IJCSIS Vol. 12 No. 4, April 2014
ISSN 1947-5500

International Journal of Computer Science & Information Security

© IJCSIS PUBLICATION 2014


Cornell University
Library


Cogprints


Google scholar


.docstoc
find and share professional documents


ScientificCommons

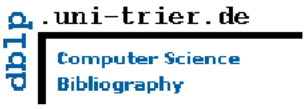

View my documents on
Scribd


BASE
Bielefeld Academic Search Engine


SCIRUS
search engine for science


SciRate.com


CiteSeerx beta


dblp .uni-trier.de
Computer Science
Bibliography


Q·Sensei


DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS


EBSCO
HOST


ProQuest

IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS
International Journal of Computer Science and Information Security (IJCSIS)
January-December 2014 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.
See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Scopus Database, Cornell University Library, ScientificCommons, ProQuest, EBSCO and more.

Deadline: see web site
Notification: see web site
Revision: see web site
Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies
Digital information processing
Cognitive science and knowledge
Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site https://sites.google.com/site/ijcsis/

For more information, please visit the journal website (https://sites.google.com/site/ijcsis/)

Editorial
Message from Managing Editor

The ***International Journal of Computer Science and Information Security*** *(IJCSIS) is a well-established forum for researchers involved in all aspects of computer science and technology to publish high quality refereed-papers. As a scholarly open access peer-reviewed journal, IJCSIS encourages emerging scholars and academicians globally to disseminate their findings, innovative ideas and research in the fields of computer science, engineering, technology and related disciplines. The objective is to bridge the research community and technology developers from academia and industry through promoting/disseminating their research–based papers, articles and case reviews on various topics of current concern on Computer Science, Security and Technology.*

IJCSIS archives all publications in major academic/scientific databases; abstracting/indexing, editorial board and other important information are available online on homepage. Indexed by the following International agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest, EBSCO. Google Scholar reported increased in number cited papers published in IJCSIS. This journal supports the Open Access policy of distribution of published manuscripts, ensuring "free availability on the public Internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of [published] articles".

IJCSIS editorial board, consisting of international experts, ensures a rigorous peer-reviewing process. We look forward to your collaboration. For further questions please do not hesitate to contact us at ***ijcsiseditor@gmail.com****.*

A complete list of journals can be found at:
http://sites.google.com/site/ijcsis/

IJCSIS Vol. 12, No. 4, April 2014 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

Dr. Yong Li
School of Electronic and Information Engineering, Beijing Jiaotong University, P. R. China

Prof. Hamid Reza Naji
Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran

Dr. Sanjay Jasola
Professor and Dean, School of Information and Communication Technology, Gautam Buddha University

Dr Riktesh Srivastava
Assistant Professor, Information Systems, Skyline University College, University City of Sharjah, Sharjah, PO 1797, UAE

Dr. Siddhivinayak Kulkarni
University of Ballarat, Ballarat, Victoria, Australia

Professor (Dr) Mokhtar Beldjehem
Sainte-Anne University, Halifax, NS, Canada

Dr. Alex Pappachen James (Research Fellow)
Queensland Micro-nanotechnology center, Griffith University, Australia

Dr. T. C. Manjunath
HKBK College of Engg., Bangalore, India.

Prof. Elboukhari Mohamed
Department of Computer Science,
University Mohammed First, Oujda, Morocco

TABLE OF CONTENTS

to different aspects of GSM technology, such as the simulation of successful calls, call drops and handover failure probabilities etc.

Keywords - Graphical NED Editor; Integrated Development Environment; Mobile Station; Base Transceiver Station; Integrated Services Digital Networks; OMNET;

4. Paper 31101318: Route optimization and roaming capability based MIPv6 protocol in internet network (pp. 28-32)

Marzieh Izanlou, Dept. of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
Mohamadali Pourmina, Faculty of Electrical and Computer Engineering, Islamic Azad University, Tehran, Iran
Afrouz Haghbin, Faculty of Electrical and Computer Engineering, Islamic Azad University
Tehran, Iran

Abstract — MIPv6 is a proper replacement for MIPv4 protocol which recommended by IETF. IPv6 lieu IPv4 has been chosen as convergence layer for next heterogeneous access networks. MIPv4 has limiting in protocol, but MIPv6 is created fundamental changes such as security enhancements, elimination of the Foreign Agent (FA) and route optimization. The MIPv6 characteristics defined by the IETF provides perspicuous host mobility within IPv6 networks. In MIPv6 MN is move between IP subnets without change in its original IPv6 address configuration. This means that MN ever is addressable in the internet via its Home Address (HoA). HoA is IPv6 address that is allocated to the MN in its home network. When away from the home network, MN can still detect by its HOA in the internet, Because packets routed to its HoA. Also In this way, mobility transparency of higher layer protocols like Transport layer or higher is achieved.

Keywords- MIPv6; routing; roaming capability

5. Paper 30031431: Utilization DCTC and Vonoroi of Tracking in Wireless Sensor Networks (pp. 33-36)

Maan younus Abdullah, University of Mosul, Education College /computer science department, Mosul, Iraq

Abstract-Wireless sensor networks (WSN) may consist of several to thousands of sensors that share the need to organize for network data collection sink routing. This paper addressed the problems of tracking moving of wireless sensor network objects. The traditional tracking method, called Dynamic Convoy Tree-Based Collaboration (DCTC) presented. In additional describe a method, called Distributed computation of Voronoi cells in sensor networks. Proposed solutions of WSNs challenges using converge cast traffic, covering networks configuration and efficient routing routines. We also present the intermediate routing sensor nodes expend an excessive amount of their energy resources. thus can achieve superior tracking accuracy with faster tracking convergence speed and reducing the network lifetime.

Index Terms - DCTC， Voronoi , Tracking

6. Paper 31031421: Effective Measurement Requirements for Network Security Management (pp. 37-44)

Dr. Rabiah Ahmad, Department of System & Computer Communication, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
Prof. Shahrin Sahib, Department of System & Computer Communication, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
M. P. Azuwa, Research Department, Cybersecurity Malaysia, Selangor, Malaysia

Abstract— Technical security metrics provide measurements in ensuring the effectiveness of technical security controls or technology devices/objects that are used in protecting the information systems. However, lack of understanding and method to develop the technical security metrics may lead to unachievable security control

objectives and incompetence of the implementation. This paper proposes a model of technical security metric to measure the effectiveness of network security management. The measurement is based on the effectiveness of security performance for (1) network security controls such as firewall, Intrusion Detection Prevention System (IDPS), switch, wireless access point, wireless controllers and network architecture; and (2) network services such as Hypertext Transfer Protocol Secure (HTTPS) and virtual private network (VPN). We use the Goal-Question-Metric (GQM) paradigm [1] which links the measurement goals to measurement questions and produce the metrics that can easily be interpreted in compliance with the requirements. The outcome of this research method is the introduction of network security management metric as an attribute to the Technical Security Metric (TSM) model. Apparently, the proposed TSM model may provide guidance for organizations in complying with effective measurement requirements of ISO/IEC 27001 Information Security Management System (ISMS) standard. The proposed model will provide a comprehensive measurement and guidance to support the use of ISO/IEC 27004 ISMS Measurement template.

Keywords- Security metrics; Technical security metrics model; Measurement; Goal-Question-Metric (GQM); Effective measurement; Network security management

7. Paper 13051401: A Survivability Strategy in Mobile Network by Key Distribution and Cross-layer protocol (pp. 45-49)

Anu Chaudhary, Department of information Technology, AKJ Institute of Technology and Management, GZB, India
K.K Gautam, Department of Computer Science & Technology, Phonics Group of Institutions, Roorkee, India
Nirbhay Ahlawat, Department of Computer Science & Technology, Phonics Group of Institutions, Roorkee, India

Abstract - The capability to provide network service even under a significant network system element disruption is the backbone for the survival of network technology in today's world, keeping this view in mind, the present paper highlights cryptosystem and Cross-Layer Protocol. A global initial key distribution method based on public key certificate chain shall be presented. And also present a method for survivability strategy in mobile network.

Keywords: Survivability, Mobile Network, Key Distribution Cross-layer protocol

8. Paper 13051402: Effect of Cross Layer optimization of Traffic Management in Ad HOC Mobile Network (pp. 50-53)

Anu Chaudhary, Department of information Technology, AKJ Institute of Technology and Management, GZB, India
K.K Gautam, Department of Computer Science & Technology, Phonics Group of Institutions, Roorkee, India
Nirbhay Ahlawat, Department of Computer Science & Technology, Phonics Group of Institutions, Roorkee, India

Abstract:- The optimal and distributed provisioning of high through output in Mobile Ad Hoc Network (MANET) is a network consisting of a set of wireless mobile routers and Communication with each other. The Network Mobility(NEMO) for the traffic represents the moving behavior of directional antenna and mobile rooters. Use the Cross-layer protocol in ad hoc wireless network we can drastically improve the utilization through overlapping communication is the different direction for the traffic. This paper highlight the challenge to find out a route of effect the cross-layer protocol for traffic-management in Ad Hoc wireless network. In present paper we propose mobility for traffic management in Ad Hoc wireless network by use of theory of Cross-layer protocol.

Keywords:-Ad hoc Network, Cross-layer protocol, Directional Antenna, Mobile Router, Network Mobility

9. Paper 31051403: Performance of and Traffic management for a Mobile networks by using Cross-layer protocol (pp. 54-58)

Anu Chaudhary, Department of information Technology, AKJ Institute of Technology and Management, GZB, India
K.K Gautam, Department of Computer Science & Technology, Phonics Group of Institutions, Roorkee, India
Nirbhay Ahlawat, Department of Computer Science & Technology, Phonics Group of Institutions, Roorkee, India

Abstract:- Over the Recent years a considerable amount of effort has been devoted towards the traffic management and root is the important capability to provide best network technology in today's world. Present paper we study the traffic management for mobile networks and we addresses current issue of the traffic management. Present the performance of Mobile Network by using Cross-layer protocol.

Index Terms:- Mobile Networks, call admission control, QoS (Quality of Service), route optimization

10. Paper 28021402: A Fast Survey Focused on Methods for Classifying Anonymity Requirements (pp. 58-63)

Morteza Yousefi Kharaji Department of Computer Science and Information Technology Mazandaran University of Science and Technology Mazanadan, Iran
Fatemeh Salehi Rizi Department of Computer Science and Information Technology Sheikh Bahaei University of Isfahan Isfahan, Iran

Abstract — Anonymity has become a significant issue in security field by recent advances in information technology and internet. The main objective of anonymity is hiding and concealing entities' privacy inside a system. Many methods and protocols have been proposed with different anonymity services to provide anonymity requirements in various fields until now. Each anonymity method or protocol is developed using particular approach. In this paper, first, accurate and perfect definitions of privacy and anonymity are presented then most important problems in anonymity field are investigated. Afterwards, the numbers of main anonymity protocols are described with necessary details. Finally, all findings are concluded and some more future perspectives are discussed.

Keywords-anonymity; privacy; online security

Building High Performance Computing Using Beowulf Linux Cluster

Sedeeq Hasan Albana Ali Al-Khazraji
College of Computer Sciences and Mathematics - Dept. of Computer Sciences
University of Mosul
Mosul - Iraq

Mohammed A. Younus Al-Sa'ati
Department of Administrative Affairs
The presidency of the University of Mosul
Mosul - Iraq

Nashwan Mahmod Abdullah
Al-hadba University College
Mosul - Iraq

A Beowulf Cluster is a type of apportioned parallel processing system, which consists of a collection of reticulated standalone computers working together as a single integrated computing resource generally having a single system image (SSI), that is the users generally view the clusters as a single system.

The relatively low cost of two commodity components which are the fast CPUs designed primarily for the personal computer and networks designed to connect personal computers together (in local area network or LAN) makes full advantage of the use of Beowulf Cluster, in this paper we benefit from these components to build larger system.

The model was implemented in this paper is using the message passing interface technique developed in C language and use Linux operating system and the goal is to build Beowulf cluster to solve large mathematic operation faster as an example for matrix multiplication and PI problem …etc. the same approach can be used in scientific applications that need supercomputing power or in various other areas like databases, multimedia, web services, etc. In addition the users can access any node of the cluster and use it independently as a local personal computer.

Keywords— parallel processing system ; Network; Networking and Systems; Linux.

I. INTRODUCTION *(HEADING 1)*

The increasing need of computing power ,and the high cost of supercomputers and their low accessibility have all led us to the research in clusters that are providing services similar to supercomputers at a low cost. Clustering has come a long time ago since the beginnings of the 1960s with the advent of high capability of the microprocessors and high speed networks. This has gained further momentum with the development of standard tools for high performance distributed computing. Clusters give us the advantage of using low cost PCs over a network that provides us a cost effective form of parallel computing. This Concept has led research institutions in discussing the possibility of sharing computing resources and the ability to meet the needs is a major consideration towards developing new systems. Based on this knowledge and experience, HPC with Linux clusters are considered in order to build a parallel computing system that will act as core role in the next-generation systems for supercomputer. To achieve that we used "Beowulf Cluster". [1]

A Beowulf Cluster is a kind of supercomputers. More specifically, is an apportioned parallel computer built from commodity components. This approach takes advantage of the astounding performance now available in commodity personal computers. By many measures, including computational speed, size of main memory, available disk space and bandwidth, a single PC of today is more powerful than the supercomputers of the past. By harnessing the power of tens to thousands of such low cost but powerful processing elements, you can create a powerful supercomputer.

a computer cluster consists of a set of loosely connected computers that work together so that in many respects they can be viewed as a single system. Clusters are usually deployed to improve performance and/or availability over that single computer, while typically being much more cost-effective than single super computers of comparable speed or availability. A cluster is a group of linked devices (computer or embedded devices), working together closely so that they form a single node virtually. The components of a cluster are generally, but not always, connected to each other through wireless or wired (Ethernet) that allows data to move between the nodes. Nodes come in many types but are usually built from processors designed for the PC. If a node contains more than one processor, it is called an SMP (Symmetric Multiprocessor) node. [2]

The main purpose of a Beowulf cluster is to perform parallel computations for solving large mathematical operations very fast. This is accomplished by running applications across many nodes simultaneously. These applications may perform in parallel; that is, they may need to coordinate during execution. On the other hand, they may be performing an

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

embarrassingly parallel task, or a large group of serial tasks. The main key factor in application performance in all cases is local node performance.

The PXE (Pre-execution environment) is a protocol by which nodes can boot the system based on a network-provided configuration and boot image. The system is implemented as a combination of two common network services. First, a node will DHCP (Dynamic Host Configuration Protocol) for an address. The DHCP server will return an offer and lease with extra PXE data. This extra data contains an IP address of a TFTP server (Trivial File Transfer Protocol), a boot image filename (that is served from the server), and an extra configuration string that is passed to the boot image. Most new machines support this, and accordingly many cluster management software systems use this feature for installations. This feature is implemented by the BIOS in motherboards with integrated Ethernet controllers, and in the on-card device initialization code on add-on Ethernet controllers.

II. REASONS TO USE CLUSTER

Cluster is used instead of a single computer for many reasons, the main reasons: performance. But the original reason for the development of Beowulf clusters was to provide cost-effective computing power for scientific applications, that is, to address the needs of applications that required greater performance than was available from single (commodity) processors or affordable multiprocessors. An application may desire more computational power for many reasons, but the following three reasons are the most common[3]:

A. The need for Real-time constraints

That is, a requirement that the computation finish within a certain period of time. Weather forecasting is an example. Another is processing data produced by an experiment; the data must be processed (or stored) at least as fast as it is produced.

B. Increase of Throughput

A scientific or engineering simulation may require large number of computations. A cluster can provide the resources to process many related simulations. On the other hand, some single simulations require so much computing power that a single processor would require days or even years to complete the calculation.

C. Memory capacty

Some of the most challenging applications require huge amounts of data as part of the simulation. A cluster provides an effective way to provide even terabytes (1012 bytes or one million megabytes) of program memory for an application

Another important reason for using clusters is to provide fault tolerance, that is, to ensure that computational power is always available. Because clusters are assembled from many copies of the same or similar components, the failure of a single part only reduces the cluster's power. Thus, clusters are particularly good choices for environments that require guarantees of available processing power, such as Web servers and systems used for data accumulation. Galan et al. [4] recognized three common hardware structure for parallel computing: shared memory machines that communicate through memory sustained on dedicated hardware and characterize with a very high bandwidth between memory and CPU; local memory device that communicate through networks of workstations and clusters; and local memory device that integrate in a loosely knit collaborative network. In these categories, Beowulf cluster falls into a local memory devices by messages through networks of workstations and clusters and each workstation maintains its individuality.

Clusters provide the computational power through the use of parallel programming, a technique for coordinating the use of many processors for a single problem [5].

III. IMPORTANT ASPECT AND COMPONENT IN CLUSTERING

There are many independent elements (component) that work together to create a cluster system the selection of operating system, networking, and security aspect. Here is the view of important aspect and component in clustering

A. Using Linux for a Beowulf

Probably the most important reason for using Linux to build a Beowulf is its adaptability and flexibility. Because Linux is open source, it can easily be modified, rearranged, and tweaked for whatever the task needed.

Some individuals may get pale at the idea of modifying the operating system, but never fear, Linux is actually very friendly. Because of the distributed development environment that has helped it become so successful, it is also easily modified and tweaked.

Linux support many types of processors. Intel, Alpha, IA32, IA64, and many others. You can choose to build your Beowulf from the fastest Intel core I7 server. Beside that Linux operating system is very small, In fact Linux can easily be compiled to use as little as 600 Kbytes of compressed disk space on a floppy so it can fit on embedded devices. And as we know small kernel is a kernel that is more likely to be stable.

B. Network Booting

Because of Linux flexibility, there are many options can be used to build a cluster. While most clusters are built using a local storage drive for booting the operating system, it is not really required. Network booting allow the kernel to be loaded from a network server. A specialized network adapters or system BIOS is required. Most companies are offering network boot-capable machines in their high-end servers. The most common standard is the Intel PXE 2.0 net booting mechanism. On such machines, the firmware boot code will request a network address and kernel from a network attached server, and then receive the kernel using TFTP.

C. Diskless Operation

Some applications and environments can work very well without the cost or management overhead of a hard drive. In some environments, operating system kernels and distributions may need to be switched frequently, or even between runs of an application. Reinstalling the operating

Identify applicable sponsor/s here. *(sponsors)*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

system on each compute node to switch over the system is generally difficult, as would maintaining multiple hard disk partitions with different operating systems or configurations. In such cases, building the Beowulf without the operating system on the local hard drive, if it even exists, can be a good solution. Diskless operation also has the added benefit of making it possible to maintain only one operating system image, rather than having to propagate changes across the system to all of the Beowulf nodes.

D. Secure shell

SSH allows for encrypted communication to and from the master node. The SSH daemon is the secure replacement of RLOGIN (remote login), RSH (Remote Shell) and Telnet (Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications). The OpenSSH package is not installed automatically with Ubuntu, which means the SSH remote access clients like SSH (Secure shell) and SCP (Secure Copy) are not available to users immediately. The SSH service should be downloaded.

Once SSH has been downloaded the root user should be able to remotely access any of the nodes in the cluster. This ability can be tremendously useful when one needs to replicate configuration files across several nodes of the cluster or to restart a service without being at the console of the specific node.

E. Parallel Programming with MPI

Message Passing Interface (MPI) is an application program interface speciation that allows processes to communicate with one another by sending and receiving messages between them. It is typically used for parallel programs running on supercomputers, where the cost of accessing non-local memory is high [6]. The processes have separate address spaces they communicate by sending and receiving messages. Each process would be running on a separate node. MPI is also supporting shared memory programming model. This means that multiple processes can read or write to the same memory location.

Sometimes normal program can be used by all the processes, but with distinct parameters. In this case, no communication occurs among the separate tasks. When the strength of a parallel computer is needed to attack a large problem with a very complex structure, however, such communication is necessary [7].

F. Measuring MPI Performance

There are many tools have been developed for performance measuring like MPPTEST program and The SKaMPI test suite. To get best test results is always obtained of own application, but a number of tests are available that can give a general overview of the performance of MPI on a cluster.

G. Hardware Considerations

Building a cluster, access to computers on which to install the software is essential. Therefore, it makes sense to cover this early in the process.

For sure it is necessary to have at least two computer machines when building a cluster. It is not essential that these machines have the same levels of performance and specifications. The only main requirement is that they both share identical architecture. For instance, the cluster should only consist of all Intel machines or all Apple machines but not a mixture of the two. In theory it is possible to mix architectures when building a cluster by using Java, but that is outside the scope of this paper.

Strictly speaking, the only hardware requirements when building a cluster is two computers and some type of networking hardware to connect them with.

1. Clusters specification

To get full benefits of a cluster, the right hardware must be used. For optimal performance, all nodes except the master node should have same hardware specifications. This is because the fact that one node which takes longer to do its work can slow the entire cluster down as the rest of the nodes must wait for the slow node to catch up. This is not always the case, but it is a consideration that must be made. Having identical hardware specs also simplifies the setup process a great deal as it will allow each hard drive to be imaged from a master instead of configuring each node individually.

2. The Master Node

There are four main considerations when building the master node. They are Processor speed, Disk speed, Network speed, and RAM.

- Processor Speed

  If the master node is participates in computation this will be critical. Many more tasks will be handled by master node than the slave nodes so a faster processor may be required to keep it from being behind others. Not forgetting that since the master node can be kept quite busy doling out work to the other nodes, a slowdown here can have a huge negative effect on the entire cluster as the slave nodes waste time waiting for their next instruction.

- Disk Speed

  As we know, major work is done on the cluster ,some time or another it need to be saved as files on a hard drive, disk speed for the master node is absolutely critical, made even more so due to the fact that most nodes make use of NFS (Network File System) which means that every node in the cluster will be competing for access of the master node's disk. A fast SCSI drive is recommended, but an IDE drive will work as well.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Network Speed

This is critical as well. Time spent transmitting data is time wasted. The faster the network, the better the performance of the cluster. This can be mitigated by a good deal if the programmer expressly tries to minimize the ratio of time on the network to time on the processor but it never hurts to have more network speed. Fast Ethernet is recommended, Gigabit Ethernet is ideal but basically any network speed will work. While not part of the master node per se, it is strongly recommended that a switch be used instead of a hub when designing the cluster network.

- RAM

In the master node RAM is crucial for two reasons. First, the more RAM, the more processes can be run without ingress the disk. Second, the Linux kernel can and will cache it's disk writes to memory and keep them there until they must be written to disk. Both of these raise the speed of the master node which is critical to good overall cluster performance.

3. Slave Nodes

The slave nodes need to execute two tasks: Perform the computations assigned to them and then send that data back out over the network. So, their disk performance is not critical. In fact, it is normal to have nodes without hard drives in a cluster. These diskless nodes reduce the cost of building a cluster and eliminate some of the time required to set a cluster up. This document, however, assumes that the slave nodes will have no hard drives DRBL(Diskless Remote Boot in Linux).

The three most important hardware considerations for slave nodes are processor speed, network speed and RAM.

- Processor Speed

Nodes primary function is executing mathematical tasks, it makes sense that the fastest processor should be used. The more processing power the better. Multiple processors for the nodes can be desirable but add another degree of complexity for programming an applications for the clusters. Not only must the programmer take distributed processing into consideration, but SMP as well. As of the time of this writing, Intel Core I 5's offer a good price/performance ratio.

- Network Speed

This affects the slave nodes in exactly the same way that it does the master node. See that section above for more information.

- RAM

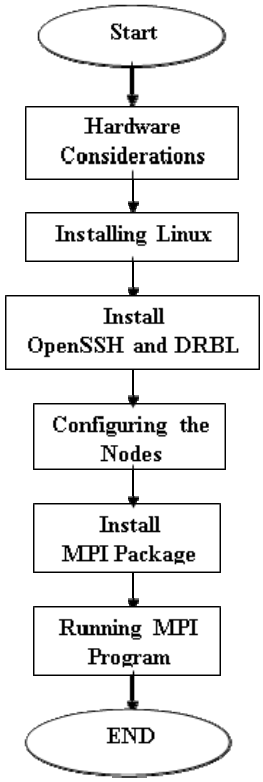
This affects the slave nodes in exactly the same way that it does the master node. See that section above for more information.

IV. DESIGN THE COMPUTER CLUSTER

Designing the Linux cluster model need a collection of Personal Computers (PCs) connected in one network together as a single resources in order to share their processors and other resources for computations and analysis that could be performed on any parallel machine. The cluster consists of a PC designated as the master while the other PCs on the network are the computational nodes as slaves.

The technology of cluster [8] that is being used is all active, that is, there is no primary or backup nodes. The cluster is designed from a set of heterogeneous mixture. The systems are networked together using a Fast Ethernet architecture of 100Mbps for data transfer and the cluster is designed in such a way that the nodes can access the master node and checks the status of the master through network commands issued from the node. Users should be able to log on to the master nodes through the client nodes.

The main steps of building the computer cluster is described in the following flowchart and this chapter will discuss each step alone:



Flowchart (1) main steps of building the computer cluster.

- **Running MPI Program**

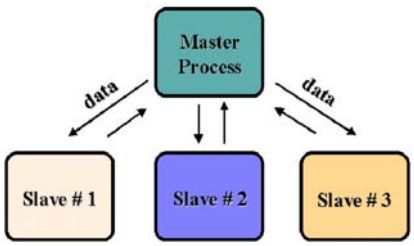


Figure 1 The client-server paradigm.

In case of run a program with multiple inputs, a parallel client-server implementation might just run multiple

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

copies of the code serially with the server granting the different inputs to each client process. As each processor finishes its task, it is assigned a new input. Alternately, task parallelism can be implemented at a deeper level within the code.

V. Testing Performance and Results

The biggest challenge we had to do for the use of a Beowulf cluster was the conversion of an existing serial code to a parallel code based on the message passing philosophy. The main difficulty with the message passing philosophy is that we have to ensure that master node is distributing the workload equally between all the other nodes. Because all the nodes have to synchronize at each time step, each PC should finish its task in about the same period of time. If the load is uneven or if the load balancing is poor, the PCs are going to synchronize on the slowest node, leading to a worst situation. Another hitch is the possibility of communication patterns that can deadlock. A typical example is if PC A is waiting to receive information from PC B, while B is also waiting to receive information from A.

- Calculating Value of Pi

A program to calculate the accurate value of mathematical constant PI (3.14) was evaluated for elapsed time and error in the calculated value. The benchmark value of PI was considered up to 25 decimal places whereas cluster computed the value up to 16 decimal places. Hence the error could be identified for 9 decimal places in accuracy as compared to the benchmark value using 25 decimal places. The error was observed to show very minor change which negligible and hence we focused mainly on the execution time of the program. Extensive use of machine file was made for submitting the processes.

The processes are allowed to move back and forth the master node depending upon the free resources. For example, say master node was allowed two processes. When the third process is to be scheduled, it will be scheduled on one of the slave node. In the meantime the fourth process is also queued and also one of the process on master node is terminated. Then there is no need to send the fourth process to the slave node, it will be executed on the master node itself.

Hence, processes were allocated dynamically depending on the free resources on a node, be it master or a compute node. Also note that the empty cells in table indicate that no output was obtained due to submission of processes beyond capacity of cluster.

Table 2 Calculation of Value of Pi

Number of Processes	Node = 1	Node = 3	Node = 5
5	0.001481	0.001008	0.001211
10	0.001641	0.003463	0.00357
50	0.047269	0.108689	0.11757
100	0.115619	0.252974	0.2752
200	-	0.55463	0.584591
300	-	0.98335	0.993251
400	-	2.901754	2.925887
550	-	-	3.102552

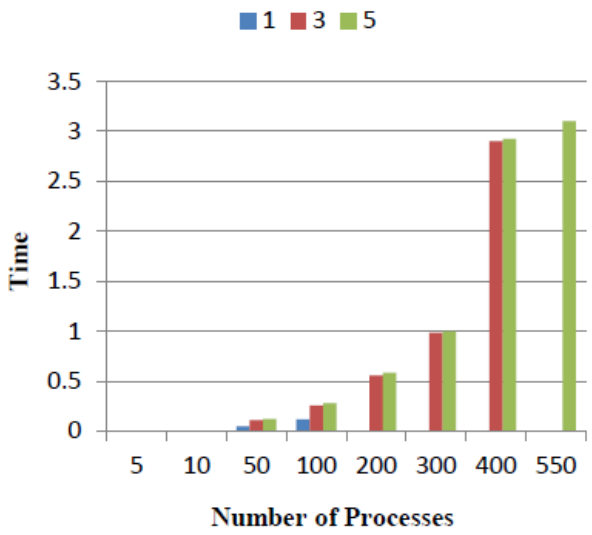


Figure 1 Calculation of Value of PI - Analysis

It can be seen from the graph that as the size of the problem increases i.e. the number of process increases the number of nodes needs to be increased else the problem cannot be solved to success. It was seen that a single node was not capable of running processes more than 100 whereas 5 nodes could run the problem as big as the 550 processes which is more than 5 times. In a sense the capacity of computation was increased by more than 5 times when running the same task on the cluster as compared to single node. Also it was seen that execution time of the same problem, on increasing the number of nodes, increased negligibly. This increase was because the time incurred on process migration which involved the process suspension on master node and resume on slave node. As the number of processes were increased to few hundred the time to break-up the problem and combine it for consolidated result was much higher than time incurred in migration. With increase in number of nodes the size of problem could also increase.

- **Matrix Multiplications**

The matrix operation is multiplying two input matrices to produce single matrix as a resultant matrix, 'a' and 'b', where matrix 'a' is a matrix of *N* rows by *P* columns and matrix 'b' is of *P* rows by *M* columns. The resultant matrix 'c' is of *N* rows by *M* columns. The serial realization of this operation is quite straightforward as listed in the following:

```
for(k=0; k<M; k++)
for(i=0; i<N; i++)
{
for(j=0; j<P; j++)
c[i][k]+=a[i][j]*b[j][k];
}
```

The algorithm of matrix multiplication is implemented in high performance Beowulf Linux cluster using the MPI send-receive paradigm. The server node reads

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

in the input data, which includes the number of slaves to be spawned, *numtasks*. Next , registering with nodes and receiving a *taskid*, then distributes the input graph information to each of them. The server obtains the result from each of the slaves. Since each slave needs to work on a distinct subset of the set of matrix elements, they need to be assigned instance IDs in the range (0... *numtasks-1*). The source code for serial and parallel is shown in Appendix A.

The matrix multiplication was run with forking of different numbers of tasks to demonstrate the speedup. Problem sizes were 100*100, 200*200, 300*300, 400*400, 500*500 and 600*600 in our experiments with one node attached to the master node. It is well known, the speedup can be defined as *Ts/Tp*, where *Ts* is the execution time using serial program, and *Tp* is the execution time using multiprocessor.

The execution times and corresponding speedups by using 20 processes with different problem sizes were listed in Figure 2. In, the corresponding speedup is increased for different problem sizes compared with the same problem size executed in serial .

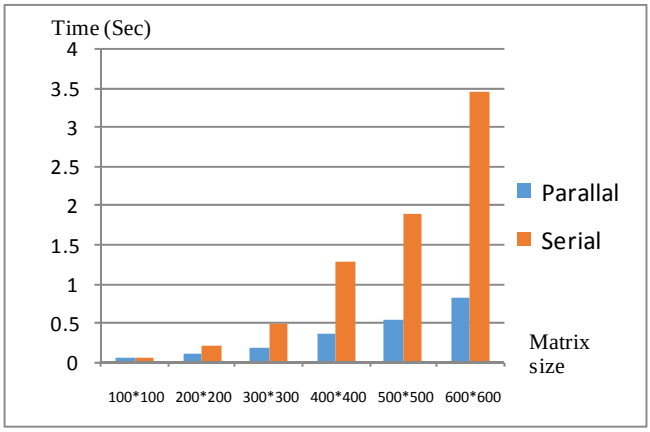


Figure 2 Execution times and corresponding speedups by using 20 processes compared with serial execution

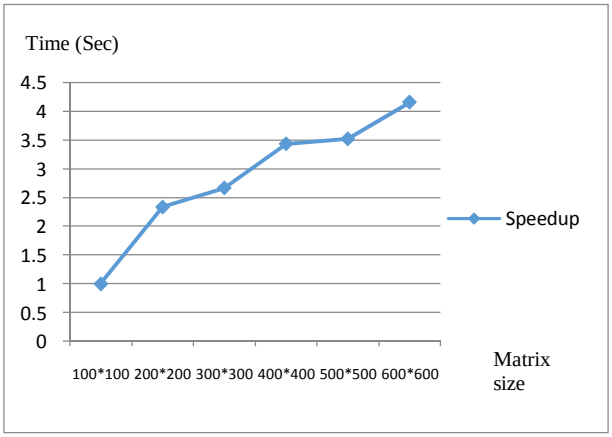


Figure 3 The speedup graph as Ts/Tp.

I. Conclusion

Scalable computing clusters are rapidly becoming the standard platforms for high performance and large-scale computing. It is believed that message-passing programming is the most obvious way to help programmer to take advantage of clustering symmetric multiprocessors (SMP) parallelism. A high performance computing cluster is built using DRBL and OpenMPI. The usage of DRBL simplifies the building process and maintenance. A hard disk is installed on each client node only to provide the local swap space. This cluster with system less clients can be one with diskless clients if the memory capacity on each clients is large enough.

It can be observed from the execution of the MPI programs that number of nodes in a cluster must be in accordance with the target application. Also that a larger application needs more number of compute nodes else the problem cannot be solved due to shortage on resources. The time required for process migration and consolidation of the result on the master node increase with increase in number of nodes. Thus it can be noted that number of nodes must be increased with a care so that performance gain can be genuinely achieved.

The performance test based on the testing codes using MPI shows consistent results. It is demonstrated that such a high performance computing cluster can be constructed from scratch for potential applications on computational physics problems.

As the number of compute nodes in modern HPC clusters continues to grow, it is critical to design clusters with low power consumption and low failure rate. In particular, it is widely known that the internal disk drives of compute nodes (in the case of disk full clusters) are a major source of failures. In addition, these disk full HPC clusters tend to require more power and cooling requirements compared to diskless clusters.

The advantages of Beowulf Diskless Remote Boot computing cluster are evident for any organization that requires high computational power. This is, when we take into account the performance/price ratio, easy scalability and upgradeability and recycling properties of the hardware components. If this is true for any organization, we are convinced that it is imperative for an academic institution like our University. Therefore we make a proposal of deployment of such a device starting with a schematic installation to be eventually enlarged and improved.

References

[1] Adams, J. and Vos, D. “Small College Supercomputing: Building a Beowulf Cluster at a Comprehensive College”, 33rd SIGCSE Technical Symposium on Computer Science Education, Covington, KY, February 2002, pp. 411-415.

[2] Shahram Nourizadeh, Y. Q. Song, J. P. Thomesse. “ A Location-Unaware Distributed Clustering Algorithm for Mobile Wireless Networks Using Fuzzy Logic”, In 7th IFAC International Conference on Field buses and Networks in Industrial and Embedded Systems (2007) Vol. 7, Part 1, 2007.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[3] Luiz André Barroso,Jeffrey Dean, and Urs Hölzle. Web search for a planet: The Google cluster architecture. IEEE Micro, 2003.

[4] Galan, J. M., Garcia, F., Alvarez, L., Ocon, A., Rubio, E. "Beowulf Cluster for High-performance Computing Tasks at the University: A very Profitable Investment. High performance Computing at Low Price", 2001. Available at <subs.emis.de/LNI/Proceedings/.../44_BeowulfClusterforHigh-PerfComp.pdf> accessed on August 25, 2011.

[5] S.Kumar C.Chong, "Sensor Networks: Evolution, Opportunities," in Proc. IEEE, Aug. 2003,vol. 91, no. 8.

[6] X.-D. Zhang, L. Xiao, and Y.-X. Qu, "Improving DistributedWorkload Performance by Sharing Both CPU and Memory Resources," Proc. 20th Intl Conf. Distributed Computing Systems (ICDCS 00), 2000.

[7] E. Gabriel, et al., "Open MPI: Goals, Concept, and Design of a Next Generation MPI Implementation," in Lecture Notes in Computer Science: Recent Advances in Parallel Virtual Machine and Message Passing Interface, Vol. 3241, D. Kranzlmuller, P. Kacsuk, J. Dongarra, Ed. Heidelberg, Germany: Springer Berlin, 2004.

[8] Bajwa, I.S., Chaudhri, A.A., Naeem, M.A. (2011) Processing Large Data Sets using a Cluster Computing Framework Australian Journal of Basic and Applied Science 5: 6. 1614-1618 June.

AUTHORS PROFILE

Sedeeq Hasan Albana Ali Al-Khazraji is a lecturert in Computer Sciences Department, College of Computers and Mathematics. University of Mosul. he received his MSC degree in computer sciences in 2011 in the speciality of operating system and computer networks. He interest with Distributed systems, Databases, and operating system subjects.

Mohammed A. Younus Al-Sa'ati I am Iraqi Nationality, an employee at the presidency of the University of Mosul , department of Administrative Affairs. I have had the GCSE in 1988 in Swansea (Dynevor comprehensive School), and B.Sc in computer science in Iraq (Mosul University) 2012. Computer Science is ever growing major. Such major is a constant state of flux meaning that new approaches are established on a daily basis and all the Iraqi universities are hardly coping with now a days streams regarding this major. Providing the opportunity to interact with peers of the same majors which provides the opportunity to engage in process of give and take process. Yours, Mohammed Akram Younus

Nashwan Mahmod Abdullah a lecturer in Al-hadba University College. The address of the thesis is digital image compression for band width reduction using jpeg standard.iam interest in computer engineering . Computer networking and communications. the subjects are microprocessor programming. digital image processing. Computer applications.

Evaluation of Cryptanalytic Algorithm for A5/2 Stream Cipher

Shahzad Khan [†], Shahzad Shahid Peracha [‡], Zain Ul Abideen Tariq[††]

Department of Communications System Engineering
School of Electrical Engineering and Computer Sciences (SEECS),
National University of Sciences and Technology (NUST), Islamabad, Pakistan

Abstract*-The stream cipher A5/2 is used in GSM (Global System for mobile Communication) for authentication and data encryption. There have been numerous successful attacks that were launched on A5/2 hence breaking down its security. In this paper an evaluation of Cipher-text only attack is presented with an easy understanding of the equation solver; how the equations are generated and solved. Furthermore this paper also reviews that how hardware-only attacker can easily recover the initial states of A5/2 that is more than enough in decrypting all other frames without any pre-computation and storage of the information. It also tries to suggest corrections in the design, if any, based on the deeper analysis of the operations.*

Keywords- A/5, GSM, cryptanalysis, stream ciphers

I. INTRODUCTION

GSM (Global System for Mobile Communication) the digital cellular system that has covered the entire mobile communications in Europe and Asia. As in mobile communication, the main dealing is with real time applications such as data, voice and video so using stream cipher is the best option for achieving authentication and data encryption. GSM uses A5/1 Stream Cipher for the very same purpose. This algorithm is implemented in Europe and is stronger version. Its variant A5/2 is used in Asia though it is a weaker version. The design of both the ciphers were confidential but were revealed in 1999 by reverse engineering.

There are some core flaws in these ciphers that are exploited and hence the security of entire GSM is easily be compromised. In any case if mobile phone supports a weaker cipher the security can be compromised whatever algorithm for security is used by GSM.

The attacks on A5/2 have been mostly based on software implementation and the efficiency count is also based on software but in this paper we analyze hardware implementation of the attack with detailed illustrations and minor adjustments to the existing algorithm. With the help of cipher-text only attack we achieve our goal of breaking the security of A5/2 without any pre-computation and storage. Hence our primary focus is on providing a review over the cipher-text attack only based on hardware implementation.

II. BRIEF DESCRIPTION OF A5/2 STREAM CIPHER

A5/2 is a stream cipher in which sender and receiver must be synchronized as this cipher is synchronous stream cipher requiring key stream, plain text and producing cipher text by XORing the plaintext with the key stream. A5/2 requires 64 bit key that we denote by $K= (k_0, k_1, k_2, k_3 \ldots\ldots\ldots k_{63})$ the key must be belonging to $GF(2^{64})$ it also required the 22 bit frame number that acts as an Initialization Vector (IV). The Initialization Vector must be defined under the GF (2^{22}) we identify the $IV = (IV_0, IV_1, \ldots. IV_{21})$. There is no privacy in the frame number as it is publicly known. In A5/2 there are four Linear Feedback Shift Registers (LFSRs). The length of each LFSR is relatively prime to each other. We recognize them R1, R2, R3 and R4 and the length of each register is 19, 22, 23, 17 bits respectively. In order to retain the desired properties of the LFSR we choose the primitive polynomial with maximum period and large linear complexity. R1, R2 and R3 are the registers used for producing the key stream and R4 is used to control the remaining 3 registers with the help of clocking signals. The internal structure of A5/2 is described in Table 1.

A. Initialization Phase

Initially the LFSRs are filled up with the 64 bit values of the key K, but before this all the registers are filled up with the 0. The key bits are inserted one bit at a time to all the registers in parallel. The first bit of the key is XORed with the ith position of register; each register is filled up with the 64 bit key. After every cycle the registers are clocked unconditionally. The similar step is followed for the Initialization Vector (IV) and its 22 bit frame number is inserted in the registers.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

LFSR	Length of LFSR	Primitive Polynomial	Clocking bit	Tapped bits
1	19	$x^{18} + x^{17} + x^{16} + x^{13} + 1$	8	13, 16, 17, 18
2	22	$x^{21} + x^{20} + 1$	10	20, 21
3	23	$x^{22} + x^{21} + x^{20} + x^{7} + 1$	10	7, 20, 21, 22
4	17	$x^{16} + x^{11} + 1$		16, 11

This process is summarized in following four steps:

Step 1: Initially all registers are filled with 0

$R1 = 0$; $R2 = 0$; $R3 = 0$; $R4 = 0$

Step 2: 64 bits of Key (K) from 0 to 63 bits are inserted

R1, R2, R3, R4 are regularly clocked

$R1[0] = R1[0] \oplus K_i$,

$R2[0] = R2[0] \oplus K_i$

$R3[0] = R3[0] \oplus K_i$

$R4[0] = R4[0] \oplus K_i$

Step 3: 22 bits of Initialization Vector (IV) from 0 to 21 bits are inserted

R1, R2, R3, R4 are regularly clocked

$R1[0] = R1[0] \oplus IV_i$,

$R2[0] = R2[0] \oplus IV_i$

$R3[0] = R3[0] \oplus IV_i$

$R4[0] = R4[0] \oplus IV_i$

Step 4: R1 [15], R2 [16], R3 [18] and R4 [10] are assigned 1

B. The Key Generation Phase

After the initialization phase the register R4 is clocked 99 times and the output is discarded. After this phase the registers R1, R2 and R3 are clocked irregularly based on the majority bits of Register R4. The clocking is determined by the bits R4[3], R4[7], and R4[10] in each clock cycle. The majority of the three bits are computed, and the registers R1, R2 and R3 are then clocked based on the majority function. R1 is clocked if R4[10] agrees with the majority. R2 is clocked if R4 [3] agrees with majority and R3 is clocked if R4 [7] agrees with the majority bit. In this way the registers are clocked irregularly and in each cycle at least two of the three registers are clocked.

C. Output Stream Bit Generation

In each register the majority of two bits and the complement of a third bit is calculated.

R1; majority (bit 12, complement of bit14, bit15)
R2; majority (bit 9, bit13, complement of bit16)
R3; majority (complement of bit 13, bit16, bit18)

The result of each majority bit and the right most bit of each register is XORed giving out the output bit. In this fashion 228 bits are generated the first 114 bits are used to encrypt the link from network to the subscriber and the remaining 114 bits are used to encrypt the link from subscriber to the network.

III. *Cryptanalysis Of A5/2 Cipher*

The cryptanalysis of the A5/2 stream cipher is presented in detail in [1] along with its hardware implementation. We present the an overview of each the individual blocks of hardware implementation of the proposed algorithm with some minor adjustments that we feel have been ignored. The cryptanalytic attack on the A5/2 stream cipher exploits some properties of the cipher blocks to deduce the initial secret states of the LFSRs. Before we look into the cryptanalytic architecture we elaborate the process of encryption tracking up to bit level the impact on the equations that are generated by the proposed architecture.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

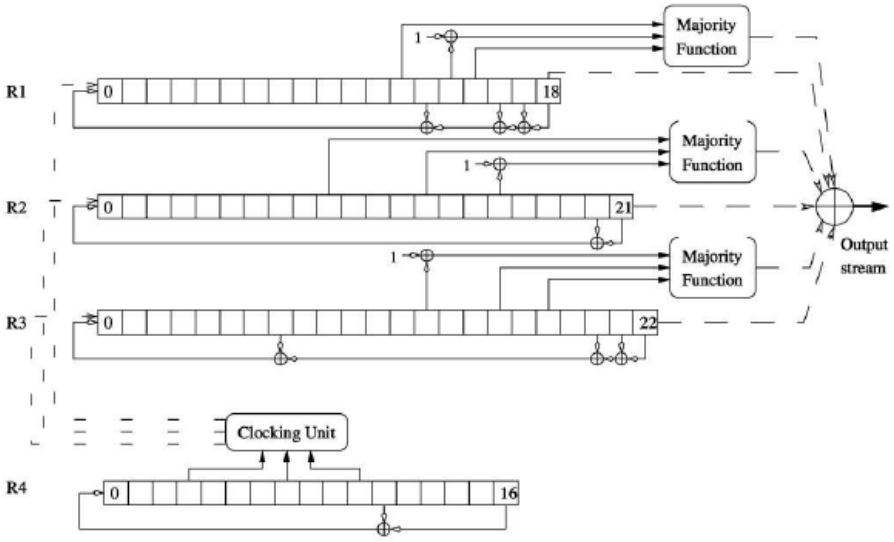


Fig 1: The schematic of the A5/2 stream cipher generation structure [1]

A. Brief Overview of Encryption Process

We have a brief overview of the encryption process as discussed by Bogdanov, Eisenbarth, and Rupp in their paper titled "A Hardware-Assisted Realtime Attack on A5/2 Without Precomputations" [1], to understand the impact of bit level processes on the cryptanalysis. The data blocks ID_0, ID_1 and ID_2 as shown in Fig 2 are passed through error correction coding block. In this case the error correction is provided by convolutional coding that adds redundancy on the data blocks and transforms 267 bit blocks into 456 bit blocks i.e CD_0, CD_1 and CD_2 respectively. That is further passed on to another block that performs reordering and interleaving on the coded blocks to evade the effect of burst errors that spreads out the errors in multiple blocks that appear as isolated errors easily corrected. The result of the reordering and interleaving block is the sixteen plaintext blocks. Thus we have data of three 456 bit blocks CD_0, CD_1 and CD_2 spread over sixteen 114 bit blocks P_0, P_1, and so on upto P_{15}. The A5/2 key stream generator takes in the initial 64 bit Key 'K' and 22 bit initialization vector IV (IV_0, IV_1, …. IV_{21}) and generates sixteen 114 bit key stream blocks S_0, S_1 and so on upto S_{15}. The stream blocks are XORed with the plaintext blocks to give cipher text blocks C_0, C_1 and so on upto C_{15}. This completes the encryption process as illustrated in Fig2.

We briefly narrow down to the reordering and interleaving block to see what really happens inside. As illustrated in the detailed diagram in Fig3, the three 456 bit blocks under consideration CD_0, CD_1 and CD_2 are reordered and interleaved resulting in the chunks of eight 57 bit blocks. The details of interleaving are narrowed down in the following section. The data of the three 456 bit blocks is spread over sixteen 114 bit plaintext blocks. As shown in Fig 3, the data of the block CD_0 is spread over eight blocks P_0, P_1 ..... P_7. Similarly the data of block CD_1 is covered by eight blocks P_4, P_5..... P_{11} and that of block CD_2 is covered by eight blocks P_8, P_9..... P_{15}. The bits in the first four 57 bit chunks of CD_0 are placed at the even positions of the plaintext blocks P_0, P_1, P_2 and P_3 while the odd positions are covered by the bits of last four chunks of the preceding block. Similarly the bit in the last four 57 bit chunks of CD_0 are placed at the odd positions of the plaintext blocks P_4, P_5, P_6 and P_7 while the even positions are covered by the bits of first four chunks of the CD_1 block. The similar procedure follows for CD_1 and CD_2.. We notice a specific property of the 456 bit encoded blocks CD_0, CD_1 and CD_2. This property can be summarized in following equation:

$$\mathbf{cdi,2j} \oplus \mathbf{cdi,2j+1} \oplus \mathbf{cdi,2j+2} \oplus \mathbf{cdi,2j+3} \oplus \mathbf{cdi,2j+6} \oplus \mathbf{cdi,2j+8} \oplus \mathbf{cdi,2j+9 = 0} \text{ where } \mathbf{0 \le j \le 184} \quad (1)$$

We exploit this specific property for cryptanalysis to find the initial secret states of the LFSRs of the A5/2 stream cipher. We notice that for any 456 bit block CDi we get 185 different equations satisfying above condition. Since the data of each of the CDi block is spread over eight plaintext blocks, we select the span of eight plaintext blocks to get the required bits

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

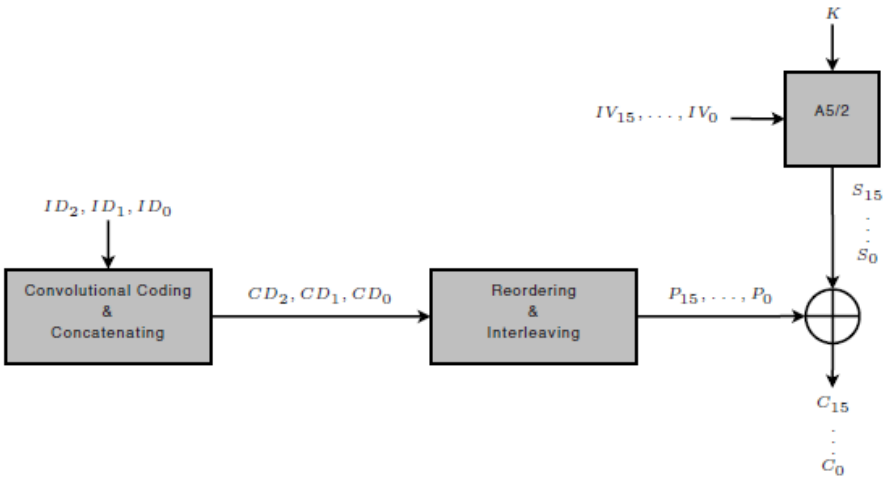


Fig 2: Block diagram showing the process flow of A5/2 Encryption [1]

satisfying above condition. These bits are carried forward onto the ciphertext blocks thus our focus shifts to eight consecutive stream bit blocks and respective ciphertext blocks satisfying above equation. This phenomenon is illustrated in Fig 3. The equation that we get becomes:

$$\begin{aligned}&\mathbf{cf}(i,2j) \oplus \mathbf{cf}(i,2j+1) \oplus \mathbf{cf}(i,2j+2) \oplus \mathbf{cf}(i,2j+3) \oplus \mathbf{cf}(i,2j+6) \\ &\oplus \mathbf{cf}(i,2j+8) \oplus \mathbf{cf}(i,2j+9) \oplus \\ &\mathbf{sf}(i,2j) \oplus \mathbf{sf}(i,2j+1) \oplus \mathbf{sf}(i,2j+2) \oplus \mathbf{sf}(i,2j+3) \oplus \mathbf{sf}(i,2j+6) \oplus \\ &\mathbf{sf}(i,2j+8) \oplus \mathbf{sf}(i,2j+9) \\ &= \mathbf{pf}(i,2j) \oplus \mathbf{pf}(i,2j+1) \oplus \mathbf{pf}(i,2j+2) \oplus \mathbf{pf}(i,2j+3) \oplus \mathbf{pf}(i,2j+6) \\ &\oplus \mathbf{pf}(i,2j+8) \oplus \mathbf{pf}(i,2j+9) \\ &= \mathbf{cd}i,2j \oplus \mathbf{cd}i,2j+1 \oplus \mathbf{cd}i,2j+2 \oplus \mathbf{cd}i,2j+3 \oplus \mathbf{cd}i,2j+6 \oplus \\ &\mathbf{cd}i,2j+8 \oplus \mathbf{cd}i,2j+9 = \mathbf{0} \end{aligned} \quad (2)$$

The function f(I,2j) in equation (2) shows the process of interleaving and reordering. After interleaving and reordering process we get the sixteen plaintext blocks and then subsequent ciphertext blocks after XORing with114 bit stream blocks. Fig 4 shows the bit level impact of the interleaving process and shows the case for CD_i when j = 1 and the equation (1) becomes

$$\mathbf{cd}i,2 \oplus \mathbf{cd}i,3 \oplus \mathbf{cd}i,4 \oplus \mathbf{cd}i,5 \oplus \mathbf{cd}i,8 \oplus \mathbf{cd}i,10 \oplus \mathbf{cd}i,11 = \mathbf{0} \quad \text{where } \boldsymbol{j} = \mathbf{1} \quad (3)$$

After reordering and interleaving we observe from Fig 4, that this equation depends on five plaintext blocks and consequently five ciphertext and stream bit blocks. For the equation (3) the blocks are P_0, P_2, P_3 , P_4, P_5. We refer to Fig 4 in the following section to see how this information helps us in understanding the cryptanalysis architecture. From this point we move on to the brief overview of the cryptanalysis process.

B. Overview of Cryptanalytic Process

As discussed in the previous section, we exploit the property of the encoded blocks that reflects in different form ehil going through the interleaving and reordering process. We keep track of the bits

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

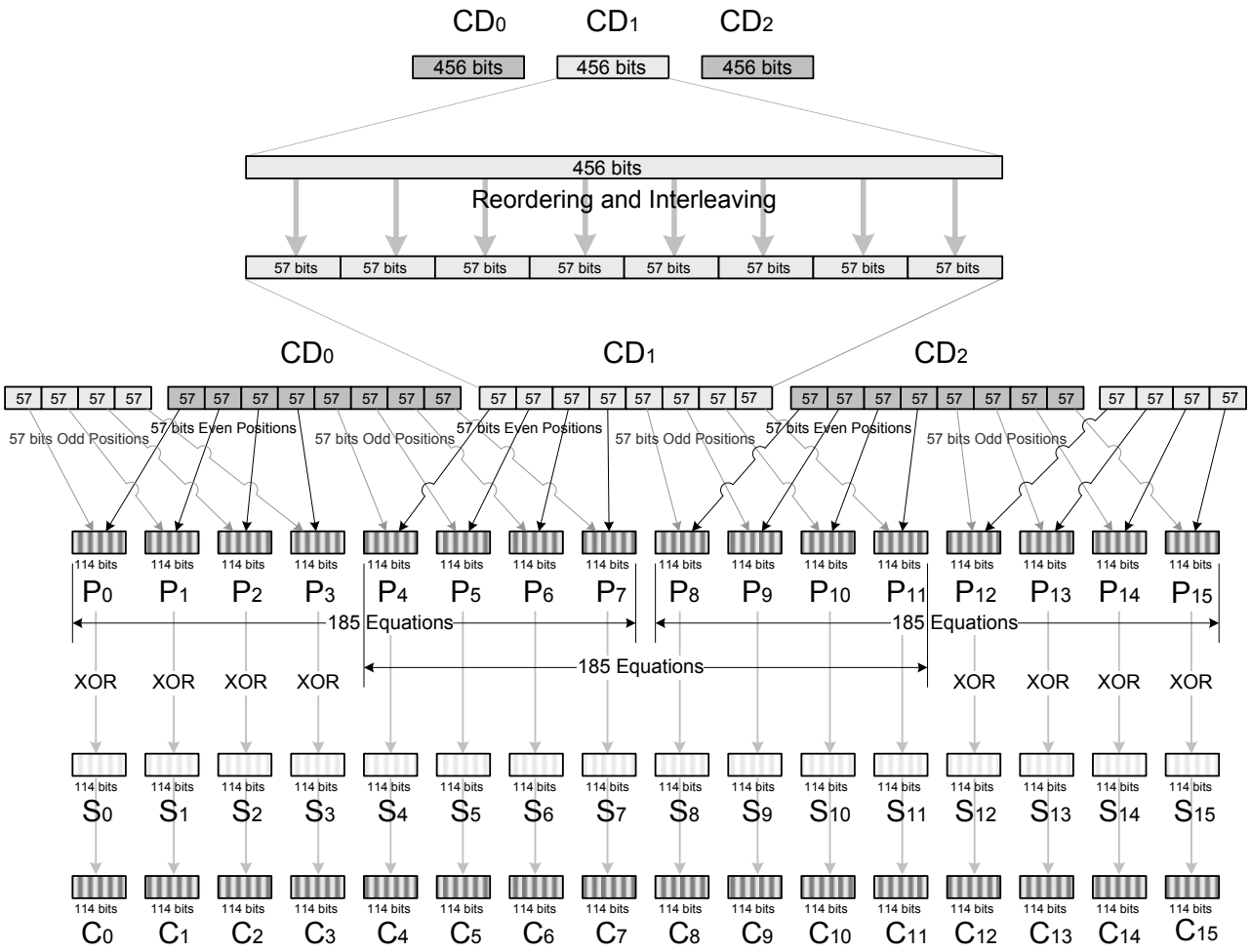


Fig 3: Detailed overview of the encryption process preceded by interleaving

0

required to satisfy one of the equations given as equation (3). The overview of the cryptanalytic architecture is given in Fig 5. The Process of cryptanalysis begins by identifying the main unknown values that are to be sorted out to break the cipher. During the process what we are available with are sixteen cipher text blocks from air. Then we know that the stream blocks used to encrypt the plaintext blocks are unknowns. To determine the stream bits we go back into the process of encryption and identify the secret initial states of the LFSR's being the main candidate of unknowns to be found out. We denote the initial secret states of the LFSR, as α_0, α_1, α_2, α_3, α_4, and so on till α_{77}. This gives us total of 78 initial secret states that we are required to find out during the process.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

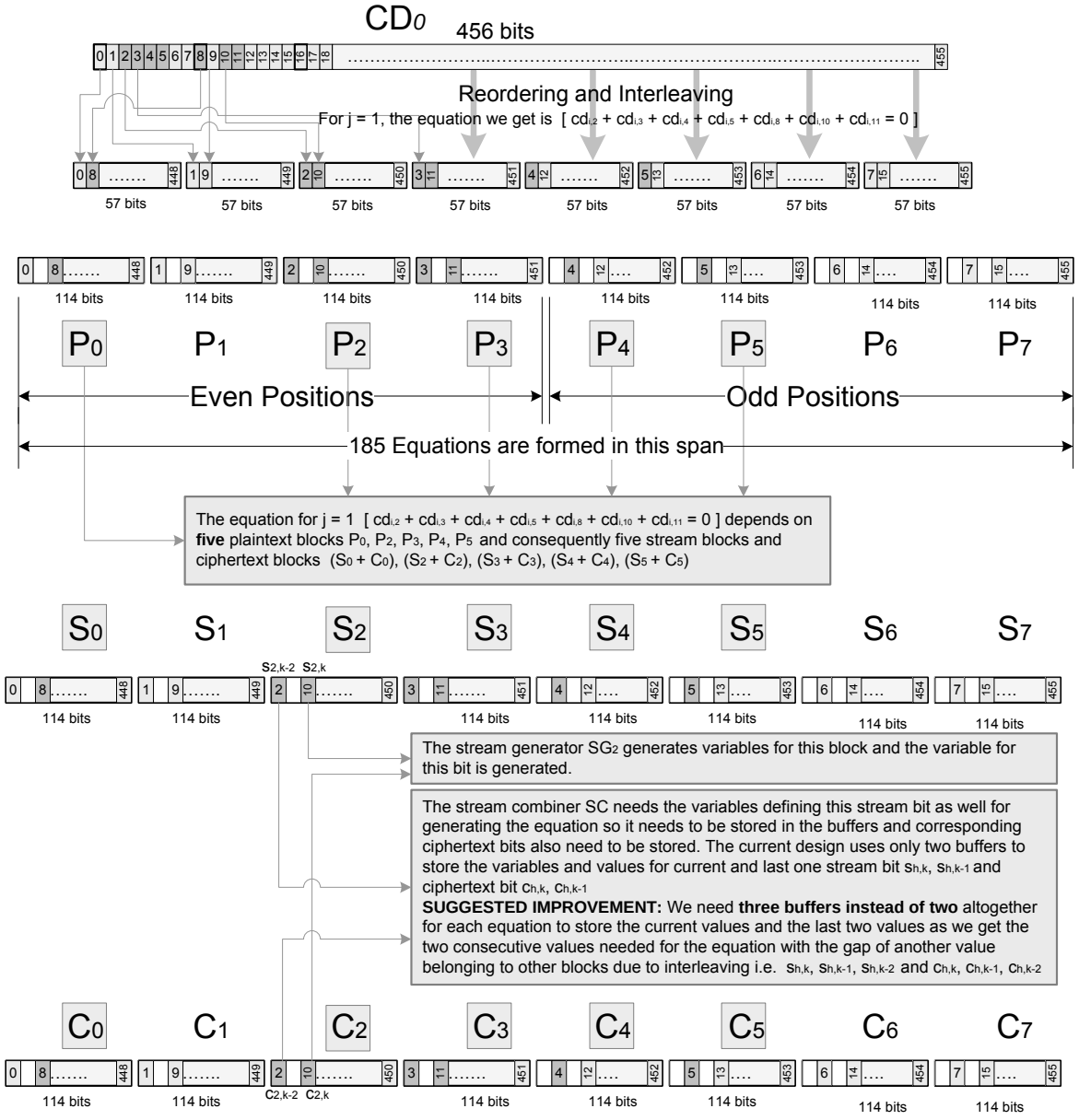


Fig 4: Detailed overview of the encryption process preceded by interleaving

During the encryption process and generation of stream bits using majority function of the three LFSRs R1, R2 and R3 we observe that we get different combinations of the terms $\alpha_0, \alpha_1, \alpha_2, \alpha_3$, to α_{60} that contribute to each of the stream bit $s_{h,k}$. We have following combinations possible:

$$^{18}C_2 + {}^{21}C_2 + {}^{22}C_2 + 61$$
$$= (18)(17)/2 + (21)(20)/2 + (22)(21)/2 + 61$$
$$= 594 + 61 = 655 \text{ (plus a constant)}$$

The above expression shows that there are 61 values comprising of single variable $\alpha_0, \alpha_1, \alpha_2, \alpha_3$, to α_{60} while 594 values are quadratic combinations of these single variables. We take these quadratic combinations as new variables, summing total variable up to 655. The different combinations of these variables give the stream bits as output. This assumption is used in [1] to propose the cryptanalytic architecture. The said architecture as shown in Fig 5 comprises of five main blocks:

1) Ciphertext Module (CM)
2) Equation Generators (EG)
3) Linear System of Equation (LSE) Solver
4) Key Tester (KT)
5) Control Logic Unit (CLU)

We briefly touch each of these blocks and present an overview of their internal working.

1) Ciphertext Module (CM)

This module contains buffers to store the ciphertext blocks an the Initialization Vectors (IV). For ciphertext block it has 24 memory locations to store the blocks in the groups of eight that are further required for processing by the Equation Generator (EG) block. The Initialization Vectors (IV) are stored in 16 memory modules. The first bit of each of the 24 ciphertext

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

memory modules is connected to the Equation Generator (EG) module that is rotated forward or backward to access other bits. Similarly the same bit are provided to Key Tester (KT) module.

2) Equation Generator (EG)

The Equation Generator Module consists of three EG sub modules named as EG_0, EG_1 and EG_2. The three sub modules are meant to generate equations for CD_0, CD_1 and CD_2. Each of the EG sub module operates on eight ciphertext blocks and generates 185 equations

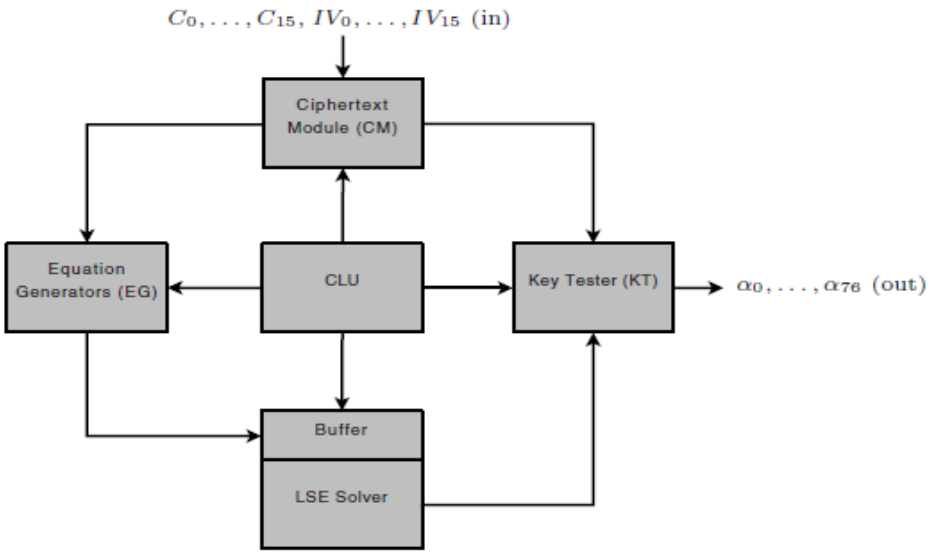


Fig 5: Overview of Cryptanalytic architecture [1]

satisfying the condition given in equation (1). The total of 555 equations generated from the three EG sub modules are then passed on to the LSE Solver for further processing. The three sub modules of EG operate on the eight consecutive ciphertext blocks to generate equations from the data spread over these blocks. The sub module EG_0operated on blocks C_0 to C_7. The sub module EG_1 operates on the blocks C_4 to C_{11} and consequently EG_2 operates on blocks C_8 to C_{15}. Fig3 clearly shows how the data of CD_0, CD_1 and CD_2 are spread over the plaintext blocks and then carried onward to the ciphertext blocks. Each of the sub modules EG_i contains eight Stream Generator SG blocks and a stream combiner (SC) block as shown in Fig 6. Each of the Stream Generators SG_i is meant to generate the 655 variable coefficients (along with a constant) for the 114 stream bits associated with each of the eight ciphertext bits. Each ciphertext bit is XORed with the constant value generate from the SG_i and then stored in the buffer. The Stream Combiner (SC) has a job of taking appropriate values from the output of each of the SG_i and combine them and pass it on to the LSE block. As shown in Fig 4 we observe that we need the current value and some of the old values to form an equation.

a) Suggested Improvement & Analysis

Fig 6 shows the buffers at the output of the SG_i but we show with the help of Fig 4 that there needs to be some correction as there are only two buffers to store the current and the previous coefficient values, while we need to have three buffers because we get the right pervious value before two stream bits due to the effect of interleaving. We show this correction in Fig 8.

Focusing on Stream Generator (SG) we have architecture as shown in Fig 7 for all three LFSRs. Instead of single row vector LFSRs was have multiple row LFSRs with each row representing 61 unknown variables and a constant value while the locations of these LFSRs represents the coefficients of those variables as their dependencies at those positions of LFSRs. Fig 7 shows the vector LFSR for R1 only and their respective dependencies. These are explained in detail in [1]. The addition of the extra buffer would increase hardware as 24 memory locations of 656 bits are added in EG module and 24 more are added in KT module. It does not increase the power consumption because only two resisters at a time are clocked to generate the equations. But there will be power overhead for there are two registers being updated for each output of SG_i in present design as shown in Fig 6 while after correction three registers are updated as shown in Fig 8.

3) Linear System of Equation (LSE) Solver

The Linear System of Equation (LSE) Solver module buffers in 555 equations in its buffers while each equation is represented by 655 variable coefficients while 655 unknowns are to be found. The process used for this purpose is Guass Jordon Elimination that is discussed in [1].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

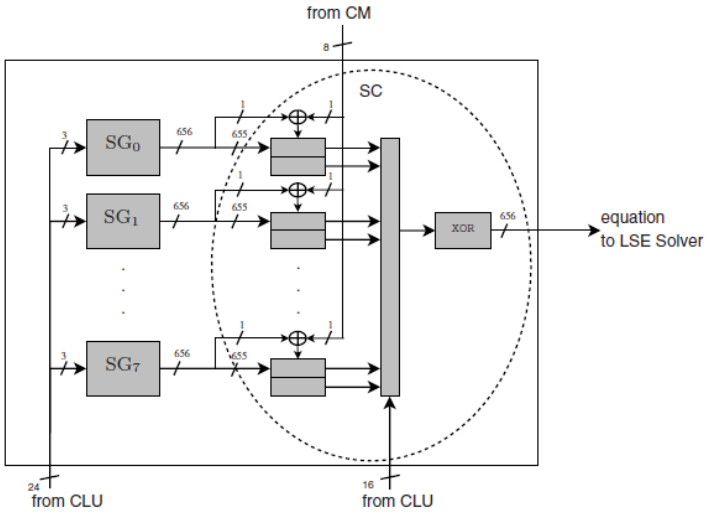


Fig 6: Overview of internal structure of Equation Generator sub module (EG_i) [1]

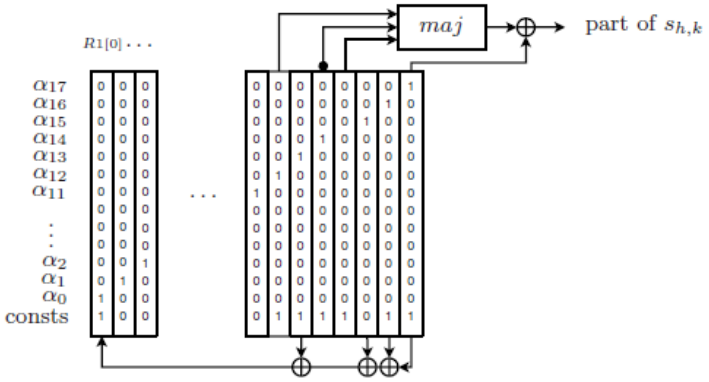


Fig 7: Overview of internal structure of LFSR R1's representation in SG[1]

The equations are arranged in m x n matrix where m is the number of rows and that equals to 555 representing the total number of equations while n represents the total number of variable inclosing the constant value that is equal to 656. Using this process we are able to get a candidate value of initial state variables α_0, α_1, α_2, α_3, to α_{60}. This candidate is then passed on to the Key Tester (KT) for verification if the calculated candidate for the initial secret state is correct or not.

4) Key Tester (KT)

The key tester module takes the candidate values from the LSE Solver and verifies its correctness. The Key Tester (KT) module contains the same A5/2 encryption architecture. It sets the initial state candidate values in the LFSRs and calculates the output stream bits that are XORed with right ciphertext bits from Ciphertext Module (CM) and then passed on to stream combiner that take in right values, generates equation satisfying condition in equation (q) to test if its values are equal to zero. If any of the values comes out to be one then the candidate fails and new candidate value is generated by LSE Solver and then tested again at Key Tester (KT) module. These values are tested for all possible values of R4 LFSR. Similarly the equations in Equation Generator (EG) module are generated for al possible values for R4 LFSR.

5) Control Logic Unit (CLU)

The Control Logic Unit (CLU) is used to control the operations of all the four modules by clocking then and giving out control signals. This is also discussed in detail in [1].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

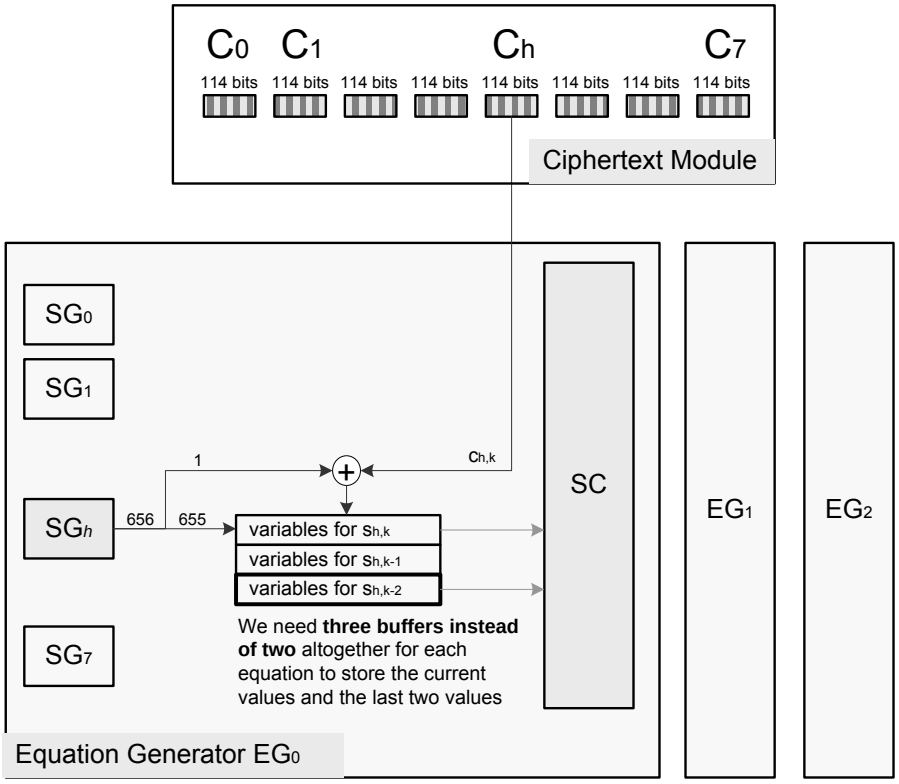


Fig 8: Overview of the Equation Generator (EG) sub module showing correction in the number of buffers to be used as three instead of two.

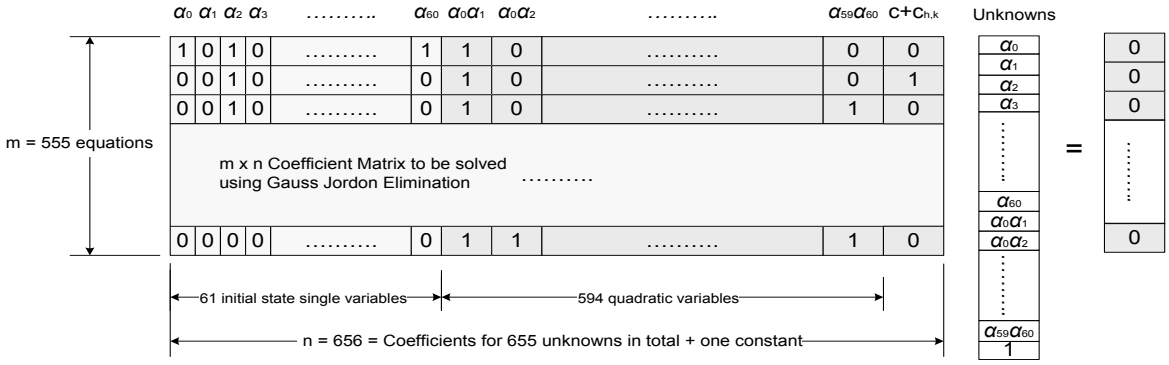


Fig 9: Overview of LSE Solver process

IV. CONCLUSION

We presented the overview of the cryptanalytic attack on the A5/2 cipher and the proposed hardware architecture to carry out the cryptanalysis and suggested some minor corrections that contribute to the improvement in the design based on the bit level analysis of the data.

REFERENCES

[1] *Andrey Bogdanov, Thomas Eisenbarth, and Andy Rupp. "A Hardware-Assisted Realtime Attack on A5/2 Without Precomputations", Horst-G¨ortz Institute for IT-Security, Ruhr-University Bochum, Germany*

[2] *Third Generation Partnership Project. KASUMI Specication. Techni-cal report, Security Algorithms Expert Group (SAGE), 1999. Version1.0.*

[3] *Gregory G.Rose and Philip Hawkes. "On the Applicability of Distin-guishing Attacks Against Stream Ciphers". 3rd Nessie Workshop, 2002.*

[4] *Matthew J.B. Robshaw. Stream Ciphers. RSA Laboratories Technical Report TR-701 (version 2.0), 1995.*

[5] *Andrew Roos. "Class of Weak Keys in the RC4 Stream Cipher". 1995.Posting in sci.crypt.*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[6] *Rainer A. Rueppel. Correlation Immunity and the Summation Generator. In Hugh C.Williams, editor, Advances in Cryptology-CRYPTO'85,Santa Barbara, California, USA, August 18-22, 1985, Proceed-ings, volume 218 of Lecture Notes in Computer Science, pages 260{272.Springer, 1986.*

[7] *Rainer A. Rueppel. Stream ciphers. In G.J.Simmons, editor, Contemporary Cryptology: The Science of Information Integrity, pages 65{134. IEEE Press, 1992.*

[8] *Bruce Schneier. Applied Cryptography, 2nd Edition. John Wiley & Sons,1996.*

[9] *Werner Schindler. A Combined Timing and Power Attack. In David Nac-cache and Pascal Paillier, editors, Public Key Cryptography, 5th Interna- tional Workshop on Practice and Theory in Public Key Cryptosystems.*

[10] *Frederik Armknecht. "A Linearization Attack on the Bluetooth Key Stream Generator. Cryptology" ePrint Archive (http://eprint.iacr.org/), Report 2002/191, 2002.*

[11] *Lenore Blum, Manuel Blum, and Mike Shub. "A Simple Unpredictable Pseudo-Random Number Generator". SIAM Journal on Computing,15:364{383, 1986. urnal on Computing,15:364{383, 1986.*

[12] *David Wagner. "My RC4 weak keys. 1995. Postinginsci.crypt,availableat http://www.cs.berkeley.edu/~daw/my-posts/my- rc4-weak-keys.*

[13] *J.Golic. "Cryptanalysis of Alleged A5 Stream Cipher". In Proc. of Eurocrypt'97, volume 1233 of LNCS, pages 239–255. Springer-Verlag, 1997.*

[14] *A.Biryukov, A.Shamir, and D.Wagner. Real Time Cryptanalysis of A5/1 on a PC. In Proc. of SE'00,volume 1978 of LNCS, pages 1–18. Springer- Verlag, 2001.*

[15] *P. Ekdahl and T. Johansson. " Another Attack on A5/1". IEEE Transactions on Information Theory,49(1):284–289, 2003.*

[16] *E. Barkan, E. Biham, and N. Keller. " Instant Ciphertext-only Cryptanalysis of GSM Encrypted Communication ". (full-version). Technical Report CS-2006-07, Technion, 2006.*

[17] *I.Goldberg, D.Wagner, and L. Green." The Real-Time Cryptanalysis of A5/2". Presented at the Rump Session of Crypto'99, 1999.*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Simulation And Modeling Of Handover Failure And Call Drop In GSM Network For Different Scenarios

Syed Foysol Islam
Faculty of Engineering
University Of Development Alternative (UODA)
Dhaka, Bangladesh

Fahmi Ahmed
Faculty of Engineering
University Of Development Alternative (UODA)
Dhaka, Bangladesh

***Abstract*— In this Research paper, the simulations of call drop and handover failure in GSM network tele-traffic through OMNeT++ are presented. The results obtained in different scenarios are examined and analyzed which simulates a large business city in busy hour a number call attempts by the mobile phone users, with different characteristics of network coverage. This simulator is a discrete event simulator programmed in OMNeT++, focusing on the research of wireless or wired networks. It is also a flexible environment which allows its extension to different aspects of GSM technology, such as the simulation of successful calls, call drops and handover failure probabilities etc.**

Keywords- Graphical NED Editor; Integrated Development Environment; Mobile Station; Base Transceiver Station; Integrated Services Digital Networks; OMNET;

I. INTRODUCTION

Building a simulation of a telephone system GSM cellular mobile OMNET using the simulator to measure the parameters Recommended minimum quality voice service. The main objective of this research paper is to create the different environments of simulation and measurement on the system of GSM cellular phone. Another objective is to design and construct a simulation of a cellular mobile telephone system GSM by using the simulator OMNET. In this research paper the specific objective is to analyze the operation under minimum parameters on the voice channel in the implementation of a simulation of a cellular telephone system GSM technology through OMNET and analyzing the results of building simulation.

II. SIMULATION TECHNIQUE FOR ANALYSIS

OMNET simulator generates an output of the simulation, which is given into data files, output vector files, output scalar files, and possibly the users own output files. The output vector file allows observing the behavior of each MS in simulation time. This is to analyze the behavior of the minimum standards of quality that must be provided to the GSM Cellular System. OMNET simulator generates an output vector file which allows observing the behavior of each MS in simulation time. This is to analyze the behavior of the minimum standards of quality that must be provided to the GSM Cellular System. OMNET contains graphical publishers Scalars and Plove which generates result in graphical form, therefore facilitating the analysis of the simulation [1].

III. RESULT ANALYSIS IN DIFFERENT SCENARIOS

A. TABLE-1: General Characteristics of Scenario 1

Properties	**Characteristics Data**
Simulation area:	1 km^2 (1000 m × 1000 m)
Number of MS:	50 mobile stations
	30 MS with linear trajectories
	20 MS with random trajectories: change direction after lifetime (random between 0 to 200 s)
Speed of MS:	(minimal 0.0 m/s) (maximum 7.1 m/s) (average 1.7 m/s)
Power measurements:	one measure per second
MSISDN:	6009000xx, where xx is the MS number (from 0 to 49)
Number of MSC:	1
Number of BTS:	1
Transmission power of BTS:	4 dBm
Position of the BTS:	The simulation area has permanent coverage of the BTS.
Number of traffic channels of the BTS:	14
Calls processing in MS:	Exponential function with inter-arrival time of 10 min
	Exponential service time distribution (duration of calls) with average service time of 2 min (120 s)
Probability of intra - MSC calls:	0% (every MS calls always to another MS out of the simulation that is assigned to a factitious MSC not present in the simulation).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Scenario 1:

There is a single BTS situated in the center, which manages the total area. The transmitted power attenuation of 4 dB m corresponds to a circumference of radius 731 m. This scenario includes 50 MSs moving inside the zone of study, 30 of which have linear trajectories and 20 have random ones. This scenario is quite simple, but contains enough GSM parameters to obtain several conclusions. The configuration file also collects information about the initial position and speed of each MS. Remember that not all MSs have the same speed. The service time distribution is exponential with average service time established in 2 min (120 s). The single BTS is also positioned on the center. Over this point, (500; 500) of the simulation area, the MS has an attenuation which fits with the maximal in the graphic. Due to the BTS having 14 traffic channels to serve the communication demand, the number of busy traffic channels is always less than or equal to 14. When the BTS has the 14 traffic channels assigned, congestion in calls is produced. During congestion, any new call attempts will be rejected. This scenario considers that all calls are out-MSC, i.e. every MS in the simulation area is calling to a fictitious MS depending on another MSC not present in the simulation area [2].

By applying this scenario we simulate the Omnet & get the following Graphs. The different analytical graphs of the same MSs according to the scenario are given below:

FIGURES OF SCENARIO 1

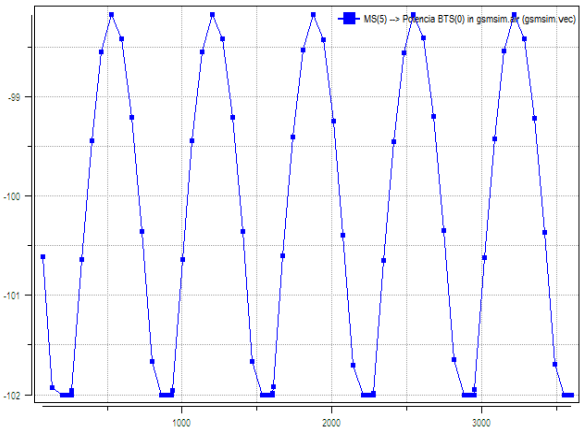


FIGURE-1: Analysis of the results Received Power & Simulation Time at MS (5) in scenario 1.

Here the examples of MS in Scenario-1, shows the received power of each MS from one BTS. This figure shows the graph of MS (5) from BTS (0). In this scenario, there is 50 MS & 1 BTS.

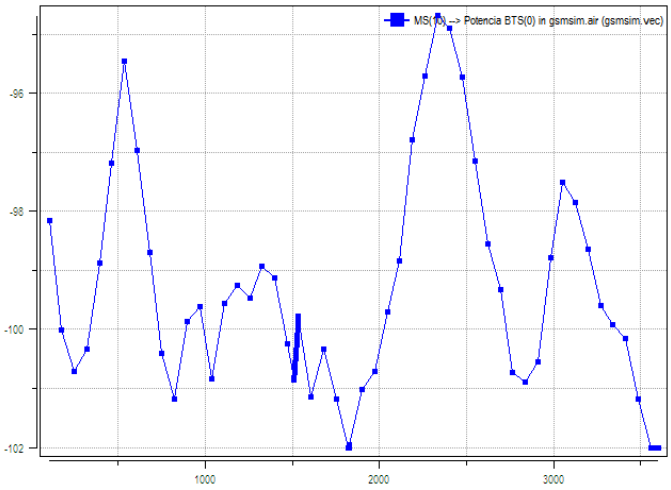


FIGURE-2: Analysis of the results Received Power & Simulation Time at MS (10) in scenario 1.

Figure-2 shows the graph of MS (10) from BTS (0). Here MS in Scenario-1 shows the received power of each MS from one BTS. In this scenario, there is 50 MS 30 linear & 20 random. Total power is 4 dB. The trajectories of every MS in the area during a busy hour simulation show the BTS coverage. Fig.1 shows MS with 5 identifier and with a linear (path type 0) trajectory. Fig.2 shows MS with 10 identifier and with a random (path type 1) trajectory.

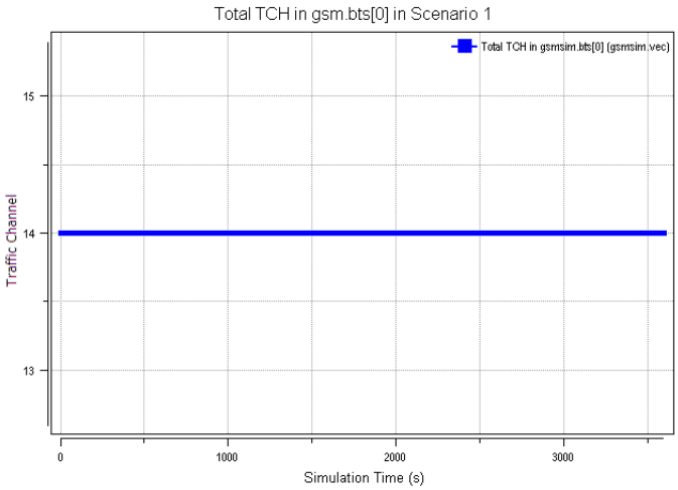


FIGURE-3: Analysis of the total channel of BTS (0) in scenario 1.

The total Traffic Channel (TCH) is a logical channel that allows the transmission of speech or data. In most second generation systems, the traffic channel can be either full or half rate.

*B. **TABLE-2**: General Characteristics of Scenario 2*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Properties	Characteristics Data
Simulation area:	4 km^2 (2000 m × 2000 m)
Number of MS:	50 mobile stations
	30 MS with linear trajectories
	20 MS with random trajectories: change direction after lifetime (random between 0 to 200 s)
Speed of MS:	(minimal 0.0 m/s) (maximum 7.1 m/s) (average 1.7 m/s)
Power measurements:	One measure per second
MSISDN:	6009000xx, where xx is the MS number (from 0 to 49)
Number of MSC:	1
Number of BTS:	3
Transmission power of BTS:	7 dBm
Position of the BTS:	there is a small area without coverage of the BTSs.
Number of traffic channels of the BTS:	7
Calls processing in MS:	Exponential function with inter-arrival time of 10 min
	Exponential service time distribution (duration of calls) with average service time of 3 min (180 s)
Probability of intra-MSC calls:	33% (probability that a call generated in the current MSC has as destination another MS located in the same MSC).

- Scenario 2:

In this scenario, there is three BTSs situated approximately equal distances, which manages the total area of MSC. The transmitted power attenuation of 7 dBm in Table-2 summaries the main characteristics of Scenario-2. Table-2 is an extract of the configuration file 'omnetpp.ini'. As in Scenario 1, it is a busy hour. The area simulation of Scenario-2 is larger than the first scenario. In this scenario we assign 2 kilometers long to both sides of the square area. Some parameters are similar in both scenarios, as number of MSs. This scenario also includes 50 MSs moving inside the zone of study, 30 of which have linear trajectories and 20 have random ones [3].

In this case, the simulation is on a network with a single MSC; however, the program can simulate calls between MSs within the simulation and other MSs which depends on a MSC out of the simulation area. Scenario-1 worked only with calls from a MS to a fictitious MS connecting to another MSC, but Scenario 2 considers calls between MSs present in the area and so is depending on the current MSC. This scenario assigns the probability of 33% of intra-MSC calls and also indicates average rates of service time & call generating distributions. The average service time call is now 3 minutes and the calls generating process of each MS is an exponential distribution of average rate of 1/600 calls per second, that means call attempts every 10 min. We consider three BTSs in the simulation. We have defined these three BTSs to be approximately of equal range. The most significant BTS characteristics are 7 traffic channels and a transmission power of 7 dB m. We observe that in this case there are MSs moving in zones without coverage. Any call attempt on those positions will fail. By applying this scenario we simulate the Omnet & get the following Graph.

FIGURES OF SCENARIO 2

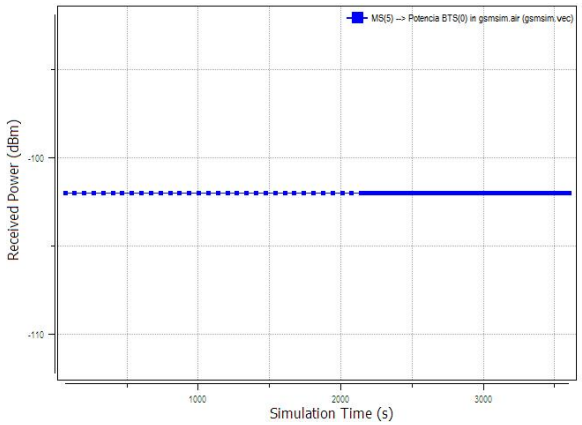


FIGURE-4: Analysis of the results Received Power & Simulation Time at MS (5) in scenario 2.

Here are the examples of MS in Scenario-2 that show the received power of each MS from the three BTS. In this scenario number of MS is 50. This figure shows the graph of MS (5) from BTS (0).

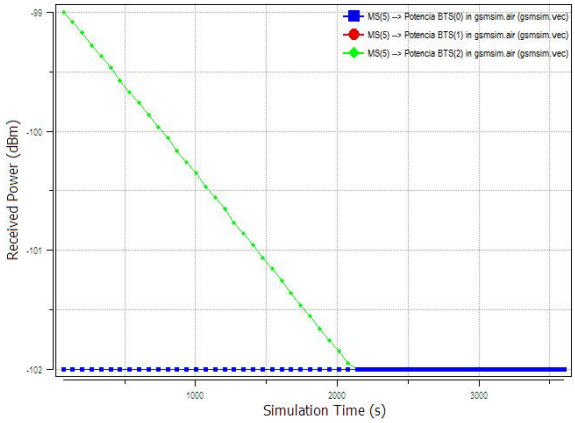


FIGURE-5: Analysis of the results Received Power & Simulation Time at MS (5) in scenario 2.

In figure-5, the examples of MS in Scenario-2 that show the received power of each MS from the three BTS. This figure shows the graph of MS (5) from BTS (0), BTS (1) & BTS (2). In this scenario, number of MS is 50.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

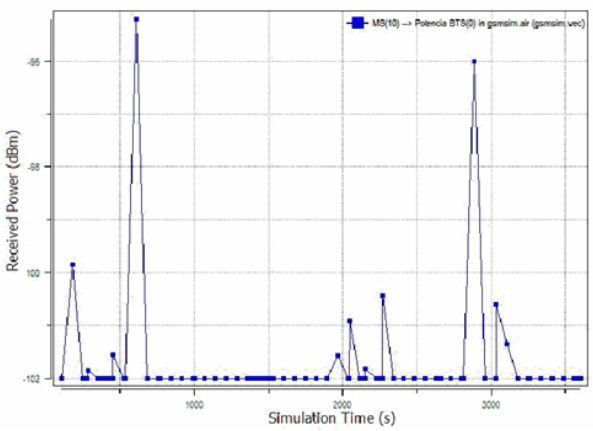


FIGURE-6: Analysis of the results Received Power & Simulation Time at MS (10) in scenario 2.

In figure-6, the example of MS in Scenario-2 shows the received power of each MS from the three BTS. Here in this scenario, number of MS is 50. This figure shows the graph of MS (10) from BTS (0).

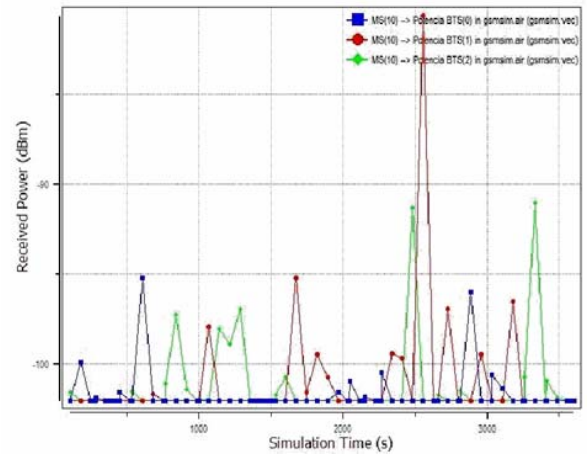


FIGURE-7: Analysis of the results Received Power & Simulation Time at MS (10) in scenario 2.

Here are the examples of MS in Scenario-2 that show the received power of each MS from the three BTS. This figure shows the graph of MS (10) from BTS (0), BTS (1) & BTS (2). Here in this scenario, number of MS is 50, 30 linear & 20 random. Total power is 7 dB. The trajectories of every MS in the area during a busy hour simulation show the BTS coverage. Fig.04 & 05 shows have MS with 5 identifier with a linear trajectory. Here path type is 0. Fig.06 & 07 shows MS with 10 identifier with a random trajectory, here path type is 1.

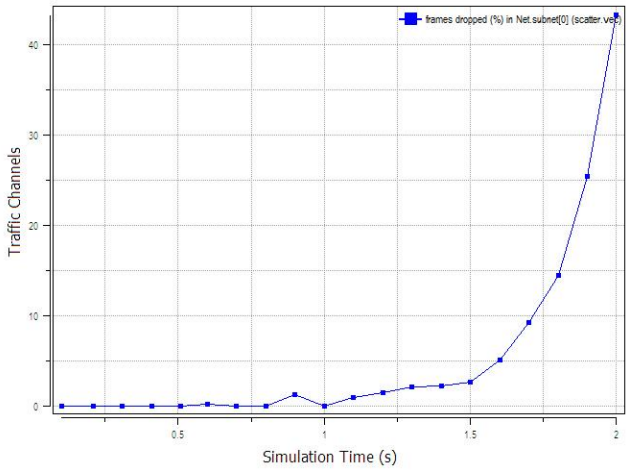


FIGURE-08: Graph of frame dropped or analysis of the result for call drop in scenario 2.

A type of time code designed to match the real time of clocks. Two frames of time code are given. On the other side, Call drop is the common term for a wireless mobile phone call that is terminated unexpectedly as a result of technical reasons, including presence in a dead zone [4].

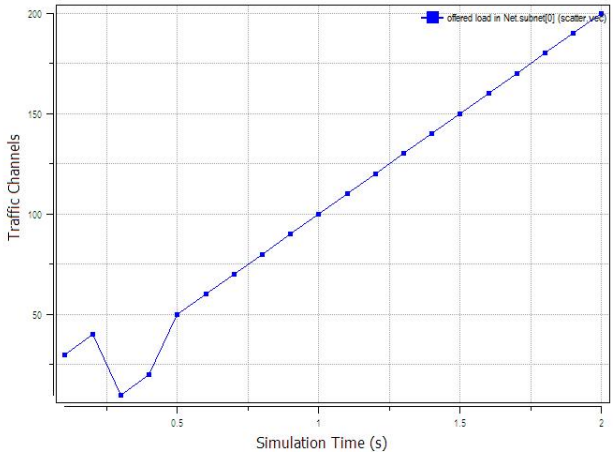


FIGURE-9: Graph of offered load to obtain results for scalar in scenario 2.

Offered Load is the total traffic load, including load that results from retries, submitted to a telecommunications system, group of servers, or the network over a circuit in the sector of telecommunication [5].

In frame relay, the data rate, as measured in bits per second (bps) offers the network for delivery. The aggregate offered load can be less than the access rate supported by the access link and the port speed of the frame relay network device but can never exceed that is less [6].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

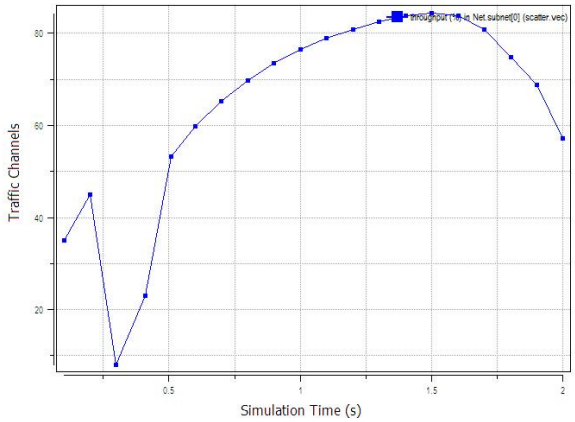


FIGURE-10: Graph of Throughput to obtain results for scalar in scenario 2.

In communication networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network. Throughput is sometimes normalized and measured in percentage, but normalization may cause confusion regarding what the percentage is related to. Channel utilization and packet drop rate in percentage are less ambiguous terms. The channel utilization, also known as bandwidth utilization efficiency, in percentage is the achieved throughput related to the net bit rate in bit/s of a digital communication channel. For example, if the throughput is 70 Mbit/s in a 100 Mbit/s Ethernet connection, the channel utilization is 70%. In a point-to-point or point-to-multipoint communication link, where only one terminal is transmitting, the maximum throughput is often equivalent to or very near to the physical data rate (the channel capacity), since the channel utilization can be almost 100% in such a network, except for a small inter-frame gap [3]. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network.

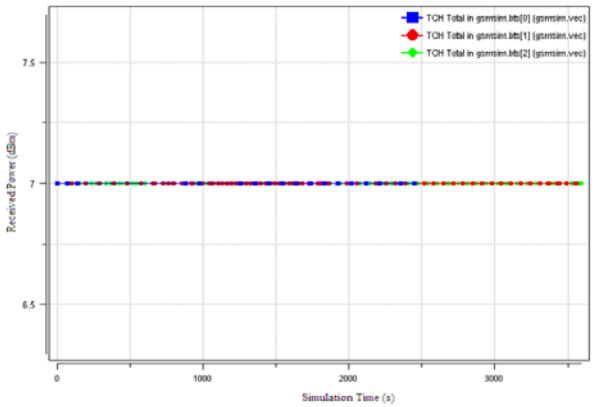


FIGURE-11: Analysis of the total channel of BTSs in scenario 2.

Total Traffic Channel (TCH) is a logical channel that allows the transmission of speech or data. In most second generation systems, the traffic channel can be either full or half rate [7].

C. TABLE 03: General Characteristics of Scenario 3

Properties	**Characteristics Data**
Simulation area:	9 km^2 (3000 m × 3000 m)
Number of MS:	85 mobile stations
	50 MS with linear trajectories
	35 MS with random trajectories: change direction after lifetime (random between 0 to 200 s)
Speed of MS:	(minimal 0.0 m/s) (maximum 7.1 m/s) (average 1.7 m/s)
Power measurements:	one measure per second
MSISDN:	6009000xx, where xx is the MS number (from 0 to 84)
Number of MSC:	1
Number of BTS:	7
Transmission power of BTS:	7 dBm
Position of the BTS:	there is a small area without coverage of the BTSs.
Number of traffic channels of the BTS:	7
Calls processing in MS:	Exponential function with inter-arrival time of 10 min
	Exponential service time distribution (duration of calls) with average service time of 3 min (180 s)
Probability of intra-MSC calls:	5% (probability that a call generated in the current MSC has as destination another MS located in the same MSC)

- Scenario 3:

In this scenario, there are seven BTSs situated at several distances that manage the total area of MSC. The transmitted power attenuation of 7 dB m. in Table-3 summarizes the main characteristics of Scenario-3. Table-3 is an extract of the configuration file 'omnetpp.ini'. As in Scenario 1, it is a busy hour. The area simulation of Scenario 3 is larger than the first and second scenarios. In this scenario we assign 3 kilometers length to both sides of the square area. Some parameters are similar in above scenarios.

This scenario includes 85 MSs moving inside the zone of study, 50 of which have linear trajectories and 35 have random ones. In this case, the simulation is on a network with a single MSC; however, the program can simulate calls between MSs within the simulation and other MSs that depends on a MSC out of the simulation area. Scenario 1 worked only

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

with calls from a MS to a fictitious MS connecting to another MSC, but Scenario 2 considers calls between MSs present in the area, and so is depending of the current MSC. We assign the probability of 5% of intra-MSC calls in this scenario.

In this table we indicate average rates of service time and call generating distributions. The average service time call is also 3 minutes in this scenario and the calls generating process of each MS is an exponential distribution of average rate of 1/600 calls per second, that means call attempts every 10 min. Here we consider seven BTSs in the simulation. We have defined these seven BTSs to be equivalent. The most significant BTS characteristics are 7 traffic channels and a transmission power of 7 dB m. We observe that in this case there are MSs moving in zones without coverage. Any call attempt on those positions will fail. By applying this scenario we simulate the Omnet & get the following Graph.

FIGURES OF SCENARIO 3

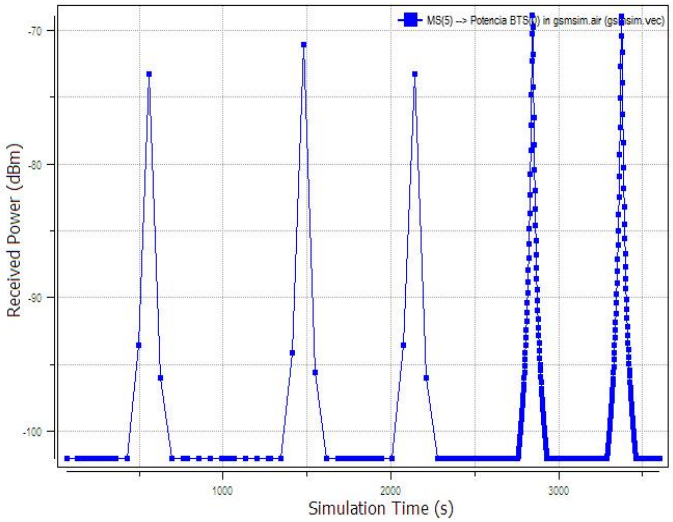


FIGURE-12: Analysis of the results Received Power & Simulation Time at MS (5) in scenario 3.

Here the examples of MS in Scenario-3 that shows the received power of each MS from the seven BTS. Here in this scenario, number of MS is 85. This figure shows the graph of MS (5) from BTS (0).

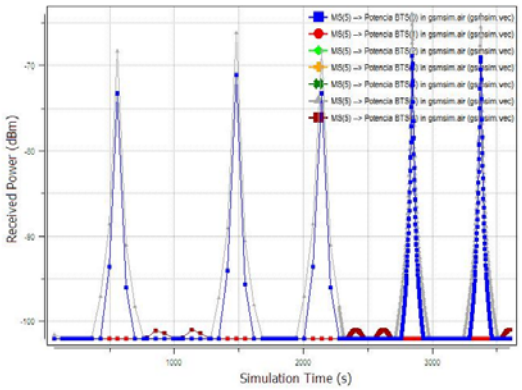


Figure-13: Analysis of the results Received Power & Simulation Time at MS (5) in scenario-3.

In figure-13, the examples of MS in Scenario-3 that show the received power of each MS from the seven BTS. This figure shows the graph of MS (5) from BTS (0) to BTS (6). Here in this scenario, number of MS is 85.

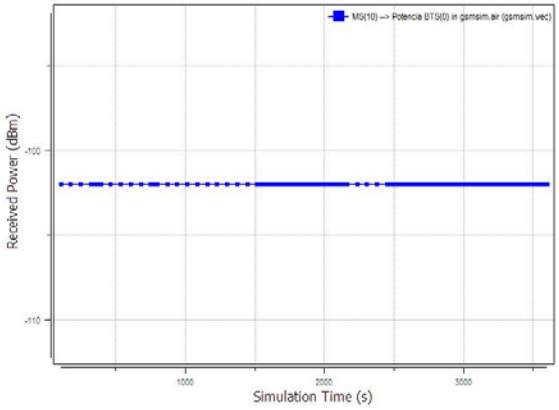


FIGURE-14: Analysis of the results Received Power & Simulation Time at MS (10) in scenario 3.

Here the examples of MS in Scenario-3 that shows the received power of each MS from the seven BTS. In this scenario, number of MS is 85. This figure shows the graph of MS (10) from BTS (0).

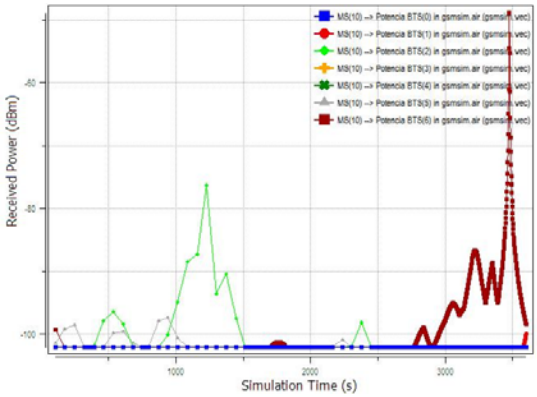


FIGURE-15: Analysis of the results Received Power & Simulation Time at MS (10) in scenario 3.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Here are the examples of MS in Scenario-3 that show the received power of each MS from the seven BTS. This figure shows the graph of MS (10) from BTS (0) to BTS (6). In this scenario, number of MS is 85, 50 linear & 35 random. Total power is 9 dB. The trajectories of every MS in this area during a busy hour simulation show the BTS coverage. Fig.12 & 13 shows MS of 5 identifier with a linear trajectory. Here path type is 0. Fig.14 & 15 shows MS with 10 identifier consisting of a random trajectory, here path type is 1.

D. ***TABLE 04:*** *General characteristics of Scenario 4*

Properties	**Characteristics Data**
Simulation area:	4 km^2 (2000 m × 2000 m)
Number of MS:	100 mobile stations
	60 MS with linear trajectories
	40 MS with random trajectories: change direction after lifetime (random between 0 to 200 s)
Speed of MS:	(minimal 0.0 m/s) (maximum 7.1 m/s) (average 1.7 m/s)
Power measurements:	one measure per second
MSISDN:	6009000xx, where xx is the MS number (from 0 to 99)
Number of MSC:	1
Number of BTS:	20
Transmission power of BTS:	7 dBm
Position of the BTS:	there is a small area without coverage of the BTSs.
Number of traffic channels of the BTS:	7
Calls processing in MS:	Exponential function with inter-arrival time of 10 min
	Exponential service time distribution (duration of calls) with average service time of 3 min (180 s)
Probability of intra-MSC calls:	33% (probability that a call generated in the current MSC has as destination another MS located in the same MSC)

- Scenario 4:

In this scenario there is twenty BTSs situated at several distances, which manages the total area of MSC. The transmitted power attenuation of 7 dB m. in Table 4 summarizes the main characteristics of Scenario-4. Table-3 is an extract of the configuration file 'omnetpp.ini'. As in Scenario-1, it is a busy hour. The area simulation of Scenario-4 is larger than the first scenario and small from second scenario, here we assign 2 kilometers length to both sides of the square area. Some parameters of this scenario are also similar in above scenarios. This scenario includes 100 MSs moving inside the zone of study, 60 of which have linear trajectories and 40 have random ones. In this case, the simulation is on a network with a single MSC; however, the program can simulate calls between MSs within the simulation and other MSs which depends on a MSC out of the simulation area. Scenario 1 worked only with calls from a MS to a fictitious MS connecting to another MSC, but Scenario 4 considers calls between MSs present in the area, and so is depending on the current MSC. Here we assign the probability of 33% of intra-MSC calls. Table 4 indicates average rates of service time and call generating distributions. The average service time call is also 3 minutes and the calls generating process of each MS is an exponential distribution of average rate of 1/600 calls per second that means call attempts every 10 min. Here we consider twenty BTSs in the simulation. We have defined these twenty BTSs to be approximately equal. The most significant BTS characteristics are 7 traffic channels and a transmission power of 7 dB m. We observe that in this case there are MSs moving in zones without coverage. Any call attempt on those positions will fail. By applying this scenario we simulate the Omnet & get the following Graph.

FIGURES OF SCENARIO 4

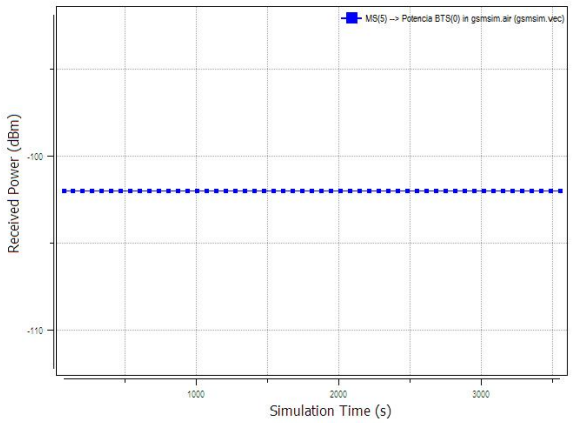


FIGURE-16: Analysis of the results Received Power & Simulation Time at MS (5) in scenario 4.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Here are the examples of MS in Scenario-4 that show the received power of each MS from the twenty BTS. Here, the scenario number of MS is 100. This figure shows the graph of MS (5) from BTS (0).

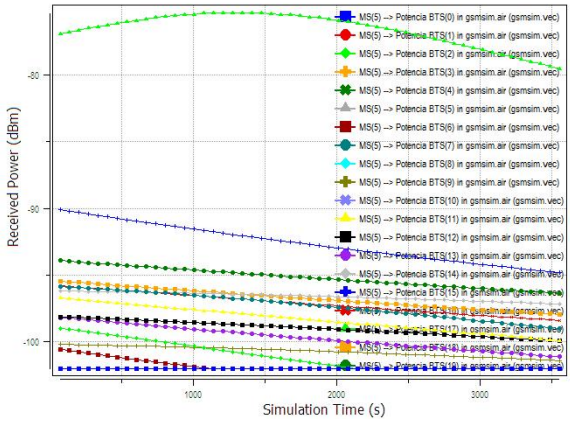


FIGURE-17: Analysis of the results Received Power & Simulation Time at MS (5) in scenario 4.

In figure-38, the examples of MS in Scenario-4 that show the received power of each MS from the twenty BTS. This figure shows the graph of MS (5) from BTS (0) to BTS (19). Here, the scenario number of MS is 100.

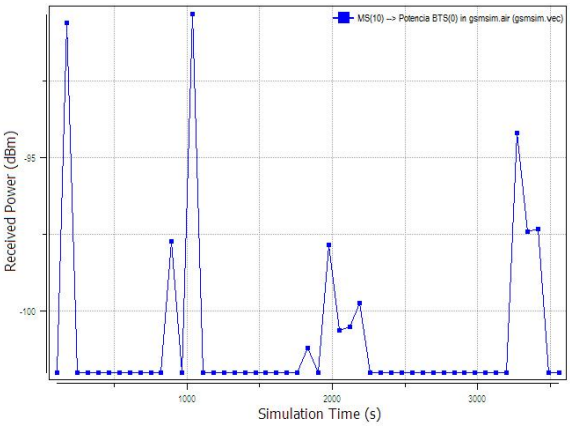


FIGURE-18: Analysis of the results Received Power & Simulation Time at MS (10) in scenario 4.

Here in figure-18, the examples of MS in Scenario-4 that show the received power of each MS from the twenty BTS. Here in this scenario, number of MS is 100. This figure shows the graph of MS (10) from BTS (0).

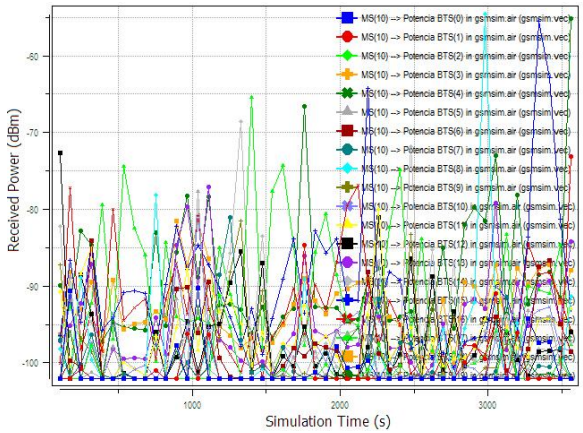


FIGURE-19: Analysis of the results Received Power & Simulation Time at MS (10) in scenario 4.

Here the examples of MS in Scenario-4 that shows the received power of each MS from the twenty BTS. This figure shows the graph of MS (10) from BTS (0) to BTS (19). In this scenario, number of MS is 100, 60 linear & 40 random. Total power is 12 dB. The trajectories of every MS in this area during a busy hour simulation show the BTS coverage. Fig.16 & 17 shows MS with 5 identifier consisting of a linear trajectory, here path type is 0. Fig.18 & 19 shows MS with 10 identifier consisting of a random trajectory, here path type is 1.

IV. Result Analysis of the Graphs

In the above graphs, linear trajectories are characterized by 'path Type = 0'; random paths are categorized by 'path Type = 1'. The program assigns a unique MSISDN to every MS, which follows the format 6009000xx, where xx is the identifier of each MS in the simulation. The configuration files collect information about the initial position and speed of each MS. All MSs have different speed [8]. Here, MSs following linear trajectories generate regular graphics of power attenuation that present symmetries, whereas MSs with random movements have no regular representations of power attenuation. The number of traffic channels is assigned during a busy hour simulation. Due to the BTSs having several traffic channels to serve the communication demand, the number of busy traffic channels is always less than or equal to the number of channels we use here. When the BTS assigned 7 traffic channels, congestion in calls is produced. During congestion, any new call attempts will be rejected. The calls generation process is a Poisson's process with average generating call rate of 6 calls per hour, which is an average inter-arrival time of 10 min or 600 s. At the beginning of a call, the MS assigned a traffic channel in the BTS which reaches the MS with the largest power. After a time, it is possible that another BTS covers the MS with a larger power [9].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The network releases a handover when the difference in power exceeds a given threshold. GSMSIM has configured this threshold to be 9 dB. Another point of these simulations are the zones without coverage. When the received power from a BTS is less or equal than –102 dB m, GSMSIM considers that the MS is out of coverage. In scenario-1, there is no area in out of coverage and the other three scenarios have few areas in out of coverage.

Finally we assume that scenario-4 is more efficient than the other scenarios because in this scenario there is more channels with respect to the MSs comparing the others scenarios. By analyzing the figures we assume that, when BTS & Channel increase with respect to area, the call drop will decrease proportionately. In this case, hand over will increase [10].

By analyzing the graph of scenario-3, we calculate the blocked calls, successful calls, failed handover & successful handover.

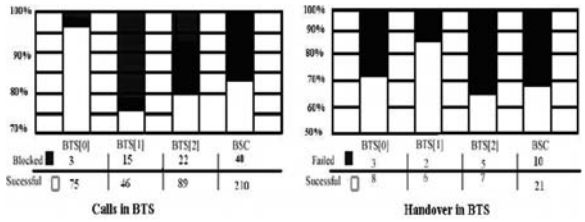


FIGURE-20: Calls in BTS & Handover in BTS by scenario-2 [16].

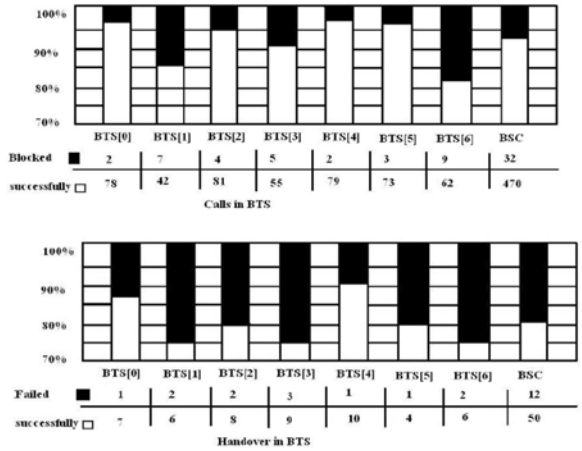


FIGURE-21: Calls in BTS & Handover in BTS by scenario-3[16].

These figures represent the percentage of successful and failed handovers and percentage of successful and blocked calls for each BTS during the simulation.

Considering the BSC of the scenario-2, the blocked calls during the busy hour simulation reaches the 16% (40 blocked calls and 210 successful calls). On the other word, the BSC of the scenario-3, the blocked calls during the busy hour simulation reaches the 6.37% (32 blocked calls and 470 successful calls).

Possible solutions to decrease these high percentages may be:

• Review the conditions for a handover;

• Check the traffic channel assignation algorithm for call attempts. If the BTS with more influence (power transmission) over a MS has any idle traffic channel, then exanimate the second BTS with more influence at scenario-2 [15].

Finally, the right part of the Figure-5(A) shows the number of handovers for every BTS and BSC. The BSC begins 31 handover during the simulation, 10 of which fail. It would be necessary to evaluate reasons for the very high percentage of failed handover operations (32%) [11]. The lower part of Figure-5(B) also shows the number of handovers for each BTS and BSC. The BSC begins 62 handover during the simulation.12 are failed in those handover. It would be necessary to evaluate reasons for the very high percentage of failed handover operations (19%) [11].

V. CONCLUSION

The criteria used in each scenario, are defined to provide a service of highest quality to users. This leads to multiple tests and changes in input parameters of each simulation. These parameters make complex designs because the network must have Multiple factors to provide quality service. The size to optimize coverage, the power to radiate the BTS for greater capacity and to ensure quality throughout the service must be also taken into account [12] [13].

Traffic demand due to the number of users in the cell determines the number of timeslots to be configured to ensure the minimum number of missed calls (missed calls). Throughout, the different simulations showed that the number of calls lost depends on the value of timeslots defined by each TRX at the station base. It is also noted that the power is a factor involving the number of dropped calls, i.e. less power than the number of dropped calls (Broken calls) [14]. Observing the percentage of calls of different scenarios compared to the minimum quality standards that must provide the GSM system, one can conclude that these depend on the network design itself, such as the number of timeslots, the power, the size of the cell, the number of users [15]. The greater the number of network users, the higher the number of timeslots. The greater the number of timeslots, the lower the number of missed calls. The greater their power, greater the coverage and lower the number of dropped calls. After a large number of simulations, one can observe the Cellular operators by the large amount of demand and use limited radio spectrum, opting to provide more coverage than quality [16].

VI. FUTURE SCOPE

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The project can be extended to study the behavior of the Handover and the development of module, the interface that enables communication between the BTS and BSC. This project can be exploring by the great discrete event simulation tool OMNET further for the study and design of different types of networks.

VII. RECOMMENDATIONS

OMNET does not require licensing since it is Open Source. This project can be used as a guide for using the simulation tool OMNET to serve as a resource in the study of different types of networks in the area Telecommunication Systems Engineering.

VIII. REFERENCES

[1] Syed Foysol Islam, Fahmi Ahmed, University of Development Alternative (UODA), Dhaka, Bangladesh. Analysis Of The Methodology Required For The Simulation Of Handover Failure In GSM Network. https://sites.google.com/site/ijcsis/vol-11-no-9-sep-2013, P 81-86 (Cited on September, 2013).

[2] JOACHIM, Tisal. The GSM network. Madrid. Spain Auditorium. 2000. P 184. (Cited on August 22, 2009 19.45 GMT).

[3] ROBERT, E Shannon. Systems Simulation. Trillas Mexico. 1997. P 419. (Cited on August 27, 2009 19.15 GMT).

[4] PLANE, Jesus Cea. GSM. www.munisurquillo.gob.pe/website/books/manuals/Jes% FAs 20Cea%% F3 20Avi n/GSM.doc. (Accessed on September 5, 2009 16.45 GMT).

[5] Cristian Andres Guital, Eduardo Esteban Muñoz Mansilla and Brandau (2006). Applying a Wireless Network model using Smart Antennas. http://cybertesis.uach.cl/tesis/uach/2006/bmfcig968a/doc/bmfcig968a.pdf. (Accessed on September 11, 2009 19.45 GMT).

[6] RICO MARTINEZ, Monica Andrea. Protocol Specification for Quality Management in Networks Telephony in Colombia. Bogotá, 2006. Master Thesis (Telecommunications Engineering). University St. Thomas Aquinas. School of Telecommunications.(Accessed on September 16, 2009 13.20 GMT).

[7] Pilar Gar, Sancho Salcedo-Sanz, Antonio Portilla-Figueras and David Núñez Clemente, GSMSIM: an educational simulation tool for teaching GSM-based mobile communications in laboratory lectures, Department of Signals and Communications Theory, Alcalá University, Madrid, Spain. (Accessed on October 6, 2009 22.45 GMT).

[8] Figure extracted from http://www.cisco.com.(Accessed on October 16, 2009 19.45 GMT).

[9] Avion, Jesus Cea. GSM.www.munisurquillo.gob.pe/website /books /manuals / Jes% FAs 20Avi%% 20Cea F3n/GSM.doc. (Cited on October 30, 2009 19.35 GMT).

[10] Arrieta Pinilla Diana Carolina, (2006). Wireless data transmission via mobile phones. Research project and design of a remote inspection Automatic(UAV).http://eav.upb.edu.co/banco/files/Tesistransmisioninalambricadatos.pdf. (Accessed on October 26, 2009 17.35 GMT).

[11] Svein Yngvar Willassen, M.Sc, Senior Investigator, Computer Forensics, Ibas AS, Forensics and the GSM mobile telephone system. (Accessed on October 29, 2009 13.45 GMT).

[12] Drozdy.G.Niemelä, J.Välimäki, etc. (1992) "Study of GSM System Performance by GSM Network Computer Simulator", IEEE vol 2. (Cited on November 8, 2009 15.15 GMT).

[13] Hoeger, Herbert. University of the Andes op.cit. (Accessed on December 3, 2009 18.45 GMT).

[14] Herrera, Jose Miguel. Technical University Federico Santa María (Valparaíso - Chile). NS2 -Network Simulator. (Cited April 28., 2007). www.inf.utfsm.cl/ jherrera / docs / mine / ns.pdf. (Accessed on December 14, 2009 15.40 GMT).

[15] Turegano, Javier Molina (mushrooms). NS-2 Simulator. linuxalbacete.org/web/content/view/149/31/. (Accessed on January 14, 2010 20.15 GMT).

[16] OMNeT++ OP.CIT. http://www.omnetpp.org. (Accessed on April 12, 2010 22.15 GMT).

AUTHORS PROFILE

Syed Foysol Islam
MSc Engg in Electrical Engineering (BTH, Sweden)
BSc, MSc in Computer Science (Rajshahi University, Bangladesh)
Assistant Professor, Department of CSE and ETE
University of Development Alternative (UODA)

Fahmi Ahmed
MEngg in Telecommunication (AIUB, Bangladesh)
BSc in Electronic and Telecommunication Engg (UODA, Bangladesh)
Senior Lecturer, Department of CSE and ETE
University of Development Alternative (UODA)

Route optimization and roaming capability based MIPv6 protocol in internet network

Marzieh Izanlou
Dept. of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University
Tehran, Iran

Mohamadali Pourmina
Faculty of Electrical and Computer Engineering, Islamic Azad University
Tehran, Iran

Afrouz Haghbin
Faculty of Electrical and Computer Engineering, Islamic Azad University
Tehran, Iran

Abstract— **MIPv6 is a proper replacement for MIPv4 protocol which recommended by IETF. IPv6 lieu IPv4 has been chosen as convergence layer for next heterogeneous access networks. MIPv4 has limiting in protocol, but MIPv6 is created fundamental changes such as security enhancements, elimination of the Foreign Agent (FA) and route optimization.**
The MIPv6 characteristics defined by the IETF provides perspicuous host mobility within IPv6 networks. In MIPv6 MN is move between IP subnets without change in its original IPv6 address configuration. This means that MN ever is addressable in the internet via its Home Address (HoA). HoA is IPv6 address that is allocated to the MN in its home network. When away from the home network, MN can still detect by its HOA in the internet, Because packets routed to its HoA. Also In this way, mobility transparency of higher layer protocols like Transport layer or higher is achieved.

Keywords- MIPv6; routing; roaming capability

I. INTRODUCTION

Mobile IPv6 (MIPv6) is a commonly accepted standard to address global mobility of Mobile Nodes (MNs) [1]. This is one of the main protocols to manage mobile node (MN) movements; refer to IETF documentation. This allows the MN to acquire and register a new IPv6 address in each visited network. Terminology used in Mobile IPv6 as follows [2]:

A node that can change its situation from one network to another, while still being reachable pre its home address, this called Mobile Node (MN). Corresponding Node (CN) is a mobile node or a fixed node that communicates or corresponds with the MN by exchanging packets with MN. The individual network that manages the MN is Home Network (HN). Foreign Network (FN) is other network that the MN is attached lieu of its HN. Home address (HOA) is an irreversible IP address assigned to MN within its home network. Home Agent (HA) is a router on a MN's home network with which the MN has registered its current CoA [3], [4]. While the MN is away from home, the HA arrests packets on the home network destine to the MN's address, encapsulates them, and tunnels them to the MN's registers CoA. Access Router gives connectivity to the mobile node at its other point of attachment to the Internet. Binding is the association of the home address of a Mobile Node (MN) with a care-of-address for that MN, along with the remaining lifetime of that association. Binding Update which including the Home Address (HOA) and the CoA [5], [6]. Care-of-Address (CoA) is An IP address associated with a MN while visiting a foreign network; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple care-of-addresses that a MN may have at a time, the one registered with the MN's Home Agent is called its primary CoA.

The paper is organized as follows: Section 2 and 3 describe the scenario 1 and scenario 2 of the proposed scheme, respectively. And, both of sections discuss simulation results. Finally, Section 4 concludes this paper.

II. SCENARIO1
(EFFECTS MIPV6-ROUTE-OPTIMIZATION-ENABLED)

The objective is to demonstrate the effects of Mobile IPv6 (MIPv6) mechanisms while two mobile nodes communicate with each other. Cases for route optimization enable and disable are evaluated.

The IPv6 network is composed by four WLAN access points connected through an IP cloud. The core of the network, represented by the IP cloud, has a constant latency of 0.1 seconds. This makes easier to note the effects of the different MIPv6 mechanisms over the application delay.

Table I and II summarize the simulation parameters and the network parameters, respectively.

A. Simulation scenario1

MN_A and MN_B communicate to each other by running a very light video application as a source of constant UDP traffic. Initially the mobiles are placed at their corresponding home networks. Then MN_A is served by home agent HA_A and MN_B is served by home agent HA_B. Both mobiles use MIPv6 to roam among the various access points in the network. The movement performed by the nodes can be described as follows:

- MN_A: (1A)- MN_A moves in a counterclockwise trajectory roaming through all four access points in the network.
- MN_B: (1B)- MN_B moves, first in a clockwise trajectory roaming through all four access points in

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

the network. (2B)- Then it moves counterclockwise re-visiting all access points again.

Fig. 1 shows the Scenario1.

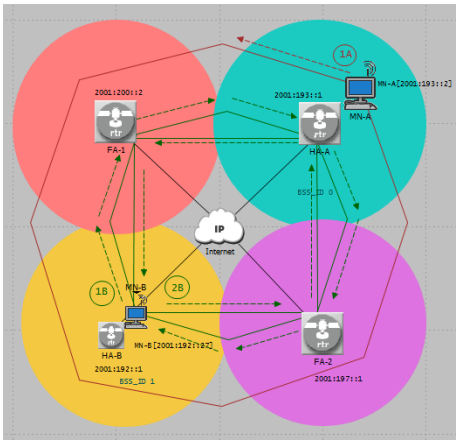


Figure 1. Simulated scenario 1

TABLE I. SIMULATION PARAMETER

Parameters	Values
Network type	Campus
Network Dimension	10 km*10 km
Technologies	Wirelesslan , Ethernet , MIPv6
Domain Quantity	4
Module Radius	1 km
Simulation time	17minute and 47 second

TABLE II. NETWORK PARAMETER

Parameters	Values
Routers Quantity	4
Routers technology	SLIP , Ethernet , Wirelesslan
Routers data rate	1 Mbps
IP clude Memory	16 MB
Paket loss of IP clude	0.1 second
Workstation Quantity	2
Workstation Rate	1 Mbps
Workstation Memory	16 MB

B. *Simulation Result For Scenario 1*

The statistics show three main aspects of the dynamics for the communication between the two mobiles.

1) *Application traffic*

Videoconferencing traffic received show the some gaps in the communication. Each gap is produced every time a mobile changes its current access point triggering MIPv6 binding procedures to inform its home agent about its new Care-of Address (CoA). When route optimization is used the mobile will also inform to all its correspondent nodes about its new CoA. While the binding procedure updates home agent and correspondent nodes all traffic directed to the mobile will be lost.

The application response time will be directly affected by the MIPv6 mechanism used by the mobile in order to communicate with correspondent nodes. There are two possible mechanisms used by MIPv6: Route optimization and Tunnel/reverse tunnel (route optimization disabled).

Notice that when route optimization is enabled the application delay is reduced compared to the case when route optimization is disabled. Below you will find a more detailed explanation for this effect.

Fig. 2 represents video conferencing traffic and video conferencing packet delay, respectively.

2) *Mobile IPv6 measurements*

Two mobiles communicating with each other. This means that at some point in the simulation the mobile nodes will be acting as both a mobile node and/or a correspondent node. This cause interesting MIPv6 effects that can be observed at the "Mobile IPv6 Traffic" statistic panel:

- When both mobiles are away from their corresponding home networks a double MIPv6 overhead will occur, either:

Two MIPv6 tunnels will be needed for the mobiles to communicate (mipv6_route_optimization_enabled). In this case the application response time delay will be mainly produced by the three times the data packet must pass through the IP cloud (Internet). Given the latency configured for the IP cloud (0.1 sec), the total application delay will be approximately 0.3 seconds.

Two IPv6 extension headers (routing extension header and destination extension header) will be used (at the same time) to transport the data traffic when using route optimization mechanism (mipv6_route_optimization_disabled). In this case the application response time will be mainly produced by only one time the data packet must pass through the IP cloud (approximately 0.1 sec). This is when both mobiles are away from home but located in different networks. Now, when both mobiles are located at the same access point, the data packets will just go through the access point, reducing the application response time even more.

- When only one mobile is away from its home network, it will act as a mobile while the other one will perform correspondent node operations. In this case:

One MIPv6 tunnel will be needed to communicate (mipv6_route_optimization_enabled).

Just one MIPv6 extension header (at a given time) will be used to transport the data traffic when using route optimization mechanism (mipv6_route_optimization_disabled).

Fig. 3 represents the result of MIPv6 traffic.

Fig. 4 shows the packet delay variation in cases enable and disable routing optimized. Variance among end to end delays for video packets received by this node. End to end delay for a video packet is measured from the time it is created to the time it is received. The packet delay variation is 2.5 in optimized enable routing that is less than optimized disable routing.

3) *Visited access points*

Under this statistic panel it is possible to observe all access points that were visited by both mobiles. Each bar in the graph represents an access point visited by the mobiles, and the bar width represents the time the mobile used the access point

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

until it move to a different one. The colors of the bars have been set so each one identifies one of the four access points according to the color of the annotation circle placed at the access point's position. Fig. 5 shows the visited access points.

III. SCENARIO 2 (ROAMING CAPABILITY IN MIPV6)

This scenario utilizes 802.11b WLAN interface with roaming capability to simulate hand-offs between mobile IP agents who are also WLAN access points. Here are some configuration specifics you have to follow to use WLAN roaming capability.

- Wireless Lan Parameters. BSS Identifier should be explicitly set on all the WLAN nodes in the network.
- There should be only one access point for a BSS network (Wireless LAN Parameters. Access Point Functionality)
- 802.11b uses the following physical attribute values: Wireless Lan Parameters. Data Rate (bps) -- 11Mbps Wireless Lan Parameters. Physical Characteristics -- Direct Sequence
- IP auto addressing scheme will assign IP addresses based on the BSS ID, i.e. all the WLAN nodes sharing the same BSS ID will be assigned an IP addresses from the same IP network.

The Mobile IP NET is a mobile subnet containing a mobile router and a client node. The mobile router node uses the mobile IP home agent service from the HA WLAN router. The MR in mobile subnet is manually configured with common BSS ID and IP network address as that of the HA WLAN router. All the foreign agents are also WLAN routers with different BSS Identifiers.

Table III and IV summarize the simulation parameters and the network parameters, respectively.

TABLE III. SIMULATION PARAMETER

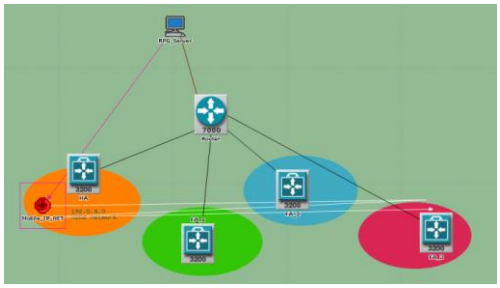
Parameters	Values
Network type	Campus
Network Dimension	55 km*55 km
Technologies	RPG, Wirelesslan , Ethernet , MIPv6
Domain Quantity	4
Module Radius	1 km
Simulation time	14minute and 59 second

TABLE IV. NETWORK PARAMETER

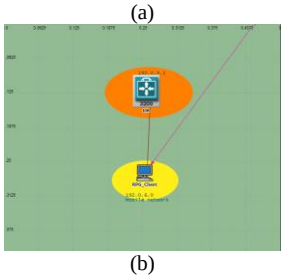
Parameters	Values
Routers Quantity	5
Routers technology	SLIP , Ethernet .Wirelesslan
Routers data rate	11 Mbps
RPG Traffic rate	1 pkt/sec
100BaseT data rate	100 Mbps
Service	Best Effort
Workstation Quantity	2
Workstation packet size	512 b
Workstation Memory	16 MB
Flow type of ip-traffic-flow	Aggregate

A. Simulation Scenario 2

The Mipv6 network, which simulated in this scenario, inclusive a mobile subnet that has a mobile router and client node. This scenario represented in fig. 6. In figure 6 the mobile subnet first stands in home domain. When simulation starts the packet which exchanges between RPG-Server and RPG-Client is serving via HA. The mobile subnet gently moves, when approaching the first neighbor domain, MR sends BU massage to HA and HA responses with BA massage. If update is allow, starts transmittal with new domain. Hereinafter the packet transmitted by server outset goes to HA and then transmission to FA and achieve to client in mobile subnet.



(a)



(b)

Figure 6. Simulated scenario 2: (a): Network, (b): Subnet

B. Simulation Result For Scenario 2

The RPG-Server node sends traffic to the RPG-Client. As the mobile subnet moves along the trajectory, it changes the access point and changes the mobile agent as well. The packets will be tunneled to different foreign agents as the mobile node changes its access points. Fig. 7 shows the tunneled traffic sent for HA and the tunneled traffic received for FAs.

As mobile subnet is move at trajectory RPG-Server send traffic to RPG-Client. Traffic sent is Total number of all RPG packet bits sent per second by this node to other RPG nodes in the network and traffic received is Total number of RPG packet bits received per second by this node from all other RPG packet sources in the network. Fig. 8 shows the Traffic sent by RPG-Server and traffic received by RPG-Client.

Fig. 9 shows throughput at various domains, which is namely total data traffic in bits/sec successfully received and forwarded to the higher layer by the WLAN MAC. This statistic does not include the data frames that are 1) unicast frames addressed to another MAC, 2) duplicates of previously received frames, and 3) incomplete, meaning that not all the fragments of the frame were received within a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

certain time, so that the received fragments had to be discarded without fully reassembling the higher layer packet.

Fig. 10 represents the media access delay that is namely the total of queuing and contention delays of the data, management, delayed Block-ACK and Block-ACK Request frames transmitted by the WLAN MAC. For each frame, this delay is calculated as the duration from the time when it is inserted into the transmission queue, which is arrival time for higher layer data packets and creation time for all other frames types, until the time when the frame is sent to the physical layer for the first time. Hence, it also includes the period for the successful RTS/CTS exchange, if this exchange is used prior to the transmission of that frame. Similarly, it may also include multiple number of back off periods, if the MAC is 802.11e-capable and the initial transmission of the frame is delayed due to one or more internal collisions.

IV. CONCLUSION

In scenario 1 has been perusing the effect of mipv6 route optimization on delay, sent and received traffic, tunneled traffic in MIPv6, delay and traffic for video conferencing. We perceive that with proper routing, situation of all of the traffics improve to a considerable extent. Even in optimal routing the incision in communication, was much less. In the other hand, delay and Video packet delay dispersion slake to a considerable extent.

The problem considered in Scenario 2, is the mobile roaming in the MIPv6 network. It was observed that, whenever the mobile enters to a new AP, traffic just has been tunneling for that AP. E.g. sending traffic of HA is totally of receiving traffic by FAs. Also media access delay in HA is more than FAs.

References

[1] David Cypher, Nada Golmie, Mun-Suk Kim, and SuKyoung Lee, "Fast Handover Latency Analysis in Proxy Mobile IPv6 ," , 2010, pp. 89-95.

[2] Wankawee Puangkor and Panita Pongpaibool, "A Survey of Techniques for Reducing Handover Latency and Packet Loss in Mobile IPv6,"2006,pp 3-4.

[3] H. Soliman, C. Castelluccia, " Hierarchical Mobile IPv6 management," IETF draft, draft-ietfmobileip-hmipv6-o7.

[4] T.Kato, R.Takechi, H.Ono, " A study on Mobile IPv6 Based Mobility Management Architecture," June 2001.

[5] D. B. Johnson, C.Perkins, and Jari Arkko, " Mobility Support in IPv6," Internet Draft, working progress, January 2003.

[6] F. Andre, J-M Bonnin, B. Deniaud, K. Guillouard, N. Montavont, " Optimized Support of Multiple Wireless Interfaces within an IPv6 End-Terminal,"2008.

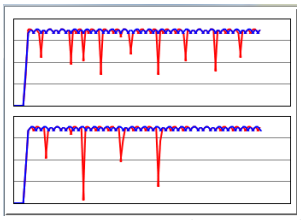


Figure 2. (a) Video conferencing traffic

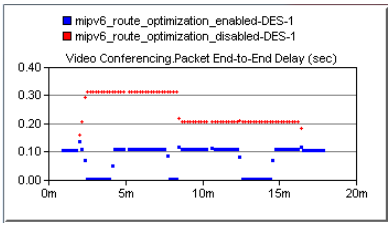


Figure2. (b) Video conferencing packet delay

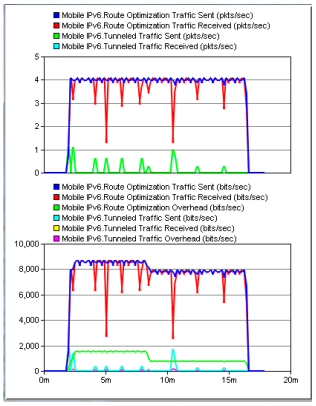


Figure 3. The result of MIPv6 traffic

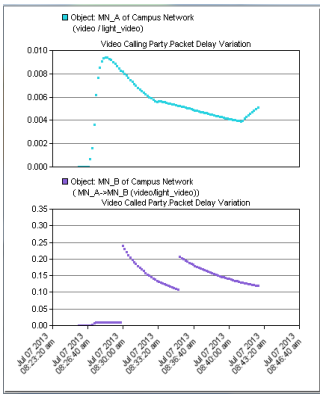


Figure 4. (a) Enable routing optimized

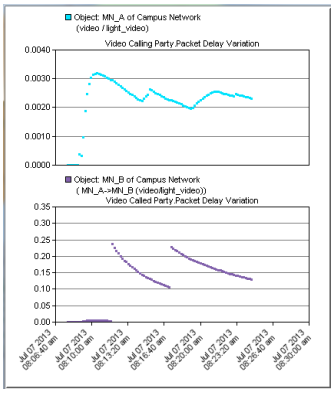


Figure 4. (b) Disable routing optimized

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

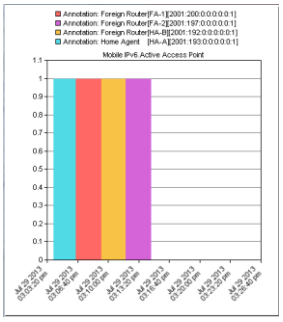


Figure 5. (a) Active access point for MN-A

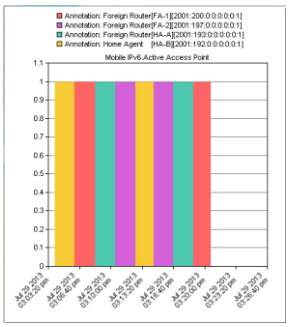


Figure 5. (b) Active access point for MN-B

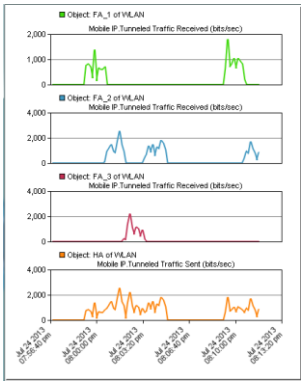


Figure 7. (a): stacked, The tunneled traffic sent for HA and the tunneled traffic received for FAs

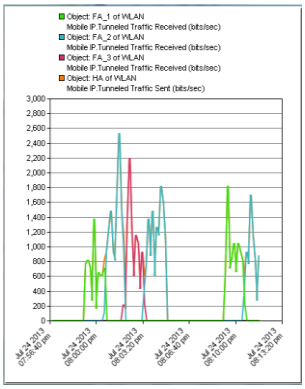


Figure 7. (b): overlaid, The tunneled traffic sent for HA and the tunneled traffic received for FAs

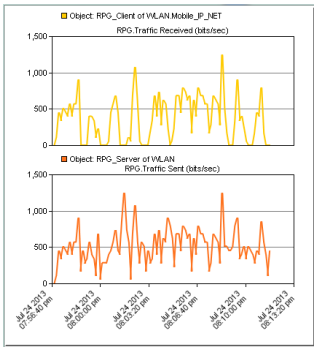


Figure 8. (a): stacked,
Traffic sent by RPG-Server and traffic received by RPG-Client

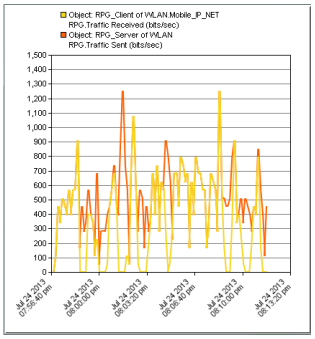


Figure 8. (b): overlaid,
Traffic sent by RPG-Server and traffic received by RPG-Client

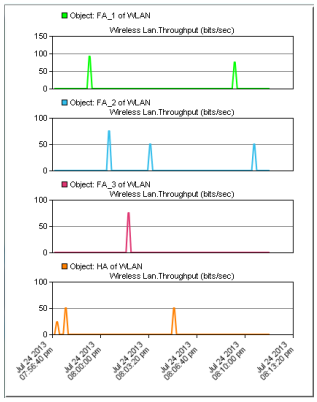


Figure 9. (a): stacked, WLAN throughput at various domain

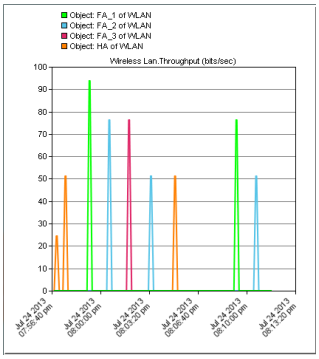


Figure 9. (b): overlaid, WLAN throughput at various domain

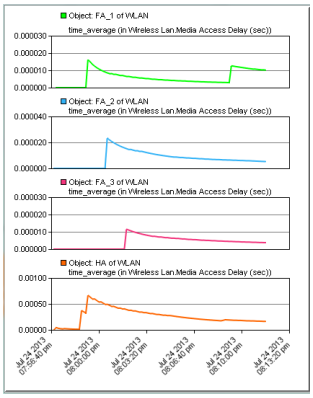


Figure 10. (a): stacked, The media access delay

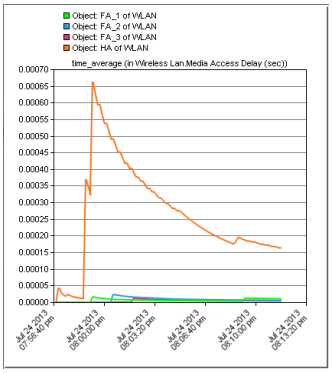


Figure 10. (b): overlaid, The media access delay

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Utilization DCTC and Vonoroi of Tracking in Wireless Sensor Networks

Maan younus abdullah
University of mosul
Education College /computer science department
mosul, Iraq

***Abstract*-Wireless sensor networks (WSN) may consist of several to thousands of sensors that share the need to organize for network data collection sink routing. This paper addressed the problems of tracking moving of wireless sensor network objects. The traditional tracking method, called Dynamic Convoy Tree-Based Collaboration (DCTC) presented. In additional describe a method, called Distributed computation of Voronoi cells in sensor networks. Proposed solutions of WSNs challenges using converge cast traffic, covering networks configuration and efficient routing routines. We also present the intermediate routing sensor nodes expend an excessive amount of their energy resources. thus can achieve superior tracking accuracy with faster tracking convergence speed and reducing the network lifetime.**

Index Terms - DCTC， Voronoi , Tracking

I. INTRODUCTION

Wireless sensor networks in any applications are used to gather intelligence about field conditions. Monitoring the activity or assess conditions and influences. A major requirement for any applications sensor networks is to reliably aggregate and disseminate information within a time frame that allows the command control to take necessary tactical decisions. This calls for communication systems that can provide high data rates with high reliability while using minimum bandwidth and power. In other words, the underlying communication network must be robust, reliable, and scalable. The choice of network architecture (topology) has strong influence on the effectiveness of the tactical applications in wireless any application sensor networks. Network architecture affects network characteristics such as latency, robustness, and capacity [1,2,3].

Almost all of the common applications require knowledge of the position of the car to work properly. Even when no applications directly take benefit of the car park, can the underlying data dissemination protocols take Feature a lot of this information [4]. To example, geocasting and guidance geographical dependence on the car and are desirable for many of the scenarios and be more suitable for applications Voronoi region is less than 6 proof. By the Euler formula [5,6]

The complexity of data routing and processing (data fusion) also depends on the topology. In this paper will be fined how to route packets efficiently in networks is an interesting and challenging research topic.

The rest of the paper is organized as follows. In the next section, we briefly outline the princebles of voronoi methods. In Section III, we describe the proposed algorithm. Simulation results are presented and discussed in Section IV. Finally, we conclude in Section V.

II. Principels of VORONOI Methods

Static point Voronoi tessellations are well known in the literature, and algorithms have been used for many years (see [7] for a summary). Less well known are dynamic algorithms, that allow point creation, deletion and movement, and also Voronoi tessellations of more complex objects - typically line segments as well as points. Algorithms for generating the simple point Voronoi tessellation have improved significantly in theoretical efficiency in recent years. Where the whole structure may be constructed at once, randomized incremental algorithms such as [8,9] can create these diagrams in expected time O(n log n), which is optimal. However, as a major motivation for this work concerned the maintaining of a map when one or more objects are moving, an alternative technique was developed that maintained the Voronoi spatial relationships while map objects were being inserted, deleted, or displaced. This is achieved by determining when the Voronoi cell of a moving point gains or loses a neighbouring cell, moving the point to that location, and locally updating the topological structure accordingly. For the case of all points moving simultaneously, [10] give a rather complex theoretical efficiency based on Davenport-Schinzel sequences, but in the case of one point being inserted at a time by splitting it from the nearest pre-existing point and then moving it to its destination (see below) the expected time efficiency should again approximate O(n log n)The WSN of active sensors suffers from serious inter-sensor in- terference and imposes new design and implementation challenges. Show that the adaptive sensor scheduling scheme can achieve superior tracking accuracy with faster tracking convergence speed.

The concept of the Voronoi diagram [7], a well-known construct from computational geometry, is used to find a maximal breach path in a sensing field. In two dimensions, the Voronoi diagram of a set of discrete points (also called sites) divides the plane into a set of convex polygons, such that all points inside a polygon are closest to

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

only one point. In Figure 1a, 10 randomly placed nodes divide the bounded rectangular region into 10 convex polygons, referred to as Voronoi polygons. Any two nodes si and sj are called Voronoi neighbors of each other if their polygons share a common edge. The edges of a Voronoi polygon for node si are the perpendicular bisectors of the lines connecting si and its Voronoi neighbors. Since by construction, the line segments in a Voronoi diagram maximize the distance from the closest sites, the maximal breach path must lie along the Voronoi edges. If it does not, then any other path that deviates from the Voronoi edges would

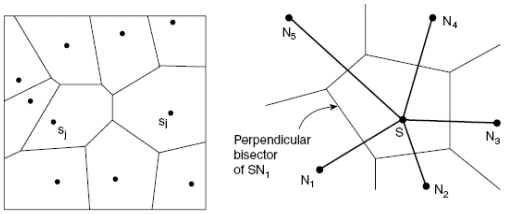


Figure 1. (a) Voronoi diagram of 10 randomly are deployed nodes; (b) Voronoi polygon for node S, constructed by drawing perpendicular bisectors of the lines connecting S and its neighbors.

Issues in wireless sensing networks are network architecture design and data routing. Hence, several researchers have addressed the issue of communication jamming in a wireless sensor network and its effect on the performance of the network. Xu et al. [11,12] discuss radio interference attacks on wireless sensor networks. They study the feasibility and effectiveness of jamming attacks on wireless networks and examine the critical issue of detecting the presence of jamming attacks. They also propose four different jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets.

III. Target Tracking Using Sensor Networks

Target tracking has been a classical problem since the early years of electrical systems. Sittler, in 1964, gave a formal description of the multiple-target tracking (MTT) problem [11]. The goal of the MTT problem is to find the moving path for each target in the field. Target tracking using a sensor network was initially investigated 2004 [13]. With the advances in the fabrication technologies that integrate the sensing and the wireless communication technologies, tiny sensor motes can be densely deployed in the desired field to form a large-scale wireless sensor network. Challenges and difficulties, however, also exist in a target tracking sensor network:

1) Tracking needs collaborative communication and computation among multiple sensors.
2) Each sensor node has very limited processing power.
3) Each node also has tight budget on energy source. Thus, for data processing and tracking should consider the impact of power saving mode in each node.

A) Different Approaches of Target Tracking

The method will need to handle a large number of moving objects at once. While our method uses a hierarchy to connect the sensors:

1) The leaves are sensors
2) the querying point as the root
3) the other nodes are communication nodes

The main idea of STUN is showed in the example figure 2 showed that the message-pruning hierarchy .Considerthe those detection messages from sensors that detected the arrival of the car. Sensors A's message will update the detected sets of all its ancestors.The message from sensors B and D do no update the detected sets of their parents and thus will be pruned at X. The main advantage of STUN Message pruning and routing routing while the disadvantage Building the tree (the structures of the tree).

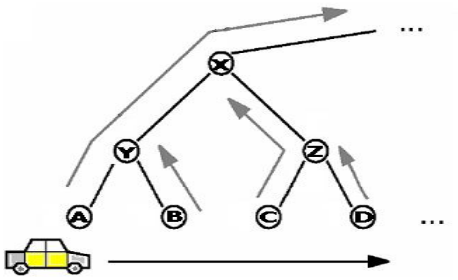


figure 2 is a message-pruning hierarchy

B) Tracking Tree Management Dynamic Convoy Tree-Based Collaboration (DCTC)

A dynamic convoy tree-based collaboration (DCTC) framework for tracking a mobile target is proposed in [14]. Heuristics are used to predict the object's moving direction. A dynamic tree is then created by adding or pruning the sensors near the moving target. The root of the tree can dynamically refine the readings gathered from various tree nodes.

Since the coverage area of individual sensor nodes usually overlaps, the work in [15] attempts to periodically search the smallest subset of nodes that covers the monitoring area. This group of nodes is referred to as the area-dominating set. A distributed spanning tree, induced by the initial interest flood over the area-dominating set, is used to aggregate the reply messages from various event sources. DCTC relies on a tree structure called"convoy tree". The tree is dynamically configured to add some nodes and prune some nodes as the target moves that DCTC–main idea. This paper studies the Efficient of detecting and tracking a mobile target, and monitoring a particular region surrounding the target in sensor networks. Figure 3 showed that the sensor nodes surrounding an adversary tank detect and track the tank and its surrounding area which may include enemy surrounding area. DCTC relies on a tree structure called convoy tree1, which includes sensor nodes around the moving target, and the tree

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

is dynamically configured to add some nodes and prune some nodes as the target moves. Figure 1 illustrates how to use the convoy tree to track a mobile target. As the target first enters the detection region, sensor nodes that can detect the target collaborate with each other to select a root and construct an initial convoy tree. Relying on the convoy tree, the roots collect information from the sensor nodes and refine this information to obtain more complete and accurate information about the target using some classification algorithms [16, 17].

The region around it in an energy efficient way, and the network should forward this information to the sinks in a fast and energy efficient way. The data report can be saved locally waiting for other node's query, or can be forwarded to single or multiple data centers (the sinks), which can be a static command center or moving soldiers. As the sensor nodes surrounding the moving target should promptly provide robust and reliable status information about the mobile target and design goals. Such as is tracking an important target (e.g., an important person) in a parade. As design goals, moving target should promptly provide robust. The data report can be saved locally waiting for other node's query, or can be forwarded to single or multiple data centers (the sinks), which can be efficient way, and the network should forward well as its surrounding area, and one of them (i.e., the root) generates a data report.

This is information to the sinks in a fast and energy efficient way. DCTC is a framework to detect and track the mobile target and monitor its soldiers. These nodes collaborate among themselves to aggregate data about the tank.

IV. Simulation and Results Disscution

Scenario: 200 → 1000 sensor nodes are thrown randomly in area of 640m x 540m. Each node has 2J (2*10^6 µJ) of energy with sensing radius = 30m and communication radius = 60m. Intruder objects are supposed moving specific paths. No data aggregation is allowed. The Utilized tools and module descriptions as a tools of OMNET++, C#, and Matlab The module description under OMNET++: Layer 0 module: Represented for physical layer. It consists of gates (in/out) and be responsible for making connection between the node and its neighbors. Its behaviors include forward messages from higher layer to its neighbors and vice versa .MAC module: Represented for pre-processing packet layers. It consists of gates (in/out) and queues (incoming queue and outgoing queue). When the queue is full, it deletes some latest messages to make sure that there is enough room in the queue for new messages. It helps to evaluate performance of the node. (Note: In current simulation, this module is temporary eliminated to speech up the performance) Application module: Represented for application layer consisting of gates (in/out). Note that, at anytime, after sending a message, the module automatically sends a decrease_energy message to energy module (through the coordinator) to let the module decrease the energy by one unit. Coordinator module: an interface to connect all modules together. It categories incoming messages to delivery them to the right module. For example, when receiving a decrease_energy message, it will forward the message to energy module.sensor module: represented for sensor board in a sensor node. if sensor_switch parameter is "on" (set to 1), the module consumes energy, so, after an interval (timer), the module send decrease_energy message to the energy module (through the coordinator). When the timer ticks, the waiting timer decreases. The waiting timer is set by sensor_refresh messages from application module. if the waiting timer is zero, the module will turn "off" (sensor_switch parameter is set to 0). Radio module: represented for the radio board in a sensor node. if radio_switch parameter is "on" (set to 1), the module consumes energy, so, after an interval (timer), the module send decrease_energy message to the energy module (through the coordinator). Energy module: represented for battery in a sensor node. at the beginning, each sensor node is set to a specific energy level (energy parameter). if the module receives a decrease_energy message, it decreases the energy level by one.

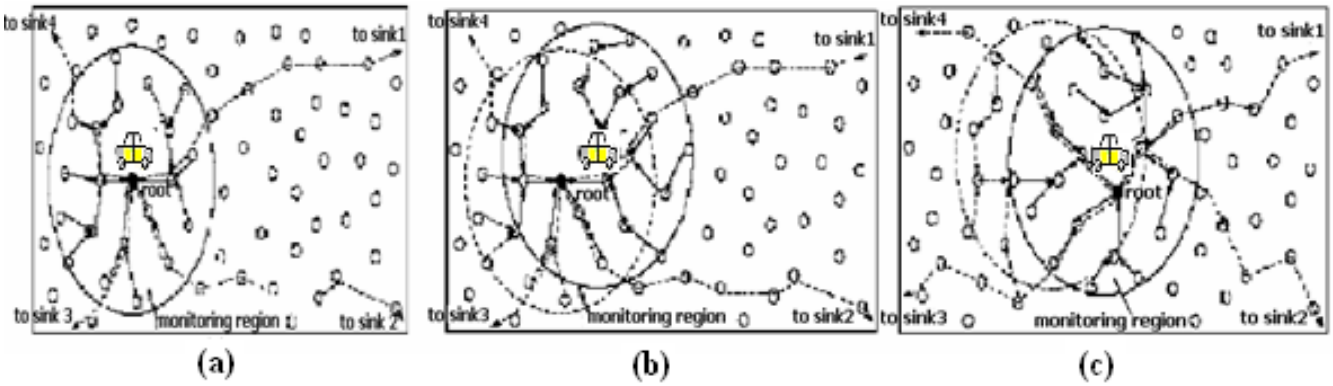


Figure 3: Adding and pruning nodes for the convoy tree in the DCTC scheme:
(a) Convoy tree at current time; (b) and (c) convoy tree at next time.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

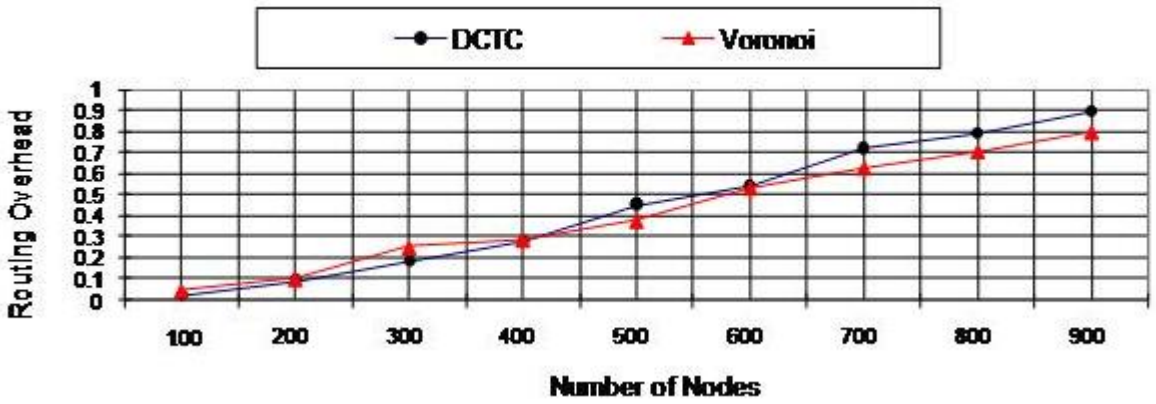


Figure 4: DCTC and Voronoi Routing

We found that the DCTC had a very small increase in routing overhead than using voronoi as shown in Figure1, because of delayed receipt of route reply by the source nodes.

I. Conclusions

However, each sensor mote has limited capabilities in terms of power, sensing, and processing abilities. Therefore, comprehensive and accurate data can be obtained only through the collaboration of sensor nodes in the network as a single node does not have the capability to provide this information. We have discussed the importance of coverage and connectivity, Which are two fundamental factors for ensuring efficient resource management in wireless sensor networks, and surveyed various methods and protocols, which are optimally cover a sensing field while maintaining global network connectivity at the same time.

REFERENCES

[1] Sugano, M.; Kawazoe, T., Ohta, Y. & Murata, M. (2006) An indoor localization system using RSSI measurement of a wireless sensor network based on the ZigBee standard" , Proceedings of the sixth IASTED International Multi-onference on Wireless and Optical Communication，pp.503-508, Banff, Canada, July 2006

[2] Tadokoro, S; Matsuno, F., Onosato, M. & Asama, H. (2003) Japan National Special Project for Earthquake Disaster Mitigation in Urban Areas, First International Workshop on Synthetic Simulation and Robotics to Mitigate Earthquake Disaster , pp.1-5, Padova, Italy , July 2003

[3] S. Yousefi, M. Mousavi, and M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives," 2006 6th Int'l. Conf. ITS Telecommun., IEEE, June 2006,ISBN 0-7803-9586-7, pages 761–66

[4] Heitor S. Ramos, Azzedine Boukerche, Richard Pazzi et al. (2012) Cooperative target tracking in vehicular sensor networks, 66-73. In IEEE Wireless Communications 19 (5). http://ieeexplore.ieee.org/lpdocs/epi...

[5] Devillers, O.: The Delaunay Hierarchy. International Journal of Foundations of Computer Science 13, 163 {180 ,2002

[6] Klein, R., Mehlhorn, K., Meiser, S.: Randomized incremental construction of ab-stract Voronoi diagrams. Computational Geometry 3(3), 157{184 (1993).

[7] A. Okabe, B. Boots, K. Sugihara, and S. N. Chiu, Spatial Tessellations: Concepts and Applications of Voronoi Diagrams, 2nd ed., Wiley July 2000.

[8] Papadopoulou, E., Xu, J.: TheL1Hausdor Voronoi diagram revisited. In: Pro-ceedings of the 8th International Symposium on Voronoi Diagrams in Science and Engineering (ISVD). pp. 67{74 (2011)

[9] Panagiotis Cheilaris, Elena Khramtcova, Evanthia Papadopoulou: Randomized incremental construction of the Hausdorff Voronoi diagram of non-crossing clusters. CoRR abs/1306.5838 (2013)

[10] Sharir, M., Agarwal, P.K.: Davenport Schinzel sequences and their geometric applications. Cambridge Univ. Press, New York (1995)

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing -MobiHoc '05, p. 46, 2005.

[12] B. Y. W. Xu, "Defending Wireless Networks From Radio Interference Attacks Defending Wireless Networks From Radio Interference Attacks," 2007

[13] W. Zhang and G. Cao, Dctc: Dynamic convoy tree-based collaboration for target tracking in sensor networks, IEEE Trans. Wireless Commun. 11(5) (Sept. 2004).

[14] W. zhang and G. Cao, "DCTC: Dynamic convoy tree-based collaboration for target tracking in sensor networks," IEEE Transactions on Wireless Communications, vol. 3, no. 5, pp. 1689–1701, Sept. 2004.

[15] J. Carle and D. Simplot-Ryl, "Energy-efficient area monitoring for sensor networks," IEEE Computer Magazine, vol. 37, no. 2, pp. 40–46, Feb. 2004.

[16] D. Jayasimha, "Fault Tolerance in a Multisensor Environment," Proc. of the 13th Symposium on Reliable Distributed Systems (SRDS'94), October 1994.

[17] L. Klein, "Sensor and Data Fusion Concepts and Applications," SPIE Optical Engr Press,WA, 1993.

Effective Measurement Requirements for Network Security Management

Dr. Rabiah Ahmad
Department of System & Computer Communication
Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
Melaka, Malaysia

Prof. Shahrin Sahib
Department of System & Computer Communication
Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
Melaka, Malaysia

M.P. Azuwa
Research Department
Cybersecurity Malaysia
Selangor, Malaysia

***Abstract*— Technical security metrics provide measurements in ensuring the effectiveness of technical security controls or technology devices/objects that are used in protecting the information systems. However, lack of understanding and method to develop the technical security metrics may lead to unachievable security control objectives and incompetence of the implementation. This paper proposes a model of technical security metric to measure the effectiveness of network security management. The measurement is based on the effectiveness of security performance for (1) network security controls such as firewall, Intrusion Detection Prevention System (IDPS), switch, wireless access point, wireless controllers and network architecture; and (2) network services such as Hypertext Transfer Protocol Secure (HTTPS) and virtual private network (VPN). We use the Goal-Question-Metric (GQM) paradigm [1] which links the measurement goals to measurement questions and produce the metrics that can easily be interpreted in compliance with the requirements. The outcome of this research method is the introduction of network security management metric as an attribute to the Technical Security Metric (TSM) model. Apparently, the proposed TSM model may provide guidance for organizations in complying with effective measurement requirements of ISO/IEC 27001 Information Security Management System (ISMS) standard. The proposed model will provide a comprehensive measurement and guidance to support the use of ISO/IEC 27004 ISMS Measurement template.**

Keywords- Security metrics; Technical security metrics model; Measurement; Goal-Question-Metric (GQM); Effective measurement; Network security management

I. INTRODUCTION *(HEADING 1)*

Network security is defined as the security of devices, security of management activities related to the devices, applications/services, and end-users, in addition to security of the information being transferred across the communication links [2]. How much protection is required in ensuring the use of information and associated networks to conduct the business are well managed? How to identify and analyze network security controls to mitigate the network security risks? These questions have derived to implement and maintain secure and functional network is absolutely critical to the success of any organization's business operations [2][3]. Thus, it is important to measure network security effectiveness in handling the risks from the current threats, vulnerabilities and attacks.

According to [4], the practical challenges and issues are what to measure and what information to report in facilitates the senior management for any decision making. Obviously, the reported information is often based on what is easier to measure instead of what is actually meaningful strategically [5], [6], [7]. Does network security management is among the "easier" information to measure?

Some organizations may be reported the measures from out of context perspective, without a baseline for comparison, or present simple measurements that do not show any kind of correlation, which greatly (or even completely) limits the value of the reported information [5][8].

A. Requirements From ISO/IEC 27001 ISMS Standard

ISO/IEC 27001:2005 Information Security Management System (ISMS) [9] is intended to bring formal specification of information security under explicit management control. It is a mandated specific requirement, where organizations can therefore be formally audited and certified compliant with the standard.

The standard provides some confidence level of information protection among business organizations. With the existence of ISO/IEC 27001 ISMS certification, these organizations can increase their protection of information by having independent assessment conducted by the accredited certification body. The certificate has proven the potential marketing to the most business organizations, where a total of 7536 organizations have already been certified worldwide [10]. Obviously, there are other 27000 series that support this standard, including ISO/IEC 27002 Code of practice for information security management [11], ISO/IEC 27003 ISMS implementation guidance [12], ISO/IEC 27004 Information security management – Measurement [13] and ISO/IEC 27005 Information security risk management [14].

There are 133 security controls in Annex-A of ISO/IEC 27001 ISMS standard. ISO/IEC 27002 [11] provides the best practice guidance in initiating, implementing or maintaining the security control in the ISMS. This standard regards that "not all of the controls and guidance in this code of practice may be

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

applicable and additional controls and guidelines not included in this standard may be required."

Information security measurement is a mandatory requirement in this standard where a few clauses are stated in [9]:

- "4.2.2(d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results;
- 4.2.3(c) Measure the effectiveness of controls to verify that security requirements have been met;
- 4.3.1(g) documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls;
- 7.2(f) results from effectiveness measurements; and
- 7.3(e) Improvement to how the effectiveness of controls is being measured."

Moreover, the new revision of ISO/IEC 27001:2013 [15] standard has also highlighted the importance of effective measurement in their mandatory requirement clauses 9 - Performance evaluation.

B. Summary

The standard highlighted that the organization must evaluate the information security performance and the effectiveness of the ISMS. The evaluation of the effectiveness should include but not limited to: (i) monitor and measure information security processes and controls; (ii) methods to use when monitor and analyze measurement for valid or significant result; (iii) time and personnel to perform the monitoring a nd measurement; (iv) determine time, duration and personnel to analyze the measurement results.

Thus, in ensuring the ISMS effectiveness, the information security measure can facilitate the management to make decision by the collection, analysis, evaluation and reporting of relevant performance-related measurements.

The importance of information security measurement is well defined and highlighted in both standards. Most of the research papers focused on information security metrics for general IT systems. However, lack of research on technical security metrics [16][17][18][19]. Thus, our research is focusing on the development of technical security measurement that will be incorporated in the technical security metric model.

II. RELATED WORK

In understanding the requirements, the security metric, measure and effective measurement must be defined. "Whatever the driver for implementing ISO 27001, it should no longer be just about identifying the controls to be implemented (based on the risk), but also about how each control will be measured. After all, if you can't measure it, how do you know it's working effectively?" [20].

In our previous study [21], we defined information security metrics is a measurement standard for information security controls that can be quantified and reviewed to meet the security objectives. It facilitates the relevant actions for improvement, provide decision making and guide compliancy to security standards. Information security measurement is a process of measuring or assessing the effectiveness of information security controls that can be described by the relevant measurement methods to quantify the data and the measurement results are comparable and reproducible.

Apparently, we also mapped the definitions of security metric, security measure and effective measurement from the previous studies [5][6][20][22][23][24][25][16][26][17][27][28][29] [30][18][31][32][33][19][34] (refer to Table 1).

From Table I, we grouped the eight (8) components of security metrics and supported by the components in security measures. The definitions of security metric and security measures are quite similar through the analysis of the descriptions. To ease the understanding, the metric is also sometimes called a "measure" [27]. However, in the development of TSMM, we intend to develop a security metric that can consist of a few security measures.

We also derived the eight (8) criteria of the effective security metric (ESM) that are supported by the following statement:

a) Meet security objectives - ESM should gauge how well organization is meeting its security objectives. It should also have a clearly defined set of variables which are acceptable, unacceptable and excellent range of values that can be easily identified by the audience to which the measure is communicated.
b) Quantifiable values – ESM should be a quantitatively measurable that derived from precise and reliable numeric values and expressed by using understood and unambiguous units of measure.
c) Simple measurement – ESM should be easily recognize and comprehended by the audience for which they are intended. The measurement method should be produced by a process or procedure to collect data, determine the data source, scale or score, analysis, and reporting of relevant data. The right and competent personnel should be identified to conduct the measurement and able to analyze and produce the accurate report.

Identify applicable sponsor/s here. *(sponsors)*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE I. A MATRIX MAPPINGS THE DEFINITIONS OF SECURITY METRICS, SECURITY MEASURES AND EFFECTIVE MEASUREMENT

Security Metric	Security Measure	Effective Measurement
(1) Security Objectives • Identify the adequacy of security controls	• Clearly defined acceptable value • Performance goals and objectives (efficiency, effectiveness)	• Meet security objectives and requirements • Clearly defined
(2) Quantifiable, computed value	• Quantifiable information • Scope of measurement (Process, performance, outcomes, quality, trends, conformance to standards and probabilities)	• The value is objective and quantifiable • Determine the Key-Performance-Indicator (KPI)
(3) Method of Measurement • Process of data collection, data from security assessment process	• Easily identified • Quantitative indications by some attributes of a control or process	• Simple measurement • Low cost and easy access • Capability to measure accurately
(4) Analysis of Data • Comparable to a scale/ benchmark/Predetermined baseline • Repeatable	• Apply formulas for analysis • Track changes • Quantifiable information for comparison	• Consistent value • Accurate time and data • Comparable and reproducible results • Security controls are implemented correctly, operating as intended, and meeting the desired outcome.
(5) Security Indicator/Characteristics • Meaningful result (score, rating, rank, or assessment result)	• Monitor the accomplishment	• Increase confidence level • Security improvement
(6) Reporting relevant data	• Communicated/Reported • Intended audience	• Present to targeted audience/ Stakeholder
(7) Decision making	• Facilitate decision making	• Facilitate corrective action
(8) Requirement to Standard, regulatory, financial and organizational reasons		• Align with business goals and regulations

d) Comparable result – ESM should produce a baseline for comparison purposes, repeatable or consistently reproducible, so that different people at different times can make the same measurement. Apparently, this supports the adequacy of in-place security controls, policies, and procedures; security controls are implemented correctly, operating as intended, and meeting the desired outcome.

e) Corrective action - ESM should provide the appropriate timeliness and frequency of measurement for the change of measurement target so that the latency of measures does not defeat their purpose. ESM should be collected and reported in a consistent manner. ESM should provide the management to decide the new investment in additional information security resources, identify and evaluate non-productive security controls, and prioritize security controls for continuous monitoring.

f) Targeted audience/Stakeholder – ESM should be easily identified by the audience/stakeholder to whom the measure is communicated. For example, provide the relevant measures that produce the significant result for the management to make decision.

g) Security Improvement – ESM should provide some indicators that could be a sign of relevant security characteristics that prescribes the meaning of obtained security values and achieves to some level of improvement.

h) Align with business goals - ESM should provide a benefit to the business it supports.

The development of our TSMM is based on the above criteria and to focus on security performance for the relevant controls (see Fig.1).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

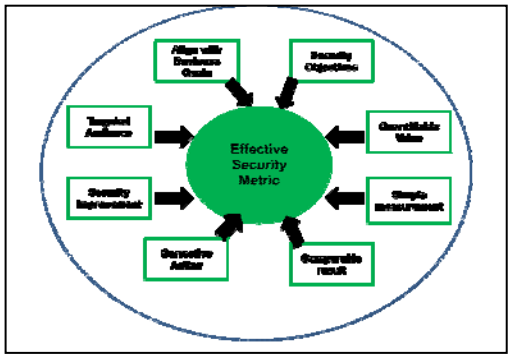


Figure 1. Eight Criteria of Effective Security Metric

III. Research Method for Development Of Technical Security Metric Model (TSMM)

The GQM approach was originally developed by Basili et.al [1] in evaluation and measurement of software products and development processes. Ever since developed, this approach was used consistently focus on the software measurement and processes [35]. There were also a few research studies on business processes [36][37][38] and security metrics [26][39][40][41][42][43][44]. However, there is no research study conducted for measuring the network security management using the same approach.

To achieve the objective of developing the TSMM, we propose a research method based on a combination of approaches. The outcome of this research method is the introduction of network security management metrics as attributes to the TSMM.

The first approach is to define the technical security metric (TSM). We set our goal to meet the requirements from ISO/IEC 27001 ISMS standard. The paradigm of Goal-Question-Metric (GQM) [1] is used and described further which to align with standard requirement (Fig.2).

We combine the developed Goal-Question-Metric (GQM) paradigm and data of literature review (Fig.3) as a first step. This approach is used for developing the initial TSM in a top-down manner, from general objective to the relevant metrics or outputs and combines the inputs from the literature review. The application results in GQM models, leading to the initial TSMM. However, this initial development work remains subjective and potentially incomplete.

In the second approach (Step 2), we use the GQM method consists of four phases [45]: planning, definition, data collection, interpretation (see Fig.4). The explanation of these phases is based on the compliancy to the requirement controls of ISO/IEC 27001 standard [9] for A.10.6 Network security management (NSM); A.10.6.1 Network controls; and A.10.6.2 Secure network services.

Our implementation adopts the processes and activities by [41] and [46].

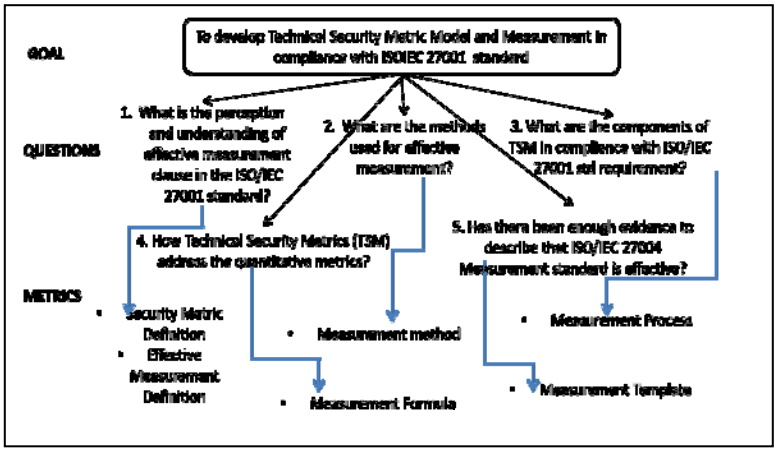


Figure 2. Eight Criteria of Effective Security Metric

- The *Planning phase*: The NSM-team is established and the compliance requirement is clearly delivered. The desired improvement areas such as performance, security and monitor are identified. The team selects and characterizes the products or controls to be studied. The result of this phase is a project plan that outlines the characterization of the products or controls, the schedule of measuring, the organizational structure, and necessary awareness and training for people involved in measurements.

- The *Definition phase*: The measurement goals are defined. This phase is also to identify and analyze the perception and understanding of effective measurement requirement from ISO/IEC 27001 standard [9]. We will create a new template to gather all related information based on some other templates from ISO/IEC 27004 [13] and NIST SP800-55 [27]. For the purpose of this, the interviews may be conducted with people (management and technical) involved in the process or product under study. Based on the goals, relevant questions are developed to identify the specific quality attributes and to re-define the goals

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

precisely. For each question a hypothesis with an expected answer should be defined. Next, the metrics are defined for each question and checked on consistency and completeness. Results of this phase are an analysis of compliance plan and a measurement plan.

- The *Data Collection phase* – the team is required to prepare the data collection within their knowledge and availability. The data may be extracted manually or electronically and may involve automated data collection tools. Results of this phase are to develop the data support system consisting of spreadsheets, statistical tools, database applications and presentation tools.
- The *Interpretation phase* - the collected data is processed and analyzed according to the metrics defined. The measurements result should be able to answer the questions, and with the answers it can be evaluated if the initial goals are attained. Moreover, the measurement result should provide some values that describing the performance measurement of the security controls.

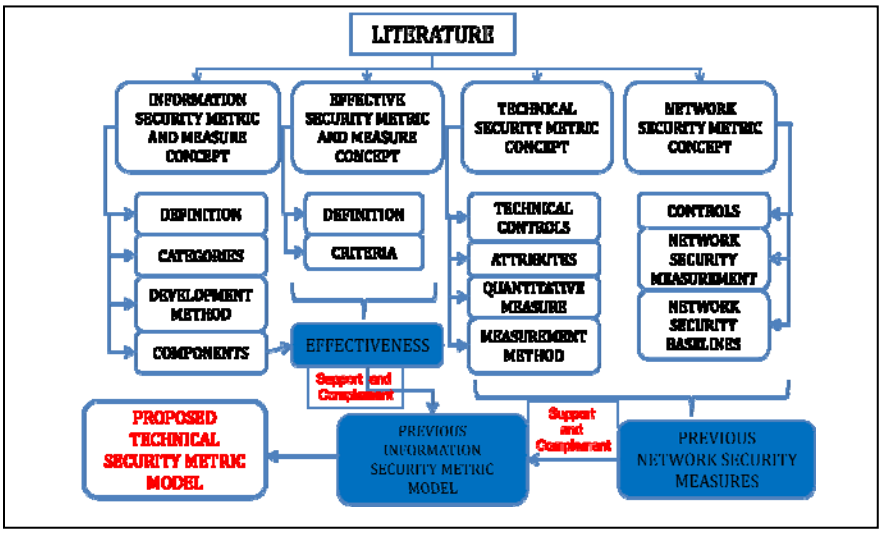


Figure 3. Data from literature review

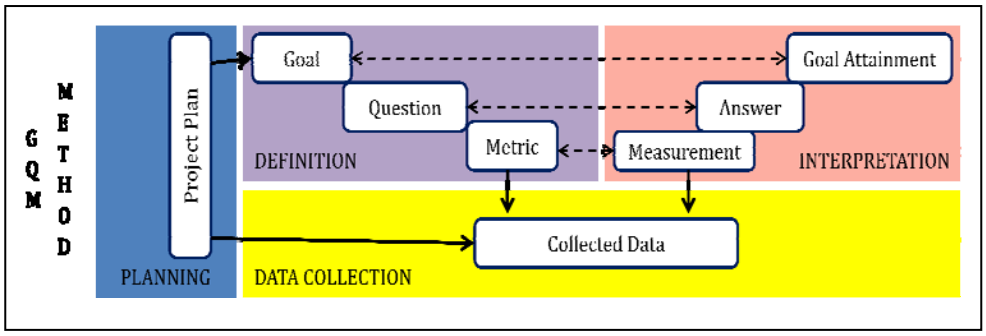


Figure 4. The four phases of GQM-method [45]

The second approach is used as a validation/improvement of the first step. It is based on a literature review of security metric standards and guidelines and measurement methods for network security controls. This approach is a bottom-up, being an analysis of the literature to identify the metrics currently used. A comparative analysis is developed between the metrics and those defined through GQM. This comparison is summarized in an analysis table.

As shown in Fig.5, we map the GQM-method with ISO/IEC 27004 template for an information security measurement construct and show the synchronization link (relevant colored-box). We refer to this standard as a reference and example to form a GQM-Measurement plan.

Once the literature is completely surveyed, the development of GQM-Measurement plan should be ready. The relevant people should be interviewed to validate the initial TSMM. Finally, the TSMM is accordingly revised.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A. GQM-Measurement Plan

We develop a GQM-Measurement plan consists of goals, questions, and metrics in a hierarchical structure (see Fig. 6) based on [1][45].

In developing the goals, the security objectives of A.10.6, A.10.6.1 and A.10.6.2 of ISO/IEC 27001 requirement controls [9] are referred. At this stage, the understanding of the security control requirements is very important. The understanding can be obtained through the interview with the relevant people and checking available process or product descriptions [46]. If goals are still unclear, a reference to ISO/IEC 27002 [11], FDIS ISO/IEC 27033 [2] and NIST SP800-55 [25] can also assist.

The proposed questions shall refine the goals make them operational enough so that it would not create difficulties to reveal the relationship to the collected data and ease the interpretation of the answers towards the goals [46]. The questions are also derived from the literature reviews.

The questions are stated in a quantitative way where data can be collected by measurements. We provide the expected answers to the questions and formulated as hypotheses. Through hypotheses, we can learn the effect from measurements and compare the knowledge before and after measurements.

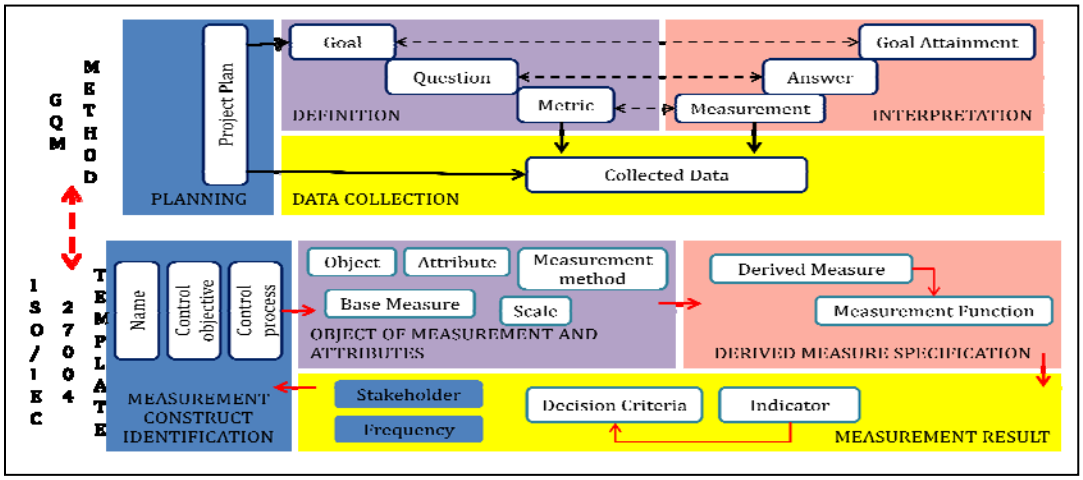


Figure 5. Synchronization between GQM-Method and ISO/IEC 27004 Measurement Template

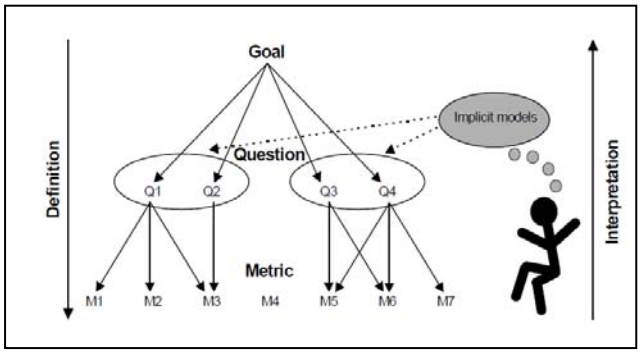


Figure 6. The GQM Paradigm by Basili et.al [1]

According to [1][41][46], we can define several metrics for each question. It is also possible that one metric may be used to answer different questions under the same goal. We choose metrics with quantitative level making it possible to assign numbers to a quality attribute. Metrics are defined to answer the relevant questions and should be able to support or reject the stated hypotheses (if any).

A simple Goal-Measurement plan is developed for the purpose of this discussion (as full development of plan is currently in progress). The example of GQM-Measurement plan as stated in Table II.

TABLE II. EXAMPLE OF GQM-MEASUREMENT PLAN

Goal	G1	A.10.6.1 Network controls - Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
Question	Q1	What are the risk levels for network controls and security controls that protect your information?
Metric	M1.1	Risk Assessment = Asset Value x Threat x Vulnerability
Question	Q2	What are the monitoring mechanisms that your organization has?
Metric	M2.1	Frequency of audit logging review
Metric	M2.2	Security Incidents report (IDS/IPS/user report) - Comparison of number of total incidents with the threshold.
Question	Q3	How often the security assessment and/or penetration testing are conducted within a year?
Metric	M3.1	Frequency of assessment conducted
Metric	M3.2	Success or failure rate for corrective action
Metric	M3.3	Conducted by trained/experience staff
Question	Q4	How often your organization conduct the security updates for network controls?

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Metric	M4.1	Success and failure rates of security updates
Metric	M4.2	Frequency/periodic of maintenance
Question	Q5	Who is responsible to ensure the effectiveness of network controls is intact?
Metric	M5.1	Rate of understanding the job description
Metric	M5.2	Qualification, Training and Education attended
Question	Q6	What are the authentication mechanism in accessing the network and systems used in your organization?
Metric	M6.1	Password quality – manual (Number of passwords which satisfy organization's password quality policy for each user)
Metric	M6.2	Password quality - automated
Metric	M6.3	Number of password being shared?
Metric	M6.4	Ratio of passwords crackable within 4 hours.
Question	Q7	Who is responsible to ensure the effectiveness of network controls is intact?
Metric	M7.1	Rate of understanding the job function
Metric	M7.2	Qualification, Training and Education attended
Metric	M7.3	Ratio of responsible personnel to total number of staff
Question	Q8	What are the mechanism used to authorize the relevant users to access the networks and systems?
Metric	M8.1	Number of restricted access methods (network segment, IP address, MAC address, firewall, etc.)

IV. Conclusion and Future Work

The objective of this paper is to identify and to define a set of metrics for the TSMM with a systematic and scientific approach to comply with ISO/IEC 27001 standard. We use the GQM approach on the TSMM and review with regards to the literature. The result of this paper is the enrichment of the TSMM with suited network security management metrics.

Although the initial developed TSMM are validated through literature analysis, their testing in a real case would provide a concrete instantiation and validation of their relevance. The GQM-Measurement plan is currently being developed to suit the security objectives. The validation will be conducted with the network security experts.

As part of the next step of our future work, the metrics will be integrated into the initial TSMM and a case study is to be conducted using our GQM-Measurement plan. This will validate the final TSMM.

Acknowledgment

The authors wish to acknowledge and thank members of the research teams of the Long Term Fundamental Research Grant Scheme (LRGS) number LRGS/TD/2011/UKM/ICT/02/03 for this work. The research scheme is supported by the Ministry of Higher Education (MOHE) under the Malaysian R&D National Funding Agency Programme. This project is also supported by the CyberSecurity Malaysia and the Universiti Teknikal Malaysia Melaka (UTeM), Malaysia.

References

[1] V. R. Basili, G. Caldiera, and H. D. Rombach, Goal Question Metric Paradigm. Encyclopedia of Software Engineering. John Wiley & Sons, Inc., 1994, pp. 532–538.

[2] FDIS 27033-1:2009, "Text of ISO/IEC FDIS 27033-1 - Information technology - Security techniques – Network security — Part 1: Overview and concepts," Int. Organ. Stand. Int. Electrotech. Comm. FDIS 27033-12009, no. Final Draft, 2009.

[3] N. Schneidewind, "Metrics for mitigating cybersecurity threats to networks," IEEE Internet Comput., vol. 14, no. 1, pp. 64–71, Jan. 2010.

[4] R. Barabanov, S. Kowalski, and L. Yngström, "Information Security Metrics : Research Directions," Stock. Univ., 2011.

[5] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional, 2007.

[6] D. S. Herrmann, Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI, 1st ed. Auerbach Publications, 2007, p. 848.

[7] W. K. Brotby, "Information Security Governance: Guidance for Information Security Managers," IT Gov. Inst., 2008.

[8] R. Ayoub, "Analysis of Business driven metrics: measuring for security value." 2006.

[9] ISO/IEC 27001:2005, "Information technology - Security techniques - Information security management systems- Requirements," Int. Organ. Stand. Int. Electrotech. Comm. ISO/IEC 270012005, 2005.

[10] "Number of Certificates Per Country," International Register of ISMS Certificates, 2012. [Online]. Available: http://www.iso27001certificates.com/. [Accessed: 08-Dec-2011].

[11] ISO/IEC 27002:2005, "Information technology - security techniques - Code of practice for information security management," International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27002:2005, vol. 2005. 2005.

[12] ISO/IEC 27003:2010, "Information technology - Security techniques - Information security management systems- Implementation Guidance," International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27003:2010. International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27003:2010, 2010.

[13] ISO/IEC 27004:2009, "Information technology - Security techniques - Information security management systems- Measurement," International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27004:2009. International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27004:2009, 2009.

[14] ISO/IEC 27005:2011, "Information technology - Security techniques - Information security risk management," Int. Organ. Stand. Int. Electrotech. Comm. ISO/IEC 270052011, 2011.

[15] ISO/IEC 27001:2013, "Information technology - Security techniques - Information security management systems- Requirements," Int. Organ. Stand. Int. Electrotech. Comm. ISO/IEC 270012013, 2013.

[16] M. Stoddard, D. Bodeau, R. Carlson, C. Glantz, Y. Haimes, C. Lian, J. Santos, and J. Shaw, "Process Control System Security Metrics – State of Practice," Inst. Inf. Infrastruct. Prot., vol. Research R, no. August, 2005.

[17] J. P. Pironti, "Developing Metrics for Effective Information Security Governance," Inf. Syst. Control J., vol. 2, 2007.

[18] J. Hallberg, M. Eriksson, H. Granlund, S. Kowalski, K. Lundholm, Y. Monfelt, S. Pilemalm, T. Wätterstam, and L. Yngström, "Controlled Information Security: Results and Conclusions from the Research Project," FOI Swedish Def. Res. Agency, pp. 1–42, 2011.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[19] R. Savola, "A Security Metrics Taxonomization Model for Software-Intensive Systems.," J. Inf. Process. Syst., vol. 5, no. 4, pp. 197–206, Dec. 2009.

[20] S. Wright, "Measuring the Effectiveness of Security using ISO 27001," SANS Inst., pp. 1–15, 2006.

[21] M. P. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "Technical Security Metrics Model in Compliance with ISO / IEC 27001 Standard," Int. J. Cyber-Security Digit. Forensics, vol. 1, no. 4, pp. 280–288, 2012.

[22] W. Jansen, "Directions in Security Metrics Research," Natl. Inst. Stand. Technol. NISTIR 7564, 2009.

[23] M. Masera and I. N. Fovino, "Security metrics for cyber security assessment and testing," Jt. Res. Cent. Eur. Comm., vol. ESCORTS D4, no. August, pp. 1–26, 2010.

[24] Y. Beres, M. C. Mont, J. Griffin, and S. Shiu, "Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Processes," Methodology, pp. 564–573, 2009.

[25] R. B. Vaughn, R. Henning, and A. Siraj, "Information assurance measures and metrics-state of practice and proposed taxonomy," Proc. 36th Hawaii Int. Conf. Syst. Sci., p. 10, 2003.

[26] R. Savola, "Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry," in International Conference on Software Engineering Advances, 2007.

[27] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance M easurement Guide for Information Security," Natl. Inst. Stand. Technol. Spec. Publ. 800-55, no. July, 2008.

[28] F. C. Freiling, "Introduction to Security Metrics," Dependability Metrics, LNCS 4909, Springer-Verlag Berlin Heidelb., pp. 129–132, 2008.

[29] W. K. Brotby, "Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement," Auerbach Publ., 2009.

[30] H. Liu and Y. Zhu, "Measuring effectiveness of information security management," Int. Symp. Comput. Netw. Multimed. Technol. 2009. CNMT 2009., pp. 1–4, 2009.

[31] K. Lundholm, J. Hallberg, and H. Granlund, "Design and Use of Information Security Metrics," FOI, Swedish Def. Res. Agency, p. ISSN 1650–1942, 2011.

[32] G. Jelen, "SSE-CMM Security Metrics," NIST CSSPAB Work. Washington, D.C., 2000.

[33] D. A. Chapin and S. Akridge, "How Can Security Be Measured?," Inf. Syst. Control J., vol. 2, 2005.

[34] M. H. S. Peláez, "Measuring effectiveness in Information Security Controls," SANS Inst., 2010.

[35] H. K. N. Leung, "Quality metrics for intranet applications," Inf. Manag., vol. 38, 2001.

[36] V. Basili, J. Heidrich, M. Lindvall, J. Münch, C. Seaman, M. Regardie, and A. Trendowicz, "Determining the impact of business strategies using principles from goal-oriented measurement.," Proc. Wirtschaftsinformatik 2009 9th Int. Conf. Bus. Informatics. Vienna., 2009.

[37] A. Azim and A. Ghani, "Complexity Metrics for Measuring the Understandability and Maintainability of Business Process Models using Goal-Question-Metric (GQM)," vol. 8, no. 5, pp. 219–225, 2008.

[38] L. S. González, F. G. Rubio, F. R. González, and M. P. Velthuis, "Measurement in business processes: a systematic review," Bus. Process Manag. J., vol. 16, no. 1, pp. 114–134, 2010.

[39] T. Perkins, R. Peterson, and L. Smith, "Back to the Basics: Measurement and Metrics," pp. 9–12, 2003.

[40] D. Lekkas and D. Spinellis, "Handling and reporting security advisories: A scorecard approach," Secur. Privacy, IEEE, 2005.

[41] N. Mayer and E. Dubois, "Towards a Measurement Framework for Security Risk Management," Proc. Model. Secur. Work., 2008.

[42] T. Heyman, R. Scandariato, C. Huygens, and W. Joosen, "Using Security Patterns to Combine Security Metrics," 2008 Third Int. Conf. Availability, Reliab. Secur., pp. 1156–1163, Mar. 2008.

[43] R. Gonzalez, "A measurement model for secure and usable e-commerce websites," Can. Conf. Electr. Comput. Eng. 2009., no. c, pp. 77–82, 2009.

[44] K. Julisch, "A Unifying Theory of Security Metrics with Applications with Applications," 2009.

[45] R. Van Solingen and E. Berghout, "The Goal/Question/Metric Method: a practical guide for quality improvement of software development," The McGraw-Hill, 1999.

[46] H. Koziolek, "Goal , Question , Metric," Dependability Metrics, LNCS 4909, Springer-Verlag Berlin Heidelb., pp. 39–42, 2008.

AUTHORS PROFILE

Rabiah Ahmad received Ph.D in Health Informatics at University of Sheffield (UK) and Master of Science in Information Security from Royal Holloway University of London (UK). She is currently appointed as Associate Professor at Universiti Teknikal Malaysia Melaka (UTeM) and acting as Deputy Director at Centre for Research Innovation and Management. Rabiah Ahmad involved with various research in information security and health informatics. She has become project leader for 4 research projects funded by the Ministry of Science, Technology and Innovation, Malaysia and the Ministry of Higher Education, Malaysia. She has wrote 3 academic books, more than 5 chapters in books, 30 articles in International Indexed Journal, 2 articles In Local Indexed Journal, more than 30 in International Proceedings and 3 in Local Proceedings. She has been invited as Manuscript Reviewer for several International Journals such as International Journal of Medical Informatics, International Journal on Cryptography and Journal of Soft Computing.

Shahrin Sahib received the Bachelor of Science in Engineering, Computer Systems and Master of Science in Engineering, System Software in Purdue University in 1989 and 1991 respectively. He received the Doctor of Philosophy, Parallel Processing from University of Sheffield in 1995. His research interests include network security, computer system security, network administration and network design. He is a member panel of Expert National ICT Security and Emergency Response Centre and also Member of Technical Working Group: Policy and Implementation Plan, National Open Source Policy. He is a Professor and Deputy Vice Chancellor Office (Academy and International) at Universiti Teknikal Malaysia Melaka (UTeM).

M.P Azuwa is the Specialist of CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation, Malaysia. Azuwa holds a Master's degree in Computer Science from the Universiti Putra Malaysia, Malaysia and a Bachelor's degree in Computer Science from the same university. She is the holder of Certified Information Security Manager (CISM) Certified in Risk and Information Systems Control (CRISC) from ISACA, USA; Professional on Critical Infrastructure Protection (PCIP) from Critical Infrastructure Institure (CII), Canada; Certified SCADA Security Architect (CSSA) from InfoSec Institute, USA; Certified BS7799 Lead Auditor – Information Security Management System (ISO/IEC 27001); SANS GIAC Security Essential Certified (GSEC). Azuwa has been awarded Information Security Practitioner Honouree in July 2011 by the (ISC)2, USA. She has contributed various publications and presented papers on topics related to vulnerability assessment, SCADA security and information security management. She is currently pursuing his PhD at the Universiti Teknikal Malaysia Melaka (UTeM), Malaysia.

A Survivability Strategy in Mobile Network by Key Distribution and Cross-layer protocol

Anu Chaudhary
Department of information Technology
AKJ Institute of Technology and Management, GZB (INDIA)

K.K Gautam
Department of Computer Science & Technology
Phonics Group of Institutions, Roorkee (INDIA)

Nirbhay Ahlawat
Department of Computer Science & Technology
Phonics Group of Institutions, Roorkee (INDIA)

Abstract:
The capability to provide network service even under a significant network system element disruption is the backbone for the survival of network technology in today's world, keeping this view in mind, the present paper highlights cryptosystem and Cross-Layer Protocol. A global initial key distribution method based on public key certificate chain shall be presented. And also present a method for survivability strategy in mobile network.

Keywords:
Survivability, Mobile Network, Key Distribution Cross-layer protocol

Introduction:
Network survivability is considered to cope with increasing demand for reliable network system. Network survivability is an essential aspect of reliable communication service. Survivability consists not only of robustness against failure occurring due to natural faults. In mobile networks infrastructure element such as base station (BS), and base station Controller (BSC), wired links, and mobile switch centre(MSC), are employed to provide and maintain essential services, hence the operation interruption of a network component affects overall or partial network services . wireless access network have unique characteristics to support mobile users which can result in different survivability and security aspect [1]. There for wireless survivability strategies must be designed to improve the service available rate of the network component system [1-2].

Due to the mobility if node, the network topology is highly dynamic and all traffic suffers from frequent path breaks. The survivability of routing protocols of such networks must be able to perform efficiently and effectively. In this paper we propose a solution on traditional survivability strategy in mobile network. Survivability is a critical requirement for reliable services in any network. This paper highlights the challenge of providing Survivability.

Over the years, cross-layer designs ,which let two or more protocols from non-adjacent layers function in concert, have become very popular. since these tend to sacrifice generality for performance improvements. The two modularity, which provides flexibility in protocol update and specialization. which uses the specificities of a network to improve performance.

Cross-layer designs may be best understood by explain in their opposite-layered scheme. The latter prevent communication between non-

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

adjacent layers in the protocol stack and limit interactions between two adjacent layers to function calls and returns. Cross-layer protocols violate these principles and use information available at two or more levels in the stack to improve the network performance and/or life time.
At one extreme, the multiplication of cross-layer interactions within a protocol stack can lead to "spaghetti" designs, whereby the modification of one aspect in a protocol may have unforeseen consequences within many protocols.
Mobile user authentication is very necessary when a mobile user wants to request service provided by the service providers survivable (SPS) in the visited domains. For the survivable the designing of an authentication survivability protocol (ASP) suitable for the mobile network. In this paper we present a survivability strategy in mobile networks method. by use of key distribution
A network could be as simple a forum held in a city between people , where people use the opportunity of being communicate with each other, they use a network by use of key distribution has the potential for setup the survivability . Fundamental to distribute mechanics is the effect of measurement on a state. If some property of a general state is measured, it collapses to an eigenstate of the property and cannot be 'rebislt' in to the original state. Information can be encoded in to a general quantum state (GQS).

In this way GQS defined by key distribution system. This paper is a survey of the issues, challenges and proposed research directions in survivability mobile network (SMN) resulting from our participation in the key distribution method and cross-layer protocol for survivable mobile network information set up.

Survivability:-

Traditional security research is primarily focused on the detection and prevention of intrusion and attacks rather than on continued correct operation while under attack. Fault tolerance is usually concerned with redundancy that is required to detect and correct up to a given number of naturally occurring faults. Nature is not malicious, and conventional failure model make significant assumptions, in particular, assuming faults to be independent and random. the presence of intelligent adversarial attacks can protocol vulnerability often become more important considerations in the presence of an adversary.

There are a number of definitions of survivability. The one we use here is from the Software Engineering Institute, which emphasizes timeliness, survivability under attack and failure, and that detection of attack is a vital capability.
Survivability is the capability of a system to fulfill its mission in a timely manner. Even in the presence of attacks or failures. Survivability goes demon security and fault. Tolerance of focus on delivery of essential service even when system is entered or experience failures. And rapid recovery of full service when conditions improve. Unlike traditional security measures that require central control and adminarstive, survivability address highly distributed unbounded network environment that lack central control and unified security policies.

The Three Rs: Resistance, Recognition, and Recovery
The focus of survivability is on delivery of essential services and preservation of essential assets. Essential service and asserts are those system capabilities that are critical o fulfilling mission objectives. Survivability depends on three key capabilities: resistance, recognition, and recovery. Resistance is the capability to detect attacks as they occur and to evaluate the extent of damage and compromise. Recovery, a hallmark of survivability is the capability to maintain essential service and asserts during attacks, limit the extent of damage, and restore full service following attack.
We further extend this definition to require that survivability system be able to quickly incorporate lesion learned from failure, evolve, and adapt to emerging threats. We call this survivability feature refinement.
We can classify survivable mobile wireless networking requirement into four categories based on [3]: (i) resistance requirement; (ii) recognition requirement; (iii) recovery requirements; and (iv) refinement requirement. We can also describe a requirement definition process [4]. This includes the definition of system and survivability requirement, legitimate and intruder usage requirement, development requirement, operation requirement, and evolution requirement. Essential service must be identified and specified for the penetration, exploration, and exploitation phases of the attack.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The approach has guided this work and is recommended for more detailed requirement analyses for future mobile wireless network.
Ultimately, there are two distinct aspects of survivability that apply at all networking layers.

Information access requirement:

Does the user have access to the information or service required to complete the task in the presence of failure or attack? For e. g. it is possible to replicate service or information and provide them locally when the network gets partitioned? End – to- end communication should not be mandated in these cases.

End- to- end communication requirement:

On the other hand there are interactive application , inter- personal communication such as voice calls, or dynamically generated information such as current sensor data, which require true end – to – end connectivity . Do existing session survive? Can the user create new session to reach the intended communication end- point even in the presence of failures and attacks? This requires that the communication end – point themselves survive and that the communication end – points themselves survive and that the adversary must not be able to permantely partition the network. Furthermore, the adversary must not be able to permantely disable access to required services such as authentication, naming, resource discovery, or routing.

Mobile Network Survivability:
Existing work on survivability in the context of cellular telephone networks concentrates primarily on infrastructure survivability (for e.g. see the outage index metrics and does not consider adversarial attacks[5-6]. However, they offer some insight on quantifying survivability and the role of network management tools.
Networks are vulnerable during upgrades, especially those involving software [7] . Furthermore, rapid evolution leads to learning – cure problems as well as – over – concentration leads or service into single points of failure. This problem is exacerbated by deficits in network management tools to operate and maintain increasingly complex system.
Architectural improvement applicable to mobile include the use of redundant networks .

Base Station:
In more environment, a cell that Is geographical region unit is geographical region unite is covered by the radio frequency of a base station. Each call is controlled by a BS which has a fixed connection to a BSC (or RNC). In mobile network infrastructure element such as base station controller (BSC), wired links and mobile switch centre (MSC) are employed to provide and maintain essential service,. Hence the operation interruption of a network component affects overall or partial network services.

A radiation antenna is classified as omni directional and directional with an ommnidirectional antenna, a single frequency spreads out in all directions of 360 coverage. A cell is directional antenna with each different set channel.
System State of Base Station:
The BS system, including antenna parts , cannot provide partial or whole service function for coverage cell when single or more fatal failures occur in the BS system . in this paper, we consider that system failures are caused by key distribution method. For example by interrupt sequence mishandling, overall system operation falls into failure state because of unanticipated handled interruption to a component of the system.

Key distribution frame work:
In mobile computing environment , when a mobile host moves to the visited domain it needs to be authenticated by the current domain before gaining the service of the provider in the domain. If the mobile host requires the current visited domain to provide service it will need a shared key with current domain authentication server. An effective method is using the hybrid authentication server. An effective method is using the hybrid authentication method including shared key cryptographic (PKC) system. PKC can verify the identity of the owner of a public key certificate can verify the identity of the owner of a public key and avoid the attack of impersonation. It is impossible to take single public key certificate (SPKC) authority to disseminate the PKC in the interrupt .so a sable Hierarchical Public key distribution (HPKD) framework is presented. According to the scale of the mobile users, the number of the layer of the framework can be decided. Figure 1 is an example of framework. The top level node S A1 is the root of the survivability certificate

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

authorities (SCA). These are n levels CA node in the hierarchical tree.

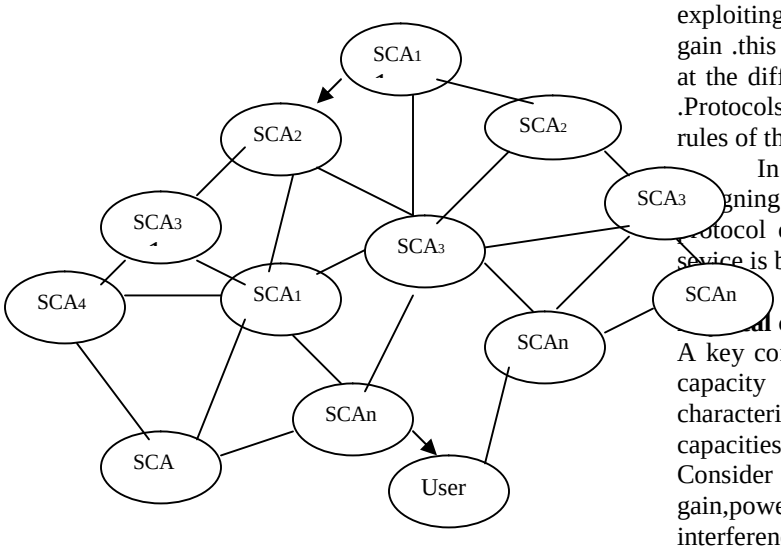


Fig Frame work of Key Distributionure-1

The distributing process of public key certificate (PKC) is described as follows:

(1) SCA_1 Sends PK^1, SC^2 to SCA_2;
(2) SCA_2 Sends $PK^1||PK^2$, $SC^2||SC^3$ to SCA_3;
(3) SCA_3 Sends$PK^1||PK^2||PK^3$,$SC^2||SC^3||SC^4$ to SCA_4
:
:

(n-1) SCA_{n-1} sends PK^1 $||PK^2||\ldots||PK^{n-1}$, SC2||SC3||SC4||….SCn

(n) SCAn Sends $PK^1||PK^2||\ldots||PK^{n-1}$ $||PK^n$, SC2||SC3||SC4|……
After the distributing process is performance the AS and user gain a certificate chain respectively.

A network is connected if these are a path between every pair of nodes. And a network is biconnected if the toss of any one link leaves the network connected. by key distributed framework it is clear that if user is linked by SCA1 then it is to important that every node connected by each other.

Cross-Layer Protocol:

It is repeatedly argued that layered architectures are not suitable for mobile networks. to illustrate this point ,researchers usually present what they call across-layer design proposal .cross-layer design refers to protocol design done by actively exploiting the dependence between protocols gain .this is unlike layering, where the protocols at the different layers are designs independently .Protocols can be designed by respecting the rules of the reference architecture.

In a layer architecture, this would means gning protocols such that a higher-layer otocol only makes use of the services at the service is being provide.

al cross-layer module:

A key concept at the physical cross-layer is the capacity of survivability region. which characterizes a tradeoff between achievable capacities at different links for survivability.
Consider a network with A, B and C_L as the link gain,power,noise,respectly. Denote D_l as the interference coefficient from link k_1 to the link k_2.assume that each node has a power boudget X_{max}. thus the power control with a physical Cross-layer module interference model may be formulated as

$$\max \sum ¥n$$

¥ is dual variable. ¥ play a key role in coordinating the survivability networking layer demand and layer supply.
n-capicity region at the physical cross-layer

$n=\log(1+SINR)$ for every $k_2 \epsilon$ E

$SINR=AB/\sum AB+C_L$ for every L ϵ E

Because of interference, the power control problem is a non convex optimization proble that is present physical cross-layer module[9] capacity approximitly.

Conclusion:

In this paper, we have proposed a scheme for mobile service use of BS system and key distribution and Cross-layer protocol.. The key distribution takes full in to account and the certificate chain is transferred in clear text, impeders can observe the home SCA controls
And cross-layer protocol for many mobile host. When the mobile host gets to visited domain, it may get a survivability scheme.

Reference:

(1) D.Tipper, S. Rammaswamy, and T. Dahiberg,"pcs network survivability" in proc. IEEE WCNC, new or leans LA, sep 1999, invited paper.

(2) D. Samfat, R. molva, N. Asokan, "Untraceability in mobilke Network" Proceeding of Mobi COM'95, Berkely, November 1995.
(3) R.J.Ellison,D.A.Ficher,R.C.Linger, H.F.Lipson,T.Longstaff and N.R. Mead, "Survivable Network Systems;An Emerging Discipline," Tech. Report CMU/SEI-97-TR-013 and ESC-TR=97-013,CarnegieMellonUniversity,software Engineering, Institute ,Nov,1997.
(4) J.Kabara , P. Krishna Murthy, and D. Tipper, "Information auuurance in wireless network". In proc. IEEE workshop on DIREN'02.
(5) U. Varshney A.P Snow and A.D. Malloy, "Designing Survivable wireless and mobile network" in proc. IEEE WCNC'99, neworeleans, LA, Sep. 1994, pp.30-34.
(6) Zhang Bin, Wujing-Xing Proc. Of the feb.2003 ICCNMC'03 IEEE.
(7) Sangjoon Park, Jiyoung Song, Byunaggi Kim, IEEE Trans of Veh. Tech. Vol. 55 pp 328-339.
(8) Ashotosh Dutta , James Burns , K. Daniel Wong, Ravi jain, Ken Young Telcordia Technologies, 445 South Street, Morristown, NJ 07960 pp 1-6
(9) Sangjoon Park , Jiyoung song, and Byunggi Kim, Member, IEEE "A Survivability Strategy in Mobile Networks. IEEE TRANSACTION ON TECHNOLOGY, VOL. 55,NO.328-340.
(10) JunYun, Zongpeng Li,Wei Yu,and Baochun Li,IEEE JOURNAL ON SELECTED AREA IN COMMUNICATIONS, VOL,24,NO,11,NOVEMBER2006.

.

AUTHORS PROFILE

Authors Profile ..Anu Chaudhary is the Head of the Department in Inforation of Technoogy & Management, Gzb and completed his PHD from Gurukul Kangari University,Haridwar (India). Prof Anu is basically working in the area of mobile network.

K K Gautam is a Director in the Phonics Group of Institutions, Roorkee (India). Prof Gautam has completed his PhD in Computer Engineering Department. He has a teaching experience of more than 20 years and also has many research paper in the field of network security and currently he is working in the area of mobile network and wireless network.

Nirbhay Ahlawat is the Astt.Prof. in the department of Computer science in Phonics Group of Institutions,Roorkee and completed his M.tech From Subharti University,Meerut (India).He is also a research scholar and presently working in the field of Network Security.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Effect of Cross Layer optimization of Traffic Management in Ad HOC Mobile Network

Anu Chaudhary
Department of information Technology
AKJ Institute of Technology and Management, GZB
(INDIA)

K.K Gautam
Department of Computer Science & Technology Phonics Group of Institutions, Roorkee
(INDIA)

Nirbhay Ahlawat
Department of Computer Science & Technology Phonics Group of Institutions, Roorkee
(INDIA)

Abstract:- The optimal and distributed provisioning of high through output in Mobile Ad Hoc Network (MANET) is a network consisting of a set of wireless mobile routers and Communication with each other. The Network Mobility(NEMO) for the traffic represents the moving behavior of directional antenna and mobile rooters. Use the Cross-layer protocol in ad hoc wireless network we can drastically improve the utilization through overlapping communication is the different direction for the traffic. This paper highilight the chalenge to find out a route of effect the cross-layer protocol for traffic-management in Ad Hoc wireless network. In present paper we propose mobility for traffic mamnement in Ad Hoc wireless network by use of theory of Cross-layer protocol.

Keywords:-Ad hoc Network, Cross-layer protocol , Directional Antenna, Mobile Router, Network Mobility

Introduction:- AD HOC NETWORKS are multiple wireless networks consisting of a large number of radio equipped nodes that may be as simple as autonomous sensors. These type of network are useful in any situation where temporary network connectivity is needed such as in disaster relief. A mobile ad hoc network (MANET), is a network comprising wireless mobile rooters (MRs) that communication with each other without centralized control. The dynamic of wireless ad hoc networks as a consequence of mobility and disconnection of mobile host. The MRs that are within each other's radio range can communication directly. Each mobile rooter's acts as host in MANET environment. Mobile rooters are free to join or leave the network at any point of time.

Here we are working towards implementing wireless ad hoc community network (WACNEC) that was small, low cost directional antenna, known as ESTAR (Electronically Steerable passive Array Radiator) antenna, with each user terming [1,2].Due to unreliability of wireless links, it has been of interest to study the impact of physical-layer techniques on the design ,including medium access control(MAC),packet scheduling, power control, routing, transport protocol, and ultimately the QoS at the application level in the wireless networks.

Mobility system define rooter, movement patterns in ad hoc networks. Since MANETs are currently not deployed on are large scale and due to inherent randomness of mobility modes, research in evaluating the performance of routing protocols on various system of mobility. In this paper the performance of MANET for the effect of cross-layer protocol [3]. In[3],a cross-layer design approach is employed to improve the performance of combined cooperative schemes. The cross-layer information is minted

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

in a separated data structure and is shared among layers.

Whatever may be routing scheme, they all rely on using Omni-directional antenna. The use of directional antenna to find out a route and use it in database has not been explored properly. Here we proposed Cross-layer protocol where each node keeps certain neighborhood information dynamically through the Maintenance of an Angle – SINR Table.

For experimental purposes we have considered A framework to evaluate the impact of different mobility models on the performance of MANET routing cross-layer protocol is provides in [4] various protocol independent matrices are provided to capture interesting mobility characteristics restrictions.

Mobility models:- The mobility model is designed to described the movement pattern of Mobility models used in the simulation study of MANET.: traces base model and synthetic base model [4]. The traces base model obtains determistic data from the real system. This mobility model is still in its early stage of research, therefore it is not recommended to be used. The synthetic based model is the imaginative model that used statics. The movement of each MN to its destination has a pattern that can be described by a statistical model that expresses the movement behavior in the real environment.

The Framework:-

Angle – SINR Table :-

In order to make the directional routing effective, a node should know how to set its transmission direction effectively to transmit a packet to its neighbors. So each node periodically collects its neighborhood information and forms an Angle- SINR Table (AST). Sinu^{s} m(t) (Signal – to – Interference and Noise Ratio) is a number associated with each link 1^{u} n, m, and is a measurable indicator of the strength of radio connection from node n to node m at an angle u with respect to n and as perceived by m at any point of time t. AST of node n specifies the strength of radio connection of its neighbors with respect to n at a particular direction . Angle - SINR Table for node n time t is shown below (Table I) where we assume that nodes I, j and k are the neighbors of n.

TABLE I. ANGLE – SINR TABLE (AST)FOR NODE n

Azimuth Angle	**SINR value as perceived by neighbors of rooters n at different angle w.r.t rooters n**		
	I	**j**	**K**
(degree)			
0	$SINR^{0}n,i^{(t)}$	$SINR^{0}n,j^{(t)}$	$SINR^{0}n,j^{(t)}$
30	$SINR^{30}n,i^{(t)}$	$SINR^{30}n,j^{(t)}$	$SINR^{30}n,j^{(t)}$
60	$SINR^{60}n,i^{(t)}$	$SINR^{60}n,j^{(t)}$	$SINR^{60}n,j^{(t)}$
…	…..	…..	….
330	$SINR^{330}n,i^{(t)}$	$SINR^{330}n,j^{(t)}$	$SINR^{330}n,j^{(t)}$
360	$SINR^{360}n,i^{(t)}$	$SINR^{360}n,j^{(t)}$	$SINR^{360}n,j^{(t)}$

In order to form AST, each node periodically sends a directional request in the form of a directional broadcast, sequentially in all direction . in this work it has been done 30 degree interval, covering the entire 360 degree space sequentially. A node is i in the neighborhood of n will wait until it receives all the request packets generated by n in all direction in that occasion. In others word, node I accumulates the entire column of the AST of n for node I, I accumulates the entire column of the AST of n for rooters i. Here, rooters i, after receiving the first request from n, has to wait a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

pre-specified amount of time to make sure that the directional broadcasts by n in all direction are over. Rooters I sends this information from all the neighbors of n, the Angle-SINR Table of n would be complete.

Omni transmission both transmission range and spatial reuse can be substantially enhance by having nodes concentrate transmitted energy only towards their destination direction, thereby achieving higher signal to noise ratio.

When there is a need to utilize only the directional characteristic, the demands are more since this is possible only when the rooters which wants to transmit and the rooters which wants to receive are synchronized with their respective related modes(i.e.) one rooters is in the transmit rooters and other is in the transmit mode and other is in the receive mode and are pointing towards each other as shown in figure 1.

If $x_1 = 60^0$, $x_2 = 120^0$, $x_3 = 180^0$, $x_4 = 240^0$,

$X_5 = 300^0$, $x_6 = 360^0$ then

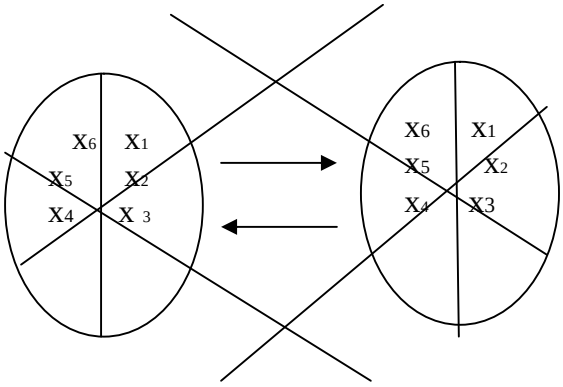


Figure : Basic mechanism for receive Mode and transmit Mode.

This is the most important task of any Cross-layer protocol for Mobile Network is to identify the set of non – interfering transmissions is an area and to coordinate the activities of the various senders. As we discussed above, the notion of non- interfering transmissions depends on the antenna orientations of the senders. Thus, an indoor directional Cross-layer protocol must not only identify the set of possible concurrent transmissions but also determine their orientations. Directional antenna has the potential to provide the necessary interference reduction by spatially confining transmission.

CROSS-LAYER PROTOCOL:

It is repeatedly argued that layered architectures are not suitable for mobile networks. to illustrate this point ,researchers usually present what they call across-layer design proposal .cross-layer design refers to protocol design done by actively exploiting the dependence between protocols gain .this is unlike layering, where the protocols at the different layers are designs independently .Protocols can be designed by respecting the rules of the reference architecture.

In a layer architecture, this would means designing protocols such that a higher-layer protocol only makes use of the services at the sevice is being provide.

Physical cross-layer module:

A key concept at the physical cross-layer is the capacity of survivability region. which characterizes a tradeoff between achievable capacities at different links for survivability.

Consider a network with A, B and C_L as the link gain,power,noise,respectly. Denote D_l as the interference coefficient from link k_1 to the link k_2.assume that each node has a power boudget X_{max}. thus the power control with a physical Cross-layer module interference model may be formulated as

$$\max \sum ¥n$$

¥ is dual variable. ¥ play a key role in coordinating the survivability networking layer demand and layer supply.

n-capacity region at the physical cross-layer

$n=\log (1+SINR)$ for every $k_2 \epsilon$ E

$SINR=AB/\sum AB+C_L$ for every $L \epsilon$ E

Because of interference, the power control problem is a non convex optimization proble that is present physical cross-layer module[9] capacity approximitly.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

CONCLUSION: - In this paper we use the Cross-layer protocol and directional antenna to find out a route optimization and we also present the effect of the Cross-layer protocol for traffic management in Ad Hoc wireless network. And we propose a system of traffic management in Ad Hoc wireless network by use of theory of directional antenna.

Reference :-

[1] M. Kawai, M.Nozaki and K.Gyoda, "A wireless Ad Hoc Community Network with Recongfigurable Topology Architecture", Proc.of the GLOBECOMM'98.1998.

[2]T. Ohira and K.Gyoda , "Electronically Steerable Passive Array Radiator (ESPAR),"Antennas for Law –cost Adaptive Beam Forming", IEEE International Conference on Phased Array System , dana Point , CA May 2000.

[3] P.D.R.Vijakumar, T.Ravichandran "Cross-layer protocol Based Multimedia Transmission usin cache in mobile Ad hoc Networks" international journal andCommunication Technoloy Research Volume2 No,5,May2012.

[4] Fan Bai, N Sadagopan and A Helmy , " IMPROTANT : a Framework to systematically analyze the impact of mobility on performance of Routing Protocol for AdHoc Neworks", IEEE 2003.

[5] S Gowrishanker, T G Basavaraju and Sabir Kumar Sarkar , "Effect of Random Mobility Models Pattern in Mobile Ad Hoc Networks"Vol.7 No.6Junme 2007.

[6] B.S. Abdur Rahaman Crescent Engineering College Vandalur , "Efficient Broadasting In Maneats Using Directional Antennas",Aug, 2000.

[7] Markus Jordan Gerd Ascheid and Heinrich Meyr , "Performance Evaluation of Opportunistic Beamforming with SINR Prediction for HSDPA", NEW Jersy 1993.

[8] C.E. Perkins, E.M Royar & S Das, Ad Hoc On Demand Distance Vector (AODV) Routing , IETF International draft, draft – ietf – manet – aodv -08.txt, March2001.

[9] Rangarajan, H. and Garcia – nLuna –Aceves, JJ. 2005 'Making On-Demand Routing Protocols Based on Destination Sequence Numbers Robust.' 2005 IEEEInternational on Communications (Icc 2005), vol.5 Pp. 3068-3072.

[10] Zhigue Ding and Kin K. Leung "Cross-layer Routing Optimization for Wireless Networks with Cooperative Diversity 978-1-4244-2644-7/08©2008IEEE.Email{zhigue,ding,kin.leung}@imperial.ac.in

AUTHORS PROFILE

Authors Profile ..Anu Chaudhary is the Head of the Department in Inforation of Technoogy & Management, Gzb and completed his PHD from Gurukul Kangari University,Haridwar (India). Prof Anu is basically working in the area of mobile network.

K K Gautam is a Director in the Phonics Group of Institutions, Roorkee (India). Prof Gautam has completed his PhD in Computer Engineering Department. He has a teaching experience of more than 20 years and also has many research paper in the field of network security and currently he is working in the area of mobile network and wireless network.

Nirbhay Ahlawat is the Astt.Prof. in the department of Computer science in Phonics Group of Institutions,Roorkee and completed his M.tech From Subharti University,Meerut (India).He is also a research scholar and presently working in the field of Network Security.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Performance of and Traffic management for a Mobile networks by using Cross-layer protocol

Anu Chaudhary
Department of information Technology
AKJ Institute of Technology and Management, GZB
(INDIA)

K.K Gautam
Department of Computer Science & Technology Phonics Group of Institutions, Roorkee
(INDIA)

Nirbhay Ahlawat
Department of Computer Science & Technology Phonics Group of Institutions, Roorkee
(INDIA)

Abstract:-

Over the Recent years a considerable amount of effort has been devoted towards the traffic management and root is the important capability to provide best network technology in today's world. Present paper we study the traffic management for mobile networks and we addresses current issue of the traffic management. Present the performance of Mobile Network by using Cross-layer protocol.

Index Terms:-

Mobile Networks, call admission control, QoS (Quality of Service).rout optimization

1. Introduction:-

Over the recent years a considerable amount of effort has been devoted towards the performance, evaluation for the traffic management of wireless mobile networks of wireless mobile networks (WMN). A considerable amount of research efforts has been used to characterize user and calling behavior and their performance impact on wireless mobile networks. At present the mobility in most mobile in most mobile networks is confined to the end users only.

With the development of mobile compfor the devolopement of traffic management the call admission schemes are ganarely adopt[1] mobile user authentication is absolutely nessesary as mobile user want to request service provided by the provide survival in the visited traffic management a networks could as simple as of forum held in a city ,state ,country ,whole world between the people . where people communicating with each other[2] .the system may need to block inas a mobile user ression the CAC schemes are generally adopted by setting thresholds for hand off calls and new call differently given the traffic condition and it is the maximum number of users that can be supported. The system may need to block incoming users if all of the entire band width has been used up to provide the highest QoS to existing users. However if these existing users can be degraded to a lower but acceptable QoS level, it is possible to reduce the blocking probability without degrading the QoS of existing users. A graceful degradation mechanism is proposed in [3]. Thus a system could free some bandwidth allocation for new users. In this paper we address current issues in traffic management for cellular mobile networks. In traffic management coming user that can be supported .the system may need to block incoming user and congestion control, courcoubetis and series device new procedures and tools for the analysis of network traffic measurement.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

2. MODEL DESCRIPTION:-

We consider uplink communication in a wireless mobile networks. As an accepted call does not always send data frames. Then for best traffic we consider the activity factor ℓ as the probability that a call is active. We represent QoS requirement of traffic by required transmission rate. The required transmission rate can be obtained by setting the target level.

Often these intra – and inter –traffic interferences of call can be large so that the target bit error rate of traffic interferences(BERIT) can not be achieved temporarily, which is called outage. The outage probability needs to approach zero as close as possible and can be different for each class. Here we assume for traffic management the allowed outage probability is the same.

3. OUTAGE PROBABILITY FOR TRAFFIC:-

In a mobile network a traffic management the supports a single class of calls, the outage probability is given by [2].

$$Pout = Pr\{N^a + M^a > (3/2)\, G(x^{-1} - (Yb/N_0)^{1})^{+1}\} \ldots\ldots (1)$$

When N^a, M^a, G, X, Y^b, and N_0 represent the number of active calls in the current call, similarly in a network that support L-Class of calls, we obtain

$$P^j out = Pr\left\{\sum_{i=1}^{L} (Ybi / Ybj)\, Ci\, (Ni^a + Mi^a) \geq Aj\right\}$$

$$= Pr\left\{\sum_{i=1}^{L} \theta I\, (Ni^a + Mi^a) \geq \eta j\right\} \ldots\ldots\ldots (2)$$

When i, j represent traffic call classes (TCC), Ci is the number of orthogonal codes needs for a TCC, 'i'. By the Gaussian random variable from the limit theorem and we can write control the outage probability of a TCC' 'j'. As

$$P^j out = Q(\eta j - \lambda / \partial\lambda) \ldots\ldots\ldots (3)$$

Where $Q(\xi) = 1/\sqrt{2\pi} \int_{\xi}^{\infty} e^{-x^2/2}\, dx$

And represent the total traffic receive single power (TRSP) i.e. $\sum_{i=1}^{L} \theta I\, (Ni^a + Mi^a)$

Therefore $\overline{\lambda} = (1+f1) \sum_{i=1}^{L} \theta I\, \overline{N}^a i, \ldots\ldots (4)$

And $\partial^2 \lambda = \sum_{i=1}^{L} \theta^2 I\, (\partial i^2 + f2\, \overline{N}^a i)$

Where $\overline{N}^a i$ and $\partial^2 I$ indicate the mean and variance of $N^a I$.

According to the assumption of TCC equal outage probability for each class we can $\eta I = \eta j$ for all I and j. there for TCC received single power meets the following relation.

$$\theta I / \theta j = CiXi\,(3G - 2CjXj) \Big/ CjXj(3G + 2CiXj) \ldots\ldots (6)$$

This indicates that the power allocation refers the target of TCC outage probability.

Call Admission Control (CAC):

System Model:-

The Communication system under consideration can be defined as

$$r[k] = \sum_{i=0}^{L} h[l] \& [k-l] + z[k] \ldots\ldots\ldots (7)$$

Where r [k] received call sequence

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

h [l] unknown channel for traffic with memory L', z [k] is an independent and identically distributed Gaussian notice sequence.

Then traffic management symbol sequence s [k] is drawn from M-ary alphabet, A with equal probability, the vector version of (1) can be written as

$$\begin{bmatrix} r[k] \\ : \\ : \\ r[1] \\ r[0] \end{bmatrix} = \begin{bmatrix} S[K-L] & ... & S[K] \\ : & ... & : \\ : & ... & : \\ S[1-L] & ... & S[1] \\ S[-L] & ... & S[0] \end{bmatrix} \begin{bmatrix} h[l] \\ : \\ : \\ h[1] \\ h[0] \end{bmatrix} + \begin{bmatrix} z[k] \\ : \\ : \\ z[1] \\ z[0] \end{bmatrix}$$

Where S_k is toeplitz data matrix.

Call Admission Control for Traffic Management:-

For call Admission Control for traffic Management [CACTM] the outage Probability is very small defined as $\frac{\partial Q(\eta)}{\partial \eta} < 0$ we can show that $\frac{\partial P_{out}}{\partial N_i} = \alpha_i \frac{\partial P_{out}}{\partial \overline{N_i}} > 0$ where α_i is the active factor for (CACTM) a class I call. It is clear that the average rate for mobile network [ARRMN] and outage probability increase with the number of users. Call admission control is a mechanism used in networks to administer quality of service (QoS). Whereas the CAC problem in time division multiple access (TDMA) based cellular networks is simply resalable to the number of physical channels available in the network, it is strongly related to the physical layer performance in WCDMA networks since the multi-access interference in them is a function of the number of users and is a limiting factor in ensuring QoS. The CAC mechanism will thus rely on the "Soft Capacity" of the W- CDMA networks as determined by the level of multi-access interference, often characterized by the signal to interference ratio. In such systems the CAC design leads to a significant interaction between the physical and medium access control layers.

Any given networks have a finite resource that is the number of node, links and buffers and the bandwidth are finite. Thus there are maximum numbers of packets that can be in a network at any given time. Although there is consideration related to the economics of network that favors operating at or close to full capacity there are other considerations

Related to QoS that provide impacts to operating at less then full capacity.

The higher the packet traffic in a network or part of a network, the greater the average delay per packet due to the limited resources. i.e. if there are more packets the Qos is lowered. Thus in order to maintain QoS the number if calls is to be limited. Rejection if calls create a perception in customer mind regarding provides inability. End to end all problem faced by the network is one od the measuring and forecasting QoS, maximizing call blocking probability and maximizing throughput while maintaining QoS.

The typical parameters that must be managed are latency, filter, bandwidth and packet loss rare [1], [2]. Packet loss is mainly due to buffer overflow packet corruption can occur, this is erroneous reception of nits due to

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

physical layer impairments. A highly loaded network affords less loss of overloaded of overcrowded buffers. Light loading can also reduce end to end delay and in wireless network based on W-CDMA protocols, lower packet corruption caused by interference. QoS proves coming refers to network capability to different classes of traffic to implement QoS proves coming, a desired QoS is negotiated between the customer and the network on each call and the network QoS parameters are set accordingly.

Physical layer issue are an essential components of QoS management in wireless network, especially with mobile with platforms as varying channels condition and number of users directly affect reliability of communication. Thus QoS schemes must potentially integrate functions at the physical and medium access control (MAC) layers.

CAC has emerged as one key component of such schemes [3].

Numerical Result:-

We now compare the performance of the consider two CACs through numerical analysis. The system bandwidth is 2.50(MHz) and each code can carry information bits at the rate of 19.2(kbps) so that the processing gain is 256. Two types of calls are considered to manifest the effect of traffic parameters on performance. Class 1 and 2 calls are voice traffic and we set their transmission rates after channel coding at 19.29(kbps). They have different Mobile Network Average Revenue Rate (MNARR) for the traffic management requirement of less than 10^{-4} and 10^{-6}, respectively, and their activity factors are set at 1.0. The coefficient for intercall interference modeling are chosen as f1 = 0.114 and f2 = 0.44[12].

CONCLUSION:

In this paper, we consider Call Admission Control for Traffic Management [CACTM] in Mobile Networks. Through the mathematical analysis and also present outage probability and a system model's for CAC and we also present an example for Call Admission Control for Traffic Management [CACTM].

REFERENCES:

[1] J. Zhang , J. W. Mark, and S.Xuemin, "An adaptive handoff priority scheme for wireless MC-CDMA cellular networks supporting multimedia application ," in Proc. IEEE Globecom, Nov/Dec. 2004, pp. 3088-3092.

[2] Z. Liu and M. E. Zarki, "SIR – based call admission control for DSCDMA cellular system," IEEE J. Select. Areas Commun, vol . 12, pp.638-644, May 1994.

[3] R. j. Boucherie and Nico M. Van Dijk, "On a queueing network model cellular mobile telecommunications networks, "Operations Research, vol 48, no, pp. 38—49, 2000.

[4] X.Chao and W. Li, "Performance analysis of a cellular network with multiple classes of calls," IEEE Trans. Coomun, vol. 53, no. 9, pp. 1542-1550,2005.

[5] C. T. Chou and K.G. Shin, " Analysis of adaptive bandwidth allocation in wireless networks with multilevel degradable quality of service," IEEE Trans. Mobile Compute, vol. 3 no. 1, pp. 5-17, 2004.

[6] Maruf Mohammad , William Tranter " Blind Acquisition of short Burst with Per – Survivor Processing" IEEE TRANSCATION ON WIRELESS COMMUNICATION, vol. 6. No. 2. February 2007.

[7] Wei Li , and Xiulichao " Call admission Control for an adaptive Heterogeneous Multimedia Mobile Network" IEEE TRANSCATION ON WIRELESS

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

COMMUNICATION, vol. 6. no. 2. February 2007. page no. 515-525.

[8]Jin-Cho Choi, Yound-June Choi, and Saewoong Bank "power – Based Admission Control for Multi Class Calls in QoS –Sensitive CDMA NETWORKS" IEEE TRANSCATIONS ON Wireless communication, vol, 6 no. 2 February 2007 page no. 469-472.

[9]P.D.R.Vijayakumar, T.Ravichandran, "Cross Layer Based MultimediaTransmission usin Cache in Mobile Ad hoc Networks"volume2 No.5,May2012,International Journal of Information and Communication Technology Research,ISSN2223-4985.

[10] Zhigue Ding and Kin K. Leung "Cross-layer Routing Optimization for Wireless Networks with Cooperative Diversity 978-1-4244-2644-7/08©2008IEEE.Email{zhigue,ding,kin.leung}@imperial.ac.in

[11]Alexandra Giagkos and Myra S.Wilson"A Cross-layer Design for Bee-Inspired Routing Protocols in MANETs" Aag07@aber.ac.uk , mxw@aber.ac.uk, Dept.-of Computer Science,Aberystwyth University

AUTHORS PROFILE

Authors Profile ..Anu Chaudhary is the Head of the Department in Inforation of Technoogy & Management, Gzb and completed his PHD from Gurukul Kangari University,Haridwar (India). Prof Anu is basically working in the area of mobile network.

K K Gautam is a Director in the Phonics Group of Institutions, Roorkee (India). Prof Gautam has completed his PhD in Computer Engineering Department. He has a teaching experience of more than 20 years and also has many research paper in the field of network security and currently he is working in the area of mobile network and wireless network.

Nirbhay Ahlawat is the Astt.Prof. in the department of Computer science in Phonics Group of Institutions,Roorkee and completed his M.tech From Subharti University,Meerut (India).He is also a research scholar and presently working in the field of Network Security.

Security.

A Fast Survey Focused on Methods for Classifying Anonymity Requirements

Morteza Yousefi Kharaji
Department of Computer Science and Information Technology
Mazandaran University of Science and Technology
Mazanadan, Iran
Yousefi@ustmb.ac.ir

Fatemeh Salehi Rizi
Department of Computer Science and Information Technology
Sheikh Bahaei University of Isfahan
Isfahan, Iran
Salehi.Fatemeh@shbu.ac.ir

***Abstract*—Anonymity has become a significant issue in security field by recent advances in information technology and internet. The main objective of anonymity is hiding and concealing entities' privacy inside a system. Many methods and protocols have been proposed with different anonymity services to provide anonymity requirements in various fields until now. Each anonymity method or protocol is developed using particular approach. In this paper, first, accurate and perfect definitions of privacy and anonymity are presented then most important problems in anonymity field are investigated. Afterwards, the numbers of main anonymity protocols are described with necessary details. Finally, all findings are concluded and some more future perspectives are discussed.**

Keywords-anonymity; privacy; online security

I. INTRODUCTION

Utilization of computer networks has been raised in recent years especially internet has become the most famous computer network in all over the world. While we are sending email or talking to our family members through internet, a lot of data or information packets are sent through internet. These packets consist of information of sender and receiver and etc. Since the packets are transmitted by several hops, everybody can monitor them and access to various information such as who started the contact and with whom and some other useful information. Although it is possible to conceal packet contents from a viewer by cryptography, the information of IP header is still accessible for a viewer. For this reason, in two past decades, some improvements have been emerged about anonymity and preserving privacy in formal and public communication field. So far, several systems have been designed and such systems are using by military groups, journalist and public sections. These systems are used to hide identities in virtual internet world .Today, there are various applications which need some methods to provide anonymity for performing their particular tasks. Some examples of these applications could be electronic voting, electronic commerce and etc.[1] Anonymity can be a branch of preserving privacy but preserving privacy is a concept wider than keeping anonymity of entities. Anonymous communication give a possibility to have contacts without disclosing their identities and it does not contain all aspects of privacy. Indeed, anonymity try to conceal operation agents' information while preserving privacy also hides whatever they perform [1].

Ignoring anonymity aspects causes to jeopardize people privacy. Hence, anonymity is one the most important issues in information security and preserving people privacy. So many applications need anonymity practically. In [3, 4, 5] these applications were categorized as follows:

- Searching information anonymously
- Maintain communication patterns to prevent traffic analysis
- Providing freedom of speech in fanatic environments
- Electronic voting
- Anonymous using of location based services
- Electronic payments
- Electronic cash
- Anonymous web browsing
- Anonymous e-mail
- Anonymous publishing

Anonymity attributes and also the level of anonymity are different in various applications. Therefore, analyzing of anonymity requirements which are used for determining accurate anonymity features in a service are very important and they must be done with high accuracy. For instance, applying a complete level of anonymity is not mostly a best

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

choice because it causes some problems in many systems. There is no ability to follow and pursue entities in a complete anonymous system while the capability of imputing operations and attacks to people or entities in the system gives a possibility to hamper people's wrongdoings [2]. Consequently, anonymity must be applied with respect to the organization completely or under some particular conditions.

II. PRESERVING PRIVACY, ANONYMITY

Information is a lifeline in the most institutes, developed organizations and scientific communities. In the institutes and organizations in which information is really important, a quick and proper way is necessary to access to information. Organization and institutes should create informatics infrastructure and try to organize their information. One of success keys in institute, organizations and scientific communities in information age is speeding to generate and offer worthwhile information. After organizing information, it is necessary to provide regular and correct use of this information for others. Along with moving to developed organization based on information technology, it is essential to plan some other methods for preserving information.

Information security points to preserve information and minimize information revealing risks in unauthorized parts. Information security is a set of tools for preventing thefts, attacks, crimes, espionage and sabotages and etc. it is a science for studying various approaches to preserve data in computers and communication systems against access to unauthorized changes. Preserving privacy could be a subcategory of information security. Privacy means such a person can separate his/her information and disclose them on others view by his/her choice. Everyone has some private information which wants to keep them from others.

III. ANONYMITY ISSUES

Today, providing anonymity approaches are considered specially preserving entities' privacy in electronic commerce and electronic voting and etc. As it is mentioned before, content of messages could be protected by cryptography methods but message rout, source and destination of message, sending time, message length and some kind of information would still remain. Sometimes, valuable information can be accessible only by observing people communication pattern. Access to entities' information in a communication would be a violation of their privacy and anonymity can prevent revealing of this kind of information. Accordingly, anonymity can be a branch of information security [1].

Nowadays, there are a lot of applications that need anonymity and each application requires special anonymity attributes. For example imagine an electronic payment system that users can search their items and select and buy them. Most customers do not like to show their identity and their private information like interests and preferences. Thus, besides concealing users' identity connection between users' different operations must be hided. However, customers' anonymity should be applied in a limited way to preserve authority of trades correctly. It means that in electronic payment system, anonymity must be applied a different way. When an entity makes a wrongdoing, it would be possible to remove its anonymity and expose its real identity. As a matter of fact, the ability of imputing responsibility of operation to people gives a possibility to hinder crime activities in system by ordaining some rules and politics [2].

On the contrary, suppose an online medical consultation such that gives consultation to patients by hiding patients' identities. Since patients' backgrounds have very serious role in correct consultation, hiding information can damages system operation. Consequently, unlike electronic payment covering users' background might destroy accuracy of disease detection in a medical system.

Several protocols were proposed to provide anonymity in applications until now. It is necessary to have an organized method for developing software security because existence of this kind of method gives a capability to users for analyzing and describing application requirements. Therefore, it can reduce complexity of software analyzing and designing. Furthermore, it can save cost and time because it can recognize and move system problems in initial phase of software development.

VI. ANONYMITY PROTOCOLS

Anonymous communication means the communication layer must not reveal potentially identifiable information such as the user's IP address or location. This can be met by so-called anonymity protocols such as mix networks [6], onion-routing systems [7].

A. Mix-Net Protocol

The Mix-Net protocol is the base for some other anonymity protocols, Web Mixes [8], ISDN-Mixes [9], and Stop-and-Go-Mixes [10], to name a few. This protocol uses some nodes, called Mix, between sender and receiver. Mixes act as mediators for sending messages and provide the anonymity of the sender against the receiver. Moreover, Mixes are used for hiding a connection against attacks. Figure1 shows this protocol.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

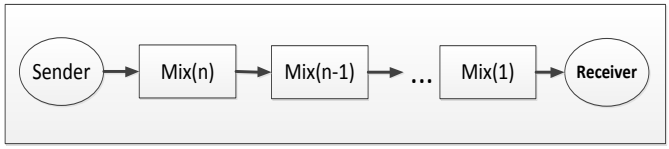


Figure 1: Mix-Net Protocol [11]

In the first step of executing the protocol, the sender defines a sequence of mixes. This can be accidentally or contractually. In this case it supposed the defined sequence is static. Then the sender encodes its message (M) by using the general key (Ki) of mixes. The sender adds the receivers address (AR) to the encoded message of last mix. The form of message is shown below:

Kn(Rn,(Kn-1(Rn-1, … , K2(R2, K1(R1, Ka(R0, M), AR))…)

In message form, there is a random number (Ri) besides of each encoded part. Therefore, before encoding the sender adds a set of random bits besides each part and this prevents the data from dictionary attack.

The important point in mix-net protocol is that even if one mix stay safe against traffic analyzing attack, the connection between sender and receiver will stay safe, because there is no relationship between the input and output of each mix [12, 13, 14].

B. Onion Routing Protocol

In the Onion-Routing protocol, the sender and receiver can identify each other. The basic goal of this protocol is to make an anonymous connection from others' viewpoint, and to prevent network traffic analysis. This protocol uses a group of computers named Onion Routers. When a user has a request for sending a message, first the user considers a sequence of Onion Routers, then, makes a data for each router and uses layer encoding with general key encoding to preserve every router's data from other routers [15].

Each node peels a layer of onion, and this means the node decodes the information with its own private key that is related to itself and sends the result to next routers. After finishing this process of peeling a rout of onion routers is created between sender and receiver that can have an anonymous connection. According to this explanation the onion routing protocol creates a two-sided real-time connection between sender and receiver.

V. PREVIOUSE WORKS ON CLASSIFICATION ANONYMITY REQUIREMENTS

These days, anonymity and preserving privacy are becoming very important issues in the digital world [5]. As a matter of fact, the requirements and the level of anonymity for different applications are different, and in many of the applications anonymity should be applied in a controlled and conditional manner. The concept of conditional privacy preservation has been widely studied in vehicular communications especially in VANETs [16]. The works in [17-20] are number of proposed methods to achieve conditional privacy.

Naessens et al. in [21, 22] introduced a methodology for designing controlled anonymity systems. This methodology defines four categories of requirements: Anonymity requirements, controlled requirements, applicability requirements and trust requirements. In their methodology, anonymity requirements come in a graph like "Unlinkable(X, Y)" which is called Linkability graph. In this system X and Y can be any kinds of operations or features. This graph shows for doing any operations what features needed to be accessed and what privileges will be required. Moreover, the proposed methodology uses Petri-Nets to represent the sequence of operations in a system. For each operation, it defines what kind of privileges will be required, when the operation will be finished, and what kind of privileges we will gain. The most important issue regarding this methodology is that it is not possible to consider all anonymity requirements from all aspects and put them into Unlinkable forms. Moreover, in this methodology there is no approach for detecting entities that might try to break the system rules.

Kavaki et al. in [23] proposed a methodology named Pris for considering privacy requirements in software development process. It is a Goal-Oriented methodology and defines the requirements as goals. The conceptual model that is used in Pris comes from Enterprise Knowledge Development framework that is shown in Figure 2. In this methodology, to reach the goals, they are divided into sub-goals until it is possible to reach each goal with a process. There exist several issues about this methodology; it divides all requirements (goals) into two categories: organizational goals and privacy goals which are too general. There are many applications with anonymity requirements, and these requirements are very different in each application; hence, sometimes considering the requirements in the form of such goals is not possible.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

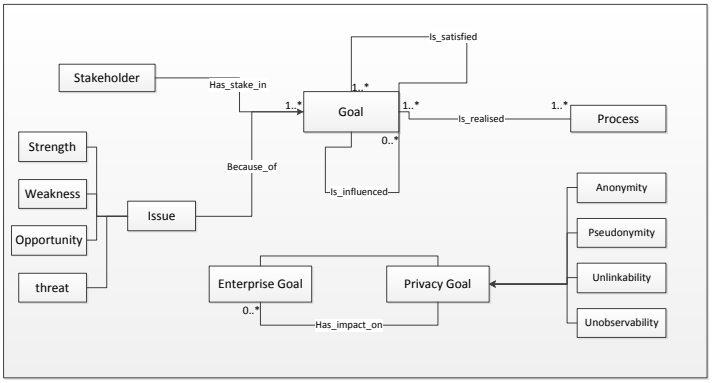


Figure2: PriS conceptual model [23]

As well as, Gürses et al in [24] proposed a methodology named CREE for Confidentiality Requirements Elicitation and Engineering which is applied to a real world project in the health care area. However, this work as stated by the authors is a primary effort and is also limited to the confidentiality and do not cover the anonymity concerns.

De Win et al. in [5] proposed a categorization for anonymity. In this categorization, they explained three features of anonymity such as traceability, linkability, and identifiability. They also proposed some combination of these features for any application that needs to be anonymous. For example if an entity is not traceable, linkable and identifiable, this entity is not anonymous, but if this entity is untraceable, unlinkable, and unidentifiable, it has the complete level of anonymity. In this approach the different combinations of these features make different levels of anonymity. Although this categorization is better than other works in this area but, this categorization is not complete enough, because they just consider some features of entities which mostly are related to the messages of entities or the connection between those entities. However, in this categorization they do not consider the features of entity itself which is selected to be anonymous.

TABLE I: DIFFERENT KINDS OF ANONYMITY [10]

Traceability	**Linkability**	**Identifiability**	**Anonymity**
√	√	√	0(no Anonymity)
×	√	√	1
√	×	√	2
×	×	√	3
√	√	×	4
×	√	×	5
√	×	×	6
×	×	×	7

Spikerman and Cranor in [25] tried to offer a holistic view of privacy engineering and a systematic structure for the discipline's topics. They have used a three-layer model of user privacy concerns to relate them to system operations (i.e. data transfer, storage, and processing) and examine their effects on user behavior. Furthermore, they have developed guidelines for building privacy-friendly systems. An interesting result of [25] is that they have shown the degree of privacy friendliness of a system is inversely related to the degree of user data identifiability. However the levels of identifiability in [25] is limited to three levels: identified, pseudonymous, and anonymous.

VI. CONCLUSION

We live in electronic society and thus many of us read online news, manage online back account, buy online and chat with friends every day. Since we spend a lot of our daily time on the internet, anonymity treats are rising extremely. Storage memories are inexpensive; hence, the information of our activities can be saved and marinated with very low cost. Fortunately, a lot of efforts have been performed to preserve users' privacy and to anonymize users' communications in cyberspace up to now. The numbers of these existence anonymity protocols and methods with different approaches were studied in this paper. An accurate Knowledge of anonymity requirements in the system could be helpful to develop more secure and utilizable software and to have more safe online communication in the future.

REFRENCES

[1] M. Edman and B. Yener, " On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems", ACM Computing Surveys, Vol. 42, No. 1, Article 5, December 2009.

[2] SEI: Software Engineering Institute, "Results of SEI Independent Research and Development Projects and Report On Emerging Technologies and Technology Trends", October 2004.

[3] M. Ispareh, B. Tork Ladani, S. Shariat Panahi,and Z. Nasr Azadani, "Toward a Software Development Methodology for Anonymity Application", EDBT '10 Proceedings of the 2010 EDBT/ICDT Workshops, Lausanne, Switzerland, March 2010.

[4] Q. Zhang, "A Fair and Anonymous E-Commerce Schema", PhD thesis, university of London, may 2007.

[5] B. De Win , V. Naessens , C. Diaz , S. Seys , C. Goemans , J. Claessens , B. De Decker , J. Dumortier , and B. Preneel, "Anonymity and Privacy in Electronic Services", APES Project, Deliverable 2 – Requirement study of different applications, 2001.

[6] D. Chaum, "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms", communications of the ACM, February1981.

[7] O. Berthold, A. Pfitzmann, and R. Standtke, "The Disadvantages of Free MIX Routes and How to overcome them", *Workshop on design Issues in Anonymity and Unobservability*, July 2000.

[8] O. Berthold, H. Federrath, and S. Kopsell, "Web MIXes: A System for Anonymous asn Unobservable Internet Access", *Proceeding International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability*, USA, 2001.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[9] A. Pfitzmann, B. Pfitzmann, and M. Waidner, "ISDN-MIXes: Untraceable Communication with Very Small Bandwidth Overhead", In *GI/ITG Conference: Communication in Distributed Systems*, February 1991.

[10] D. Kesdogan, J. Egner, and R. Buschkes, "Stop-and-go-Mixes Providing Probabilistic in an Open System", In *Information Hiding*, April 1998.

[11] D. Chaum, "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms", communications of the ACM, February1981.

[12] G. Danezis, "Better Anonymous Communications", PhD thesis, University Of Cambridge, 2004.

[13] DIAZ, C., "Anonymous and Privacy in Electronic Services", PhD Thesis, Katholieke University, 2005.

[14] M. Freedman, " Design and Analysis of an Anonymous Communication Channel for the Free Haven Project", BS thesis, MIT, 2000.

[15] B. Bauer, "Extending UML for the Specification of Interaction Protocols", *submission for the 6th Call for Proposal of FIPA and revised version part of FIPA 99*, 1999.

[16] S. Moses, P. Angelin, "A Comparative Study of Conditional Privacy Preservation Approaches in VANET'S" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). Volume 1, Issue 9, November 2012.

[17] X. Zhou; P. Wei, "Proxy Authorization Signature with Conditional Anonymity and Its Application," Knowledge Acquisition and Modeling, 2008. KAM '08. International Symposium on , vol., no., pp.799-803, 21-22 Dec. 2008.

[18] R. Lu; X. Lin; H. Zhu; P. Ho; X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," INFOCOM 2008. The 27th Conference on Computer Communications. IEEE , vol., no., pp.1229,1237, 13-18 April 2008.

[19] C. Jung, C. Sur, Y. Park, and K. Rhee, "A Robust Conditional Privacy Preserving Authentication Protocol in VANET," in Proc. MobiSec 2009, Turin, Italy, June 2009.

[20] Y.Sun, R. Lu, X. Lin, X. Shen, J. Su, "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications," Vehicular Technology, IEEE Transactions on , vol.59, no.7, pp.3589,3603, Sept. 2010.

[21] V. Naessens, "A Methodology for Anonymity Control in Electronic Services Using Credentials", PhD thesis, Katholieke Universiteit Leuven, June 2006.

[22] V. Naessens and B. De Decker, "A Methodology for Designing Controlled Anonymous Applications", *In Proceedings of the 21th IFIP International Information Security Conference: Security and Privacy in Dynamic Environments*, May 2006

[23] E. Kavakli and C. Kalloniatis, "Incorporating Privacy Requirements into the System Design Process: The Pris Cnoceptual Framework", Internet Research Vol. 16 No. 2, pp. 140-158, 2006.

[24] S. Brands, "Rethinking public key infrastructure and digital certificates – building in privacy", PhD thesis, Technical University Eindhoven, 1999.

[25] S. Spiekermann and L. F. Cranor, "Engineering Privacy", IEEE Trans. Softw. Eng., Vol. 35, No. 1, Jan 2009. pp. 67-82.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IJCSIS AUTHORS' & REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

Prof. Ning Xu, Wuhan University of Technology, China
Mr Mohammed Salem Binwahlan, Hadhramout University of Science and Technology, Yemen
& Universiti Teknologi Malaysia, Malaysia.
Dr. Aruna Ranganath, Bhoj Reddy Engineering College for Women, India
Mr. Hafeezullah Amin, Institute of Information Technology, KUST, Kohat, Pakistan
Prof. Syed S. Rizvi, University of Bridgeport, USA
Mr. Shahbaz Pervez Chattha, University of Engineering and Technology Taxila, Pakistan
Dr. Shishir Kumar, Jaypee University of Information Technology, Wakanaghat (HP), India
Mr. Shahid Mumtaz, Portugal Telecommunication, Instituto de Telecomunicações (IT) , Aveiro, Portugal
Mr. Rajesh K Shukla, Corporate Institute of Science & Technology Bhopal M P
Dr. Poonam Garg, Institute of Management Technology, India
Mr. S. Mehta, Inha University, Korea
Mr. Dilip Kumar S.M, University Visvesvaraya College of Engineering (UVCE), Bangalore University, Bangalore
Prof. Malik Sikander Hayat Khiyal, Fatima Jinnah Women University, Rawalpindi, Pakistan
Dr. Virendra Gomase , Department of Bioinformatics, Padmashree Dr. D.Y. Patil University
Dr. Irraivan Elamvazuthi, University Technology PETRONAS, Malaysia
Mr. Saqib Saeed, University of Siegen, Germany
Mr. Pavan Kumar Gorakavi, IPMA-USA [YC]
Dr. Ahmed Nabih Zaki Rashed, Menoufia University, Egypt
Prof. Shishir K. Shandilya, Rukmani Devi Institute of Science & Technology, India
Mrs.J.Komala Lakshmi, SNR Sons College, Computer Science, India
Mr. Muhammad Sohail, KUST, Pakistan
Dr. Manjaiah D.H, Mangalore University, India
Dr. S Santhosh Baboo, D.G.Vaishnav College, Chennai, India
Prof. Dr. Mokhtar Beldjehem, Sainte-Anne University, Halifax, NS, Canada
Dr. Deepak Laxmi Narasimha, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
Prof. Dr. Arunkumar Thangavelu, Vellore Institute Of Technology, India
Mr. M. Azath, Anna University, India
Mr. Md. Rabiul Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh
Mr. Aos Alaa Zaidan Ansaef, Multimedia University, Malaysia
Dr Suresh Jain, Professor (on leave), Institute of Engineering & Technology, Devi Ahilya University, Indore (MP) India,
Dr. Mohammed M. Kadhum, Universiti Utara Malaysia
Mr. Hanumanthappa. J. University of Mysore, India
Mr. Syed Ishtiaque Ahmed, Bangladesh University of Engineering and Technology (BUET)
Mr Akinola Solomon Olalekan, University of Ibadan, Ibadan, Nigeria
Mr. Santosh K. Pandey, Department of Information Technology, The Institute of Chartered Accountants of India
Dr. P. Vasant, Power Control Optimization, Malaysia
Dr. Petr Ivankov, Automatika - S, Russian Federation

Dr. Utkarsh Seetha, Data Infosys Limited, India
Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal
Dr. (Mrs) Padmavathi Ganapathi, Avinashilingam University for Women, Coimbatore
Assist. Prof. A. Neela madheswari, Anna university, India
Prof. Ganesan Ramachandra Rao, PSG College of Arts and Science, India
Mr. Kamanashis Biswas, Daffodil International University, Bangladesh
Dr. Atul Gonsai, Saurashtra University, Gujarat, India
Mr. Angkoon Phinyomark, Prince of Songkla University, Thailand
Mrs. G. Nalini Priya, Anna University, Chennai
Dr. P. Subashini, Avinashilingam University for Women, India
Assoc. Prof. Vijay Kumar Chakka, Dhirubhai Ambani IICT, Gandhinagar ,Gujarat
Mr Jitendra Agrawal, : Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal
Mr. Vishal Goyal, Department of Computer Science, Punjabi University, India
Dr. R. Baskaran, Department of Computer Science and Engineering, Anna University, Chennai
Assist. Prof, Kanwalvir Singh Dhindsa, B.B.S.B.Engg.College, Fatehgarh Sahib (Punjab), India
Dr. Jamal Ahmad Dargham, School of Engineering and Information Technology, Universiti Malaysia Sabah
Mr. Nitin Bhatia, DAV College, India
Dr. Dhavachelvan Ponnurangam, Pondicherry Central University, India
Dr. Mohd Faizal Abdollah, University of Technical Malaysia, Malaysia
Assist. Prof. Sonal Chawla, Panjab University, India
Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India
Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia
Mr. Md. Rajibul Islam, Ibnu Sina Institute, University Technology Malaysia
Professor Dr. Sabu M. Thampi, .B.S Institute of Technology for Women, Kerala University, India
Mr. Noor Muhammed Nayeem, Université Lumière Lyon 2, 69007 Lyon, France
Dr. Himanshu Aggarwal, Department of Computer Engineering, Punjabi University, India
Prof R. Naidoo, Dept of Mathematics/Center for Advanced Computer Modelling, Durban University of Technology, Durban,South Africa
Prof. Mydhili K Nair, M S Ramaiah Institute of Technology(M.S.R.I.T), Affliliated to Visweswaraiah Technological University, Bangalore, India
M. Prabu, Adhiyamaan College of Engineering/Anna University, India
Mr. Swakkhar Shatabda, Department of Computer Science and Engineering, United International University, Bangladesh
Dr. Abdur Rashid Khan, ICIT, Gomal University, Dera Ismail Khan, Pakistan
Mr. H. Abdul Shabeer, I-Nautix Technologies,Chennai, India
Dr. M. Aramudhan, Perunthalaivar Kamarajar Institute of Engineering and Technology, India
Dr. M. P. Thapliyal, Department of Computer Science, HNB Garhwal University (Central University), India
Dr. Shahaboddin Shamshirband, Islamic Azad University, Iran
Mr. Zeashan Hameed Khan, : Université de Grenoble, France
Prof. Anil K Ahlawat, Ajay Kumar Garg Engineering College, Ghaziabad, UP Technical University, Lucknow
Mr. Longe Olumide Babatope, University Of Ibadan, Nigeria
Associate Prof. Raman Maini, University College of Engineering, Punjabi University, India

Dr. Maslin Masrom, University Technology Malaysia, Malaysia
Sudipta Chattopadhyay, Jadavpur University, Kolkata, India
Dr. Dang Tuan NGUYEN, University of Information Technology, Vietnam National University - Ho Chi Minh City
Dr. Mary Lourde R., BITS-PILANI Dubai , UAE
Dr. Abdul Aziz, University of Central Punjab, Pakistan
Mr. Karan Singh, Gautam Budtha University, India
Mr. Avinash Pokhriyal, Uttar Pradesh Technical University, Lucknow, India
Associate Prof Dr Zuraini Ismail, University Technology Malaysia, Malaysia
Assistant Prof. Yasser M. Alginahi, College of Computer Science and Engineering, Taibah University, Madinah Munawwarrah, KSA
Mr. Dakshina Ranjan Kisku, West Bengal University of Technology, India
Mr. Raman Kumar, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India
Associate Prof. Samir B. Patel, Institute of Technology, Nirma University, India
Dr. M.Munir Ahamed Rabbani, B. S. Abdur Rahman University, India
Asst. Prof. Koushik Majumder, West Bengal University of Technology, India
Dr. Alex Pappachen James, Queensland Micro-nanotechnology center, Griffith University, Australia
Assistant Prof. S. Hariharan, B.S. Abdur Rahman University, India
Asst Prof. Jasmine. K. S, R.V.College of Engineering, India
Mr Naushad Ali Mamode Khan, Ministry of Education and Human Resources, Mauritius
Prof. Mahesh Goyani, G H Patel Collge of Engg. & Tech, V.V.N, Anand, Gujarat, India
Dr. Mana Mohammed, University of Tlemcen, Algeria
Prof. Jatinder Singh, Universal Institutiion of Engg. & Tech. CHD, India
Mrs. M. Anandhavalli Gauthaman, Sikkim Manipal Institute of Technology, Majitar, East Sikkim
Dr. Bin Guo, Institute Telecom SudParis, France
Mrs. Maleika Mehr Nigar Mohamed Heenaye-Mamode Khan, University of Mauritius
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Mr. V. Bala Dhandayuthapani, Mekelle University, Ethiopia
Dr. Irfan Syamsuddin, State Polytechnic of Ujung Pandang, Indonesia
Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius
Mr. Ravi Chandiran, Zagro Singapore Pte Ltd. Singapore
Mr. Milindkumar V. Sarode, Jawaharlal Darda Institute of Engineering and Technology, India
Dr. Shamimul Qamar, KSJ Institute of Engineering & Technology, India
Dr. C. Arun, Anna University, India
Assist. Prof. M.N.Birje, Basaveshwar Engineering College, India
Prof. Hamid Reza Naji, Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran
Assist. Prof. Debasis Giri, Department of Computer Science and Engineering, Haldia Institute of Technology
Subhabrata Barman, Haldia Institute of Technology, West Bengal
Mr. M. I. Lali, COMSATS Institute of Information Technology, Islamabad, Pakistan
Dr. Feroz Khan, Central Institute of Medicinal and Aromatic Plants, Lucknow, India
Mr. R. Nagendran, Institute of Technology, Coimbatore, Tamilnadu, India
Mr. Amnach Khawne, King Mongkut’s Institute of Technology Ladkrabang, Ladkrabang, Bangkok, Thailand

Dr. P. Chakrabarti, Sir Padampat Singhania University, Udaipur, India
Mr. Nafiz Imtiaz Bin Hamid, Islamic University of Technology (IUT), Bangladesh.
Shahab-A. Shamshirband, Islamic Azad University, Chalous, Iran
Prof. B. Priestly Shan, Anna Univeristy, Tamilnadu, India
Venkatramreddy Velma, Dept. of Bioinformatics, University of Mississippi Medical Center, Jackson MS USA
Akshi Kumar, Dept. of Computer Engineering, Delhi Technological University, India
Dr. Umesh Kumar Singh, Vikram University, Ujjain, India
Mr. Serguei A. Mokhov, Concordia University, Canada
Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia
Dr. Awadhesh Kumar Sharma, Madan Mohan Malviya Engineering College, India
Mr. Syed R. Rizvi, Analytical Services & Materials, Inc., USA
Dr. S. Karthik, SNS Collegeof Technology, India
Mr. Syed Qasim Bukhari, CIMET (Universidad de Granada), Spain
Mr. A.D.Potgantwar, Pune University, India
Dr. Himanshu Aggarwal, Punjabi University, India
Mr. Rajesh Ramachandran, Naipunya Institute of Management and Information Technology, India
Dr. K.L. Shunmuganathan, R.M.K Engg College , Kavaraipettai ,Chennai
Dr. Prasant Kumar Pattnaik, KIST, India.
Dr. Ch. Aswani Kumar, VIT University, India
Mr. Ijaz Ali Shoukat, King Saud University, Riyadh KSA
Mr. Arun Kumar, Sir Padam Pat Singhania University, Udaipur, Rajasthan
Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia
Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA
Mr. Mohd Zaki Bin Mas'ud, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
Prof. Dr. R. Geetharamani, Dept. of Computer Science and Eng., Rajalakshmi Engineering College, India
Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India
Dr. S. Abdul Khader Jilani, University of Tabuk, Tabuk, Saudi Arabia
Mr. Syed Jamal Haider Zaidi, Bahria University, Pakistan
Dr. N. Devarajan, Government College of Technology,Coimbatore, Tamilnadu, INDIA
Mr. R. Jagadeesh Kannan, RMK Engineering College, India
Mr. Deo Prakash, Shri Mata Vaishno Devi University, India
Mr. Mohammad Abu Naser, Dept. of EEE, IUT, Gazipur, Bangladesh
Assist. Prof. Prasun Ghosal, Bengal Engineering and Science University, India
Mr. Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne City, Australia
Mr. R. Mahammad Shafi, Madanapalle Institute of Technology & Science, India
Dr. F.Sagayaraj Francis, Pondicherry Engineering College,India
Dr. Ajay Goel, HIET , Kaithal, India
Mr. Nayak Sunil Kashibarao, Bahirji Smarak Mahavidyalaya, India
Mr. Suhas J Manangi, Microsoft India
Dr. Kalyankar N. V., Yeshwant Mahavidyalaya, Nanded , India
Dr. K.D. Verma, S.V. College of Post graduate studies & Research, India
Dr. Amjad Rehman, University Technology Malaysia, Malaysia

Mr. Rachit Garg, L K College, Jalandhar, Punjab
Mr. J. William, M.A.M college of Engineering, Trichy, Tamilnadu,India
Prof. Jue-Sam Chou, Nanhua University, College of Science and Technology, Taiwan
Dr. Thorat S.B., Institute of Technology and Management, India
Mr. Ajay Prasad, Sir Padampat Singhania University, Udaipur, India
Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India
Mr. Syed Rafiul Hussain, Ahsanullah University of Science and Technology, Bangladesh
Mrs Fazeela Tunnisa, Najran University, Kingdom of Saudi Arabia
Mrs Kavita Taneja, Maharishi Markandeshwar University, Haryana, India
Mr. Maniyar Shiraz Ahmed, Najran University, Najran, KSA
Mr. Anand Kumar, AMC Engineering College, Bangalore
Dr. Rakesh Chandra Gangwar, Beant College of Engg. & Tech., Gurdaspur (Punjab) India
Dr. V V Rama Prasad, Sree Vidyanikethan Engineering College, India
Assist. Prof. Neetesh Kumar Gupta, Technocrats Institute of Technology, Bhopal (M.P.), India
Mr. Ashish Seth, Uttar Pradesh Technical University, Lucknow ,UP India
Dr. V V S S S Balaram, Sreenidhi Institute of Science and Technology, India
Mr Rahul Bhatia, Lingaya's Institute of Management and Technology, India
Prof. Niranjan Reddy. P, KITS , Warangal, India
Prof. Rakesh. Lingappa, Vijetha Institute of Technology, Bangalore, India
Dr. Mohammed Ali Hussain, Nimra College of Engineering & Technology, Vijayawada, A.P., India
Dr. A.Srinivasan, MNM Jain Engineering College, Rajiv Gandhi Salai, Thorapakkam, Chennai
Mr. Rakesh Kumar, M.M. University, Mullana, Ambala, India
Dr. Lena Khaled, Zarqa Private University, Aman, Jordon
Ms. Supriya Kapoor, Patni/Lingaya's Institute of Management and Tech., India
Dr. Tossapon Boongoen , Aberystwyth University, UK
Dr . Bilal Alatas, Firat University, Turkey
Assist. Prof. Jyoti Praaksh Singh , Academy of Technology, India
Dr. Ritu Soni, GNG College, India
Dr . Mahendra Kumar , Sagar Institute of Research & Technology, Bhopal, India.
Dr. Binod Kumar, Lakshmi Narayan College of Tech.(LNCT)Bhopal India
Dr. Muzhir Shaban Al-Ani, Amman Arab University Amman – Jordan
Dr. T.C. Manjunath , ATRIA Institute of Tech, India
Mr. Muhammad Zakarya, COMSATS Institute of Information Technology (CIIT), Pakistan
Assist. Prof. Harmunish Taneja, M. M. University, India
Dr. Chitra Dhawale , SICSR, Model Colony, Pune, India
Mrs Sankari Muthukaruppan, Nehru Institute of Engineering and Technology, Anna University, India
Mr. Aaqif Afzaal Abbasi, National University Of Sciences And Technology, Islamabad
Prof. Ashutosh Kumar Dubey, Trinity Institute of Technology and Research Bhopal, India
Mr. G. Appasami, Dr. Pauls Engineering College, India
Mr. M Yasin, National University of Science and Tech, karachi (NUST), Pakistan
Mr. Yaser Miaji, University Utara Malaysia, Malaysia
Mr. Shah Ahsanul Haque, International Islamic University Chittagong (IIUC), Bangladesh

Prof. (Dr) Syed Abdul Sattar, Royal Institute of Technology & Science, India
Dr. S. Sasikumar, Roever Engineering College
Assist. Prof. Monit Kapoor, Maharishi Markandeshwar University, India
Mr. Nwaocha Vivian O, National Open University of Nigeria
Dr. M. S. Vijaya, GR Govindarajulu School of Applied Computer Technology, India
Assist. Prof. Chakresh Kumar, Manav Rachna International University, India
Mr. Kunal Chadha , R&D Software Engineer, Gemalto, Singapore
Mr. Mueen Uddin, Universiti Teknologi Malaysia, UTM , Malaysia
Dr. Dhuha Basheer abdullah, Mosul university, Iraq
Mr. S. Audithan, Annamalai University, India
Prof. Vijay K Chaudhari, Technocrats Institute of Technology , India
Associate Prof. Mohd Ilyas Khan, Technocrats Institute of Technology , India
Dr. Vu Thanh Nguyen, University of Information Technology, HoChiMinh City, VietNam
Assist. Prof. Anand Sharma, MITS, Lakshmangarh, Sikar, Rajasthan, India
Prof. T V Narayana Rao, HITAM Engineering college, Hyderabad
Mr. Deepak Gour, Sir Padampat Singhania University, India
Assist. Prof. Amutharaj Joyson, Kalasalingam University, India
Mr. Ali Balador, Islamic Azad University, Iran
Mr. Mohit Jain, Maharaja Surajmal Institute of Technology, India
Mr. Dilip Kumar Sharma, GLA Institute of Technology & Management, India
Dr. Debojyoti Mitra, Sir padampat Singhania University, India
Dr. Ali Dehghantanha, Asia-Pacific University College of Technology and Innovation, Malaysia
Mr. Zhao Zhang, City University of Hong Kong, China
Prof. S.P. Setty, A.U. College of Engineering, India
Prof. Patel Rakeshkumar Kantilal, Sankalchand Patel College of Engineering, India
Mr. Biswajit Bhowmik, Bengal College of Engineering & Technology, India
Mr. Manoj Gupta, Apex Institute of Engineering & Technology, India
Assist. Prof. Ajay Sharma, Raj Kumar Goel Institute Of Technology, India
Assist. Prof. Ramveer Singh, Raj Kumar Goel Institute of Technology, India
Dr. Hanan Elazhary, Electronics Research Institute, Egypt
Dr. Hosam I. Faiq, USM, Malaysia
Prof. Dipti D. Patil, MAEER's MIT College of Engg. & Tech, Pune, India
Assist. Prof. Devendra Chack, BCT Kumaon engineering College Dwarahat Almora, India
Prof. Manpreet Singh, M. M. Engg. College, M. M. University, India
Assist. Prof. M. Sadiq ali Khan, University of Karachi, Pakistan
Mr. Prasad S. Halgaonkar, MIT - College of Engineering, Pune, India
Dr. Imran Ghani, Universiti Teknologi Malaysia, Malaysia
Prof. Varun Kumar Kakar, Kumaon Engineering College, Dwarahat, India
Assist. Prof. Nisheeth Joshi, Apaji Institute, Banasthali University, Rajasthan, India
Associate Prof. Kunwar S. Vaisla, VCT Kumaon Engineering College, India
Prof Anupam Choudhary, Bhilai School Of Engg.,Bhilai (C.G.),India
Mr. Divya Prakash Shrivastava, Al Jabal Al garbi University, Zawya, Libya

Associate Prof. Dr. V. Radha, Avinashilingam Deemed university for women, Coimbatore.
Dr. Kasarapu Ramani, JNT University, Anantapur, India
Dr. Anuraag Awasthi, Jayoti Vidyapeeth Womens University, India
Dr. C G Ravichandran, R V S College of Engineering and Technology, India
Dr. Mohamed A. Deriche, King Fahd University of Petroleum and Minerals, Saudi Arabia
Mr. Abbas Karimi, Universiti Putra Malaysia, Malaysia
Mr. Amit Kumar, Jaypee University of Engg. and Tech., India
Dr. Nikolai Stoianov, Defense Institute, Bulgaria
Assist. Prof. S. Ranichandra, KSR College of Arts and Science, Tiruchencode
Mr. T.K.P. Rajagopal, Diamond Horse International Pvt Ltd, India
Dr. Md. Ekramul Hamid, Rajshahi University, Bangladesh
Mr. Hemanta Kumar Kalita , TATA Consultancy Services (TCS), India
Dr. Messaouda Azzouzi, Ziane Achour University of Djelfa, Algeria
Prof. (Dr.) Juan Jose Martinez Castillo, "Gran Mariscal de Ayacucho" University and Acantelys research Group, Venezuela
Dr. Jatinderkumar R. Saini, Narmada College of Computer Application, India
Dr. Babak Bashari Rad, University Technology of Malaysia, Malaysia
Dr. Nighat Mir, Effat University, Saudi Arabia
Prof. (Dr.) G.M.Nasira, Sasurie College of Engineering, India
Mr. Varun Mittal, Gemalto Pte Ltd, Singapore
Assist. Prof. Mrs P. Banumathi, Kathir College Of Engineering, Coimbatore
Assist. Prof. Quan Yuan, University of Wisconsin-Stevens Point, US
Dr. Pranam Paul, Narula Institute of Technology, Agarpara, West Bengal, India
Assist. Prof. J. Ramkumar, V.L.B Janakiammal college of Arts & Science, India
Mr. P. Sivakumar, Anna university, Chennai, India
Mr. Md. Humayun Kabir Biswas, King Khalid University, Kingdom of Saudi Arabia
Mr. Mayank Singh, J.P. Institute of Engg & Technology, Meerut, India
HJ. Kamaruzaman Jusoff, Universiti Putra Malaysia
Mr. Nikhil Patrick Lobo, CADES, India
Dr. Amit Wason, Rayat-Bahra Institute of Engineering & Boi-Technology, India
Dr. Rajesh Shrivastava, Govt. Benazir Science & Commerce College, Bhopal, India
Assist. Prof. Vishal Bharti, DCE, Gurgaon
Mrs. Sunita Bansal, Birla Institute of Technology & Science, India
Dr. R. Sudhakar, Dr.Mahalingam college of Engineering and Technology, India
Dr. Amit Kumar Garg, Shri Mata Vaishno Devi University, Katra(J&K), India
Assist. Prof. Raj Gaurang Tiwari, AZAD Institute of Engineering and Technology, India
Mr. Hamed Taherdoost, Tehran, Iran
Mr. Amin Daneshmand Malayeri, YRC, IAU, Malayer Branch, Iran
Mr. Shantanu Pal, University of Calcutta, India
Dr. Terry H. Walcott, E-Promag Consultancy Group, United Kingdom
Dr. Ezekiel U OKIKE, University of Ibadan, Nigeria
Mr. P. Mahalingam, Caledonian College of Engineering, Oman

Dr. Mahmoud M. A. Abd Ellatif, Mansoura University, Egypt
Prof. Kunwar S. Vaisla, BCT Kumaon Engineering College, India
Prof. Mahesh H. Panchal, Kalol Institute of Technology & Research Centre, India
Mr. Muhammad Asad, Technical University of Munich, Germany
Mr. AliReza Shams Shafigh, Azad Islamic university, Iran
Prof. S. V. Nagaraj, RMK Engineering College, India
Mr. Ashikali M Hasan, Senior Researcher, CelNet security, India
Dr. Adnan Shahid Khan, University Technology Malaysia, Malaysia
Mr. Prakash Gajanan Burade, Nagpur University/ITM college of engg, Nagpur, India
Dr. Jagdish B.Helonde, Nagpur University/ITM college of engg, Nagpur, India
Professor, Doctor BOUHORMA Mohammed, Univertsity Abdelmalek Essaadi, Morocco
Mr. K. Thirumalaivasan, Pondicherry Engg. College, India
Mr. Umbarkar Anantkumar Janardan, Walchand College of Engineering, India
Mr. Ashish Chaurasia, Gyan Ganga Institute of Technology & Sciences, India
Mr. Sunil Taneja, Kurukshetra University, India
Mr. Fauzi Adi Rafrastara, Dian Nuswantoro University, Indonesia
Dr. Yaduvir Singh, Thapar University, India
Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece
Dr. Vasantha Kalyani David, Avinashilingam University for women, Coimbatore
Dr. Ahmed Mansour Manasrah, Universiti Sains Malaysia, Malaysia
Miss. Nazanin Sadat Kazazi, University Technology Malaysia, Malaysia
Mr. Saeed Rasouli Heikalabad, Islamic Azad University - Tabriz Branch, Iran
Assoc. Prof. Dhirendra Mishra, SVKM's NMIMS University, India
Prof. Shapoor Zarei, UAE Inventors Association, UAE
Prof. B.Raja Sarath Kumar, Lenora College of Engineering, India
Dr. Bashir Alam, Jamia millia Islamia, Delhi, India
Prof. Anant J Umbarkar, Walchand College of Engg., India
Assist. Prof. B. Bharathi, Sathyabama University, India
Dr. Fokrul Alom Mazarbhuiya, King Khalid University, Saudi Arabia
Prof. T.S.Jeyali Laseeth, Anna University of Technology, Tirunelveli, India
Dr. M. Balraju, Jawahar Lal Nehru Technological University Hyderabad, India
Dr. Vijayalakshmi M. N., R.V.College of Engineering, Bangalore
Prof. Walid Moudani, Lebanese University, Lebanon
Dr. Saurabh Pal, VBS Purvanchal University, Jaunpur, India
Associate Prof. Suneet Chaudhary, Dehradun Institute of Technology, India
Associate Prof. Dr. Manuj Darbari, BBD University, India
Ms. Prema Selvaraj, K.S.R College of Arts and Science, India
Assist. Prof. Ms.S.Sasikala, KSR College of Arts & Science, India
Mr. Sukhvinder Singh Deora, NC Institute of Computer Sciences, India
Dr. Abhay Bansal, Amity School of Engineering & Technology, India
Ms. Sumita Mishra, Amity School of Engineering and Technology, India
Professor S. Viswanadha Raju, JNT University Hyderabad, India

Mr. Asghar Shahrzad Khashandarag, Islamic Azad University Tabriz Branch, India
Mr. Manoj Sharma, Panipat Institute of Engg. & Technology, India
Mr. Shakeel Ahmed, King Faisal University, Saudi Arabia
Dr. Mohamed Ali Mahjoub, Institute of Engineer of Monastir, Tunisia
Mr. Adri Jovin J.J., SriGuru Institute of Technology, India
Dr. Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia
Mr. Rakesh Bharati, Dehradun Institute of Technology Dehradun, India
Mr. Shervan Fekri Ershad, Shiraz International University, Iran
Mr. Md. Safiqul Islam, Daffodil International University, Bangladesh
Mr. Mahmudul Hasan, Daffodil International University, Bangladesh
Prof. Mandakini Tayade, UIT, RGTU, Bhopal, India
Ms. Sarla More, UIT, RGTU, Bhopal, India
Mr. Tushar Hrishikesh Jaware, R.C. Patel Institute of Technology, Shirpur, India
Ms. C. Divya, Dr G R Damodaran College of Science, Coimbatore, India
Mr. Fahimuddin Shaik, Annamacharya Institute of Technology & Sciences, India
Dr. M. N. Giri Prasad, JNTUCE,Pulivendula, A.P., India
Assist. Prof. Chintan M Bhatt, Charotar University of Science And Technology, India
Prof. Sahista Machchhar, Marwadi Education Foundation's Group of institutions, India
Assist. Prof. Navnish Goel, S. D. College Of Enginnering & Technology, India
Mr. Khaja Kamaluddin, Sirt University, Sirt, Libya
Mr. Mohammad Zaidul Karim, Daffodil International, Bangladesh
Mr. M. Vijayakumar, KSR College of Engineering, Tiruchengode, India
Mr. S. A. Ahsan Rajon, Khulna University, Bangladesh
Dr. Muhammad Mohsin Nazir, LCW University Lahore, Pakistan
Mr. Mohammad Asadul Hoque, University of Alabama, USA
Mr. P.V.Sarathchand, Indur Institute of Engineering and Technology, India
Mr. Durgesh Samadhiya, Chung Hua University, Taiwan
Dr Venu Kuthadi, University of Johannesburg, Johannesburg, RSA
Dr. (Er) Jasvir Singh, Guru Nanak Dev University, Amritsar, Punjab, India
Mr. Jasmin Cosic, Min. of the Interior of Una-sana canton, B&H, Bosnia and Herzegovina
Dr S. Rajalakshmi, Botho College, South Africa
Dr. Mohamed Sarrab, De Montfort University, UK
Mr. Basappa B. Kodada, Canara Engineering College, India
Assist. Prof. K. Ramana, Annamacharya Institute of Technology and Sciences, India
Dr. Ashu Gupta, Apeejay Institute of Management, Jalandhar, India
Assist. Prof. Shaik Rasool, Shadan College of Engineering & Technology, India
Assist. Prof. K. Suresh, Annamacharya Institute of Tech & Sci. Rajampet, AP, India
Dr . G. Singaravel, K.S.R. College of Engineering, India
Dr B. G. Geetha, K.S.R. College of Engineering, India
Assist. Prof. Kavita Choudhary, ITM University, Gurgaon
Dr. Mehrdad Jalali, Azad University, Mashhad, Iran
Megha Goel, Shamli Institute of Engineering and Technology, Shamli, India

Mr. Chi-Hua Chen, Institute of Information Management, National Chiao-Tung University, Taiwan (R.O.C.)
Assoc. Prof. A. Rajendran, RVS College of Engineering and Technology, India
Assist. Prof. S. Jaganathan, RVS College of Engineering and Technology, India
Assoc. Prof. (Dr.) A S N Chakravarthy, JNTUK University College of Engineering Vizianagaram (State University)
Assist. Prof. Deepshikha Patel, Technocrat Institute of Technology, India
Assist. Prof. Maram Balajee, GMRIT, India
Assist. Prof. Monika Bhatnagar, TIT, India
Prof. Gaurang Panchal, Charotar University of Science & Technology, India
Prof. Anand K. Tripathi, Computer Society of India
Prof. Jyoti Chaudhary, High Performance Computing Research Lab, India
Assist. Prof. Supriya Raheja, ITM University, India
Dr. Pankaj Gupta, Microsoft Corporation, U.S.A.
Assist. Prof. Panchamukesh Chandaka, Hyderabad Institute of Tech. & Management, India
Prof. Mohan H.S, SJB Institute Of Technology, India
Mr. Hossein Malekinezhad, Islamic Azad University, Iran
Mr. Zatin Gupta, Universti Malaysia, Malaysia
Assist. Prof. Amit Chauhan, Phonics Group of Institutions, India
Assist. Prof. Ajal A. J., METS School Of Engineering, India
Mrs. Omowunmi Omobola Adeyemo, University of Ibadan, Nigeria
Dr. Bharat Bhushan Agarwal, I.F.T.M. University, India
Md. Nazrul Islam, University of Western Ontario, Canada
Tushar Kanti, L.N.C.T, Bhopal, India
Er. Aumreesh Kumar Saxena, SIRTs College Bhopal, India
Mr. Mohammad Monirul Islam, Daffodil International University, Bangladesh
Dr. Kashif Nisar, University Utara Malaysia, Malaysia
Dr. Wei Zheng, Rutgers Univ/ A10 Networks, USA
Associate Prof. Rituraj Jain, Vyas Institute of Engg & Tech, Jodhpur – Rajasthan
Assist. Prof. Apoorvi Sood, I.T.M. University, India
Dr. Kayhan Zrar Ghafoor, University Technology Malaysia, Malaysia
Mr. Swapnil Soner, Truba Institute College of Engineering & Technology, Indore, India
Ms. Yogita Gigras, I.T.M. University, India
Associate Prof. Neelima Sadineni, Pydha Engineering College, India Pydha Engineering College
Assist. Prof. K. Deepika Rani, HITAM, Hyderabad
Ms. Shikha Maheshwari, Jaipur Engineering College & Research Centre, India
Prof. Dr V S Giridhar Akula, Avanthi's Scientific Tech. & Research Academy, Hyderabad
Prof. Dr.S.Saravanan, Muthayammal Engineering College, India
Mr. Mehdi Golsorkhatabar Amiri, Islamic Azad University, Iran
Prof. Amit Sadanand Savyanavar, MITCOE, Pune, India
Assist. Prof. P.Oliver Jayaprakash, Anna University,Chennai
Assist. Prof. Ms. Sujata, ITM University, Gurgaon, India
Dr. Asoke Nath, St. Xavier's College, India

Mr. Masoud Rafighi, Islamic Azad University, Iran
Assist. Prof. RamBabu Pemula, NIMRA College of Engineering & Technology, India
Assist. Prof. Ms Rita Chhikara, ITM University, Gurgaon, India
Mr. Sandeep Maan, Government Post Graduate College, India
Prof. Dr. S. Muralidharan, Mepco Schlenk Engineering College, India
Associate Prof. T.V.Sai Krishna, QIS College of Engineering and Technology, India
Mr. R. Balu, Bharathiar University, Coimbatore, India
Assist. Prof. Shekhar. R, Dr.SM College of Engineering, India
Prof. P. Senthilkumar, Vivekanandha Institue of Engineering and Techology for Woman, India
Mr. M. Kamarajan, PSNA College of Engineering & Technology, India
Dr. Angajala Srinivasa Rao, Jawaharlal Nehru Technical University, India
Assist. Prof. C. Venkatesh, A.I.T.S, Rajampet, India
Mr. Afshin Rezakhani Roozbahani, Ayatollah Boroujerdi University, Iran
Mr. Laxmi chand, SCTL, Noida, India
Dr. Dr. Abdul Hannan, Vivekanand College, Aurangabad
Prof. Mahesh Panchal, KITRC, Gujarat
Dr. A. Subramani, K.S.R. College of Engineering, Tiruchengode
Assist. Prof. Prakash M, Rajalakshmi Engineering College, Chennai, India
Assist. Prof. Akhilesh K Sharma, Sir Padampat Singhania University, India
Ms. Varsha Sahni, Guru Nanak Dev Engineering College, Ludhiana, India
Associate Prof. Trilochan Rout, NM Institute of Engineering and Technlogy, India
Mr. Srikanta Kumar Mohapatra, NMIET, Orissa, India
Mr. Waqas Haider Bangyal, Iqra University Islamabad, Pakistan
Dr. S. Vijayaragavan, Christ College of Engineering and Technology, Pondicherry, India
Prof. Elboukhari Mohamed, University Mohammed First, Oujda, Morocco
Dr. Muhammad Asif Khan, King Faisal University, Saudi Arabia
Dr. Nagy Ramadan Darwish Omran, Cairo University, Egypt.
Assistant Prof. Anand Nayyar, KCL Institute of Management and Technology, India
Mr. G. Premsankar, Ericcson, India
Assist. Prof. T. Hemalatha, VELS University, India
Prof. Tejaswini Apte, University of Pune, India
Dr. Edmund Ng Giap Weng, Universiti Malaysia Sarawak, Malaysia
Mr. Mahdi Nouri, Iran University of Science and Technology, Iran
Associate Prof. S. Asif Hussain, Annamacharya Institute of technology & Sciences, India
Mrs. Kavita Pabreja, Maharaja Surajmal Institute (an affiliate of GGSIP University), India
Mr. Vorugunti Chandra Sekhar, DA-IICT, India
Mr. Muhammad Najmi Ahmad Zabidi, Universiti Teknologi Malaysia, Malaysia
Dr. Aderemi A. Atayero, Covenant University, Nigeria
Assist. Prof. Osama Sohaib, Balochistan University of Information Technology, Pakistan
Assist. Prof. K. Suresh, Annamacharya Institute of Technology and Sciences, India
Mr. Hassen Mohammed Abduallah Alsafi, International Islamic University Malaysia (IIUM) Malaysia
Mr. Robail Yasrab, Virtual University of Pakistan, Pakistan

Mr. R. Balu, Bharathiar University, Coimbatore, India
Prof. Anand Nayyar, KCL Institute of Management and Technology, Jalandhar
Assoc. Prof. Vivek S Deshpande, MIT College of Engineering, India
Prof. K. Saravanan, Anna university Coimbatore, India
Dr. Ravendra Singh, MJP Rohilkhand University, Bareilly, India
Mr. V. Mathivanan, IBRA College of Technology, Sultanate of OMAN
Assoc. Prof. S. Asif Hussain, AITS, India
Assist. Prof. C. Venkatesh, AITS, India
Mr. Sami Ulhaq, SZABIST Islamabad, Pakistan
Dr. B. Justus Rabi, Institute of Science & Technology, India
Mr. Anuj Kumar Yadav, Dehradun Institute of technology, India
Mr. Alejandro Mosquera, University of Alicante, Spain
Assist. Prof. Arjun Singh, Sir Padampat Singhania University (SPSU), Udaipur, India
Dr. Smriti Agrawal, JB Institute of Engineering and Technology, Hyderabad
Assist. Prof. Swathi Sambangi, Visakha Institute of Engineering and Technology, India
Ms. Prabhjot Kaur, Guru Gobind Singh Indraprastha University, India
Mrs. Samaher AL-Hothali, Yanbu University College, Saudi Arabia
Prof. Rajneeshkaur Bedi, MIT College of Engineering, Pune, India
Mr. Hassen Mohammed Abduallah Alsafi, International Islamic University Malaysia (IIUM)
Dr. Wei Zhang, Amazon.com, Seattle, WA, USA
Mr. B. Santhosh Kumar, C S I College of Engineering, Tamil Nadu
Dr. K. Reji Kumar, , N S S College, Pandalam, India
Assoc. Prof. K. Seshadri Sastry, EIILM University, India
Mr. Kai Pan, UNC Charlotte, USA
Mr. Ruikar Sachin, SGGSIET, India
Prof. (Dr.) Vinodani Katiyar, Sri Ramswaroop Memorial University, India
Assoc. Prof., M. Giri, Sreenivasa Institute of Technology and Management Studies, India
Assoc. Prof. Labib Francis Gergis, Misr Academy for Engineering and Technology (MET), Egypt
Assist. Prof. Amanpreet Kaur, ITM University, India
Assist. Prof. Anand Singh Rajawat, Shri Vaishnav Institute of Technology & Science, Indore
Mrs. Hadeel Saleh Haj Aliwi, Universiti Sains Malaysia (USM), Malaysia
Dr. Abhay Bansal, Amity University, India
Dr. Mohammad A. Mezher, Fahad Bin Sultan University, KSA
Assist. Prof. Nidhi Arora, M.C.A. Institute, India
Prof. Dr. P. Suresh, Karpagam College of Engineering, Coimbatore, India
Dr. Kannan Balasubramanian, Mepco Schlenk Engineering College, India
Dr. S. Sankara Gomathi, Panimalar Engineering college, India
Prof. Anil kumar Suthar, Gujarat Technological University, L.C. Institute of Technology, India
Assist. Prof. R. Hubert Rajan, NOORUL ISLAM UNIVERSITY, India
Assist. Prof. Dr. Jyoti Mahajan, College of Engineering & Technology
Assist. Prof. Homam Reda El-Taj, College of Network Engineering, Saudi Arabia & Malaysia
Mr. Bijan Paul, Shahjalal University of Science & Technology, Bangladesh

Assoc. Prof. Dr. Ch V Phani Krishna, KL University, India
Dr. Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies & Research, India
Dr. Lamri LAOUAMER, Al Qassim University, Dept. Info. Systems & European University of Brittany, Dept. Computer Science, UBO, Brest, France
Prof. Ashish Babanrao Sasankar, G.H.Raisoni Institute Of Information Technology, India
Prof. Pawan Kumar Goel, Shamli Institute of Engineering and Technology, India
Mr. Ram Kumar Singh, S.V Subharti University, India
Assistant Prof. Sunish Kumar O S, Amaljyothi College of Engineering, India
Dr Sanjay Bhargava, Banasthali University, India
Mr. Pankaj S. Kulkarni, AVEW's Shatabdi Institute of Technology, India
Mr. Roohollah Etemadi, Islamic Azad University, Iran
Mr. Oloruntoyin Sefiu Taiwo, Emmanuel Alayande College Of Education, Nigeria
Mr. Sumit Goyal, National Dairy Research Institute, India
Mr Jaswinder Singh Dilawari, Geeta Engineering College, India
Prof. Raghuraj Singh, Harcourt Butler Technological Institute, Kanpur
Dr. S.K. Mahendran, Anna University, Chennai, India
Dr. Amit Wason, Hindustan Institute of Technology & Management, Punjab
Dr. Ashu Gupta, Apeejay Institute of Management, India
Assist. Prof. D. Asir Antony Gnana Singh, M.I.E.T Engineering College, India
Mrs Mina Farmanbar, Eastern Mediterranean University, Famagusta, North Cyprus
Mr. Maram Balajee, GMR Institute of Technology, India
Mr. Moiz S. Ansari, Isra University, Hyderabad, Pakistan
Mr. Adebayo, Olawale Surajudeen, Federal University of Technology Minna, Nigeria
Mr. Jasvir Singh, University College Of Engg., India
Mr. Vivek Tiwari, MANIT, Bhopal, India
Assoc. Prof. R. Navaneethakrishnan, Bharathiyar College of Engineering and Technology, India
Mr. Somdip Dey, St. Xavier's College, Kolkata, India
Mr. Souleymane Balla-Arabé, Xi'an University of Electronic Science and Technology, China
Mr. Mahabub Alam, Rajshahi University of Engineering and Technology, Bangladesh
Mr. Sathyapraksh P., S.K.P Engineering College, India
Dr. N. Karthikeyan, SNS College of Engineering, Anna University, India
Dr. Binod Kumar, JSPM's, Jayawant Technical Campus, Pune, India
Assoc. Prof. Dinesh Goyal, Suresh Gyan Vihar University, India
Mr. Md. Abdul Ahad, K L University, India
Mr. Vikas Bajpai, The LNM IIT, India
Dr. Manish Kumar Anand, Salesforce (R & D Analytics), San Francisco, USA
Assist. Prof. Dheeraj Murari, Kumaon Engineering College, India
Assoc. Prof. Dr. A. Muthukumaravel, VELS University, Chennai
Mr. A. Siles Balasingh, St.Joseph University in Tanzania, Tanzania
Mr. Ravindra Daga Badgujar, R C Patel Institute of Technology, India
Dr. Preeti Khanna, SVKM's NMIMS, School of Business Management, India
Mr. Kumar Dayanand, Cambridge Institute of Technology, India

Dr. Syed Asif Ali, SMI University Karachi, Pakistan
Prof. Pallvi Pandit, Himachal Pradeh University, India
Mr. Ricardo Verschueren, University of Gloucestershire, UK
Assist. Prof. Mamta Juneja, University Institute of Engineering and Technology, Panjab University, India
Assoc. Prof. P. Surendra Varma, NRI Institute of Technology, JNTU Kakinada, India
Assist. Prof. Gaurav Shrivastava, RGPV / SVITS Indore, India
Dr. S. Sumathi, Anna University, India
Assist. Prof. Ankita M. Kapadia, Charotar University of Science and Technology, India
Mr. Deepak Kumar, Indian Institute of Technology (BHU), India
Dr. Dr. Rajan Gupta, GGSIP University, New Delhi, India
Assist. Prof M. Anand Kumar, Karpagam University, Coimbatore, India
Mr. Mr Arshad Mansoor, Pakistan Aeronautical Complex
Mr. Kapil Kumar Gupta, Ansal Institute of Technology and Management, India
Dr. Neeraj Tomer, SINE International Institute of Technology, Jaipur, India
Assist. Prof. Trunal J. Patel, C.G.Patel Institute of Technology, Uka Tarsadia University, Bardoli, Surat
Mr. Sivakumar, Codework solutions, India
Mr. Mohammad Sadegh Mirzaei, PGNR Company, Iran
Dr. Gerard G. Dumancas, Oklahoma Medical Research Foundation, USA
Mr. Varadala Sridhar, Varadhaman College Engineering College, Affiliated To JNTU, Hyderabad
Assist. Prof. Manoj Dhawan, SVITS, Indore
Assoc. Prof. Chitreshh Banerjee, Suresh Gyan Vihar University, Jaipur, India
Dr. S. Santhi, SCSVMV University, India
Mr. Davood Mohammadi Souran, Ministry of Energy of Iran, Iran
Mr. Shamim Ahmed, Bangladesh University of Business and Technology, Bangladesh
Mr. Sandeep Reddivari, Mississippi State University, USA
Assoc. Prof. Ousmane Thiare, Gaston Berger University, Senegal
Dr. Hazra Imran, Athabasca University, Canada
Dr. Setu Kumar Chaturvedi, Technocrats Institute of Technology, Bhopal, India
Mr. Mohd Dilshad Ansari, Jaypee University of Information Technology, India
Ms. Jaspreet Kaur, Distance Education LPU, India
Dr. D. Nagarajan, Salalah College of Technology, Sultanate of Oman
Dr. K.V.N.R.Sai Krishna, S.V.R.M. College, India
Mr. Himanshu Pareek, Center for Development of Advanced Computing (CDAC), India
Mr. Khaldi Amine, Badji Mokhtar University, Algeria
Mr. Mohammad Sadegh Mirzaei, Scientific Applied University, Iran
Assist. Prof. Khyati Chaudhary, Ram-eesh Institute of Engg. & Technology, India
Mr. Sanjay Agal, Pacific College of Engineering Udaipur, India
Mr. Abdul Mateen Ansari, King Khalid University, Saudi Arabia
Dr. H.S. Behera, Veer Surendra Sai University of Technology (VSSUT), India
Dr. Shrikant Tiwari, Shri Shankaracharya Group of Institutions (SSGI), India
Prof. Ganesh B. Regulwar, Shri Shankarprasad Agnihotri College of Engg, India
Prof. Pinnamaneni Bhanu Prasad, Matrix vision GmbH, Germany

Dr. Shrikant Tiwari, Shri Shankaracharya Technical Campus (SSTC), India
Dr. Siddesh G.K., : Dayananada Sagar College of Engineering, Bangalore, India
Mr. Nadir Bouchama, CERIST Research Center, Algeria
Dr. R. Sathishkumar, Sri Venkateswara College of Engineering, India
Assistant Prof (Dr.) Mohamed Moussaoui, Abdelmalek Essaadi University, Morocco
Dr. S. Malathi, Panimalar Engineering College, Chennai, India
Dr. V. Subedha, Panimalar Institute of Technology, Chennai, India
Dr. Prashant Panse, Swami Vivekanand College of Engineering, Indore, India
Dr. Hamza Aldabbas, Al-Balqa'a Applied University, Jordan
Dr. G. Rasitha Banu, Vel's University, Chennai
Dr. V. D. Ambeth Kumar, Panimalar Engineering College, Chennai
Prof. Anuranjan Misra, Bhagwant Institute of Technology, Ghaziabad, India
Ms. U. Sinthuja, PSG college of arts &science, India
Mr. Ehsan Saradar Torshizi, Urmia University, Iran
Mr. Shamneesh Sharma, APG Shimla University, Shimla (H.P.), India
Assistant Prof. A. S. Syed Navaz, Muthayammal College of Arts & Science, India
Assistant Prof. Ranjit Panigrahi, Sikkim Manipal Institute of Technology, Majitar, Sikkim
Dr. Khaled Eskaf, Arab Academy for Science ,Technology & Maritime Transportation, Egypt
Mr. Nishant Gupta, University of Jammu, India
Assistant Prof. Nagarajan Sankaran, Annamalai University, Chidambaram, Tamilnadu, India
Assistant Prof.Tribikram Pradhan, Manipal Institute of Technology, India
Dr. Nasser Lotfi, Eastern Mediterranean University, Northern Cyprus
Dr. R. Manavalan, K S Rangasamy college of Arts and Science, Tamilnadu, India
Assistant Prof. P. Krishna Sankar, K S Rangasamy college of Arts and Science, Tamilnadu, India
Dr. Rahul Malik, Cisco Systems, USA
Dr. S. C. Lingareddy, ALPHA College of Engineering, India
Assistant Prof. Mohammed Shuaib, Interal University, Lucknow, India
Mr. Sachin Yele, Sanghvi Institute of Management & Science, India
Mr. T. Thambidurai, Sun Univercell, Singapore
Prof. Anandkumar Telang, BKIT, India
Assistant Prof. R. Poorvadevi, SCSVMV University, India
Dr Uttam Mande, Gitam University, India
Dr. Poornima Girish Naik, Shahu Institute of Business Education and Research (SIBER), India
Prof. Md. Abu Kausar, Jaipur National University, Jaipur, India
Mr. Mohammed Zuber, AISECT University, India
Prof. Kalum Priyanath Udagepola, King Abdulaziz University, Saudi Arabia

CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2014
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

© IJCSIS PUBLICATION 2014
ISSN 1947 5500
http://sites.google.com/site/ijcsis/