenerate wrong reports, and users might receive spam and losetheir privacy. The Sybil accounts not only spread spamand advertisements, but also disseminate malware and fishingwebsites to others to steal other users' private information. Inaddition, in a distributed vehicular communication system and mobile social systems, Sybil attackers generate biasedoptions with "legible" accounts. Without an effective detectionmechanism, the collective results will be easily manipulatedby the attackers. Since most Sybil attackers behave similarly tonormal users, to find out whether an account is Sybil or not isextremely difficult, which makes Sybil defense of paramountimportance in the IOT.[3]

II. SYBIL ATTACKS

Sybil attacks exist in the IOT to maliciously manipulate thesystems. There are three types of Sybil attacks.At the beginning, we present the social graph model. Supposean undirected social graph denoted as *G* with *n* honest nodes *H*and totally *m* edges. Sybil nodes are denoted as *S*. In the socialgraph, we use node to represent user, identity, or account inthe real network. The edge between every pair of two nodes isweighted by their social relationships. An attack edge *AG* isthe edge connecting an honest node and a Sybil one.

A. SA-1 Sybil Attacks

The SA-1 attackers usually build connections within theSybil community as shown in i.e., Sybil nodes tightlyconnect with other Sybil nodes. However, the SA-1's capabilityof building social connections with honest nodes isnot strong. In other words, the number of social connectionsbetween Sybil nodes and honest ones is limited, i.e., the number of SA-1 attack edges is limited.

The SA-1 attackers usually exist in sensing domain andsocial domain, i.e., OSN, voting or mobile sensingsystems. The main goal is to manipulate the overall optionor popularity. For example, in an online voting system, SA-1can illegally forge a massive number of identities to act asnormal users and submit the votes with the biased options.The final voting result might be manipulated by the SA-1attackers, since a considerable portion of votes are from the SA-1 attackers. Similarly, in mobile sensing system, SA-1can forge the false sensing data and indirectly change theaggregated data. Therefore, in some cases, the behaviors ofSybil attackers are indistinguishable from the normal users[1]

B.SA-2 Sybil Attacks

SA-2 attackers usually exist in social domain. Unlike SA-1,SA-2 is able to build the social connections not only amongSybil identities but also with the normal users. In otherOnline social networking behaviors and transition probabilities ofSybil attackers and normal users.

(a) State transitions for a Sybil user.(b) State transitions for a normal user. Words, the capability of SA-2 is strong to mimic the normaluser's social structures from the perspective of social graph.Therefore, the number of attack edges is large.The goal of SA-2 is to disseminate spam, advertisements,and malware; steal and violate user's privacy; and maliciouslymanipulate the reputation system. For example, in OSN,SA-2 can forge the profiles and friend list as normal users,but purposely spread spam, advertisements, and malwares.In addition, SA-2 could generate plenty of positive reviewcomments in a service evaluation system to exaggerate theadvantages of service, or generate many negative commentsto underestimate services. SA-2 would focuson some specific behaviors and repeat them in the highfrequency. The behaviors of SA-2 and normal onescan be modeled as a Markov chain.[1]

C.SA-3 Sybil Attacks

There are SA-3 Sybil attackers in mobile networks (i.e., mobile domain). The primary goal of SA-3 is similar to that of SA-2. However, the impact of SA-3 may be in a local area or within a short period. Due to the dynamics of mobile networks, mobile users cannot keep connections with others for the long time, or the connections are intermittent.Furthermore, the centralized authority cannot exist in mobile networks at all the time. Thus, unlike that in

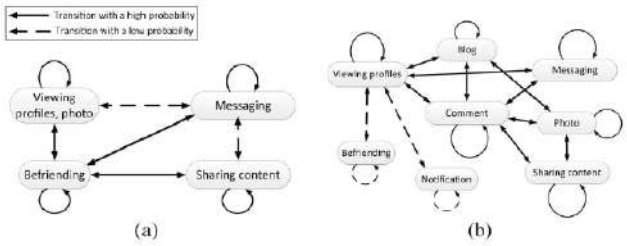


Fig 1

(a). state transition for a sybil user

(b). state transition for a normal user

Table 1: Sylabi Attack

Categories of Sybil attacks	Social graph features	Attack goal	Behavior discrimination	Mobility
SA-1	Sybils exist in the same region or community, and the number of attack edges is limited	Maliciously or purposely upload the biased reports or comments (positive or negative) to manipulate the overall option and dominate the whole system	Perform as the normal users, and repeat specific behaviors frequently	×
SA-2	Sybils may tightly connect with normal users, and generate more attack edges	Disseminate spam and malware to launch some other attacks, camouflage as normal users, or violate other users' privacy	Purposely repeat some specific behaviors in the high frequency	×
SA-3	Sybils may tightly connect with normal users	Manipulate the local popularity, disseminate spam in the mobile environment, or violate user's privacy	Repeat specific behaviors frequently	√

mobile networks at allthe time. Thus, unlike that in the online system, the socialrelationships, global social structure, topology, and historicalbehavior patterns in mobile networks are not easy to obtain forSybil defense toward SA-3. The mobility and lack of globalinformation

result in difficulties in SA-3 defense comparedwith the defense on SA-1 and SA-2.[1]

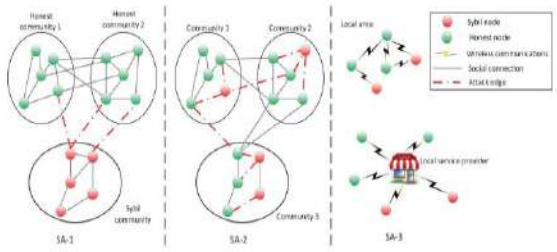


Fig 2: Three types of Sybil attacks: SA-1,SA-2,SA-3

III. SYBIL DEFENSE MECHANISMS

A. SYBIL DETECTION

Sybil detection schemes have been designed for *identity-based*social systems. Each user is intended to have a single identity,and can establish friendship links to the identities of other users they recognize in the system, thereby building a socialnetwork. Sybil detection uses this social network as a basis foridentifying users with multiple identities. We call a user withmultiple identities a *Sybil user*and each identity she uses a*Sybil identity*. The goal of Sybil detection is to label identitiesin the system as either *Sybil* or *non-Sybil*with high accuracy. The system or individualusers in the system can then take an appropriate action to handle identities labeled as Sybil. For example, they could block all detected Sybil identities from interacting with other identities in the system.[7]

1. Common assumptions and system model

Social network-based Sybil detection schemes rely on the assumption that although the attacker can create an arbitrarynumber of Sybil identities in the social network, he or shecannot establish an arbitrarily number of social connectionsto non-Sybil identities in the network. Intuitively, thisassumption is rooted in the observation that establishing newsocial links with honest users' identities takes some effort,because honest users are unlikely to accept a friend invitationfrom an identity they do not recognize.Effectively, existing social network-based Sybil detectionschemes work by analyzing the structure of the social network.To identify Sybil, all schemes make three commonassumptions:

1) The non-Sybil region of the network is densely connected(or fast-mixing)meaning random walks inthe non-Sybil region quickly reach a stationary distribution.

2) Although an attacker can create an arbitrary number ofSybil identities in social network, she cannot establishan arbitrary number of social connections to non-Sybilidentities, i.e., the attacker cannot easily infiltrate thedensely connected non-Sybil network.

3) The system is given the identity of at least one trustednon-Sybil.

These three assumptions, together, form the basis of Sybildetection. Since the non-Sybil region of the network is denselyconnected (assumption 1), and the Sybil region of the network is attached by a limited number of links (assumption 2), existing detection schemes look for resulting topological featuresto partition the network into Sybil and non-Sybil regions (seeFigure 1). They then look for the partition that contains the known non-Sybil identity (assumption 3) to decide which is the non-Sybil region.[7]

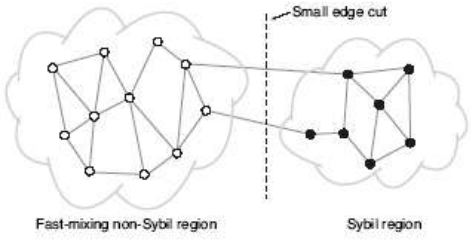


Fig 3

2. Example systems

We now give a brief overview of existing social network-based Sybil detection systems. Our goal here is to illustrate that while the precise algorithms used vary greatly between these systems, they all rely on analyzing the network structure to identify Sybil identities.

SybilGuard and SybilLimit are among the first Sybil detection schemes to be proposed. SybilGuard uses the intersections between modified random walks to determine whether identities should be accepted. SybilLimit improves on SybilGuard's bound by using multiple walks, accepting fewerSybil identities per attack edge. Both of these schemes can be implemented in a centralized or decentralized fashion.

SybilInfer is a centralized protocol that assumes full knowledge of the social graph. It uses a Bayesian inference technique to assign a probability of being Sybil to each identity. Unlike SybilGuard and SybilLimit, Sybil Infer does not provide any analytical bounds on the number of Sybil identities accepted per attack edge.

GateKeeperis a decentralized Sybil detection protocol that improves over the guarantees provided by SybilLimit. It uses avariant of the ticket distribution algorithm used in SumUpfrom multiple random identities in the graph to detect Sybil.

MobID is a Sybil detection system proposed for mobilesettings. MobID defends against Sybil attacks on in-rangeportable devices using two social networks: a network

offriends and a network of foes (or suspicious devices). MobIDuses network centrality measures to analyze the social networkstructure and flag identities as Sybil or non-Sybil.

Wh-anau is a DHT routing protocol built in conjunctionwith a Sybil identity detection scheme. Wh¯anau only selectsnodes for routing if they meet certain random walk intersectioncriteria over a social network.[7]

B.SYBIL TOLERANCE

We now examine Sybil tolerance approaches, which alsodefend against Sybil attacks, but do so without attemptingto explicitly label identities as Sybil or non-Sybil. A numberof schemes exist for different applications we briefly discuss three of them.

Ostralimits unwanted communication (or spam) sent byusers who create Sybil accounts. Ostra uses a social network,with credit values assigned to links. When a message is sent,Ostra finds a path with available credit from the sender to thereceiver. If no such path is found, the message is blocked. If apath is found, credit is transferred from each user to the nextalong the path.

Bazaar protects buyers and sellers in online marketplaceslike eBay by limiting the reputation manipulation that ispossible through the creation of Sybil accounts. It uses maxflow-based techniques to estimate the reputation of usersinvolved in a transaction and flags fraudulent transactions.

Sum Upsecures online voting against users who createSybil accounts and vote multiple times. SumUp chooses a votecollector in the network and distributes tokens (or credits) onthe links in the network inside a voting envelope. Voters mustfind a path to the vote collector with available credit in order to cast a vote.We now demonstrate that this class of schemes, whichwe refer to as *Sybil tolerance*, shares a common underlyingapproach.

We now demonstrate that this class of schemes, which we refer to as *Sybil tolerance*, shares a common underlying approach.[7]

A. Common assumptions, model, and goals

Similar to the model of Sybil detection described in the previous section, each of these schemes is designed to be appliedto an existing identity-based system (e.g., a communicationsystem, an online marketplace, or a content-rating system) andassumes the existence of a network connecting the identities.This network may be derived from an external social network(in the case of Ostra and SumUp), or built internally bythe system itself (in the case of Bazaar). The schemes makeno assumptions about the cost of creating identities, but doassume that an attacker cannot establish an arbitrary number oflinks to non-Sybil identities (assumption 2 from Section A).Tolerance schemes rely on assumptions about the structureof the network as well as the workload the system experiences.In particular, they assume that users perform pair wise transactions (e.g., sending a message, purchasing an item, casting a vote). They achieve a defense against Sybil by assigning *credits* to the network links, and then allowing actions only if *paths with sufficient credit* exist between the source and destination of an action. In Ostra, a message can only sent if a path with at least one credit exists between the source and destination; in Bazaar, a item can only be purchased if a path with the item's price in credits exists between the buyer and seller; in SumUp, a user can only vote if a path with at least one credit exists between the voter and vote collector.The goal of Sybil tolerance, then, is to ensure that the number of transactions that a (human) user can initiate is independent of the number of identities she possesses. Doing so would remove the creation of multiple accounts as an attack vector, thereby making the application tolerant of Sybil. In comparison to Sybil detection—where the system reasons about guarantees concerning the ability to identify Sybil identities—Sybil tolerance schemes reason about the impact (in terms of transactions) that identities have on oneanother. As a result, a certain pair of identities may be allowed to participate in certain transactions and not others, and may be allowed to interact at certain times and not others, depending on the state of the system.[7]

B. Understanding credit network-based Sybil tolerance

In this section, we describe how existing Sybil tolerance schemes are implemented using *credit networks*. We first provide some background on credit networks and discuss the Sybil tolerant nature of credit networks.

1) Credit networks: Credit networks werefirst introduced in electronic commerce to build transitive trustprotocols in an environment where there are only pairwise trustaccounts and no central trusted entities. In a credit network,identities (nodes) trust each other by offering pairwise credit(links) up to a certain limit. Nodes can use the credit to payfor services they receive from each other. The credit network can be used for payments between nodes that do not directly extend credit to each other. For this purpose, nodescan route credit to a node via network paths that traverse over links with available credit. (See Figures 4 and 5.) Formally, a *credit network* is a directed graph G = (V,E) where V is the set of nodes and E is the set of labeled edges. Each directed edge (a, b) 2 E is labeled with a dynamic scalar value cab, called the *credit available*, and is initialized to Cab. Intuitively, Cab represents the initial credit allocation that b gives to a, and cab represents the amount of unconsumed credit that b has extended to a. Note that cab _ 0 at all times. Transactions between two nodes in a credit network are contingent upon the availability of credit along network paths connecting the nodes. If a node a wishes to obtain a favor or resource from b, then a path

a u_1 ... u_n b

(which could just be a b) must exist where credits are available on each (i, j) link (i.e., $c_{ij} > 0$). If so, the credit available on each directed edge c_{ij} on the path from a to b is decreased and the credit available on each directed edge Cji on the reverse path is increased. As a result of this action, each node "pays" credits to its successor on the path to b, in exchange for the favor or service a obtains from b.[7]

Fig 4

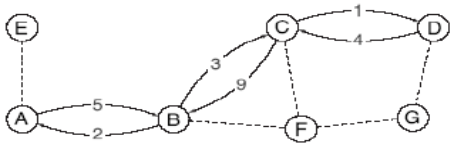


Fig 5

2) Credit networks from social networks:

One can build a credit network from a social network as follows: For each identity in the social network, we generate a node in the credit network. For each edge between a pair of identities in the social network, we generate an edge in the credit network between nodes corresponding to the users. Undirected edges in the social network (e.g., Facebook friend links) are replaced by two directed edges, one in each direction, between the nodes adjacent to the edges. Because social networks are known to be richly connected credit networks inherit the rich connectivity they require for liquidity. Further, each directed edge, (a, b), is assigned an initial credit allocation C_{ab} by the destination node b. The system must exercise care when assigning credit allocations. For instance, when a new social link is created, the requesting node should be required to grant the accepting node some initial credit but not vice-versa, to prevent an attacker from obtaining credit by initiating social links.[7]

3) Sybil tolerant nature of credit networks:

Next, we show that credit networks built from social networks are naturally tolerant to Sybil attacks. Specifically, we argue that a Sybil attacker cannot increase the credit available to her from the rest of the network. An attacker can mount a Sybil attack by creating many different identities in the social network, each corresponding to a different node in the credit network. However, per our assumptions about credit assignment to links, having many user accounts does not by itself allow the attacker to obtain additional available credit with other users (though she can create an arbitrary number of links with arbitrary credit between her Sybil identities). As shown in Figure 6, the total amount of credit available to a single user is the sum of the credit available on her links to other (human) users. An attacker with an arbitrary number of Sybil identities has exactly the same available credit as the attacker with just one identity; in this case, the relevant set of edges is the cut between the sub graph consisting of the attacker's Sybil identities and the rest of the network. Any credit available on edges between the attacker's Sybil identities does not matter, because it does not enable additional "purchases" from legitimate nodes. Thus, available credit in a credit network is resilient to Sybil attacks.[7].

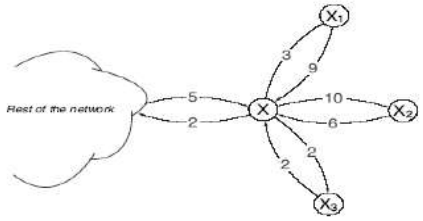


Fig 6

IV. DETECTION VS. TOLERANCE

Having examined the design offered by social network-based Sybil detection and tolerance schemes separately, we now compare them from the perspective of an operator wishing to deploy these schemes to defend her system from Sybil attacks. Conceptually, Sybil detection schemes offer a simple model that is easy to integrate with any application. For instance, the

system can simply deactivate identities that are classified as likely Sybil and allow all activity from identities classified as non-Sybil. However, this simplicity and ease of applicationcomes at a high cost for mis-classifying an identity as Sybil or non-Sybil. An innocent user who is misclassified (false positive) is denied all service, while a misclassified attacker identity (false negative) is not limited in its malicious activity. Furthermore, existing Sybil detection schemes rely solely on the network structure to identify non-Sybil and Sybil identities, ignoring other relevant information about the activity of identities. To achieve accuracy, Sybil detection requires the underlying social network to satisfy certain constraints, such as the absence of small cuts within the non-Sybil region (i.e., non-Sybil region should be fast-mixing). Unfortunately, there is mounting evidence that many real-world social networks fail to meet these requirements,either because a significant fraction of their nodes are sparsely connected or their users organize themselves into small tightly-knit communities that are sparsely interconnected. When applied to such networks, Sybil detection schemes suffer from a high rate of misclassified identities. Credit network-based Sybil tolerance schemes, on the other hand, allow or deny individual transactions among users based on the prevailing system state. This state reflects the history of transactions among users as well as the social graph structure. Thus, Sybil tolerance schemes are deeply embedded in the

operation of the system and have to be tailored for each application; they are limited to applications for which an appropriate mechanism is known that lends Sybil tolerance to the relevant system properties. Sybil tolerance schemes leverage both social network structure and the transaction history, which enables high classification accuracy. Moreover, they allow or deny individual transactions, which leads to a graceful degradation in the presence of false positives or false negatives. It is highly unlikely that all of a legitimate identity's transactions would be blocked due to false positives, or that all of a Sybil identity's transactions would be allowed due to falsenegatives. To illustrate these points, consider applying Sybil detection and tolerance schemes to the problem of email spam. Sybil detection schemes would generate a blacklist and whitelist of Sybiland non-Sybil identities. Any sparsely connected nodes in the fringes of the social network would be blacklisted, while any whitelisted attacker node can send unlimited spam. Sybil tolerance, on the other hand, bounds the rate of spam messagesthat legitimate users receive from spammers. Sparselyconnected legitimate nodes at the fringe of the social networkwould at worst be limited in the rate at which they can sendlegitimate messages. Simultaneously, no user has the abilityto send an unlimited number of spam messages.[7]

CONCLUSION

In this paper, we have provided a survey of Sybil attacks and their defense schemes. Specifically, we have defined three types of Sybil attacks in the distributed IOT and presented some Sybil defense schemes with the comparison. We consider the two defense mechanisms, namely, Sybil detection and Sybil tolerance. Sybil detectionis conceptually simple, application-independent, and easy toapply. However, it relies on strong assumptions about thesocial graph structure.

Sybil tolerance, on the other hand, allows or denies individual transactions between users, which enables its performance to degrade gracefully in the presence of false positives or negatives. Tolerance schemes can potentially achieve higher accuracy because they consider the pattern and history of user transactions, in addition to the social graph structure, as the basis for allowing transactions. However, Sybil tolerance schemes require application-specific mechanisms that distinguish attack activity from legitimate activity, without making the system vulnerable to denial-of-service attacks.

REFERENCES

[**1**]A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management ofresource constrained devices in the Internet of Things," *IEEE Commun.Mag.*, vol. 50, no. 12, pp. 144–149, Dec. 2012.

[**2**]K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authenticationin wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 6,no. 11, pp. 4136–4144, Nov. 2007.

[**3**]Kuan Zhang, *Student Member, IEEE*, Xiaohui Liang, *Member, IEEE*,Rongxing Lu, *Member, IEEE*, and XueminShen, *Fellow, IEEE*, Sybil Attacks and Their Defensesin the Internet of Things.

[**4**]Neil Zhenqiang Gong, *Student Member, IEEE*, Mario Frank, and Prateek Mittal, *Member, IEEE*SybilBelief: A Semi-Supervised Learning Approachfor Structure-Based Sybil Detection

[**5**]J. R. Douceur, "The Sybil attack," in *Proc. 1st Int. Workshop Peer-to-Peer Syst.*, 2002.

[**6**](2012, Aug.). *Malicious/Fake Accounts in Facebook* [Online]. Available: http://www.cnn.com/2012/08/02/tech/social-media/facebookfake-accounts/index.html

[**7**]BimalViswanath,MainackMondal, Allen Clement_, Peter Druschel, Krishna P. Gummadi, Alan Mislove, and AnsleyPostMax Planck Institute for Software Systems (MPI-SWS)Kaiserslautern and Saarbruecken, Germany College of Computer and Information Science, Northeastern University Boston, MA, USA, "Exploring the design space ofsocial network-based Sybil defenses".

[**9**]N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-Resilient OnlineContent Voting," in *NSDI*, 2009.

[**10**]H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "SybilGuard:Defending Against Sybil Attacks via Social Networks," in *SIGCOMM*,2006.

Automatic Railway Gate Controller by using Microcontroller

Hanuveenakirutiga P[1], Hariom mishra[2], Avinash verma[3], Nandini G[4]
[1,2,3]UG Scholar, [4]Asst. Professor ,Dept. Of CSE,RRCE,Bengaluru
E-mail:hanusiva10@gmail.com, hariommishra165@gmail.com,avinashverma165@gmail.com, nanduamma@gmail.com

Abstract: The aim of this paper is to construct an automatic railway gate controller by replacing the gates operated manually by gatekeeper in the level crossing by using the 89C51microcontroller. There many railway accidents are happening due to the manual operation of railway gate. By using this concept major disasters in railway track can be prevented and human lives can be saved. This can also save the road users by preventing the accidents occurring due to train speed at level crossing. This concept is divided into two divisions. The first division is the hardware development and in this microcontroller acts as a main unit of the system. The second division is the software programming which operates the hardware structure of the system.

Keywords-Automatic railway gate controller, Level crossing, 89C51Microcontroller.

I. INTRODUCTION

The rail route is one of the major and an important mode of transport. Even though it is an important transportation, the accidents which occurs are more dangerous compared to other mode of transport. This system is safe for both rail route users and road route users. This system reduces the accidents and increases the safety for both rail and road users. The accident occurs due the mistakes made by gate keepers and the road users. This system has two main purpose, the first thing is to provide safety for the users by reducing accidents and the second thing is to reduce the time for which gate has to be opened or closed manually by gate keepers. In this system we use microcontroller which performs complete operation of this railway gate controller. The operations which are performed by microcontroller are warning alarms, light indicators, opening and closing gates, sensing. The sensors are used in this system which is placed at a certain distance from the gate and detects

The distance of the approaching train and controls the operation of gate. This signal activates the microcontroller to operate the operations such alarms, lights, gates. The sensors should be fixed at 1000 meters on both sides of the Gate. The two sides of the gates are the fore side and the after side. Thefore side sensors are towards the train coming to the gate and the aft side sensors are after the train crosses the gate. At the time train crosses the fore side sensor it gives the signal to the gate receiver and by which the gate is closed. The alarm is activated to clear the gate area for driver about some few seconds. The gate motor is switched on in fore side sensors and the gate is closed .It remains closed till the gate reaches the aft side sensors and when aft side receiver gets activated the motor switched in opposite direction and the gate opens which stops the motor. The alarm is used as a caution measure for the rail and road users.

II. HARDWARE IMPLEMENTATION

The materials and components that are to be used in programmed railway door control system will be discussed in the chasing. As with normal control design, system can be approximately divided as suggestions, final result and processing areas. The key pieces of system are:

1. Microcontroller:

89C51 microcontroller can be used as a main control unit to control the process of the full system.

2. Railway Receptors:

They are really put at two sides of gate. You can use it to sense the arrival and departure of the teach.

3. Engine new driver:

The H-Bridge uses the four diffusion motor driver rounds that are being used to turn forward or invert course of DC motor unit for opening and final the gate.

4. CRISTAL LIQUID Screen:

It displays the train gate open or close section and alert concept for motorists.

5. Buzzer and light indication:

That they are being used to warn the road user about the approach of train by Power Supply.

III. OVERVIEW OF THE SYSTEM

This figure shows over all block diagrams for train gate control system by using microcontroller. Therefore, one 89C51microcontroller is employed to operate the following function of the railway gate control system:

- To sense the arrival and leaving of the train.
- To open and close the railway gate automatically by using two power motor.
- Buzzer and lightweight signal for caution the street users.

Screen the status of the railway gate system with LCD (Liquid Crystal Display) modules

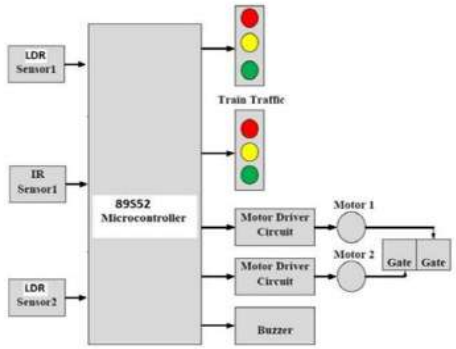


Fig 1: Block Diagram Description

A motor unit driver circuit is employed to drive the gatemotor unit for buying and selling gate. This kind of system usesbuzzer and light signal for alert the road users. The PIC (Peripheral Interface Controller) microcontroller controls all machine. Themain program of the railway gateway control system iswritten in 89C51 microcontroller and which iscreated by PIC Basic Expert Programming Language.

A. Initial Signal Display

Indicators SG1, SG2, SG3 and SG4 are located nearby the gate each at a particulardistance. SG1 and SG4 are put at 2Km on either aspect of the gate although SG2 andSG3 are put at 180m from the gate. The people may be approaching the gate in either path. So all four alerts are made CRIMSON in the beginning to indicate that door is openand vehicles are passing through the gate.The road customer signals are created GREEN so that they can readily undertakethe gate buzzer is done 'OFF' since there is no approach of train and road users need not be cautioned.

B. Train Arrival Detection

Discovery of a train drawing nearer the entryway can be detected by method for sensorsR1, R2, R3 and R4 set on either side of the door. In a specific course of methodology, R1 is utilized to sense the entry while R3 faculties the flight of train. Similarly, R4 faculties the methodology and R2 the take off individually in the other bearing of train landing. In light of the vibration of the track as the train approaches the sensor works. The sensor contains an IR (Infrared) transmitter, IR collector, a comparator and a transistor switch. IR transmitter gives IR beams whose wavelength relies on the vibration of track that compares to the info recurrence. In the event that recurrence builds its wavelength increments and hence decreases the resistance of the IR beneficiary. It lessens voltage drop over the recipient. Its yield voltage is the contrast between this voltage drop and info voltage to the sensor. This is nourished to the comparator whose reference voltage depends on the edge recurrence which is least recurrence brought about by a moderate train. In this manner, the comparator produces - 12V immersion when it detects a train and +12V if not. Correspondingly, a transistor switch produces +5V and 0V individually. This is transmitted utilizing FM (Frequency modulator) to the microcontroller.

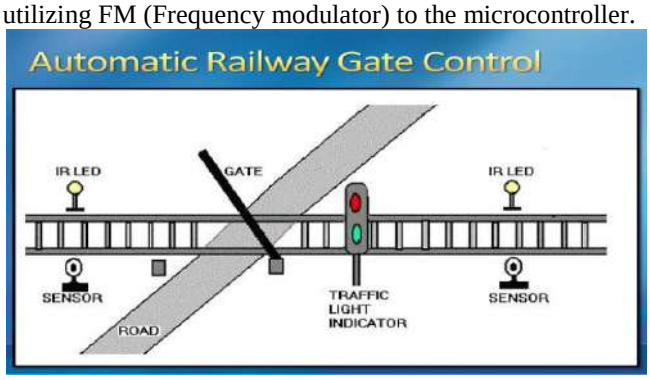


Fig 2: Proposed model

C. Warning for road user

Right now the train entry is detected on either side of the entryway, street clients are cautioned about the train approach by RED signs set to alert the street clients going through the door. RED sign shows up for the street client once the train cuts the transfer sensor set 5Km preceding the entryway. A ringer is made ON as a prudent step for the street client and that no one ought to enter the door right then and there.

D. Detecting for road Vehicles

Laser light can be utilized as a source and LDR (Light Dependent Resistors) as an instrument for acknowledging reason. At the point when light strokes on LDR its measure of resistance reductions and when light does not strike LDR its resistance stays at ordinary quality. This change of resistance of LDR can be utilized for detecting by the miniaturized scale controller 89C51 by the utilization of remuneration. At the point when there is no vehicle in the middle of or underneath the entryways, then the laser light from the source falls on the LDR on the grounds that there is no snag. Since there is no vehicle or snag, sign is made GREEN to educate the passageway. The same is connected for in the other course and SG3 and SG4 are made ORGANIC and entryways are fixed. Due to some unavoidable conditions, in the event that you have a sudden breakdown of a vehicle between the entryway, then the light from laser source would not fall on LDR. This shows the event of vehicle and the sign for train ought to be delivered RED with a specific end goal to ease back up the train to maintain a strategic distance from mishap. At that point the impediment ought to acknowledge to clear the way.

E. Gate closing operation

After the microcontroller senses that there is no vehicle inside, then it automatically produces the signal to control the motor through relay routine and hence close the gate for the verse of train. When any occurrence of obstacle is sensed, 89C51 gives transmission for obstacle to clear the path and once the path is cleaned out, motor is operated to shut the gate. In fact rotary motion occurs in a motor. This rotary motion is converted to linear motion of the gate by using a gear.

F. Gate Opening

At the point when the train takeoff is detected by the sensors, sign is given to the Microcontroller which works the engine in opposite bearing and the entryways are opened. Once the door is opened sign for street clients are made GREEN so that the vehicles can go through the entryway.

Advantages

- Human error can be reduced.
- Time saving system.
- Manual work will be replaced.
- People will find it safer to use.
- Less chances of accidents.

CONCLUSION

The automatic railway gate controller is a useful way to reduce the railway accidents. This system is useful for both remote areas also where there are no gate keepers and stations. By using sensors we can detect the arrival and road and rail route users and also for railway management. This system is fully automated so it can be used in rural and departure of the trains. In this system motors are used to open and close the gates in level crossing. This railway gate controller is controlled by many operations like alarms, lights, sensors. Our project is a latest approach to get rid of the problems faced by the people. By using this concept we can reduce the increased number of accidents and problems faced by the people waiting a long time in level crossing. The automatic system plays a very important role in all the fields and also has many applications.

REFERENCES

[1] Krishna, ShashiYadav and Nidhi, "Automatic Railway Gate Control Using Microcontroller", Oriental Journal Of Computer Science &Technology, Vol.6, No.4, December 2013.

[2] Ahmed Salih Mahdi. Al-Zuhairi,"Automatic Railway Gate and Crossing Control based Sensors &Microcontroller", IN International Journal of
Computer Trends and Technology (IJCTT) – Volume 4 Issue 7– July 2013

[3] J. Banuchandar, V. Kaliraj, P. Balasubramanian, S. Deepa, N. Thamilarasi," Automated Unmanned Railway Level Crossing System", in
International Journal of Modern Engineering Research (IJMER)Volume.2, Issue.1, Jan-Feb 2012 pp-458-463

[4] Fred Coleman III, Young J. Moon (2011) Trapped Vehicle Detection System for Four Quadrant Gates in High Speed Rail Corridors,
Transportation Research Record 1648

[5] Fred Coleman III, Young J. Moon (2010) Design of Gate Delay and Gate Interval Time for Four Quadrant Gate System at Railroad-Highway
Grade Crossings Transportation Research Record.

SDSG-SMART DOORS FORSMART GENERATION

Ashith Sashidhar[1], Raksha K Shetty[2], Bharath J[3]
[1,2]UG Scholar, [3]Asst. Professor, Dept of CSE, RRCE, Bengaluru
E-Mail: awesomeashith@gmail.com , rasharaksha@gmail.com

Abstract - In this paper we are presenting a real time smart door system for home security many of the systems use numerous sensor devices as main support for smart doors. As there are many security issues, technologies have evolved. Picture based smart door systems have recently become an efficient approach with the development of micro cameras technology. Using these technologies in the proposed system will bring several advantages in providing safety and security in terms of visualizing and identifying people who visit our home. In the proposed system, there will be two different significant techniques to provide home security. By connecting the smart door system with the mobile phone through an application, the owner of the home may have several options such as controlling the home door, getting instant picture of the visitor, receiving and sending messages and initiating the alarm system. The results after experimentation show that the proposed system may be able to provide us a consistent security and assistance for safe and secure home.

Keywords – Security and Safety, Smart Door System.

I. INTRODUCTION

The system is developed using Mobile Communication and Safety Powered Smart Door System. The smart Door which is simple and reliable ,basically a part of our door is a touch enabled which is similar to the touch screen technology used in the smart phones .In addition to this the smart door has a mini camera and a mike installed within the boundary of touch enabled screen. This can be a manual and the smart door also has an application controlled locking system. Making it simple, when someone is at your place they knock or touch the smart door. When anyone touches your door the inbuilt mini-camera clicks a picture of whomever in front of the door with an inbuilt flash, the inbuilt flash helps us to click pictures of the visitor without their knowledge. The clicked picture is sent to an application on the smart door user's mobile phone so the user is always aware who is their visitor, it's a stranger or a friend.

With increasing safety and security issues, the use of smart door system increased consistently with the advent of security related electronics, such as digital door locks, advanced picture conversation devices, and wire-less home security networks [1]. There are many smart systems proposed to provide safety and security at home and offices. Facial and fingerprint recognition and positioning detection techniques are presented in [2].IBEACO (BLE) integrated with an early warning system will be developed to provide safety of home and the system will be integrated on an embedded system device which is called Raspberry Pi [3].This smart door is secure for girls staying alone in homes or children left alone when parents go shopping. If we are not at our home we can send a message through smart door app stating something like "hi, I'm not at home right now. Please come at 5:30 pm." This message is displayed on the smart door fixed at our home and the visitor comes to your place whenever you are available. Now we all wonder all of a sudden whether we have locked our door or not , as a solution to this problem we have an application controlled locking system which locks the door when we set the lock option in our smart door application but we cant open the door through the application as it again leads to a threat to secure system if we give our phone to any other person our mobile is lost. This application can be installed to all the members of the family and all the members has access to their homes smart door. The application connects to the door through a unique finger print scanned at the time of installation of the door.Touch enabled sensors, Biometric sensors -is an input device normally layered on the top of an electronic visual display of an information processing system. A user can give input or control the information processing system through simple or multi-touch gestures by touching the screen with a special stylus/pen and or one or more fingers, Some touch screens use an ordinary or specially coated gloves to work while others use a special stylus/pen only. Biometric sensors are used to convert a person's fingerprint into electronic signals. This sensor also reads pressure, temperature etc.

II. RELATED WORKS

"Real Time Smart Door System For Home Security" - Burak Sarp, Netas Company , Kurtkoy, Istanbul, Turkey : Idea Has Been Reffered With Respect To Rasberry-Pi And Ibeco.

"**The Design Of Video Door Phone And Control Sysytem For Home Secure Applications",** Ching-Lung Chang And Han-Yu Tsai : Idea Has Been Reffered With Respect To Image And Text Messaging.

III. PROPOSED SYSTEM

This system is developed to bring evolution in the intelligent door systems for various security issues. The

system will have the following specifications and applications:

System includes hardware, software, mobile communications and cloud computing for storage purposes.

- The smart door system is planned to be installed to the middle part of the door and the application in our mobile phones gives us access to it.
- Text to speech feature are added to the system, we plan to have a project in advanced intelligent door security systems .Images will be captured by the mini camera and stored in the cloud for the later use. Thus, the important data will be in the cloud for future checking or maintenance.
- Another important issue is to provide security in the system that other people cannot access the system. Therefore, encryption will be used between mobile device and smart door system, cloud and smart door system vice versa. Thus, the data will be protected.
- The system will be integrated on an embedded system device which is called Raspberry Pi. The device will have mini Camera, Sensors and microphone as shown in Figure 1.
  In order to provide communication between smart door visitor and mobile device we used APNS&GCM technology. Besides this, the system will provide SMS

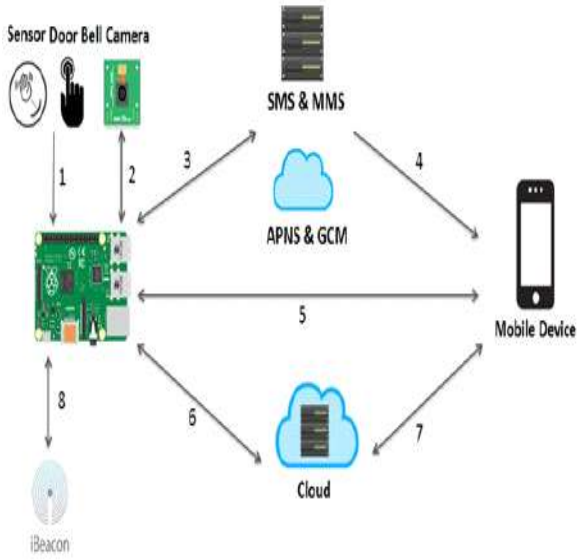


Figure 1. Diagram of the overall system

IV. RESULT ANALYSIS

The result of our proposed system will be that when a visitor visits our home his picture will be captured as visitor touches the door and will ask for fingerprint ,if the visitor is a member of home then their finger print is scanned and converted to electronic signals and access is granted if it matches the stored finger print.

Each time when visitor touches the door ,picture of them is captured and sent to the corresponding application in owners or users phone . The picture is also stored in cloud storage for future uses.

Incase if the finger print does not match a warning along with visitor image is sent to the application and alarm tone is initiated and owner is notified.

.

Figure 2. Image and video communication between smart door system and Mobile phone.

The algorithm uses the input images from a mini camera for communication. The image of home visitor is delivered to the owner via wireless communication. Figure 2 shows the diagram of the image and text message communication system which will be pro-vided between the Raspberry PI and Mobile device. The owner may also send text data to the smart door system to communicate with the visitor. Thus, there will be a communication between visitor and owner. As a result, owner may know the visitor and inform the visitor for her/his current location. On the other hand, the client may call the security if the visitor is unknown.

CONCLUSION

We have proposed a system of real time smart door to provide security and safety to home owners. To provide an effective system, we used Raspberry Pi system which is integrated on the smart door. The system is based on image and fingerprint technology which is a very popular for providing security and safety . Raspberry Pi is used because it is strong and reliable embedded system device for solving complex and challenging tasks. Using technologies in the system provide various benefits to increase the efficiency in terms of communication between visitor and owner of the house and providing safety of home. In the proposed system, two different important

techniques have been used for home security. First is the use of image capturing technology to click the images of visitor and the second is to offer communication between the visitor and owner of the house via door system.

REFERENCES

[1] Ching-Lung Chang and Han-Yu Tsai, "The design of Video Door Phoneand Control System for Home Secure Applications," IEEE International Conference. Innovative Mobile and Internet Services in Ubiquitous Comput-ing, Vol. 5, pp. 1-5, 2011.

[2] Kai-Tai Song and Jian-Liang Chen, "Sound direction recognition using a con-denser microphone array," IEEE International Symposium. Computational Intelligence in Robotics and Automation, Vol. 3, pp. 1445, Istanbul TURKEY, July 2003.

[3]Charles H. Knapp, "The General-ized Correlation Method for Estimation of Time Delay," IEEE Transactions on Acoustic, Speech, and Signal Processing, Vol. ASSP-24, No. 4, pp. 320-327, 1976.

Research and Application Based On Virtual Reality and WebVR

Ms. Saniya Parveez[1], Mrs. Swathi Priya N[2], Mr. Prabaharan J[3]
[1]UG Scholar, [2,3]Asst.Professor, Dept. of CSE ,RRCE, Bengaluru
E-mail:saniyap@rocketmail.com,swathinatrajan@gmail.com,prabaharan.jothi@gmail.com

ABSTRACT-With the development of VR and relative domains, only the analog and simulation to real sceneshave not completely fulfilled the users. Under this background, the combination of WEB3D and VR is the necessary tendency for the technical development. WebVR uses ActiveX controls to extract the desired texture skin from industry strength browsers, providing a unique mechanism for data fusion and extensibility. This paper mainly presents an investigation to webVR that is recently being introduced and the comparative study between the augmented and virtual reality. It also includes a brief about webVR and VR and its working. Special emphasis is given in building of web based VR. The paper also highlights the arising of virtual technology in medicine, games, scientific visualization and also the basic requirements needed in making the VR. It also focuses on the future era!

Keywords- webVR, VR, Augmented reality, virtual reality.

I. INTRODUCTION

2016 has been named "the year of VR", with so many industry milestones happening across the year. Among the most notable ones, Vive and Oculus started to ship Virtual Reality (VR) is stimulating the user‟s senses in such a way that a computer generated world is experienced as real. In order to get a true illusion of reality, it is essential for the user to have influence on this virtual environment. The VR industry is moving incredibly fast, Hand controls make a tremendous difference in VR. The technology being built is tailored to the film, gaming, and sports entertainment worlds

In order to support and enhance learning through web based virtual environment pedagogical methods should be applied. This paper investigates this area and aims at collaborative learning to fulfil the objectives.In medicine the virtual technology plays a vital role. The scientists and medical professionals have been at the drawing, developing and implementing in many ways that can help them train, diagnose, and treat in myriad situations. The reality experiences provide for a controlled environment in which patients can face their fears and breaking patterns of avoidance. The technology is being put to use to help soldiers with post traumatic stress disorder. This fact is of great importance that the virtual web reality in medical field has shown a very great potential.

II. EQUIPMENTS

A wraparound headset (HMD) and data gloves, wired into a powerful workstation or supercomputer. What differentiates VR from an ordinary computer experience (using your PC to write an essay or play games) is the nature of the input and output where an ordinary computer uses things like a keyboard,mouse,or (more exotically) speech recognitionfor input, VR uses sensors that detect how your body is moving. And where a PC displays output on a screen (or a printer), VR uses two screens (one for each eye), stereo or surround-sound speakers, and maybe some forms of haptic (touch and body perception) feedback as well.

A. Head-Mounted Displays (Hmd)

There are two big differences between VR and looking at an ordinary computer screen: in VR,we see a 3D image that changes smoothly, in real-time, as we move our head. That's made possible by wearing a head-mounted display, which looks like a giant motorbike helmet or welding visor, but consists of two small screens (one in front of each eye), a blackout blindfold that blocks out all other light (eliminating distractions from the real world), and stereo headphones. The two screens display slightly different, stereoscopic images, creating a realistic 3D perspective of the virtual world. HMDs usually also have built-in accelerometersor position sensors so they can detect exactly how your head and body are moving (both position and orientation—which way they're tilting or pointing) and adjust the picture accordingly. The trouble with HMDs is that they're quite heavy, so they can be tiring to wear for long periods; some of the really heavy ones are even mounted on stands with counterweights.

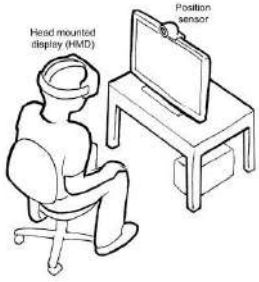


Fig 1. Head-Mounted Displays

B. Data Gloves

A glove equipped with sensors that sense the movements of the hand and interfacesthose movements with a computer. Data gloves are commonly used in virtual realityenvironments where the user sees an image of the data glove and can manipulate the movements of the virtual environment using the glove.A data glove may also contain control buttons or act as an output device, e.g. vibrating under control of the computer. The user usually sees a virtual image of the data glove and can point or grip and push objects.

It is capable of simple gesture recognition and general tracking of three-dimensional hand orientation.The data gloves

are several types of electromechanical devices used in haptics application.

Fig 2. Data glove

III. VIRTUAL REALITY

Virtual reality is the creation of a virtual environment presented to our senses in such a way that we experience it as if we were really there. The technology is becoming cheaper and more widespread.

In technical terms, Virtual reality is the term used to describe a three-dimensional, computer generated environment which can be explored and interacted with by a person.

IV. WORKING OF VR

Virtual reality headsets present sensory information to the user from a virtual envrionment. This technique relies on accurate head tracking

- More advanced versions of these glasses contain head tracking systems. This system is connected to a computer which sends signals to adjust the images seen by the wearer as they move around their environment.
- These glasses enable the wearer to see three dimensional images which give an illusion of depth of perception.
- Many types of glasses contain a tracking system which maps the wearer‟s movements and adjusts the images accordingly. Each time the wearer moves his head, walks in a particular direction or takes some other form of action.
- The tracking system is connected to a computer which adjusts these images so that the wearer is shown a realistic environment with a realistic depth of perception.
- The glasses enable the wearer to see two separate images which the brain combines into one. This is what gives the illusion of 3D depth.

V. WEBVR

WebVR is a virtual reality platform that allows the users to experience VR in their web browsers. WebVR allows the users to access their browsers through their VR devices. VR content can be created with WebGL, a javascript API for rendering 3D graphics.Currently WebVR is available for Mozilla Firefox and Google Chrome

VI. WORKING

Google has brought the WebVR APIs to its Chrome web browser. If we look at the present scenario, one needs to put on the VR headset and take it off as one explores non-WebVR and WebVR sites. These new VR capabilities have been recently spotted on the latest builds of Google Chrome Dev and Google Chrome Beta for Android. Chrome Beta now comes with a WebVR setting that brings enhanced virtual reality abilities to the websites that are build using the WebVR standards.

VII. APPLICATIONS

A .In Medicine

Apart from its use in things like surgical training and drug design, virtual reality also makes possible telemedicine (monitoring, examining, or operating on patients remotely). A logical extension of this has a surgeon in one location hooked up to a virtual reality control panel and a robot in another location (maybe an entire continent away) wielding the knife. The best-known example of this is the daVinci surgical robot, released in 2009, of which several thousand have now been installed in hospitals worldwide.

Prior to stereotactic surgery the target tissue must be located in 3D and the location must be transformed to the coordinate frame. VR based planning stations have been developed, which not only display anatomical relationships but also the radiation beam.

One treatment for general anxiety can be meditation. A new app for Oculus Rift called DEEPaims to help users learn how to take deep, meditative breathes by making breathing the only control for the game. The app works with a band worn around the chest that measures breathing. The VR experience is something like being in an underwater world. Breathing is what gets a user from one place to another.

In a more recent example, headset maker Fove, undertook a crowd funding campaignto create an app called Eye Play the Piano which would allow kids with physical disabilities to play the piano using the headset's eye tracking technology.

Hence,VR approaches can be used to stimulate working environments comprised by medical equipment ,machines,furniture and even patients and medical stuff in order to design and optimize it .

B. Games And Entertainment

From flight simulators to race-car games, VR has long hovered on the edges of the gaming world— never quite good enough to revolutionize the experience of gamers, largely due to computers being too slow, displays lacking full 3D, and the lack of decent HMDs and datagloves.

All that may be about to change with the development of affordable new peripherals like the Oculus Rift.

C. Scientific Visualization

Anything that happens at the atomic or molecular scale is effectively invisible unless you're prepared to sit with your eyes glued to an electron microscope.

But suppose you want to design new materials or drugs and you want to experiment with the molecular equivalent of LEGO. That's another obvious application for virtual reality.

Instead of wrestling with numbers, equations, or two-dimensional drawings of molecular structures, you can snap complex molecules together right before your eyes.

VIII. COMPARISON BETWEEN AUGUMENTED AND VIRTUAL REALITY

Purpose

Augmented reality enhances experiences by adding virtual components such as digital images, graphics, or sensations as a new layer of interaction with the real world. Contrastingly, virtual reality creates its own reality that is completely computer generated and driven.

Delivery Method

Virtual Reality is usually delivered to the user through a head-mounted or hand-held controller. This equipment connects people to the virtual reality, and allows them to control and navigate their actions in an environment meant to simulate the real world.

Fig 3. A VR Head Machine

Augmented reality is being used more and more in mobile devices such as laptops, smart phones, and tablets to change how the real world and digital images, graphics intersect and interact.

Fig 4. Augmented VR Device

Augmented reality however, takes our current reality and adds something to it. It does not move us elsewhere. It simply "augments" our current state of presence, often with clear visors

Virtual reality is all about the creation of a virtual world that users can interact with. This virtual world should be designed in such a way that users would find it difficult to tell the difference from what is real and what is not.

IX. SIMILARITIES

Augmented reality and virtual reality are inverse reflections of one in another with what each technology seeks to accomplish and deliver for the user. Virtual reality offers a digital recreation of a real life setting, while augmented reality delivers virtual elements as an overlay to the real world. Both virtual reality and augmented reality are similar in the goal of immersing the user, though both systems to this in different ways. With AR, users continue to be in touch with the real world while interacting with virtual objects around them. With VR, the user is isolated from the real world while immersed in a world that is completely fabricated. As it stands, VR might work better for video games and social networking in a virtual environment, such as Second Life, or even PlayStation Home.

Augmented and virtual reality has one big thing in common. They both have the remarkable ability to alter our perception of the world. Where they differ,is the perception of our presence. Virtual reality is able to transpose the user. In other words, bring us someplace else. Through closed visors or goggles, VR blocks out the room and puts our presence elsewhere.

In view to this I believe both AR and VR will succeed; however, AR might have more commercial success though, because it does not completely take people out of the real world.

X. FUTURE OF VR

On June 26, Mozilla Research launched an experimental build of Firefox with VR-enablers bundled, empowering developers to turn any website into a virtual reality experience. No plugins installs or expensive development tools required. The technologies for VR on the web already exist. These technologies, such as Javascript and WebGL, lack precision and the low latency required for powerful VR experiences. Mozilla has been working on a new specification known as WebVR. This provides a purpose built interface for VR hardware. There are already WebVR „nightly builds" of both Chrome and Firefox and once this technology has been optimised it will be incorporated into the main releases of these browsers.

The second hurdle to overcome is web interface. We are used to two dimensional websites and browsers and websites are designed for this. These two dimensional websites are interacted with via mouse and keyboard. So how could we display and interact with the web in a sensible way with virtual reality and make the most of what the VR experience has to offer?

The bigger challenge, perhaps, is the need to render websites in a way that will make sense in VR. Two dimensional websites could be rendered in the 3D environment or at least have 3D parts / portals in them. For example, Amazon could have a full virtual shop where you could walk around and see products in full 3D VR. The future of web design will be very exciting as we enter the VR era!

CONCLUSION

The pervasive nature of web-based content has lead to the development of applications and user interfaces that port between a broad range of operating systems and databases, while providing intuitive access to static and time-varying information. However, the integration of this vast resource into virtual environments has remained elusive.

WebVR provides access to a 3D web browser framework, enabling users to search for arbitrary information on the Internet and to seamlessly augment those results into virtual environments. WebVR provides access to the standard data input and query mechanisms while supporting active texture-skins of web content that can be mapped onto arbitrary surfaces within the environment

As a result, any surface within the environment can be turned into a web-enabled resource that provides access to user-definable data. In order to leverage from the continuous advancement of browser technology and to support both static as well as streamed content, WebVR uses ActiveX controls to extract the desired texture skin from industry strength browsers, providing a unique mechanism for data fusion and extensibility.

REFERENCES

[1]. Kosmas Dimitropoulos,"Building Virtual Reality Environment for Distance Education on Web",*International Journal of Social Sciences*, 2008,vol.2,pp.1306-973X.

[2]. Learning online [available] at: http://www.vrs.org.uk/virtual-reality/what- is-virtual-reality.html

[3]. https://developer.mozilla.org/en-US/docs/Web/API/WebVR_API

[4]. http://www.augment.com/blog/virtual-reality-vs-augmented-reality/

[5]. http://uploadvr.com/3-reasons-webvr-future-virtual-reality/

Big Data Networking and Big Data Analysis With Map Reduced Model

Ms. Prajwala R[1], Ms. Varshini B[2], Ms. Yashaswini G[3], Mr. Prabaharan J[4]
[1,2,3]UG Scholar,[4] Asst. Professor, Dept. of CSE
ammu.prajwala@gmail.com, varshinigowda84@gmail.com, yashaswinig710@gmail.com, prabaharan.jothi@gmail.com

ABSTRACT - Big data is the data search so large and complicated that it becomes difficult to process by using traditional data management tools or processing applications. This paper reveals progress on a big data networking as well as big data. We have reported efforts into four general categories. Firstly, reported are efforts related to classic big data technology such as storage, Software-Defined Network, data transportation and analytics. Secondly, important aspects of big data in cloud computing such as resource management and performances optimization are introduced. Lastly, we introduce interesting benchmarks and progress in search engines and mobile networking. Upon detailed summary and analysis, limitations of the proposed works and possible future research directions have been proposed.

Keywords-Big Data, Big Data Networking, MapReduce, Cloud Computing, Benchmark, Mobile Networking.

I. INTRODUCTION

Big data includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process data within a tolerable elapsed time. Big data "size" is a constantly moving target, since 2012 ranging from a few dozen terabytes to many petabytes of data. It requires a set of techniques and technologies with new forms of integration to reveal insights from datasets that are diverse, complex, and of a massive scale.

Big data is the term for data sets so large and complicated that is difficult to process using traditional data management tools or processing applications. This paper reveals recent progress on big data and big data networking i.e., and supporting networking infrastructure has to manage information by year 2020. Taking into the considerations of efficiency, economics and privacy should be carefully planned while including new big data building blocks into existing data and networking infrastructure.

In addition to big data challenges the traditional data generation, consumption, and analytics at a much largerscale, newly emerged characteristics of big data has shown important trends on mobility of data, faster data access and consumption, as well as ecosystem capabilities Fig.1 illustrates a general big data network model with Map Reduce. A distinct application in the cloud has put demanding requirements for transportation and analytics of structured and unstructured data.

The major objectives are as follows:

1) Privacy: During the data learning process, only learning results are revealed by learning parties and nothing else.

2) Accuracy: The final learning result from local learning tasks should be closely related to one from the centralized learning task.

3) Malicious learning party detection: The secure learning scheme should be able in detection of a party which is being compromised and as a malicious party.

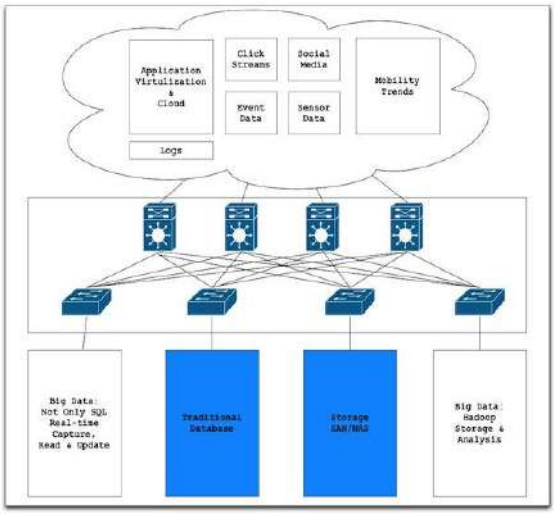


Fig.1 General Framework of Big data Networking

The specific topics covered in big data andbig data networking includes classic big data networking technologies e.g., Hadoop and MapReduce, big data technologies in could compute, big data benchmarking projects, and mobile big data networking which pays close attention to recent progress made on big data and big data networking

II. EFFORTS IN CLASSIC BIG DATA NETWORKING

The traditional big data technologies such as Hadoop, MapReduce and NoSQL, plausible progresses have been made in the past two years on big data networking. Classic big data networking is summarized into 4 parts: storage and warehouse, data transportation, Software-Defined Networking and big data Analytics.

A .Storage and warehouse

The Data storage isthe basis for big data networking. Representative technologies are Relational database and Not Only SQL databases and data warehouse.

The considerable progresses have been made in database research,others remains to be done: firstly, by handling streaming high-rate data in relational models remains as an open problem; secondly, statistical analysis and machine learning algorithms for big data need to be more easier to use; lastly but more importantly, an ecosystem-alike mechanism should be built around the big data algorithms such that data management and usage can evolve on top of the proposed algorithms.

The important aspect in big data related database is data placement structures. One of the traditional data placement structures are row-stores, column-stores and hybrid-stores.

RCFile (Record Columnar File) has been implementation in Hadoop, which meets fast data loading, query processing, efficient storage space utilization, and strong adaptability to dynamic workload patterns. Basic idea of RCFile is depicted as in Fig. 2.

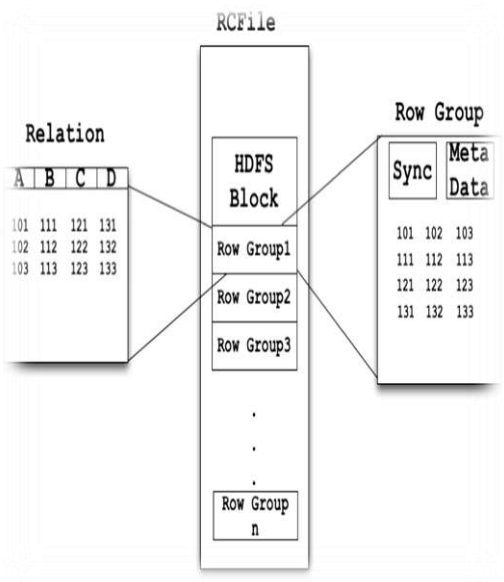


Fig 2. Table Architecture of RCFile

As in Fig. 2, tables in HDFS of RCFile have multiple HDFS blocks, and each HDFS block is organized with basic units of row groups and all groups have the same size. This clustering idea enables RCFile to more efficiently manage data rows.

RCFile has adopted by Hive and Pig. However, RCFile can still be optimized. For example, currently RCFile does not support arbitrary writings since HDFS currently supports only data writes to the end of files. Automatic selection of the best compression algorithm for each column would be another direction that RCFile can pursue.

B. Software-Defined Network

With the Software-Defined Network (SDN) the critical transportation media of big data plays a critical role in big data applications would not be possible without the underlying support of networking because of extremely large volume and computing complexity.SDN has attracted great interest as a new paradigm in networking recently. This allows logical centralization of feedback control, and decisions are made by the "network brain" with a global network view, which eases network optimization. In SDN, data plane elements had become highly efficient and programmable packet forwarding devices, while the control plane elements are represented by a single entity, the controller. While compared to traditional networks, it is much easier to develop and deploy applications in SDN. In addition, with the global view in SDN, it is straightforward to enforce the consistency of network policies. SDN represents a major paradigm shift in the evolution of networks, introducing a new pace of innovations in networking infrastructure. While some excellent work has been done on big data and SDN, the two important areas have traditionally been addressed separately in most previous works. However, SDN as an important networking paradigm will have significant impact on big data applications. In particular, several good features such as separation of the control and data planes, logically centralized control, global view of the network, ability to program the network can greatly facilitate big data acquisition, transmission, storage, and processing. For example, big data is usually processed in cloud data centers. Compared to traditional data centers, SDN-based data centers can have better performance by dynamically allocating resources in data centers to different big data applications to meet the service level agreements (SLAs) of these big data applications in big data networking.

C. Analytics

The Collection and transportation of big data share a common goal: analyzing the data for insights and better application guidance.

Big data analytics is the use of advanced analytic techniques against very large, diverse data sets that include different types such as structured/unstructured and streaming/batch and different sizes from terabytes to zettabytes. Big data is applied to data sets whose size or type is beyond the ability of traditional relational databases to capture, manage, and process the data with low-latency. It has one or more of the

following characteristics – high volume, high velocity, orhigh variety. Big data comes from sensors, devices, video/audio, networks, log files, transactional applications, web, and social media - much of it generated in real time and in a very large scale.

Analyzing big data allows analysts, researchers, and business users to make better and faster decisions using data that was previously inaccessible or unusable. By using advanced analytics techniques such as text analytics, machine learning, predictive analytics, data mining, statistics, and natural language processing, businesses can analyze previously untapped data sources independent or together with their existing enterprise data to gain new insights resulting in significantly better and faster decisions.

The focus of this work is to mitigate the knowledge gap between new users and the sophisticated configurations of Hadoop and its default MapReduce layer.

Integration, development and runtime measurement on a few data transformation tasks have validated feasibility of Radoop for big data analytics with scalable network size and data volumes. System architecture of Radoop can be seen in Fig. 3.

As in Fig. 3, integration of RapidMiner and Hadoop has enabled Radoop to fully take advantage of both sides; however, a further step of componentizing Radoop blocks to further leverage cross-layer tradeoff seems to be a promising step.

Fig 3. System Architecture of Radoop

Specifically for big data analytics, IBM Smart Analytic System, Radoop represent one step towards efficient data management, system adaptation/tunning, and large-scale big data transportation and analysis, respectively. The efforts will check the basis of big data and big data network.

III. PROGRESS OF BIG DATA IN CLOUD COMPUTING

Cloud computing is one of the important application in environment for big data which has attracted tremendous attentions from the research community. Remarkable progress of big data networking has also been reported in this area. we introduce big data research issues and solutions related to Cloud Computing. Specially, we are interested in some following topics: opportunities and challenges of big data networking in Cloud Computing, cloud resource management of big data, and performance optimization of big data in Cloud Computing.

A. Overview and Resource Management

The Resource management plays a vital role in big data applications in the cloud.Some of the key operational challenges such as support cost-saving technologies, rapid deployment, support for mobile and pervasive access,and development of enterprise-grade network design is discussed extensively. Despite existing efforts taking care of these challenges, an open question remains for making these objectives possible in a real-time and scalable fashion**.**

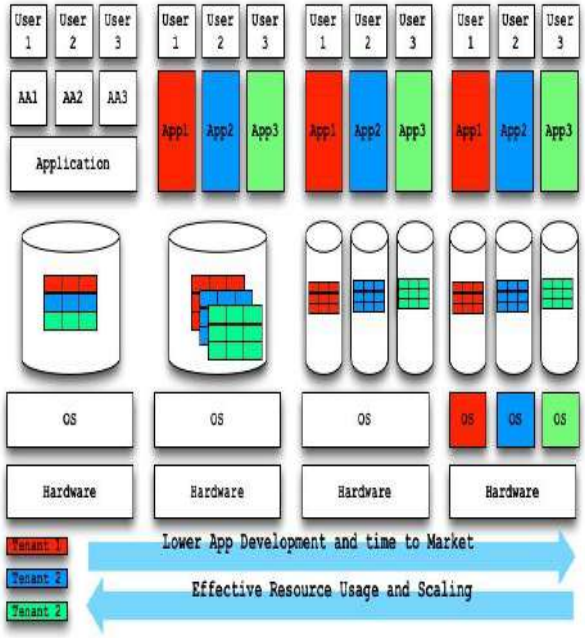


Fig 4. Multi-tenant model: left to right, share table, shared database shared OS and shared hardware.

In Fig.4 tells us the representative forms of the challenging multi-tenant model and trade-offs associated with different forms of sharing. Since models share resources at different levels of abstraction, isolation guarantees which can be achieved differently accordingly.

Representative problems such as large datasets versus limited computational resources, data complexity versus limited knowledge, varying data structures/formats versus

the need to integrate different tools. A case study with spatial temporal data set validated effectiveness of the proposed framework. The main theme is to make better use of computational and storage resources with the help of componentized software and cross-layer communications.

In addition to this pervasive computing of big data in the cloud, computational resource and data complexity management, and energy consumption manipulations for big data in the cloud are fundamentally important aspects. The works have made plausible progress in terms of system design and implementation, but much remains to be done with consideration of system validation in larger, real-world applications.

B.Performance Optimization

Performance optimization is another classic and important topic in cloud computing because appropriate optimization techniques will provide better application experiences with comparable or even less system resource consumption, when compared to non-optimized cases. This work specifically focused on real-time cost minimizations for uploading massive and dynamic data onto the cloud. The two online algorithms have achieved competitive cost reduction ratios. However, the proposed methods are only evaluated in a limited scale. The proposed algorithms need to be further evaluated at higher competitive scales, e.g., data streaming applications with larger topologies.

The performance in the proposed algorithm, is the worst case, would be little more than the current algorithm due to the overhead. On an average, we will have a great improvement over current algorithm, when proposed algorithm is used as the mobile applications have incremental data to transfer.In addition to this, Hitune and the Fijitsu laboratory approaches have been focused on promoting user experiences by using some fundamental big data techniques such as event processing and work flow description. Tools and case studies in these informational and offer more choices to users. Moreover, online cost-minimizing as another promising direction has been proved to be effective in big data applications. We expect a many scalable and efficient algorithms to be proposed in the future.

IV. BIG DATA BENCH MARK AND MOBILE NETWORKING

We briefly reveal two important counterparts of big data networking research: benchmarks and mobile networking with big data considerations. The works represents not only the dedicated efforts but also possible popular trends in big data networking research.

A. Big Data Benchmarks

Big data benchmarks play a fundamental role in these data-centric research areas, because scientifically collection and organization of informational data will provide important ground truth for further methodology verifications.

There are five application domains in BigDataBench, namely search engine, social network, e-commerce, multimedia, and bioinformatics. This describes the details of each domain by which implementation of BigDataBench is guided. By describing the workloads, we use natural language in English.

As an interesting big data benchmark project based on open-source data interfaces of web search engines. As we all know that, the search engines have been entrance point of the whole Internet. Hence, the insightful collection of informational data sets is not only valuable but also hard because of the privacy regulations. This reported work has called in Internet giants such as Baidu, Sougou, Facebook, Yahoo, Huawei and preliminary results have been shown. This has been specific that, the data collection techniques in this work is based on open source solutions of search engines and anonymous Web access logs. Two interesting case studies have been presented. We have a reason to be positive about this benchmark effort considering the big names in the crew.

In addition, remarkable benchmarking efforts have been initiated in both traditional Internet and mobile networking. With an emphasis on privacy-respecting and scalable information collection, the discussed benchmark problems represent the promising step for big data and big networking research in the long run. However, we are also expecting the more insights and inspiring observations which are extracted from these large scale studies.

B.Mobile Networking

Mobile networking is becoming a more and more important counterpart of traditional Internet and big data. The mobile networking is becoming larger and larger due to releasing of hundreds of thousands of cell phones and pads. Because of this evolution of cellular network has enables mobile devices to be connected fast and reliably.

The massive data in mobile cellular networks hasn't been paid much attention. With data constantly accumulated in the database and the technologies of big data analytics rapidly developed, the great value hide behind data has gradually been revealed. It is desirable tomake good use of this precious resource, big data, to improve the performance of mobile cellular networks and maximize the revenue of operators. Traditional data analytics shows its in-adequateness when encountered with the big cellular data. Firstly, traditional data analytics deals with structured data. The large amount of App-based data is, generally not structured. Secondly, the implementation of data analysis is traditionally confined within a department, or a business unit. The final analytical conclusions come from very limited, local angles, rather than global perspectives. Thirdly,

the analytics mainly aims at transaction data, and pays less attention to the operational data, due to its incapability to make realtime decisions.Hence this work only covers only basic aspects of big data, which simultaneously considers both personality study and large scale data.

In sum, mobile networking is an important counterpart of traditional Internet. More importantly, benchmarks and case studies have reflected usefulness of studying mobile big data. Hence, considering the fast and reliable requirement of mobile networking requirements, the effective interactions of the cloud and end users (i.e., close-loop control/interaction) have also might be another interesting research direction.

V. SUMMARY

In this work, we have done in-depth reviews on recent efforts dedicated to big data and big data networking. The important aspect in big data related database is data placement structures. The focus of this work is to mitigate the knowledge gap between new users and the sophisticated configurations. Big data analytics is the use of advanced analytic techniques against very large, diverse data sets. This is a case study with spatial temporal data set validated effectiveness of the proposed framework. The main theme is to make better use of computational and storage resources with the help of componentized software and cross-layer communications.

We have reviewed the progresses in fundamental big data technologies such as storage and warehousing, SDN, transportation and analytics. Important aspects of big data networking in cloud computing such as new challenges and opportunities, resource management and performance optimizations are also introduced and discussed with independent viewpoints. Lastly but not the least, we have also reported important efforts in big data benchmarking and mobile networking, which represent foundations of big data research and promising trends, respectively.

To sum up, we conclude that promising progresses have been made in the area of big data and big data networking, but much remains to be done. Almost all proposed approaches are evaluated at a limited scale, for which the reported benchmarking projects can act as a helpful compensation for larger-scale evaluations. Moreover, software-oriented studies also need to systematically explore cross-layer, cross-platform tradeoffs and optimizations.

REFERENCES

[1] [Laurila12] Laurila, Juha K., et al. The mobile data challenge: Big data for mobile computing research. Proceedings of the Workshop on the Nokia Mobile Data Challenge, in Conjunction with the 10th International Conference on Pervasive Computing. 2012. https://research.nokia.com/files/public/MDC2012_Overview_LauriloaGaticaPerezEtAl.pdf

1. [2] [Costa12] Costa, Paolo, et al. Camdoop: Exploiting in-network aggregation for big data applications. USENIX NSDI. Vol. 12. 2012.http://research.microsoft.com/en-us/um/people/pcosta/papers/costa12camdoop.pdf
2. [3] [Monga12] Monga, Inder, Eric Pouyoul, and Chin Guok. Software-Defined Networking for Big-Data Science-Architectural Models from Campus to the WAN. High Performance Computing, Networking, Storage and Analysis (SCC), 2012 SC Companion. IEEE, 2012.http://www.es.net/assets/pubs_presos/ESnet-SRS-SC12-paper-camera-ready.pdf
3. [4] [Lakew13] Lakew, Ewnetu Bayuh. Managing Resource Usage and Allocations in Multi-Cluster Clouds.2013, http://www8.cs.umu.se/~ewnetu/papers/lic.pdf
4. [5] [Madden12] Madden, Sam. From databases to big data. Internet Computing, IEEE 16.3 (2012): 4-6. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6188576
5. [6] [Bakshi12] Bakshi, Kapil. "Considerations for big data: Architecture and approach." Aerospace Conference, 2012 IEEE. IEEE, 2012.http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6187357
6. [7] [He11] He, Yongqiang, et al. "RCFile: A fast and space-efficient data placement structure in MapReduce-based warehouse systems." Data Engineering (ICDE), 2011 IEEE 27th International Conference on. IEEE, 2011. http://www.cse.ohio-state.edu/hpcs/WWW/HTML/publications/papers/TR-11-4.pdf

Energy Conservation Reliable Routing Protocol in Wireless Sensor Networks

Sunita Patil [1], Mareeswari V[2], Amulya B S[3] , Arpitha B R[4]

Dept. of CSE, ACSCE, Bangalore

E-Mail: sunita.chalageri@gmail.com , mareesh.prasanna@gmail.com , amulyasrinivasan@gmail.com, himarpitha@gmail.com

Abstract –Wireless sensor networks (WSNs) sometimes called as wireless sensor and actuator networks (WSAN) are resource constrained. They are partially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, pressure etc and to cooperatively pass their data through the network to a main location. Energy is one of the most important resources in such networks. Therefore, optimal use of energy is necessary. In this paper, we present a novel energy-efficient routing protocol for WSNs. The protocol is reliable in terms of data delivery at the base station (BS). We consider mobility in sensor nodes and in the BS. The proposed protocol is hierarchical and cluster based. Each cluster consists of one cluster head (CH) node, two deputy CH nodes, and some ordinary sensor nodes. The reclustering time and energy requirements have been minimized by introducing the concept of CH panel. At the initial stage of the protocol, the BS selects a set of probable CH nodes andforms the CH panel. Considering the reliability aspect of the protocol, it puts best effort to ensure a specified throughput level at the BS. Depending on the topology of the network, the data transmission from the CH node to the BS is carried out either directly or in multihop fashion. Moreover, alternate paths are used for data transmission between a CH node and the BS. Rigorous simulation results depict the energy efficiency, throughput, and prolonged lifetime of the nodes under the influence of the proposed protocol. Future scope of this work isoutlined.

Keywords- BS, CH, WSN, DSR, DCH

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of several resource- constrained sensor nodes randomly deployed over a geographic region. These sensor nodes forward sensory data toward a resourceful base station (BS). Depending on the application type, the BS is located either far away from the sensor field or within the sensor field . Such networks have wide range of applications in military and civil domains. Some application areas of WSN are as follows: combat field surveillance, target tracking in battlefields, intrusion detection, postdisaster rescue operations, smart home, monitoring and alarming systems for supermarkets, wildlife monitoring systems, and many safety and security relatedapplications.

In the aforementioned applications, the sensor nodes generate sensory data from the environment of interest. The sensed data are finally forwarded toward the BS for further processing and decision making with regard to the control for meeting the objectives of the system in place. Depending on the application type, the sensor nodes and the BS can be static or mobile. In a typical WSN, the sensor nodes are highly resource constrained. The sensor nodes are inexpensive, disposable, and expected to last until their energy drains out. Therefore, energy is a very limited resource for a WSN system, and it needs to be managed in an optimal fashion. Reliable and successful data delivery at the BS is desired. Energy efficiency is an important aspect of any application of WSN. Routing of data in WSN is a critical task, and significant amount of energy can be saved if routing can be carried out tactfully. Routing is an issue linked to the network layer of the protocol stack of WSN. In multihop communication, the majorissue may be the selection of the intermediate nodes in the route. The intermediate nodes are to be selected in such a way that the energy requirement is minimized. At the same time, the data are to be delivered at the BS reliably and successfully. Hierarchical routing is considered to be an energy-efficient and scalable approach. There are several hierarchical routing protocols proposed for WSN. All these protocols consider a WSN with static sensor nodes. Theses protocols are not suitable to handle mobility of the sensor nodes and the BS. Although dynamic source routing (DSR), ad hoc on- demand distance vector (AODV) routing, destination-sequenced distance vector (DSDV) routing, temporally ordered routing algorithm (TORA), and zone routing protocol are some routing protocols that exist for mobile ad hoc networks, these are not well suited for WSN setup. This is so, due to different features of WSN and the unique constraintsWSN suffersfrom.

Moreover, the WSN applications have different sets of requirements. Routing in a WSN setup in which both the sensor nodes and the BS are mobile is a challenging problem. Existing routing protocols reported do not consider the mobility in sensor nodes and in the BS, and therefore, these are not directly applicable to a mobile WSN. In a mobile WSN, the communication links may come up and fail very dynamically. Therefore, the routing protocol has to take care of the connectivity issue also in such a WSN setup. Data packets are to be routed taking this connectivity issue into consideration. Otherwise, there will be significant loss of data packets due to failed links apart from all other reasons such as frequent death of sensor nodes or noise of the wirelesslinks.

II. RELATED WORK

In the literature, several energy- aware protocols have been proposed for WSNs. Again, there are several routing protocols proposed for WSN, in which the main focus is on reliable data delivery. However, they are designed keeping static sensor nodes and static BS in mind. In the wired networks, the design emphasis has been on maximizing end-to-end throughput and minimizing delay. However, in wireless networks, apart from these two design objectives, there are two more dominating design issues. These are *energy constraints* and *signal interference*, which have attracted most attention from the researchers in the past decade. These have become important issues along with the growing popularity of the wireless consumer devices. Due to the unattended nature of the sensor nodes in the WSN applications, the energy efficiency issue has become extremely important. Energy efficiency can be improved at various layers of the communication protocol stack of WSN. There are several results reported that focus on hardware-related energy efficiency aspects of wireless communications systems.

For example, low-power electronics, power-off modes, and energy- efficient modulations are hardware-based approaches. Significant energy efficiency can be also achieved at the software level. Tactful design of routing mechanisms, which is a network layer issue of the communication protocol stack, may lead to acceptable level of energy saving along with reliable routing service. Network- layer energy efficiency related studies are available in the literature, specifically for static sensor networks. Most of the proposed routing protocols for WSN do not consider mobile sensor nodes and mobile BS. Very limited work for mobile sensor networks is available. When the mobility is introduced in the sensor nodes, the topology becomes very dynamic, and the task of finding out the stable routes (i.e., reliable and long living) under such circumstances becomes challenging. Moreover, it is infeasible for the WSN nodes to cope up with the overhead of maintaining routing tables mainly due to onboard memory constraints. Therefore, different table-driven routing protocols for wireless networks are not directly applicable to WSN. Thus, DSR, AODV, DSDV, and TORA are some representative routing protocols for mobile ad hoc networks, but these are not feasible for mobile WSN.

RAP, SPEED, and Multi-path and Multi- SPEED routing protocol (MMSPEED) are some routing protocols designed for WSN, which can meet objectives such as timely delivery and/or reliable delivery of data packets. Low-energy adaptive clustering hierarchy (LEACH), threshold-sensitive energy-efficient sensor network (TEEN), adaptive TEEN, power-efficient gathering in sensor information systems, and hybrid energy-efficient distributed clustering are some examples of energy-efficient and hierarchical routing protocol for WSN. However, all these protocols consider static WSN only. Hierarchical Information gathering protocol with Multiple Associated Leaders within A Yard (HIMALAYA) is a hierarchical energy-efficient routing protocol for WSN, which considers the BS mobility but does not consider node mobility. BeamStar, energy- efficient clustering scheme, energyaware routing protocol, Self Organizing Network Survivability routing protocol (SONS), Directed Alternative Spanning Tree (DAST), and energy-efficient routing algorithm to prolong lifetime are some recent work reported, in the direction of energy-efficient routing. However, these protocols do not consider the issue of reliability in data delivery. Moreover, these protocols are designed for static WSN. In the authors proposed energy- balanced routing protocol, in which the packets move toward the BS through dense energy area and thus protects the nodes with relatively low residual energy. It uses the concept of potential in physics and constructs a mixed virtual potential field in terms of depth, energy density, and residual energy.

The protocol prolongs the lifetime of the network, but it does not consider the issue of reliable data delivery. Moreover, the protocol does not consider mobility of the sensor nodes and the BS. The modified LEACH (MLEACH) is an extension of the LEACH protocol, which can handle mobility of sensor nodes. However, M-LEACH, again, does not consider mobility in the BS. LEACH is also enhanced in order to support mobile sensor nodes. In node mobility in the WSN is supported by adding membership declaration to the LEACH protocol. It declares the membership of a cluster as they move and confirms whether sensor nodes are able to communicate with a specific CH node. This version also does not support mobility in the BS. Thus, none of the existing protocols can achieve all the following goals at the sametime:

1) guaranteeing reliability in an energy- efficient manner in presence of node and BSmobility.managing mobility of the nodes and maintaining connectivity through alternate paths.

2) minimizing message overhead and overcoming less reliable wireless links. Therefore, energy-efficient and reliable routing in mobile WSN environment is still an open issue. In this paper, our contributions may be summarized as follows.

1) We consider the mobility of the sensor nodes and the BS while routing decisions aremade.
2) The notion of deputy cluster head (DCH) is used, which increases the lifetime of thenetwork.
3) The notion of cluster head (CH) panel is used, which also increases the lifetime of thenetwork.
4) The notion of feedback by the BS regarding data delivery in it isconsidered.
5) The protocol ensures reliability in terms of data delivery at the BS; this is achieved through the use of multiple routes and switching of the routes as decided by the BS.
6) We adapt a probability-based mathematical model that can be used for identifying the most suitable path for data forwarding.

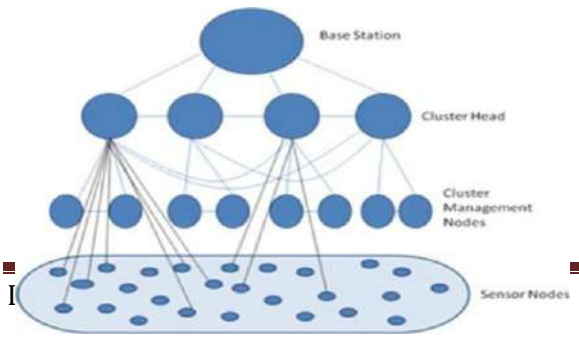
EXISTING SYSTEM

In the system under consideration, it is assumed that the sensor nodes are all similar in hardware, software, and capabilities (i.e., computing and sensing). Initially, all the sensor nodes have equal amount of energy. After some time of operation, nodes may be left with unequal energy levels. The sensor nodes and the BS are mobile with medium mobility level. A medium mobility level indicates a speed range of the sensor nodes and the BS, which is neither very high nor very low. At the time of implementation, the range may be specified quantitatively. It is assumed that the sensor nodes know their mobility level. We consider three different mobility levels, i.e., high medium, and low.

The BS is highly reliable and resourceful. After deployment of the sensor nodes in the field, the field is logically partitioned into some clusters. The BS forms these clusters by executing some suitable clustering algorithm. Each cluster contains one CH node and two supporting DCH nodes. DCH nodes are also called *cluster management node*. Communication takes place inhierarchical

fashion, e.g., Sensor Node → CH →BS.

Again, communication between a CH node and the BS may take place in multihop fashion depending on the current network topology. Fig. 1 depicts the system architecture and shows the sensor nodes with different roles in the system.



The selection of nodes for various roles, e.g., CH or DCH, is carried out at the BS. Each sensor node is assumed to be capable of operating in an *active mode* or in a *dormant mode* (i.e., low power). We assume that there exists some Geographic Position Systems (GPS)-free low-cost solution to know the geographic location of each node by itself. The energy source, i.e., the battery, of the sensor nodes cannot be refueled. In the system under consideration, it has been assumed that there exists only a single BS and that the BS is located away from the sensor field. Although the BS is mobile, it never moves across the sensorfield.

Problem Statement:

The major goal of this work is to design an energy-efficient and reliable routing protocol for a mobile WSN that operates in an unattended manner and, sometimes, in hostile environment. As the sensor nodes are resource constrained (*particularly limited energy and limited onboard storage capacity*), the routing protocol should consume low power and should not burden the nodes with storage overhead.

PROPOSED PROTOCOL

Here, we propose a novel scheme for routing in a mobile WSN in which both the sensor nodes and the BS are mobile. The proposed protocol, which is called E2R2, achieves fault tolerance by offering some alternate routes to forward data in presence of any fault in the existing route. The main objective is to extend the lifetime of the sensor nodes in the network The protocol offers some suitable alternate routes for packet forwarding in presence of node or link failure in the current route. This arrangement does not allow the throughput level at the BS, in terms of packet delivery, to degrade drastically. The protocol takes care of the energy efficiency and the reliability of the routes. The data packets are routed through multiple hops in order to minimize the transmission energy requirements at the sender nodes. In addition, some sensor nodes are intelligently scheduled for *dormant state*, which is a low-power state. Those nodes are scheduled for dormant state, whose services are not required at a particular instant in time. At a later stage, these nodes may perform state transition and again become *active* while needed. The state transition is dictated by the BS. This saves significant amount of energy at the nodes.

Thus, the battery lives of the sensor nodes get prolonged. After the deployment of the sensor nodes, the BS creates groups of different sensor nodes in order to form clusters. Each cluster contains a CH node and two DCH nodes. The BS selects a set of suitable sensor nodes

from each cluster, which can act as CH or DCH at a later stage. This set of nodes is also called *CH panel*. The cluster members i.e., the sensor nodes, forward data to the respective CH node. The CH nodes do the data aggregation to remove redundancy and then forward the aggregated data toward the BS. The DCH nodes do several cluster management tasks that include mobility monitoring also. Other cluster management tasks are, for example, collecting location information of cluster members regularly and communicating this location information to the BS. They also remain ready to act as intermediate hop in presence of faults in some CH nodes. Therefore, the DCH nodes are also called cluster management nodes. The CH nodes do not transmit data directly to the BS, unless it is the nearest one to the BS. The communication pattern or the route for the CH nodes is determined by the BS and distributed to the respective CH nodes. Fig. 1 depicts the overall organization of the sensor network system. It is assumed that the BS has an idea about the expected number of data packets (i.e., the volume of data) to be arrived in it during a specified time interval. Therefore, the BS keeps on monitoring the actual volume of data arrived from different clusters in the network. If the BS observes less arrival of data packets from some clusters in comparison with a prespecified threshold level, then it informs the respective CH nodes to check their connectivity with their cluster members. The CH considers this as feedback from the BS and accordingly checks the current connectivity with its cluster members. If the connectivity status of the cluster members with the respective CH is very poor, the BS decides to shift the charge of cluster headship to another suitable member from within the CH panel. Depending on the connectivity scenario, the cluster headship may be transferred to one of the two DCH nodes also. The routing decisions are made at the BS and then communicated to the sensor nodes. Since the sensor nodes are resource constrained and, moreover, the nodes are also committed to data processing and communication apart from sensing activities, it is always advantageous to offload the routing decision making process from the sensor nodes. Therefore, this protocol exploits the resourcefulness of the BS by shifting routing and some cluster management activities to theBS.

CONCLUSION

In this paper, we have proposed an energy- efficient and reliable routing protocol for mobile WSNs. The proposed protocol E2R2 is hierarchical and cluster based. Each cluster contains one CH node, and the CH node is assisted by two DCH nodes, which are also called cluster management nodes. We analyze the performance of the proposed protocol through simulations and compare with M- LEACH. The proposed protocol outperforms M-LEACH in terms of lifetime and throughput. In the proposed protocol, the throughput improvement is 15% *on average* over M-LEACH. Such a routing protocol is useful when the sensor nodes and the BS are mobile. This work can be extended to improve the throughput even in the high-data-rate situation, where the sensor nodes generate data at a very high constant rate. The proposed protocol can be also tested under the influence of highly mobile sensornodes.

REFERENCES

[1]I.F.Akyildiz,W.Su,Y.Sankarasubramani am, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] W. Heinzelman, A. Chandrakasan, and H.Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. HICSS*, 2000, pp.1–10.

[3] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in *Proc. IEEE Aerosp. Conf.*, 2002, pp.1125–1130.

[4] A. Manjeshwar and D. P. Agarwal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," in *Proc. 15th IPDPS Workshops*, 2000, pp. 2009–2015.

[5] A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proc. IPDPS*, 2002.

[6] D. B. Johnson, and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*. Norwell, MA, USA: Kluwer Publishers, 1996, pp. 153–181.

[7] C. Perkins and E. Royer, "Ad hoc on demand distance vector routing," in *Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl.*, 1999, pp. 90–100.

[8] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance- vector routing (DSDV) for mobile computers," in *Proc. Conf. Commun. Archit. , Protocols Appl.*, 1994, pp. P234– P244.

CLASSIFICATION OF GROUND GLASS LUNG OPACITY BY HARD THRESHOLDING

Dr.Punal M Arabi[1], Prathibha. T.P[2], Nanditha Krishna[3], Rohith.N.Reddy[4]
[1]Professor,[2,3] Asst.Professor,UG Scholar,Dept. of BME,ACSCE, Bangalore
E-mail: arabi.punal@gmail.com , prathi.tp@gmail.com , nanditha13@gmail.com rohithnreddy12345@gmail.com

Abstract: The doctor patient ratio in India is less than world health organization (WHO) prescribed limit of 1:1000 i.e the total number of doctors in India is much more smaller than the official figure and we may have one doctor per 2000 population or even more. As India's population is feverishly increasing the ratio might go even worse than this in years to come. Unless the Computer aided diagnosis (CAD) methods are developed ensuring the quality life of people would be a dream. Lung diseases in India are increasing year by year. Respiratory diseases like asthma, chronic obstructive pulmonary disease (COPD), Interstitial Lung Disease (ILD), pneumonia, tuberculosis (TB) are most common and major health problems . As per a report given by the WHO the deaths due to lung diseases in India are on a rise which accounts for 11% of the total deaths. As many as 142.09 in every 1 lakh, died of one form or other form of lung disease giving India the dubious distinction of ranking first in lung disease deaths in the world. This paper presents a method to identify a ground glass affected lung by CAD method.

Keywords: CAD, classification, ground glass, HRCT lung images, Hard thresholding by pixel intensity level of 128

1. INTRODUCTION

Lung diseases in India are increasing year by year. The doctor patient ratio in India is less than world health organization (WHO) prescribed limit of 1:1000 i.e the total number of doctors in India is much more smaller than the official figure and we may have one doctor per 2000 population or even more[4].Respiratory diseases like asthma, chronic obstructive pulmonary disease (COPD), Interstitial Lung Disease (ILD), pneumonia, tuberculosis (TB) are most emerging and major health problems in India[1]. As per a report given by the WHO the deaths due to lung diseases in India are on a rise which accounts for 11% of the total deaths. As many as 142.09 in every 1 lakh, died of one form or other form of lung disease giving India the dubious distinction of ranking first in lung disease deaths in the world[7].Imaging modalities and image processing techniques play a very important role in disease diagnosis, treatment planning and monitoring.

Thoracic HRCT(High resolution computed tomography) images contain lots of information about lung textures including bronchus, pulmonary veins and arteries, which provide powerful information for research of automatic CAD systems [5]. Sang CheolPark et.al [2] developed and tested a CAD scheme for detecting pulmonary embolism depicted on CT(Computed tomography) images to improve detection sensitivity and specificity. Fazliet.al [3] proposed adaptive method for segmentation of lung CT images. The proposed algorithm uses adaptive mean shift method which estimate the bandwidth parameter by using fixed bandwidth estimation. Chong et.al [6] developed Robustness-Driven method for feature selection. This improved the robustness of a SVM (support vector machine) for fibrotic interstitial lung disease by maintaining its performance. Ground glass opacification refers to a blurred area of increased attenuation in the lung with bronchial and vascular markings. It can be referred to as chronic interstitial disease and acute alveolar disease.

2. METHODOLOGY

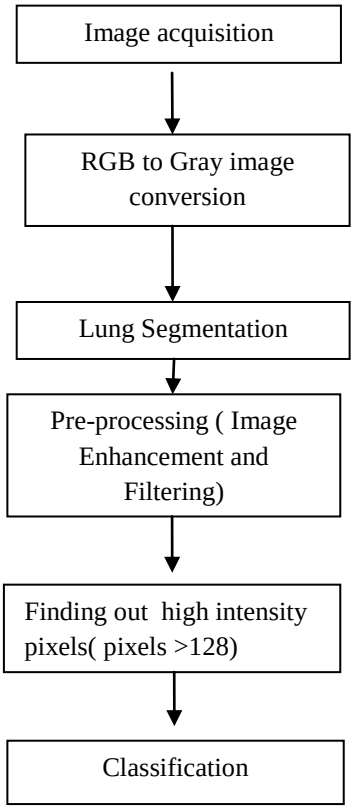


Fig.1 Block diagram

Figure.1 shows the block diagram of the proposed method. A set of 10 images is taken among which 5 images are of normal lung and 5 images are of ground glass lung. The acquired images are converted to gray which are then filtered using low pass filter and enhanced by contrast stretching method. The lung is then segmented by thresholding technique; segmented lung is converted into binary.

Pixel intensity level 128 is used to find out find out higher intensity pixels present in each lung i.e the pixels having intensity level more than 128 are taken as higher intensity pixels. Using these values of higher intensity pixels a reference value is calculated. A decision is made if either left or right lung is having more number of higher intensity pixels than the reference value it is termed as the lung affected with ground glass opacity or else as normal lung.

3.RESULTS

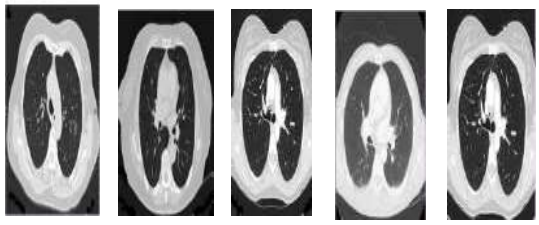


Fig. 2: Normal lung images

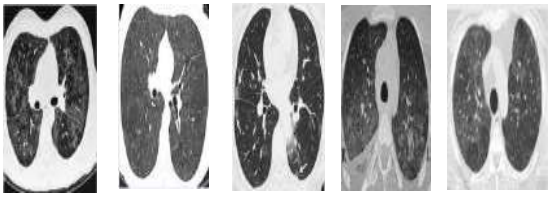


Fig. 3: Ground glass structure lung images

Table1. Number Of Pixels >128 For Normal Lung And Ground Glass Structure Lung Images

Type of Lung	Right lung	Left lung
Normal image 1	289	330
Normal image 2	201	147
Normal image 3	239	370
Normal image 4	607	512
Normal image 5	239	370
Average of Normal image	315	345
Ground glass 1	8705	9588
Ground glass 2	3739	4115
Ground glass 3	573	945
Ground glass 4	1703	1523
Ground glass 5	3249	3737
Average of Ground glass image	3593	3981

Calculation of Reference value (R) :

$$R = \frac{\text{Average of normal lung (Right and Left)} + \text{Average of ground glass lung (Right and Left)}}{4}$$

$$R = \frac{315+345+3593+3981}{4}$$

$$R = 2058 \sim 2000$$

4. DISCUSSION

A set of 10 images are taken for experimentation out of which 5 images are that of normal lung and 5 images are that of ground glass lung . The higher number of pixels having intensity level >128 are observed and tabulated for both normal and ground glass lung as shown in table1.

From table-1 it could be seen that , the reference value of higher number of pixels obtained for both normal and ground glass lung is 2000. If the values of right and left lung are higher than the reference value it is classified as abnormal lung, if they are lesser than reference value they are taken to be as normal lung.

From table 1. Out of ten total lung images (five images of normal lung and five images of ground glass lung) eight images are satisfying the decision rule. All the five normal images are classified showing an accuracy of 80% to classify between a normal and ground glass lung.

CONCLUSION

The proposed method is tested with a set of five ground glass lung images and five normal lung CT images. The results obtained show that the proposed method works well to identify the ground glass structures. A set of ten lung images consists of five normal lung images and five ground glass structure lung images, out of five normal lung images all five images are rightly identified as normal lung and out of five ground glass structure lung images three images are rightly identified as a suspicious image(ground glass lung) giving a total of 80% accuracy. If it is specific to identification of ground glass structures the accuracy reduces to 60% i,e, three images are rightly identified out of five. This may be related to the threshold taken. However to confirm the percentage of accuracy of this method more number of images are to be taken and tested. Analyzing the average pixel value of the left and right , and fixing up a threshold value based on the average value may be considered for further analysis.

ACKNOWLEDGMENT

The authors thank the Management and Principal of ACS College of engineering, Mysore road, Bangalore for permitting and supporting us to carrying out this research work.

REFERENCES

[1] www. Business-standard.com
[2] Sang CheolPark ," A Multistage Approach to Improve Performance of Computer-Aided Detection of Pulmonary Embolisms Depicted on CT Images: Preliminary Investigation", IEEE transactions on biomedical engineering, vol. 58, no. 6, June 2011.
[3] Fazil"Automated lung CT image segmentation using kernel mean shift analysis", 8th Iranian Conference on Machine Vision and Image Processing ,978-1-4673-6184-2/13/2013 IEEE
[4] www. Indiatoday.intoday.in
[5] Tong TONG, Yufeng HUANG, Xingjia WANG, Huanqing FENG, "Automatic Extraction of Three Dimensional Lung Texture Tree from HRCT Images", 978-1-4244-6775-4/10/ 2010 IEEE.
[6] Daniel Y. Chong ," Robustness-driven feature selection in classification of fibrotic interstitial lung disease patterns in computed tomography using 3D texture features", 0278-0062 (c) 2015 IEEE.
[7] www. thehindu.com

Big Data As A Service And Web Based Coactive Big Data Analysis

Deepika M[1], Sreenivasa B R[2]

[1]PG Scholar, [2]Asst. Professor, Dept. of CSE, RRCE, Bengaluru.

Email: deepikamgowda4@gmail.com, br.sreenu@gmail.com

Abstract-The overwhelming of service-generated data become too large and complex to be effectively processed by traditional approaches. The store, manage, and creation from the service-oriented big data become an important problem. To solve this challenge, the proposed method provides an overview of Big Data-as-a-Service and web based coaction big data analytics. Big Data-as-a-Service, includes Big Data Infrastructure-as-a-Service, Big Data Platform-as-a-Service, and Big Data Analytics Software-as-a-Service, is developed to provide common big data services to users to increase efficiency and minimizing the cost. A coaction big data analytics environment for big data as a service. Developers can coact with each other on the platform by sharing data they use, algorithms, and services. Therefore, big data analytics platform effectively and efficiently help to manage big data related things and to develop analytics algorithms and services for the big data , coacting with data owners, data scientists, and service developers on the Web.

Keywords – Big data, BDaaS (Big Data as a Service), Big Data Analytics, web based coaction Big Data Analytics.

I. INTRODUCTION

The global economic structure is transferring from "industrial income" to "service income". According to the World Bank, the statistics tells that the result of current service industry takes more than 80 percent of the world output, while the percentage in developing countries exceeds 75%. The competition in the area of current service industries is becoming a major point of the world's income/wealth development. There has been more and more research and development in data generation by the services with the use of mobile devices, user public used networks, and large servicerelated systems. The more service-related data become too large and multiplex to be effectively and efficiently processed by traditional old approache. Big data are high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, i discovery and process optimization [1].

The emerging large-scale service-oriented often a huge number of services with multiplex structures. The big data generated from these systems have features such as heterogeneous, of multiple data types, and highly dynamic. Due to the rapid increase in the system size and the associated large volume of service-deveoped data, creating value in the presence of complex system and data becomes an inexorable task. Similar to other types of big data, the service generated big data initiatives span four unique dimensions [4]: (1) volume: nowadays' large-scale systems are awash with ever-growing data, easily amassing terabytes or even petabytes of information; (2) velocity: time-sensitive processes, such as bottleneck detection and service QoS prediction, could be achieved as data stream into the system; (3) variety: structured and unstructured data are generated in various data types, making it possible to explore new insights when analyzingthese data together; and (4) veracity: detecting an correcting noisy and inconsistent data are important to conduct trustable analysis. Establishing trust in big data presents a big challenges the variety and number of sources grows. These four unique characteristics of service-generated big data provide great challenge for data management and analysis [2].

Big Data-as-a-Service inludes various big data storage, management, and analytics methods into services and provides big data related services to customers via programmable APIs, which greatly enhances efficiency, reduce cost and effectively[3].

Big data analytics systems enable the users to collect, order, and analyze large sets of data to discover patterns and other useful information. Big data platforms points on processing large data and do not support coacion among users so that it takes more and more time for users to develop services including data collection, data pre-processing, data analysis, and algorithm development. To support more efficient and effective service development environment, we are introducing a

new coactive big data analytics platform that supports users to focus on developing their own services efficiently and effectively to share the algorithms, and services among them[5].The rest of this paper is organized as follows: Section 2 provides an information about Big Data as-a-Service; section 3 provides details BDaaS (Big Data as-a-Service) as a web based coactive Big Data Analytics and section 4 concludes the paper.

II. BIG DATA AS A SERVICE (BDAAS)

Big Data as a Service is the providing of correct analysis tools and information by an provider that supports organizations understand and use information gained from l data sets in order to gain a effective advantages. Big Data as a Service consists of three layers, Big Data Infrastructure as a Service, Big Data Platform as a Service, and Big Data Analytics Software as a Service [4] and it is shown in the figure 1. In the platform as a service data and database are used as a service and in the infrastructure as a service storage and computing is used as a service the purpose of our proposed method is to provide Big Data as a Service and to enable users to develop cloud service more efficiently. And we have designed coactive analytics platform with focusing on Big Data Analytics Software as a Service in BDaaS layers using the standard and programmable APIs, Big Data-as-a-Service activates dynamic integration of different big data and integration of different big data analytics methods to create correct value from the service-enabled big data.

The value of data has been widely recognized. Data can be analyzed for a lot of purposes, such as enhancing system performance, guiding decision making, assessing risk, trimming costs, lifting sales, and so on [7], such kinds of data analysis tasks are separately conducted by different organizations, although these tasks include a lot of common steps, such as information extraction, data cleaning, modeling, visualization, and so on. With the increasingly large amount of data, building separate systems to analyze data becomes expensive and infeasible, caused by not only the cost and time of building the systems, but also the required professional knowledge on big data management and analysis. Therefore, it is necessary to have a single infrastructure which provides common functionality of big data management, and flexible enough to handle variety types of big data and big data analysis works [8].

Big Data-as-a-Service provides general big data related services to users to enhance efficiency, effectiveness and reduce cost. It typically includes three layers, i.e., big data infrastructure, big data platform, and big data analytics. These three layers in Big Data-as-a-Service provide variety levels of abstractions to users, where Big Data Infrastructure provides the most basic services and the higher layers provide more advanced services. Although cloud is a natural architecture for Big Data-as-a-Service, the service is not limited to ajust cloud architecture. Other distributed architecture can also be implemented to launch the big data services [6].

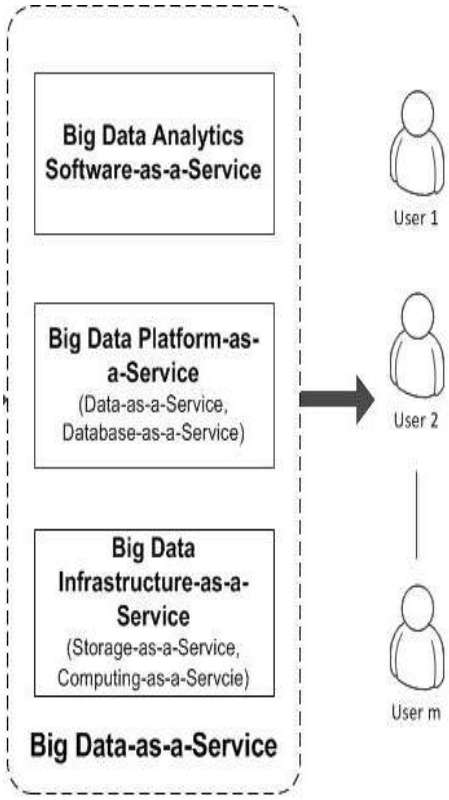


Figure 1. Big data as a Service.

The big data platform, there are variety of ways for data managementand data storage, including cloud storage, Data as-a-Service (DaaS), and Database-as-a-Service (DBaaS)[11]. The key differences between these different ways can be summarized as follows[17]:

• **DaaS (Data-as-a-Service)** defines data lists in a cloud service and allow limited A. Big Data Infrastructure-as-a-Service

The infrastructure provides correct computing and storage capacity for big data. Big data infrastructure can support Infrastructure-as-a-Service (IaaS) in cloud computing, including Storage-as-a-Service and Computing-as-a-Service, to store and process the huge data. Although present technologies such as cloud computing provide infrastructure for automation of data collection, storing, processing and visualization, big data provide noteworthy challenges to the traditional old infrastructure, due to the characteristics of the threes in the big data. current Internet and scientific research

projects develop more amount of data with multiplex inter connection[15].

B. Big Data Platform-as-a-Service

A big data platform allows users to access, analysis and build analytic applications on top of huge data sets [14]. In a big data platform, the big data analysis different steps. For certain steps, APIs provided by the big data platform can be used to conduct common processing on the data. For other

Remaining steps, the users has to provide their own specified processing and analysis rules, and the big data platform to be flexible enough in communicating different kinds of big data analysis works. expropriate high level declarative language is required to specify variety of user tasks. The summons of designing such kind of language include not only the seamless integration of different steps but also the consideration of data locations to enable efficient and effective data management, aggregation, and analysis. At access to the data through Web API. DaaS cannot be accessed via languages such as SQL. DaaS is suitable only for basic data management querying and manipulation.

• **DBaaS (Database-as-a-Service)** offers full database service, which can be retrieved via some specified general sets of APIs. The provided database services can be traditional old relational databases, NoSQL data stores, in-memory databases, and so on.

A. Big Data Software-as-a-Service

More and more organizations turn to Big Data Software-as-a-Service to obtain the business intelligence (BI) service that turns their unstructured data into an enhanced asset [9].Big Data Software-as-a-Service provides huge amounts of structured and unstructured data to accessed in real time and intelligent results, providing users to perform self-service provisioning, analysis, and collaboration. Big Data Software-as-a-Service is typically Web-hosted, multi-tenant and use Hadoop, noSQL [10].

III. BDAAS AS A WEB BASED COACTIVE BIG DATA ANALYTICS

Big Data Analytics SaaS exploits huge amounts of structured and unstructured data to provide real time and correct outputs, allowed users to perform self-service providing analysis, and coactive. Big Data Analytics SaaS is typically multi-tenant, Web-hosted and use noSQL, Hadoop, and a range of pattern discovery and machine learning techniques [12]. Users would execute queries and scripts that data researchers and programmers implement for them to produce reports and graphics[13].

Different big data analytic methods can be designed and provided for the services. By using this the customers will be able to contact with Web-based analytics services in a efficient way without worrying about the data storage, management, and analytical procedures.

As shown in Figure 2, the big data analysis typically involves multiple distinct phases [14] i), big data are sampled and recorded from some data generation. ii) Since the collected data may not be in a format ready for analytics, we need to utilize the required data from the specified sources, and correct the inaccurate records. iii) given the varieties of the data, data integration and representation are required. After above steps, data analysis and modeling can be done on the resulting integrated and big data is cleaned. Finally, data interpretation and graphically are required because big data analytics alone is of limited value if users cannot understand the analysis outcomes.

Table 1. Examples of Big Data Analytics Techniques Usage

Analytic Techniques	Usages
Performance problem diagnosis	Identify the cause system performance problems
Fault tolerance	Improve the reliability of systems
QoS prediction	Enhance quality of the service-oriented systems
Marketing and sales	Identify potential customers, enhance company profit
Manufacturing process analysis	Identify the causes of manufacturing problems
Insurance	Fraudulent claim detection, risk assessment
Item recommendation	Model user preferences from data employing collaborative filtering , etc.
User behavior modeling	Learn user characteristics from data

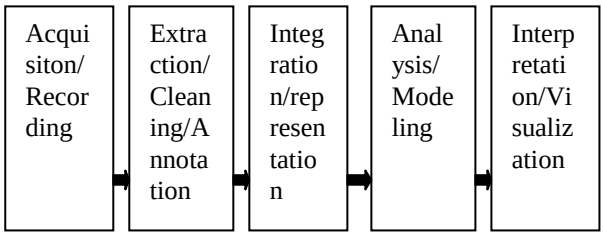


Figure 2. Big Data Analysis pipeline

A. Collaborative Analytics Platform for BDaaS

There are varieties of use cases for the big data analytics like after-sales service, smart traffic control system, searching for missing people, and crisis management system. In order to use analytics services, many steps separately such as data collection, data pre-processing, data extraction, and visualization are conducted. Therefore, developing different systems to analyze big data is require to take more cost and more knowledge on big data technology and tools. The focus of the Big data platform is to enable Big Data as a Service and to customers to develop cloud service more efficiently and effectively. Specially, we have designed coactive analytics platform with pointing on Big Data Analytics SaaS in BD as a Service layers Figure 3 shows the general concept of co-active big data platform for Big Data as a Service. For these services, the platform provides different web-based service requirements and provides resource sharing. For data owners, the platform offers data management . It also enables data scientists and service developers with algorithm and service development platform. The platform supports role-based access control on data owner, data scientist, service developer, and platform manager. Data owners access to the platform to post their data information and share their own data. Data owners collect various data and register information of data via the web portal. Data scientists develop and optimize analytics algorithms on the platform. Data scientists can explore and request data registered by data owners and measure the performance of algorithm. Finally, service developers implement analytics services using available components in the workflow-based tools.

B. Web Service Portal

The web service portal illustrated in Figure 3. The main use of the web service portal is to provide the end- users connection and data sharing on the platform for efficient and effective service development. Therefore, the web service portal enables a web board on which all users can share their data. They can explore data, services, algorithms, and using catalogue services and post their requirements on the board. This coactive among users is possible due to the multi-tenancy architecture. Web service portal provides each user with different web pages according to its use as follows [10].Data owners access data list , data registration, data modification , data catalogue and data monitoring pages to manage their own data. Data catalogue access the users to senquiry about the data easily and efficiently by differentiating data and by handling metadata.

.

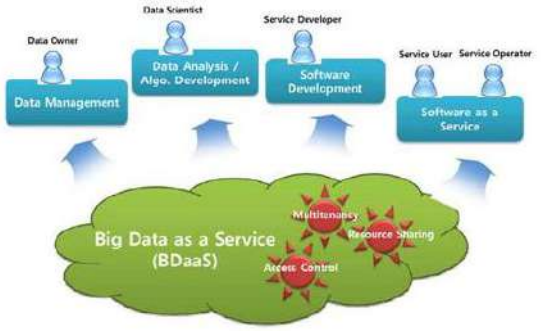


Figure3: Collaborative Big data for BDaaS

C. Analytics Portal

Many big data platforms that generally consist of various open software do not provide useful development tools for customers. Analytics portal is a web development tool to improve development productivity under big data platform. Analytics portal is accessed via web service portal and supports various tools as follows[14].

Query Editor: Analytics portal gives a web interface for hive queries and database queries. The hive query editor consists of query list, text window, and result window. The result window shows log and query history that are recently done. The window also givesthe query results and a reports are generated for them in the form of chart. Data researchers test their hive queries and can register them as the algorithms.

Data Browser: Analytics portal provides two kinds of data browsers. One is for the metastore data browser and the other is for Hbase data browser. Metastore keeps database schema data used in the platform cluster. A platform manager handle metadata stored in the metastore by using a data browser. Developers can handle data stored in HBase and can be used as source or result data of each process through the data browser.

Workflow Designer: Analytics portal provides users who have little experiences in providing services with a useful IDE tool, a web-based service modeling tool that enables users to develop services rapidly using algorithm

component. Workflow consists of independent processes that are the unit of job. We can define the job as a process and monitor the status of the workflow using the workflow designer.

CONCLUSION

We provide an highlights of Big Data as a Service and BDaaS as a web based coactive big data analytics. To provide general functionality of big data management and analysis, Big Data-as-a-Service is investigated to provide APIs for used for co-active big data analytics platform. The big data platform provides a kinds of web portal: web service portal for co-active and analytics portal for developing BDaaS services.

REFERENCES

[1] M. A. Beyer and D. Laney, "The importance of 'big data': A definition," Gartner, Tech. Rep., 2012.

[2] D. Austin, "eDiscovery Trends: CGOCs Information Lifecycle Governance Leader Reference Guide," "http://www.ediscoverydaily.com", May 2012.

[3] The Economist, "A special report on managing information: Data, data everywhere," *The Economist*, February 2010.

[4] IBM, "What is big data? ł bringing big data to the enterprise," "http://www-01.ibm.com/software/data/bigdata", 2013.

[5] H. Mi, H.Wang, Y. Zhou, M. R. Lyu, and H. Cai, "Towards fine-grained, unsupervised, scalable performance diagnosis for production cloud computing systems," *IEEE Transactions on Parallel and Distributed Systems*, no. PrePrints, 2013.

[6] B. H. Sigelman, L. A. Barroso, M. Burrows, P. Stephenson, M. Plakal, D. Beaver, S. Jaspan, and C. Shanbhag, "Dapper, a large-scale distributed systems tracing infrastructure," Google, Inc., Tech. Rep., 2010

[7] "Why big data analytics as a service?" "http://www.analyticsasaservice.org/why-big-data-analytics-as-aservice/", August 2012.

[8] P. O'Brien, "The future: Big data apps or web services?" "http://blog.fliptop.com/blog/2012/05/12/the-future-big-data-appsor-web-services/", 2013.

[9] S. Lohr, "The age of big data," *New York Times*, vol. 11, 2012.

[10] "Challenges and opportunities with big data," leading researchers across the United States, Tech. Rep., 2011.

[11] C. Lynch, "Big data: How do your data grow?" *Nature*, vol. 455, no. 7209, pp. 28–29, 2008.

[12] Z. Zheng, J. Zhu, and M. R. Lyu, "Service-generated big data and big data-as-A-service: An overview," pp. 403-410, 2013.

[13] S. Lohr, "The age of big data," New York Times, vol. 11, 2012.

[14] "Challenges and opportunities with big data," leading researchers across the United States, Tech. Rep., 2011.

[15] E. Slack, "Storage infrastructures for big data workflows," Storage Switchland, LLC, Tech. Rep., 2012.

[16] E. Thereska and G. R. Ganger, "Ironmodel: robust performance models in the wild," in Proceedings of the International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS '08), 2008, pp. 253–264.

[17] M. Chen, E. Kiciman, E. Fratkin, A. Fox, and E. Brewer, "Pinpoint: problem determination in large, dynamic internet services," in Proceedings of the International Conference on Dependable Systems and Networks (DSN'02), pp. 595–604.

[18] W. Xu, L. Huang, A. Fox, D. Patterson, and M. I. Jordan, "Detecting large-scale system problems by mining console logs," in Proceedings of the ACM 22nd Simposium on Operating Systems Principles (SOSP'09), 2009, pp. 117–132.

Enhance Confidentiality in Cloud Computing by using Biometric Encryption.

Usharani J[1], Dr. Usha Sakthivel[2]
[1]PG Scholar, [2]Professor ,Dept of CSE, RRCE, Bengaluru
Email: usharanismg@gmail.com , sakthivelusha@gmail.com

Abstract: Virtualization is the base technology used in Cloud computing and it enables the Cloud computing to provide hardware and software services to the users on demand. Literally, many companies migrates to the Cloud computing for many reasons such as capabilities of processor, size of storage, bus speed, memory and managed to reduce the cost of dedicated servers. However, Cloud computing and virtualization contain many security weaknesses that affects the confidentiality of biometric data in the Cloud computing. Such security issues are VM ware escape, hopping, mobility, diversity monitoring and etc. Further, the privacy of a particular user is an issue in biometric data i.e. the face reorganization data for a famous peoples. Therefore, we proposed biometric encryption technique to improve the confidentiality in Cloud computing for biometric data. We discussed virtualization for Cloud computing, as well as biometrics encryption. Actually, we overviewed the security weaknesses of Cloud computing and how biometric encryption can improve the confidentiality in Cloud computing environment. Apart from this, confidentiality is enhanced in Cloud computing by using biometric encryption for biometric data.

Keywords - Biometric Encryption, Cloud computing, Virtualization.

I. INTRODUCTION

Cloud computing is not a new technology; rather it is a new way of delivering computing resources and services. The development of Cloud computing has brought new changes and opportunities to IT industry. Its general purpose is to dynamically allocate scalable resources to multiple users. Users of the cloud can acquire on-demand basis cloud services and access it globally. Cloud computing also provides measured services, that is to say customers only pay for what they use. Furthermore, Cloud computing offers an effective way to reduce IT expenses, Capital Expenditure (CapEx), and Operational Expenditure (OpEx), and thus it offers economic benefits to users and organizations. It utilizes many technologies that make the cloud environment today. Among these technologies which Cloud computing utilizes is Virtualization. Virtualization is a technology commonly defined as abstraction or execution environment which hides the complexity of hardware layer and allows multiple operating systems to run without the need of real hardware. Virtualization has also been used to offer dynamic resource allocation and service provisioning, particularly in IaaS Cloud environment. After all, virtualization plays a big role in making Cloud computing environment. Cloud computing environment solely depends on virtualization technology to deliver its business services SaaS, PaaS, and IaaS. It is very important to understand virtualization technology at all levels and not only focusing in CPU, Memory, rather virtualization now involves also application system storage and networking.

II. RELATED WORK

In the past few years, a fair number of research and development efforts have been dedicated to the enhancement of virtualization technology. Most of the efforts can be classified into two categories: (i) performance monitoring and enhancement of VMs on a single physical machine, and (ii) performance evaluation, enhancement, and migration of VMs running on multiple physical hosts. Below we provide a brief summary about the research conducted. We can characterize this line of research in two directions. On one hand, a number of research projects have been devoted to performance monitoring tools for VMM and VMs, represented by the monitoring tools for Xen. On the other hand, a fair amount of work has been conducted on varying CPU scheduler configurations or network I/O related parameter tuning, such as network bridging, TCP Segmentation Offload (TSO).

Some previous study has shown that the performance interference exists among multiple virtual machines running on the same physical host due to shared use of computing resources and the implicit resource scheduling of different virtual machines done by VMM in privileged driver domain. For ex, in the current Xen implementation, all the I/O requests have to be processed by the driver domain, and Xen does not explicitly differentiate the Domain0 CPU usage caused by I/O operations for each guest domain. The lacking of mechanism for Domain0 to explicitly separate its usage contributes to the unpredictable performance interference among multiple guest domains.

III. VIRTUALIZATION IN CLOUD COMPUTING

Virtualization is one of the base technologies used in Cloud computing. In 1960s when applications were multiplexed on very high cost mainframes there was a need of technology that allow as much as possible of resource utilization, hence virtualization technology emerged. In hardware resource multiplexing Virtualization uses virtual machine monitor VMM, server consolidation and to support simultaneous execution of

multiple instances of Oss (typically called Guest OS), therefore, VMM can take control over the executing flow of the guest OS. VMM is a thin layer software layer which conventionally runs on a machine's hardware. It also might run on top of a host OS on the host system. VMM is responsible of managing the VMs and allows no direct interaction with the host hardware. Guest OSs running on VMs interacts with the host systems resources only via the VMMs. The VMM generally runs in the most privileged level and considered trusted component while the guest OS is considered not trusted and hence runs on user mode. Later, as technology advanced which causes advancing in the capabilities of processor, bus speed, size of storage, memory and managed to reduce the cost of dedicated servers, there was almost no need to utilize such a technology as virtualization. Despite of all aforementioned aspects of new technology, new challenges arose. This new advanced cheapest technology led to increase of underutilized machines that brought upon it a significant space and management overhead. Therefore, organizations realized the necessity of using VM, as they could not afford keeping track of every server's application versions, patches. In addition, securing these servers became a major burden for the organizations. So, to overcome these challenges organizations moved back to VMs, merged those VMs onto few physical servers and efficiently managed those VMs via VM monitor VMM; sometime refer to as the hypervisor.

IV. TYPES OF VIRTUALIZATION

There are two types of virtualization environments in which VMM is used. Type I is Full virtualization where VMM is interfacing directly with the system hardware, this type of architecture is also called as native architecture, shown in Figure 1. The Type II is not interfacing directly with the hardware of the system, rather it runs as an application alongside with the host OS. And theType II is called Para-virtualization Figure 2. We would like to discuss these two types and how these two architectures impact the security of virtualization environment such as virtualized cloud environment.

A- Full virtualization

Full virtualization is considered when the hypervisor is implemented directly on top of physical hardware or embedded in host OS kernel. It is also called hardware virtualization because shared resources such as device drivers and hardware layer resources are virtualized by the VMM for guest OS. An example of this type is the , KVM hypervisor and Xen hypervisor.

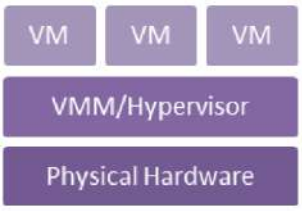


Fig.1. Full Virtualization Architecture

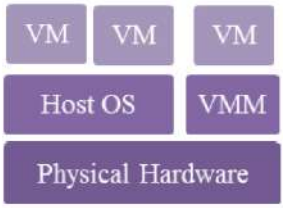


Fig.2. Para-Virtualization Architecture

B- Para virtualization

Para virtualization is commonly installed on those machines that don't support Full virtualization like Intel "x86" architecture. It runs as software and is enabled by the host OS which provides I\O drivers and bootstrapping code. This type is called to be less secure because no matter how secure the VMM is, it is effected by the security of the host OS itself. An example of this virtualization architecture is the implementation of virtual environments using VMware, Sun VirtualBox, and Microsoft Virtual PC. In both the above architectures, VMM's main goal is to support three key attributes in virtual environment.:

- Isolation
- Interposition
- Inspection

- Isolation

The hypervisor or VMM provides isolation through virtual memory abstraction and will not let the VMs to share physical memory. Thus, it lets the VM's to think that each of them is posses its own address space and has full control over it.

- Interposition

This key requires that VMM has the capability to manage all privileged operations on a physical hardware. This means VMM is always interfacing with the physical hardware and mediate all the requests from the guest OS to the underlying hardware. This provides some level of security. It ensures that no direct interaction with lower hardware layer.

- Inspection

Inspection refers to VMM have full access to all VMs states. This includes CPU, memory, and device states. However, Virtualization has now primarily contributed as solution for security, reliability, and administration in that along with its associated techniques help to solve number of security issues. According to IBM researcher in, a single system could implement a multiple-level secure system by dividing it into multiple single- level virtual systems and securely separating them.

V. ADVANTAGES OF VIRTUALIZATION

A) Resource Pool

This characteristic provides a uniform abstraction of resources. This means that a physical machine is not

viewed as limited entity with particular fixed capabilities, in fact, this feature shows how virtualization consolidates a collection of VMs onto a single machine. Thus, it lowers resource costs and space requirements.

B) Flexibility

This feature allows the user to run multiple instances of an operating system one a single computer. VMs can be migrated easily to another physical machine. It is also possible to change the specifications of virtual computers while they are running; Adding RAM, HDD.

C) Availability

Availability ensures that VM image can continuously run in the need of shutting down the physical node. This means that if an upgrade or maintenance is to be done to that physical machine; it can be done without affecting the availability of the VM instance. Therefore, a VM hosted in the particular physical machine needs to be migrated to another physical machine and can be restored back after maintenance is completed.

D) Scalability

This feature shows the virtualization technology strong involvement in making up the cloud. Scalability is considered one of the basic features of virtualization. It assures the process of adding or removing VM instances when the demand for capacity or new VMs increases over time.

E) Cost

Virtualization offers effective cost-reducing due to resource utilization. This can be achieved by consolidating number of servers into one physical server, hence reducing the capital expenditure (CapEx).

F) Security

Though there are many argue that virtualization is facing security challenges, it offers isolation between the VM instances. Isolation provides encapsulation, i.e. no VM is allowed to communicate directly with the other. However, isolation, if not deployed properly, it pauses threat by itself. This highlight that virtualization offers some level of security. For example, a web server VM hosted in a machine alongside with database VM and email VM and If the attacker compromised that web server VM the other VM instances are unaffected.

VI BIOMETRIC ENCRYPTION

Authentication is a mechanism used to identify the people and to provide the authorization to them. Authentication and identification are used in many fields to provide proper security mechanisms. Authentication and identification are used in access control, security audit, verification, etc. Furthermore, identification can be achieved by using the behaviour features or physiological features. Apart from this, the science of using these features is called biometric identification.

Biometric identification includes voice, fingerprint, iris, and face reorganization etc., Biometric identification is more flexible authentication method than secret key, because it is extremely difficult to be forgotten or even lost. Yet, the secret key is considered more secure approach, due to some Biometric identification has been hacked using fake Biometric information attack, such as fake fingerprints attacks. In public security and banks, biometric identification has been applied as a strong security mechanism and strong solution .

Biometric encryption (BE): This is a solution that has been used to protect biometric identification. Actually, cryptography is the solution to overcome the threats on biometric identification. So, encryption was proposed as a patent by Bodo. Later, the first version of biometric encryption was proposed by other researchers. Biometric encryption also proposed for face reorganization to enhance the privacy. Also, biometric encryption is used in Tele-healthcare systems. Moreover, biometric encryption was implemented in a standalone system using fingerprint fuzzy fault schema. In addition, a new framework of biometric encryption was proposed with filter-bank based fingerprint feature. Besides, the security of Mobile-ad hoc network was enhanced through uni-modal biometric encryption key. Furthermore, a cell phone was developed with biometric encryption based on user's behaviour to authenticate the cell phone user. Actually, biometric encryption technology uses three models: key release, key binding and key generation. At a recent tim, the feasibility of deploying biometric encryption has been conducted for mobile Cloud computing.

Biometric encryption was differs from normal password encryption, because it merges the biometric images with random generated key using "BE binding algorithm" to generate Biometrically-encrypted key. In the decryption process, the Biometrically-encrypted key is merged with the biometric image using "BE retrieval algorithm" to get the key retrieved.

Cloud Computing Security Issues and BE Effects:

Despite of all those charming features and strong support that the virtualization technology provides to the computing environment is utilizes it. It has a great impact on the development of these relying environments. Eventhough, as mentioned before, virtualization is not new technology as Cloud, it has several security issues. These security issues have migrated into Cloud computing environment. Most of these security issues are based on the virtualization level.

However, Biometric encryption provides extra Security level for privacy against these security issues. It is most important to mention that Biometric encryption does not solve the security issues in Cloud computing. But, it secures Biometric data against most of these security issues. BE provides extra level of security for the attacker in the Cloud which is the encryption mechanism.

A. VM Hopping

This kind of threats are directly affecting the users/customers of the Cloud. It was always because of resource sharing, a feature which virtualization offers. Resource sharing allows physical machine and its resources such as memory ,CPU, networking and storage to be shared among users reside in the particular physical machine, these users/tenants are called residents and thus the machine is going to provide co-residency/multi-tenancy. Even though multi-tenancy is one of the most crucial goals of virtualization, it is considered to be the weak point in a chain. It exposes the virtualized environments to heavy risk and hence, it is huge threat to the Cloud computing. Nevertheless, this attack cannot directly occur from outside. This means that an attacker needs to be placed in that particular physical machine as where his target resides. Even though, the attacker should follow some steps vary from allocating his victim to execute arbitrary commands, this should allow the attacker to be able to break the isolation control and attack his victim.

BE effects: When VM hopping occurs, the attacker can get access to neighbour's VM ware; however, the biometric data is encrypted and it is not readable for the attacker. However, if the attacker could control the whole VM ware and get access to the biometric device, the biometric information will be readable for the attacker.

B. VM Mobility

VM mobility addresses a crucial security issue. VM mobility offers some flexibility in migrating VM instance from storage to another over the network. This security issue is usually due to weak configuration of the cloud network environment. Although this flexibility provides robust support to physical security to protect against stealing the storage, yet it leads to other security issues such as, it allows the attacker to get a copy of the VM which is transmitted from a machine to another. This type of breach violates the confidentiality and integrity of users' data and thus shows that users' data is at risk when it is stored in the cloud. However, mitigating the risk caused by VM Mobility is not a duty of the users. Cloud providers also share some responsibilities in reducing such risk. Therefore, security management of users data stored in the cloud should be written in a Service Level Agreements (SLA) that clearly states the obligations of both Cloud providers and Cloud users.

BE effects: even though the attacker can get a copy of the VM, the attacker gets encrypted biometrics data.

C. VM Diversity

Virtualization technology offers an ease of use in which it allows the users to efficiently create many VMs. This freedom shows that securing and managing these VMs is a huge burden due to various OSs that can be deployed in seconds. This kind of diversity makes VM security management a challenge. However, a proper SLA could help address this issue. Looking at Cloud computing delivery service models, we can say that VM security management in this context is not the responsibility of the cloud service provider (CSP) alone, in fact, it is also the responsibility of the cloud user. For example, in IaaS, the CSP must ensure security and robustness of the underlying infrastructure such as the hypervisor, whereas the user must properly ensure that his VM and offered service is configured properly and secured, and this includes keeping the guest OS patched and up-to-date. However, this is not limited to IaaS. PaaS service model also requires some security and maintenance but PaaS is somewhat robust against VM diversity.

BE effects: different VMs may contain different types of operating systems. These operating systems contain different weaknesses, so it is the duty of the VMs owners to keep their VMs updated as well as BE. This approach can protect their data in case of intrusion to their VMs.

D. Denial of service

Denial of service is shutting down an available service; also it is blocking the performance and the functionality of the source. Virtualization environment is a shared resources environment where VMs share the same CPU, memory, bandwidth and disk. Furthermore, the provider always has limited capacity of those resources. Apart from this, one VM can exhaust these shared physical resources which will cause denial of services. Moreover, if the VMs in the same physical machine which use the shared resources at the same time, denial of service will occur. The provider should be aware of the maximum usage of its resources which the VMs can use. Also the provider should configure its resources in a proper manner to prevent denial of services. Denial of service is a serious matter that should be treated with well configuration and monitoring.

BE effects: when the service is down, there are no effects for biometrics encryption. Biometric encryption targets the confidentiality of biometric information only and it is not targeting the availability of the data.

E. VM Escape

VMM is designed to allow VMs to share system resources in controlled approach. Therefore, VMM must enforce isolation between VMs and system resources by preventing any direct interaction with the lower hardware layer. Exploiting a compromised VM in a way that allows an attacker to take control over the hypervisor is known as VM escape. VM escape, the program running in a virtual machine is able to completely bypass the virtual layer (hypervisor layer), and get access to the host machine. Thereby, it escalates to root privileges, basically escape from the virtual machine privileges. This vulnerability will allow the attacker to likely have control over all guest Oss resulting in a complete breakdown of the security framework of the environment. VM escape is the worst

case when the isolation between the VMs and host is compromised.

BE effects: when VM escape occurs, the attacker will control the main host machine and get the root privileges. Therefore, the attacker can have access to all the resource as well as biometric devices, so the attacker can read the

biometric information. When VM escape occurs BE does not help to protect biometric information.

F. VM Monitoring

The primary characteristic in virtualization technology is isolation VMs from each other inside a single host. Apart from this, without a proper configuration for the host machine, one VM can get an access and monitor other VMs. This means the provider lost the confidentiality of the system. One VM can lunch a cross-VM side channel attack to extract the memory information about the victim. Moreover, ARP poisoning can be lunched to turn the traffic from the victim VM to the attacker VM, which allows the attacker to monitor all the traffic of the victim VM. Monitoring VMs is a critical issue which the provider must prevent to keep the confidentiality of its system .

BE effects: if the attacker could sniff the data of another VMs, the data of BE will be encrypted which will provide other security layer and extra challenges for the attacker.

G. The communication between virtual machines

A clipboard in virtual machine technology allows the communication between the hosts VMs; this is very convenient method to do the communication between hosts. However, in the same time, malicious can be transferred easily as well. Another example, some of the providers do not apply full isolation for the VMs by allowing the VMs to access the host virtual machine and use a common application. This action is very risky and proper isolation should be applied. In virtual machine environment, encryption is a good practice to keep the transferred data secured and confidential.

BE effects: malicious codes can transmit the desired data to the attacker or allow the attacker to apply a successful intrusion to other VMs. BE keeps the biometric data encrypted and not readable for the attacker.

H. Host Control virtual machines

The host is the controller of all the virtual machines; the host is the manager, the inspector and the protector of the virtual machines on it. So the host can monitor all the traffic of those virtual machines, and control them as well. Different studies on the virtualization technology showed that the host can affect the VMs. So the host security is very important to secure the virtual machines, also a proper configuration should be applied and access control restriction to the host to keep all the virtual machines secured as well.

BE effects: it is a good practice to keep the data of the VMs, encrypted in the host; therefore, even if the host is controlled by an attacker, the attacker cannot read the encrypted biometrics data. However, if the attacker could gain the root privileges, biometric information will be readable to the attacker.

CONCLUSION

Virtualization has some security issues. These security issues migrated to the cloud environments which is affecting the confidentiality of biometric data. Biometric encryption is a solution which is proposed in this paper. Actually, Biometric encryption provides confidentiality to the biometrics data in the cloud. Therefore, Biometric encryption is highly recommended to be implemented in the Cloud computing. Indeed, this approach provides extra security level to the Cloud computing. Moreover, it overcomes many security weaknesses in Cloud computing related to biometric data confidentiality. Indeed, confidentiality is enhanced in Cloud computing by using biometric encryption for biometric data. However, Biometric encryption does not solve the security issues in Cloud computing, rather it secures Biometric data against most of those security issues. Until this moment, there is no related research studied Biometric encryption in Cloud computing. However, biometric encryption in Cloud

computing will be implemented in the future. Therefore, biometric encryption for biometric data in Cloud computing will be deployed and evaluated as well.

REFERENCES

[1] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," Communications Surveys & Tutorials, IEEE, vol. 15, pp. 843-859, 2013.

[2] M. A. Bamiah and S. N. Brohi, "Seven deadly threats and vulnerabilities in cloud computing," International Journal of Advanced Engineering Sciences and Technologies, Vol,(9), 2011.

[3] T. Brooks, C. Caicedo, and J. Park, "Security challenges and countermeasures for trusted virtualized computing environments," in Internet Security (WorldCIS), 2012 World Congress on, 2012, pp. 117-122.

[4] M. Price, N. Wilkins-Diehr, D. Gannon, G. Klimeck, S. Oster, and S. Pamidighantam, "The Paradox of Security in Virtual Environments."

[5] Y. Dai, X. Wang, Y. Shi, J. Ren, and Y. Qi, "Isolate secure executing environment for a safe cloud," in Communications in China (ICCC), 2012 1st IEEE International Conference on, 2012, pp. 79-84.

[6] Y. Wen, J. Zhao, G. Zhao, H. Chen, and D. Wang, "A Survey of Virtualization Technologies Focusing on Untrusted Code Execution," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on, 2012, pp. 378-383.

[7] C. Li, A. Raghunathan, and N. K. Jha, "A trusted virtual machine in an untrusted management environment," Services Computing, IEEE Transactions on, vol. 5, pp. 472-483, 2012.

[8] F. Sabahi, "Virtualization-level security in cloud computing," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, pp. 250-254.
[9] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, pp. 1-11, 2011.
[10] Z. Wang, R. Dou, Y. Leng, and J. Wang, "A new framework of Biometric encryption with filter-bank based fingerprint feature," in Signal Processing Systems (ICSPS), 2010 2nd International Conference on, 2010, pp. V3-169-V3-173.
[11] H. Diwanji and J. Shah, "Enhancing security in MANET through unimodal biometric encryption key," in Engineering (NUiCONE), 2011 Nirma University International Conference on, 2011, pp. 1-3.
[12] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Cell phone-based biometric identification," in Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, 2010, pp. 1-7.
[13] Y.-L. Huang, B. Chen, M.-W. Shih, and C.-Y. Lai, "Security Impacts of Virtualization on a Network Testbed," in Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference on, 2012, pp. 71-77.
[14] S. N. Brohi, M. A. Bamiah, M. N. Brohi, and R. Kamran, "Identifying and analyzing security threats to Virtualized Cloud Computing Infrastructures," in Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on, 2012, pp. 151-155.

Epileptic Seizure Monitor and Alarm system using wearable devices

Bhagya Lakshmi.D.N[1], Poonam Kumari[2], Usha Sakthivel[3]
[1] Software Engineer, EADYN Software India Pvt Ltd, [2] Assistant Professor, [3] Professor, Dept. of CSE ,RRCE
Email: connect.bhagya@gmail.com , poonamkumari2388@yahoo.co.in, usha_sakthivel@yahoo.co.in

Abstract- The aim is to propose a seizure detection system based on accelerometer for the detection of epileptic seizure which should be affordable and can easily worn by the patient. EEG* activity has traditionally required complex equipment costing thousands of dollars. In this research used sensors are wireless, which can improve quality of life for patientsThis monitoring system is based on Wireless Sensor Networks that can determine the location of the patient when a seizure is detected and sends an alarm to hospital staff or their relatives. Measuring EEG* activity has traditionally required complex equipment costing thousands of dollars.

Keywords- EEG, E-Health Care system

I. INTRODUCTION

Epilepsy is one of the most common neurological disorders, affecting almost 60 million people all over the world. Most of the affected people can be treated successfully with drug therapy (67%) or neurosurgical procedures (7%-8%). Nevertheless 25% of the affected people cannot be treated by any available therapy. A variety of technologies have been developed to detect and predict ongoing seizures. Like EEG, ECG, accelerometer, and electro dermal systems are among those that have been described. EEG is known to be reliable for seizure detection, but this is only an advantage in a hospitalized situation, where the patient is equipped with either intracranial electrodes or several scalp electrodes. In a home situation other devices for measurements of the pathological signals are more appropriate, such as the novel (with respect to epilepsy) methods measuring signals describing the movements of the patients.

Measurements of brain electrical activity with EEG have long been one of the most valuable sources of information for epilepsy research and diagnosis, yet this rich resource may still be underutilized. Electroencephalography carries a large amount of complex information that is valuable in detecting ongoing seizures. Automated methods of EEG analysis are emerging from the concept that normal brain dynamics, which involve limited, transient synchronization of disorganized neural activity, evolve into a persistent, highly synchronized state that incorporates large regions of the brain during epileptic seizures [1]. While EEG provides a great wealth of data that can be interpreted via automated methods, it can be difficult for patients to wear the EEG electrodes for prolonged periods of time, and prolonged surface electrode recordings may become difficult to read because of increasing impedance. Additionally, some patients may develop skin abrasions due to prolonged exposure to surface electrodes

The monitoring of epileptic seizures is mainly done by means of electroencephalogram (EEG) monitoring. Although this method is accurate, it is not comfortable for the patient as the EEG-electrodes have to be attached to the scalp which hampers the patient's movement. Measuring EEG* activity has traditionally required complex equipment costing thousands of dollars. Now, with research-grade, embeddable biosensor can be developed. EEG biosensors collect electrical signals not actual thoughts to translate brain activity into action. The emergence of wireless sensor networks (WSNs) has motivated a paradigm shift in patient monitoring and disease control. Wireless sensor networks are composed of a large number of sensor nodes; communicate with each other through wireless transmission. Many feasible applications are proposed such as industrial sensor networks, volcano monitoring networks, habitat monitoring, health monitoring, and home automation etc. The organization of internal software and hardware should be in a manner that will allow them to work properly and be able to adapt dynamically to new environments, requirements and applications. Similarly, it makes sure to be general enough to be suited for as many applications as possible [6].

Epilepsy management is one of the areas that could especially benefit from the use of WSN. By using miniaturized wireless electroencephalogram (EEG) sensors, it is possible to perform ambulatory EEG recording and real-time seizure detection outside clinical settings.

The aim is to propose a seizure detection system based on accelerometry for the detection of epileptic seizure. The used sensors are wireless, which can improve quality of life for patients.

In the last few years, there have been many reports of hacking into the electronic ATM system and caused billion dollars of losses in the banking company itself. Oracle attack on authentication protocols and breaches affecting the ATM machine such as cloning of cards and hacking of PIN code have been reported increasingly. Some popular ATM frauds/attacks are listed below [15].

Skimming attacks.

Card Trapping.

PIN Cracking.

Phishing / Vishing Attacks.

ATM Malware.

Physical Attack.

1.1. Security Measures

As technology advances, as ATM applications become more ubiquitous, as more confidential data is transmitted over the ATM system, as more sensitive transactions are conducted, as more threats breaches are reported, the challenge of securing the system becomes more urgent.

II. LITERATURE SURVEY

[1]Over the last few decades, methods have been developed to detect seizures utilizing scalp and intracranial EEG, electrocardiography, accelerometer and motion sensors, electro dermal activity, and audio/video captures. To date, it is unclear which combination of detection technologies yields the best results, and approaches may ultimately need to be individualized. To unlock a new world of affordable solutions for health and wellness.

Golshan Taheri Borujeny[2] proposed Datasets from patients suffering from heavy epilepsy were used for the development of an automatic detection algorithm. In this system, three 2D accelerometer sensors were positioned on the right arm, left arm and left thigh of epileptic patients. Datasets were acquired from three patients suffering from severe epilepsy. The datasets of the epileptic patients were recorded during the day. We recorded 20 epileptic seizures.

Patients were asked to perform a sequence of everyday normal activities but were not told specially how to do them. Normal activities that we recorded included static activities such as reading, working with computer, brushing of teeth, and lying and dynamic activities such as walking.

However, their algorithm still could not always find the optimal solutions of some of their test cases.

Another author proposed with the Datasets from patients suffering from heavy epilepsy were used for the development of an automatic detection algorithm. In this system, three 2D accelerometer sensors were positioned on the right arm, left arm and left thigh of epileptic patients. Datasets were acquired from three patients suffering from severe epilepsy. The datasets of the epileptic patients were recorded during the day. We recorded 20 epileptic seizures.

Patients were asked to perform a sequence of everyday normal activities but were not told specially how to do them. Normal activities that we recorded included static activities such as reading, working with computer, brushing of teeth, and lying and dynamic activities such as walking. The sampling frequency of the accelerometer is 3 Hz. Figure 2 shows the pure output of accelerometers when sampling frequency is 3 Hz. It shows at first lying and then seizure signal. In this Figure the seizure has begun from 180 samples. Acceleration has been measured based on gravity (g=9.8m/s2)

For analyzing and detecting seizures from this huge data sequence, the best way is cutting the acceleration sequences into many overlapping windows (segments) of the same length. For our data, the size of this window is considered 50 samples and it is repeated for every 25 samples. Since the sampling frequency is 3 Hz, we cut the data sequence every 9 seconds and analyzed this window of the ACM data to detect seizure. Figure 3 shows the acceleration data and overlapping window that located the signal.

Preprocessing

The output of an accelerometer attached to the human body consists of different components:

Noise from sensor and measurement system Noise sources from the environment: (a) accelerations produced by external sources like vehicles; (b) accelerations due to bumping of the sensor or the body against other objects Noise sources from the body: (a) Muscle tremor; (b) Heart; (c) Respiration; (d) Blood flow

Detection based on other modalities

Not only the detection and classification of seizures based on the manifestation of the movements is investigated as an alternative for the video/EEG monitoring. Also other modalities are investigated, including several autonomic signals such as heart rate, temperature, skin conductivity (sweating) and respiration. Some of these modalities are, for example, already used in the polysomnography (PSG) for the study of sleep, such as EOG, ECG and respiration monitoring. Below, a list of the diff erent modalities that are used or investigated is given.

• Audio signals: Audio signals can indicate the occurence of a seizure, as the patients may utter sounds during seizures such as stereotyped screams, singing or humming, (autonomic) laughing or weeping, lip smacking or bed noises as a result of movement.

The advantage of recording audio is that the equipment has a low cost and is easy to install in the patient's room. Furthermore, the sensor is non-invasive and even contactless, so there is a maximal comfort for the patient. However, detection systems based on audio generally perform poorly. It is hard to distinguish the specific sound during seizures from normal vocalizations such as speech or snoring or noises that originate from the

background. Sometimes these types of noise can also be part of a seizure manifestation. Tonic-clonic seizures for example are often followed by stertorous breathing (snoring) in the post-ictal period [1].

III. ARCHITECTURE

Data Collecting

Datasets from patients suffering from heavy epilepsy were used for the development of an automatic detection algorithm. In this system, three 2D accelerometer sensors were positioned on the right arm, left arm and left thigh of epileptic patients. Datasets were acquired from three patients suffering from severe epilepsy. The datasets of the epileptic patients were recorded during the day. We recorded 20 epileptic seizures.

Patients were asked to perform a sequence of everyday normal activities but were not told specially how to do them. Normal activities that we recorded included static activities such as reading, working with computer, brushing of teeth, and lying and dynamic activities such as walking. The sampling frequency of the accelerometer is 3 Hz. Figure 2 shows the pure output of accelerometers when sampling frequency is 3 Hz. It shows at first lying and then seizure signal. In this Figure the seizure has begun from 180 samples. Acceleration has been measured based on gravity (g=9.8m/s2)

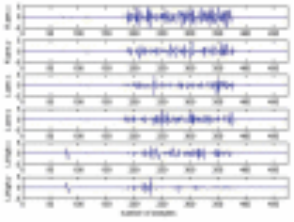


Figure 2

The pure output of accelerometers For analyzing and detecting seizures from this huge data sequence, the best way is cutting the acceleration sequences into many overlapping windows (segments) of the same length. For our data, the size of this window is considered 50 samples and it is repeated for every 25 samples. Since the sampling frequency is 3 Hz, we cut the data sequence every 9 seconds and analyzed this window of the ACM data to detect seizure. Figure 3 shows the acceleration data and overlapping window that located the signal.

The output of an accelerometer attached to the human body consists of different components:

Noise from sensor and measurement system

Noise sources from the environment: (a) accelerations produced by external sources like vehicles; (b) accelerations due to bumping of the sensor or the body against other objects

Noise sources from the body: (a) Muscle tremor; (b) Heart; (c) Respiration; (d) Blood flow

Gravitational acceleration

Acceleration due to movements of the body

In comparison to body movements, the noise from the sensor and measurement system can be neglected. All data used in this study were recorded while the patients were in their living environment, thus there were no accelerations produced by external sources.

When there is no movement, physiological perturbations, like respiration and heart rate and gravitational acceleration are visible in the signal. A preprocessing step is executed on the raw data for deleting these perturbations. To do that, we use a moving average filter. If the received signal is denoted as X(k), the filtered signal is given by following equation:

Where Xs(k) is the output of the filter. 2 L + 1 is the size of the sliding window expressed in the number of samples, the filter length. We introduce a delay of LT in the flow of data. In practice T = 1/3, so for L = 2, the delay is 0.6 seconds.

Feature Extraction

The selection of discriminative features is the basis of almost all detection algorithms. The choice for certain features is based on the physiological phenomena that need to be detected.[13] In this way we should extract the features that help us to detect seizures. We used three features as follows:

Variance measures the magnitude of a varying quantity in the signal. If xi = Xs(k), the variance of samples σ2i can be calculated by:

$$\sigma 2i=E\{|xi–\bar{x}\ i|2\}$$

Where $\bar{x}\ i = E\{xi\}$ is the average of samples

Correlation is calculated between the two axes of each accelerometer. The correlation Cij between x and y axes is given by:

$$Cij = E\{(xi–\bar{x}\ i)\}(yj–\bar{y}j)\}$$

Where xi and yj are ACM input signals of x and y axes , respectively, so $\bar{x}\ i = E\{xi\}$ and $\bar{y}i = E\{yi\}$ are its mean. Energy is the sum of the squared discrete FFT (Fast Furrier Transform) component magnitudes of the signal. If the length of window is N, discrete FFT component magnitudes Xk of the signal and its energy Es are given by:

Energy parameter is used to discriminate sedentary activities from other activities.

Choice of the Classifier

In our work, two classifiers were constructed to recognize seizure movements from daily activities. The first classifier is ANN and the second classifier is KNN.

ANN

The structure of the ANN classifier is shown in Figure 4. It consists of an input layer, a hidden layer, and an output layer u={u1,u2,…,ur}T and y={y1,y2,…,yh}T are the input and output vectors, respectively, where r represents the number of elements in the input feature set and h is the number of classes. Tangent sigmoid functions are selected as the activation functions *f* in the hidden and output neurons. In general, the back propagation learning algorithm (a gradient descent optimization method) is used to train the ANN. However, it is known that the gradient descent learning method is subject to slow convergence and local minima.[14]

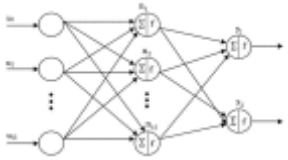


Figure 1 Structure of artificial neural network

Levenberg-Marquardt backpropagation is one of the best solutions for neural network training.[14] A multilayer perceptron with a hidden layer of 15 nodes and with Levenberg-Marquardt backpropagation as the training algorithm was used in the ANN classifier.

KNN

This rule classifies x by assigning it to the label which is the most frequently represented among the k nearest samples; in other words, the KNN query starts at the test point and grows a spherical region until it encloses k training samples, and labels the test point by a majority vote of these samples. The criterion of distance in KNN classification is the Euclidean distance that is given by the following equation.

dE=[(x–mi)T(x–mi)]½

where x is a test point and mi is a training sample.

Network Topology

There are several architectures that can be used to implement WSN applications, including star, mesh, and star-mesh hybrid. Each topology presents its own set of challenges, advantages, and disadvantages. The topology refers to the configuration of the hardware components and how the data are transmitted through that configuration.

XMesh is a full featured multi-hop, ad-hoc, mesh networking protocol developed by Crossbow,[15] for wireless network. An XMesh network consists of nodes that wirelessly communicate to each other and are capable of hopping radio messages to a base station where they are passed to a central server. The hopping effectively extends radio communication range and reduces the power required to transmit messages. By hopping data in this way, XMesh can provide two critical benefits: improved radio coverage and improved reliability. Two nodes do not need to be within direct radio range of each other to communicate. Xmesh provides to support both Zigbee standards (802.15.4) and advanced mesh networking. XMesh provides a TrueMesh networking service that is both self-organizing and self-healing. In Figure 5 is presented the diagram for XMesh network.

Figure 5

X Mesh network diagram

3.2 **Hardware Requirement**

We have implemented this system with our wireless sensor nodes, Motes, developed by Crossbow Technology. The device is built upon the IEEE 802.15.4 standard and has an 8-bit Atmel ATmega microcontroller. It uses the Chipcon CC2420, ZigBee ready radio frequency transceiver designed for low-power and low-voltage wireless communication in the 2.4 GHz unlicensed ISM band.[15]

For the purpose of seizure detection, we use MTS310 sensor board. MTS310 has a variety of sensing modalities including an accelerometer two-axis device. Figure 6 shows an MICAz Mote and an MTS310 sensor board.[16]

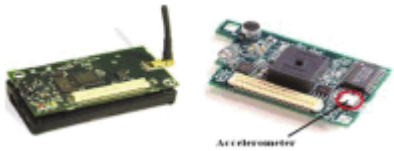


Figure 6

(a-b) MICAz mote, MTS310 sensor board

Locating the Patient

As mentioned above, the static nodes have an interface role between mobile sensor nodes and base-station. Also, location of each mobile node can be determined by the closest static node. So the location of static nodes must be chosen such that at any time, a mobile node connects to one and only one static node, since each mobile node is localized by the nearest static node. Although a large radio range for the nodes increases the power consumption and decreases the accuracy for localizing the mobile nodes, it helps to cover a building with fewer static nodes. So, we

should set a trade-off between the number of nodes and radio range for them.

We set the node's power on 316 μW. In this power, the radio range of nodes is 30 m in a line of sight area and we can cover a building using eight static nodes.

IV. APPLICATIONS

Smartphone application The Smartphone application can access the real time data provided by the accelerometer via the Bluetooth standard.The inertial data in terms of the windows is first captured, and then the features related to the window are calculated by the application which is capable of detecting the on-going seizures.For this,first the feature computation is performed,and second a threshold must be applied to this data to determine the occurrence of the seizure.The feature extraction steps include filtering of the received data,feature computation and feature reduction [13].The second step of seizure determination involves model parameters to be evaluated to judge the presence or absence of seizures.

The smartphone contains a domain specific Digital Signal Processing Module that is capable of performing feature extraction. But the signal needs to be pre-processed in the microcontroller unit itself before it is sent via Bluetooth to the smartphone.The pre-processing steps involve downconverting the frequency to about 10 Hz and reducing the window size to about 128 bytes.

The smartphone application must extract the frequency domain characteristics from the power spectral density of each window obtained using a 256 point Fast Fourier Transform[13].From this, the peak frequency value in the signal is determined .The smartphone application algorithm is then written to detect in case this determined peak frequency crosses the threshold value set to 10Hz.The decision making algorithm then sends an email notification via 3G/4G network to the emergency ward of the nearest hospital(whose location is determined by the GPS installed in the phone itself) along with the GPS location of the smartphone,thus calling for immediate care.

CONCLUSION

One of the most interesting applications of WSN is health monitoring. In this paper we introduced a monitoring system based on WSN for detection of epilepsy seizures. This system can be used for patients living in a clinical environment or at their home, where they do only their daily routine. Our system can determine the location of the patient when a seizure is detected and sends an alarm to hospital staff or the patient's relatives. Since our sensors are wireless, the subject under test can move without restrictions. In addition, because of the small size of the sensor nodes, they are wearable for patients. Our experimental results showed that 5 Nearest Neighbors provides better results than the ANN classifier. Furthermore, there is no need for training the algorithm for each new patient.

ACKNOWLEDGMENT

Any work would not be complete without the mention of the people whose guidance and encouragement lead to the development of the work. I consider myself privileged to express gratitude and respect towards all those who guided throughout my work.

I would like to express my gratitude to, **Dr. Bhagyashekar M.S**, Principal, Rajarajeswari College of Engineering, Bangalore, for their inspiration.

I am very proud and thankful to **Mrs. Usha Sakthivel**, Professor & HOD, Department of Computer Science and Engineering for his valuable advice and ideas at various stage of this work.

I thank my survey guide **Mrs. Bhagya Lakshmi D.N**, Asst. Professor, Department of Computer Science and Engineering, under whose able guidance this survey work has been carried out and completed successfully.

I extend my sincere thanks to the teaching and non-teaching staffs for their co-operation, for providing a very good infrastructure and all the kindness forwarded to me in carrying out this survey work in college.

I also thank my classmates and friends for their kind help in bringing out this survey work within the stipulated time. The report would be incomplete if I do not thank my parents and well-wishers for their moral support during this survey.

REFERENCES

1. https://pure.tue.nl/ws/files/3111794/200811448.pdf
2. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3788195/
3. https://pure.tue.nl/ws/files/3111794/200811448.pdf
4. Sandor Beniczky, TilmanPolster, Troels W. Kjaer, HelleHjalgrim, Detection of GTCS by a wireless wrist accelerometer: A prospective, multicentre study. [5] Sandor Beniczky, TilmanPolster, Troels W. Kjaer, HelleHjalgrim, Detection of GTCS by a wireless wrist accelerometer: A prospective, multicentre study.
[6] Lockman J, Fisher RS, Olson DM, Detection of seizurelike movements using a wrist accelerometer.
[7] Tamara M.E. Nijsen, Johan B.A.M Arends, Paul A.M. Griep, Pierre J.M Cluitmans, The potential value of three-dimensional accelerometry for detection of motor seizures in severe epilepsy.
[8] Fisher R, van Emde Boas W, Blume W, Elger C, Genton P, Lee P, Engel J, Epileptic seizures and epilepsy: definitions proposed by the ILAE and IBE.
[9] Witte H, Iasemidis LD, Litt B. Special issue on epileptic seizure prediction. IEEE Trans Biomed Eng. 2005;50:537–9.

[10] Binnie CD, Aarts JH, Van Bentum-De Boer PT, Wisman T. Monitoring at the institute for epilepsy fight in Bosch. Electroencephalogr and Clin Neurophysiol Suppl. 1985;37:341–55. [PubMed]
[11] Mathie MJ, Celler BG, Lovell NH, Coster AC. Classification of basic daily movements using a triaxial accelerometer. Med Biol Eng Comput. 2004;42:679–87. [PubMed]
[12] Veltink P, Bussmann HB, de Vries W, Martens WL, Van Lummel RC. Detection of static and dynamic activities using uniaxial accelerometers. IEEE Trans Rehabil Eng. 1996;4:375–85. [PubMed]

Secure, Efficient and Dynamic Multi-keyword Ranked Search over Encrypted Cloud Data

Renuka H N[1], Dr. Malathy[2]
[1] PG Scholar, [2]Associate.Prof, Dept.CSE, RRCE
E-Mail: renuka.hk99@gmail.com, anandanmalathy@gmail.com

Abstract: Due to increasing popularity of cloud computing, most of the data owners are motivated to outsource their data to the cloud servers for great convenience and low cost in data management. However, sensitive data must encrypted before outsourcing for the privacy requirements, which obsoletes data utilization like keyword-based document retrieval. We presented a secure, efficient and dynamic multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations such as deletion and insertion of documents. Specifically, the vector space model and the TFIDF model are combined in the index construction and query generation. We had constructed a special tree-based index structure and we propose a "Greedy Depth-first Search" algorithm to provide efficient and robust multi-keyword ranked search. The Robust KNN algorithm is utilized to encrypt the index and query vectors, and meantime, ensure accurate relevance score calculation between query vectors and encrypted index. In order to resist statistical attacks, phantom terms were added to the index vector for blinding search results. Due to the use of special tree-based index structure, the proposed scheme we can achieve sub-linear search time and we can deal with the deletion and insertion of documents flexibly. Repeated experiments are conducted to demonstrate the efficiency of the proposed scheme.

Index Terms— cloud computing, dynamic update, multi-keyword ranked search, Searchable encryption.

I. INTRODUCTION

Cloud computing has been considered as a new model of enterprise IT infrastructure, which can organize huge resource of computing, applications and storage, and enable users to enjoy pervasive, convenient and on-demand network access to a shared pool of resources with great efficiency and minimal economic overhead. Attracted by these appealing features, both enterprises and individuals are motivated to outsource their data to the cloud, instead of purchasing software and hardware to manage the data themselves.

The cloud service providers (CSPs) that keep the data to access end-users sensitive data without authorization. A general approach to protect the data confidentiality is to encrypt the data before outsourcing. Yet, this will cause a huge cost in terms of data usability. For example, keyword-based information retrieval is widely used on the plaintext data, cannot be directly applied on the encrypted data. Download all the data from cloud and decrypt locally is obviously impractical.We proposes a secure tree-based search scheme over the encrypted cloud data, which supports dynamic operation and multi-keyword ranked search on the document collection. In order to obtain high search efficiency, we construct a index structure i.e tree-based and we propose a "Greedy Depth-first Search" algorithm based on index tree. Due to the special structure of tree-based index, the proposed search scheme can flexibly achieve sub-linear search time and deal with the insertion and deletion of documents. The Robust KNN algorithm is utilized to encrypt the query vectors and index, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist different attacks in different threat models, we had constructed two secure search schemes: (i) the basic dynamic multi-keyword ranked search (BDMRS) scheme in cipher text model, and (ii) the enhanced dynamic multi-keyword ranked search (EDMRS) scheme in the known background model. Our contributions are mentioned as follows:

1) We designed a searchable scheme that supports both the accurate multi-keyword ranked search and flexible dynamic operation on document collection.

2) In the special structure of tree-based index, the search complexity of the proposed scheme is basically kept to logarithmic. And the proposed scheme can achieve better search efficiency by executing "Greedy Depth-first Search" algorithm. Furthermore, parallel search can be flexibly performed to further reduce the time cost of search process.

II. PROBLEM FORMULATION

Vector space model with TF×IDF rule is widely used in plaintext data retrieval that efficiently supports ranked multi-keyword search. The term frequency (TF) is the number of times a given term (keyword) appears within a document, and the reverse document frequency (IDF) is get through dividing the cardinality of document collection by the number of documents containing the keyword. The vector space model enotes each document by a vector, whose elements are the normalized TF values of keywords in that document.

The System and Threat Models:

The system model involves three different entities: (i)data owner, (ii) data user and (iii) cloud server,. Data owner has a collection of documents that wants to be outsource

to the cloud server in encrypted form. In this scheme, the data owner first builds a secure searchable tree index I from document collection F , later generates an encrypted document collection C for F . After that the data owner outsources the secure index I and the encrypted collection C and to the cloud server, and securely distributes the trapdoor key information generation and the document decryption to the authorized data end-users. Once the Data users are authorized to access the documents of data owner. With the use of 't' query keywords, authorized user can generate a trapdoor TD according to the search control mechanisms to fetch 'k' encrypted documents from cloud server. Later, the data user can decrypt the documents with the shared secret key. Cloud server stores the encrypted searchable tree index I and the encrypted document collection C and for data owner.

Cloud server is considered as "honest-but-curious" in the proposed scheme, which is employed by lots of works on secure cloud data search. Explicitly, the cloud server correctly and honestly executes the instructions in the designated protocol. Meantime, it is curious to infer and analyze the received data, which helps it to acquire additional information. We adopt the two threat models depending on what information the cloud server knows, the Known Cipher text Model. In this model, the cloud server only knows the searchable index tree I, the encrypted document collection C and the search trapdoor TD sent by the authorized user. That means the cloud server can conduct "cipher text-only attack" in this model. Known Background Model is Compared with the known cipher text model, the cloud server in this stronger model is equipped with more and more knowledge, like term frequency (TF) statistics of the document collection. The statistical information records how many documents are there for each term frequency of a specific keyword in the whole document collection. which could be used as the keyword identity. Equipped with such statistical information, the cloud server can conduct TF statistical attack to reduce or even identify some keywords through analyzing histogram and value range of the corresponding frequency distributions.

Design Goals

To enable secure, robust, efficient, dynamic and accurate multi-keyword ranked search over outsourced encrypted cloud data under the above said models, our system has the below design goals.

Dynamic: Our proposed scheme is designed to provide not only accurate result ranking and multi-keyword query, but also dynamic update on document collections. In the Search Efficiency: The scheme is aims to achieve sub-linear search efficiency by exploring efficient search algorithm and a special tree-based index and an. In the Privacy-preserving: Our scheme is designed to prevent the cloud server from learning additional information about the index tree, the document collection, , and the query. The specific privacy requirements are mentioned as follows:

1) Query Confidentiality and Index Confidentiality: The underlying plaintext information, including key-words in the query and index, key-words TF values are stored in the index, and IDF values of query keywords, should be protected from cloud server;

2) Trapdoor Unlink ability: The cloud server should not be able to determine whether two encrypted queries are generated from the same search request;

3) Keyword Privacy: The cloud server could not identify the specific keyword in index, query, or document collection by analyzing the statistical information like term frequency. Our proposed scheme is not designed to protect access pattern, i.e., the sequence of returned documents.

III. THE PROPOSED SCHEME

We first describe the "unencrypted dynamic multi-keyword ranked search" (UDMRS) scheme which is constructed on basis of vector space model and KBB tree. Based on UDMRS scheme, two secure search schemes such as BDMRS and EDMRS schemes are constructed against two threat models.

3.1 Index Construction of UDMRS Scheme

We briefly introduced the KBB index tree structure, which guide us in introducing the index construction. In the process of index construction, first we generate a tree node for each document in the collection. These nodes are the leaf nodes of the index tree. Later, the internal tree nodes are generated based on these leaf nodes.

3.2 Search Process of UDMRS Scheme

In the UDMRS scheme the search process is a recursive procedure over the tree, known as "Greedy Depth-first Search (GDFS)" algorithm. We constructed a result list denoted as RList, whose element is explained as RScore; FID. Here, the RScore is the relevance score of document 'f' FID to the query, which is calculated. The RList stores the 'k' accessed documents with largest relevance scores to the query. The elements of the list are ranked in descending order according to RScore, and will be timely updated during the search process.

IV. PERFORMANCE ANALYSIS

We implemented our proposed scheme using C++ language in Windows 8 operation system and test its robustness and efficiency on a real-world document collection: Request for Comments (RFC). The experiment includes 1)Search precision on different privacy level. 2) the efficiency of index construction, trapdoor generation, searching, and updating. Most of our experimental results are obtained with an Intel Core(TM) Duo Processor (2.93 GHz), except that the efficiency of search is tested on a server with two Intel(R) Xeon(R) CPU E5-2620 Processors (2.0 GHz), which has 12 processor cores and supports 24 parallel threads.

Precision and Privacy

The search precision of the scheme is affected by dummy keywords in EDMRS scheme. Here, the 'precision' is defined as : Pk = k=k, where 'k' is the num of real top-k documents in the retrieved 'k' documents. If a smaller standard deviation is set for the random

Efficiency: Index Tree Construction

The index tree construction process for document collection F includes two steps: i) building an unencrypted KBB tree based on the document collection F , and ii) encrypting the index tree with splitting operation and two multiplications of a (m × m) matrix. The index structure can be constructed by following a post order traversal of the tree based on the document collection F, O(n) nodes are generated during the traversal. For each node, generation of an index vector takes O(m) time, vector splitting process takes O(m) time, and two multiplications of a (m×m) matrix takes O(m 2) time. Overall, the time complexity for index tree construction is O(nm 2). Evidently, the time cost for building index tree depends on the cardinality of document collection F and the number of keywords in dictionary W.

The time cost of index tree construction is almost linear with the size of document collection, and it is proportional to number of keywords in the dictionary. Because of dimension extension, the index tree construction of EDMRS scheme is little bit more time-consuming than BDMRS scheme. However, the index tree construction consumes relatively much time at the data owner side, it is significant that this is a one-time operation. On the other hand, since the underlying balanced binary tree has space complexity" O(n) and every node stores two m-dimensional vectors, the space complexity of the index tree is O(nm). When the document collection is fixed i.e n = 1000, the storage consumption of the index tree is determined by the size of the dictionary.

Trapdoor Generation

The generation of trapdoor includes vector splitting operation and two multiplications matrix (m × m). So, the time complexity is O(m2). Usually typical search requests consist of just a few keywords. Number of query keywords has bit influence on the overhead of trapdoor generation when dictionary size is fixed. Because of the dimension extension, the time cost of EDMRS scheme is a bit higher than BDMRS scheme.

Search Efficiency

In the search process, if relevance score at node 'u' is larger than the minimum relevance score in the result list RList, then cloud server examines the children of that node; or else it returns. So, lot of nodes is not accepted during a real search. We are denoting the number of leaf nodes that contain one or more keywords in the query. Usually, the number of leaf nodes is larger than the number of required documents k, but far-less than cardinality of the document collection n.

The real search time is less than m log n. That is because of: i) many leaf nodes contain the queried keywords are not visited according to the search algorithm. ii) The accessing paths of some different leaf nodes shares mutual traversed parts. Additionally, the parallel execution of search process can increase the efficiency a lot.

We examine the search efficiency of proposed scheme on the server that supports 24 parallel threads. The search performance is tested by starting 1, 4, 8 and 16 threads. We compared the search efficiency of our proposed scheme with that of Sun et al.. In the implementation of Sun's code, we divide 4000 keywords into 50 levels. So, each level contains 80 keywords. Accordingly, the higher level the query keywords reside, higher the search efficiency is. In our system, we chose ten keywords from 1st level for search efficiency comparison.

An intuitive method to handle this problem is to construct multiple result lists. However, in our scheme, it will not help to improve the search efficiency a lot. It is because that we need to find k results for each result list and time complexity for retrieving each result list is O(m log n=l). In this case, the multiple threads will not save much time, and selecting k results from the multiple result list will further increase the time consumption. We show the time consumption when we start the multiple threads with multiple result lists.

CONCLUSION

We are proposing a secure, robust, efficient and dynamic search scheme that supports not only the accurate multi-keyword ranked search but also the dynamic insertion and deletion of documents. We constructed a special keyword balanced binary tree as index and proposed a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search. Additionally, the parallel search process can be carried out to reduce the time cost. Security of the scheme is protected against two threat models by making use of the secure KNN algorithm. Experimental results demonstrate the efficiency of our proposed scheme.

REFERENCES

1] K. Ren, C. Wang, Q. Wang et al., "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.

[3] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simula-tion on oblivious rams," Journal of the ACM (JACM), vol. 43, no. 3, pp. 431–473, 1996.
[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.
[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp. 50–67.
[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.
[8] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
[9] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proceedings of the Third in-ternational conference on Applied Cryptography and Network Security. Springer-Verlag, 2005, pp. 442–455.
[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient con-structions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.
[11] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–5.
[12] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Data Engineering (ICDE), 2012 IEEE 28th International Conference on. IEEE, 2012, pp. 1156–1167.
[13] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 451–459.
[14] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, 2014.
[15] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.
[16] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunc-tive keyword search and its extension to a multi-user system," in Proceedings of the First international conference on Pairing-Based Cryptography. Springer-Verlag, 2007, pp. 2–22.
[17] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient con-junctive keyword searches over encrypted data," in Proceedings of the 7th international conference on Information and Communications Security. Springer-Verlag, 2005, pp. 414–426.
[18] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proceedings of the 4th conference on Theory of cryptography. Springer-Verlag, 2007, pp. 535–554.

Secure Data Aggregation Technique for Wireless Sensor Network In The Presence Of Collusion Attack

Arpitha J[1], Varsha K[2], Naveen Gowda K[3], Mahantesh Matapathi[4]
Dept. of CSE, ACS College of Engineering, Bangalore
E-Mail:arpitha.j14@gmail.com, varshak568@gmail.com, navidon.k143@gmail.com, manteshkrishna@gmail.com

Abstract—Sensor nodes in wireless sensor network have very limited energy resources.Using simple averaging method data aggregation from multiple sensor nodes is done by aggrgatingnode.But in such aggregation node are at high risk for compromising attacks.Iterative filtering algorithm hold great promise to make sure trustworthiness of data and reputation of sensor nodesmaking WSN less risk of attack.In this algorithm data are assigned weight factors that can help in simultaneous data aggregation from many sources and provide trust assessment. Here we propose enhanced iterative algorithm to address security issue.

I. INTRODUCTION

Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. This cannot be remedied by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus, better, more sophisticated algorithms are needed for data aggregation in the future WSN. Such an algorithm should have two features.

1. In the presence of stochastic errors such algorithm should produce estimates which are close to the optimal ones in information theoretic sense. However, such estimation should be achieved without supplying to the algorithm the variances of the sensors, unavailable in practice.
2. The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data, such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node.
3. A trustworthiness assessment at any given moment represents an aggregate of the behavior of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behavior. There are a number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation can severely impair the performance of such a system. The main target of malicious attackers is aggregation algorithms of trust and reputation systems.

Sensors deployed in hostile environments may be subject to node compromising attacks by adversaries who intend to inject false data into the system. In this context, assessing the trustworthiness of the collected data becomes a challenging task. WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms; an example is the recent emergence of multi-core and multi-processor systems in sensor nodes. Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems—data aggregation and data trustworthiness assessment—using a single iterative procedure. Such trustworthiness estimate of each sensor is based on the distance of the readings of such a sensor from the estimate of the correct values, obtained in the previous round of iteration by some form of aggregation of the readings of all sensors. Such aggregation is usually a weighted average; sensors whose readings significantly differ from such estimate are assigned less trustworthiness and consequently in the aggregation process in the present round of iteration their readings are given a lower weight. In recent years, there has been an increasing amount of literature on IF algorithms for trust and reputation systems. The performance of IF algorithms in the presence of different types of faults and simple false data injection attacks has been studied, for example in where it was applied to compressive sensing data in WSNs. In the past literature it was found that these algorithms exhibit better robustness compared to the simple averaging techniques; however, the past research did not take into account more sophisticated collusion attack scenarios. If the attackers have a high level of knowledge about the aggregation algorithm and its parameters, they can conduct sophisticated attacks on WSNs by exploiting false data injection through a number of compromised nodes. This paper presents a new sophisticated collusion attack scenario against a number of existing IF algorithms based on the false data injection. In such an attack scenario, colluders attempt to skew the aggregate value by forcing such IF algorithms to converge to skewed values provided by one of the attackers. Although such proposed attack is applicable to a broad range of distributed systems, it is particularly dangerous

once launched against WSNs for two reasons. First, trust and reputation systems play critical role in WSNs as a method of resolving a number of important problems, such as secure routing, fault tolerance, false data detection, compromised node detection, secure data aggregation, cluster head election, outlier detection, etc.,

Second, sensors which are deployed in hostile and unattended environments are highly susceptible to node compromising attacks . While offering better protection than the simple averaging, our simulation results demonstrate that indeed current IF algorithms are vulnerable to such new attack strategy. In this paper, we propose a solution for such vulnerability by providing an initial trust estimate which is based on a robust estimation of errors of individual sensors. When the nature of errors is stochastic, such errors essentially represent an approximation of the error parameters of sensor nodes in WSN such as bias and variance. However, such estimates also prove to be robust in cases when the error is not stochastic but due to coordinated malicious activities. Such initial estimation makes IF algorithms robust against described sophisticated collusion attack, and, we believe, also more robust under significantly more general circumstances; for example, it is also effective in the presence of a complete failure of some of the sensor nodes. This is in contrast with the traditional non iterative statistical sample estimation methods which are not robust against false data injection by a number of compromised nodes [18] and which can be severely skewed in the presence of a complete sensor failure. Since readings keep streaming into aggregator nodes in WSNs, and since attacks can be very dynamic (such as orchestrated attacks [4]), in order to obtain trustworthiness of nodes as well as to identify compromised nodes we apply our framework on consecutive batches of consecutive readings. Sensors are deemed compromised only relative to a particular batch; this allows our framework to handle on-off type of attacks (called orchestrated attacks in [4]). Our simulation results illustrate that our robust aggregation technique is effective in terms of robustness against our novel sophisticated attack scenario as well as efficient in terms of the computational cost. Our contributions can be summarized as follows:

1. Identification of a new sophisticated collusion attack against IF based reputation systems which reveals a severe vulnerability of IF algorithms

2. A novel method for estimation of sensors' errors which is effective in a wide range of sensor faults and not susceptible to the described attack

3. Design of an efficient and robust aggregation method inspired by the MLE, which utilizesan estimate of the noise parameters, obtained using contribution 2 above.

4. Enhanced IF schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs from contributions 2 and 3 above.

II. BACKGROUND, ASSUMPTIONS THREAT MODEL AND PROBLEM STATEMENT

In this section, we present our assumptions, discuss IF algorithms, describe a collusion attack scenario against IF algorithms, and state the problems that we address in this paper.

Network Model

For the sensor network topology, we consider the abstract model proposed by Wagner in [20]. Fig. 1 shows our assumption for network model in WSN. The sensor nodes are divided into disjoint clusters, and each cluster has a cluster head which acts as an aggregator. Data are periodically collected and aggregated by the aggregator. In this paper we assume that the aggregator itself is not compromised and concentrate on algorithms which make aggregation secure when the individual sensor nodes might be compromised and might be sending false data to the aggregator. We assume that each data aggregator has enough computational power to run an IF algorithm for data aggregation.

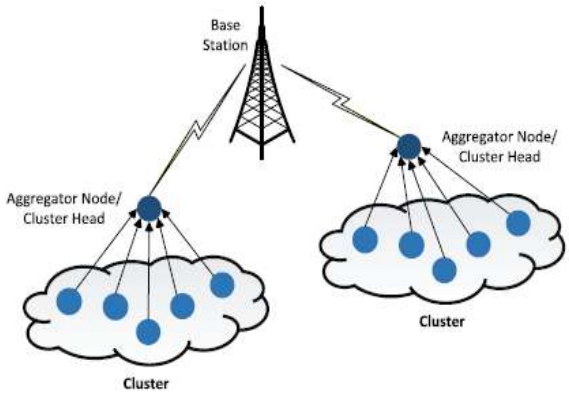


Fig.1. Network model of WSN.

Iterative Filtering in Reputation Systems

Kerchove and Van Dooren proposed in [8] an IF algorithm for computing reputation of objects and raters in a rating system. We briefly describe the algorithm in the context of data aggregation in WSN and explain the vulnerability of the algorithm for a possible collusion attack. We note that our improvement is applicable to other IF algorithms as well. We consider a WSN with n sensors Si, i = 1;...;n. We assume that the aggregator works on one block of readings at a time, each block comprising of readings at mconsecutive instants. Therefore, a block of readings is represented by a matrix X={x1,x2.....xn} where xi=[x1,x2….xm] represents the ithm -dimensional reading reported by sensor node Si. Let r=[r1 r2 ... rm]^T denote the aggregate values for instants t = 1,...m, which authors of [8] call a reputation vector,2 computed iteratively and simultaneously with a sequence of weights w=[w1,w2….wn]^T reflecting the trustworthiness of sensors. We denote by $r^{(1)}$,$w^{(1)}$ the approximations of r; w obtained at lth round of iteration (l>=0). The iterative procedure starts with giving equal credibility to all

sensors, i.e., with an initial value $w^{(0)}= 1$. The value of the reputation vector $r^{(l+1)}$ in round of iteration l+1 is obtained from the weights of the sensors obtained in the round of iteration l as $r^{(l+1)} = X.w^{(l)} / w(i)$: Algorithm 1 illustrates the iterative computation of the reputation vector based on the above formulas.

ALGORITHM 1: iterative filtering algorithm.

INPUT: X,n,m

OUTPUT: The reputation vector r

l←0;

$w^{(0)}$ ←1;

REPEAT:

Compute $r^{(l+1)}$;Type equation here.

Compute d;

Compute $w^{(l+1)}$;

l←l+1;

Until reputation has converged;

A. Adversary Model

In this paper, we use a Byzantine attack model, where the adversary can compromise a set of sensor nodes and inject any false data through the compromised nodes . We assume that sensors are deployed in a hostile unattended environment. Consequently, some nodes can be physically compromised. We assume that when a sensor node is compromised, all the information which is inside the node becomes accessible by the adversary. Thus, we cannot rely on cryptographic methods for preventing the attacks, since the adversary may extract cryptographic keys from the compromised nodes. We assume that through the compromised sensor nodes the adversary can send false data to the aggregator with a purpose of distorting the aggregate values. We also assume that all compromised nodes can be under control of a single adversary or a colluding group of adversaries, enabling them to launch a sophisticated attack. We also consider that the adversary has enough knowledge about the aggregation algorithm and its parameters. Finally, we assume that the base station and aggregator nodes cannot be compromised in this adversary model; there is an extensive literature proposing how to deal with the problem of compromised aggregators; in this paper we limit our attention to the lower layer problem of false data being sent to the aggregator by compromised individual sensor nodes, which has received much less attention in the existing literature.

Collusion Attack Scenario

Most of the IF algorithms employ simple assumptions about the initial values of weights for sensors. In case of our adversary model, an attacker is able to mislead the aggregation system through careful selection of reported data values. We use visualization techniques from to present our attack scenario.

Assume that 10 sensors report the values of temperature which are aggregated using the IF algorithm proposed in with the reciprocal discriminant function. We consider three possible scenarios;

In scenario 1, all sensors are reliable and the result of the IF algorithm is close to the actual value.

In scenario 2, an adversary compromises two sensor nodes, and alters the readings of these values such that the simple average of all sensor readings is skewed towards a lower value. As these two sensor nodes report a lower value, IF algorithm penalizes them and assigns to them lower weights, because their values are far from the values of other sensors. In other words, the algorithm is robust against false data injection in this scenario because the compromised nodes individually falsify the readings without any knowledge about the aggregation algorithm.

In scenario 3, an adversary employs three compromised nodes in order to launch a collusion attack. It listens to the reports of sensors in the network and instructs the two compromised sensor nodes to report values far from the true value of the measured quantity. It then computes the skewed value of the simple average of all sensor readings and commands the third compromised sensor to report such skewed.

III. ROBUST DATA AGGREGATION

In this section, we present our robust data aggregation method.

A. Framework Overview

In order to improve the performance of IF algorithms against the afore mentioned attack scenario, we provide arobust initial estimation of the trustworthiness of sensornodes to be used in the first iteration of the IF algorithm. Most of the traditional statistical estimation methods for variance involve use of the sample mean. For this reason, proposing a robust variance estimation method in the case of skewed sample mean is an essential part of our methodology. In the remainder of this paper, we assume that the stochastic components of sensor errors are independent random variables with a Gaussian distribution; however, our experiments show that our method works quite well for other types of errors without any modification. Moreover, if error distribution of sensors is either known or estimated, our algorithms can be adapted to other distributions to achieve an optimal performance. Fig. 2 illustrates the stages of our robust aggregation framework and the interconnections. As we have mentioned,our aggregation method operates on batches of consecutive readings of sensors, proceeding in several stages.In the first stage we provide an initial estimate of two noiseparameters for sensor nodes, bias and variance.Based on such an estimation of the bias and variance ofeach sensor, the bias estimate is subtracted

from sensorsreadings and in the next phase of the proposed framework, we provide an initial estimate of the reputation vector calculatedusing the MLE. In the third stage of the proposed framework, the initialreputation vector provided in the second stage is used toestimate the trustworthiness of each sensor based on thedistance of sensor readings to such initial reputation vector.

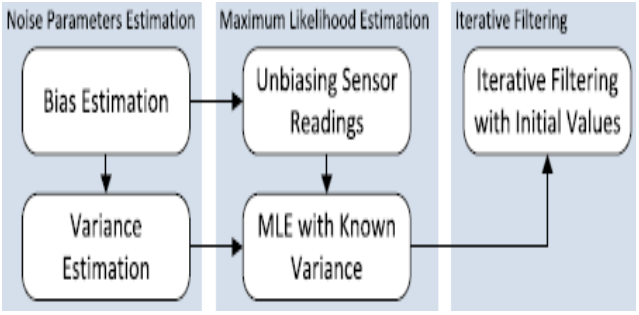


Fig.2.Our robust data aggregation framework.

B. Enhanced Iterative Filtering

According to the proposed attack scenario, the attacker exploits the vulnerability of the IF algorithms which originates from a wrong assumption about the initial trustworthiness of sensors. Our contribution to address this shortcomings is to employ the results of the proposed robust data aggregation technique as the initial reputation for these algorithms. Moreover, the initial weights for all sensor nodes can be computed based on the distance of sensors readings to such an initial reputation. Our experimental results illustrate that this idea not only consolidates the IF algorithms against the proposed attack scenario, but using this initial reputation improves the efficiency of the IF algorithms by reducing the number of iterations needed to approach a stationary point within the prescribed tolerance.

IV. ACCURACY WITH COLLUSION ATTACK

In order to illustrate the robustness of the proposed dataaggregation method in the presence of sophisticated attacks, we synthetically generate several data sets by injecting the proposed collusion attacks. Therefore, we assume that the adversary employs c (c < n) compromised sensor nodes to launch the sophisticated attack scenario proposed in Section 2.4. The attacker uses the first c - 1 compromised nodes to generate outlier readings in order to skew the simple average of all sensor readings. The adversary then falsifies the last sensor readings by injecting the values very close tosuch skewed average. This collusion attack scenario makes the IF algorithm to converge to a wrong stationary point. In order to investigate the accuracy of the IF algorithms with this collusion attack scenario, we synthetically generate several data sets with different values for sensors variances as well as various number of compromised nodes (c). the collusion attack scenariocan circumvent all the IF algorithms . Moreover, the accuracy of the algorithms dramatically decreases byincreasing the number of compromised nodes participated in the attack scenario. As explained before, the algorithms converge to the readings of one of the compromised nodes, namely, to the readings of the node which reports values very close to the skewed mean. This demonstrates that an attacker with enough knowledge about the aggregation algorithm employed can launch a sophisticated collusion attack scenario which defeats IF aggregation systems.

V. ACCURACY WITH SIMPLE ATTACK SCENARIO

An attack scenario against traditionalstatistical aggregation approaches. We described thescenario in Section 2.4 and the second round of Fig. 2 as asimple attack scenario using a number of compromisednode for skewing the simple average of sensors readings. Inthis section, we investigate the behavior of IF algorithmsagainst the simple attack scenario. Note that the objective ofthis attack scenario is to skew the sample mean of sensorsreadings through reporting outlier readings by the compromisednodes.

In order to evaluate the accuracy of the IF algorithms against the simple attack scenario, we assume that the attacker compromises c(c < n) sensor nodes and reportsoutlier readings by these nodes. We generate syntheticallydata sets for this attack scenario by taking into account differentvalues of variance for sensors errors as well asemploying various number of compromised nodes. Moreover, We generate biased readings for all sensor nodes withbias provided by a random variable with a distribution$N(0, \alpha^2_b)\alpha^2_b$ with the variance of bias chosen to be α^2_b.=4

CONCLUSION

In this paper, we introduced a novel collusion attack scenario against a number of existing IF algorithms. Moreover, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging. In future work, We will investigate whether our approach can protect against compromised aggregators. we also plan to implement our approach in a deployed sensor network.

REFERENCES

[1] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," *Comput. Netw.,*vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] L. Wasserman, All of Statistics : A Concise Course in Statistical Inference.New York, NY, USA: Springer,.

[3] A. Jøsang and J. Golbeck, "*Challenges for robust trust and reputation systems," in Proc. 5th Int. Workshop Security Trust Manage.,*
Saint Malo, France, 2009, pp. 253–262.

[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surveys, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.

[5] R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, "Trust and reputation systems for wireless sensor networks," in Security and Privacy in Mobile and Wireless Networking, S. Gritzalis, T. Karygiannis, and C. Skianis, eds.,Leicester, U.K.:Troubador Publishing Ltd, 2009 pp. 105–128,.
[6] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proc. 7th Int. Workshop
Data Manage. Sensor Netw., 2010, pp. 2–7.
[7] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN,"in Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput., 2011, pp. 1–4.
[8] C. de Kerchove and P. Van Dooren, "*Iterative filtering in reputation systems*," SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.
[9] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," Europhys.Lett., vol. 94, p. 48002, 2011.
[10] P. Laureti, L. Moret, Y.-C.Zhang, and Y.-K. Yu, "Information filtering via iterative refinement," Europhys.Lett., vol. 75, pp. 1006– 1012, Sep. 2006.
[11] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding information from noisy, redundant, and intentionally distorted sources," Physica A: Statist. Mech. Appl., vol. 371, pp. 732–744, Nov. 2006.
[12] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputation based ranking on bipartite rating networks," in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.

Performance Evaluation of Aodv and Lar with 802.15.4 Standard

Akshaya.T.M[1], Bhagya Lakshmi.D.N[2],

[1] Asst. Professor, Dept of EEE, East West College Of Engineering, [2]Software Engineer, EDAYN Software Pvt. Ltd,

akshayag55@gmail.com, connect.bhagya@gmail.com

Abstract: Wireless Sensor Networks (WSN) play a key role in sensing, computing and communicating the information in most of the fields bringing substantial improvements in a broad spectrum of modern technologies. Data to be routed from source to destination is very difficult in WSN due to the mobility of the network elements and lack of central administration. In this paper an attempt has been made to evaluate the performance of reactive routing protocols, Ad-hoc On-demand Distance Vector routing(AODV) and Location aided routing(LAR) for the wireless sensor nodes(IEEE 802.15.4 standard). The performance of routing protocol is analyzed using various metrics like total packets received, average end-to-end delay, total bytes received using Qualnet 5.2 simulator.

Keywords-WSN, AODV,LAR,end to end Delay, bytes received, PDR, throughput, IEEE 802.15.4 standard, Reactive routing, Qualnet 5.2.

I. INTRODUCTION

Advances in micro-electro-mechanical systems, digital electronics and wireless communications have led to the emergence of inexpensive wireless communication, computation and sensing devices called wireless sensor nodes [1]. Tens and thousands of these nodes cooperatively organizing themselves will constitute Wireless sensor networks (WSN) and this again develops an important and exciting new technology with great potential for improving many current applications as well as creating new revolutionary systems. This will potentially affect all aspects of our lives, bringing about substantial improvements in a broad spectrum of modern technologies ranging from battlefield surveillance, environmental monitoring, biological detection, smart spaces, disaster search and rescue, industrial diagnostics, sensing a building integrity or structural vibrations during an earthquake, the stress of an airplane's wings, are some of the applications where WSN [2,3] promise to change how researchers gather their data. Routing is the process of selecting paths in a network along which to send network traffic. Routing protocols can be classified as Proactive or table driven routing protocols, on-demand routing protocols and hybrid routing protocol. In this paper performance evaluation of AODV and LAR routing protocols are carried out for node densities 20,40,60,80 and 100 stationary and nodes with mobility speed of 20mps.

A. Reactive Routing Protocol

Reactive routing Protocol is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Adhoc On-demand Distance Vector routing (AODV) and Location aided routing (LAR) etc.

i) Ad-hoc On-demand Distance Vector routing protocol (AODV):

The AODVrouting protocol [4] is a reactive routing protocol; therefore, routes are determined only when needed. Figure 1 illustrates the message exchanges of the AODV protocol.

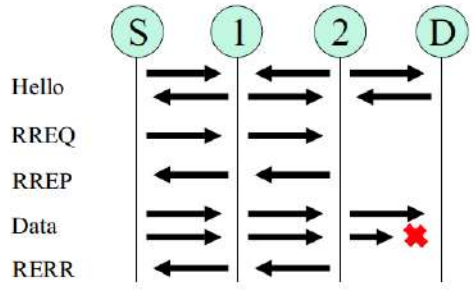


Fig.1.AODV Protocol Messaging

Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. When a RREQ is received by an intermediate node, a route to the source is created. If the receiving node has not received the RREQ [5] before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ.

If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by-hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source

receives the RREP, it records the route to the destination and begins sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. If data is flowing and a link break is detected, a Route Error (RERR) message is sent to the source of the data in a hop-by-hop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery, if necessary.

1.1.1 Location Aided Routing (LAR):

Location aided routing [6], is an enhancement to flooding algorithms to reduce flooding overhead.

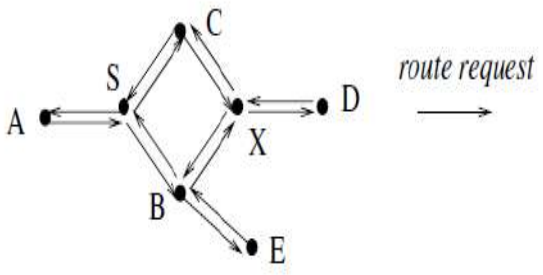


Fig.2 Illustration of flooding in LARRoute Discovery Using Flooding.

Figure.2. illustrates LAR algorithm. In this figure, node S needs to determine a route to node D. Therefore, node S broadcasts a route request to its neighbors. When nodes B and C receive the route request, they forward it to all their neighbors. When node X receives the route request from B, it forwards the request to its neighbors. However, when node X receives the same route request from C, node X simply discards the route request.

Most of the on-demand routing protocols including DSR and AODV use flooding to obtain a route to the destination. LAR aims to reduce the overhead to send the route requests only into a specific area, which is likely to contain the destination. For this purpose the notions of expected zone and request zone are introduced. The expected zone covers the area in which the destination is expected. Since the expected zone need not contain the source node, a larger area must be covered by flooding. This expanded expected zone is called request zone and is used to restrict the flooding; i.e. only nodes that are part of the request zone can forward a route request. On unsuccessful route discoveries, the request zone may need to be expanded further, possibly covering the whole network. Such subsequent route requests increase the initiallatency for connections. This results in a tradeoff between reduced overhead and increased latency which needs to be balanced carefully.

II. RELATED WORK

A number of wireless routing protocols are already proposed to provide communication in wireless environment using open source simulators.In the paper [7] four routing protocols AODV, TORA [8], DSDV and DSR are compared using ns-2. It is shown through simulation results that DSR generates less routing load than AODV. AODV suffers from end to end delay while TORA has very high routing overhead.Performance comparison of AODV and DSR routing protocols in a constrained situation is done using GolMoSim by R. Misra et.al. The authors claim that the AODV outperforms DSR in normal situation but in the constrainedsituation DSR outperforms AODV, where the degradation is as severe as 30% in AODV whereas DSR degrades marginally as 10%.A comparison of Link State, AODV and DSR protocols for two different traffic classes, in a selected environment is done. It is claimed that AODV and DSR perform well when the network load is moderate and if the traffic load is heavy then simple Link State outperforms the reactive protocols.

There are several other efforts related to the work under study. In the work of Perkins, Royer, Samir.R. Das and Manesh, evaluation of DSR and AODV using nS-2 network simulator for 50 and 100 nodes in a rectangular space was studied. The traffic and mobility models they used are the ones incorporated into nS-2 include ZRP, neither had they tried to find the impact of specific attributes of DSR or AODV in network performance. The mobility models were not different but instead they used a uniform distributed speed of nodes between 0-20 m/sec. in various mobility scenarios since the nodes move in a mean 10m/sec speed. Another relative work has been presented by Broch, Maltz, Johnson, Hu, and Jetcheva. They evaluated four ad-hoc routing protocols including AODV and DSR. They also used nS-2 to simulate 50-node network models with mobility and traffic scenarios similar to the scenarios Perkins et al did. On the other hand in this paper an exponentially distributed packet size of 512 bytes are used which makes the comparison fair between DSR and LAR.

In this paper an effort is made to compare the performance evaluation of on-demand reactive protocols AODV and LAR for IEEE 802.15.4standard (WSN), withvarious node densities for stationary and mobile nodes using Qualnet5.2 network simulator [9].

III.SIMULATIONSCENARIO

Table.1. Scenario Parameters

Routing protocols	AODV /LAR	
Radio type	802.15.4 IEEE	
No. Of Channels	One	
Channel frequency	2.4 GHz	
Mobility	Random way point	20mps
	none	0
Path loss model	Two Ray	
Energy model	Mica Motes	
Shadowing model	Constant	
Pause time	10 second	
Simulation time	500 second	
Battery model	Linear model	
Simulation area	500m X 500m	
Number of nodes	20,40.60,80,100	
Node Placement	Grid	
Simulator	Qualnet 5.2	
Transmission Power(dBm)	3.0	

In this work Qualnet 5.2 simulator has been used to evaluate the performance of AODV and LAR for IEEE 802.15.4 standard [10].The parameter considered for simulation is given in table.1.the simulation has been carried out for node density of 20 nodes placed in area of 500mx500mwith (20mps) and without node mobility for AODV protocol, by consideringthe metrics like throughput,packet delivery ratio, end to end delay, total bytes receivedfor stationary and nodes with mobility of 20mps.The data rate considered in this simulation is 256Kbps.The simulation is repeated for 40, 60, 80 and 100nodes with and without mobility.

The simulation has been repeated for LAR routing protocol with 20, 40, 60, 80 and 100 nodes. Settings, parameters and metrics used in this simulation studies are same as that of previous simulation studies forAODV protocol.Figure.3 shows the snapshot forQualnet 5.2.Simulation scenario of 60 nodes with no mobility for AODV routing protocol representing the route discovery mechanism.

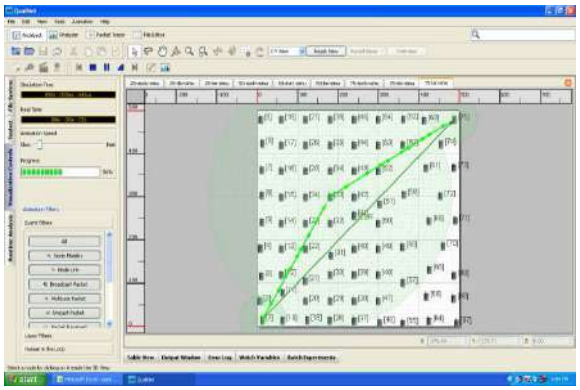


Fig.3: Snapshotof Qualnet simulator showing Route discovery mechanism in AODV for 60 nodes with no mobility

IV. RESULTS AND DISCUSSIONS

Packet Delivery Ratio (PDR): It's the ratio between the numbers of packets received at the application layer of the destination node to the number of packets sent from the application layer on the sourcenode.

The variation of packet delivery ratio for various node density is shown in figure.4.It can be observed from the figure.4 that AODV and LAR protocol with (20mps) and without mobility perform better in low node densities.

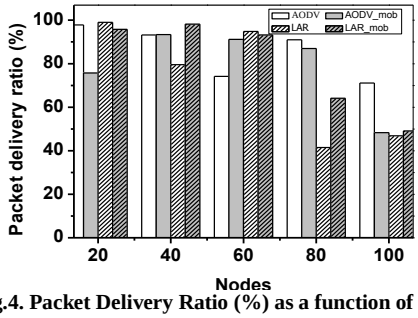


Fig.4. Packet Delivery Ratio (%) as a function of node density for all the routing protocols.

End to End Delay (millisecond): It is the time taken for a packet to be transmitted from the source node to the destination node which includes all possible delays caused by buffering.

The variation of average end-to-end delay at the receiver node is shown in figure.5.It can be observed that AODV has less end to end delay as compared to LAR.

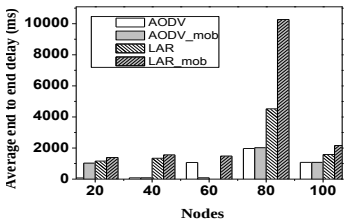


Fig.5: Plot of End-to-End Delay (ms) for AODV protocol undervarious node density scenarios.

Total Bytes Received: It is the number of bytesof datareceived at the application layerof the destination node [11].

Total bytes received for AODV protocol under various node density scenarios are shown in figure.6. Total bytes received forAODV and LAR nodes with mobility are higher than nodes without mobility.

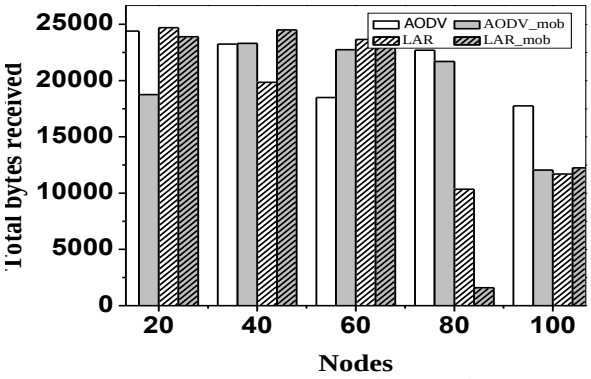


Fig.6: Total Bytes Received as a function of node density

Throughput (Bits/second): It is the average number of messages successfully delivered per unit time i.e. average number of bits delivered per second.

Throughput (bits/s) as a function of node density is shown in fig.7. It is clear from the figure.7 that AODV with (20mps) and without mobility has higher throughput than LAR.

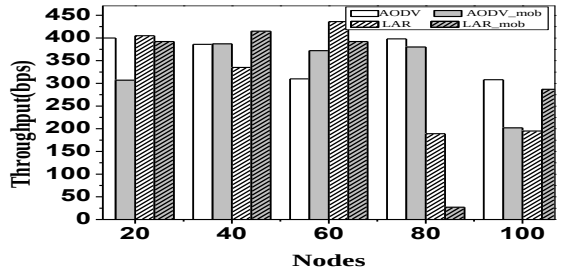


Fig 7.Throughtput (bits/s) as a function of node density.

CONCLUSION

In this paper an attempt is made to study the performance of the AODV and LAR for wireless sensor network module IEEE 802.15.4 using Qualnet network simulator 5.2. In the scenarios selected for the study, node density is varied (20, 40, 60, 80 and 100)for stationary and nodes with mobility (20mps), the metrics like packet delivery ratio, end-to-end delay,total bytes received and throughput are studied.

REFERENCES

[1] M.Subramanya Bhat, ‘‘wireless sensor networks: A performance study of IEEE 802.15.4 Standard”, volume 3, no.5, Sept-Oct 2012, International Journal of advanced research in computer science, ISSN No.0976-5697

[2] D.Johnson, D.Maltz and Yih-Dynamic Source Routing Protocol for Mobile AdHoc-http://www.ietf.org /internet-drafts/draft manet-DSR-09.txt, IETF Internet draft, Apr. 2003.

[3] David.B.Johnson and David.A.Maltz.TomaszImielinski and Hank Korth, chapter -5, pages 153-181. Kluwer Academic Publishers, 1996.

[4] H.Ehsan and Z.A. Uzmi (2004), “Performance Comparison of Ad HocWireless Network Routing Protocols”, IEEE INMIC 2004.

[5] J.Hill, R.Szewczyk, A.Woo, S.Hollar, D.Culler and K. Pister, “System architecture directions for networked sensors,” in the 9th International Conference on Architectural Support for Programming Languages and Operating Systems, 2000.

[6] J.M.Tjensvold, Comparision of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards, IEEE, September 18, 2007.

[7] J. Hill, R.Szewczyk, A. Woo, S.Hollar, D.Culler and K. Pister, “System architecture directions for networked sensors,” in the 9th International Conferenceon Architectural Support for Programming Languages and Operating Systems, 2000.

[8] C.Perkins, E.M.Royer, S.R.Das and M.K.Marina, comparison of twoon-demand Routing Protocols for AdHoc Personal Communications, pp. 16-28, Feb. 2001

[9] QualNet documentation, “QualNet5.0.2 Model Library: Wireless sensor networks”; Available: http://www.Scalable-networks.com/products/qualnet/download.

[10] J.M.Tjensvold, Comparison of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards, IEEE, September 18, 2007.

[11] M.Petrova, J.Riihijarvi, P.Mahonen, S.Labella, “Performance study of IEEE 802.15.4 using measurements and simulations”, IEEE-2006.

SMART RAIL LOCO ENGINE FOR AUTO DETECTION OF CRACK AND HUMAN PRESENCE ON TRACK

M. Madhurekha[1], Dr. M. Malathy[2], N. Swathipriya[3], K.Thulasi[4]

[1]Lecturer/Tutor, [2]Professor, [3]Assistant Professor, [4]Programmer, Dept. of CSE, RRCE, VTU, Bangalore-74.

E-mail: madhurekha.m@gmail.com , swathinatarajan@gmail.com

Abstarct-Indian Railway comprising of large infrastructure and covering vast distance of area, Is one of the most flexible Commercial mode of transportation carried out by the people in India. We are presenting this project for automatic rail crack, living begin detection on the railway tracks using ultrasonic sensors like IR sensor, PIR sensor for detection application and by integrating GPS module and GSM modem for communicating the message to the Train driver and nearby railway station. Thus help us to find and send railway geometric parameter of cracks and living beings to the Train driver and nearest railway station.

Keywords- Cracks and Human begin detection, railway security, ARM 7, IR sensor, PIR sensor, GSM, GPS.

I. INTRODUCTION

Indian railways are one of the world largest railway network comprising 115,000km of track over a route of 67,312km and 7,500 stations. India possesses the fourth largest railway network in the world. The railways traverse the length and breadth of the country and carry over 30 million passengers and 2.8 million tons of freight daily. In spite of, boasting of such admirable information, the Indian rail network is still on the developed trajectory attempting to fuel the economic needs of our Indian nation, any problems would cause the major impact on the Indian economy and societal impact of life and Social life.

Today we see many times in news that many of the accidents take place due to the undetected cracks on the railway tracks. The reasons can be due to human negligence of inability, or even it can be due to the bad timing of detection. The one more problem that we come across today is that accidents by train this can also be due to negligence of people or unusual acts like suicide. So there is a need to develop a project which monitors the cracks on the railway track efficiently and also detects the people on the track and take appropriate measures to overcome the same efficiently.

Fig.1 Rail Derailment

Now a day the Rail Crack and human begin detection has become a challenging task and problem for the railway department, much research effort has been taken for the development of automatic reliable rail crack and human begin detection on the railway tracks. The recent research analysis on the recent news of rail accidents, statistics reveal thatapproximately 70% of the major rail accidents are due to the derailments as their cause, of which about 90% are due to cracks on the rails either due to natural causes (like excessive expansion due to heat) or due to antisocial elements. Hence these cracks in railway lines have been a major problem which has to be disused with utmost attention due to the frequent use of railways. While crack detection in the rail is a difficult task few rail crack detection techniques using ultrasonic and eddy current methods are used neither technique is particularly effective for the detection of cracks in the rail foot to overcome the limitation of this older system. We are designing this Automatic Smart Rail Loco Engine.

Our project presents a new crack and human begin detection method for rail cracks and human begin, this system which utilizes the change in infrared emission through the rail surface during the train movement along the wheels. Initial data for this infrared method are taken from the laboratory-based three-point bend specimen studies and a short section of rail. The results of these two studies help to have ability to locate and quantify surface-connected notches and cracks. The most important advantages of this project are the detection is possible both at day and night times.

II.RELATED WORK

In 2015 Shailesh D. Kuthe1, Sharadchandra A. Amale and Vinod G. Barbuddhye suggested the use of Smart Robot for Railway Track Crack Detection System Using LED-Photodiode Assembly[1] which was not giving accurate result is improvised in our project by using high efficient IR Sensors[1],

In 2014 MuneendraRao , B. R. BalaJaswanth and Ch. MuneendraRao " proposed Crack Sensing Scheme in Rail Tracking System" using ARM for the first time. The enhancement of this project is done by adding PIR sensor and GPS for locating the carks location [2].

III. CURRENT SYSTEM

At present the rail crackdetection is based on the principle ofLDR (Light dependent Resistor), LVDT (Linear Variable Differential Transformer),LED (light emitting photo diodes), Ultrasonic and eddy current methods of track crack detection system which is of high cost and less accurate, to overcome this in our project we are using the ultrasonic sensor for Rail Crack and human begin detection with Transmission Module consisting of GSM and GPS Module for the data transmission and Acquisition at low cost and high accuracy. Till date human begin detection on the track has not been proposed which is been implemented in our proposed project We are implementing IR sensor for the crack and PIR sensor for human begin detection in this project thus avoid manual checking for the presences of cracks and human being.

IV .PROPOSED SYSTEM

The proposed system consists of componentslike IR sensor, PIR sensor, Buzzer, LCD, GSM &GPRS modules. The Carks on the railways tracks are detected by IR sensor which are placed in front of the loco engine thus the any cracks identifies crack signal is given to ARM modules ARM gives the command to the Motor and break module and the message is been displayed by LCD display for the Train drivers notice by trigger on the buzzer, Using GSM and the GPS Module the message and the location of the crack is been Located and been transmitted to the nearest railway station. The Human begin detection done using PIR sensor which is also placed in front of the loco engine thus the any Human begin identified the signal is given to ARM modules ARM gives the command to the Motor and break module and the message is been displayed by LCD display for the Train drivers notice by trigger on the buzzer, Using GSM and the GPS Module the message and the location of the crack is been Located and been transmitted to the nearest railway station.

Temperature Sensor is used to detect any fire accident caused due to unusual factor in the rail and the train.

Block Diagrams:

Automatic Smart Rail Loco Engine Block Diagram

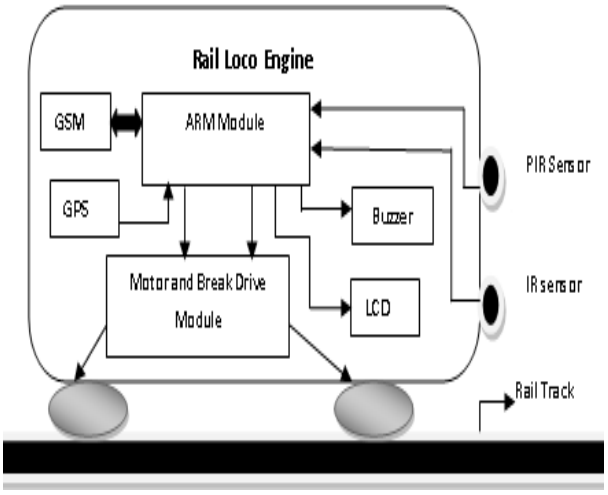


Fig.2 Automatic Smart Rail Loco Engine Block Diagram

ARM Module Detailed block Diagram:

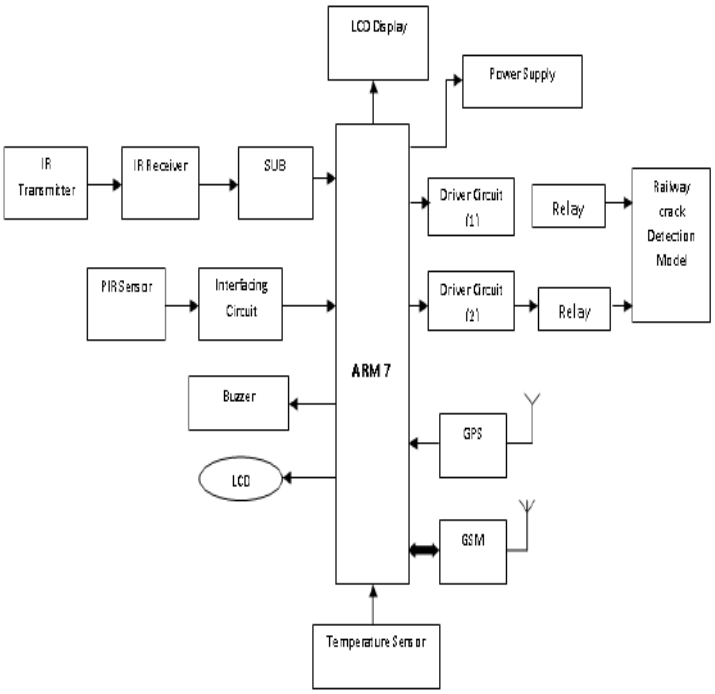


Fig.3 ARM Module Detailed block Diagram

Block Diagram Description:

The IR Sensor which emits infrared rays is called as IR Transmitter and sensor which receives the transmitted signal are IR Receiver. One important point is both IR

transmitter and receiver should be placed in the straight line to each other. The signal is received by the receiver when there is Deviation or errors in signal then it are taken as crack is detected. The crack detection signal is given to ARM controller which in turn given the signal to GPS and GSM for sending message, latitude and longitude value to the train driver and to the nearby railway station. The same principle holds good for the PIR Sensor its works same as that of IR sensor but by detecting the IR radiations reflected by the Human begins. ARM 7 as a controller process and guide the other electronic devise to work and sanctify the desired conditions and parameters thus having safety control over the train and avoiding the accidents.

HARDWARE & SOFTWARE REQUIREMENTS

IR SENSOR:

IR sensor used in our project to detect the crackson the railway track. It consist of transmitter and receiver. Infrared (IR) transmitter is an IR LED which emitsinfrared light, it means that it emits light in the range of Infrared frequency. The wavelength of Infrared ranges from (700nm – 1mm) and this IR rays are just beyond the normal visible light. Everything which produce sheat emits infrared like our human body. Infrared have the same properties as visible light, like it can be focused, reflected and polarized like visible light.

IR have light emitting angle of approx. 20-60 degree and distances ranges from few centimeters to several feet's, it depends upon the type of IR transmitter and the manufacturer. Some of the IRcan transmitter up to few kilometers distance.

PIR SENSOR:

An objects with temperature above absolute zero has a property of emitting heat energy in the form of a radiation. These radiations are not visible to human eye as it radiates infrared wavelengths. A device designed for the purpose to detect infrared wavelength exists and is known as Passive Infra-Red Sensors. PIR sensors in short measure Infrared Light Radiation from objects on the railway track.

The PIR device is used widely only for the purpose to detect the emitted infrared radiation and does not in any manner create any kind of waves for sensing purpose. The PIR device analyses the infrared rays that is generated by the object that is above absolute zero. An object depending on the temperature and surface omits the infrared radiation that is observed by the PIR Sensor. Supposing that a living being pass in front of the background like a concrete the heat at that point in the sensor's vicinity will increase the room temperature to body temperature and then back again. Now the resulting change is converted by the sensor by the incoming infrared radiation into an entry in the output voltage. This activates the detection in Sensor. The omission pattern of an object depends on its surface properties and depending on it the infrared pattern is different, so moving them with respect to the background may start the PIR sensor on its own.Depending on the functionality of the PIR, there are many kind of configurations available for different purpose. The most used version has multiple Fresnel lenses or Mirror segments, an effective range of roughly 10 meters and a field of view less than 180 degrees for the analysis. An ideal wall mount design usually has wider fields of view, including 360 degrees. There are some PIRs used for detection in long range over around 100 feet away and usually are made with single segment mirrors. PIRs designed with reversible orientation mirrors that covers a wide angle of 110 degrees wide or very narrow "curtain" coverage or with individually selectable patterns to "shape" an analyzing area. In this project of crack detection we are using a 180 degree PIR Sensor.

ARM7:

Increasing use of embedded systems, the developers and system-on-chip designers select specific microprocessor cores and a family of tools with libraries, and off-the-shelf components to develop new processor-based products and applications devices. Over the last few years, the ARM architecture has become the most prevalent, ARM 7 is a low power consumption 32-bit CMOS based microcontroller which is based on the enhanced RISC architecture, and ARM 7 can execute many powerful instructions with less time at single clock pulse. ARM is one among the major controller used for embedded system electronic circuit by the developers. ARM processors are embedded as the controlled in many electronic products ranging from cell/mobile phones to automotive braking systems. ARM7 is one of the widely used micro-controller family in embedded system application. ARM processors are more effective with less cost it requires fewer transistors than any other typical processors. Thus reducing the costs, heat and power consumption of the designed device. These simple design help is manufacturing larger multi core processor and high performance device at low cost and efficiently.

In our project we are usingARM 7 Based (LPC2148) which works at 1 MIPS per MHz thus allowing the system designed to consume less power and at higher processing speed.

GPS:

GPS stands for Global Positioning System. The GPS is mainly used for collecting the location and position data's from the vehicle and display it as a map for the better identification and mapping It is used for interfacing the communication links and detect the location of the cracks on the track too will have the interface to the communication link. The higher module of GSP is

enhanced with special features like video coverage, trace mode, history track, vehicle database, network support.

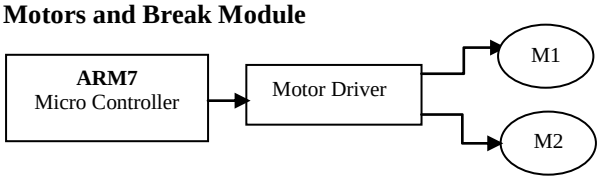
GSM module:

The GSM stand for (Global System for Mobile communication)for the wireless transmission of data from one place other place is done using GSM Mobile SIM which provides a low cost, long range, wireless communication channel for applications that need connectivity rather than high data rates. It is used to send the SMS to the train driver and nearby railway station about the cracks, location of crack and human being on the track to the train and also the nearest railway station to take precautionary measure for avoiding accidents.

LCD module:

A **liquid-crystal display** (**LCD**) is anelectronic visual display, which is used for displaying the data collected from the sensors and GPSthat can be showed to the train deriver as the reference on the LCD display in the train.

Motors and Break Module



The Motor and Break Driver Module is controlled by the ARM Controller for controlling the speed of the train and to stop the train when the crack are the human is and Control, July2008, pp. 231-239

detected on the railway tracks.

CONCULSION

Thus by implementing Automatic Smart Rail Loco Engine in the railway department. We could avoid many problems like rail derailment, major accidents like train crash, human begins and animal's accidents, accurate track crack detection with exact location of the cracks. By using systemusesAutomatic ARM module, sensors, GSM and GSP the system works 24X7 providing us more secure safe travel, thus the project reduces the efforts of man power and provide the best ever secured railway system.

REFERENCES

[1]Smart Robot for Railway Track Crack DetectionSystem Using LED-Photodiode Assembly Shailesh D. Kuthe1, Sharadchandra A. Amale2 and Vinod G. Barbuddhye3

[2]Ch. MuneendraRao , B. R. BalaJaswanth and Ch. MuneendraRao " Crack Sensing Scheme in Rail Tracking System" in Int. Journal of Engineering Research and Applications, January 2014, pp. 13-18.

[3]Avinash. V. animireddy and D. ArunaKumari "Automatic Broken Track Detection Using LED-LDR Assembly" in International Journal of Engineering Trends and Technology (IJETT), - July 2013, pp. 289-292.

[4]QiaoJian-hua; Li Lin-sheng; Zhang Jing-gang; "Design of RailSurface Crack-detecting System Based on Linear CCD Sensor", in IEEE Int. Conf. on Networking, Sensing

Online Cost Effective Face Authentication System

Dr.M.Malathy[1], M.Sarala[2]
[1]Professor,Dept. of CSE, [2]Programmer, Dept. of ISE, RRCE, VTU, Bangalore-74.
E-Mail:anandanmalathy@gmail.com, ksgvanand@gmail.com

ABSTRACT- In the biometric world, storing the biometric multimedia data and fast retrieving is very important challenge. Biometric images are mainly used for national identity of human being. Based on the population the data become a Big Data. We have to handle the billions of the data in real time. Fast Storinng and retrieving is essential for our fast networking era and also need cost effective online authentication system This paper is mainly focused on online cost effective face authentication system using Oracle BLOB.

Keywords: Biometric, Face Image, Multi-Media data, BLOB.

I. INTRODUCTION

In the Recent network world, identifying and verifying the person is necessary for every communication. Where authorization is essential for every application, like writing the online examination, employee attendance in any organization, an aircraft application, an authentication is almost important of an individual as well as group of individuals. Online processing and also real time authentication is using all the fields. In real time biometric processing we are taking the face image for authentication purposes. Low cost effective authentication system using oracle blob data type is using for storing the image as well as text data. Fast Storing and retrieving is a big challenge in the multi-media data. In Big Data analytics in biometric data is also the important research area nowadays. There are some areas were large volumes of data are stored in centralized or distributed databases. Few of these areas, are: online libraries, bioinformatics, medical imaging, healthcare, finances and investments in business areas, manufacturing production and marketing strategies, communication media, scientific research areas, web development area and biometric authentication area. Generally in these databases the multimedia data like images, video, audio, etc are stored either in separate files or folder, or inside the database in BLOB data types. This paper presents a online cost effective face authentication system with effective Indexing database management system.

The paper is structured as follows: in Section II Related works, Section II Proposed Online cost effective face authentication system, Section III Implementation Result and in the Section IV Conclusion and Future Scope.

II. RELATED WORKS

Yogesh Simmhan [1] have proposed,Benchmarking Fast-Data Platforms for theAadhaar Biometric Database, how to handle large volume of Aadhaar biometric data of Indian national identity. [1].Malathy M & Arputha V.Selvi [2] have proposed, 2-DWT and AES: Secure Authentication Management for Polar Iris Templates Using Visual Cryptography, from this paper, to protect the iris template against the spoofing attacks in the database storage level. Two shares were stored separately and merging the shares then only authentication system accessed the genuine user. Malathy M & Arputha V.Selvi [3] have proposed, the liviness face detection based on the binary image of the eye images. These eye images are cropped from the face images and photo face images, the gray scale value of the photo eye image had converted in to binary images and found the liviness. Akhtar, et al [4] have investigated, a real spoof attack samples that verify the multimodal biometric systems. Spoofed face and iris samples were replicated with a photo attack method. The photo of each individual was put in front of the capture device. While spoofed fingerprint samples was created by the same method. For each individual, 10 spoofed face, fingerprint and iris samples were created. The biometric systems were not intrinsically robust against spoof attacks contrary to the common belief. It can be cracked by spoofing only one biometric trait. Schwartz, et al[5] have presented a face spoofing detection through partial least squares and low-level descriptors. Partial Least Squares regression to provide a feature weighting to distinguish between live and spoof images or videos. The use of a robust set of feature descriptors renders many classical machine learning methods intractable due to extremely large resulting feature space, which becomes more evident when the temporal function was considered. The reduced number of training samples was compared to the number of descriptors.

III. PROPOSED IMAGE ANALYZER

In the proposed Image analyzer, the real face image and the scanned photo image were analyzed according to the variations in the histogram equalizer. The Fig 1.2 shows the system architecture of the image analyzer. It has two modules. One is acquiring the face image in the different type of devices. The face image captured from the webcam and stored it in the system. The photo face image scanned from the scanner and stored it in the system. The both images are given to the input of the image analyzer. The analyzer has to find the contrast of images using the histogram equalizer. The histogram equalizer, the image is divided in to two frames horizontally vertically row and col of the pixel intensity taken to find the cumulative sum of the image. The contrast, correlation, energy and

homogeneity are found by the image analyzer based on the following equations, Eq.No.(1) represents the mathematical equation of the contrast.

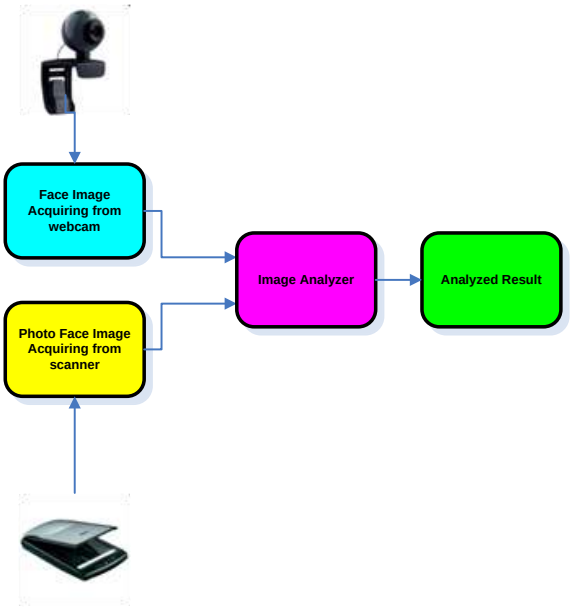


Fig.1.2 System Architecture of Image Analyzer

$$\text{Contrast} = \sum_{(i,j)} [i-j]^2 P(i,j) \quad \ldots\ldots\ldots\ldots \quad (1)$$

Where p=image, i,j=coordinates , p(i.j)=Intensity value at i,j

Eq.No.(2) represents the mathematical equation of the correlation.

$$\text{Correlation} = \sum_{(i,j)} P(i,j) \left[\frac{(i-\mu)(i-\mu)}{\sqrt{(\sigma)2(\sigma)2}}\right] \quad \ldots\ldots\ldots \quad (2)$$

Eq.No.(3) represents the mathematical equation of the Energy.

$$\text{Energy} = \sum_{(i,j)} P(i,j)^2 \quad \ldots\ldots\ldots\ldots \quad (3)$$

Eq.No.(4) represents the mathematical equation of the Homogeneity.

$$\text{Homogeneity} = \sum_{(i,j)} \frac{P(i,j)2}{1+(i-j)} \quad \ldots\ldots\ldots\ldots \quad (4)$$

The final result, the differences of the values of all the parameters are found and using these different values analysis shown the original and fake images are found for an authentication system.

IV. IMPLEMENTATION RESULT

The implementation results are given below. The Fig. 1.3 shows the Original webcam image that corresponding histogram image and also histogram equalized image with the corresponding histogram equalized image.

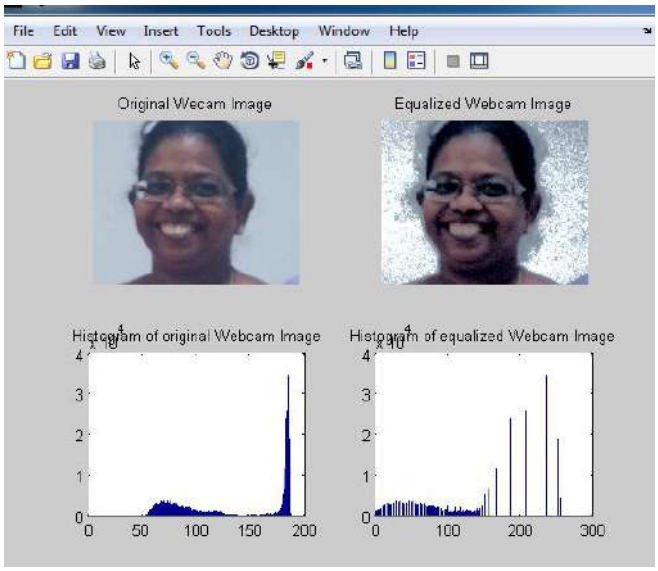


Fig. 1.3 Webcam image with the corresponding histograms

The Fig. 1.4 shows the Scanned photo image that corresponding histogram and also histogram equalized scanned photo image with the corresponding histogram equalized image.

Fig. 1.4 Scanned photo image with the corresponding histograms

Table 1.1 Difference between the parameters of scanned photo image and the real photo image

Sl. No	Type of the Images	Images	Contrast	Correlation	Energy	Homogeneity
1	Scanned Photo Image		**0.239**	**0.945**	**0.198**	**0.907**
2	Real Photo Image		**0.036**	**0.992**	**0.321**	**0.982**
Difference =(Real Photo image - Scanned photo image)			**-0.203**	**0.047**	**0.123**	**0.075**

The table 1.1Shows the different between the parameters of the two types of images.

CONCLUSION

Comparison of two face images, one is webcam face image, another one is scanned face image, both inputs are given to the image analyzer, the image analyzer analysis the images based on the histogram equalizer. Finally, conclude that the parameters differences are, contrast is -0.203, correlation is 0.047, energy is 0.123 and homogeneity is 0.075. Based on the results the two images are different. It will useful to identify the original and fake images in the authentication system. In future work, database should be increase and train the image analyzer to find the printed photo image, all type of original and fake biometric images.

REFERENCES

[1] Malathy, M & Arputha Vijaya Selvi,J,'Spoofed Iris Recognition: Synthesis of Gabor and LBP descriptor usingPPC', Australian Journal of Basic and Applied Sciences(ISSN 1991-8178), pp. 433-442. 2014

[2] Malathy, M. & Arputha Vijaya Selvi, J., "2-DWT and AES: Secure Authentication Management for Polar. Iris Templates Using Visual Cryptography," Journal of Testing and Evaluation, Vol. 45, No. 2, 2017, pp. 1– 2015; published online February 2, 2016.

[3] Malathy, M & Arputha Vijaya Selvi,J,'Face Liveness Authentication/Anti-Spoofing Engine using Morphological-shared weight Neural Network', Advances in Mathematics Scientific Developments and Engineering Application,Narosa Publishing House Pvt.Ltd., ., ISBN-978-81-8487-074-9, pp.550-557. 2010

[4] Akhtar, Zahid, and Sandeep Kale. "Security Analysis of Multimodal Biometric Systems against Spoof Attacks." Advances in Computing and Communications. Springer Berlin Heidelberg, 2011. 604-611.

[5] Schwartz, William Robson, Anderson Rocha, and Helio P. Edrini. "Face spoofing detection through partial least squares and low-level descriptors."Biometrics (IJCB), 2011 International Joint Conference on. IEEE, 2011.

[6] Heo, Jingu, and Marios Savvides. "Gender and ethnicity specific generic elastic models from a single 2D image for novel 2D pose face synthesis and recognition." Pattern Analysis and Machine Intelligence, IEEE Transactions on 34.12 (2012): 2341-2350.

[7] Malathy M & Arputha Vijaya Selvi J, "Survey of Cyber Security and Laws for Social Media Sites (SMS)', Proceedings of International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS-2016) at Kings College of Engineering, Thanjavur India, 978-1-4673-6725-7/16/213-216 ©2016 IEEE

[8] Malathy, M & Arputha Vijaya Selvi,J 2012,'Multimodal Biometric Decision Fusion for Liveness Authentication Authentication / Anti-Spoofing Engine', Electronic Design and Signal Processing Narosa Publishing House Pvt.Ltd., ISBN 978-81-8487-160-9, pp.195-201.

[9] Feng, Zhen-Hua, et al. "Random cascaded-regression copse for robust facial landmark detection", IEEE Signal Processing Letters 1.22 (2015): 76-80.

[10] M. Malathy & J. Arputha Vijaya Selvi,J 2011," Multimodal Biometric Expert Decision Fusion", International Journal of Mathematics, Computer Sciences and Information Technology Vol. 4, No. 1, January-June 2011, pp. 113-123

FUZZY LOGIC BASSED INTELLIGENT QUESTION PAPER GENERATOR

Gaurav Kumar[1], Amit Parmar[2], Manigandan J[3]

[1,2]UG Scholar, 3Asst. Professor ,*Dept of CSE, RRCE, Bengaluru*

E-Mail: gaurav.99344@gmail.com, amit9610209066@gmail.com

Abstract- Assessment plays an essential role in deciding the quality of students. Generating an efficient question paper is a task of great importance of any educational initiate. Conventionally question papers are developed normally in this paper a fuzzy reasoning based model is prepared for autonomous paper technology, using MATLAB. Comparative evaluation with classical method is done and fuzzy model is found to be more reliable fast and logical.

Keywords- Fuzzy Logic, Iqpgs, Classical Method, A/D, E/M/D.

I. INTRODUCTION

As we all know that examination plays a very important role, so the system should be design in a systematic way. The examination system being followed by most educational system is conventional and is enable to access knowledge of the students. Previously ht classical method is used i.e. a predetermined number of faculties were given responsibility to frame a question paper out of a given syllabus and then one of those question papers is picked up randomly to use for the purpose. This system has a number of disadvantages like:probability of error due to dependency on intelligence of single person,important part of syllabi may not be covered depending on personal interest,secrecy may not be maintained, and full resource utilization might not be possible, hence raising the cost. So here we come up with a better autonomous system named as intelligent questions paper generation system (IQPGS). This system will give more efficient, reliable and will improve its quality and also reduce the time taken by setting the question paper manually. it will help to solve some critical issues like duplicity, storage of previous data and above all secrecy of question paper. Humans are good in approximate reasoning but not in precise one, converse is true for machines. So we need to take the advantage of both types of reasoning computation. fuzzy logic will at utilize human reasoning effectively[4].this approach is implemented for logical selection of this parameters while framing questions papers for every subject irrespective of its discipline .this system considers the all parameters itself by taking some inputs from user. All dependent and independent parameters are categorized based upon some logic so that the system can easily be acquainted with them. We can categorized questions paper in two ways: contents of the paper (sub category: analytical(A),descriptive (D)) and difficulty level of the paper (subcategory: easy(E),medium(M),difficult(D))we can set both descriptive and analytical questions of any difficulty level

so all these A/D and E/M/D. parameters are considered as impediment of each other.

II. RELATED WORKS

A. FUZZY LOGIC

In recent times, the number and variety of applications of fluffy logic have increased significantly. The applications cover anything from consumer products such as digital cameras, camcorders, washing machines, and microwave ovens to professional process control, medical arrangement, decision-support systems, and collection selection.

In 1965, zadeh proposed a complete theory of fuzzy sets to represent and manipulate ill-defined concepts and according to zadeh “contrary to traditional hard computing, soft computer exploits the tolerance for imprecision, uncertainty, and just a few truths to achieve tractability, robustness, low solution-cost, and better rapport with reality" [4]. Fuzzy reason is a method to formalize your capacity of imprecise or approximate thinking. Such reasoning represents the human ability to reason approximately and judge under uncertainty. In fuzzy common sense, all truths are just a few or approximate [7]. It uses a multi-valued membership function to signify membership of a target in a category alternatively than the classical binary true or false beliefs. Fuzzy set is explained with a member dispatch function (?) that maps a collection of objects on the interval of real numbers between 0 and 1. In standard established theory, a subject is either a member of a set or not a member of the set. In fuzzy collection, the transition from membership rights to non-membership is steady rather than abrupt since there are non-distinguishable restrictions [6].

B. SAMPLE DATA

A short overview of complete system is provided by a block develops something lender from all t this individual question papers entered by all the users, using which it provides an analysis of internal process with final output as a developed question paper. Quantity of users, skeleton of paper and everything other details provided here are not rigid; system is quite flexible and parameters are super easy to change as per requirements**..**

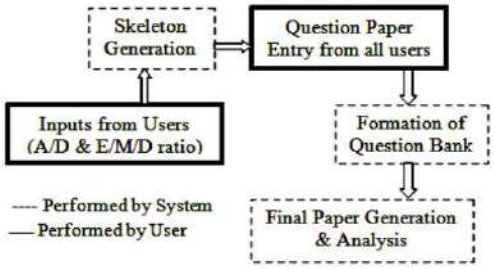


Fig.1. Overview of Proposed System

III. PROPOSED SYSTEM

If we consider the short comings of conventional system, we feel and eager need to redesign the whole examination system. The system was closely absorbed. The system should carry some qualities like, automatic development of question bank, limiting the human involvement for secrecy standards, providing for flexibility in logical section of questions for skeleton framing and handling multiple attributes containing imprecise data to perform human -like reasoning effectively.

Till the second phase i.e. skeleton generations is performed using fuzzy logic but the picking logic of question paper from question bank and analysis part of paper generation processes i.e. the third phase is performed using the statically method .

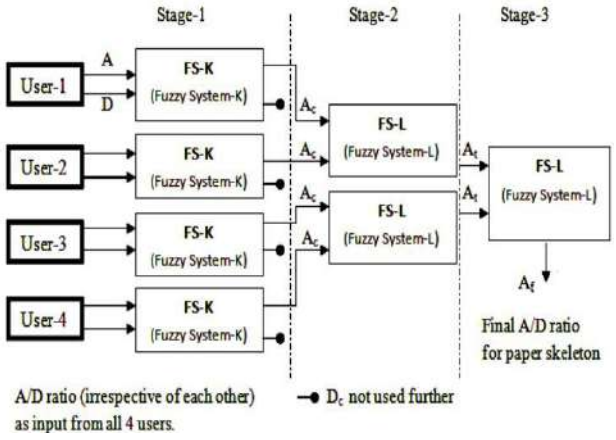


Fig. 2. Selection of A/D Parameter

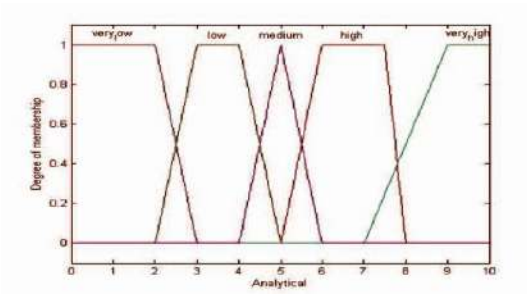


Fig. 3. membership function for analysis

Above fig.1 represents a fuzzy model i.e. used for deciding final A/D valve by processing choices of all users .this model uses two MAMDANI type FIS(fuzzy interface system) named as FS-K(fuzzy system k) and FS-L(FUZZY SYSTEM-L) are used .The membership function for first input, both outputs of FS-K and for two inputs and 1 output of FS-L is represented in fig.3

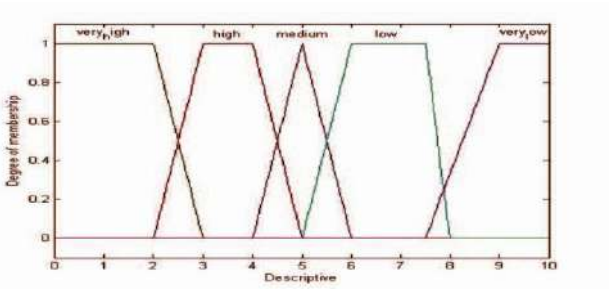


Fig. 4. Membership functions for Descriptive

A. RULES OF INFERENCE

The next step in development of fuzzy logic model is

deciding the if-then rules by multiplying the number of fuzzy sets of all input we calculate the maximum number of fuzzy rules. Let we have 2 inputs with five fuzzy sets kin each input, we will be having total 25 if-then rules. Every rule is deduced by using each possible combination of every fuzzy set of both the inputs of FS-K and then it is mapped on to the fuzzy set of the output by finding maximum u value. example considering a as high and d as very underscore high; find out the points having membership value=1 .in the set of high for A the candidates having u=1 are 6,7(considering only integer and in the set of very high for D such candidates are 0,1,2.now finding out the average of every possible combinations of these value({6+0)}/2=3,{6+1}/2=3.5,{6+2}/2=4,{7+0}/2=0.5,{7 +1}/2=4,{7+2}/2=4.5). Then we arrange these averages in defending order go frequencies and are map on the output membership function. Now we can find out which points carry maximum value of u collectively (frequency of 3.5 and 4 is 2, sumo individual u is 2 for both and they belong to same group in output; for a out is high and d out is low and can be confirmed from rule number 5), by tracking these values on membership function for output of FSK-Kismet rules are as follows:

1. If analytical is very low and descriptive is very low then analytics underscore out is medium and descriptive underscore out is medium.
2. If analytical; is low and descriptive is very low then analytical _out becomes high and descriptive _out is low.
3. If analytical is medium and descriptive is very low then analytical _out is high, descriptive underscore out is low.

4. If analytical is high and descriptive is very low then analytical out is high and descriptive out is low.
5. If analytical is high and descriptive is very high then analytical underscore out is high, descriptive underscore high is low.

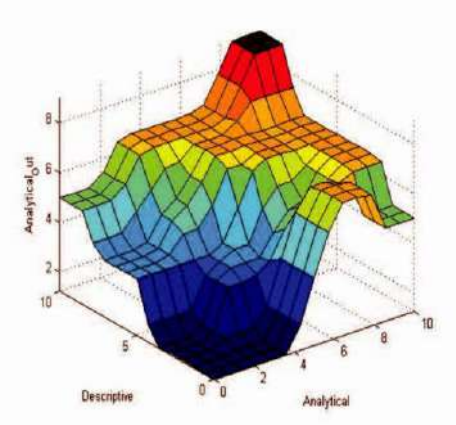


Fig. 5. Surface viewer of FS-K

B. SELECTION OF PARAMETERS (1 PHASE)

In this stage -1,FS-K requires all users to enter their inputs for A\d;north inputs are modified by system to corrected one on the scale of 0-10 as A and d becomes counter part of each other .(for ex. user 1 enters a=9.56,d=4;d is treated as 6{10-4=6} in FS-K because membership function will be design in converse nature, the output of this system FS-K will be Ac=7,dc=3)the corrected analytical and descriptive values are ac\dc. The cascade part of FS-K is FS-L,in stage-2. It receives only ac from output of FS-K; because once we know ac, we can easily evaluate dc by subtracted it from 10 .now the 4 values of ac are clubbed into 2 groups (on the basic of weight age).

Now the 2 groups are taken by separated fed to the FS-L and two outputs will be taken, then in stage 3 again the outpost of FS-L are taken for input for FS-L to give one final output called AF,(fuzzy set follow the associatively low [4]).

A similar system like FS-L can be used to calculate the final value for E\M\D. The ranges go membership function defers for E\M\D from those in FS-l system for A\D. clubbing the valued of E from all the four users in to two groups, further gives two values, one from each group on the weight agebases these two outputs are calculated by the same system to get final value of E .in the same way all the final values are calculated from inputs of 4 users. The algorithm given above explains how to decide the difficulty level (E\M\D) and content (A\d) of each question according to the final values of parameters.fig.6 explains the algorithm for skeleton generation using a flow chart. Where 'w' is the number of questions in particular part .example final values i.e. obtained by fuzzy logics are A=7, D=3 and E=3, M=5, D=2. the value of A\d indicate that paper of 70 marks is analytical and paper of 30 marks is descriptive, out of 100 marks .E\M\D ratio is maintained individually in every part.

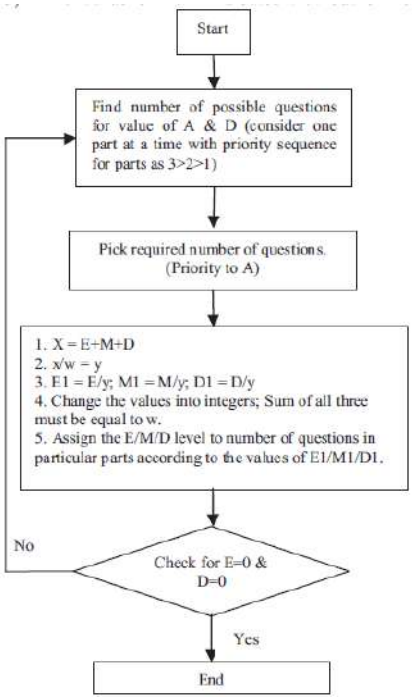


Fig 6: F low chart for skeleton generation

According to the algorithm,first priority goes to part -3 and requires 5 questions of 15 marks. now divide marks for both of a and d by 15 to obtained the integer value(like, no of possible question for a is 70 /15=4,and for d it is 30/15=2);to find out the possible number of question of a and d it needs 5 questions for part 3 and priority is given to a ;now select a questions from a and remaining 1 questions from d from nest steps x=10(x=E+M+D).

Hence w =5 and y=(x/w),so y=2 here ,since number of questions in part 3 is 5.'y'is the parameter used to find the number of questions that will be easy/medium/difficult in each par and is done by dividing the values for every E/M/D by 'y', ex.,E1=3/2,M1=5/2,D1=2/2 hence E1=1.5, M1=2.5,D1=1 converting these parameters into integer value according to their floating part weight age and some of all 3 must be equal to number of questions.

The priority is given to the lower level in case of two parameters having same weight age. In next step remaining value of a=10(four questions are selected as A HENCE {70-(15*4) =10}) and D=10 check the value of a and d both and the algorithm if they are 0 else go to step 1 again and start selecting questions for remaining parts.

C. SECOND-PHASE (QUESTION BANK FORMATION)

Skeleton generated in first phase is taken as fixed for a particular paper and the system requires all the four users to enter question paper with the given parameter. the user is provided an enter phase for question papers entry .the user can't provide two questions from the same unit in one part while entering the questions,system itself locks the unit number one selected ,for the corresponding part only.

Now the system will form the question bank in a excel file having all two marks question in group-1(g-1), allfive-mark questions in group-2(g2, all fifteen marks question in group-3(g-3).

D. THIRD PHASE (FINAL PAPER GENERATION AND ANALYSIS)

In the final phase of IQPGS 1 question paper will be generated from question bank which is dividing in the 3 groups reprinting different type of question based on marks. Final interphase is only for the authorized person at the examination end considering the security issue. Logic four picking questions from the question bank,giving due considerations to the Important part of syllabi and duplicity removal in the questions has been explained using the algorithm, in the fig. 7 given below. According to this algorithm, g-1 is taken first because the priority goes to the g-1 of the question bank. It consists of five questions of 2-marks from each user which makes a total of 20 question of 2- mark from all .find the frequencies of all the units' i.e. Which unit has been selected by more number of users and select those which are having maximum frequency of questions according to unit number. Suppose from unit-5, four questions are there in question bank and from unit 7, from 4 questions are also present. In this case maximum frequency clashes so, questions from both unit 7 and 5 will be considered as qualify question in the next step a random number (range 1-10,000) is assigned to each question. The questions will be selected as first question of 2 marks from paper which are having maximum numbers .a unit number of the particular question and the question itself both will be locked is the no. of questions required in current part, part-1 corresponds to 2 marks question so the total number of question required for part-1 is 5, hence X =5. As all the questions are selected will keep on decreasing by 1 i.e. X-1 until the X value becomes =0. If a condition occurs where X~=0 and all units are locked then all units will be unlocked again but the selected questions will not be unlocked .once the condition X=0 occur, system will check that either the questions for all groups are selected or not. Ifnot, then all units will be again unlocked because the group is changed in this manner all questions. In this way all question s will be selected one by one and final generated paper will be exported by the system to an excel file for further use.

IV. RESULTS

Given method is proposed method much more faster and efficient, reliable then classical method (manual) .full utilization of resources, logical selection of question (unbiased selection) duplicity removal in questions,uncompromised secrecy issues, environmental concerns considerations, emphasis on important part of syllabi and less man power requirement are the key advantages of this purpose system and there are lot of problems also which are being solved buy the system IQPGS. a new paper can be framed in seconds by just one click in case of the question paper is leaked while in classical method , it will require the whole process get repeated. Fuzzy part of IQPGS also has a very good computing advantage over classical method. both methods have been compare for deciding the Parameter (A/D AND E/M/D) for comparison all the possible combination of a and d like 0. 0.5.1, 1, 1.5, 2, 2.5…10 have been calculated and absorbed that the classical method does not vary in range or gives fixed values (doesn't justify human reasoning well) and it always takes value of a quite higher than that in fuzzy. If the value of 1 parameter is fixed and we check all combination of it with vary g values other parameter, then their always exist one or two teams here it is not able to calculate (refer table 1.) in the same way, comparison is perform for E/M/D system also and fuzzy logic is found for advantages.

CONCLUSION

The paper we are suggesting introduces a new fluffy logic based IQPGHS system for autonomous paper technology. If we match up against classical method it implies that the propose system is very reliable in conditions of duplicity removing, un compromised issues, listen closely man power, logical in conditions of unbiased selection and more faster as the use of weird logic in machines mimic and precise reasoning are considered. at a later date, to make this system more increased flexibility by using feedbacks make the system improve itself via self-learning system and the detection of vague data entry will be further introduced.

ACKNOWLEDGEMENT

The author gratefully acknowledges the support of management and Dr.Balakrishna R, Principal, RajaRajeshwari College of Engineering, Bengaluru, Dr.Usha Sakthivel, Professor, Head of Computer Science Department, RRCE, Bengaluru and my teachers, friends and family for their invaluable support and encouragement.

REFERENCES

[1] R. Bhatt and D. Bhatt, "Fuzzy Logic based Student performance evaluation Model for practical component of

Engineering Institution subjects," International Journal of Technology and Engineering Education, vol. 8, No. 1,pp 1-7, 2011.

[2] A.F. Baba, D. Kuscu and K. Han, "Developing a Software for Fuzzy Group decision support System: A Case Study," The Turkish Online Journal of Educational Technology, vol. 8, No. 3, pp 22-29, 2009.

[3] R. S. Yadav and V. P. Singh, "Modeling academic performance evaluation using Soft Computing Techniques: A Fuzzy Logic approach," International Journal on Computer Science and Engineering.

[4] S.N. Sivanandam and S. N. Deepa, Principles of Soft Computing. John Wiley & Sons, Inc, 2nd edition, 2009.

[5] Fuzzy Logic Tool Box user guide Matlab (Sep. R2012b, online).

[6] A. B. Badiru and J. Y. Cheung, Fuzzy Engineering Expert Systems, John Wiley & Sons, Inc, 1st online, 2002.

[7] T. J. Ross, Fuzzy Logic with Engineering Applications. John Wiley & Sons, Inc, 3rd edition, 2010.

A Survey Of Classification Of Self-Organizing Hierarchical Mobile Adhoc Network Routing Protocols

Lalithashree.S[1], Krithika.D[2], Lokesh.G[3], Anitha K[4]

[1,2,3]UG Scholar, [4]Asst. Professor, Dept of CSE, RRCE, Bengaluru

E-Mail: lalithashree97@gmail.com , krithikadharma@rocketmail.com, lokesh.g888@gmail.com, anithakrishna14@gmail.com

Abstract- MANET is one of the special kind of wireless network with a continuous self-configuring, infrastructure-less collection of nodes connected wirelessly.Each devicein aMANET is free to move independently in any direction, and thus changes its links to other devices at regular intervals by treating every available device as an intermediate switch, therebyspanning the range of mobile devices well beyond that of their base transceivers. Other convenience of MANET includes simple configuration and upgrade, Self-configuration, Self-healing low cost and maintenance , more flexibility, and the ability to make use of new and efficient routing protocols for wireless communication .In this paper we present four routing algorithms , Its classifications, their advantages and disadvantages.

Keywords-MANETRouting Algorithms, Routing Topology, Routing Protocols and Quality of Service.

I. INTRODUCTION

For instance, if our objective is to connect a couple of office floors using short range wireless communication devices, efficiently. Each of the employees would possess a mobile or an immobile device(or both)-like desktops ,fax machine printer and so on. The first probability is to connect all these devices physically, i.e., creating a wired network which uses access points, but the disadvantage of this option is that, it makes the network less versatile, and adds immense load on it, as communication here is based routing etiquettes to transmit data to a control centre.

Even if most of the automatons or robots are disabled or knocked down, the remaining ones would be able to adapt and recompose themselves and continue transmitting information.

II. ROUTING IN MANETS

The cardinal challenges that a routing etiquette designed for Ad hoc wireless networks faces are resource constraints, error prone channel state, mobility of nodes and visible and invisible terminal problems. Due to the above mentioned problems of wireless network environment, wired network protocols cannot be used in ad hoc wireless upon the existing etiquette set up for wired communication. The second possibility is to set up a network of dedicated and mutually connected base stations which provides for cellular communication, but the disadvantage in this approach is that, it takes lot of time and possess high insulation and maintenance cost. The optimal solution is to build a mobile extempore or Ad hoc network by making use of the electronic devices in the immediate environment as intermediate switches, when they are ideal and if they are capable of performing this task. For person passing through the lobby in the particular floor, then from the tablet to a digital wrist watch on the next floor, from there to a coffee maker, from there to a laser printer and from there to its destination- say another staff's desktop. Tilldate, MANET's basically finding their application for military purposes, while commercial application is just beginning to come to light. One of the major prospective of practical application of MANET's is in a conference room where a group of people probably meeting each other for the first time come together for an pragmatic meeting. They may wish to exchange data securely or substantially with their laptops or palmtops without any additional framework or support.

Small scale MANET's are also effective for quandary or emergency search and rescue battle field scrutiny and other communication application in precarious environments. For example, automatons or robots are set up in an environment inaccessible to humans could employ a simple MANET networks, Hence they require atypical routing protocols that tackles the above mentioned challenges. The characteristics that a routing protocol should possess are:

- It must be fully distributed, as centralized routing involves high control superiority and hence is not ductile. Distributed routing is more robust than centralized routing
- It must be adoptive to frequent topology amendments caused by the mobility of nodes
- It must be localized as global state alimentation involves huge state propagation control overhead

- It must be free from loops and stale routes it must use resources such as bandwidth, memory and battery power optimally
- Transmissions should be dependable to minimize data loss and to prevent the occurrence of ductile routes .
- Alterations in the remote parts of the network must not cause updates in the topology information kept in the node
- It should be able to avail a certain level of quality of service(QoS) as required by the applications, and should offer support for time- sensitive traffic.

III. CLASSIFICATION OF ROUTING PROTOCOLS

Routing protocols for MANET can be classified into distinct types based on different conditions. The routing protocols for Adhoc wireless networks can be widely classified into four categories based on

- Routing data update mechanism
- Use of temporal information for routing
- Routing topology
- Utilization of specific resource

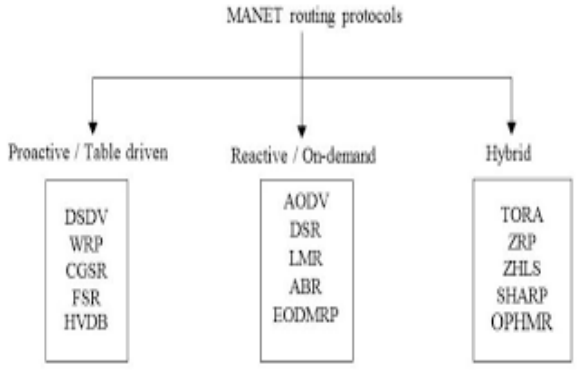


Fig 1: Classification of MANET routing protocols

A. Based on the Routing Data Update Mechanism

The routing protocols can be divided into three important categories based on the routing data
Update mechanism. They are

1) Proactive Protocols

Tables driven protocols is the other name for these proactive protocols .In proactive protocols, the route to all the nodes is maintained in routing table by exchanging routing information. Periodically. Routing information generally flows through out the network. Whenever a node requires an information to be transferred over a specifiedroute in the routing table, it runs an appropriate path-finding algorithm .Examples of proactive protocols are
CGSR – Clustered Head Gateway Switch Routing [5]
HSR – Hierarchical State Routing [8]
WRP – Wireless Routing Protocol [4]
STAR – Source Tree Adaptive Routing [6]
OLSR – Optimized Link State Routing [7]
GSR – Global State Routing
FSR – Fisheye State Routing [8]
DSDV – Destination- Sequenced Distance-Vector [3]

2) Reactive protocols

These protocols can also be known as *on-demand* routing protocols.It is more efficient than proactive routing. A route between a source and destination is obtained when it is required.The route to all the nodes is not maintained by these protocols periodically.Some of the current routingprotocols that belong to this category are given below.
DSR – Dynamic Source Routing
Routing AODV – Ad hoc On-Demand Distance Vector
SSA – Signal Stability Based Adaptive Routing
FORP – Flow-Oriented Routing Protocol
ABR – AssociativityBased Routing
PLBR – Preferred Link-Based Routing

3) Hybrid Routing Protocols

These protocols are the combinations of best features of proactive protocols and reactive protocols . Nodes concerned within a certain distance or within a particular geographical region are said to be within the routing zone of the given node. Proactive PROTOCOLS like ARE used for routing within this zone. reactive protocols used for nodes that are located beyond this zone. Some of the protocols in this
category are;
ZHLS – Zone-Based Hierarchical Link State Routing
CEDAR – Core Extraction Distributed Adhoc Routing
ZRP – Zone Routing Protocol.

B. Based on the Use of Temporal Information for Routing

This classification of routing protocols depends on the use of temporal information used for routing. As Ad hoc wireless networks are highly effective and path breaks are frequent in wireless compared to wired networks , the use of temporal information about the lifetime of the wireless links and the lifetime of the paths preferred are significant. The protocols that belongs to this category can be further divided
into two types:

1) Routing Protocols Using former Temporal Information

The protocols using the former temporal information make use information about former status of the links or the status of the links while routing to make routing decisions. For example, the routing metric based on the time of wireless connections along with a shortest path-finding algorithm, provides a path that may be adequate and reliable at the time of path-finding.

The path may get immediately brooked of due to the topological changes, making the path undergo a resource-wise expensive path reinvigoration (renewal) process . some of the examples for these protocols are:
WRP – Wireless Routing Protocol

DSDV – Destination- Sequenced Distance-Vector
STAR – Source Tree Adaptive Routing
DSR – Dynamic Source Routing
AODV – Adhoc On-Demand Distance Vector Routing
HSR – Hierarchical State Routing
FSR – Fisheye State Routing
GSR – Global State Routing

2) Routing Protocol That use Ultimate Temporal Information

Protocols of this category use the information about the expected ultimate status of the wireless links to make proximate routing divisions. Apart from the life-span of wireless links, the ultimate status information also includes information about the lifetime of the node (which is based on the remaining battery charge and battery discharge rate of the non replace able resources), prediction of location and link availability. The protocols in this category are;
LBR - Link Life-time based Routing Protocol
RABR – Route-Lifetime Assessment –based Routing
FORP – Flow-Oriented Routing Protocol

C. Based on the Routing Topology

Routing topology being used in the Internet is hierarchical in order to decrease the state information maintained at the root routers. Adhoc wireless networks, due to their comparative smaller number of nodes, can make use of one among the flat topology and hierarchical topology for routing.

1) Flat Topology Routing Protocols

Flat addressing system which is identical to the one used in IEEE 802.3 LANs is make used by these Flat Topology Routing Protocols . It infers the presence of a globally exclusive (or exclusively connected part of the network) addressing system for nodes in an Adhoc wireless networks. Some of them are:
DSR – Dynamic Source Routing
AODV – Adhoc On-Demand Distance Vector Routing
SSA – Signal Stability Based Adaptive Routing
FORP – Flow-Oriented Routing Protocol
ABR – Associatively Based Routing
PLBR – Preferred Link-Based Routing
LAR – Location-aided routing is a n example of Geographical Information Assisted Routing.

2) Hierarchical Topology Routing Protocols

An associated addressing system ie., Logical hierarchy in the network is make used by these *Hierarchical Topology Routing Protocols.* The hierarchy could be based on geographical information or it could be on hop distance. Some of these protocols are
CGSR – Clustered Head Gateway Switch Routing
FSR – Fisheye State Routing
HSR – Hierarchical State Routing

D. Based on the Utilization of specific Resources

1) Power-aware Routing

Reducing the consumption of major resources in the Ad hoc wireless networks i.e., the battery power is the main of these Power-aware Routing.The routing decisions are depends on reducing the power consumption either locally or all over the network.
PAR – Power-Aware Routing Protocol one of the Protocol based on the utilization of specific resources.

2) Geographical Information Assisted Routing

Geographical Information Assisted Routing enhancethe performance of routing and reduce the control overhead by effectively utilizing the network information available.

CONCLUSION

In this paper, the main problem involved in design of routing protocols and the different classification of routing protocols for ad hoc wireless networks were described . classification of ad hoc protocols , comparison of single path routing protocols and the multipath routing protocols .the major challenges of routing protocols are scalability, security, node cooperation ,aggregation ,multicast ,energy efficiency ,quality of services. Routing data update mechanism ,use of temporal information routing ,routing topology ,utilization of specific resource were discussed as the classification of routing protocols.

REFERENCES

[1]UdayachandranRamasamy, Professor & Head, Department of Computer Science & Engineering Sri Ramakrishna Institute of Technology, Coimbatore – 641 010, India,
[2]K. Sankaranarayanan Principal, Akshaya College of Engineering and Technology Kinathukadavu, Coimbatore – 642 109, India
[3] S.Murthy and J.J.Garcia-Luna-Aceves, "An efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks
[4]C.K.TOH,"Associativity-Based Routing for Adhoc Mobile Networks", Wireless Personal Communications
[5]D.B Johnson and D.A Maltz, "Dynamic Source Routing in Adhoc Wireless Networks", Mobile Computing, Kluwer Academic Publishers,