Online ISSN : 0975-4172
Print ISSN : 0975-4350

Global Journal of Computer Science and Technology : E

Network, Web & Security

DISCOVERING THOUGHTS AND INVENTING FUTURE

HIGHLIGHTS

- Performance Evaluation of AODV
- Knowledge Management System
- Designing and Implimentation
- Secure Group Communication Plane

Computer Server Farm

Volume 12 | Issue 16 | Version 1.0 ENG

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 12 Issue 16 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

(A Delaware USA Incorporation with "Good Standing"; Reg. Number: 0423089)

Sponsors:Global Association of Research

Open Scientific Standards

Publisher's Headquarters office

Global Journals Inc., Headquarters Corporate Office, Cambridge Office Center, II Canal Park, Floor No. 5th, ***Cambridge (Massachusetts)***, Pin: MA 02141 United States

USA Toll Free: +001-888-839-7392

USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Association of Research, Marsh Road, Rainham, Essex, London RM13 8EU United Kingdom.

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investers@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Editorial Board Members (HON.)

Dr. Bart Lambrecht
Director of Research in Accounting and FinanceProfessor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD (Cambridge)

Dr. Carlos García Pont
Associate Professor of Marketing
IESE Business School, University of Navarra
Doctor of Philosophy (Management), Massachusetts Institute of Technology (MIT)
Master in Business Administration, IESE, University of Navarra
Degree in Industrial Engineering, Universitat Politècnica de Catalunya

Dr. Fotini Labropulu
Mathematics - Luther College
University of ReginaPh.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windso

Dr. Lynn Lim
Reader in Business and Marketing
Roehampton University, London
BCom, PGDip, MBA (Distinction), PhD, FHEA

Dr. Mihaly Mezei
ASSOCIATE PROFESSOR
Department of Structural and Chemical Biology, Mount Sinai School of Medical Center
Ph.D., Etvs Lornd University
Postdoctoral Training,
New York University

Dr. Söhnke M. Bartram
Department of Accounting and FinanceLancaster University Management SchoolPh.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño
Professor of Decision Sciences
IESE Business School
Barcelona, Spain (Universidad de Navarra)
CEIBS (China Europe International Business School).
Beijing, Shanghai and Shenzhen
Ph.D. in Mathematics
University of Barcelona
BA in Mathematics (Licenciatura)
University of Barcelona

Philip G. Moscoso
Technology and Operations Management
IESE Business School, University of Navarra
Ph.D in Industrial Engineering and Management, ETH Zurich
M.Sc. in Chemical Engineering, ETH Zurich

Dr. Sanjay Dixit, M.D.
Director, EP Laboratories, Philadelphia VA Medical Center
Cardiovascular Medicine - Cardiac Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng
MD., Ph.D
Associate Professor and Research
Department Division of Neuromuscular Medicine
Davee Department of Neurology and Clinical NeuroscienceNorthwestern University
Feinberg School of Medicine

Dr. Pina C. Sanelli
Associate Professor of Public Health
Weill Cornell Medical College
Associate Attending Radiologist
NewYork-Presbyterian Hospital
MRI, MRA, CT, and CTA
Neuroradiology and Diagnostic Radiology
M.D., State University of New York at Buffalo,School of Medicine and Biomedical Sciences

Dr. Roberto Sanchez
Associate Professor
Department of Structural and Chemical Biology
Mount Sinai School of Medicine
Ph.D., The Rockefeller University

Dr. Wen-Yih Sun
Professor of Earth and Atmospheric SciencesPurdue University Director
National Center for Typhoon and Flooding Research, Taiwan
University Chair Professor
Department of Atmospheric Sciences, National Central University, Chung-Li, TaiwanUniversity Chair Professor
Institute of Environmental Engineering, National Chiao Tung University, Hsin-chu, Taiwan.Ph.D., MS The University of Chicago, Geophysical Sciences
BS National Taiwan University, Atmospheric Sciences
Associate Professor of Radiology

Dr. Michael R. Rudnick
M.D., FACP
Associate Professor of Medicine
Chief, Renal Electrolyte and Hypertension Division (PMC)
Penn Medicine, University of Pennsylvania
Presbyterian Medical Center, Philadelphia
Nephrology and Internal Medicine
Certified by the American Board of Internal Medicine

Dr. Bassey Benjamin Esu
B.Sc. Marketing; MBA Marketing; Ph.D Marketing
Lecturer, Department of Marketing, University of Calabar
Tourism Consultant, Cross River State Tourism Development Department
Co-ordinator , Sustainable Tourism Initiative, Calabar, Nigeria

Dr. Aziz M. Barbar, Ph.D.
IEEE Senior Member
Chairperson, Department of Computer Science
AUST - American University of Science & Technology
Alfred Naccash Avenue – Ashrafieh

Contents of the Volume

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Evaluation of AODV and DSDV Routing Protocols for Ad-hoc Networks

By Er.Abhishek Sengar & Er.Sandeep Shrivastav

Electronics and Communication College of Science and Engineering Jhansi, India

Abstract - Ad-hoc networks are basically self organizing and self configuring multi-hop mobile wireless network in which the information packets are transmitted in a store and forward manner from a source to an arbitrary destination via intermediate nodes. The main objective of this paper is to performance evaluation of AODV (Ad-hoc on demand distance vector) and DSDV (Destination sequence distance vector) routing protocols on the basis of different performance metrics. In this paper, an attempt has been made to evaluate the performance of two well known routing protocols AODV, DSDV by using three performance metrics such as throughput, packet delivery ratio and Routing overheads. The Performance evaluation has been done by using simulation tool NS2 (Network Simulator) which is the main simulator.

Keywords : *AODV, DSDV, dsr, ns2.*

GJCST-E Classification : *C.2.2*

Strictly as per the compliance and regulations of:

Performance Evaluation of AODV and DSDV Routing Protocols for Ad-hoc Networks

Er.Abhishek Sengar[α] & Er.Sandeep Shrivastav[α]

Abstract - Ad-hoc networks are basically self organizing and self configuring multi-hop mobile wireless network in which the information packets are transmitted in a store and forward manner from a source to an arbitrary destination via intermediate nodes. The main objective of this paper is to performance evaluation of AODV (Ad-hoc on demand distance vector) and DSDV (Destination sequence distance vector) routing protocols on the basis of different performance metrics. In this paper, an attempt has been made to evaluate the performance of two well known routing protocols AODV, DSDV by using three performance metrics such as throughput, packet delivery ratio and Routing overheads. The Performance evaluation has been done by using simulation tool NS2 (Network Simulator) which is the main simulator.

IndexTerms : *AODV, DSDV, dsr, ns2.*

I. Introduction

Wireless networking is an emerging technology that allows user to access information and services electronically, regardless of their geographic position. Wireless network can be classified in two types- Infrastructure networks and Infrastructure Less networks or Ad-hoc Networks [6].

Infrastructure Networks:-Infrastructure network consist of fixed and wired gateways. A mobile host communicates with a bridge in the network (called base station) within its

Communicate radius. The mobile unit can move geographically while it is communicating. When it goes out of Range of one base station, it connects with new base station and start communicating through it. This is called handoff. In this approach the base station are fixed [7].

Infrastructure Less (Ad-hoc) Networks:-Ad-hoc networks are collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or stand-alone infrastructure [1]. Ad-hoc network are basically peer-to-peer self organizing and self configuring multi-hop mobile wireless network where the structure of the network changes dynamically [2]. This is mainly due to the mobility of nodes [3]. Nodes in this network utilize the same random access wireless channel, cooperating in friendly manner to engaging themselves in multi-hop Forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in the network [2].

Author α : Electronics and Communication College of Science and Engineering Jhansi, India.

Routing is used to decide best suitable path for packet transmission from one place to another place. In this paper an attempt has been made to evaluate the performance of proactive and reactive routing protocols. Ad-hoc network flat routing protocols may classify as:-

Proactive routing (Table-driven) protocols:- Proactive routing or table- driven routing protocols attempt to maintain consistent, up-to date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to change in network topology by propagating route update throughout the network to Maintain consistent network view.

Reactive (On-demand) routing protocols:-In reactive or on demand routing protocols, the routes are created as when required. When a source wants to send to a destination, it invokes the route discovery mechanism to find the path to the destination. This process is completed when once a source is found or all possible route permutation has been examined. Once a route has been discovered and established, it is maintained by some form of route maintenance procedure until either the destination becomes inaccessible along every path from the source or route is no longer desired.

With the increase of portable of devices as well as progress in wireless communication, Ad-hoc network gaining importance with the increasing number of widespread application. The following point shows the importance of ad hoc networks:

Instant Infrastructure: Unplanned meetings, spontaneous interpersonal communications etc., cannot rely on any infrastructure, it needs planning and administration. It would take too long to set up this kind of infrastructure; therefore ad-hoc connectivity has to setup [6].

Disaster Relief: Infrastructure typically breakdown in disaster areas. Hurricanes cut phone and power lines, floods destroy Base stations, fires burn servers. No forward planning can be done, and the set-up must be externally fast and reliable. The same applies to many military activities, which are, to be honest, one of the major driving forces behind mobile ad-hoc networking research [9].

Effectiveness: Service provided by existing infrastructure might be too expensive for certain

applications. If, for example only connection oriented cellular network exist, but an application sends only small status information every other minute, cheaper ad-hoc packet-oriented network might be a better solution. Registration procedure might take too long and communication overheads might be too high with existing networks. Tailored ad- hoc networks can offer a better solution [5].

Remote Areas: Even if infrastructure could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely populated areas. Depending on the communication pattern, so ad-hoc networks or satellite infrastructure can be a solution [9].

Other applications of wireless ad-hoc networking are Due to their quick and economically less demanding deployment, this network finds applications in several areas. Some of these include: military applications, collaborative and distributed computing, emergency operations, wireless mesh networks, wireless sensor networks, and hybrid wireless network [6].

II. Chalanges of Manet

The major issues that affect the design, deployment, performance of an ad-hoc network wireless system are as follows:

Packet losses due to transmission errors:- Mobile ad hoc network experiences a much higher packet losses due to some factors such as high bit error rate (BER) in the wireless channel, increased collision due to the hidden terminal problem, presence of interference, location dependent contention, unidirectional links, frequent path break due to node mobility and the inherent fading property of wires medium [6].

Route changes due to mobility: The network topology in an ad-hoc wireless network is highly dynamic due to mobility of nodes; hence an on-going session may suffer from frequently path breaking. This session often leads to frequent route changes therefore mobility management itself is very vast research topic in ad-hoc networking [7]. Security issues: The radio channel is used for ad-hoc wireless network is broadcast in nature and is shared by all the nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So attacker can easily snoops the data being transmitted by a node in the network. Here the Requirement for confidentiality can be violated if an adversary is able to interpret the data gathered through snooping [6].

Limited wireless transmission range: In wireless network the radio band will be limited and hence data rates it can offer are much lesser than what a wired network can offer. This requires an optimal manner by keeping the overhead as low as possible [6].

Routing overhead: In wireless ad hoc networks, nodes often change their location within the network. So stales route are generated in the routing tables which lead to unnecessary routing overhead.

Battery constraints: This is one of the limited resources that form a major constraint for the node in an ad hoc network. Devices used in these networks have restriction on the power source in order to maintain portability, size, and weight of the device. [7].

Potentially frequent network partition:- The randomly moving nodes in an ad- hoc can lead to network partition. In major cases the intermediate nodes are the one which are highly affected by this partitioning [7].

Asymmetric links: Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad hoc networks as the nodes are mobile and constantly changing their position within network. Consider a MANET where node c sends a signal to node B but does not tell anything about the quality connection in the reverse direction [8].

III. Classification of Routing Protocols

Ad-hoc network routing protocols may be classified in many ways depending on their routing algorithm, network structure communication model, and state of information etc, but most of the protocols depending on their routing algorithm, and network structure [3][10].

Based on the network structure ad-hoc network classify as Flat routing, hierarchical routing, geographical position assisted routing. Flat routing covers two types of routing protocols based on routing algorithm.

Based on the Routing algorithms, routing protocols are classified as Proactive routing protocols and Reactive Routing protocols.

- Proactive Routing: DSDV (Destination Sequence Distance Vector Routing)
- Reactive Routing: AODV (Ad-hoc on-demand distance vector routing protocol), DSR (Dynamic source routing)

DSDV:-DSDV destination sequenced distance vector routing protocol is a table driven algorithm based on the classical Bellman – Ford routing mechanism. The improvement is made include freedom from loops in routing tables. Every mobile node in the network maintains a routing table for all possible destinations within the network and the number of hops to each destination node. Each entry is marked with a sequence number, number assigned by the destination node Routing table updates are periodically transmitted throughout the network in order to maintain table consistency.

Large amount of network traffic, route updates can employ in two types of packets they are first is the "Full Dump" and second is the "Incremental routing". A full dump sends the full routing table to the neighbors and could cover many packets whereas, in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. When the network is relatively stable, incremental updates are sent to avoid extra Traffic and full dump are relatively infrequent. In a fast changing network, incremental packets can grow big, so full dumps will be more frequent [13].

AODV: The AODV is a Reactive on demand ad-hoc distance vector routing algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on demand basis as opposed to maintaining a complete list of routes, as in the DSDV algorithm. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the destination. In AODV each router maintains route table entries with the destination IP address, destination sequence number, hop count, next hop ID and lifetime [11].

RREQs route requests and RREPs route replies are the two message types defined by the AODV. When a route to a new destination is needed, the node uses a broadcast RREQ to find a route to destination. A route can be determined when the request reaches either the destination itself or an intermediate node with a fresh route to the destination. The route is made available by unicasting a RREP back to the source of RREQ. Each node maintains its own broadcast id, sequence number. The broadcast ID is incremented for every RREQ packet. Since each node receiving the request keeps track of a route back to the source of the request, the RREP reply can be unicast back from the destination to the source, or from any intermediate node that is able to satisfy the request back to the source [10].

IV. Simulation Based Analysis

This section described the simulation tool, network setup, Simulation parameters and simulation results. The performances of proactive and reactive routing protocols are evaluated on the basis of three performance metrics: Throughput, Packet delivery ratio, Routing overhead.

a) Simulation Tool

In this paper simulation of proactive and reactive routing protocols is done by using network simulator (NS2) software due to its simplicity and availability. NS is a discrete event Simulator targeted at networking research. NS provides substantial support for simulation of TCP, routing, and multicast routing protocols over a wired and wireless network. NS2 is written in C++ and OTCL. C++ for data per event packets and OTCL are used for periodic and triggered event. NS2 include a network animator called network animator which provides visual view of simulation. NS2 preprocessing provides traffic and topology generation and post processing provide simple trace analysis. AWK programming is used for trace file analysis.

b) Network Setup and Simulation Parameters

The following network setup and simulation parameters are used in this paper to analyze the performance of proactive and reactive routing protocols.

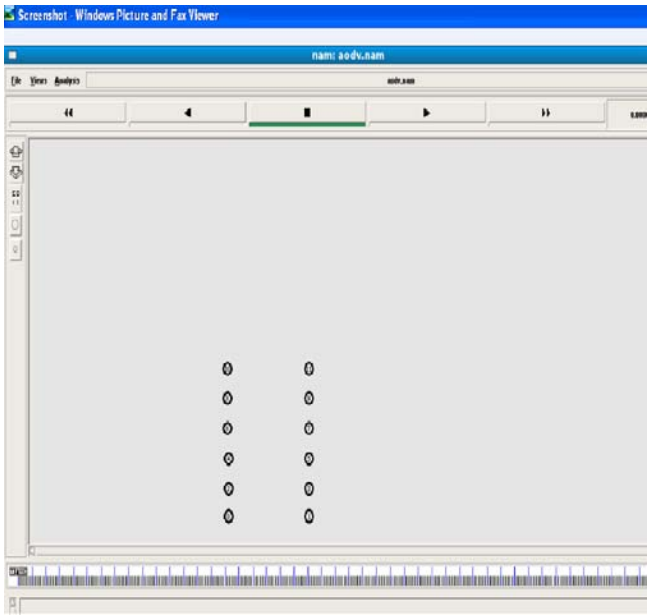


Fig. 1 : Network Setup

This topology is consists by 12 nodes, where 6 nodes are senders and remaining are receivers. All the senders start traffic at different time. So the transmitting node share the channel bandwidth with other previous transmitting nodes. This topology is generated by the network animator, by considering the following simulation parameters table.

Table 1 : Simulation Parameters

Channel	Channel/Wireless Channel
Propagation	Propagation/Two ray ground
Network interface	Phy/WirelessPhy
NS version	NS-allinone-2.31
MAC	Mac/802_11
CBR Packet Size	512 bytes
Interface Queue	Queue/Droptail/PriQueue
Link layer	LL
Antenna	Antenna/Omni Antenna
Interface Queue Lenth	50
No. of nodes	12 (6-senders, 6-eceivers)
Simulation area size	700*600
Simulation duration	60 second
Routing protocols	AODV, DSDV
Performance Metrics	Throughput, Packet Delivery Ratio, Routing Overhead

c) Performance Metrics

The following metrics are used in this paper for the performance analysis of AODV, DSDV Routing protocols. These are:

i. Throughout: It is the amount of data transferred over the period of time expressed in bits per second.
ii. Packet delivery ratio: It is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node.
iii. Routing Overhead: The number of control packets generated by each routing protocol.
iv. Average end to end delay:

d) Simulation Results

The simulation results are shown in the following section in the form of graphs and charts. In this paper an attempt has been made to evaluate the performance of two well known routing protocol DSDV, AODV according to his simulation results. The simulation results are genrated through the Excel graphs according to above mentioned criteria shown in table.

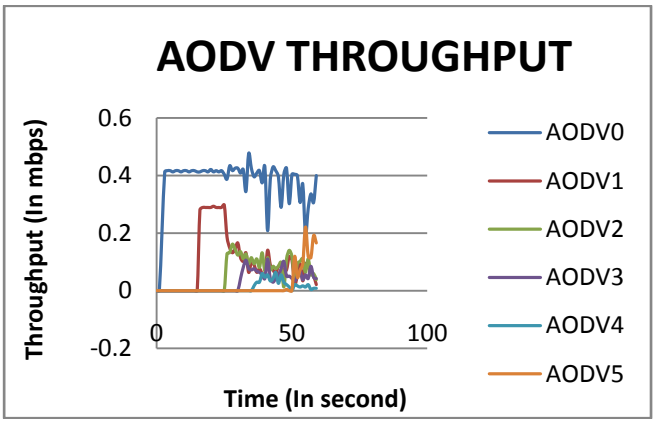


Fig. 2 : AODV Throughput (Node= 12)

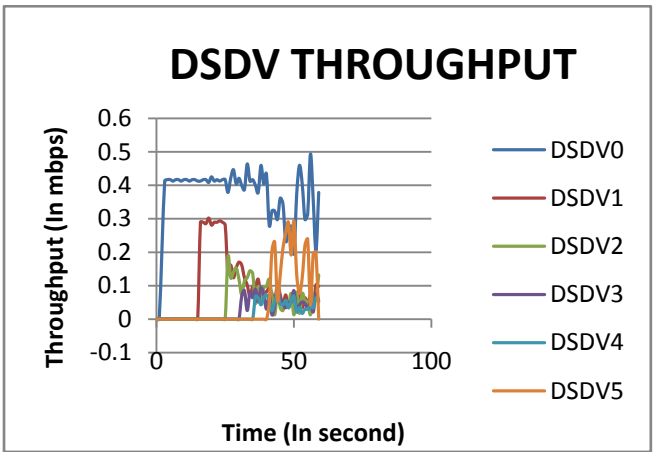


Fig. 3 : DSDV Throughput (Node =12)

According to above all 'Throughput graphs' and 'network topology' the 6 nodes are sender and remaining are receivers. First node start traffic at 1.5 second and utilize the full channel bandwidth. So the throughput of first node is gretter than others nodes.

After Second node start the traffic at 15 second and this node shares the channel banwidth with first node. So the throughput of second node is lower than first node because of late starting of traffic and throughput of first node is also decresed because of sharing bandwidth.

Similerly third node start traffic at the 25 second then the three nodes share the channel bandwidth. so the throughput of first two nodes are gretter, and third node's throughput is lower because of late starting of traffic and sharing of bandwidth.

Similerly fourth node, fifth node, and sixth node start traffic at 30 second, 35 second, and 40 second. if we increase the no. of senders and receivers and increse the traffic between sender and receivers, the throughput is decreses of all the senders and receivers.

On the basis of above graph, it is observed that the throughput of AODV is better than DSDV.

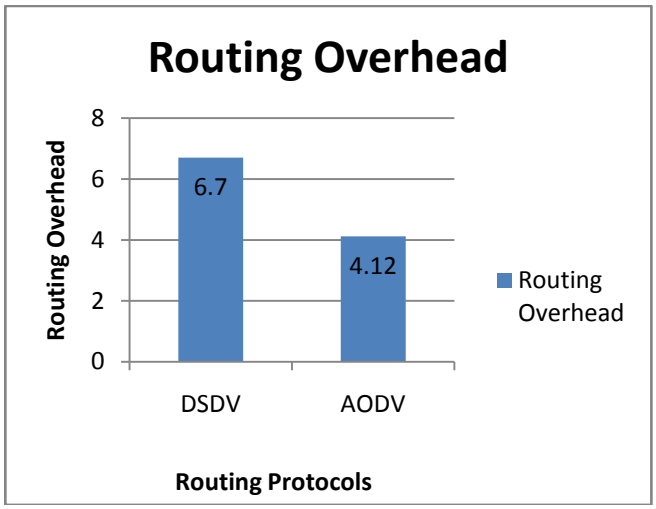


Fig. 4 : Routing overhead of (DSDV, AODV)

According to above Routing overhead chart, The Routing overhead of DSDV Routing protocol is maximum, and the AODV routing protocol is minimum.

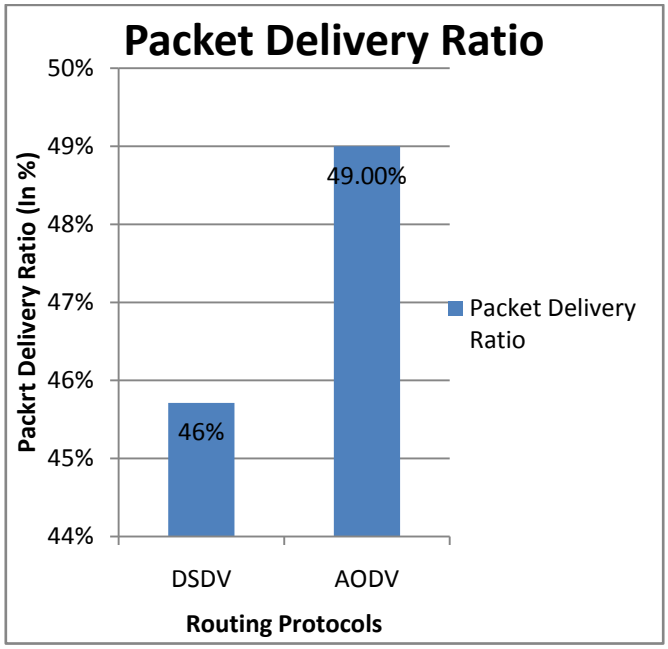


Fig. 5 : Packet Delivery Ratio For (DSDV, AODV)

According to above packet delivery ratio graph, the packet delivery ratio of DSDV is minimum, and AODV is maximum.

V. Conclusions

In this paper, the performance evaluation of AODV and DSDV routing protocols is done in the above mentioned criteria. The simulation results of all Excel graphs provide the information that if the number of nodes increases in the transmission then the throughput decreases. First graph shows that AODV throughput is better than DSDV because of his consistent performance. Second graph shows that AODV has minimum routing overhead and DSDV has maximum routing overhead. Third graph shows that AODV provides highest packet delivery ratio and DSDV provides lowest packet delivery ratio. In the analyzed scenario, it is found that the overall performance of AODV is better than 'DSDV'.

References Références Referencias

1. David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. Technical report, Carnegie Mellon University, 1996.
2. Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollong, NSW 2522. Motorola Australia Research Centre, 12 Lord st., Botany , NSW 2525, Australia, 2003.
3. Xiaoyan Hong, Kaixin Xu, and Mario Gerla. Scalable routing protocols for mobile ad hoc networks. 2002.
4. Integration of mobile ad-hoc networks, EU project DAIDALOS, Susana Sargento, Institute of Telecommunications.
5. Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing Jun-Zhao Sun MediaTeam,Machine Vision and Media Processing Unit.
6. C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition,Low price Edition, Pearson Education, 2007.
7. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010"ANALYZING THE MANET VARIATIONS, CHALLENGES, CAPACITY AND PROTOCOL ISSUES" G. S. Mamatha1 and Dr. S. C. Sharma
8. Jochen Schiller. Mobile Communications. Addison-Wesley, 2000.
9. Krishna Moorthy Sivalingam, "Tutorial on Mobile Ad Hoc Networks", 2003.
10. Elizabeth M. Royer and Chai-Keong Toh. A review of current routing protocols for adhoc mobile wireless networks.Technical report, University of California and Georgia Institute of Technology, USA, 1999.
11. Mobile Ad Hoc Networking Working Group – AODV, http://www.ietf.org/rfc/rfc3561.txt
12. Mobile Ad Hoc Networking Working Group – DSR, http://www.ietf.org/rfc/rfc4728.txt.
13. "Wireless Ad Hoc Networks" Zygmunt J. Haas, Jing Deng, Ben Liang, Panagiotis Papadimitratos, and S. SajamaCornell University School of Electrical and Computer Engineering
14. Nsnam web pages: http://www.isi.edu/nsnam/ns/
15. IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009 261"PerformanceEvaluation of AODV, DSDV & DSR

Routing Protocol in Grid Environment" Nor Surayati Mohamad, Usop Azizol Abdullah, Ahmad Faisal Amri Abidin.

16. Tutorial for Simulation-based Performance Analysis of MANET Routing Protocols in ns-2By Karthik sadasivam.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Shallow Water Acoustic Networking [Algorithms & Protocols]

By Rohini Avinash Nere & Mrs. Uma Nagraj

Maharashtra Academy Alandi Pune

Abstract - Acoustic networks of autonomous underwater vehicles (AUVs) cannot typically rely on protocols intended for terrestrial radio networks. This work describes a new location-aware source routing (LASR) protocol shown to provide superior network performance over two commonly used network protocols—flooding and dynamic source routing (DSR)—in simulation studies of underwater acoustic networks of AUVs. LASR shares some features with DSR but also includes an improved link/route metric and a node tracking system. LASR also replaces DSR's shortest-path routing with the expected transmission count (ETX) metric. This allows LASR to make more informed routing decisions, which greatly increases performance compared to DSR. Provision for a node tracking system is another novel addition: using the time-division multiple access (TDMA) feature of the simulated acoustic modem, LASR includes a tracking system that predicts node locations, so that LASR can proactively respond to topology changes. LASR delivers 2-3 times as many messages as flooding in 72% of the simulated missions and delivers 2–4 times as many messages as DSR in 100% of the missions. In 67% of the simulated missions, LASR delivers messages requiring multiple hops to cross the network with 2–5 times greater reliability than flooding or DSR.

Keywords : *acoustic network, auv, under water communication.*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

Shallow Water Acoustic Networking [Algorithms & Protocols]

Rohini Avinash Nere[α] & Mrs. Uma Nagraj[σ]

Abstract - Acoustic networks of autonomous underwater vehicles (AUVs) cannot typically rely on protocols intended for terrestrial radio networks. This work describes a new location-aware source routing (LASR) protocol shown to provide superior network performance over two commonly used network protocols—flooding and dynamic source routing (DSR)—in simulation studies of underwater acoustic networks of AUVs. LASR shares some features with DSR but also includes an improved link/route metric and a node tracking system. LASR also replaces DSR's shortest-path routing with the expected transmission count (ETX) metric. This allows LASR to make more informed routing decisions, which greatly increases performance compared to DSR. Provision for a node tracking system is another novel addition: using the time-division multiple access (TDMA) feature of the simulated acoustic modem, LASR includes a tracking system that predicts node locations, so that LASR can proactively respond to topology changes. LASR delivers 2-3 times as many messages as flooding in 72% of the simulated missions and delivers 2–4 times as many messages as DSR in 100% of the missions. In 67% of the simulated missions, LASR delivers messages requiring multiple hops to cross the network with 2–5 times greater reliability than flooding or DSR.

Keywords : acoustic network, auv, under water communication.

I. Introduction

As autonomous underwater vehicles (AUVs) continue to become less expensive and more capable, they are being deployed in larger groups. As a result, the need to communicate between multiple, mobile underwater systems is growing as well. Underwater communication is best accomplished through the use of acoustic links, and interconnecting multiple underwater vehicles is best accomplished through the use of an acoustic network. Such a network, one using a shared medium and comprising mobile nodes, is called a mobile ad hoc network (MANET). It is difficult to efficiently forward data across a MANET because node mobility means network topology—the overall set of connections between nodes—changes over time. The network must spontaneously organize, learn the topology, and begin routing with a minimum of overhead traffic for route discovery and maintenance. There has been a great deal of attention paid to this problem, but almost exclusively as it applies to wireless radio networks [1–4].In a network, a node is a communication endpoint able to send and receive data.

Author α σ : Department of computer engineering, Maharashtra academy of engineering alandi pune. E-mail : rohini.nere9@gm ail.com

When two nodes can communicate with one another, they are said to have a link between them. Links can be of varying quality: some links may deliver almost every message without error, others may deliver only a small fraction of the messages sent across them. In shared-medium communications like underwater acoustics, every transmission has exactly one sender but can have one or more receivers.A message may have to be forwarded across one or more links to intermediate nodes before reaching its intended destination. Routing is the process of choosing the links that will comprise the route the message will follow across the network. A routing protocol is responsible for selecting the route. Most routing protocols collect, manage, and disseminate information about the network in order to function, for example, by monitoring network topology, specifying the next hop of a message, queuing messages awaiting routes, and tracking which messages have already been processed. Unlike in a traditional, wired network, routing in a mobile ad hoc network (MANET) is complicated by the possibly rapid and unpredictable topological changes caused by movement of the nodes. A given routing protocol is typically intended for a particular type of network, and many have been developed specifically for MANETs [5–9].Little of the existing research into MANET routing protocols addresses the specific limitations of underwater acoustics [10]. While few MANETs are as drastically low-bandwidth as an underwater acoustic network, many have little bandwidth when compared with wired networks, and some MANET techniques specifically address this by reducing protocol overhead [11–13]. The greater problem is that the existing research assumes—almost without exception—that wireless networks in general, and MANETs in particular, use radio links. The particular problem is the speed of the nodes compared to the communication latency. Most advanced routing protocols need to propagate topology information throughout the network. The high latency of acoustic links means that the movement of underwater vehicles can change the network topology more quickly than updates can be propagated. This is especially a problem for protocols developed for radio MANETs, which overall assume a much slower rate of topology change compared to communication latency [11–17].This paper describes the location-aware source routing (LASR) protocol, a network routing protocol specifically designed for use in low-bandwidth, high-

latency underwater acoustic networks of mobile nodes. LASR is loosely based on the dynamic source routing (DSR) [9] protocol and is specifically designed for use in underwater acoustic networks where the topology changes frequently. The results presented here show that, in simulated underwater acoustic networks of AUVs, LASR outperforms both blind flooding and DSR in throughput and packet delivery ratio. Note that LASR is intended for use in missions where vehicle movement dominates energy consumption, so that it maximizes successful communication rather than energy conservation. A performance comparison between protocols in terms of energy consumption is not the focus of this publication, but it is an important future study.The remainder of this paper is organized as follows. Related work is discussed in Section 2. The new LASR protocol is described in Section 3. Specifics of handling routes and messages are covered in Section 4. Section 5 presents some results of LASR in a simulated underwater network. Section 6 summarizes our conclusions.

II. Swan Communication Architecture

A TWO DIMENTIONAL ARCHI for ocean bottom monitoring. These are constituted by sensor nodes that are anchored to the bottom of the ocean. Typical applications may be environmental monitoring, or monitoring of underwater plates in tectonics.

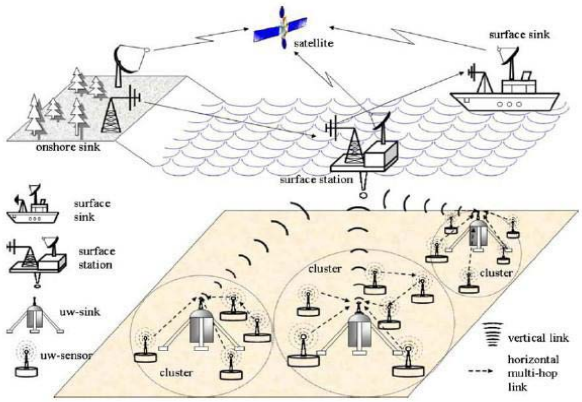


Fig. 1 : Two-dimensional underwater Sensor Networks

Reference architecture for two-dimensional underwater networks is shown in the figure above. A group of sensor nodes are anchored to the bottom of the ocean with deep ocean anchors. By means of wireless acoustic links, underwater sensor nodes are interconnected to one or more underwater sinks (uw-sinks), which are network devices in charge of relaying data from the ocean bottom network to a surface station. To achieve this objective, uw-sinks are equipped with two acoustic transceivers, namely a vertical and a horizontal transceiver. The horizontal transceiver is used by the uw-sink to communicate with the sensor nodes in order to: i) send commands and configuration data to the sensors (uw-sink to sensors); ii) collect monitored data (sensors to uw-sink)[9]. The vertical link is used by the uw-sinks to relay data to a surface station. Vertical transceivers must be long range transceivers for deep water applications as the ocean can be as deep as 10 km. The surface station is equipped with an acoustic transceiver that is able to handle multiple parallel communications with the deployed uw-sinks. It is also endowed with a long range RF and/or satellite transmitter to communicate with the onshore sink (os-sink) and/or to a surface sink (s-sink).

Sensors can be connected to uw-sinks via direct links or through multi-hop paths. In the former case, each sensor directly sends the gathered data to the selected uw-sink. This is the simplest way to network sensors, but it may not be the most energy efficient, since the sink may be far from the node and the power necessary to transmit may decay with powers greater than two of the distance.

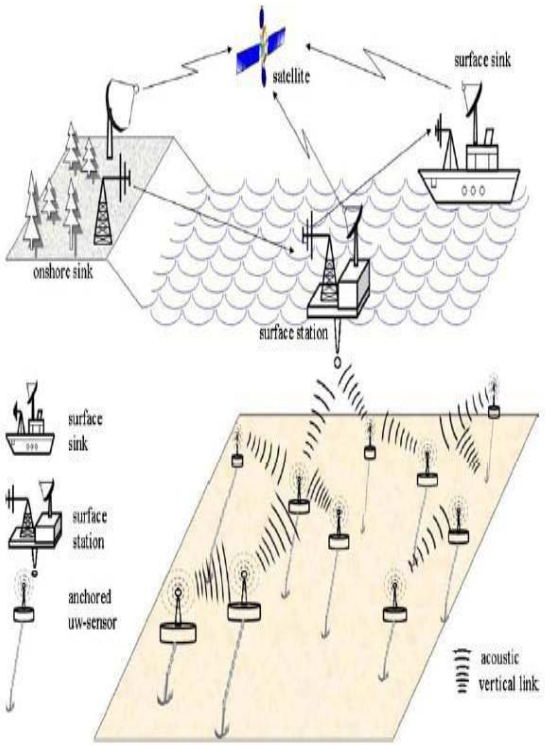


Fig. 2 : Three-dimensional underwater Sensor Network

Furthermore, direct links are very likely to reduce the network throughput because of increased acoustic interference due to high transmission power. In case of multi-hop paths, as in terrestrial sensor networks, the data produced by a source sensor is relayed by intermediate sensors until it reaches the uw-sink. This results in energy savings and increased network capacity, but increases the complexity of the routing functionality as well. In fact, every network device usually takes part in a collaborative process whose objective is to diffuse topology information such that

efficient and loop free routing decisions can be made at each intermediate node. This process involves signaling and computation. Since, as discussed above, energy and capacity are precious resources in underwater environments; in UW-ASNs the objective is to deliver event features by exploiting multi-hop paths and minimizing the signaling overhead necessary to construct underwater paths at the same time [9].

Three-dimensional networks of Autonomous Underwater Vehicles (AUVs).

These networks include fixed portions composed of anchored sensors and mobile portions constituted by autonomous vehicles. Three dimensional underwater networks are used to detect and observe phenomena that cannot be adequately observed by means of ocean bottom sensor nodes, i.e., to perform cooperative sampling of the 3D ocean environment. In three-dimensional underwater networks, sensor nodes float at different depths in order to observe a given phenomenon. One possible solution would be to attach each uw-sensor node to a surface buoy, by means of wires whose length can be regulated so as to adjust the depth of each sensor node. However, although this solution allows easy and quick deployment of the sensor network, multiple floating buoys may obstruct ships navigating on the surface, or they can be easily detected and deactivated by enemies in military settings. For these reasons, a different approach can be to anchor sensor devices to the bottom of the ocean. In this architecture, depicted in the figure above, each sensor is anchored to the ocean bottom and equipped with a floating buoy that can be inflated by a pump. The buoy pushes the sensor towards the ocean surface. The depth of the sensor can then be regulated by adjusting the length of the wire that connects the sensor to the anchor, by means of an electronically controlled engine that resides on the sensor. Many challenges arise with such an architecture, that needs to be solved in order to enable 3D monitoring, including:

Sensing coverage: Sensors should collaboratively regulate their depth in order to achieve full column coverage, according to their sensing ranges. Hence, it must be possible to obtain sampling of the desired phenomenon at all depths.

Communication coverage: Since in 3D underwater networks there is no notion of uw-sink, sensors should be able to relay information to the surface station via multi-hop paths. Thus, network devices should coordinate their depths such a way that the network topology is always connected, i.e., at least one path from every sensor to the surface station always exists.

Sensor Networks with Autonomous Underwater Vehicles (AUVs):

AUVs can function without tethers, cables, or remote control, and thus have a multitude of applications in oceanography, environmental monitoring, and underwater resource study. Previous experimental work has shown the feasibility of relatively inexpensive AUV submarines equipped with multiple underwater sensors that can reach any depth in the ocean hence, they can be used to enhance the capabilities of underwater sensor networks in many ways. The integration and enhancement of fixed sensor networks with

AUVs is an almost unexplored research area which requires new network coordination algorithms, such as:

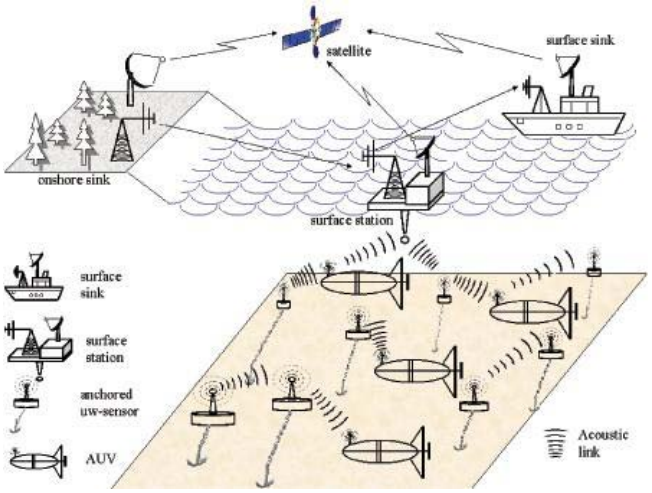


Fig. 3 : Three-Dimensional Sensor Network with AUVs

Adaptive sampling: This includes control strategies to command the mobile vehicles to places where their data will be most useful. This approach is also known as adaptive sampling and has been proposed in pioneering monitoring missions. For example, the density of sensor nodes can be adaptively increased in a given area when a higher sampling rate is needed for a given monitored phenomenon [9].

Self-Configuration: This includes control procedures to automatically detect connectivity holes due to node failures and request the intervention of an AUV. AUVs can either be used to deploy new sensors or as relay nodes to restore connectivity.

N easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

III. Routing Issues and Protocols

Y2.1. Medium Access Control Radio and acoustics are both shared medium techniques: multiple senders and receivers use the same medium (e.g., the water of the ocean) and there must be some sort of medium access control (MAC) to keep them from all "talking at once". Inherent in shared-medium systems is the problem of collision—the interference among multiple, simultaneously-received signals. A large number of MAC protocols have been developed, some better suited to mobile underwater acoustic use than

others [10, 18–24].Time-division multiple access (TDMA) divides the medium into time-slots [4]. Each node may use the entire bandwidth, but may only transmit according to a given schedule. LASR must use TDMA as its MAC protocol. The TDMA transmit-time information is what allows LASR to collect implicit time-of-flight information for the nodes in the network and is crucial for effective use of its tracking system.2.2. Blind Flooding Blind flooding is a network broadcasting protocol [4], and the simplest of the flooding protocols. It delivers its messages to every node in the network, and does so without knowledge of the topology. The basic operation is simple: the first time a node receives a given message, the node automatically rebroadcasts it. Because blind flooding does not require the topology to be known, many of the more-sophisticated routing protocols employ it before routes are known, for example, during route discovery. Blind flooding's advantages include operation without topological information and low end-to-end delay. The main disadvantage of blind flooding is that it can produce a significant amount of unnecessary traffic, especially as the size of the network increases.2.3. Shortest-Path Routing Flooding delivers a message by network broadcast, and every node in the network receives the message. This is very inefficient when the destination is a single node. An alternative is shortest-path routing, where a message follows the path with the fewest hops. This is much more efficient: rather than every node in the network forwarding the message to all its neighbors by broadcast, each node along the shortest path forwards the message to the next hop by unicast. However, this makes it necessary for the network nodes to have at least partial knowledge of the network topology. It is also important to avoid routing loops, which occur when mismatches in topology information across several nodes cause messages to be routed in circles. Examples of shortest-path routing include the Destination-Sequenced Distance Vector (DSDV) protocol [5], Ad hoc On-demand Distance Vector (AODV) [6], Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [8], and the Temporally-Ordered Routing Algorithm (TORA) [7]. Of particular interest here is the Dynamic Source Routing (DSR) protocol [9], a reactive protocol which, depending on the implementation, uses either distance-vector or link-state routing. In source routing, the entire route to the destination is determined by the originator (the source) and is carried along with the message. Routes are discovered as needed via a route-request/route-reply process, and there are no periodic updates.2.4. Delay-Tolerant Routing In some networks, there may never be an end-to-end connection. Instead, individual mobile nodes must hold data until a forwarding opportunity arises [25]. For example, a protocol can exploit vehicles' nonrandom mobility patterns to improve routing performance [26]. These routing techniques are not necessarily suitable to the cooperating-AUVs problem. When cooperating, the nodes will likely actively work to stay connected, that is, each node will maneuver such that it always stays within range of the network. More importantly, certain types of data do not need to be delivered immediately and can tolerate significant delay in their delivery, but when cooperating on short time-scales, some communication is very likely to be time-sensitive and delivery cannot wait long periods for an opportune vehicle motion to put it in range.2.5. Position-Based and Location-Aware Routing A routing protocol spends most of its time determining and tracking the network topology. With communication technologies such as radio and acoustics, which links are available largely depends on the distance between the various nodes. Some routing protocols use knowledge of the location of network nodes to provide or augment topology information. These are known as location-aware or position-based protocols. Routing by absolute geographical location typically employs a locating service that is queried by nodes to look-up the current location of a destination node. Messages are routed to the neighbor that is geographically nearest to the destination. Routing by relative location typically requires both relative location (e.g., range and bearing) as well as traditional topology information. LASR routes by relative location. A protocol similar to LASR is [27], which also estimates range from one-way time-of-flight using TDMA and uses it to discover network topology for routing via DSR. However, it includes pseudo noise probe patterns as a part of each frame because localization is of primary importance in that system. The network supports only very few nodes and the overall communication rate is extremely low. The new LASR protocol has been specifically designed to address the problems of routing in low-bandwidth, high-latency underwater acoustic networks of mobile nodes. It is loosely based on the DSR [9] protocol. Like DSR, LASR is a self-organizing, infrastructureless, distributed protocol. It learns and maintains only those routes that are in use. LASR uses the source route principally as a means to communicate topology information. Each intermediate node updates the source route in every message it forwards, applying the route most likely to require the fewest transmissions (which does not necessarily correspond to the fewest hops) to reach the destination. Every message transmission is therefore routed according to the most current topological knowledge, rather than DSR's approach which routes according to the topological knowledge at the time the message was originated.3.2. Assumptions The LASR protocol is designed for small underwater networks using low-speed acoustic links. The network should not contain more than 20–30 nodes, a reasonable assumption given typical multiple-AUV operations such as [28]. This network size limitation is due in lesser part to the source route header overhead in each message.

The size of the source route grows linearly with the length of the longest path through the network. In greater part, this assumption is due to LASR's required use of TDMA, which does not scale well into large networks. Nodes may move at any time and in any direction. The only restriction on node motion is that speeds should be in the range 0–3 m/s; this speed range is typical for most current AUVs. This assumption is necessary to limit the rate at which node motion can change the network topology. All nodes must use identical LASR algorithms, and all must fully participate in the protocol, including forwarding the messages of others. Every node must have accurate timekeeping, for example, by means of a low-drift clock. No two node clocks may differ by more than 50 milliseconds throughout a mission, although this network time may differ from true time by any amount. This is necessary for TDMA window timing. Equipped with the optional time synchronization feature, the FAU Dual Purpose Acoustic Modem (DPAM) fits this requirement over 8 hours using low-drift clocks [29]. Also, prior work [30] has shown that for LASR, this is the minimum timekeeping precision necessary to preserve the accuracy of the time-of-flight range estimates based on TDMA window timing. The communication link endpoints should be identical acoustic modems, and these modems should be effectively omnidirectional. They must support overhearing—the reception of messages not specifically addressed to them. Overhearing is an important source of topology information. To allow the tracking system to function, each modem must report the time at which any incoming transmission is detected, regardless of whether or not the transmission can be successfully decoded. The detection time reporting must be accurate to within 30 milliseconds. As with the timekeeping precision, this reporting precision has been shown [30] to be the minimum necessary for time-of-flight range estimate accuracy. LASR's implementation of ETX assumes that network links are bidirectional (acoustic modem links are traditionally bidirectional, albeit half-duplex) and symmetrical, meaning packets can cross the link between any pair of nodes in either direction with equal probability of success. In practice, the links are not perfectly symmetrical, but symmetry is a fair assumption so long as the transducer is assumed omnidirectional and the environmental conditions (and range between nodes) do not change significantly between two transmissions. The development of a nonsymmetrical and unidirectional version of LASR is beyond the scope of this article, but constitutes a future key for development of LASR. The links are assumed to be through a shared medium. The network must use TDMA as the MAC protocol so that implicit time-of-flight range estimate is possible. The ETX implementation also assumes that a medium model exists for the modem, which can provide a reasonably accurate estimate of the frame-error rate (FER) between two modems given the distance between them. The FER is the probability that a given transmission (a frame) on the link will be received in error. All nodes must use identical medium models and the FER estimate must be deterministic: every use of the model at every node must return the same FER for a given range. Note that the FER model includes other input parameters (sea state, ambient noise, water depth, bottom type …). A complete list is provided in [31]. The FER model used in the simulation was developed from field data [32]. For simplicity, the study assumes that every input parameter is constant, with the exception of range. These other parameters impact the FER, thus the LASR performance. At fixed range, the authors showed in [33] that the LASR performance drops with ambient noise and sea state, as the FER increases with these two parameters. A range-only tracking system is assumed to be available at each node. Regular measurements of the distance from the local node to each of the various other nodes within detection range will be available from a combination of the modem's transmission detection and TDMA window timing. The tracking system must use those time-of-flight based range measurements to predict the current location of those nodes relative to the local node. Prior work [30] has shown that the tracking system must predict relative node position to within 200 m of the true relative node position. If the estimated prediction error exceeds this amount for a given node, the tracking system must cease reporting the predicted position of that node.3.3. Link Metric The expected transmission count (ETX) [34] estimates the number of times a node will have to transmit a message before it successfully receives an acknowledgment. The ETX of a route is simply the sum of the ETXs of each link in the route, and any two ETX route metrics are directly comparable. The ETX is calculated from a link's FER. The technique described in [34] to calculate the ETX uses probe messages sent periodically across a link—once a sufficient number of probe messages have been sent, it is possible to estimate the link's FER, and then to calculate the ETX. In a MANET however, node motion can cause considerable variation in link quality over short time scales. This is a problem because, while ETX outperforms hop-count in a static network, hop-count can react more quickly to link changes and outperforms ETX when nodes are moving [35].LASR uses expected transmission count (ETX), but overcomes this mobile-node measurement-delay problem by calculating the delivery ratio directly from the FER estimated by the medium model. LASR assumes symmetric links, so the probability that a message and its acknowledgement will cross a link successfully is, making the equation for ETX:

How LASR handles the ETX information is described in Appendix B.3.4. Tracking System Neighborhood topology is predicted by the tracking

system based on information from both implicit and explicit communication. Combining the time-of-detection information from the modem with the current TDMA state provides both an estimated time-of-flight and the identity of the transmitter. The range to the transmitter can then be estimated using the medium model. A series of range estimates to other nodes, coupled with knowledge of a node's own motion, can form the basis for localization and tracking of the other nodes. When combined with minimal information from the other nodes about their ranges to each other, the relative, progressive location of the other nodes can usually be uniquely determined to some accuracy. A tracking system was not implemented as part of this work. The behavior of the tracking system was simulated based on the minimum established performance requirements. A recursive state-estimation filter, such as a particle filter, is expected to be able to localize and track some or all of the network nodes, depending on the amount of information available about each node. The more information that is available about another node, the more accurate tracking and location prediction can be. Even a low-order motion model (e.g., maximum, minimum, and typical speed and turning rate) will help constrain tracking and prediction uncertainty. A behavior model providing knowledge of the types of behaviors the node may exhibit (e.g., lawn mowing, line-following or hovering) can further reduce uncertainty. Information for tracking can be characterized as either explicit or implicit. Explicit information is carried as overhead in network messages. The LASR source routes, for example, carry explicit link range information. Implicit information is communicated without overhead, simply by the act of communicating. An example of implicit information is the time-of-flight measured when a message is received. Some modems, such as the FAU DPAM [31], preface each packet with a known sequence of symbols. The optional time synchronization feature of the FAU DPAM is used for TDMA communications and tracking [29]. This detection sequence is used by the receiver to identify an incoming transmission because, unlike the coded variable data in a message, the symbols in the detection sequence are known a priori, making them substantially easier to identify, even in very weak signals. It is frequently possible to correctly identify the detection sequence in transmissions from ranges far beyond the range at which there is sufficient signal to successfully decode the variable data. Under such modems, incoming transmissions fall into three categories: strong enough to decode (providing implicit range and explicit data), strong enough to detect but too weak to decode (providing implicit range only), and too weak to detect (providing nothing). Because the detection sequence can be reliably identified even across a link with an extremely high FER, the second category includes transmissions from nodes far beyond the useful explicit range of the modem. A comparison of implicit and explicit data is shown in Figure versus explicit data. Node transmits a message for node and each detect and receive it (the message is intended for but has overheard it). The detection provides an implicit range estimate to node; the reception provides all of the explicit routing information contained in the message (e.g., in the source route). Node detects but does not receive the message, thus gains an implicit range estimate to node

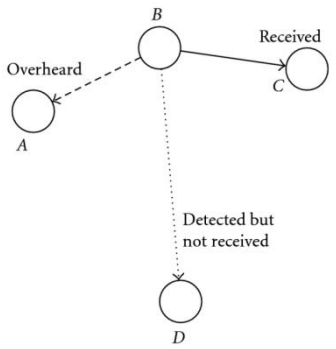


Fig. 1 : Implicite vs explicit data

But gets none of the explicit data.3.5. LASR Packet Structure Each LASR packet contains one or more messages. A message can contain user data or protocol data. A user-data message contains a source-route in addition to the user data. There are several protocol message types; these are described in Appendix A. Packets are small in a typical acoustic network, typically on the order of tens to hundreds of bytes only. This makes header overhead very expensive as even a small header can represent a large fraction of a packet. LASR uses a different header structure than DSR in order to reduce the size of the header as much as possible. LASR's header structure is shown.in

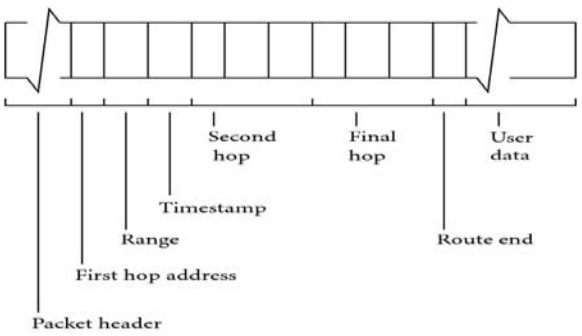


Figure 2 : Lasr header

The number of bits added to the header by a given layer can change from message to message. To accommodate this, the header is implemented as a stack of bits.7659: The LASR header is a variable-size stack of bits. This shows the source route portion of a three-hop route. A source route is structured as a series of triples followed by an end marker. Each triple is a hop

in the route starting at the originator and ending one hop before the destination. A triple comprises the address of the node, the best-available estimate of the range from the node to the next hop (or the destination) and the timestamp of the range estimate. Both the range and its timestamp are quantized to conserve space in the header, see [30] for details on the quantization. The route end is the special network address zero, which is never a valid address. The network addresses are represented as the smallest number of bits that can represent the number of nodes in the network, plus one for the special zero address. For example, a 16 node network would require 17 unique addresses and would therefore require 5-bit addresses.

IV. Network Design Challenges

a) Underwater Acoustic Sensor Networks: Design Challenges

In this section, we itemize the main differences between terrestrial and underwater sensor networks, detail the key challenges in underwater communications that influence protocol development, and give motivations for a cross-layer design approach to improve the efficiency of the communication process in the challenging underwater environment [5].

b) Differences with Terrestrial Sensor Networks

The main differences between terrestrial and underwater sensor networks can be outlined as follows:

- Cost. While terrestrial sensor nodes are expected to become increasingly inexpensive, underwater sensors are expensive devices. This is especially due to the more complex underwater transceivers and to the hardware protection needed in the extreme underwater environment [9].
- Deployment. While terrestrial sensor networks are densely deployed, in underwater, the deployment is generally more sparse.
- Power. The power needed for acoustic underwater communications is higher than in terrestrial radio communications due to higher distances and to more complex signal processing at the receivers to compensate for the impairments of the channel.
- Memory. While terrestrial sensor nodes have very limited storage capacity, uw-sensors may need to be able to do some data caching as the underwater channel may be intermittent.
- Spatial Correlation. While the readings from terrestrial sensors are often correlated, this is more unlikely to happen in underwater networks due to the higher distance among sensors.

Underwater acoustic communications are mainly influenced by path loss, noise, multi-path, Doppler spread, and high and variable propagation delay. All these factors determine the temporal and spatial variability of the acoustic channel, and make the available bandwidth of the Under Water Acoustic channel (UW-A) limited and dramatically dependent on both range and frequency. Long-range systems that operate over several tens of kilometers may have a bandwidth of only a few kHz, while a short-range system operating over several tens of meters may have more than a hundred kHz bandwidth. In both cases these factors lead to low bit rate [9].

Hereafter we analyze the factors that influence acoustic communications in order to state the challenges posed by the underwater channels for underwater sensor networking. These include:

c) Path loss

Attenuation: It is mainly provoked by absorption due to conversion of acoustic energy into heat, which increases with distance and frequency. It is also caused by scattering a reverberation (on rough ocean surface and bottom), refraction, and dispersion (due to the displacement of the reflection point caused by wind on the surface). Water depth plays a key role in determining the attenuation.

Geometric spreading: This refers to the spreading of sound energy as a result of the expansion of the wave fronts. It increases with the propagation distance and is independent of frequency. There are two common kinds of geometric spreading: spherical (Omni-directional point source), and cylindrical (horizontal radiation only).

d) Noise

Man made noise. This is mainly caused by machinery noise (pumps, reduction gears, power plants, etc.), and shipping activity (hull fouling, animal life on hull, cavitation), especially in areas encumbered with heavy vessel traffic.

Ambient Noise: Is related to hydrodynamics (movement of water including tides, current, storms, wind, rain, etc.), seismic and biological phenomena.

e) Multi-path

Multi-path propagation may be responsible for severe degradation of the acoustic communication signal, since it generates Inter-Symbol Interference (ISI).

The multi-path geometry depends on the link configuration. Vertical channels are characterized by little time dispersion, whereas horizontal channels may have extremely long multi-path spreads. The extent of the spreading is a strong function of depth and the distance between transmitter and receiver [9].

High delay and delay variance

The propagation speed in the UW-A channel is five orders of magnitude lower than in the radio channel. This large propagation delay (0.67 s/km) can reduce the throughput of the system considerably.

The very high delay variance is even more harmful for efficient protocol design, as it prevents from accurately estimating the round trip time (RTT), which is

the key parameter for many common communication protocols.

f) Doppler spread

The Doppler frequency spread can be significant in UW-A channels, causing degradation in the performance of digital communications: transmissions at a high data rate cause many adjacent symbols to interfere at the receiver, requiring sophisticated signal processing to deal with the generated ISI.

The Doppler spreading generates: i) a simple frequency translation, which is relatively easy for a receiver to compensate for; ii) a continuous spreading of frequencies, which constitutes a non-shifted signal, which is more difficult for a receiver to compensate for.

If a channel has a Doppler spread with bandwidth B and a signal has symbol duration T, then there are approximately BT uncorrelated samples of its complex envelope. When BT is much less than unity, the channel is said to be under spread and the effects of the Doppler fading can be ignored, while, if greater than unity, it is overspread [9].

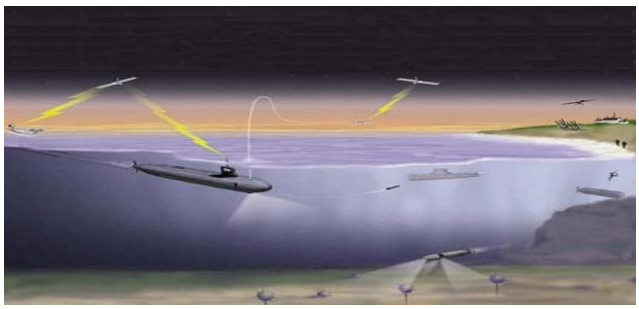
In the above sections the introduction, communication architectures and design challenges of the underwater acoustic network are discussed. Now in the further section some technologies for real-time monitoring of SWANs are discussed.

V. Realization of Underwater Networking

a) Realization of Underwater Networking

A realization of underwater acoustic networking is the U.S. Navy's experimental Telesonar and Seaweb program. Telesonar links interconnect distributed underwater nodes, potentially integrating them as a unified resource and extending naval net centric operations into the underwater battle space. Seaweb provides a command control, communications, and navigation infrastructure for coordinating autonomous nodes to accomplish given missions in arbitrary ocean environments. More generally Seaweb networking is applicable for oceanographic telemetry, underwater vehicle control, and other uses of underwater wireless digital communications. Telesonar and Seaweb experimentations address the many aspects of this problem including propagation, signaling, transducers, modem electronics, networking command-centre interfacing and transmission security. The major sea tests have included Seawebs '98,'99 and 2000[3].

Fig. 5 : Seaweb underwater acoustic networking enables data telemetry and remote control and other autonomous peripherals and Gateways



VI. New Protocol Results

This section discusses the simulation results for the new LASR protocol for underwater acoustic networks. The new protocol has been tested under a variety of simulated underwater missions, each in several operational scenarios. For comparison purposes, these tests are also conducted with the flooding and DSR protocols. The results demonstrate that the LASR protocol provides improved network communication performance compared to flooding and DSR.DSR is run without any of its optional features enabled as initial work demonstrated that each of the optional features negatively impacted DSR performance in an acoustic network. Three configurations of the LASR protocol are tested, which differ in number of retries and time spent waiting for acknowledgment. The LASR acknowledgment guarantee means that a receiver will acknowledge receipt within the specified time; this controls how much delay is introduced when a message, or its acknowledgment, fails to cross a link. The acknowledgment period is a multiple of the TDMA frame duration, to give each possible receiver some number of opportunities to transmit an acknowledgment (either implicit or explicit). The three LASR configurations are as follows. (a)LASR-0+3: no retries, unacknowledged messages are never retransmitted. However, receivers are still obligated to send an acknowledgment within three TDMA frames. (b)LASR-2+3: two retries, acknowledgment required within three TDMA frames. (c)LASR-2+6: two retries, acknowledgment required within six TDMA frames.5.1. Scenarios every scenario uses 16 vehicles, which is selected as an average network size for LASR. The parameters are exhaustively combined, with each combination defining a scene. Each scenario contains all scenes. Due to the stochastic nature of the communication model, each scene is run 20 times and the results averaged to smooth the performance results. The authors limit the study to 20 runs per scene due to computation time. This paper shows only a small fraction of the extensive simulation results; full results are available in [33].The vehicles originate messages

containing arbitrary data and send the messages to randomly chosen destinations. Every node transmits at every opportunity. If no message is ready to be sent when the node's transmission time-slot opened, a new message is generated by either the application layer or a protocol layer. Here, we assume that there is always at least one packet in the buffer of each transmitting node, with the objective to discover the maximum possible throughput (in practice, the LASR performance is also related to the mean packet generation rate). The random selection of the destination node is according to a uniform distribution: each node (except the originating node itself) has an equal probability of being selected as the destination. This means the network had full utilization at all times: there is never a TDMA time-slot that passes without a transmission, either to forward a protocol or user-data message or to originate a new user-data message. Each vehicle is equipped with an FAU dual-purpose acoustic modem (DPAM). Every modem uses Frequency-Hopped, M-ary Frequency Shift Keying (FH-MFSK) modulation with convolutional coding [31]. Packets are fixed-size, carrying 32 source bytes each. Each transmission takes 2.65 s and has a guard time of 2.35 s, for a total TDMA time-slot duration of 5 s. The FER is determined at run-time using the FAU DPAM medium model [32], a stochastic model derived from the Nakagami model, which considers channel geometry, fading characteristics, background noise, bottom type, modulation, and error coding. The network simulation tool was developed at FAU and is described in detail in [32, 33]. The best-case conditions for communication are when Nakagami-m is 2.0 and noise PSD is -55dB/√ Hz, the worst-case when Nakagami-m is 1.5 and noise PSD is 65dB/√Hz.7.2. Graph Methodology There are two graphed network metrics: messages-delivered versus range and message success ratio. These metrics measure different aspects of the network performance: messages-delivered measures throughput, success ratio measures reliability. Note that every message size is fixed to 32 bytes, so that the message-based analysis can be easily converted to a byte-based analysis. The graphs count as delivered or successful only unique user-data messages that reach the intended destination. User-data messages which never reached their destination, duplicate user-data messages received at the destination and protocol-only messages are not counted as delivered or successful. The uncounted messages are the protocol's message overhead. The messages-delivered graphs show the total number of originated user-data messages that are successfully delivered versus the distance between the originating node and the delivery node at the time of message origination. It does not consider protocol messages (e.g., route requests and route replies) and counts only messages containing user data. The successful delivery of a protocol message is not counted towards messages-delivered, so in general, the greater a protocols message overhead, the lower its messages-delivered count. These graphs provide a measure of throughput versus range. The messages-delivered graphs should be consulted if throughput is of primary importance, especially if the loss of packets can be tolerated. The delivery success ratio graphs show the ratio of user-data messages successfully delivered to user-data messages originated. Again, only user-data messages are considered. This ratio is graphed versus the same distances as the messages-delivered graphs. Messages still in the network when the simulation ends are considered lost, and so reduce the success ratio. This metric provides a measure of reliability versus range, that is, the probability that a user-data message sent over a given range will eventually be delivered. The success ratio graphs should be consulted if assured delivery is of primary importance, especially if a loss of throughput can be tolerated. Note that it is not valid to assume that delivering a greater volume of messages implies that messages are also delivered with greater reliability, or vice versa. They are commonly inversely related because increasing the delivery reliability generally requires increasing protocol overhead, which reduces the total number of messages that can be delivered for a given network bandwidth. A protocol with little overhead may be able to send a tremendous number of user-data messages, losing most but still delivering a large number. On the other hand, a protocol with large overhead may be able to send only a few user-data messages, but may deliver almost all of them. These metrics both count messages, not bytes. Larger packets would likely increase byte throughput but are also likely slightly decrease both messages-delivered and message success ratio because larger packets would take longer to transmit, thus lengthening the TDMA window, and would probably increase the FER of the links.

VII. Conclusion

In this paper we discussed introductory part of Shallow water acoustic network, its different architectures-Two dimensional underwater sensor network and three dimensional underwater sensor networks. Also we compare underwater acoustic network with the terrestrial sensor network and found challenges for implementing under water sensor network. Underwater acoustic communications are mainly influenced by path loss, noise, multi-path, Doppler spread, and high and variable propagation delay. Over the next decade, significant improvements are anticipated in the design and implementation of shallow water acoustic networks as more experience is gained through at-sea experiments and network simulations.

References Références Referencias

1. J. J.-N. Liu and I. Chlamtac, "Mobile Ad Hoc networking with a view of 4Gwireless: Imperatives and challenges," in Mobile Ad Hoc Networking, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic,Eds., chapter 1, pp. 1–45, Wiley-Interscience, 2004.
2. J. P. Macker and M. S. Corson, "Mobile Ad Hoc networks (MANETs): routing technology for dynamic wireless networking," in Mobile Ad Hoc Networking, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Eds., chapter 9, pp. 255–273, Wiley-Interscience, 2004.
3. R. Rajaraman, "Topology control and routing in Ad Hoc networks: a survey," SIGACT News, vol. 33, no. 2, pp. 60–73, 2002. S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Eds., Ad Hoc Networking, Wiley-Interscience, 2004.
4. C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94), pp. 234–244, ACM Press, New York, NY, USA, 1994. E. M. Belding-Royer and C. E. Perkins, "Evolution and future directions of the Ad Hoc on-demand distance-vector routing protocol," Ad Hoc Networks, vol. 1, no. 1, pp. 125–150, 2003.
5. View at Publisher • View at Google Scholar • View at ScopusR. Ogier, F. Templin, and M. Lewis, "Topology dissemination based on reverse-path forwarding (TBRPF)," RFC 3684, IETF MANET Working Group, February 2004.
6. V. D. Park and M. S. Corson, "Highly adaptive distributed routing algorithm for mobile wireless networks," in Proceedings of the 16th IEEE Annual Conference on Computer Communications (INFOCOM '97), pp. 1405–1413, April 1997.
7. View at ScopusD. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The dynamic source routing protocol for mobile Ad Hoc networks (DSR)," INTERNET-DRAFT, IETF MANET Working Group, July 2004.
8. E. M. Sozer, M. Stojanovic, and J. G. Proakis, "Underwater acoustic networks," IEEE Journal of Oceanic Engineering, vol. 25, no. 1, pp. 72–83, 2000.
9. View at Publisher • View at Google Scholar • View at ScopusH. Ju, I. Rubin, K. Ni, and C. Wu, "A distributed mobile backbone formation algorithm for wireless Ad Hoc networks," in Proceedings of the 1st International Conference on Broadband Networks (BroadNets '04), pp. 661–670, October 2004.
10. View at ScopusM. K. Marina and S. R. Das, "Performance of route caching strategies in dynamic source routing," in Proceedings of the International Conference on Distributed Computing Systems Workshop, pp. 425–432, 2001.
11. B. C. Seet, B. S. Lee, and C. T. Lau, "Optimisation of route discovery for dynamic source routing in mobile Ad Hoc networks," Electronics Letters, vol. 39, no. 22, pp. 1606–1607, 2003.
12. View at Publisher • View at Google Scholar • View at ScopusF. Bai, N. Sadagopan, B. Krishnamachari, and A. Helmy, "Modeling path duration distributions in MANETs and their impact on reactive routing protocols," IEEE Journal on Selected Areas in Communications, vol. 22, no. 7, pp. 1357–1373, 2004. View at Publisher • View at Google Scholar • View at Scopus.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Efficient Authentication in RFID Devices Using Et Al's Algorithm

By Vinita Sharma, Jitendra Kumar Gupta & K. K. Mishra

SR Group of Institution, CSE Campus Jhansi, India

Abstract - Security plays a vital role during the transmission of private data from one sender to the other. Although there are many security algorithms implemented but here we are providing the security algorithms on the RFID devices. The authentication techniques implemented in RFID is based on the new algorithm based on smart cards. The data send through the tags can be made secure using the proposed algorithm so that the un-authorised users can't access the data without any further unique numbers.

Keywords : *RFID, tags, reader, authentication, counterfeiting, privacy, security.*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

Efficient Authentication in RFID Devices Using Et Al's Algorithm

Vinita Sharma[α], Jitendra Kumar Gupta[σ] & K. K. Mishra[σ]

Abstract - Security plays a vital role during the transmission of private data from one sender to the other. Although there are many security algorithms implemented but here we are providing the security algorithms on the RFID devices. The authentication techniques implemented in RFID is based on the new algorithm based on smart cards. The data send through the tags can be made secure using the proposed algorithm so that the un-authorised users can't access the data without any further unique numbers.

Keywords : RFID, tags, reader, authentication, counterfeiting, privacy, security.

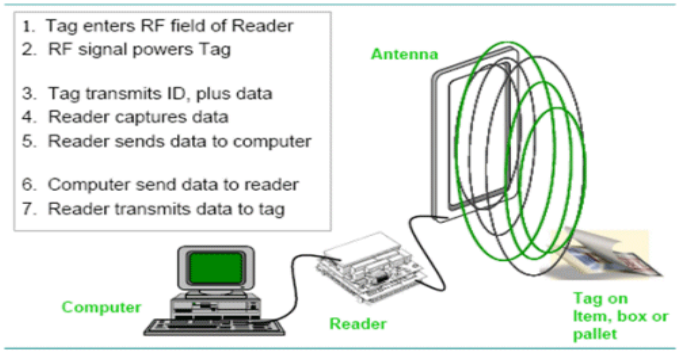
I. Introduction

Radio Frequency Identification (RFID) system is the latest technology that plays an important role for object identification as ubiquitous infrastructure. RFID has many applications in access control, manufacturing automation, maintenance, supply chain management, parking garage management, automatic payment, tracking, and inventory control.

RFID tag: is a tiny radio chip that comprises a simple silicon microchip attached to a small flat aerial and mounted on a substrate. The whole device can then be encapsulated in different materials (such as plastic) dependent upon its intended usage. The tag can be attached to an object, typically an item, box, or pallet, and read remotely to ascertain its identity, position, or state. For an active tag there will also be a battery. Reader or Interrogator: sends and receives RF data to and from the tag via antennas. A reader may have multiple antennas that are responsible for sending and receiving radio waves.

RFID offer several advantages over barcodes: data are read automatically, line of sight not required, and through non conducting materials at high rate and far distance. The reader can read the contents of the tags by broadcasting RF signals via antennas. The tags data acquired by the readers is then passed to a host computer, which may run middleware (API). Middleware offers processing modules or services to reduce load and network traffic within the back-end systems. RFID basic operations can be summarized as in Figure.

RFID systems are vulnerable to a broad range of malicious attacks ranging from passive eavesdropping to active interference. Unlike in wired networks, where computing systems typically have both centralized and host-based defenses (e.g. firewalls), attacks against RFID networks can target decentralized parts of the system infrastructure, since RFID readers and RFID tags operate in an inherently unstable and potentially noisy environment. Additionally, RFID technology is evolving quickly – the tags are multiplying and shrinking - and so the threats they are susceptible to, are similarly evolving.



Basic Operations of RFID

RFID tags may pose a considerable security and privacy risk to organizations and individuals using them. Since a typical tag answers its ID to any reader and the replied ID is always the same, an attacker can easily hack the system by reading out the data of a tag and duplicating it to bogus tags. Unprotected tags may have vulnerabilities to eavesdropping, location privacy, spoofing, or denial of service (DoS). Unauthorized readers may compromise privacy by accessing tags without adequate access control. Even when the content of the tags is protected, individuals may be tracked through predictable tag responses.

a) Security Issues

1. Security of the tag and the reader as well as the server: As the data from tag moves to the reader, security has to be maintained during the flow of data. Hence the security is maintained at the tag and the reader for the better efficiency of the data.
2. The original data stored at the receiver side: The original data from the tag is readed by the reader and is stored at the server, if the server can be accessed in an unauthorized manner and if the server damages the data will be lost, hence chances of fault tolerance.

Author α : M,Tech Scholar, Department of Computer Science & Engineering, SR Group of Institution, CSE Campus Jhansi, India.
Author σ : Assistant Professor, Department of Computer Science & Engineering, SR Group of Institution, CSE Campus Jhansi, India.

3. Low computational and storage cost: During the manufacturing of tag and the reader devices various functions have been designed for the better authorization of the data, hence when this function are been implemented the tag and the reader should not increase the computational and the storage cost.
4. Various security features implemented in various protocols: The table shown below is the various security features that are implemented in various protocols used in RFID devices. Hence the protocol that doesn't contain these security features is not very efficient and can be attacked by the external or internal user.
5. Chances of eavesdropping: The protocols that are implemented for the security of the data from tag to reader should be authenticated so that the chance of eavesdropping has been reduced.
6. Synchronization between tag and the reader: Synchronization between the tag and the reader is the flow of control from tag to the reader. The data moved from tag to the reader should be synchronized such that the data can't be lost and the chance of congestion has been reduced.

b) Performance

RFID schemes cannot use computationally intensive cryptographic algorithms for privacy and security because tight tag cost requirements make tag-side resources (such as processing power and storage) scarce.

- **Capacity minimization:** The volume of data stored in a tag should be minimized because of the limited size of tag memory.
- **Computation minimization:** Tag-side computations should be minimized because of the very limited power available to a tag.
- **Communication compression:** The volume of data that each tag can transmit per second is limited by the bandwidth available for RFID tags [4, 18].
- **Scalability:** The server should be able to handle growing amounts of work in a large tag population. It should be able to identify multiple tags using the same radio channel [11]. Performing an exhaustive search to identify individual tags could be difficult when the tag population is large [6].

II. Related Works

Most of the security protocols implemented in RFID are based on cryptographic and hash functions. But these security protocols are not much secure. The OSK protocol was proposed by Ohkubo, Suzuki and Kinoshita (OSK) in 2004. Its aim is to assure the valid answer of the tag even under an active attack. In this scheme each tag is initialized with a secret value xi and two unidirectional functions h1 and h2. When a tag receives a request from a reader, it updates the value xi with the new value obtained from the computation of ht 1(xi).

Weis, Sarma, Rivest and Engels proposed in 2003 the use of hash-locks in RFID devices. A first approach, called Deterministic hash locks, was presented in. A tag is usually in a \locked" state until it is queried by a reader with a specific temporary meta-identifier Id. This is the result of hashing a random value (nonce) selected by the reader and stored into the tag. The reader stores the Id and the nonce in order to be able to interact with the tag. The reader can unlock a tag by sending the nonce value. When a tag receives it, the value is checked [22].

Most of the security protocols implemented in RFID are based on cryptographic and hash functions. But these security protocols are not much secure. The OSK protocol was proposed by Ohkubo, Suzuki and Kinoshita (OSK) in 2004 [13]. Its aim is to assure the valid answer of the tag even under an active attack. In this scheme each tag is initialized with a secret value xi and two unidirectional functions h1 and h2. When a tag receives a request from a reader, it updates the value xi with the new value obtained from the computation of ht 1(xi) [8].

YA-TRAP (Yet-Another Trivial RFID Authentication Protocol) was proposed by Tsudik in 2006 [14]. This protocol describes a technique for the inexpensive untraceable identification of RFID tags. YA-TRAP involves minimal interaction between devices and a low computational load on the back-end server. With these features, this scheme is attractive for applications where the information is processed in data groups [8].

Weis, Sarma, Rivest and Engels proposed in 2003 [15] the use of hash-locks in RFID devices. A first approach, called Deterministic hash locks, was presented in. A tag is usually in a \locked" state until it is queried by a reader with a specific temporary meta-identifier Id. This is the result of hashing a random value (nonce) selected by the reader and stored into the tag. The reader stores the Id and the nonce in order to be able to interact with the tag. The reader can unlock a tag by sending the nonce value. When a tag receives it, the value is checked [8].

In 2012, Dr.S.Suja proposed an RFID Authentication protocol for security and privacy which is based on Cyclic Redundancy Check (CRC) and Hamming Distance Calculation in order to achieve reader-to-tag authentication and the memory read command is used to achieve tag-to reader authentication. It will resist against tracing and cloning attacks in the most efficient way [1].

In 2011, Liangmin WANG, Xiaoluo YI, implies improved protocol merely uses CRC and PRNG operations supported by Gen-2 that require very low communication and computation loads. They also develop two methods based on BAN logic and AVISTA to prove the security of RFID protocol. BAN logic is used

to give the proof of protocol correctness, and AVISTA is used to affirm the authentication and secrecy properties [2].

In 2008, Tieyan Li analyze the security vulnerabilities of a family of ultra-lightweight RFID mutual authentication protocols: LMAP, M2AP and EMAP[17]*, which are proposed by Peris-Lopez et al. Here they identify two effective attacks, namely de-synchronization attack and full disclosure attack, against their protocols. The former permanently disables the authentication capability of a RFID tag by destroying synchronization between the tag and the RFID reader [3].

The weakness of this authentication protocol comes from the fact that each round the advesary gets some information from the same key. So a quick way to counter our attack is to include a key-updating mechanism similar to OSK[18] at the end of the protocol using a one-way function. In this case, adversaries do not get more than P equations for each key so that the security proof and reduction to the SAT problem become sound. The resulting protocol is even forward-private providing that adversaries do not get side-channel information from the reader [28].

D. N. Duc, J. Park, H. Lee, and K. Kim. Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning. In Symposium on Cryptography and Information Security — SCIS 2006, Hiroshima, Japan[7],

Hash-based Access Control (HAC), as defined by Weis et al. [16]*, is a scheme which involves locking a tag using a vone-way hash function. A locked tag uses the hash of a random key as its metaID. When locked, a tag responds to all queries with its metaID. However, the scheme allows a tag to be tracked because the same metaID is used repeatedly [5].

In[13] Ohkubo, Suzki, and Kinoshita (OSK) propose an RFID privacy protection scheme providing indistinguishability (i.e. a tag output is indistinguishable from a truly random value and unlinkable to the ID of the tag) and backward untraceability. This scheme uses a low-cost hash chain mechanism to update tag secret information to provide these two security properties.

III. Problem Statement

The attack on SASI is a passive one. Passive attacks are achievable in practice since they only necessitate only eavesdropping, which is a typical hazard or threat in RFID setting where the physical wireless communication station or channel is open to parties within communication and transmission. The security provided by the SASI might be more but for the passive attacks only and the chances of eavesdropping is more.

IV. Proposed Solution

Registration Phase - In the registration phase, Tag Ti wants to register himself/herself in remote server S. Firstly Tag chooses his/her ID and PW. Before register on Server, registration authority computes h (ID) and h (ID||PW) and sends to Reader R over a secure channel. Upon receiving the registration request from Tag Ti. Reader R computes same parameters related to the Tag Ti.

R computes Ai= h (ID) xor h (X || h (ID))
Bi = Ai xor h (ID || PW)
Ci = h (Ai)
Di = h (ID || PW) xor h(X)

And stored some of them in the memory and issues this to Tag Ti.

Login Phase- This phase provides the facility of a secure login to the Tag .Tag wants to access same services on remote server S. first it gain the access right on the remote server S. Tag keys in ID* and PW*. The Tag device memory computes –

$$Ai^* = Bi \text{ xor } h(ID^* || PW^*)$$

And Ci* = h (Ai*) and checks whether Ci (stored in the Tag memory) and Ci* are equal or not. If not, terminate to again login process. Otherwise yes, Tag Ti is legitimate bearer of the device. Then the Tag device generates a random nonce Ri and computes –

Ei = Ai* xor Ri
Cid = h (ID || PW) xor Ri
Fi = h (Ai || Di || Ri || Tu)

Where Tu is current time when login request proceed. And send the login request massage {Fi, Ei, Cid, Tu, h (ID)} to remote Reader R.

Verification Phase- Upon receiving the login request massage {Fi, Ei, Cid, Tu, h (ID)}. Reader verifies the validity of time delay between Tu‟ and Tu. Where Tu' is the travel time of the massage. Tu'-Tu ≤ ΔT where ΔT denotes expects valid time interval for transmission delay. Then Reader accepts the login request and go to next process, otherwise the Reader reject login request.

Reader computes –

Ai* = h (ID) xor h (X || h (ID))
Ri* = Ai* xor Ci
G = h (ID || PW)* =Cid xor Ri
Di* = h (ID || PW)* xor h(X)

And computes F* = h (Ai* || Di* || Ri* || Tu) And checks whether F and F* are equal or not. If they are not then reject the login request. If equal, then Reader R

Computes–

$$Fs = h(h(ID) || Di || Ri || Ts)$$

Where, Ts is remote Reader current time. And send acknowledge massage {Fs, G, Ts} to Tag Ti.

Upon receiving acknowledge massage Tag device compute G* = h (ID || PW) Fs* = h (h (ID) || Di || Ri || Ts) And checks where G =G*and Fs = Fs* are same or not. It is mutual authentication process. In which both Reader and Tag verify to each other. If they are same then Tag device makes session key (Sk) and both Reader and Tag share it. Sk = h (h (ID) || Ts || Tu || Ai) Otherwise terminate to again login process.

Password change Phase- This phase is involved whenever Tag T want to change the password PW with a new Password PWnew. Tag T keys in ID* and PW* and request to change password. The Tag device checks whether C = C* are equal or not. If it is satisfy User U is a legitimate bearer of the device. Then the Tag device asks the Tag Ti to input new password PWnew. After entering the new password the Tag calculate-

Bnew = Ai xor h (ID || PWnew) and

Dnew = h (ID || PWnew) xor h (ID || PW) xor Di

And change B with Bnew and D with Dnew in Tag device memory.

Tag Ti	Reader Ri
Initial Phase	
	Select p,q,x Keep p,x secretly
Registration Phase	
Select IDi and PWi	A=h(ID^x mod p) xor h(pWi) Store (ID,A,h(.),E(.) into package
	<---------- card
Login and Authentication Phase	
Input IDi and PWi Select R K=A xor h(PWi) W=EK(R xor Tu) Cu=h(Tu||R||W||IDi) --------→	verify IDi and Tu K=h(ID^x mod p) R'=DK(W) xor Tu Cu'=h(Tu||R||W||IDi) Verify cu'=cu Cs=h(IDi||R'||Ts)
Verify ID and Ts Cs=h(IDi||R||Ts) Verify Cs'==Cs	<----------
Compute Common Secrete Key	
Sk=h(IDi||Ts||||Tu||R) ←--------→	Sk=h(IDi||Ts||Tu||R')

V. Result Analysis

Storages /Scheme	Our Scheme	Yoon Yoo al et. [3]	Liou al et. [7]	R.Song al et.[10]
Tag	480 bits	480 bits	480 bits	320 bits
Server	160 bits	320 bits	320 bits	480 bits

Table 1 : Storage Capacity Comparison

Table 1 shows, the storage comparison of the proposed scheme with the relevant user authentication based on smart card, Which shows our proposed scheme is reduced burden on the server, because the Server has store only server secret key (X).

Communication/Scheme	Our Scheme	Yoon Yoo et al. [3]	Liou et al. [7]	R.Song et al.[10]
Authentication (bits)	5*160	5*160	6*160	5*160

Table 2 : Communication Cost

The proposed scheme requires little more computation cost and equal to related user authentication scheme, Because our proposed scheme has strong secure mutual authentication scheme is resistance to insider attack, resistance to masquerade attacks, parallel session attack, replay attack, password attack, secure password change, protecting server spoofing attack, session key generation and agreement and other possible attack, that why some cost of execution are little more. Table 2 shows, the communication cost of the proposed scheme with the relevant user authentication based on Tag memory, which shows communication cost weightage between Tag and Reader in term of authentication.

Resistance to / Scheme	Our Scheme	Yoon Yoo et al. [3]	Liou et al. [7]	R.Song et al.[10]
Insider attack	Yes	No	Yes	No
Masquerade attack	Yes	No	Yes	Yes
Parallel session attack	Yes	No	Yes	No
Replay attack	Yes	Yes	Yes	No
Offline password attack	Yes	No	Yes	No
Secure password change process	Yes	Yes	Yes	Yes
Denial of service	Yes	No	Yes	No
Session key generation and agreement	Yes	No	No	Yes

Table 3 : The Efficiency Comparison

The efficiency of the proposed algorithm is very high because it is not involved in any time consuming modular exponential computing as shown in the Table 3.

VI. Conclusion

In this paper we show that the other authentication techniques involved in RFID are not so much secure and have high communication cost. We showed that our scheme is vulnerable to Denial-of-Service attack, Insider attack, Offline password attack Forward secrecy attacks. We present an efficient and secure ID- base remote user authentication scheme. The proposed scheme is proved to be able to withstand the various possible attacks. The proposed algorithm provides here provides a more authenticated protocol using the concept of pre shared secrete key for the authenticity between the tags and the reader using the technique of card generation.

References Références Referencias

1. An rfid authentication protocol for security and privacy,dr.s.suja, m.e.,phd., associate professor, electrical and electronics engineering, coimbatore institute of technology, coimbatore. a. arivarasi, m.e, embedded and real time systems, coimbatore institute of technology, coimbatore.
2. Security improvement in authentication protocol for gen-2 based rfid system, liangmin wang, xiaoluo yi, chao lv, yuanbo guo ,school of computer science and communication engineering, jiangsu university, zhenjiang 212013, china school of communication engineering, xidian university, xi'an, 710071, china school of electronic technology, information engineering university of pla, zhengzhou, 450004, china doi:10.4156/jcit.vol6. issue1.18.
3. Security analysis on a family of ultra-lightweight rfid authentication protocols tieyan li, institute for infocomm research (i2r), 21 heng mui keng terrace, singapore 119613.
4. G. avoine. Cryptography in radio frequency identification and fair exchange protocols. phd thesis, ecole polytechnique federale de lausanne (epfl), lausanne, switzerland, december 2005.
5. H. chien and c. chen. Mutual authentication protocol for rfid conforming to epc class 1 generation 2 standards. Computer standards & interfaces, 29(2):254–259, february 2007.
6. H. lee, j. yang, and k. kim. Enhanced mutual authentication protocol for low-cost rfid. White paper wp-hardware-031, auto-id labs, 2006.
7. d. n. duc, j. park, h. lee, and k. kim. Enhancing security of epcglobal gen-2 rfid tag against traceability and cloning. In symposium on cryptography and information security — scis 2006, hiroshima, japan, january 2006. The institute of electronics, information and communication engineers.
8. A brief survey on rfid privacy and security j. aragones-vilella_, a. martinez-ballest_e and a. solanas crises reserch group unesco chair in data privacy dept. of computer engineering and mathematics, rovira i virgili university.
9. T. le, m. burmester, and b. medeiros. Forward secure rfid authentication and key exchange. Cryptology eprint archive report 2007/051, iacr, 2007. [18] m. ohkubo, k. suzki, and s. kinoshita. Cryptographic approach to "privacy-friendly" tags. In rfid privacy workshop, mit, ma, usa, november 2003. http://www.rfidprivacy.us/2003/agenda.php.
10. P. peris-lopez, j. c. hernandez-castro, j. m. estevez-tapiador, and a. ribagorda. lmap: a real lightweight mutual authentication protocol for low-cost rfid tags. in: proc. of 2nd workshop on rfid security, july 2006.
11. P. peris-lopez, j. c. hernandez-castro, j. m. estevez-tapiador, and a. ribagorda. m2ap: a minimalist mutual- authentication protocol for low-cost rfid tags. In: proc. of international conference on ubiquitous intelligence and computing uic'06, lncs 4159, pp. 912-923. springer- verlag, 2006.
12. P. peris-lopez, j. c. hernandez-castro, j. m. estevez-tapiador, and a. ribagorda. emap: an efficient mutual authentication protocol for low-cost rfid tags. In: otm federated conferences and workshop: is workshop, november 2006.
13. M. ohkubo, k. suzuki, and s. kinoshita. Efficient hash chain based rfid privacy protection scheme. In international con- ference on ubiquitous computing - ubicomp, workshop privacy: current status and future directions, 2004.
14. G. tsudik. Ya-trap: yet another trivial rfid authentication protocol. In fourth annual ieee international conference on pervasive computing and communications work- shops (percomw'06), pages 640{643, 2006.
15. Weis, sarma, rivest and Engels: a brief survey on rfid privacy and security. Crises reserch groupunesco chair in data privacy, 2003.
16. Boyeon song, chris j mitchell "rfid authentication protocol for low-cost tags" wisec'08, alexandria, virginia, usa.copyright 2008 acm 978-1-59593-814-5/08/03. march 31–april 2, 2008
17. Tieyan li, guilin wang, robert h. deng," security analysis on a family ofultra-lightweight rfid authentication protocols" journal of software, vol. 3, no. 3, march 2008
18. Md. endadul hoque," protecting privacy and ensuring security of rfid systems using private authentication protocols" marquette university, 2010.
19. E. Yoon and Yoo, 2005 "More efficient and secure remote user authentication scheme using smart card", in proceeding of 11th international conference on Parallel and Distributed System, pp.73-77.
20. Y.P. Liou, J. Lin and S.S. Wang, 2006 "A New Dynamic ID Based Remote User Authentication

Scheme using Smart Cards," Proc. 16th Information Security Conference, Taiwan, pp. 198-205, July.
21. R. Song. 2010 "Advanced smart card based password authentication Protocol". Computer Standards & Interfaces, Volume 32, Issue 4, June, Pages 321-325.
22. A Brief Survey on RFID Privacy and Security J. Aragones-Vilella_, A. Martinez-Ballest_e and A. Solanas CRISES Reserch Group UNESCO Chair in Data Privacy Dept. of Computer Engineering and Mathematics, Rovira I Virgili University.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Ordered Cross Layer Approach for Multicast Routing in Mobile Ad hoc Networks: Qos by Clogging Control

By N. Nagaraju & M.L.Ravichandra

Netaji Institute of Engineering and Technology, Hyderabad, AP, India

Abstract - Here in this paper a MAC layer level clogging detection system has been projected. The planned model aims to explores a system to compute the degree of clogging at victim node with maximal accuracy. This clogging detection apparatus is integrated with a Two-Step Cross Layer Clogging Control Routing Topology. The proposed model involves controlling of clogging in two steps with effective energy capable blocking detection and optimal cost of routing. Packet drop in routing is mostly due to link crash and clogging. Most of the existing clogging control solutions do not have the ability to distinguish between packet loss due to link collapse and packet loss due to clogging. As a result these solutions aim towards action against packet drop due to link malfunction which is an unnecessary effort and ends with of energy resources. The other limit in most of the available way out is the utilization of energy and resources to detect clogging state, degree of clogging and alert the source node about blocking in routing path. This paper explores a cross layered model of clogging recognition an control mechanism that include energy efficient clogging detection, Multicast Group Level Clogging Evaluation and Handling Algorithm [MGLCEH] and Multicast Group Level Load Balancing Algorithm [MGLLBA], which is a hierarchical cross layered base clogging recognition and avoidance model in short can refer as Qos Optimization by cross layered clogging handling (MGLCEH). This paper is supported by the investigational and simulation results show that better store utilization, energy efficiency in clogging detection and clogging control is possible by the proposed topology.

Keywords : *Ad-hoc networks, manets, clogging, cross-layer design, optimization, random access, wireless network.*

GJCST-E Classification : *C.2.2, C.2.6*

Strictly as per the compliance and regulations of:

Ordered Cross Layer Approach for Multicast Routing in Mobile Ad hoc Networks: Qos by Clogging Control

N. Nagaraju[α] & M.L.Ravichandra[σ]

Abstract - Here in this paper a MAC layer level clogging detection system has been projected. The planned model aims to explores a system to compute the degree of clogging at victim node with maximal accuracy. This clogging detection apparatus is integrated with a Two-Step Cross Layer Clogging Control Routing Topology. The proposed model involves controlling of clogging in two steps with effective energy capable blocking detection and optimal cost of routing. Packet drop in routing is mostly due to link crash and clogging. Most of the existing clogging control solutions do not have the ability to distinguish between packet loss due to link collapse and packet loss due to clogging. As a result these solutions aim towards action against packet drop due to link malfunction which is an unnecessary effort and ends with of energy resources. The other limit in most of the available way out is the utilization of energy and resources to detect clogging state, degree of clogging and alert the source node about blocking in routing path. This paper explores a cross layered model of clogging recognition an control mechanism that include energy efficient clogging detection, Multicast Group Level Clogging Evaluation and Handling Algorithm [MGLCEH] and Multicast Group Level Load Balancing Algorithm [MGLLBA], which is a hierarchical cross layered base clogging recognition and avoidance model in short can refer as Qos Optimization by cross layered clogging handling (MGLCEH). This paper is supported by the investigational and simulation results show that better store utilization, energy efficiency in clogging detection and clogging control is possible by the proposed topology.

IndexTerms : Ad-hoc networks, manets, clogging, cross-layer design, optimization, random access, wireless network.

I. Introduction

The regular TCP clogging control mostly adapted for internet is not an apposite for MANETs because MANETs are known to affect topology and topology stacks of control mechanisms .also the MANETs are environmentally irreconcilable with standard TCP.

The packet salvage setbacks and losses in MANETs are primarily due to their node mobility combined with intrinsically unexpected medium which is a direct consequence of the common wireless multi hop channel cannot be construe as clogging losses .

The primary individuality of a wireless multi hop channel is that within interfering range of one node only a single data is transmitted. In MANETs' networks in an complete area are congested due to shared standard where as internet clogging is single router. A note valuable point is that in a MANET the nodes are not overcrowded.

The main reason for the incompatible of a regular TCP and a MANET is the fact that package losses in MANET may not always be due to network clogging and the transmission times (including the round trip times) vary highly making the package losses quite difficult to observe .

It is difficult to find the source of clogging in a multi hop network because a single user has the capability to produce a clogging resulting in comparatively lower bandwidth of mobile ad-hoc networks .The wireless networks are more susceptible to clogging problems when compared with the traditional wire line network. Therefore a balanced clogging control system is to be employed compulsorily for the stability and superior performance of a wireless network.

The non homogeneous nature of the application topologys in the multihop wireless networks, a single and unified solution for the clogging related problems cannot be obtained .Instead a suitable clogging control depending upon the properties and functions of the related network can be designed .As a result, these proposal majorly form a subset of solutions for the identified problems rather than a complete, instantly used topology. They pose as a parent for application-tailored topology stacks. Exceptionally, few of the topology properties serve wide range of applications.

The recent years have witness a much more focus on the clogging control methods directed on the modeling, analysis, algorithm development of closed loop control schemes (e.g. TCP) making them sympathetic for adaption to the mobile hoc networks .under the provision of constraints of routing path and bandwidth algorithms possessing the ability to unify and stabilize operation have been evolved .Another major constraint to be painstaking in a wireless hoc network is due to the MAC[Media access Control) layer. Majority of

Author α : M.Tech at Dept of ECE, Netaji institute of engineering and technology, Hyderabad, AP, India.
E-mail : nagarajumittapally@yahoo.com
Author σ : Associate Professor & HOD, Dept of ECE, Netaji institute of engineering and technology, Hyderabad, AP, India.
E-mail : nietece2009@gmail.com

wireless MACs possess a time constriction permitting a single user to access a physical channel at a given time. The sections in the paper are organized to provide the following details as regards. The section2 explores the most cited works in the area of text .section3 gives a detail discussion of the projected topology and section 4 relies on the simulation and their results to be consummate by conclusion and references.

a) Related Work

QoS centric clogging control solution can be found in [1]. was Yung Yi et al [13] proposed few metrics for clogging aware routing] Xiaoqin Chen et al [2] introduced metrics to evaluate data-rate, MAC transparency and buffer delay, which helps to identify and deal the blocking contention area in network. Hongqiang Zhai, et al., [3] projected a solution by arguing that clogging and severe medium debate is interrelated. Tom Goff et al., [5] discussed a set of algorithms that initiates different path usage when the quality of a path in use turns out to be suspect. A cross-layer hop-by-hop clogging control scheme projected by Xuyang et al., [6] to improve TCP performance in multihop wireless networks. Dzmitry et al [7] presents the impact blocking on transport layer that decreases the performance. Duc et al.[15] proposed that current designs for routing are not adjustable to clogging.

The existing models aim at identify clogging losses in routing path .The packet loss generate a link failure. Making efforts to manage the packet losses that cause link failure are in effective. Another exclusive approach is regularizing the outflow at all nodes participating in routing. In majority of cases of control the clogging at hop level [13][8]. Henceforth outflow regularization at each node of the network involves operation of expensive wealth. Here in this paper we argue that it is a important to identify the reason for packet loss. Hence we can avoid the clogging control process via outflow regularization under the status of link failure. And also we continue the spat that hop level blocking control alone is not plenty when the hop levels are unable to normalize themselves. The outflow load to control the blocking by utilizing the same resources can be done as in spring level outflow regularization models. Here we propose a cross layer based clogging control routing topology that contains Clogging detection and clogging control models.

II. Groups Structure Based Multi Cast Routing: An Ordered Cross Layer Approach for QoS Provisioning by Clogging Control

a) Measuring degree of clogging at Relay hop level node

Unlike conventional networks, nodes in the ad hoc network exhibit a high degree of heterogeneity in terms of both hardware and software configurations. The heterogeneity of the relay hop nodes can reflect as varied radio range, maximum retransmission counts, and barrier capacity. Hence the degree of communication load, packet drop frequency, and degree of buffer consumption at relay hop level node is minimum combination to find the degree of clogging. The usage of these three purposeful values supports to decouple the clogging measure process from other MAC layer behavior.

The degree of channel load, packet drop rate and degree of buffer operation together provide a scope to envisage the blocking due to inappropriate ratio between collision and retransmission count. When retransmissions compared to collision rate are significantly low then outflow delay of relay hop node will increase proportionally, which leads to clogging and reflected as clogging due to buffer overflow.

b) Measuring degree of clogging at path level traffic

The degree of clogging at each relay hop together helps to identify the degree of clogging at path level traffic from source to goal node. Each relay hop level node receives the degree of clogging from its neighbor node in hierarchy. Since the destination node, which is last node of the routing path is not outlet the emptiness status. Hence the destination node initiates to assess the degree of clogging at path level traffic. The interrupted updates of clogging status at each relay hop level node to its heir in routing path is significantly energy consuming activity. Hence to conserve the energy, the clogging update strategy considers two restricted behavior, which follows:

1. Degree of blocking $d_c(h_i)$ at relay hop level node h_i will be sent to its successor h_{i+1} iff the ' $d_c(h_i)$ ' is greater than the node level clogging threshold $d_c(\tau)$. Hence the energy conserves due to conditional transmission.
2. If degree of blocking at path level traffic $d_c(rp)$ that received by node h_i from its doorway initiator h_{i-1} is smaller than $d_c(h_i)$ then it update the $d_c(rp)$ else it remains same, hence energy conserve due to prevention of $d_c(rp)$ update.

III. Cross Layered Model for Clogging Control

The packet dipping often occurs in Manets. The reasons for this packet plummeting are as below

- Transmission Link failure.
- Inferred Transmission due to weighed down Inflow that leads inflow balancing ability to low. This also

can claim as packet dropping due to blocking at routing.

The clogging control can be evaluated in two stages by turning over of the zonal head with the network partitioned into Cells as follows

- The Status of blocking at intra Group level
- The status of clogging at inter Group level

This helps in minimization of source level outflow balancing cost and balances the power consumption.

Table 1 : Notations Used in Proposed Model

Group	A geographical area, which is the part of preferred mobile ad hoc network
DPG	Distance Power Gradient
EIL	Inflow inferred Loss
LFL	Link Failure Loss
IRS	Inflow balancing ability
IRS_p	Present Inflow balancing ability
IRS_e	Expected Inflow balancing ability
RP	Routing Path
dt_n	Delay time at node n
N	Number of nodes in entire network
Zn_i	Number of nodes in a Group i
zh_i	Group head of the i^{th} Group
zh'_i	Reserved Group head of the i^{th} Group
Z_c	Current Group in the hierarchy
Z_p	Preceding Group to the current Group Z_c in hierarchy
Z_f	Fallowing Group to the current Group Z_c in hierachy
Z_i	i^{th} Group in the routing path
n_z	Group of the node n
ζ_Z	Group level Transmission Load Threshold
ζ_n	Node level Transmission Load Threshold
ζ_T	projected threshold that indicates interval among two transmissions at one hop level
ζ_t	Interval observed between last two transmissions
ζ_{et}	time spent since last transmission at one hop level
IRS_{ζ_T}	Average Inflow balancing ability threshold observed for predefined interval ζ_T
∂'	Average threshold of the receiving strength
IRS_{ce}	Expected Inflow balancing ability threshold at current interval
IRS_r	Inflow balancing ability ratio
IRS_{cr}	Current inflow balancing ability ratio
BT_n	Buffering time at node n
$zdil_i$	Group level degree of inflow load, here i is a Group id.
$ndil_k$	Node level degree of inflow load, here k is the node id of Group i

a) Network and Node activities under projected topology

The network is to be crack into Cells

For each Group i where $i = 1..|Z|$; ($|Z|$ is entirety number of Cells)

Select Group-head for each Group i

Find spread load threshold ζ_n for each Group i

By using ζ_n of each Group spread load threshold for entire network can be measured.

b) Splitting the network into Groups

We opt to the approach described by Mohammad M. Qabajeh et al [15]. With the knowledge of the presented nodes the region is divided into equal partitions. Hexagon is mostly chased for the zonal shape because it covers a highest surface and also provides the improvement of communicating with more neighbors as they have near circular shape of the transmitter. The availability of small, economical low power GPS receiver makes it possible to apply position-based in MANETs. The communication range of node is denote as R and the side of hexagon as L.As the nodes should be able to correspond with each other the R and L are related as L=R/2.

Each Group has a Group characteristics (zid), Group Header (zh) and Group Leader Backup (zh'). The zh node maintains in sequence about all the nodes in a Group with their positions and IDs. Also, maintain information about the zh of the neighboring Cells as shown in the figure 1. The CLB node keeps a copy of the data stored at the zh so that it is not lost when the zh node is off or touching the Group. By knowing the coordinates of a node location, nodes can execute our self-mapping algorithm of their present locations onto the current Group and calculate it's zid easily. Figure 1.shows the general overview of the network architecture.

c) Selecting Group Heads

A Group-Head selection occur under the pressure of the Following metrics:

a. Node positions: A node with a position *p* that is close to the centre is more likely to act as a Group head.
b. Optimum energy available: a node with higher energy e more probably acts as a Group head.
c. Computational ability: the node with high computational ability c is more possible to act as a Group Head.
d. Low mobility: the mobility *m of* a node is inversly proportional to its selection as a Group head.

Each node of the Group broadcasts its (p,e,c,m). The node that identified itself as most optimal in (p,e,c,m) metrics, announces itself as Group head zh. The next optimal node in sequence claims itself as reserve Group head zh'.

d) Information sharing within multicast group [between Node and group head]

Each node n that is a subset to Group Z verifies the Inflow load and shares degree of inflow load dil_n with Group head. Once $ndil_k$ received from each node k of the Group i, the Group head zh calculates the degree of inflow load at Group level $zdil_i$.

$$zdil_{z_i} = \frac{\sum_{k=1}^{zn_i} ndil_k}{zn_i}$$

e) Multicast Group Level Clogging Evaluation and Handling Algorithm (MGLCEH)

Multicast Group Level Clogging Evaluation and Handling Algorithm abbreviated as MGLCEH is presented in this section. MGLCEH is an optimal algorithm that helps in locating the packet dropping under clogging. This evaluation occurs under Mac layer and then alerts network layer.

At an event of inflow receiving by node i *:*

Updating Inflow balancing ability:

$if\ (\zeta_t < \zeta_T)do$

$$\delta' := \frac{1}{2}\left(\frac{IRS_{cr} - IRS_{\zeta_T}}{\zeta_t}\right) + \frac{1}{2}(\delta')$$

$$IRS_{\zeta_T} := IRS_{cr}\left(\frac{\zeta_t}{\zeta_T}\right) + IRS_{\zeta_T}\left(\frac{\zeta_T - \zeta_t}{\zeta_T}\right)$$

$endif$

$if\ ((\zeta_t) \neg < (\zeta_T))do$

$$\delta' := \frac{IRS_{cr} - IRS_{\zeta_T}}{\zeta_t}$$

$$IRS_{\zeta_T} := IRS_{cr}$$

$endif$

Detecting transmission failure by Mac layer level

$$IRS_{ce} = IRS_{\zeta_T} + \delta' \zeta_{et}$$

$if\ (IRS_{ce} < IRS_r)do$

$macAlert{:}link-failure$

$else$

$MacAlert{:}congestion$

$endif$

Fig. 2 : MGLCEH for determining clogging caused packet dropping

f) Multicast Group Level Load Balancing Algorithm (MGLLBA)

This event occurs if Mac-layer alert indicates the clogging circumstance. Once the routing topology [4] gets an alert from the Mac layer a propos the blocking at a node i, it alerts the fellow citizen node which is the source node s for conflict node i. Hence s evaluates it's dil_s by comparing with $zdil$ of Z_c (Group of the node s). If dil_s is more in magnitude than $zdil_{z_c}$ the variation between dil_s and $zdil_{s_z}$ should be either greater or equal to the outflow threshold ε then node s regularizes the outflow load by manipulate its buffer time BT_s such that $ndil_s \geq zdil_{s_z} + \varepsilon_{s_z}$.

Here ε can be calculated with following equation

$$\varepsilon_j = \frac{\sum_{k=1}^{zn_j} zdil_j - dil_k}{zn_j}$$

In case that the node s not able to normalize its outflow so that disagreement node i terminates

blocking then it alerts the zh_{s_z} (Group-head of the Z_c, $s \in Z_c$). Subsequent that event zh_{z_c} alerts all the nodes in the network building the all nodes in the upstream of source node to way out load using the above stated slant. Then all nodes update their $ndil$ and send to Group-head zh_{z_c}, then Group-head zh_{z_c} calculate $zdil$ and confirms integrity of the $zdil$ by evaluation with dil. $zdil_{z_c} \geq dil + \overline{\varepsilon}$ concludes that clogging at contention node maintained by outflow regularization at current Group level. If $zdil_{z_c} < dil + \overline{\varepsilon}$ then CEA will be started at Z_p, which is adjacent upstream Group to Z_c in transmissible. In this process Group head of the Z_c firstly alerts the Group head of the counterpart Z_p then zh_{z_p} alerts all nodes that belongs to Z_p, of the route path. The above procedure of outflow regularization at Group level can be referred as BGLLBA (Multicast Group Level Load Balancing Algorithm). Hence the nodes belong to Z_p regularize their outflow load by utilize BGLLBA and alert Group-head about their efficient degree of inflow load $ndil$. Then zh_{z_p} measures $zdil_{z_p}$ and verifies the result of $zdil_{z_p} \geq dil + \overline{\varepsilon}$ .True indicates the elimination or minimization of clogging at the Group due to the outflow regularization at Group Z_p, if false then Group head of the Z_p performs the action of alerting all other Group heads using a broadcasting[12] instrument about the clogging at adjacent Group in downstream of the heridetary. Hence all Cells in the upstream side of the Z_p apply BGLLBA and the Cells in downstream side of the Z_p fill in their $zdil$. Then all Cells broadcast $zdil$ to resource Group. Hence the source Group revaluates the dil .Basing on the dil, source node regularize its outflow load.

Notations used in Algorithm:
i: Node that had been effected by emptiness
s: source node of the i.
Z_c : current Group where $i, s \in Z_c$
Z_p : Immediate Group to Z_c in upstream side of the pecking order.
$\{n_{u1}, n_{u2}, ..., n_{uk}\}_{Z_c}$: All upstream nodes to s.
$\{n_{d1}, n_{d2}, ..., n_{dk}\}_{Z_c}$: All downstream nodes to s.
$\{Z_S, Z_{u1}, Z_{u2}, ..., Z_{uk}\}$: Set of upstream Cells to Z_p in routing path, here Z_S is a Group that contains source node of the routing path
$\{Z_{d1}, Z_{d2}, ..., Z_{dm}, ..., Z_T\}$: Set of downstream Cells to Z_p in routing path, here Z_T is a Group that contain target node of the routing path
ε : Group level outflow threshold
$\overline{\varepsilon}$: Network level Outflow threshold
Algorithm:

Mac layer alerts about the blocking at node of Group Z_c to routing topology, hence the following steps perform in sequence

$$\varepsilon_{Z_c} = \frac{\sum_{k=1}^{zn_{Zc}} zdil_{Z_c} - dil_k}{zn_{Z_c}}$$

complete following at node s

If $ndil_s > zdil_{Z_c}$ and $ndil_s - zdil_{Z_c} \geq \varepsilon_{Z_c}$ begin

$$BT_s = BT_s + bt$$

Note: Value of buffer threshold bt should be certain such that $dil_s \geq zdil_{Z_c} + \varepsilon_{Z_c}$

Return.
Endif

s sends alert to zh_{Z_c} about conflict node i.

zh_{Z_c} alerts all nodes that belongs to Group Z_c

$\{n_{u1}, n_{u2}, ..., n_{uk}\}_{Z_c}$ updates their $ndil$ by apply BGLLBA recursively and alerts zh_{Z_c}

$\{n_{d1}, n_{d2}, ..., n_{dk}\}_{Z_c}$ measures their $ndil$ and alerts zh_{Z_c}

zh_{Z_c} Measures $zdil$ as fallows

$$zdil_{z_c} = \frac{\sum_{k=1}^{zn_{Zc}} ndil_k}{zn_{Z_c}}$$

If $zdil_{Z_c} > dil$ and $(zdil_{Z_c} - dil) \geq \overline{\varepsilon}$ begin

Alert: blocking at contention node handle at current Group Z_c level.
Return.
Endif

zh_{Z_c} Alerts zh_{Z_p}

zh_{Zp} Alerts all nodes that belong to Group Z_p

For each node $n \in Z_p$ begin

If $ndil_n > zdil_{Z_p}$ and $ndil_n - zdil_{Z_p} \geq \varepsilon_{Z_p}$ begin

$BT_n = BT_n + bt$

Note: Value of barrier threshold bt should be decided such that $dil_n \geq zdil_{Z_c} + \varepsilon_{Z_c}$

Endif

Find dil_n and send dil_n to zh_{Z_p}

End-of-for each

zh_{Z_p} measures $zdil_{Z_p}$

if $zdil_{Z_p} > dil$ and $(zdil_{Z_p} - dil) \geq \overline{\varepsilon}$ begin

Alert: Outflow regularization at Z_p leads to overcome clogging situation at contention Group.

Return;

Endif

zh_{Z_p} Alerts all Group heads in network regarding clogging contention Group.

For each Group z in $\{Z_S, Z_{u1}, Z_{u2}, ..., Z_{uk}\}$ begin

zh_z Alerts all nodes that belongs to Group z

For each node $n \in z$ begin

If $ndil_n > zdil_z$ and $ndil_n - zdil_z \geq \varepsilon_z$ begin

$BT_n = BT_n + bt$

Note: Value of barrier threshold bt should be understood such that $dil_n \geq zdil_z + \varepsilon_z$

Endif

Find dil_n and send dil_n to zh_z

End-of-foreach

zh_z measures $zdil_z$ and broadcast towards source Group.

End-of-foreach

For each Group z in $\{Z_{d1}, Z_{d2}, ..., Z_{dm}, ..., Z_T\}$ begin

For each node n belong to Group z begin

determine $ndil_n$ and sends to zh_z

End-of-foreach

zh_z measures $zdil_z$ as

$$zdil_z = \frac{\sum_{k=1}^{zn_z} ndil_k}{zn_z}$$

zh_z Sends $zdil_z$ to source Group via propagation [12]

End-of-foreach

Z_S Measures dil as

$$dil = \frac{\sum_{i=1}^{|Z|} zdil_i}{|Z|}$$

Hence source node S of Group ZS, which is source node of the routing path regularize it's outflow load to direction-finding path

Hence source node S of t's outflow l

oad to direction-finding path.

Fig. 3 : Multicast Group Level Load Balancing Algorithm

IV. Simulations and Results Discussion

In this section we discuss the outcome acquired from simulation conducted using a simulation model developed by using MXML in this section. We evaluated concert using madhoc with the following considerations:

Table 2 : Parameters Used in Simulation Model for Performance Analysis

No of Hops	225
Approximate Hop distance	300 meters
Approximate total network	1000X1000 meters
fairly accurate Group Rdious	100X100 meters
Physical channel bandwidth	2mbps
Mac Layer:	802.11 DCF with option of handshaking prier to data transferring
Physical layer illustration	802:11B
presentation Index	Outflow regularization cost and end-to-end throughput
be very successful simulation time	150 sec

The simulations are conducted on three routes differing by the no of hops and length.

a. Short length path: A route with 15 hops
b. Middling length : A route with 40 hops
c. Max Length: A route with 81 hops

The same load is given to all the paths with regular intervals. The figure 3 indicates the load given in simulations. The fig 4 concludes the improvement of MGLCEH over clogging control topology [8] in clogging control cost. A. The clogging detection cost evaluation between MGLCEH and clogging control topology[8] is explore in fig 5 that elevates the energy good organization achieved under.

The process of capacity of clogging control and clogging detection cost is as follows:

Based on the resource ease of use, bandwidth and energy, for individual operation a threshold value between 0 and 1 assigned. In the mechanism of clogging detection and control the total cost is calculated by summing the cost threshold of every involved event. In fig 5 the judgment between clogging

costs observed for MGLCEH and clogging and contention control model [8] are shown.

$$\cos t_{ch} = \sum_{e=1}^{E} ct_e$$

Here $\cos t_{ch}$ is the price of a clogging controlling activity ch, E is total amount of events included. ct_e is the threshold cost of an event e. The example events are:

1. "Alert to source node from Mac layer"
2. "Alert from node to Group head", "propagation by Group head to other Group heads"
3. "Inflow judgment and outflow regularization".
4. Alert about $d_c(h_i)$
5. Bring up to date $d_c(rp)$

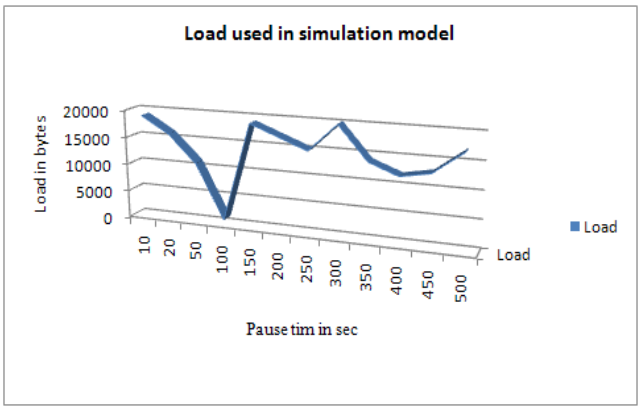


Fig. 3 : Load in bytes drive by source node of the routing path [in regular interval of 10 sec]

V. Conclusion

This manuscript discussed about proposed "Energy Efficient Cross layered blocking Detection and Control Routing Topology" in short referred as MGLCEH (Clogging Detection and have power over with Control seaplane Functionality). MGLCEH derived a cross layered clogging detection mechanism with energy effectiveness as primary criteria that included as clogging detection.

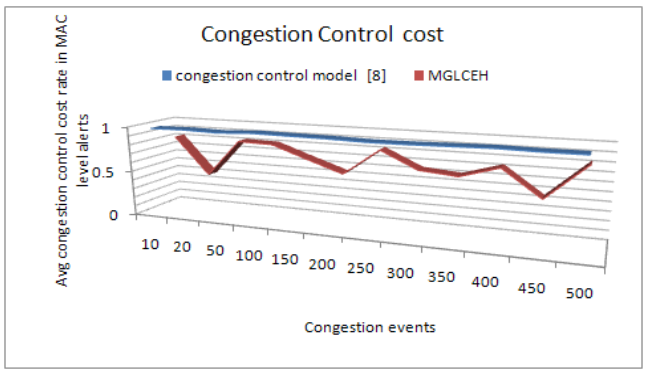


Fig. 4 : Clogging Control cost

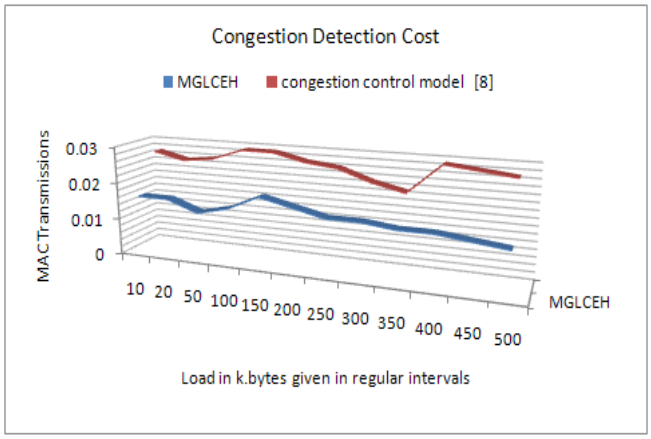


Fig. 5 : Clogging detection cost

References Références Referencias

1. Michael Gerharz, Christian de Waal, and Matthias Frank, "A Practical View on Quality-of-Service Support in Wireless Ad Hoc Networks", BMBF
2. Xiaoqin Chen, Haley M. Jones, A .D .S. Jayalath, "Cogestion-Aware Routing Topology for Mobile Ad Hoc Networks", IEEE, 2007
3. Hongqiang Zhai, Xiang Chen, and Yuguang Fang, "Improving Transport Layer Performance in Multihop Ad Hoc Networks by Exploiting MAC Layer Information", IEEE, 2007
4. Giovanidis, A. Stanczak, S., Fraunhofer Inst. for Telecommun., Heinrich Hertz Inst., Berlin, Germany This paper appears in: 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009
5. Tom Goff, Nael B. Abu-Ghazaleh, Dhananjay S. Phatak and Ridvan Kahvecioglu, "Preemptive Routing in Ad Hoc Networks", ACM, 2001
6. Xuyang Wang and Dmitri Perkins, "Cross-layer Hop-byhop Congestion Control in Mobile Ad Hoc Networks", IEEE, 2008.
7. Dzmitry Kliazovich, Fabrizio Granelli, "Cross-layer Congestion Control in Ad hoc Wireless Networks," Elsevier, 2005
8. Yingqun Yu; Giannakis, G.B.; , "Cross-layer congestion and contention control for wireless ad hoc networks," Wireless Communications, IEEE Transactions on , vol.7, no.1, pp.37-42, Jan. 2008
9. Nishant Gupta, Samir R. Das. Energy-Aware On-Demand Routing for Mobile Ad Hoc Networks, OPNET Technologies, Inc. 7255 Woodmont Avenue Bethesda, MD 20814 U.S.A., Computer Science Department SUNY at Stony Brook Stony Brook, NY 11794-4400 U.S.A.
10. Laura, Energy Consumption Model for performance analysis of routing topologys in MANET,Journal of mobile networks and application 2000.
11. LIXin MIAO Jian –song, A new traffic allocation algorithm in AD hoc networks, "The Journal of

ChinaUniversity of Post and Telecommunication", Volume 13. Issue3. September 2006.

12. Chun-Yuan Chiu; Wu, E.H.-K.; Gen-Huey Chen; "A Reliable and Efficient MAC Layer Broadcast Topology for Mobile Ad Hoc Networks," Vehicular Technology, IEEE Transactions on, vol.56, no.4, pp.2296-2305, July 2007
13. Yung Yi, and Sanjay Shakkottai, "Hop-by-Hop Congestion Control Over a Wireless Multi-Hop Network", IEEE, 2007
14. Outay, F.; Vèque, V.; Bouallègue, R.; Inst. of Fundamental Electron., Univ. Paris-Sud 11, Orsay, France This paper appears in: 2010 IEEE 29th International Performance Computing and Communications Conference (IPCCC)
15. Duc A. Tran and Harish Raghavendra, "Congestion Adaptive Routing in Mobile Ad Hoc Networks", 2006.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Integration of Knowledge Management System in Telecommunication: A Case Study of Saudi Telecom

By Khalid AlRowaily & Abdulaziz O.Alsadhan

King Saud University, Riyadh, Saudi Arabia

Abstract - Accelerated business growth has pushed telecommunication companies to implement knowledge management systems to systematically manage knowledge created within the organization. This helps them to retain their competitive edge in the rapid changing telecom sector. This study plan to explore the emerging role of Knowledge Management (KM) system in telecommunication industry. Moreover it also encompasses KM issues related to people and technology in telecom sector. The results of this study are based on field interviews /observations and will be compared with existing body of research in the field.

Keywords : *saudi telecom, knowledge management, taxonomy, knowledge management strategy.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

Integration of Knowledge Management System in Telecommunication: A Case Study of Saudi Telecom

Khalid AlRowaily[α] & Abdulaziz O.Alsadhan[σ]

Abstract - **Accelerated business growth has pushed telecommunication companies to implement knowledge management systems to systematically manage knowledge created within the organization. This helps them to retain their competitive edge in the rapid changing telecom sector. This study plan to explore the emerging role of Knowledge Management (KM) system in telecommunication industry. Moreover it also encompasses KM issues related to people and technology in telecom sector. The results of this study are based on field interviews /observations and will be compared with existing body of research in the field.**

Keywords : saudi telecom, knowledge management, taxonomy, knowledge management strategy.

I. Introduction

Telecommunication got immense growth in the last few years. Saudi Telecom (STC) is one of the growing telecom sectors worldwide. The rapid growth in this market makes it one of the leading businesses in Saudi Arabia The mutual understanding of sharing expedient data steadily become the most important perspective in STC culture. KM applications deploy in telecommunications refereeing to the real case study, to identify and observe that how management tools impact the whole business process effectively by allocating resources using KM methods. The best methods of attaining vital information need comprehensive investigation through interview, conferences and analysis reviews.

Subsequently having skilled experiences from field observation, the main emphasis on different events related to KM methods within the telecommunication business. As for more analysis of strengthen and weaknesses of the KM implementation is concerned, this study suggested some recommendation for improvement because future prospectus of KM development still needs improvement within the industry.

a) Role of Knowledge Management in the Telecommunication Industry

Telecommunication has taken up a protracted development history in Saud Arabia economy. Typically it is directly liable for the expansion of the service sector within the community. With state-of-the-art IT infrastructure and excellent world network designed, telecommunication business demonstrates its true price to the Saudi Arabia society. Since 2005, telecommunication market in Saudi Arabia is open for keen competition [13]. Following STC the other 3 new firms (Mobily, Zain and Atheeb) were licensed respectively to produce telecommunication services on a competitive basis. Consequently, a high level of quality in telecommunication services is obtainable within the market at affordable prices. To maintain glorious service and to survive within the competitive market, individual organization has developed a scientific approach resulting in the achievement of final business goals [11,12].

b) Serve as important business intelligence

In [2] the author claims telecommunication industry as the "Sunset industry" due to the reason of rapid growth in technological developments and product innovations. In the competitive environment, to hold a significant position in the market, business organizations have to keep updated with the global trend and current status about telecommunications. "In view of the business structure, telecommunications are featured with hybrid science of collaborations among people, process and technology". To take more benefit business organizations are concerned to integrate these three components with a consistent and promising management system. The advantage of shared knowledge system is to exchange knowledge from individuals to the whole enterprises, in order to retain valuable information and skillful experiences within the companies. "Besides, intellectual capital from workers offers as knowledge experts for business activities and future development at different aspects. When facing business conflicts and production problems, the knowledge intensive process works with the case by providing effective solutions for performance improvement. In addition, business intelligence enhances communications among departments so that co-operative team production can be more integrated with strong collaboration from different divisions. Having a high degree of accuracy and accessibility for

Author α : Department of Information System, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. E-mail : kalrwaily@ksu.edu.sa

Author σ : Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. E-mail : alsadhan@ksu.edu.sa

informationenables the organizations to respond more quickly upon market changes and decision-making"[2].

c) Keep along as good practice captured

In [2] the authors also demonstrate that now a days KM is the essential parameter for industrial growth. By employing professional experts and consultants, workers are trained with the use of KM in order to follow creative ways for the successful achievements of business targets. The interactions between workers and understanding between departments are enhanced by incorporating KM as the key production mechanism. Finding new production processes with the idea of KM, enhance the business feats. Such learning is useful which flows around in the KM cycle for creating new thinking.

d) Manage relationships with key customers

The authors argued that People are the primary core in knowledge management application in the telecommunication market, to assimilate several informative connections to form inventive business knowledge. For conventional telecommunication company, typically sales persons work at the forefront in the business fabrication and deal with consumers to provide high-quality services and in return, gets frequent business connections. By the resources of KM, data is held and kept with suitable arrangements so that it can be easily regained and transported concerning different needs urged from employees. In the past, employees had to hunt out the material in persons and such cases really tool up a long time and even a high cost for business processes [2].

The paper is organized as follows. Section 1 presents the literature review. Section 2 describes Saudi Telecom (STC) as a case study. Section 3 lists findings and results of implementing KM in STC. Finally section 4 concludes the paper.

II. Literature Review

The general introduction of KM is

a) What is KM?

In [6] the authors give the best and simple definition that KM is the set of processes that seeks to change the organization's present pattern of knowledge processing to enhance it and its outcomes.

b) KM in Telecommunications Industry

KM is crucial to all or any styles of trades which might facilitate the organizations to think about how to capture the tenant information within the organization. Mostly in telecommunication sector throughout the world, a large number of data staff have been hired to perform the schedule operation of the organization, it is vital for them to speak and share their knowledge. Therefore, telecom corporations today are willing to invest and capture the maximum amount of knowledge as attainable from their most experienced staff. Some massive telecommunications service provider begins to form a senior-level management position in their organization to make sure that KM operates effectively [7,8]. According to authors in [16],some reputable telecom corporations like British Telecom, AT & T, and Deutsche Telekom have created chief information officer positions in their organization., It demonstrates the fact that the telecommunications industry believe that intellectual assets have worth.

The following numerous factors identified in [16] which are important for an effective KM systems in telecommunication sector.

i. IT supports needs to be adequate in both scale and communications response time.
ii. Database should include user-friendly search capabilities.
iii. Tools in the search engine need to pinpoint the proper information when requested.
iv. Processes need to support the facilitation of information retrieval and must be in place to assist in the creation of new information.
v. System performance metrics should be maintained in order to help to determine the criteria for new data to enter the system.
vi. Type of data to be available must pass tests defined in the design phase, it should be limited to information that will increase the performance of employees or improve the customer's experience.
vii. Effective incentives and supportive core values should be encouraged to the most expert employees to share their knowledge.

People conjointly perpetually argue that the advantages of information management systems seem to be too theoretical to measure; the subsequent is an example of returns from implementing KM in telecommunication trade [5]. Quantification of advantages is most blatant in client service sectors like sales and client support department for instance, a client service center may use a KM system to assist service representatives to spot the supply of issues by listing troubleshooting measures that were successful within the past. Therefore, additional issues are resolved with one decision in client service centers [1]. Telecommunications service suppliers have used KM systems to extend their sales productivity. Sales representatives tend to concentrate on those services sold successfully in past. KM systems will assist to extend sales services by providing data to the sales representative in smaller amount. [9, 10, 17].

The progressive development made in ontologies to represent knowledge. The aim of developing ontologies is to provide flexibility and richness in KM. To develop semantics KM, researchers paying attention to contribute significantly in developing

theoretical and practical understanding of ontologies [3,4].

The authors describe a research project to deploy knowledge networks in a high technology company. The aim of implementing this project was to make deep understanding of network setup and show to be sustained. In this paper two different projects are discussed with two different level of maturity and some tentative modules were analyzed as follows [14, 15].

- To categorize and support knowledge activists.
- Apply strategic agenda to put knowledge networks.
- Major organizational changes may be vulnerable to formal networks.
- To build and understand that how formal networks can coincide with line organization.

III. STC Case Study

This section elaborates the present study and investigation on integration of KM implementation with STC.

a) Saudi Telecom Overview

The following figure shows the years wise planning of knowledge management in STC

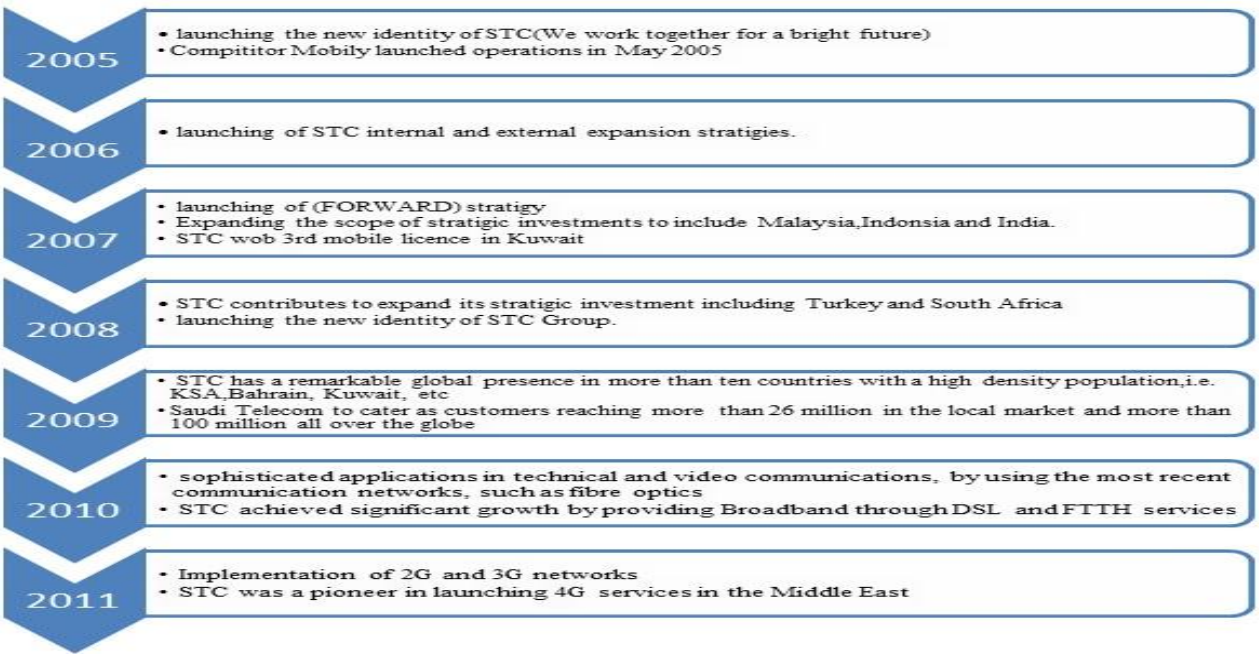


Fig. 1 : Important historical events [18]

b) STC Mission

To be a leader in world of constant change, STC strives to exceed our customer's expectations to reach new horizons

i. *STC Values*

- Loyalty Honesty
- Commitment
- Cooperation
- Respect
- Initiative

c) Saudi Telecom Company Strategy

Fig. 2 : Main STC Strategy [18] (Adopted from STC)

F (**Fulfill Mobile Potential**) Shift voice traffic to mobile and deploy mass 3.5G

O (**Offer Wholesale Services**) Grow wholesale business through broadening service offering to capture revenue opportunity from national and international customers

R1 (**Re-invent Home Communication**) Accelerate retail broadband adoption in the kingdom supported by Multi-Play offering

W (**Win Enterprise Customers**) Address untapped potential in the enterprise customer segment and optimize STC cost to serve

A (**Achieve External Growth**) Pursue non-organic growth aiming at generating 10% of STC revenues from external sources by 2010.

R2 (**Re-organize Internal Structure**) Adopt customer facing organizational model supported by strategic and transactional support functions

D (**Derive Operational Efficiencies**) Implement "True Shared Services" and pursue manpower optimization

1. Maintain the leading role at market and bolster STC competitiveness in the Saudi market
2. Upgrade STC operational efficiency
3. Achieve further expansions abroad

d) Saudi Telecom Organization Structure

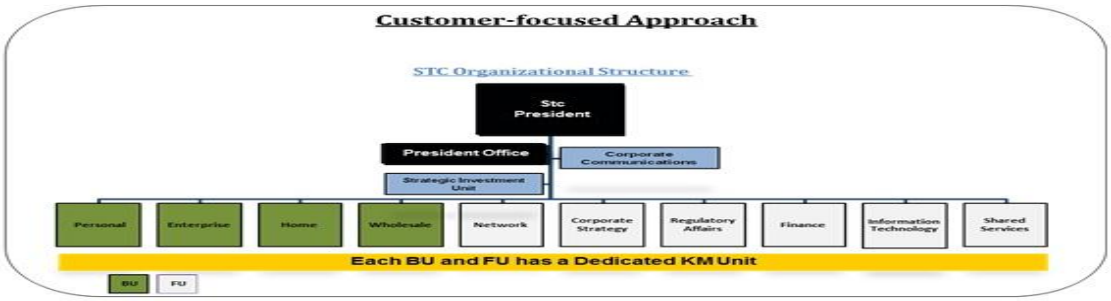


Fig. 3 : KM position in STC hierarchy [18] (Adopted from STC)

e) Project Work Plan

The project work flow having four phases summarized in the following Figure 4:

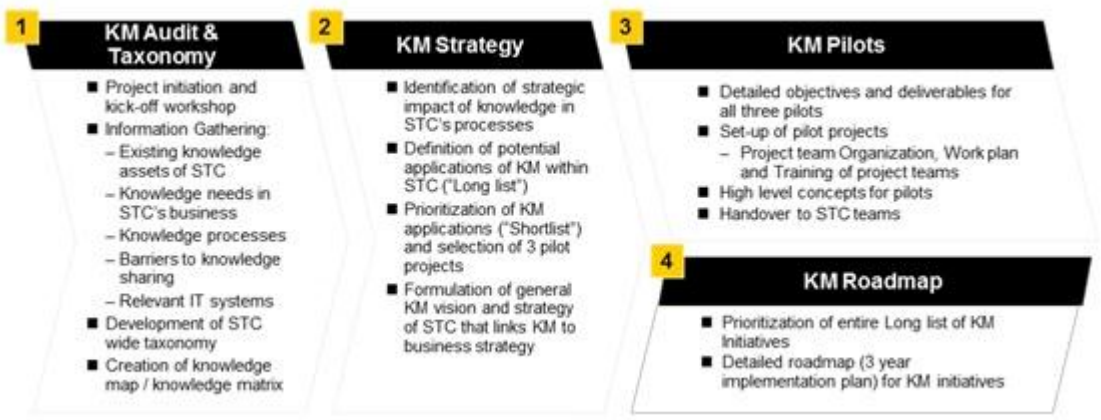


Figure 4 : Project Work Plan[18](Adopted from STC)

i. *KM Audit & Taxonomy*

The different characteristics of KM Audit and Taxonomy are as under

a. *Basic Characteristics of Taxonomy*

Taxonomy is the systematic methodology used to classify data, information & knowledge into a standard hierarchy of ordered groups based on certain natural similarities and relationships.

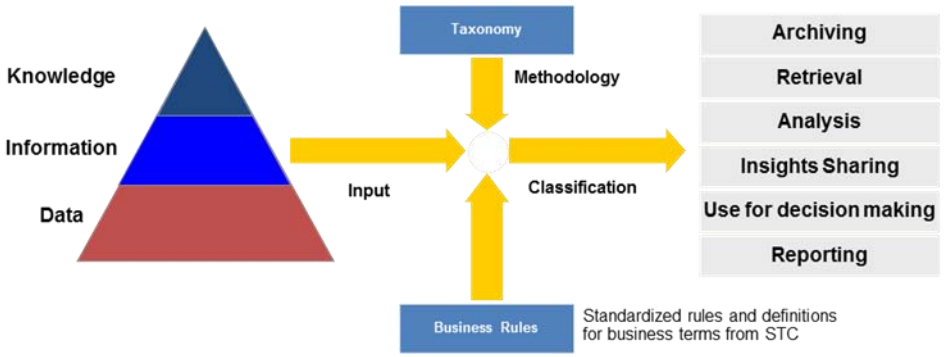


Fig. 5 : Audit & Taxonomy [18](Adopted from STC)

The below are two basic characteristics of Taxonomy:

- Taxonomy is purely a methodology for classification
- It is independent of the company's corporate strategy, and is an enabler which depends on the industry and characteristics of the specific firm under consideration

b. *Knowledge Management and Taxonomy*

Effective knowledge sharing is possible only if a common terminology and classification of concepts exists to create a common ground for sharing in the entire organization.

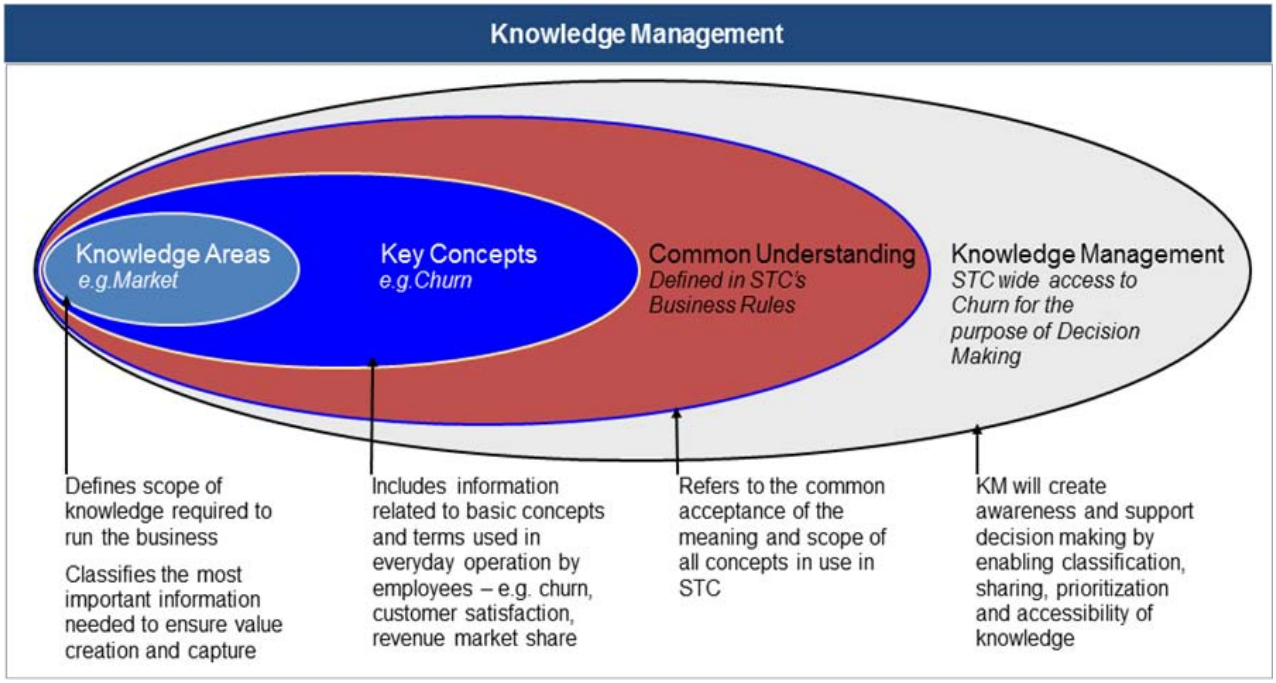


Fig. 6 : KM & Taxonomy[18](Adopted from STC)

c. *Development of Taxonomy – Knowledge Required by STC*

This visual representation gives a view of all the data, information and knowledge – internal and external-required by STC to create and capture value common to all stakeholders, this representation of the business concepts will easily enable everyone in STC to interact and therefore will be used to create a Knowledge Base.

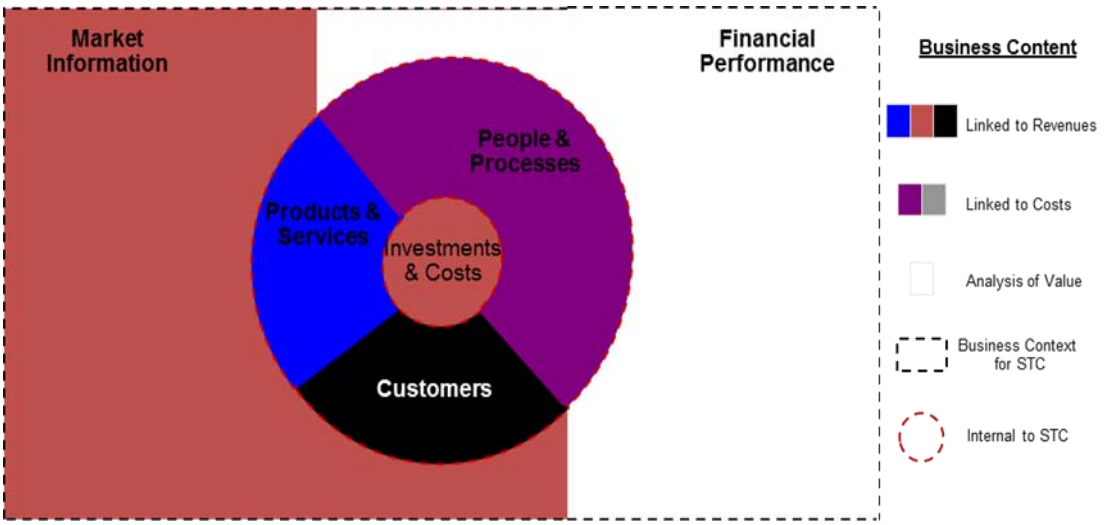


Fig. 7 : Development of Taxonomy[18](Adopted from STC)

d. *Taxonomy- Knowledge Areas*

In this taxonomy, all content of STC categorized into the following seven broad knowledge areas as shown in Fig 9.

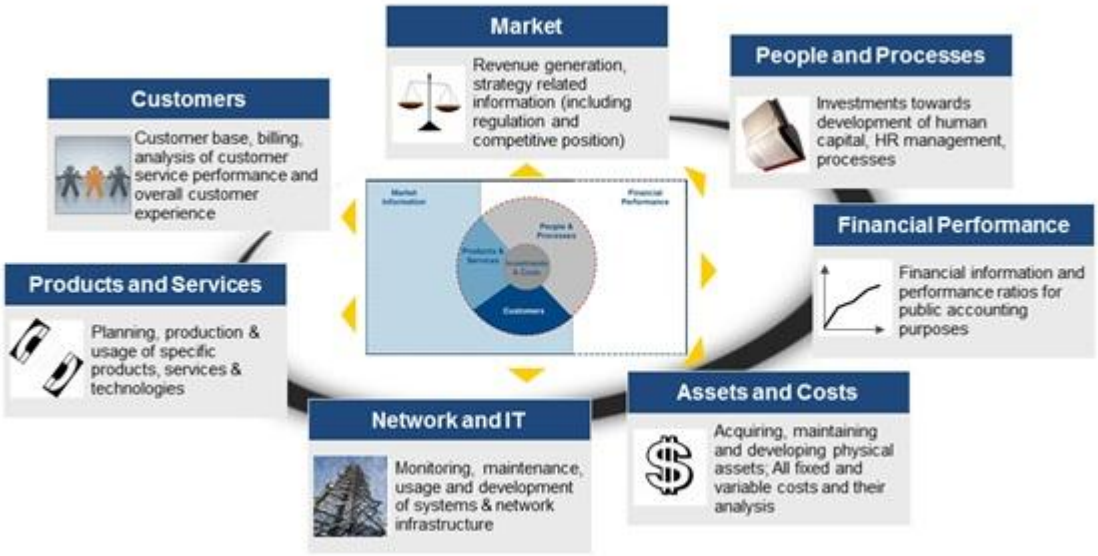


Fig. 8 : Knowledge areas [18] (Adopted from STC)

e. *Deployment of STC Taxonomy-Process for Completion of Concepts*

The concepts lists will be completed by STC across knowledge areas to obtain a version 1 of the lists as addition is possible after periodic intervals.

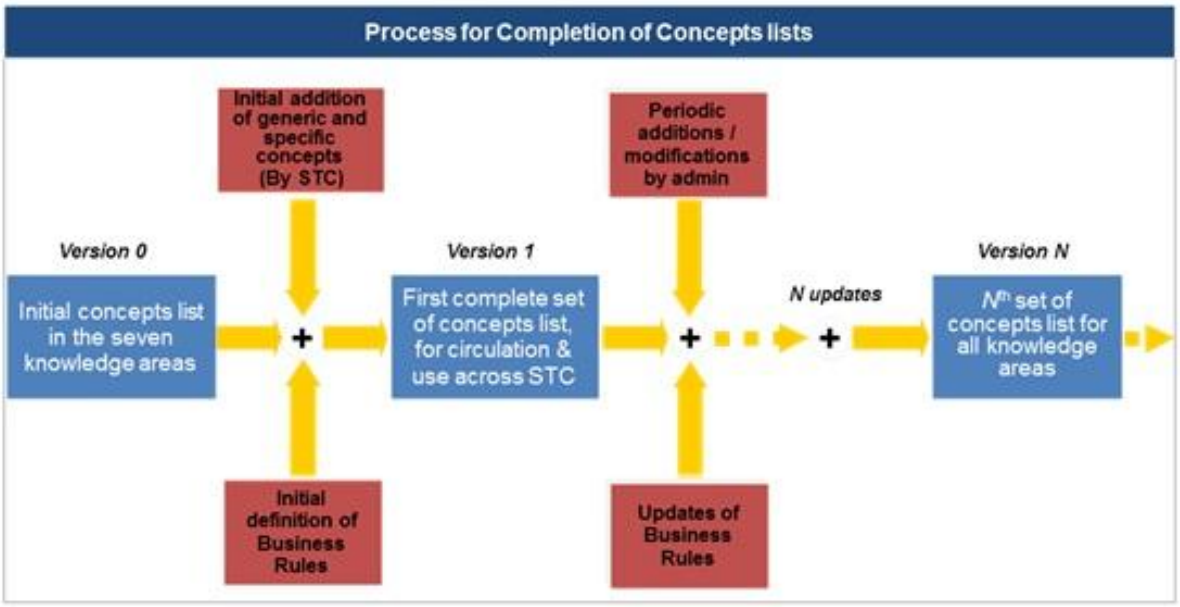


Fig. 9 : Deployment of Taxonomy[18](Adopted from STC)

f. *Deployment of STC Taxonomy – Roles & Responsibilities of the Administrator*

The administrators of the taxonomy will make these additions to the taxonomy, circulate it, train users, and support their needs as explained below:

Administration

- Monitoring, suggesting and managing the periodic addition of new concepts to the taxonomy long lists

Training

- Training of KM, user support within each sector to support and propagate taxonomy usage within sectors
- Training of employees towards using the taxonomy effectively

Taxonomy Support

- Ensure compatibility and integration of business rules in the taxonomy
- Manage email for all queries and taxonomy-support taxonomy@stc.com.sa

Circulation and Usage

- Circulation of taxonomy concepts list across STC
- Fostering use of taxonomy by all STC employees through targeted initiatives

ii. *KM Strategy*

The KM strategy features described below in detail:

a. *KM Strategy Directions*

STC has identified three work streams for the KM strategy to focus on, after analyzing the results of the KM audit and the collaboration requirements to implement FORWARD.

Fig. 60 KM Strategy Direction[18](Adopted from STC)

b. *KM Strategy – Summary*

The KM Strategy is aimed at aligning KM in STC so as to support the execution of FORWARD, with priority on inter-sector collaboration

i. **KM Strategy Objectives**

Completion of 3 KM initiatives in 3 months, 20 initiatives in 18 months and 40 initiatives in 36 months

ii. **Content**

STC identified over 200 telecom concepts & divided them into 3 levels of conceptualization (data, information and knowledge) across **7 knowledge areas**.

iii. **Targeted Groups**

STC has defined the content targets in accordance with the **clusters** arising from FORWARD.

iv. **Organization / Process**

Based on the 4 clusters, STC has created a functional organization structure that enables increased access to content, process efficiencies and superior collaboration, in line with the FORWARD strategy priorities

v. **KM Roles and Responsibilities**

STC increased the complementarities of the KM resources by specializing them either on STC-wide activities, or on specific work streams (**Content Sourcing, User Support and KM initiatives leader**) that benefit all internal clients of each cluster

vi. **Infrastructure / Media**

STC has emphasized the fact that the priority should be **utilizing current infrastructure** to its full potential & increasing the opportunities for knowledge sharing in specific contexts according to FORWARD requirements

vii. **Culture**

STC specified the role of Change Management and drew guidelines to deliver clear messages to employees in order to influence their practices of knowledge sharing

c. *KM Strategy & Objectives*

KM needs to achieve specific short, medium and long term objectives, in accordance with the KM Strategy which supports FORWARD and prioritizes inter-sector collaboration.

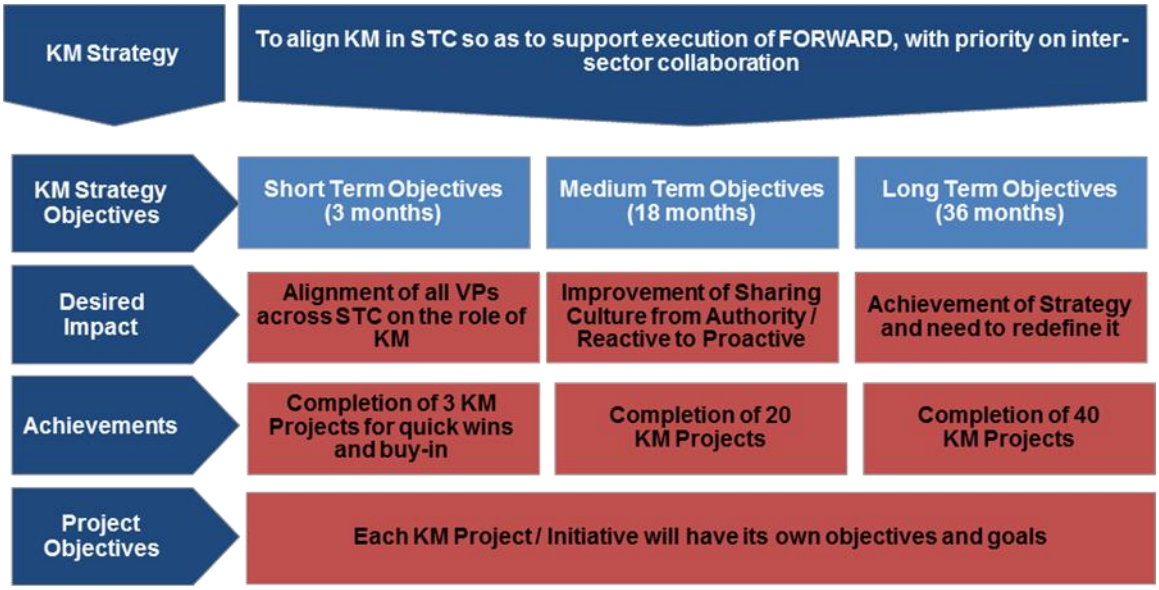


Fig. 71 KM Strategy Objectives[18](Adopted from STC)

d. *KM Strategy Directions- KM Support to FORWARD:*

The specific KM initiatives to support FORWARD, the pilot projects and KM Roadmap will be determined through the following three steps in next phase as shown in following Fig. 13

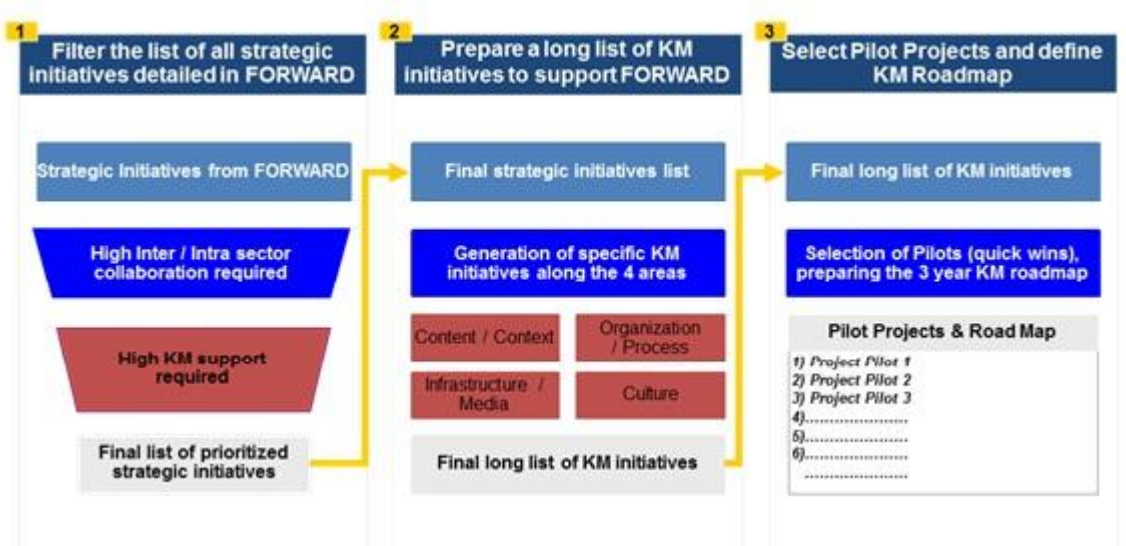


Fig. 82 KM Support to FORWARD[18](Adopted from STC)

iii. *KM Potential Pilot Projects*

The objectives of the prospective pilot projects fall into two categories – to support FORWARD and to put in place the fundamentals required for KM in STC

Potential Pilot Projects

a. *FORWARD*

Objective

Specific KM Initiatives identified to support the FORWARD strategy implementation

Codification used

F1, F2…; O1, O2,…; R1 1, R1 2, …

b. *KM Fundamentals*

Objective

Basic KM Initiatives to support the KM strategy

Codification used

KM Fund 1, KM Fund 2, KM Fund 3, …

The list of prospective pilots will contain both KM Initiatives to support FORWARD, & initiatives to set up KM Fundamentals in STC, which will be later used to select the top 2 pilot projects for quick wins.

c. *Two main pilot projects*

STC has shortlisted number of potential pilot projects after prioritizing the entire KM long list in terms

of quick wins (ease of implementation and business impact). Below are the first two:

i. Retention Best Practices

Initiative Name: Share best practices for retention and win back strategy between Personal and Home

Project Description

- Within STC, the Personal BU has been in a competitive market for a few years while Home is now starting to face competition. In this context, Home needs a strong retention program to avoid churn.
- The project will bring together retention teams from Home and Personal and leverage their experience in customer retention, through
  - Identification of existing best practices for retention in both BUs, and analyzing the potential synergies between them
  - Creation of new retention best practices resulting from the knowledge sharing between sectors
- The implementation will require some joint efforts between the marketing teams and additional support from Customer care, Human Capital and IT

Objectives

- Support the FORWARD strategy in its customer retention objectives
- Create new common programs between the two Sectors, based on current Best Practices

Deliverables

- Personal and Home presentations of Best Practices
- New Best Practices presentations and implementation plans
- Training materials

ii. Business Rules

Initiative Name: Finance to develop and share business rules for STC-specific concepts (from the taxonomy) across all sectors.

Project Description

- STC specific concepts may be defined in different ways, and need to be explicitly defined & commonly agreed upon across STC
- Business Rules will define them so as to be generally accepted across the entire organization
- Examples of STC specific concepts
  - Revenue (defined for STC based on revenue recognition)
  - Churn (defined for STC based on when a customer is designated as churning)
- Concepts defined by Business Rules need to be tagged (marked out) in Systems and Media. Users will then be able to refer to the definitions of these concepts and reaffirm their understanding of the term

Objectives

Provide a common definition for key business concepts used across STC, so as to

- Have a common understanding of STC-specific concepts
- Ensure that these concepts are used systematically for all content across the organization

Deliverables

- List of Business Rules (definition and specification)
- Business rules creation, storage, sharing and update processes
- Systems to support storage and sharing of Business Rules
- Committee for definition and maintenance of Business Rules

iv. *KM Roadmap*

The following are the two main characteristics of KM road map. The specific KM objectives for Saudi Telecom using a proven KM approach shown in Fig. 14.

- Prioritization of entire Long list of KM Initiatives
- Detailed roadmap (3 year implementation plan) for KM initiatives

Fig. 10 : STC KM approach [18](Adopted from STC)

IV. Findings and Analysis of the Case Study

KM integration in Telecom sector helps to improve monitoring, assessing, etc., STC has also implemented various policies to improve some functional units of customer services and attain satisfactory result up to some extent. But still exist a little resistance from functional unit's staff. The following areas in customer services have been improved.

- The ability of front line to solve customer complaint.
- Realizing of needs of customer service center and marketing department.
- The functional units level of communication.

In result of achieving such e benefits, management has considered some changes in the future, such as:

- Dedicated functional unit to track the quality of service (QoS).
- Improve marketing environment and tools, e.g. online marketing, marketing through games and competition, to improve the self-service motivation.
- Giving more authority to the outstanding performing employees.
- Staff has given incentives and awards on their performance to motivate him for future.

V. Conclusion

Learning from the real case study, literature and KM text books, maintaining the sustainability of KM is a long term task. It concludes that success of KM project in an organization depends on the involvement and contribution of all the parties, especially strong initiative and passionate Top Management. The inter-related characteristics of KM create the complexity on real world practice. In order to develop an Enterprise-wide KM, an integrated view must be adopted. The courtesy should not be only given to theoretical and technology aspects, but also the cultural adoption and education among the participants needs to be given more attention.

This study helps in implementing different policies to improve various functional units and achieve satisfactory results. Customer services also improved like ability of front line to solve customer complaints, to realize needs of customer service and marketing departments.

This study also gives clue to management for future change such as to track quality of service (QoS), Improve marketing environment using various tools i.e. online marketing, marketing through games and competition

In this study, the paper outlined the role of KM in the telecommunication industry. On the basis of Literature review, KM integration and implementation is analyzed in Saudi Telecom (STC) as a case study and finally some findings and results are highlighted.

References Références Referencias

1. Auckland, Marc. .COMPETING THROUGH KNOWLEDGE. Knowledge Management Review, vol.1 (6), 2-6,(1999)
2. Chang Mei Ying, WIndy; Chow Wai Ching, Vivian; Huen Mei Ying, Harmony; Lam Tsz Kwan, Katherine; Yeung Sum Sze, Cissie.." Knowledge Management cases in Asia/Knowledge Management Practice in Telecommunication Industry Commissioned Report". London(2010).
3. Coleman, D "Taking the best approach to knowledge management". Computer Reseller News, 791, pp.111-112. (1998).
4. Davies, N J. " Knowledge Management. BT Technology" Journal ,vol 62 pp.1-12 ,2000.
5. Dykeman, J.B." Knowledge management moves from theory toward practice". Managing Office Technology, 43, pp.12-14,(1998)
6. Joseph M. Firestone, Mark W. McElroy, "Doing knowledge management", Learning Organization, The, Vol. 12 Iss: 2, pp.189 – 212,(2005)
7. Kogut, B. & Zander, U.)." Knowledge of the firm, combinative capabilities, and the replication of technology". Organization Science, 3(3), pp.383-96. (1992)
8. Lewis-Chan, Betsy. ". BUILDING POWER TOOLS FOR KNOWLEDGE WORKERS". Knowledge Management Review,vol. 1(5), pp.22-27,(1998)
9. Malhotra, Y. " Deciphering the Knowledge Management Hype". Journal for Quality & Participation, 53, pp.58-60.(1998)
10. Minogue-White, Lisa. ." CAPITALIZING ON INTERNAL EXPERTISE AT ORANGE". KM Review, vol.9(5), pp.24-27, (2006)
11. Nonaka, I "Harvard Business Review.", The Knowledge creating company, 6 (8), pp. 96-104,(1991).
12. Nonaka, I. & Takeuchi, H.. "The Knowledge-Creating Company - How Japanese Companies Create the Dynamics of Innovation". New York: Oxford University Press.(1995)
13. http://www.ofta.gov.hk/en/index.html "Office of the Telecommunications Authority, Hong Kong. (2007).
14. Orlikowski, W.J. . Knowing in practice: enacting a collective capability in distributed organizing. Organization Science, vol.13(3), pp.249-73,(2002)
15. Schönström, M. ". Creating knowledge networks: lessons from practice", Journal of Knowledge Management,vol. 9(6),pp. 17-29,(2005)
16. Strouse, Karen G. " Strategies for Success in the New Telecommunications" Marketplace. Boston: Artech House Telecommunications Library,(2001)
17. Wiig, K. " Knowledge Management: Where Did it Come From and Where Will It Go?". Journal of Expert Systems with Applications,Vol. 13(1),pp. 50-60,(1997).

18. http://www.stc.com.sa/cws/portal/en/stc/stc-landing/stc-lnd-abtsaudtelc/stc-lnd-abtst-anlrpt

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Security in Wireless Sensor Networks

By Koffka Khan, Wayne Goodridge & Diana Ragbir

The University of the West Indies

Abstract - Wireless Sensor Networks (WSNs) pose a new challenge to network designers in the area of developing better and secure routing protocols. Many sensor networks have mission-critical tasks, so it is clear that security needs to be taken into account at design time. However, sensor networks are not traditional computing devices, and as a result, existing security models and methods are ill suited. The security issues posed by sensor networks represent a rich field of research problems. Improving network hardware and software may address many of the issues, but others will require new supporting technologies. With the recent surge in the use of sensor networks, for example, in ubiquitous computing and body sensor networks (BSNs) the need for security mechanisms has a more important role. Recently proposed solutions address but a small subset of current sensor network attacks. Also because of the special battery requirements for such networks, normal cryptographic network solutions are irrelevant. New mechanisms need to be developed to address this type of network.

Keywords : *wireless sensor networks, routing, protocol, security, cryptographic.*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

Security in Wireless Sensor Networks

Koffka Khan [α], Wayne Goodridge [σ] & Diana Ragbir [ρ]

Abstract - Wireless Sensor Networks (WSNs) pose a new challenge to network designers in the area of developing better and secure routing protocols. Many sensor networks have mission-critical tasks, so it is clear that security needs to be taken into account at design time. However, sensor networks are not traditional computing devices, and as a result, existing security models and methods are ill suited. The security issues posed by sensor networks represent a rich field of research problems. Improving network hardware and software may address many of the issues, but others will require new supporting technologies. With the recent surge in the use of sensor networks, for example, in ubiquitous computing and body sensor networks (BSNs) the need for security mechanisms has a more important role. Recently proposed solutions address but a small subset of current sensor network attacks. Also because of the special battery requirements for such networks, normal cryptographic network solutions are irrelevant. New mechanisms need to be developed to address this type of network.

Keywords : wireless sensor networks, routing, protocol, security, cryptographic.

I. Introduction

Wireless Sensor Networks (WSNs) are made up of a group of sensor nodes; each node is equipped with its own sensors and actuators, radio frequency transceiver, power source, processing capability – Digital Signal Processing (DSP) chips [1] or CPUs and memory [2], which can monitor and sense changes in the environment and forward that data to a sink or base station in the network. Sensor nodes can measure a variety of properties in the environment based on the sensors and actuators that are built into them. These include physical properties – pressure, temperature, humidity, flow; motion properties – acceleration, velocity, position; contact properties – force, strain, vibration, slip, torque; presence – proximity, motion, tactile/contact, distance/range; biochemical; identification – vision, retinal scans, fingerprints; noise levels; and lighting conditions [1].

The sensors in-built into the nodes depend on the specific application area in which the WSN is implemented. WSNs have been used traditionally in military applications but other areas include environmental such as ocean, wildlife, wildfire, and pollution monitoring; medical such as wearable sensors – temperature measurement, respiration and heart monitors, glucose sensors, and implanted sensors – endoscope capsule, brain liquid pressure sensor, cardiac arrhythmia monitor; crisis management; smart spaces; building safety and earthquake monitoring; water quality monitoring; and machinery performance monitoring in production and delivery [5], [10].

Given the broad range of applications, there is intensive, active research being undertaken in WSNs involving networking, hardware and system design, distributed algorithms, data management, and security. At present most of the major wireless sensor network (WSN) routing protocols are insecure, because during their initial development very little emphasis was put around security as a foremost goal. However it became a relevant issue with the deployment of such networks, for example, in border control systems. Due to the complexity involved addressing the security issues of WSNs is non-trivial to fix. Emphasis must be placed around the routing protocols of sensor networks themselves and security must be designed using a bottom-up approach, that is, it must be designed into the protocol from scratch or during the earliest possible development time for such networks.

There are specific classes of attacks which affect wireless sensor networks and are applicable to only such types of networks. This is because wireless sensor networks have special characteristics (security protocols cannot maintain much state, communication bandwidth is extremely dear, power is the scarcest resource of all, which distinguish themselves from other types of networks, for example, mobile ad hoc networks. Further to this countermeasures and design considerations for sensor networks (we must discard many preconceptions about network security) need to be proposed or developed to address the special needs for such networks. Because power is the most important consideration when deploying such networks, public key cryptography cannot be used as it is too expensive. Even fast symmetric-key ciphers must be used sparingly. Hence some ad-hoc network security mechanisms based on key cryptography are unsuitable for sensor networks.

New security mechanism must be proposed for wireless sensor networks. In I we introduce the problem statement. Attacks on sensor network routing are discussed in I. Section III shows some countermeasures and conclusions are given in IV.

II. Problem Statement

The characteristics of WSNs that make security a difficult challenge, in terms of being different from security in traditional networks, are their limited power,

Author α : Koffka Khan. E-mail : koffka.khan@sta.uwi.edu
Author σ : Wayne Goodridge. E-mail : wayne.goodridge@sta.uwi.edu

communication and processing or computation capabilities [5], [11]. Additional challenges to security in WSNs are that they operate in real-time as opposed to not real-time, have dynamically changing sets of resources as opposed to a fixed set of resources, the aggregate behavior of all nodes is important as opposed to a wired network where every node is important, their location is critical as opposed to location independent networks and finally, they utilize sensors and actuators instead of screen and mice as interfaces to the nodes. WSNs also communicate wirelessly, are deployed in an ad hoc fashion and are self-organized.

Römer and Mattern in [3] offered dimensions in the design of WSNs which could be used to better understand what security measures should be implemented in a given WSN. The first dimension of design is network size – nodes can range from a few to thousands and the size of the network affects the design of protocols and algorithms. The lifetime of WSNs can be measured in hours or up to years and impacts the power efficiency and robustness of nodes. Connectivity within a WSN can be fully connected all the time, have intermittent connectivity or designed to be sporadic – nodes occasionally enter the transmission range of other nodes. Connectivity has an influence on methods of data gathering and choice of communication protocols.

Furthermore, coverage within a WSN can be sparse, dense, or redundant based on the degree of coverage of the nodes in the network. High coverage (redundant nodes) is important to the robustness of the network. The topology of the WSN is another dimension and can be single-hop, star, tree or graph; this affects the diameter of the network which influences latency, robustness and capacity. Heterogeneity of the WSN means either it consists of homogenous nodes in terms of hardware and software or heterogeneous, where nodes can be different devices with various functions. This affects complexity and security of the system. Complexity and security of the system is also affected by the cost, size, resource and energy dimensions of a WSN.

Other dimensions include mobility – degree of mobility, frequency of movement, active or passive movement; deployment – one-time or continuous set up of nodes, random locations or chosen spots; communication modality – radio, light, inductive, capacitive or sound transmissions; and finally quality of service (QoS) – robustness, real-time constraints, eavesdropping resistance, tamper resistance and unobtrusiveness or stealth. These dimensions also impact security measures in various ways.

These unique characteristics and design dimensions of WSNs pose constraints to applying existing security approaches and provide obstacles in developing security defenses [4]. These unique characteristics and dimensions contain several vulnerabilities of WSNs to which threats can occur. When threats are carried out, they are considered attacks.

Generally radio links are insecure. Nodes can be either a general type or one with more capabilities (generally the base stations with more transmitting power). The adversary can deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes or can "turn" a few legitimate nodes into threat agents. Since sensor nodes were not developed with security in mind these nodes are not tamper resistant. Base stations are generally assumed to have a higher trust factor, while aggregation points can be suspect of being threat agents.

Threat models are categorized as being either mote-class attacks versus laptop-class attacks or outsider attacks versus insider attacks. For WSNs the security goals that should be prioritized are integrity, authenticity and availability of messages.

III. Sensor Network Routing Attacks

First, several threat models will be explained, followed by the attacks categorized by the network architecture layer to which they apply. There are two types of attackers, mote class and laptop class. Mote class attackers only have access to a few nodes, whereas, laptop class attackers have access to more powerful devices such as laptops with great battery power, powerful CPUs, sensitive antennas and high power radio transmitters. Two types of attacks include insider and outsider attacks. In an insider attack, the attacker is considered to be an authorized member of the network, whereas, outsider attackers do not have authorized access to the network. Additionally, insider attacks can take place from laptops using stolen data from legitimate nodes or from compromised sensor nodes.

Attacks in the first four layers of the network architecture are now discussed [7], [12]. The attacks in the Physical layer are Jamming and Tampering [7]. Jamming occurs when an adversary blocks the radio frequencies that legitimate nodes are using. A complete Denial of Service (DoS) (cf. Figure 1) occurs if the adversary blocks the entire network. Tampering refers to physical damage, replacement or modification of a node or part of a node. Damage to sensors, modification of circuitry, replacement of a node's hardware or of the entire node, and replacement of sensors with malicious sensors are examples of tampering. Additionally, an adversary can interrogate nodes electronically to gain access to cryptographic data and information on accessing other communication layers.

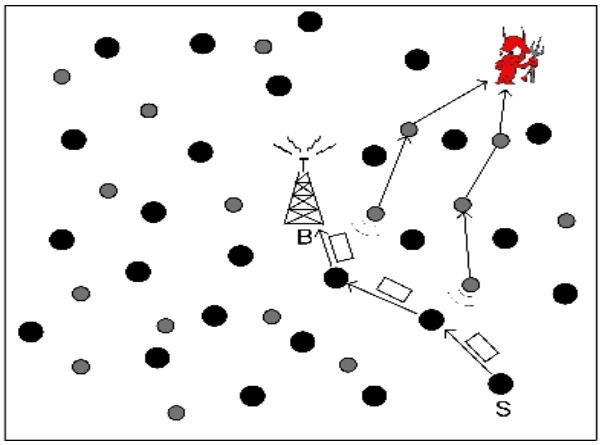


Fig.1 : Denial of Service Attack

Collisions, Unfairness and Exhaustion are attacks in the data link layer [7]. Collision is a type of link layer jamming. Part of the transmission is corrupted so that a mismatch in the checksum occurs. This leads to a disruption of the packet. Also, an attacker could deny access to a channel, intentionally, leading to more collisions in other channels or to packets never being received at the destination.

Unfairness happens when MAC priority schemes are abused, which leads to degradation of service though loss of real-time deadlines. Exhaustion attacks aim to drain power resources of the node.

In the data link layer, repeated retransmissions even after late collisions can drain power. Also, compromised nodes can self-sacrifice by continuously asking for access to a channel; its neighbors are then forced to respond with a 'clear to send' message, draining resources of many nodes.

The network layer has the most kinds of attacks - spoofed, altered or replayed information; Sybil attacks; sinkhole attacks; selective forwarding; hello flood attacks; wormholes; and acknowledgement spoofing [7]. Firstly, Spoofed, Altered or Replayed Information is the most direct attack. Here, the attacker complicates the network and many negative consequences may result including the creation of routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, replay attacks (cf. Figure 2), increase end-to-end latency, etc.

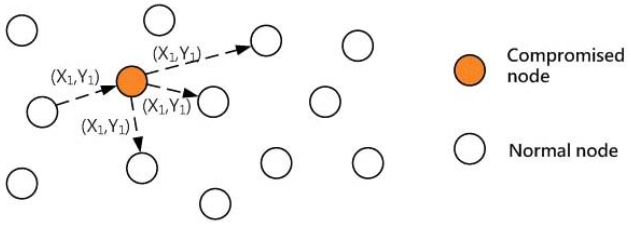


Fig. 2 : Replay Attack

The Sybil attack works by using a compromised node to pose multiple identities to the network in order to confuse geographic routing protocols, since the adversary appears to be in multiple locations at once (cf. Figure 3). The Sybil attack targets fault tolerant schemes such as multipath routing, dispersity, distributed storage and topology maintenance.

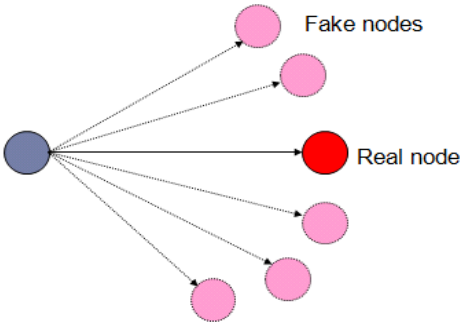


Fig. 3 : Sybil Attack

In Sinkhole attacks, the goal is to bait traffic to a malicious part of the network (cf. Figure 4). This is done by first making a compromised node look appealing to its neighbors in terms of routing of packets. The compromised node advertises low latency routes and fooled legitimate neighbor nodes forward their packets to the lying node, thus creating a sinkhole in the network.

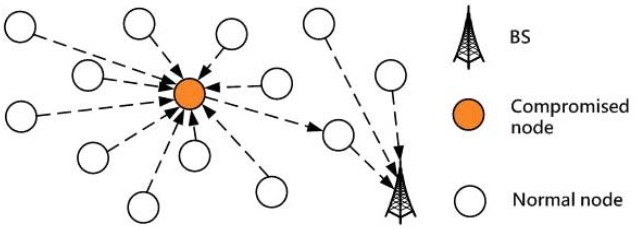


Fig. 4 : Sybil Attack

In Selective Forwarding, an adversary includes itself in the data flow path of interest. (cf. Figure 5) The adversary can then choose not to forward packets sent to it, thus creating a kind of black hole. Instead, the adversary can drop packets that come from a specific source while continuing to route all other packets reliably. In this case, the attack is harder to detect.

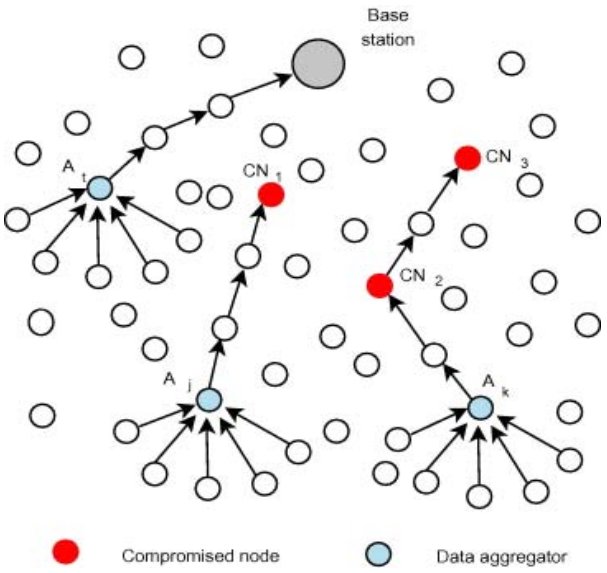


Fig. 5 : Selective Forwarding

In Wormhole attacks, the messages received in one part of the network are channeled over a low latency link, to be replayed in another part of the network (cf. Figure 6).

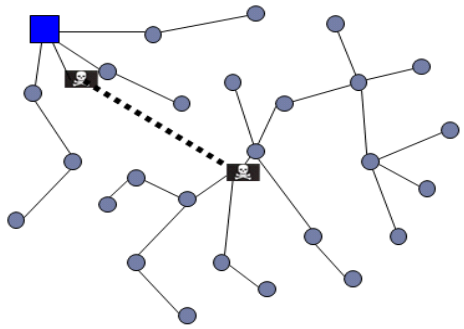


Fig. 6 : Wormhole Attack

In this attack, faraway nodes are convinced that they are neighbors, thus quickly depleting their power resources through inefficient routing. For instance, an attacker near the base station can convince nodes which are many hops away that they are close to the base through the wormhole.

HELLO' messages are broadcasted to announce their presence to neighboring nodes (cf. Figure 7). In the Hello Flood attack, the goal is to convince every node in the network that it is its neighbor, as well as advertising that it has a high quality route. This is done by the attacker using a high powered antenna. Thus, nodes that are a great distance away from the attacker will send packets to it, into oblivion, since the messages will never reach, causing confusion in the network.

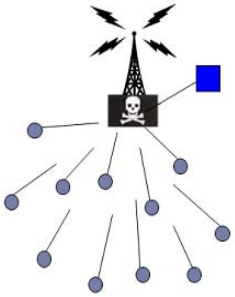


Fig. 7 : HELLO Flood Attack

Another attack is called Acknowledgement Spoofing (cf. Figure 8). The acknowledgement packet is spoofed to convince the node that a weak link is strong or a dead node is alive. Essentially, packets sent along such links will be lost. Protocols prone to this attack are those that choose the next hop based on reliability issues.

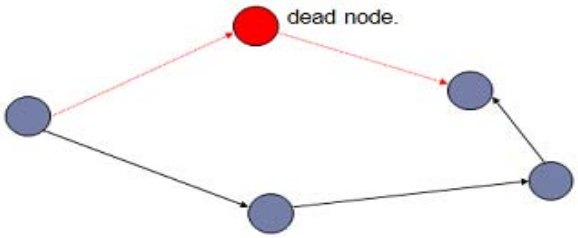


Fig. 8 : HELLO Flood Attack

In the transport layer Flooding and Desynchronisation attacks occur [7]. Flooding is similar to SYN attacks in TCP and the aim is to deplete a victim's memory resources. When many connection establishment requests are sent, the victim must allocate memory to maintain state for each connection, thus eventually overloading its memory. In desynchronisation, the attacker forges messages between sender and receiver, changing sequence numbers and control flags in the packet header. The sender and receiver could be prevented from ever exchanging messages if the attacker gets the timing right since they will continually request retransmission of previous invalid messages. This causes an infinite cycle which depletes power resources.

There are four additional attacks that will not be discussed within a particular network layer. These are Traffic Analysis attacks, Node Replication attacks, attacks against Privacy and Data Aggregation attacks [8]. There are two types of traffic analysis attacks, rate monitoring attack, in which nodes closest to the base station are observed as forwarding more packets than those farther away from the base, and time correlation attacks, in which the adversary generates an event to be sensed and observes to whom packets are sent. In both cases, the base station can be determined and disabled.

In Node Replication attacks, the ID of an existing sensor node in the WSN is copied. This can disrupt network performance through corrupted and misrouted packets leading to false sensor readings and a disconnected network. Also, if physical access is gained and cryptographic keys are copied, the replicated node can be inserted at strategic points in the network leading to manipulation or disconnection of a certain part of the network. Monitoring, eavesdropping, traffic analysis and camouflaging of adversary nodes in the network are all attacks against privacy.

Due to the computational constraints placed on individual sensor nodes, Data Aggregation [5] is used where some nodes act as aggregators and are responsible for collecting the raw data from nodes and processing/aggregating it into more usable data. This technique is vulnerable to attack since only the aggregator node needs to be targeted. A specific attack called the Stealthy attack seeks to provide incorrect results to the user without its knowledge.

IV. Countermeasures

This section looks at solutions to each of the attacks described in the previous section. Firstly, in Jamming, spread spectrum communication, at least until the jammers figure out how to block a wider part of the radio frequency band, is one solution. Code spreading is another, but it requires more design effort and power. Changing the mode of communication to infrared or optical can work but is costly. Also, the network can be made to switch to a low power cycle which it is under attack [7]. Additionally, channel hopping and blacklisting are part solutions [9]. Finally, neighboring nodes under attack could alert the base station, or could observe a change in the background noise of their neighbours and send an alert [7].

For Tampering, it is necessary to provide tamper-resistant packaging, but this is costly [7]. Camouflaging of nodes, programming nodes to erase sensitive data on capture [7] and protection and changing of keys are alternative solutions [9].

For prevention of Collision attacks, collision detection, error correcting codes – though costly, cyclic redundancy checks (CRCs) and time diversity are possible solutions [9]. For prevention of Unfairness attacks, prevent the channel from being captured for long time periods using small time frames [7]. To prevent exhaustion attacks, the problem of indefinite postponement during collisions can be solved using time division multiplexing [7]. Additionally, the link layer can ignore excessive requests without having to send radio messages by using the MAC admission control rate. Finally, protection of network ID and other data that is required for joining the network is part solution [9].

To defend against data being Spoofed, Altered or Replayed, link layer encryption and authentication must be used [7]. Also, use of different paths for resending failed messages can work [9]. For Selective Forwarding, redundancy via multi-path routing as well as regular network monitoring using source routing are adequate defenses [7], [9].

The countermeasure to the Sybil attack is verification of identities of participating nodes [7]. The first step is to have each node share a unique key with the base station. Then, two neighboring nodes can share data by encrypting data using a shared key and verifying the link between them. The base station can limit the number of legitimate nodes a compromised node can communicate with by limiting the number of verified neighbors a node can have. However, a compromised insider can still participate in the network, but should only be allowed through using compromised identities and no additional ones. Sybil attacks can also be prevented in the lower layers by regular changing of keys, resetting and physical protection of devices [9].

Since wormholes use invisible channels and the routes advertised by sinkholes are hard to verify, it is difficult to defend against Wormhole and Sinkhole attacks [7]. One solution is to use Geographic Routing Protocols which routes messages to the physical location of the base station. False links are easily discovered when the physical distance of a route exceeds the radio signal ranges of nodes. Providing tight time synchronization is another solution, but this is difficult. Finally, regular monitoring of the network and physical monitoring of field devices can be done [9].

Hello Flood attacks can be defended against by determining whether action should be taken on information received over a link through verifying the bi-directionality of that link [7]. This is known as the Needhan-Schroeder verification protocol. The base station can prevent this attack entirely by reducing the number of verified neighbours. Defense against Acknowledgement Spoofing entails authentication using encryption of all sent packets and packet headers [7]. Countermeasures for WSN attacks are shown on Table I.

Attacks	Countermeasures
Link layer	Link layer encryption. Selective forwarding, sinkhole and Sybil attacks stopped
Selective forwarding	Use multi-path routing and probabilistic-based routing.
Sybil	Unique symmetric keys. Verify identities of neighbors
Wormhole	Use private channel
Sinkhole	Verify routing metric information (such as remaining energy).
HELLO flood	Verify the bi-directionality of a link
Outsider	Authentication using a globally shared key. Selective forwarding, sinkhole and sybil attacks stopped

Table 1 : Countermeasures for WSN attacks [13]

To prevent Flooding attacks, the sender must solve a puzzle in order to get a connection. The puzzle is distributed with each connection request [7]. To flood the network, the attacker has to consume more energy; however, to get connected, legitimate nodes also have to use up additional resources. For Desynchronisation, two solutions can be used. The first is to authenticate all packets sent and all control fields, but requires expenditure of resources for legitimate nodes [7]. The second is to use different neighbours for time synchronization [9]. For Traffic Analysis attacks, regular monitoring of the network and sending of dummy packets in quiet hours are solutions [7], [9]. For Eavesdropping, defenses are using keys to protect the Data Link Protocol Data Unit and the Transport Protocol Data Unit from eavesdroppers [9].

Finally, in Stealthy attacks, data plausibility checks can be used, but requires some redundant information [8]. Additionally, multiple levels of aggregator nodes, use of deviation query where only values that deviate from a pre-defined base are transmitted, and the (CDA) concealed data aggregation approach using encryption can be used [6]. On Table II are shown security schemes for WSNs.

Security Schemes	Attacks	Major Features
JAM	DoS Attack (Jamming)	Avoidance of jammed region by using coalesced neighbour nodes
Wormhole based	DoS Attack (Jamming)	Uses wormholes to avoid jamming
TinySec, TinyPK [8]	Data and information spoofing, Message Replay Attack	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & µTESLA	Data and information spoofing, Message Replay Attack	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead
SMACS – Self-Organized Medium Access Control for Sensor Networks, EARS – Eavesdrop and Register [12]	Data Link Layer protocol for WSNs [12]	Responsible for medium access, error control, multiplexing of data streams and data frame detection. Correcting of transmission errors [12]
SMECN – Small Minimum Energy Communication Network, LEACH – Low Energy Adaptive Clus-tering Hierarchy [12]	Network Layer Protocols for WSNs [12]	Responsible for intra-network operation, different type addressing routing information through the sensor network, finding the most efficient path for a packet to travel on its way to a destination [12]
Zigbee, 802.15.4 Standard [7]	Shared Keys, encryption [7]	Hardware-based symmetric keying [7]
DES – Data Encryption Standard, 3DES – triple DES, RC5, AES [8]	Use in symmetric cryptography [8]	Utilizing a shared key for both encrypting and decrypting data. [8]
LIDS – local intrusion detection system [8]	An intrusion detection architecture [8]	All LIDS within the network exchange both security data and intrusion alerts. [8]
Statistical En-Route Filtering	Information Spoofing	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution	Sybil Attack	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting Sybil entity
Bi-directional Verification, Multipath multi-base station routing	Hello Flood Attack	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security	Information or Data Spoofing	Efficient resource management, Protects the network even if part of the network is compromised
TIK	Wormhole Attack, Information or Data Spoofing	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Pre-distribution	Data and information spoofing, Attacks on information in Transit	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
REWARD	Black hole attacks	Uses geographic routing, Takes advantage of the broadcast inter-radio behaviour to watch neighbour transmissions and detect black hole attacks

Table 2 : Security Schemes for WSNs [4]

V. Conclusions

Because of these strict requirements of wireless sensor networks modern security mechanisms needs to be developed. These security solutions have to be incorporated into the network protocol and have to be adapted to suit the nature of sensor networks. Currently proposed solutions solve specific attacks and much more work has to be done to find solutions that would solve the majority of sensor network attacks. Presently research efforts have been made on cryptography, key management, secure routing, secure data aggregation, and intrusion detection in WSNs, but there are still some challenges to be addressed. First, the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application-specific. Second, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. With advances in

technology motes may get stronger and existing solutions, though limited, will have to be upgraded to meet the new technological landscape.

Two future research topics are: (1) Exploit the availability of private key operations on sensor nodes: recent studies on public key cryptography have shown that public key operations may be practical in sensor nodes. However, private key operations are still very expensive to realize in sensor nodes. As public key cryptography can greatly ease the design of security in WSNs, improving the efficiency of private key operations on sensor nodes is highly desirable. (2) QoS and security: performance is generally degraded with the addition of security services in WSNs. Current studies on security in WSNs focus on individual topics such as key management, secure routing, secure data aggregation, and intrusion detection. QoS and security services need to be evaluated together in WSNs. By more carefully considering the threats posed to sensor networks, applications with intrinsic security considerations become immediately realizable.

References Références Referencias

1. Lewis, F. L. 2004. Wireless Sensor Networks. In Smart Environments: Technologies, Protocols, and Applications. Ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004. Available: http://arri. uta. edu/acs/networks/WirelessSensorNetChap04.pdf
2. Stankovic, J. Wireless Sensor Networks. Chapter in Handbook of Real-Time and Embedded Systems, CRC Press, 19 pages, 2008. Available: https:// www.cs.virginia.edu/~stankovic/psfiles/wsn.pdf
3. Römer, K., Mattern, F. The Design Space of Wireless Sensor Networks. IEEE Wireless Communications, Vol. 11, No. 6, pp. 54-61, December 2004. Available: http://wsn. cse. wustl. edu/images/8/8c/Wsn-design04.pdf
4. Khan Pathan, A., Lee, H., &Hong, C. S. Security in Wireless Sensor Networks: Issues and Challenges, Proceedings of the 8th International Conference on Advanced Communication Technology (IEEE ICACT 2006), Volume II, 20-22 February, Phoenix Park, Korea, 2006, pp. 1043-1048. Available: http://arxiv. org/ftp/arxiv/papers/0712/0712.4169.pdf
5. Perrig, A., Stankovic, J., & Wagner, D. Security in Wireless Sensor Networks, In Communications of the ACM (CACM), Vol. 47, No. 6, June 2004. Available: http://www.cs.virginia.edu/~stankovic/ psfiles/security.pdf
6. Westhoff, D., Girao, J., & Sarma, A. Security solutions for wireless sensor networks. NEC Journal of Advanced Technology, 59(2), June 2006. Invited paper. Available: http://www.ist-ubisecsens.org/ publications/SecuritySolutionsWSN.pdf
7. Kaplantzis, S. Security Models for Wireless Sensor Networks. Supervisors Dr, N. Mani, Prof. M. Palaniswami, Prof G. Egan. CiteSeerX: 10.1.1.87.4605, 2006. Available: http://members. iinet.com.au/~souvla/transfer-final-rev.pdf
8. Walters, J.P., Liang, Z., Shi, W., & Chaudhary, V. Wireless sensor networks security: a survey, Technical Report MIST-TR-2005-007, July 2005. Available: http://www.eecis.udel.edu/~fei/reading/ 070426.wsn.security.survey.pdf
9. Kalita, H., K., Kar, A. Wireless Sensor Network Security Analysis. International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009. Available: http://airccse.org/ journal/ijngn/papers/1.pdf
10. Ameen, M., A., Jingwei, L., & Kyungsup, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. Journal of Medical Systems. 2012-02-01. Springer Netherlands.SN - 0148-5598, Pg 93 – 101. Vol 36. No. 1. DOI 10.1007/s10916-010-9449-4, 2012. Available: http://dx.doi.org/10.1007/s10916-010-9449-4
11. Sora, D. Security Issues in Wireless Sensor Networks. International Journal of Online Engineering (iJOE). 6(4): 26-30 (2010). ISSN: 1861-21216, 2010. Available: http://www.online-journals. org/index.php/i-joe/article/view/1466
12. Singh, S., Verma, H., K. Security For Wireless Sensor Network. International Journal on Computer Science and Engineering (IJCSE) 3(6), 2393 – 2399. 2011. Available: http://www.enggjournals.com/ ijcse/doc/IJCSE11-03-06-131.pdf
13. C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE Int'l Workshop on Sensor Network Protocols and Applications, May 2003.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Network Security in Organizations Using Intrusion Detection System Based on Honeypots

By Mukta Rao & Dr Nipur

Gurukul Kangri Vishwavidyalaya, Haridwar, India

Abstract - The role of the Internet is increasing and many technical, commercial and business transactions are conducted by a multitude of users that use a set of specialized / sophisticated network applications. Today we face threats of the network which cause enormous damage to the community day by day to the Internet. In this context, the task of network monitoring and surveillance is of utmost relevance and honeypots are promising tools for information and understanding of "areas of interest" of the attackers, and the possible relationship between blackhat teams. In this situation, people are increasingly trying to prevent their network security using traditional mechanisms, including firewalls, Intrusion Detection System, etc. Among them honeypot is a versatile tool for a practitioner security, of course, they are tools that are intended to be attacked or interacted with other information about the attackers, their motives and tools. In this paper, we describe a comparative analysis of various IDS and their usefulness on various aspects. Two major categories of HoneyPot viz. low interaction honeypot and high-interaction honeypot have also been discussed in detail. In this paper, low-interaction honeypot is used as a traffic filter. Activities such as port scanning can be effectively detected by the weak interaction honeypot and stop there. Traffic that cannot be processed by the weak interaction honeypot is delivered over high-interaction honeypot. In this case, the weak interaction honeypot is used as a proxy for high-interaction honeypot then offer optimal realism.

Keywords : *intrusion detection system, honeypot, network security, ip address mapping.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

Network Security in Organizations Using Intrusion Detection System Based on Honeypots

Mukta Rao [α] & Dr Nipur [α]

Abstract - The role of the Internet is increasing and many technical, commercial and business transactions are conducted by a multitude of users that use a set of specialized / sophisticated network applications. Today we face threats of the network which cause enormous damage to the community day by day to the Internet. In this context, the task of network monitoring and surveillance is of utmost relevance and honeypots are promising tools for information and understanding of "areas of interest" of the attackers, and the possible relationship between blackhat teams. In this situation, people are increasingly trying to prevent their network security using traditional mechanisms, including firewalls, Intrusion Detection System, etc. Among them honeypot is a versatile tool for a practitioner security, of course, they are tools that are intended to be attacked or interacted with other information about the attackers, their motives and tools. In this paper, we describe a comparative analysis of various IDS and their usefulness on various aspects. Two major categories of HoneyPot viz. low interaction honeypot and high-interaction honeypot have also been discussed in detail. In this paper, low-interaction honeypot is used as a traffic filter. Activities such as port scanning can be effectively detected by the weak interaction honeypot and stop there. Traffic that cannot be processed by the weak interaction honeypot is delivered over high-interaction honeypot. In this case, the weak interaction honeypot is used as a proxy for high-interaction honeypot then offer optimal realism.

IndexTerms : intrusion detection system, honeypot, network security, ip address mapping.

I. Introduction

No matter how well defended your chicken coop is, a sly fox still finds the hole and carry off the most fat chicken. All the holes do not shut up ... But you can try to catch a fox in a trap by placing it towards a tempting bait, and then - Broads! - Shot at point-blank from a gun. With computers - the same story. The software is vulnerable and prone to all attacks. The timely installation of patches, cuts off only the most stupid of the hacker attacks, and is not accustomed to think of his head. Professional burglars also involved in an independent search for new holes, patches do not stop.

This tactic is commonly used for the detection of computer attacks. Vulnerable server is installed in a conspicuous place in the network, safely isolated from all other nodes. This server tracks unauthorized access attempts in real-time transmission of IP-address of the attacker in the FSB or similar bodies. Even if the hacker hides behind clever words (proxy), IDS will still find it and coming out of the trap of an IDS is not an easy task[1-3].

The server, acting as a decoy, the hacker jargon is called a ***"honey pot,*** a network of such servers, respectively, ***honeynet.*** A more practical, but more restrictive, definition is given by pcmag.com: "A server that is configured to detect an intruder reflecting an actual production system. It appears as a ordinary server doing a job, but all data and transactions are false. Located inside or outside the firewall, the honeypot is used to learn about techniques intruders, and to identify vulnerabilities in the real system "[4]. The etymology of this name goes back to the English belief that if you leave a pot of honey, the bees will fly to it (the hackers). Honeypots [3-9] can be useful for two main purposes. The first relates to an important possible assistance in finding rootkits, Trojans and potential risks of the network. The second objective relates to the chances of obtaining information and understanding of "areas of interest 'of attackers and the possible relationship between “blackhat” teams. Despite the relevance of the problem, only a limited number of works devoted to illustrate the results obtained by inspection of the network are present in the literature [10]. The honeypot logs all actions and interactions with users. Since honeypots do not provide legitimate services, any activity is prohibited (and possibly malicious). In practice working of honeypots is being analogous to the use of wet cement to detect human intruders [11].

The value of a Honeypot is directly proportional to the quantity and type of information that we can achieve with success from it. In addition to the collection of information, a honeypot has the ability to distract opponents from the most important machines on a network, and can provide warning signs of a new type of attack and exploitation trends, and provides a thorough examination of adversaries during and after exploitation of a host. Another function that allows the capture of Honeypot is key entered by an opponent attempting to compromise the Honeypot - this provides a particularly interesting if an attacker uses the compromised host as an IRC chat server. Two levels of interaction Honeypots are described as low and high interaction.

The honeypot was the first publicly available as Deception ToolKit by Fred Cohen in 1998 which was "intended to reveal to attackers as if the system works

Author α : Gurukul Kangri Vishwavidyalaya, Haridwar, India.

DTK a large number of known vulnerabilities" [12]. More honeypots became both publicly and commercially available throughout the nineties. As began to proliferate from 2000, honeypots proved imperative to capture and analyze the worms. In 2004, virtual honeypots were introduced that allow you to run multiple honeypots on a single server. The paper laid the groundwork for the honeyd project and describes building virtual honeypots which meet help honeypots meet the need to monitor a large network address space [13]. A detailed history of honeypots can be found in [14] and [15].

To resist honeypot is extremely difficult. Externally, they are no different from the normal servers, but in reality are well-disguised Trap[16]. One false step and the hacker has nothing to help.

II. Inside the Pot

A typical honeypot is a huge hardware-software complex consisting of the following components: a node-bait, a network of sensor and the reservoir (storage media)[17].

There are currently two types of honeypots: a physical honeypot is a real machine with its IP address, and a virtual honeypot is simulated by some another machine that reads network traffic. Physical honeypots are often termed as high-interaction, since the system can be totally compromised and are expensive to install. For instance- if someone wants to implement physical honeypot for a given/specified range of IPs on the LAN, he should create a separate physical honeypot for each IP address. Virtual Honeypots are often labeled as low interaction due to the implementation of low cost maintenance features.

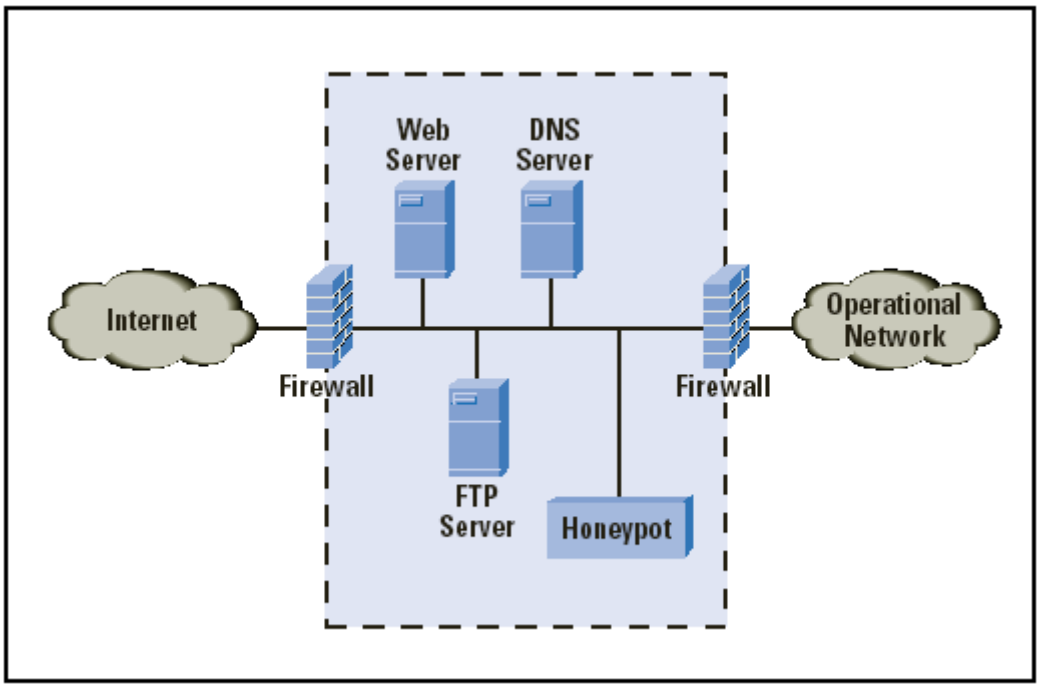


Figure 1 : Common Strategy for placement of Honeypot in Network

The other variety of HoneyPot i.e. virtual honeypot is able to simulate services of multiple operating systems together, and maintain a separate TCP / IP stack for each instance of a Honeypot on that one machine. An example of a virtual honeypot service is Honeyd, which simulates almost all TCP / IP interactions of target multiple operating systems, in order to fool TCP / IP stack fingerprinting tools like Nmap from xProbe. These Virtual honeypots are used more frequently than physical honeypots because they are low in cost as lesser computer systems are required, which eventually reduces maintenance costs. The other advantage is that they provide a greater variety of hosts to be observed.

Sensor network is most often realized on the basis of a UNIX-like operating systems, and for monitoring the information tcpdump utility is used or its analogs. Depending on network configuration, the sensor can be found as one of the nodes in this segment of the LAN and a router, located in front of the honeypot[18]. Sometimes the sensor network is combined directly with the bait as shown in figure 3. This greatly simplifies and reduces the cost of the system of honeypot, but it weakens the immune system (taking control of the lure, the attacker will quickly discover the sensor and make him safe). Placing the sensor in the broadcast segment gives it the greatest secrecy[19]. Network interface sensor may not have its own IP-

address, listening to traffic on Stealth-mode, which is achieved by physically cutting the wires transmitting the NIC[17].

Dumps collected from tcpdump and others are processed by different analyzers (eg, intrusion detection systems) in the first place that recognize the fact of the attack, and secondly, determining the IP-address of the offender. Intrusion related information ends up in the reservoir, which is the heart of the database. This is the most vulnerable spot of honeypot. Administrator must choose in advance a clear set of criteria to uniquely identify what actions are normal and what are not. Otherwise, the administrator will either be constantly jerking, shivering from each port scanning, or skip lightly modified version of the well-known attacks.

There is another problem. If the bait has no other traffic, except for the hacker (which is easy to determine the nature of change in the ID field in the IP-packet headers, details of which were described in an article by wagner [20]. Then the attacker shall immediately recognize the trap and will not attack it. If the lure is serving the users outside the network then direct analysis of the traffic dump becomes impossible and the attacker does not cost anything. Very effective bait is a database with credit card numbers or other confidential information (of course, spurious.) Any attempt to access this file, as well as the use of stolen information on the usages of debit cards is a clear indication of cracking. There are other ways to catch offenders, but they are somehow reduced to rigid patterns and, hence, in principle, unable to detect hackers with non-trivial way of thinking.

III. Preparation for the Attack

To start the hacker will need a reliable channel of communication from the authorities that could not trace him. Strictly speaking, all channels are monitored, however, the degree of security of each of them different. If you are in a broadcast network, the successful cloning of masking can restrict someone else's IP and MAC-address (of course, cloned vehicle at the time of the attack must be inactive). Provided that the network does not impose any additional equipment to determine the perpetrators, to identify the attacker is practically impossible, although there is a "but." If the machine is vulnerable to hackers, honeypot can quietly throw his computer "bug" with all the ensuing consequences. Many novice attackers are caught in the cookie, passed through a browser.

a) Tearing the veil of darkness

Before, to rush into battle, you must carefully examine his opponent: to reconstruct the network topology, determine the place of greatest congestion of opposing forces and, of course, to try to identify all the honeypots. The main weapon at this stage, the hacker will attack the port scanner that runs through "dumb" node and therefore concealing reliable IP-attacker. Clearly vulnerable server is better to discard, where a high probability of being caught with them are present.

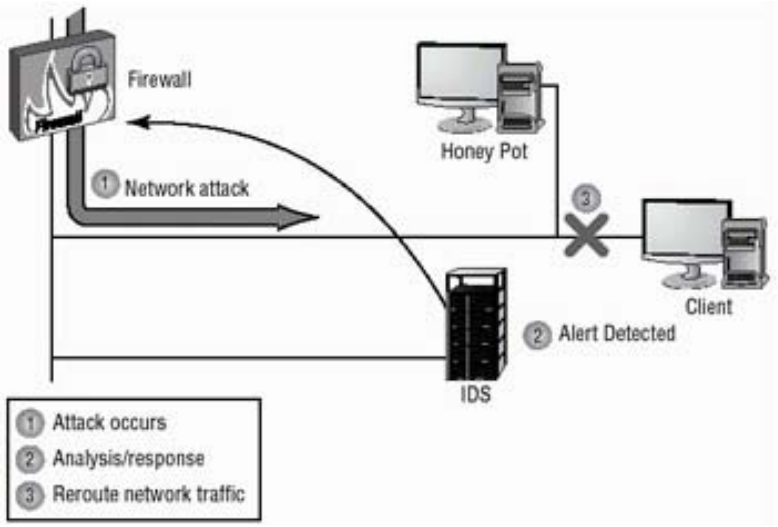


Figure 2 : Network Attack being defended

It is safest to attack workstations, corporate networks, bred for the firewall (if it really is). The probability of running into a honeypot is minimal. Unfortunately for the attacker, workstations contain a lot less holes than a server-based applications, and therefore to attack here, and nothing in particular.

IV. Attack on the Honeypot

Being by nature common network node, honeypot subject to various DoS-attacks [21]. The most vulnerable network sensor is obliged to listen to all the passing traffic. If an attacker can take it out of

the game, the fact that the invasion of the system at some time go unnoticed. Naturally, the attacked site should stay alive, otherwise no one will attack. We assume that the sensor to take all the packages, then sending a packet to a nonexistent node, or addressed to any other unnecessary node.

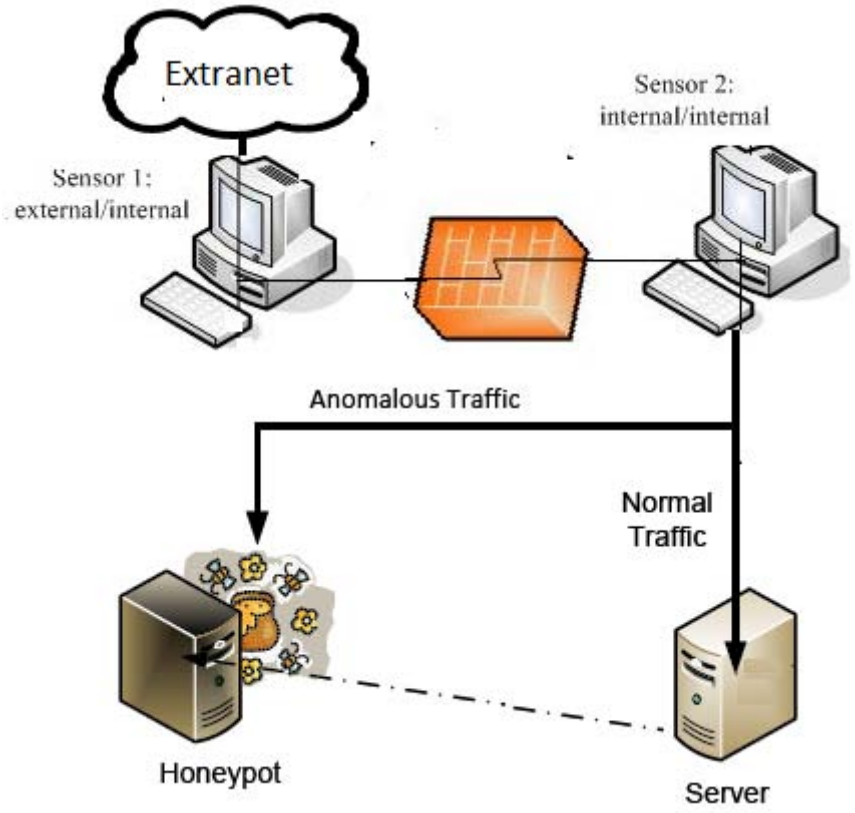


Figure 3 : Dual Sensor Based Arrangement For Anomaly Detection

Alternatively, one can flood the network of SYN-packets (look on the internet description of the SYN-attack) or call the ECHO - death (Storm ICMP packets directed at the victim with a few dozen high-end servers, which is achieved by spoofing IP-addresses - That is, sending echo requests from the victim's behalf)

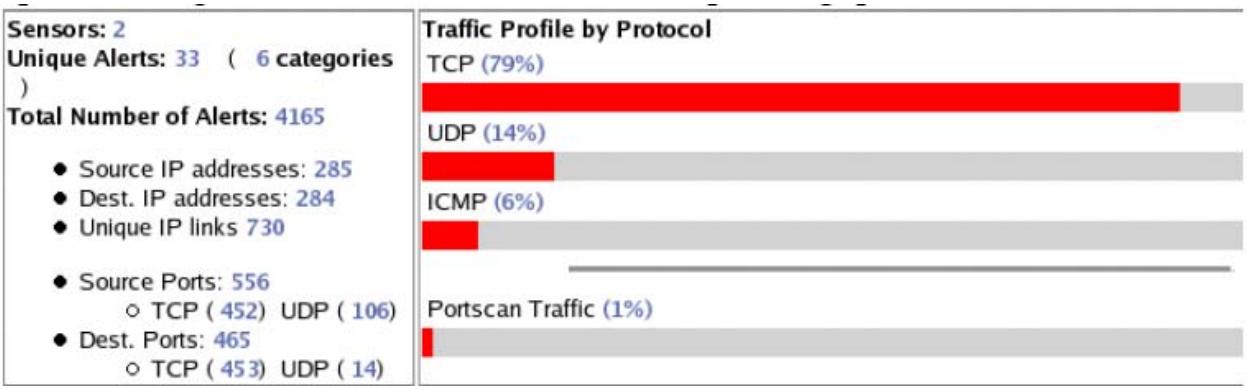


Figure 4 : Snap-Shot of IDS Capturing/Monitoring Network Interactions

The very same attack is best done over the protocols that are resistant to the interception of traffic, and support transparent encryption, blinding the sensor network. Most often used for this purpose SSH (Secure Shell), however, it limits the choice of attacking only the explicit support of its nodes, which negates the whole advantage of the encryption.

V. Drowned in Honey

If the attacked site had Honeypots installed, the attacker will not take any success (the vulnerable server silently "eats" an abandoned shell-code, continuing to work properly), or show empty resource does not contain almost anything interesting because Honeypots are dumb stations. In this situation the

main thing is not to panic and not to get confused. The first step is to get rid of compromising your Machine by disconnecting from network for some time. Next is to destroy everything related to the attack, software and related files, including temporary. Naturally, the above applies only to attacks on the really serious resources (government websites, banking institutions, etc.). Expect that after breaking someone's home page for you will take seriously, a bit naive. Reinstallation of web-pages will temporarily resolve the issue and then after the behavior/pattern of attack should be made learnt to the IDS. An example of such sequence of actions has been shown in Figure-5 below.

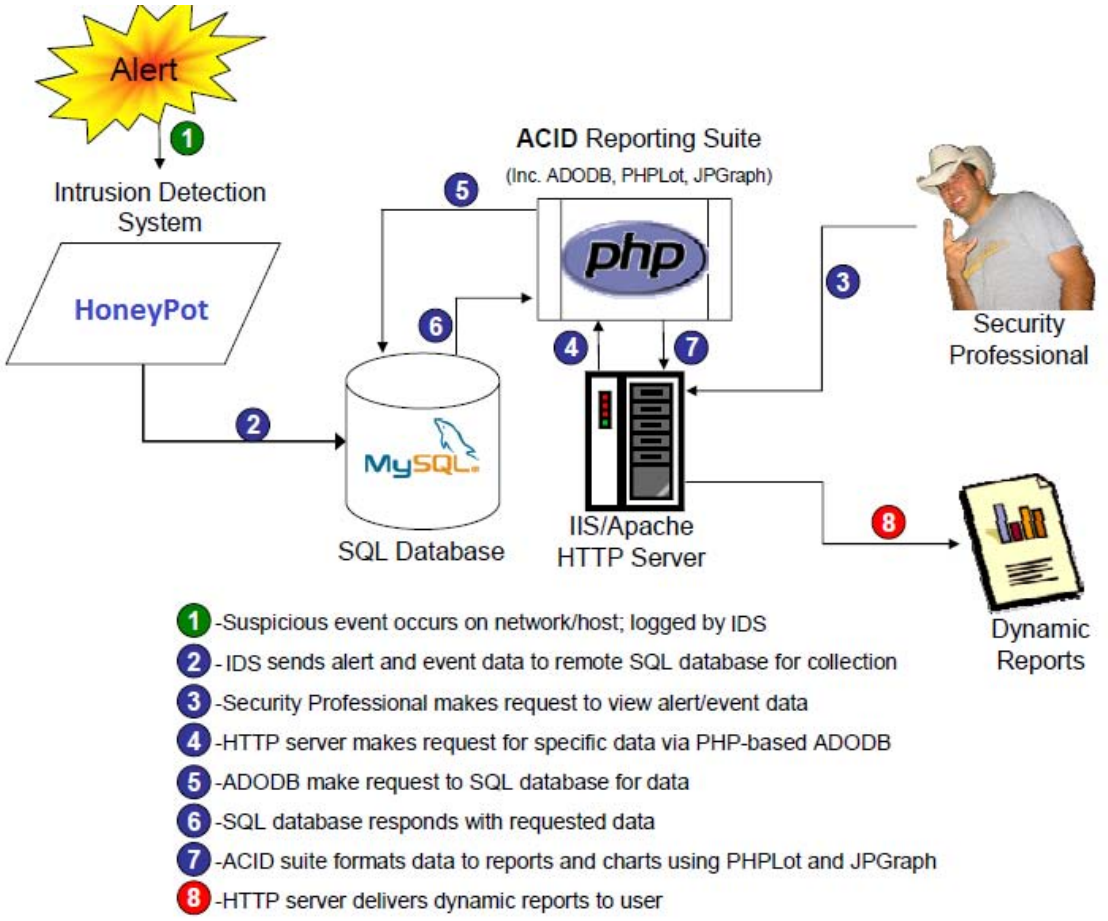


Figure 5 : The Attacker Thinks He Is Attacking The Vulnerable Service, In Fact, He Fells Into A Pot (With Honey)

VI. Conclusion

The strength of honeypot lies in their novelty and obscurity. Hackers are no adequate methods of confrontation with them, however one should not expect that such a balance of power will continue in the future. Architecture of honeypot is still ill-defined and vulnerable. Even today, nothing is impossible for experienced attacker (to bypass honeypots), tomorrow every teenager shall be capable of bypassing such IDS.

Honeypots are positioned to become an essential tool for defending the corporate enterprise from hacker attacks, it is a way to spy on your enemies, it might even be a form of concealment. Hackers could be misled into thinking they have achieved a corporate network, when in reality they are just kicking around a honey pot, while the real network remains safe and sound. Honeypots have gained increased prominence in the strategy to protect against intrusions overall business. Security experts do not recommend that these systems replace existing technologies for intrusion detection security, they see the honeypots as a complementary technology to protect against network and host intrusion.

The advantages that honeypots provide to intrusion protection strategies are difficult to ignore. In time, as security officials understand the benefits, honeypots will become an essential ingredient in a operation of enterprise-class security. We believe that although honeypots have legal problems now, they do provide useful information regarding the security of a network. It is important that new legal policies be formulated to promote and support research in this area. This will help solve the current challenges and

make possible to use honeypots to benefit the Internet community at large.

References Références Referencias

1. Sobh TS. Wire and wireless intrusion detection system: classification, good characteristics and state of art. Computer Standard Interface 2006; 28(6):670–694.
2. Münz G, Li S, Carle G. Traffic anomaly detection using K-means clustering. Proceedings of GI-IGT Workshop, MMBnet, Hamburg, September 2007; 13–14.
3. Sourour M, Adel B, Tarek A. Ensuring security in depth based on heterogeneous networks security technologies. International Journal of Information Security 2009; 8(4):233–246.
4. honeypot Definition - PC Magazine. pcmag.com. 24 March 2009. http://www.pcmag.com/encyclopedia_term/ 0,2542,t=honeypot&i=44335,00.asp PC Magazine's encyclopedia entry for honeypot
5. Intrusion Detection, Honeypots, and incident Handling Resources. Available from: www.honeypots.net.
6. Spitzner L. Honeypots: Tracking Hackers. Addison Wesley: Boston, MA, 2002. ISBN 0-321-1095-7.
7. Development of the Honeyd Virtual Honeypot. Available from: www.honeyd.org.
8. Project Honey Pot. Available from: www.projecthoneypot.org.
9. The Honeynet Project. Available from: www.honeynet.org/project.
10. Verwoerd, Theuns and Ray Hunt. "Intrusion detection techniques and approaches." Computer Communications 15 September 2002: 1356-1365. Aavailable at http://sureserv.com/technic/datum_detail.php?id=468
11. Talabis, Ryan. "Honeypots 101: A Honeypot By Any Other Name." 2007. Available http://www.philippinehoneynet.org/index2.php?option=com_docman&task=doc_view&gid=1&Itemid=29
12. Cohen, Fred. "The Deception ToolKit." The Risks Digest 9 March 1998.The announcement can be found at http://catless.ncl.ac.uk/Risks/19.62. html#subj11
13. Provos, Niels. "A Virtual Honeypot Framework." In Proceedings of the 13th USENIX Security Symposium. 2004. 1-14. . The paper is located at http://www.citi.umich.edu/techreports/reports/citi-tr-03-1.pdf.
14. Spitzner, Lance. Honeypots: Tracking Hackers. Addison-Wesley Professional, 2002.
15. Talabis, Ryan. "Honeypots 101: A Brief History of Honeypots." 2007. Available at http://www.philippinehoneynet.org/index2.php?option=com_docman&task=doc_view&gid=2&Itemid=29
16. Anagnostakis, K. G., et al. "Detecting targeted attacks using shadow honeypots." Proceedings of the 14th conference on USENIX Security Symposium. ACM, 2005. 129-144.
17. He, Xing-YuLam, Kwok-Yan, et al. "Real-Time Emulation of Intrusion Victim in HoneyFarm." Content Computing. Springer Berlin / Heidelberg, 2004. 143-154.
18. Mukherjee, B., L. Heberlein and K. Levitt. "Network Intrusion Detection." IEEE Network May/Jun 1994: 26-41
19. honeynet Project. "Know Your Enemy: Honeynets." 24 March 2008. http://old.honeynet.org/papers/honeynet/
20. Wagner, David and Paolo Soto. "Mimicry Attacks on Host-Based Intrusion Detection Systems." Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002. 255 - 264. Available at http://www.scs.carleton.ca/~soma/id-2007w/readings/wagner-mimicry.pdf
21. Hussain, Alefiya, John Heidemann and Christos Papadopoulos. "A framework for classifying denial of service attacks." Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. ACM, 2003. 99 - 110.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Designing and Implimentation of Spatial IP Address Assignment Scheme for a Wireless Network

By Fazal Wahab Khattak

ICMS, Hayatabad, Peshawar, Pakistan

Abstract - Wireless sensor networks are composed of large numbers up to thousands of tiny radio- equipped sensors. Every sensor has a small microprocessor with enough power to allow the sensors to autonomously form networks through which sensor information is gathered. Wireless sensor networks makes it possible to monitor places like nuclear disaster areas or volcano craters without requiring humans to be immediately present. Many wireless sensor network applications cannot be performed in isolation; the sensor network must somehow be connected to monitoring and controlling entities. This research paper investigates a novel approach for connecting sensor networks to existing networks: by using the TCP/IP protocol suite in the sensor network, the sensors can be directly connected to an outside network without the need for special proxy servers or protocol converters.

Bringing TCP/IP to wireless sensor networks is a challenging task, however. First, because of their limited physical size and low cost, sensors are severely constrained in terms of memory and processing power. Traditionally, these constraints have been considered too limiting for a sensor to be able to use the TCP/IP protocols. In this research paper, I show that even tiny sensors can communicate using TCP/IP. Second, the harsh communication conditions make TCP/IP perform poorly in terms of both throughput and energy efficiency.

With this research paper, I suggest a number of optimizations that are intended to increase the performance of TCP/IP for sensor networks. The results of the work presented in this research paper have a significant impact on the embedded TCP/IP networking community. The software evolves as part of the research paper has become widely known in the community. The software is mentioned in books on embedded systems and networking, is used in academic courses on embedded systems, is the focus of articles in professional magazines, is incorporated in embedded operating systems, and is used in a large number of embedded devices

GJCST-E Classification : C.2.1

Strictly as per the compliance and regulations of:

Designing and Implimentation of Spatial IP Address Assignment Scheme for a Wireless Network

Fazal Wahab Khattak

Abstract - Wireless sensor networks are composed of large numbers up to thousands of tiny radio- equipped sensors. Every sensor has a small microprocessor with enough power to allow the sensors to autonomously form networks through which sensor information is gathered. Wireless sensor networks makes it possible to monitor places like nuclear disaster areas or volcano craters without requiring humans to be immediately present. Many wireless sensor network applications cannot be performed in isolation; the sensor network must somehow be connected to monitoring and controlling entities. This research paper investigates a novel approach for connecting sensor networks to existing networks: by using the TCP/IP protocol suite in the sensor network, the sensors can be directly connected to an outside network without the need for special proxy servers or protocol converters.

Bringing TCP/IP to wireless sensor networks is a challenging task, however. First, because of their limited physical size and low cost, sensors are severely constrained in terms of memory and processing power. Traditionally, these constraints have been considered too limiting for a sensor to be able to use the TCP/IP protocols. In this research paper, I show that even tiny sensors can communicate using TCP/IP. Second, the harsh communication conditions make TCP/IP perform poorly in terms of both throughput and energy efficiency.

With this research paper, I suggest a number of optimizations that are intended to increase the performance of TCP/IP for sensor networks. The results of the work presented in this research paper have a significant impact on the embedded TCP/IP networking community. The software evolves as part of the research paper has become widely known in the community. The software is mentioned in books on embedded systems and networking, is used in academic courses on embedded systems, is the focus of articles in professional magazines, is incorporated in embedded operating systems, and is used in a large number of embedded devices.

I. Introduction

Wireless sensor networks consist of large numbers of sensors equipped with a small microprocessor, a radio transceiver, and an energy source, typically a battery. The sensors nodes autonomously form network through which sensor readings are transported. Applications of wireless sensor networks can be found in such diverse areas as wild-life habitat monitoring [5], forest fire detection [6], alarm systems [3], medicine [8], and monitoring of volcanic eruptions [12].

In order to make large scale networks feasible, the sensor nodes are required to be physically small and inexpensive. These requirements severely constraints the available resources on each sensor node in terms of memory size, communication bandwidth, computation speed, and energy. Many wireless sensor network applications do not work well in isolation; the sensor network must somehow be connected to monitoring and controlling entities.

Since communication within the sensor network is done using short range radios, a straightforward approach to connecting the sensors with the controlling entities is to deploy the controlling entities physically close to the sensor network. In many cases however, placing those entities close to the sensors, and hence to the phenomenon being observed, is not practical.

Instead, by connecting the sensor network and the controlling entities to a common network infrastructure the sensors and the controlling entities can communicate without being physically close to each other. Because of the success of the Internet, the TCP/IP protocols have become the de-facto standard protocol stack for large scale networking. However, conventional wisdom states that TCP/IP is inherently unsuitable for communication.

Author : ICMS, Hayatabad, Peshawar, Pakistan.
E-mail : pakis007@gmail.com

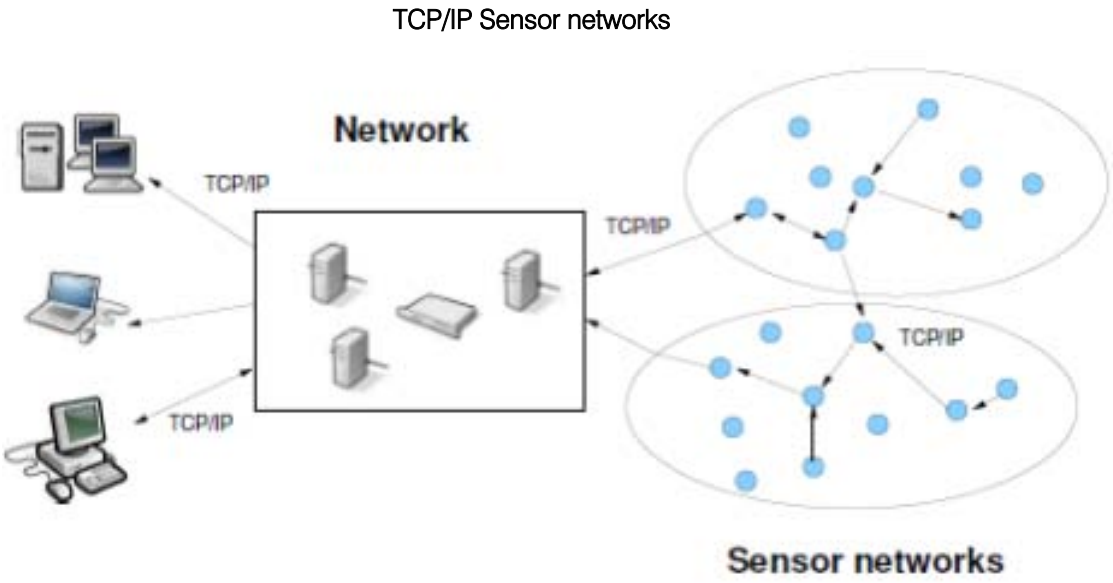


Figure 1.1 : Using TCP/IP both outside of and inside the wireless sensor network

Using TCP/IP both outside of and inside the wireless sensor network station within wireless sensor networks, because of the extreme communication conditions in sensor networks. Hence, a large number of protocols specifically tailored for sensor networks have been developed. While it is unquestionably true that the TCP/IP protocols were not designed to run in the kind of environments where sensor networks are envisioned, the claim that TCP/IP is inherently unsuitable for wireless sensor networks has not been verified.

The purpose of this licentiate research paper is to lay the groundwork for exploring the use of TCP/IP for wireless sensor networks. Using TCP/IP for sensor networks allows connecting the sensor networks directly to IP network infrastructures, as shown in Figure 1.1. In a set of four papers I present the software for an experimental platform, describe the problem area, and propose a set of mechanisms that are intended to allow TCP/IP to be efficiently used in wireless sensor networks.

The software platform consists of a lightweight implementation of the TCP/IP protocol stack and an equally lightweight and flexible operating system. Both the operating system and the protocol implementation are specifically designed to run on resource constrained sensor nodes.

a) Method

In order to explain and motivate the work in this research paper, I use two perspectives: the engineering perspective and the research perspective.

Engineering is about founding solutions to complex problems, within a given set of limitations. Research is about developing understanding. In experimental computer science [20], this understanding commonly is developed by producing artifacts and solving complex problems doing engineering and drawing conclusions from the solutions.

A single solution may not be possible to generalize, but taken together, a number of solutions can be said to span a solution space to a particular problem. Exploring, characterizing, and analyzing this solution space develops understanding for the character of the problem. This classification of engineering and research is based on definitions from Brooks' [15] and Phillips and Pugh [6].

The research in this research paper has mostly been exploratory. The problem area was not defined in advance, but has been developed as part of the research paper work. The exploratory method starts with finding an interesting question to answer. The question usually involves an interesting problem to solve.

The problem is then solved in a set of different ways, using either different tools or methods or variations of the same method. Based on observations of the solutions, or of the process leading to the solutions, an initial answer to the question can be formulated. From the answer and the solutions to the problems, it might be possible to generalize the question into a hypothesis.

This hypothesis can then be tested using experimentation in order to validate or invalidate it. The process of testing the hypothesis typically leads to a number of questions that need to be answered.

Thus the research process is iterative in that a research question leads to a hypothesis, which leads to further questions. In this research paper, the initial question was if the TCP/IP protocol stack could be implemented so that it would fit in a severely memory constrained system. After twice solving the problem of implementing TCP/IP with limited resources, the question could be answered: the TCP/IP protocol stack

can be implemented using very small amounts of memory.

This observation lead to the generalized question if TCP/IP could be useful is wireless sensor networks. This generalization was made because of the similarities of parts of the problem domains sensor network nodes have severely limited memory resources. as well as intuition developed when answering the initial question. The event-driven nature of sensor networks seemed to fit the event-driven design of the small TCP/IP implementations.

Furthermore, it appeared that many of the problems with TCP/IP in sensor networks could be solved with relatively straight-forward mechanisms. These observations lead to the hypothesis that TCP/IP could be a viable alternative for wireless sensor networks. This research paper takes the first steps towards validating or invalidating this hypothesis.

b) Research Issues

This research paper takes the first steps towards the use of the TCP/IP protocol suite in wireless sensor networks. This section summarizes the research issues that are indentured and treated in this research paper. Many of these issues are of the engineering kind: a problem that needs a solution that is not only correct, but also is able to work within the available limitations. These issues are the primary focus of papers A and B. Papers A and B solve the specific problems of implementing TCP/IP on a limited device and on designing an operating system for sensor nodes that allows rapid prototyping and experimentation.

Papers C and D focus on the research challenges involved in TCP/IP for wireless sensor networks. The formulation of these challenges are based on the software artifacts developed in paper A. Paper B presents a software framework designed to support future experimentation.

i. *TCP/IP on a Limited Device*

The TCP/IP protocol suite, which forms the basis of the Internet, is often perceived to be .heavy-weight. in that an implementation of the protocols requires large amounts of resources in terms of memory and processing power. This perception can be corroborated by measuring the memory requirements of popular TCP/IP implementations, such as the one in the Linux kernel [13] or in the BSD operating system [16]. The TCP/IP implementations in these systems require many hundreds of kilobytes of random access memory (RAM).For most embedded systems; cost typically is a limiting factor.

This constrains the available resources such as RAM and processor capabilities. Consequently, many embedded systems do not have more than a few kilobytes of RAM. Within the constraints of such a small embedded system, it is impossible to run the TCP/IP implementations from Linux or BSD Within this research paper, I investigate the solution space to the problem of running TCP/IP within constrained memory limits.

By developing a very small TCP/IP Implementation that is able to run even on a system with very small amounts of memory, I demonstrate that the solution space of the problem is larger than previously shown. While this is not an exhaustive investigation of the solution and, hence, cost are not technical limitations, but functions of business models. It is therefore out of scope of this research paper to discuss these matters in any detail. For simplicity, I assume that cost is proportional to memory size and processor resources, but at the same time note that this is a gross oversimplification.

c) Research Issues

Space, it does show that the solution space is large enough to accommodate even small embedded devices.

i. *Operating Systems for Wireless Sensor Networks*

The resource limitations and application characteristics of wireless sensor networks place specific requirements on the operating systems running on the sensor nodes. The applications are typically event-based: the application performs most of its work in response to external events. Resources are typically severely limited: memory is on the order of a few kilobytes, processing speed on the order of a few MHz, and limited energy from a battery or some other non-renewable energy source. Early research into operating systems for sensor networks [4] identified the requirements and proposed a system, called TinyOS, that solved many of the problems.

The TinyOS designers did, however, decide to leave out a set of features commonly found in larger operating systems, such as multithreading and run-time module loading. In this research paper, I argue that multithreading and run-time loading of modules are desirable features of an operating system for sensor network nodes. I have implemented an operating system that includes said features and runs within the resource limitations of a sensor node, and thereby show that these features are feasible for sensor node operating systems.

ii. *Connecting Sensor Networks and IP Networks*

A number of practical problems manifest themselves when doing a real-world deployment of a wireless sensor network. One of these is how to get data into and out of the sensor network, which may be deployed in a remote location. One way to solve this problem is to connect the sensor networks to an existing network infrastructure as an access network to the sensor network.

Today most network infrastructures, including the global Internet, use the Internet Protocol (IP) [17] as its base technology. It is therefore interesting to

investigate how wireless sensor networks can be connected to IP network infrastructures. From the engineering perspective, the problem of connecting a sensor network with an IP network can easily be solved. In many cases, it is possible to simply place a PC inside or on the border of the sensor network and connect the PC both to the IP network and to the sensor network.

The PC then acts as the gateway between the sensor network and the IP network. There are also many other possibilities, such as using a special-purpose device that connects the two Networks [17] or using satellite access to a special base station connected to the sensor network [9]. From the research perspective, however, the problem still has opportunities for investigation.

Paper C is a first step towards characterizing the solution space. It presents three different types of solutions to the problem: proxy architectures overlay networking and direct connection by using TCP/IP in the sensor network. This research paper focuses on the last solution: connecting sensor networks and IP networks by using the TCP/IP protocols inside the sensor network as in the outside IP network.

iii. *TCP/IP for Wireless Sensor Networks*

From the research perspective, investigating the use of TCP/IP in wireless sensor networks is of importance because the intersection of the TCP/IP protocol suite, the dominating communication protocol suite today, and wireless sensor networks, a new area in computer networking research, has not been previously studied. In general, the purpose of research is to provide understanding of problems and to gain new knowledge.

Within this particular problem, we can develop new understanding of the interaction between wireless sensor networks and wired network infrastructures by identifying, solving, and studying the problems with TCP/IP in sensor networks. From the engineering perspective, however, using the TCP/IP protocol suite inside the wireless sensor network may not be the best approach to solving the problem of connecting wireless sensor networks to IP networks, for some arbitrary definition of best.

There may be many other solutions to the problem that perform better both in a quantitative sense, e.g. that provide higher throughput or better energy efficiency, and in a qualitative sense, e.g. that provide a better security architecture. Prior to this research paper, however, no research has to the best of my knowledge been carried out to support claims in either way. There are a number of problems with TCP/IP for wireless sensor networks. An enumeration of the problems, which are identified in paper D, follows.

d) IP Addressing Architecture

In ordinary IP networks, each network interface attached to a network is given its own unique IP address. The addresses are assigned either statically by human configuration, or dynamically using mechanisms such as DHCP [8]. This does not fit well with the sensor network paradigm. For sensor networks, the addresses of the individual sensors are not interesting as such. Rather, the data generated by the sensors is the main interest. It is therefore advantageous to be able to loosen the requirement that each sensor has a unique address.

e) Address Centric Routing

Packet routing in IP networks is *address centric*, i.e., based on the addresses of the hosts and networks. The application specific nature of sensor networks makes *data centric* routing mechanisms [14] preferable. Data centric routing uses node attributes and the data contained in the packets to route packets towards a destination. Additionally, data centric mechanisms are naturally adapted to in-network data fusion [12].

f) Header Overhead

The protocols in the TCP/IP suite have a high overhead in terms of protocol header size, particularly for small packets. For small data packets, the header overhead is over 95%. Since energy conservation is of prime importance in sensor networks, transmission of unnecessary or redundant packet header fields should be avoided.

g) TCP Performance and Energy Efficiency

The reliable byte-stream protocol TCP has serious performance problems in wireless networks, both in terms of throughput [7] and in terms of energy efficiency. To be able to use TCP as a reliable transport protocol in wireless sensor networks, methods must be developed to increase the performance of TCP in the specific setting of sensor networks. The end-to-end acknowledgment and retransmission scheme employed by TCP is not energy efficient enough to be useful in wireless sensor networks. A single dropped packet requires an expensive retransmission from the original source. Because sensor networks often are designed to be multi-hop, a single retransmission will incur transmission and reception costs at every hop through which the retransmitted packet will travel.

h) Limited Nodes

Sensor nodes are typically limited in terms of memory size and processing power. Any algorithm developed for sensor networks must therefore take these limitations into consideration.

II. Contributions and Results

The main scientific contributions of this research paper are:

- The design and implementation of the uIP and the lwIP TCP/IP stacks that demonstrate that TCP/IP can be implemented on systems with very limited

memory resources, without sacrificing interoperability or compliance.

- The formulation of initial solutions to the problems with TCP/IP for sensor networks, which point towards the feasibility of using TCP/IP for wireless sensor networks. This opens up opportunities for new research.
- The design and implementation of the Contiki operating system that has a number of features currently not found in other operating systems for the same class of hardware platforms. These features enable rapid experimentation for further research into the area of this research paper.

The work presented in this research paper has had a visible impact on networking for embedded systems and, to a lesser degree, on sensor networks. Less than a year after paper D was published, the 6lowpan IETF workgroup [16] was established. The focus of the workgroup is on standardizing transmission of IP packets over IEEE 802.15.4 [4], a sensor networking radio technology.

The workgroup charter explicitly cites paper D and the uIP stack presented in paper A. The work in this research paper is mentioned in books on embedded systems and networking [5, 6] and cited in numerous academic papers (e.g. [3, 11, 14, 9, 13, 4, 12, 15, 16, 13, 5, 6, 7]). Articles in professional magazines have been written by using the uIP software for wireless sensor networks [8].

The software has been used in academic projects [5, 2], in courses e.g. at University of California, Los Angeles (UCLA) [74] and Stanford University [19], as well as in laboratory exercises [18, 79]. Finally, the software is being used in embedded operating systems [1, 11], and in a large number of embedded products (e.g. [12, 20, 2, 12, 13, 16, 17, 18, 15]).

III. Related Work

This chapter presents related work. The discussion is divided into four sections: small TCP/IP implementations, operating systems for sensor networks, connecting IP networks with sensor networks, and TCP/IP for sensor networks.

a) Small TCP/IP Implementations

There are several small TCP/IP implementations that fit the limitations of small embedded systems. Many of those implementations does, however, refrain from implementing certain protocol mechanisms in order to reduce the complexity of the implementation.

The resulting implementation may therefore not be fully compatible with other TCP/IP implementations. Hence, communication may not be possible many small TCP/IP implementations are tailored for a specific application, such as running a web server. This makes it possible to significantly reduce the implementation complexity, but does not provide a general communications mechanism that can be used for other applications. The PICmicro stack [10] is an example of such a TCP/IP implementation.

Unlike such implementations, the uIP and lwIP implementations are not designed for a specific application. Other implementations rely on the assumption that the small embedded device always will be communicating with a full-scale TCP/IP implementation running on a PC or work-station class device. Under this assumption it is possible to remove certain mechanisms that are required for full compatibility. Specifically, support for IP fragment reassembly and for TCP segment size variation are two mechanisms that often are left out.

Examples of such implementations are Texas Instrument's MSP430 TCP/IP stack [12] and the TinyTCP code [19]. Neither the uIP or the lwIP stack are designed under this assumption.

In addition to the TCP/IP implementation for small embedded systems, there is a large class of TCP/IP implementations for embedded systems with less constraining limitations. Typically, such implementations are based on the TCP/IP implementation from the BSD operating system [6].

These implementations do not suffer from the same problems as the tailored implementations.

Such implementations does, however, in general require too large amount of resources to be feasible for small embedded systems. Typically, such implementations are orders of magnitude larger than the uIP implementation.

b) Operating Systems for Sensor Networks

TinyOS [14] is probably the earliest operating system that directly targets the specific applications and limitations of sensor devices. TinyOS is built around a lightweight event scheduler where all program execution is performed in tasks that run to completion. TinyOS uses a special description language for composing a system of smaller components [13] which are statically linked with the kernel to a complete image of the system. After linking, modifying the system is not possible [15].

The Contiki system is also designed around a lightweight event-scheduler, but is designed to allow loading, unloading, and replacing modules at run-time. In order to provide run-time reprogramming for TinyOS, Levis and Culler have developed Mat´e [15], a virtual machine for TinyOS devices. Code for the virtual machine can be downloaded into the system at run-time.

The virtual machine is specifically designed for the needs of typical sensor network applications. Similarly, the Magnet OS [9] system uses a virtual Java machine to distribute applications across the sensor network. The advantages of using a virtual machine

instead of native machine code is that the virtual machine code can be made smaller, thus reducing the energy consumption of transporting the code over the network. One of the drawbacks is the increased energy spent in interpreting the code. For long running programs the energy saved during the transport of the binary code is instead spent in the overhead of executing the code.

Contiki does not suffer from the executional overhead as modules loaded into Contiki are compiled to native machine code.

c) Connecting IP Networks with Sensor Networks

SensorWare [13] provides an abstract scripting language for programming sensors, but their target platforms are not as resource constrained as ours. Similarly, the EmStar environment [18] is designed for less resource constrained systems. Reijers and Langendoen [19] use a patch language to modify parts of the binary image of a running system.

This works well for networks where all nodes run the exact same binary code but soon gets complicated if sensors run slightly different programs or different versions of the same software. The Mantis system [2] uses a traditional preemptive multi-threaded model of operation. Mantis enables reprogramming of both the entire operating system and parts of the program memory by downloading a program image onto EEPROM, from where it can be burned into fiash ROM.

Due to the multithreaded semantics, every Mantis program must have stack space allocated from the system heap, and locking mechanisms must be used to achieve mutual exclusion of shared variables. In Contiki, only such programs that explicitly require multi-threading need to allocate an extra stack.

At the time of publication of paper C, there was very little work done in the area of connecting wireless sensor networks and IP networks. Recently, however, a number of papers on the subject has been published. Ho and fall [4] have presented an application of Delay Tolerant Networking (DTN) mechanisms to sensor networks.

Their work is similar to that presented in paper C, but is more focused on the specifics of the DTN architecture. The overlay architecture presented by Dai and Han [12] unifies the Internet and sensor networks by providing a sensor network overlay layer on top of the Internet. While this work is similar in scope to the work in this research paper, it explores a slightly different path: this research paper explores the interconnectivity in a lower layer of the protocol stack.

The FLexible Interconnection Protocol (FLIP) [18] provides interconnectivity between IP networks and sensor networks, but relies on protocol converters at the border of the sensor network. This research paper investigates an architecture where no explicit protocol converters are required. Finally, the Plutarch architecture [2] changes the communication architecture of the Internet in a way that is able to accommodate natural inclusion of sensor networks in the new communication architecture.

This work is orthogonal to the work in this research paper. The intention with this research paper is to investigate how sensor networks can be connected with today's IP network infrastructures.

d) TCP/IP for Wireless Sensor Networks

While I am not aware of any previous work on TCP/IP for wireless sensor networks, the area of mobile ad-hoc networks (MANETs) is the area which is most closely related to the area of TCP/IP for wireless sensor networks. MANETs typically use the TCP/IP protocol suite for communication both within the MANETs and with outside networks.

There are, however, a number of differences between sensor networks and MANETs that affect the applicability of TCP/IP. First, MANET nodes typically has significantly more resources in terms of memory and processing power than sensor network nodes. Furthermore, MANET nodes are operated by human users, whereas sensor networks are intended to be autonomous.

The user-centricity of MANETs makes throughput the primary performance metric, while the per-node throughput in sensor networks is inherently low because of the limited capabilities of the nodes. Instead, energy consumption is the primary concern in sensor networks. Finally, TCP throughput is reduced by mobility [16], but nodes in sensor networks are usually not as mobile as MANET nodes.

While the specific area of TCP/IP for wireless sensor networks has not been previously explored, there are a number of adjacent areas that are relevant to this licentiate research paper. The following sections presents the related work in those areas.

i. *Reliable Sensor Network Transport Protocols*

Reliable data transmission in sensor networks has attained very little research attention, mostly because many sensor network applications do not require reliable data transmission. Nevertheless, a few protocols for reliable data transport have been developed.

Those protocols target both the problem of reliable transmission of sensor data from sensors to a sink node, and the problem of reliable transmission of data from a central sink node to a sensor. Potential uses of reliable data transmission is transport of important sensor data from one or more sensors to a sink node, transmission of sensor node configuration from a central server to one or more sensors, program downloads to sensor nodes, and other administrative tasks.

Most protocols for reliable transport in sensor networks are designed specifically for sensor networks and therefore cannot be readily used for e.g.

downloading data from an external IP network, without protocol converters or proxy servers. Reliable Multi-Segment Transport (RMST) [18] provides a reliable transport protocol for bounded messages on top of the Distributed Diffusion routing paradigm [4]. RMST uses either hop-by-hop reliability through negative acknowledgments and local retransmissions, or end-to-end reliability by using positive acknowledgments and end-to-end retransmissions. The authors provide simulation results and conclude that reliable transport for sensor networks is best implemented on the MAC layer. The results provided rely on the fact that the Directed Diffusion routing substrate is able to find relatively good paths through the network, however.

Pump Slowly Fetch Quickly (PSFQ) [3] is a reliable transport protocol that focuses on one-to-many communication situations and uses hop-by-hop reliability. In PSFQ, data is slowly pumped towards the receivers, one fragment at a time. If a nodes along the path towards the receiver notices that a data fragment has been lost, it issues a *fetch* request to the closest node on the backward path.

The number of fetch requests for a single fragment is bounded and fetch requests are issued only within the time frame between two data fragments are pumped. Event-to-Sink Reliable Transport (ESRT) [13] is a transport protocol that provides a semi-reliable transport in only one direction. Data that is sent from sensors to a sink is given a certain amount of reliability. The sink node, which is assumed to have more computational resources than the sensors, computes a suitable reporting frequency for the nodes.

ii. *Header Compression*

Header compression is a technique that reduces packet header overhead by refraining from transmitting header fields that do not change between consecutive packets. The header compressor and the decompressor share the state of streams that pass over them. This shared state is called the header compression *context*.

The compression works by not transmitting full headers, but only the delta values for such header fields that change in a predictable way. Early variants of header compression for TCP were developed for low speed serial links [15] and are able to compress most headers down to only 10% of their original size.

Early header compression schemes did not work well over lossy links since they could not recover from the loss of a header update. A missed header update will cause subsequent header updates to be incorrect because of the context mismatch between the compressor and the decompressor. The early methods did not try to detect incorrectly decompressed headers. Rather, these methods trusted recipients to drop packets with erroneous headers and relied on retransmissions from the sender to repair the context mismatch.

Degermark et al. [16, 17] have presented a method for compressing headers for both TCP/IP and for a set of real-time data protocols. The method is robust in the sense that it is able to recover from a context mismatch by using feedback from the header decompressor. The feedback information is piggybacked on control packets such as acknowledgments that travel on the reversepath. Furthermore, authors introduces the TWICE algorithm.

The algorithm is able to adapt to a single lost header delta value by applying the received delta value twice. Incorrectly decompressed headers are identified by computing the checksum of the decompressed packet. If the checksum is found to be incorrect by the decompressor, a full header is requested from the compressor, thus synchronizing the header compression context. Sridharan et al. [17] have presented Routing-Assisted Header Compression (RAHC), a header compression scheme that is particularly well-suited for multi-hop networks.

Unlike other header compression schemes, the RAHC algorithm works end-to-end across a number of routing hops. The algorithm utilizes information from the underlying routing protocol in order to detect route changes and multiple paths.

iii. *TCP over Wireless Media*

TCP [18] was designed for wired networks where congestion is the predominant source of packet drops. TCP reduces its sending rate detecting packet loss in order to avoid overloading the network. This behavior has shown to be problematic when running TCP over wireless links that have potentially high bit error rates. Packet loss due to bit errors will be interpreted by TCP as a sign of congestion and TCP will reduce its sending rate. TCP connections running over wireless links may therefore see very large reductions in throughput.

A number of mechanisms for solving these problems have been studied. Wireless TCP enhancements can be divided into three types [6]: *splitconnection*, *end-to-end*, and *link-layer*. The split-connection approach, as exempli fied by Indirect TCP [5] and M-TCP [16], splits each TCP connections into two parts: one over the wired network and one over the wireless link. Connections are terminated at a base station to allow a specially tuned protocol to be used between the base station and the wireless host. TCP snoop [7] is a link-layer approach that is designed to work in a scenario where the last hop is over a wireless medium.

TCP snoop uses a program called the *snoop agent* that is running on the base station before the last hop. The snoop agent intercepts TCP segments and caches them. If it detects a failed transmission, it will

immediately retransmit the lost segment .When duplicate acknowledgements to be sent towards the original sender of the segment. A-TCP [5] is primarily designed for wireless ad-hoc networks and is an example of the end-to-end approach. A-TCP inserts a conceptual layer in between IP and TCP that deals with packet losses because of transmission errors and unstable routes. Unlike the other approaches, A-TCP requires modifications to the end-host.

iv. *Addressing in Sensor Networks*

Addressing in sensor networks is different from addressing in other computer networks in that the sensors do not necessarily need to have individual addresses [12]. Instead, many sensor network applications benefit from seeing the *data* sensed by the network the primary addressing object [15]. This allows routing to be *data-centric* rather than the traditional address-centric.

One of the earliest data-centric routing protocols is Directed Diffusion [14] which propagates an information interest through the network. When a sensor obtains information for which an interest has been registered, it transmits the information back towards the source of the information interest. A different approach is taken by TinyDB [18] where the sensor network is viewed as a distributed data base.

The data base is queried with an SQL-like language. Query strings are processed by a base station, and compressed and optimized queries are disseminated through the sensor network. Results are distributed back through the routing tree that was formed when the query was propagated. This is an addressing scheme where the data is explicitly addressed and where individual nodes are not possible to address directly.

IV. Conclusions and Future Work

This licentiate research paper takes the first steps towards the use of the TCP/IP protocol suite in wireless sensor networks. It builds the framework in which the use of TCP/IP can be further investigated, identifies the problems with TCP/IP for sensor networks, and formulates initial solutions to the problems. The contribution of this work is that it for the first time brings TCP/IP, the dominant protocol stack, together with wireless sensor networks.

The results of the work presented in this research paper have had a significant impact on the embedded TCP/IP networking community. The software developed as part of the research paper has become widely known in the community.

The software is used in academic research projects, academic courses, as well as a large number of embedded devices. I will continue this work with experimental studies of the use of TCP/IP in wireless sensor networks.

Further investigation must be made before the hypothesis that TCP/IP is a viable protocol suite for wireless sensor networks can be validated or invalidated.

We have already made simulation studies of the Distributed TCP Caching mechanism [13] and are designing a MAC layer that will support DTC. We intend to evaluate the energy efficiency of TCP/IP for sensor networks by using the method described by Ritter et al. [17].

While this method has been developed to experimentally evaluate a model of life-time bounds [4], it also is useful for comparing the energy efficiency of communication protocols. I will also continue to investigate software construction for memory stressed systems, based on the bindings in papers A and B.

This work consists of developing mechanisms and methods for implementing computer programs for resource limited embedded systems and sensor nodes. I am currently working on a lightweight mechanism called proto threads that provides sequential flow of control for event-driven systems.

References Références Referencias

1. eCos Embedded Configurable Operating System. Web page. URL: ttp://sources.redhat.com/ecos/
2. H. Abrach, S. Bhatti, J. Carlson, H. Dai, J. Rose, A. Sheth, B. Shucker J. Deng, and R. Han. Mantis: system support for multimodal networks of in-situ sensors. In *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, pages 50.59, 2003.
3. P. Agrawal, T.S. Teck, and A.L. Ananda. A lightweight protocol for wireless sensor networks. March 2003.
4. J. Alonso, A. Dunkels, and T. Voigt. Bounds on the energy consumption of routings in wireless sensor networks. In *Proceedings of the 2ndWiOpt, Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, Cambridge, UK, March 2004.
5. A. Bakre and B. R. Badrinath. I-TCP: Indirect TCP for mobile hosts. In *Proceedings of the 15th International Conference on Distributed Computing Systems*, May 1995.
6. H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz. A comparison of mechanisms for improving TCP performance over wireless links. *IEEE/ACM Trans. Netw.*, 5(6):756.769, 1997.
7. H. Balakrishnan, S. Seshan, E. Amir, and R. Katz. Improving TCP/IP performance over wireless networks. In *Proceedings of the first ACM Conference on Mobile Communications and Networking*, Berkeley, California, November 1995.
8. D. Barnett and A. J. Massa. Inside the uIP Stack. *Dr. Dobb's Journal*, February 2005.

9. R. Barr, J. C. Bicket, D. S. Dantas, B. Du, T. W. D. Kim, B. Zhou, and E. Sirer. On the need for system-level support for ad hoc and sensor networks. *SIGOPS Oper. Syst. Rev.*, 36(2):1.5, 2002.
10. J. Bentham. *TCP/IP Lean: Web servers for embedded systems*. CMP Books, October 2000.
11. S. Beyer, K. Mayes, and B. Warboys. Application-compliant networking on embedded systems. In *Proceedings of the 5th IEEE Internation Workshop on Networked Appliances*, pages 53.58, October 2002.
12. C. Borrelli. TCP/IP on Virtex-II Pro Devices Using lwIP. XAPP 663, Xilinx Inc., August 2003.
13. A. Boulis, C. Han, and M. B. Srivastava. Design and implementation of a framework for efficient and programmable sensor networks. In *Proceedings of The First International Conference on Mobile Systems, Applications, and Services (MOBISYS `03)*, May 2003.
14. M. Britton, V. Shum, L. Sacks, and H. Haddadi. A biologically-inspired approach to designing wireless sensor networks. In *Proceedings of the Second European Workshop on Wireless Sensor Networks*, Istanbul, Turkey, 2005.
15. F. P. Brooks Jr. The computer scientist as a toolsmith II. *Communications of the ACM*, 39(3):61.68, March 1996.
16. K. Brown and S. Singh. M-TCP: TCP for mobile cellular networks. *ACM Computer Communications Review*, 27(5):19.43, October 1997.
17. P. Buonadonna, D. Gay, J. Hellerstein W. Hong, and S. Madden. TASK: Sensor Network in a Box. In *Proceedings of the Second European Workshop on Sensor Networks*, 2005.
18. B. F. Cockburn. CMPE 401 - Computer Interfacing. Web page. URL: http://www.ece.ualberta.ca/. cmpe401/
19. G. H. Cooper. TinyTCP. Web page. 2002-10-14. URL: http://www.csonline.net/bpaddock/tinytcp/
20. Nu Horizons Electronics Corp. TCP/IP Development Kit. Web page. URL: http://www.nuhorizons.com/

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

RASCP: Providing for a Secure Group Communication Plane Using RFID

By K S Jagadeesh, Dr. Somashekhar C Desai, Chandramouli.H & Kashyap D Dhruve

JJT University, Jhunjhunu, Rajasthan, India

Abstract - Predominantly large distributed networks currently provide support for group oriented protocols and applications. Regardless of the type of distributed network there is a need to provide communication privacy and data integrity to the information exchange amongst the group members. This paper introduces a protocol named *RFID* Authentication based Secure Communication Plane *(RASCP)*. *RASCP* adopts the commutative RSA algorithm to maintain data integrity. The proposed protocol not only eliminates the overheads resulting from key distribution and key compromise attacks but also provide for information security in the presence of colluded group members. Radio Frequency Identification *(RFID)* tags is used for group member identification. The RACP protocol is compared with the RFID extended Secure Lock *(RSL)* group communication protocol and its efficiency in terms of the computational complexity involved is discussed in this paper.

Keywords : *RFID, RFID security, RFID authentication secure group communication, cryptography, commutative rsa, secure plane, computational cost, sieve of eratosthenes algorithm , prime numbers, pseudo random number generators, secure lock.*

GJCST-E Classification : *E.3*

Strictly as per the compliance and regulations of:

RASCP: Providing for a Secure Group Communication Plane Using RFID

K S Jagadeesh [α], Dr. Somashekhar C Desai[σ], Chandramouli.H [ρ] & Kashyap D Dhruve [ω]

Abstract - Predominantly large distributed networks currently provide support for group oriented protocols and applications. Regardless of the type of distributed network there is a need to provide communication privacy and data integrity to the information exchange amongst the group members. This paper introduces a protocol named ***RFID*** Authentication based Secure Communication Plane (***RASCP***). ***RASCP*** adopts the commutative RSA algorithm to maintain data integrity. The proposed protocol not only eliminates the overheads resulting from key distribution and key compromise attacks but also provide for information security in the presence of colluded group members. Radio Frequency Identification (***RFID***) tags is used for group member identification. The RACP protocol is compared with the RFID extended Secure Lock (***RSL***) group communication protocol and its efficiency in terms of the computational complexity involved is discussed in this paper.

Keywords : RFID, RFID security, RFID authentication secure group communication, cryptography, commutative rsa, secure plane, computational cost, sieve of eratosthenes algorithm , prime numbers, pseudo random number generators, secure lock.

I. Introduction

RFID systems and standards established by IEEE [1,2] are envisioned to be one of the most commonly used identification mechanisms in the near future [3]. A RFID authentication system primarily consists of a tag and a reader with a database to store the tag details. Tags available are of several types and classes [1][2] but the research work presented here considers the most commonly available passive RFID tags of class 0. A lot of research is ongoing to provide security to the existing standards and the technology involved in manufacturing and Radio Frequency (RF) communication systems in place. Currently there exist several threats to the existing RFID deployments like Denial of Service Attacks, RFID Tag Cloning, RFID Tag Tracing, Eavesdropping, Replay Attacks Data Forging, Invading Privacy Information and Hot-listing to name a few [3][4][5][6][7][8][9][10]. More often than not researchers have focused on the eliminating the threats that currently exist in the RFID technology and methods towards improving it. In the research work presented here the use of the existing RFID technology for identification is adopted. The proposed protocol i.e. $RASCP$ assumes that the RFID communication module considered is secure and free of the above mentioned defects/attacks.

Communication provisioning is considered as the basic essentials of any network. The prevalent large scale distributed networks existent provide support for various business, personal, commerce, banking, military, intelligence applications and services. These networks are prone to varied kind of attacks and data compromise issues. To counter the issue of data compromise cryptography is commonly used. Cryptographic algorithms could be broadly classified into two types namely Symmetric and Asymmetric type. The $RASCP$ protocol proposed utilizes the asymmetric commutative RSA Algorithm to provide for security. These algorithms are discussed in detail in the future sections of this paper.

The remaining paper is organized as follows. Section II discusses the commutative RSA algorithm. The Sieve of Eratosthenes prime number generation algorithm is discussed in the next section. The fourth section of the paper provides an in depth explanation of the proposed $RASCP$group communication scheme. The fifth section of the paper presents the RFID extended secure lock group communication scheme. The penultimate section of the paper discusses the experimental evaluation wherein the propose $RASCP$ and the RSL are compared. The conclusion and the future work is discussed in the last section of the paper.

II. Commutative Rsa

A secure plane is realizable provided the data communicated over the plane is protected and cannot be colluded. The use of cryptographic techniques is generally preferred, hence the $RASCP$ proposed in this paper adopts the commutative RSA algorithm. The $RASCP$ considers two prime numbers $Param\_P_p^{CRSA}$ and $Param\_Q_q^{CRSA}$ initialized amongst all the group members. Let G_A and G_B represent the group members required to communicate over the secure plane. To compute the encryption keys and decryption key pairs of the commutative RSA algorithm the parameters

Author α : Research Scholar, JJT University, Jhunjhunu, Rajasthan, India. E-Mail : Ksj_20012002@yahoo.co.in
Author σ : Professor, BLDEA College of Engineering, Bijapur, India. E-Mail : desaisc07@gmail.com
Author ρ : Research Scholar, JJT University, Jhunjhunu, Rajasthan, India. E-Mail : hcm123cool@rediffmail.com
Author ω : Technical Director, Planet-I Technologies, Bangalore, India. E-Mail : kashyapdhruve@hotmail.com

$Param\_N^{CRSA}$ and $Param\_\phi^{CRSA}$ are computed using the following

$$Param\_N^{CRSA} = \left[\left(Param\_P_p^{CRSA}\right) \times \left(Param\_Q_q^{CRSA}\right)\right]$$

$$Param\_\phi^{CRSA} = \left[\left(Param\_P_p^{CRSA} - 1\right) \times \left(Param\_Q_q^{CRSA} - 1\right)\right]$$

From the above equations it is clear that $Param\_N_A{}^{CRSA} = Param\_N_B{}^{CRSA}$ and $Param\_\phi_A{}^{CRSA} = Param\_\phi_B{}^{CRSA}$ for A and B. The encryption key pair of A and B represented as $(Param\_N_A{}^{CRSA}, Param\_E_A{}^{CRSA})$ and $(Param\_N_B{}^{CRSA}, Param\_E_B{}^{CRSA})$

is to be obtained. The $Param\_E^{CRSA}$ is obtained by randomly selecting numbers such that it is a co prime of $Param\_\phi^{CRSA}$ or in other terms

$$\mathcal{FN}_{GCD}(Param\_E^{CRSA}, Param\_\phi^{CRSA}) = 1$$

Where $\mathcal{FN}_{GCD}(x, y)$ represents the greatest common divisor function between two variables x and y.

The decryption key pair of A and B is represented by $(Param\_N_A{}^{CRSA}, Param\_D_A{}^{CRSA})$ and $(Param\_N_B{}^{CRSA}, Param\_D_B{}^{CRSA})$ and the parameter $Param\_D^{CRSA}$ is computed based on the following equation

$$Param\_D^{CRSA} = (Param\_E^{CRSA})^{-1} \, Mod(Param\_N^{CRSA})$$

Let Enc_X represent the encrypted data X. The encryption operation is defined as follows

$$Enc_X = X^{Param\_E^{CRSA}} \, Mod(Param\_N^{CRSA})$$

The commutative RSA decryption operation on the encrypted data Y is defined

$$Dec_Y = Y^{Param\_D^{CRSA}} \, Mod(Param\_N^{CRSA})$$

a) Commutative proof RSA Algorithm

The commutative property of the RSA algorithm adopted in $RASCP$ can be proved if data X encrypted by A and then encrypted by B provides the same resultant if the encryption is performed by B followed by the encryption performed by A i.e.

$$Enc^B(Enc_X{}^A) \equiv Enc^A(Enc_X{}^B)$$

$$Enc^B\left(X^{Param\_E_A{}^{CRSA}} \, Mod(Param\_N_A{}^{CRSA})\right) \equiv Enc^A\left(X^{Param\_E_B{}^{CRSA}} \, Mod(Param\_N_B{}^{CRSA})\right)$$

$$X^{(Param\_E_A{}^{CRSA} \times Param\_E_B{}^{CRSA})} \, Mod\left(Param_{N_A}{}^{CRSA}\right) = X^{(Param\_E_B{}^{CRSA} \times Param\_E_A{}^{CRSA})} \, Mod(Param\_N_B{}^{CRSA})$$

As $Param_{N_A}{}^{CRSA} = Param\_N_B{}^{CRSA}$ it can be concluded that

$$X^{(Param\_E_A{}^{CRSA} \times Param\_E_B{}^{CRSA})} \, Mod\left(Param_{N_A}{}^{CRSA}\right) = X^{(Param\_E_B{}^{CRSA} \times Param\_E_A{}^{CRSA})} \, Mod(Param\_N_A{}^{CRSA})$$

And hence

$$Enc^B(Enc_X{}^A) \equiv Enc^A(Enc_X{}^B)$$

III. Prime Number Generation

Prime number generation functions and their application to the arena of cryptography have been extensively studied by researchers. The $RACP$ proposed in this paper utilizes the Sieve of Eratosthenes Algorithm [11] to find a set of prime numbers based on the user $RFID$ tags. Let n_{Max} represent a number derived from the user $RFID$ tag. Let us consider a Boolean Set B_{Tmp} having n_{Max} Boolean values, each element are represented as b_{Indx} where $b \in \{T, F\}$ and $Indx$ represents the index corresponding to the number in $\mathcal{N}_{Tmp} = \{2,3,4, \ldots\ldots n_{Max}\}$. Let $Var1 = F_{Least}(n, \mathcal{N}_{Tmp}, B_{Tmp})$ represent a function that returns the smallest number $Var1 \in \mathcal{N}_{Tmp}$ in $\mathcal{N}_{Tmp}$ that is greater than n and $b_n = F$ and $b_n \in B_{Tmp}$ .The Sieve of Eratosthenes Prime number generation algorithm is adopted to generate prime number set P. The Sieve of Eratosthenes algorithm adopted is given below

Algorithm 1: Sieve of Eratosthenes Prime number generation algorithm

Input:

User RFID based Number n_{Max}

Output:

Prime Number Set P

Algorithm:

I. Initialize $\mathcal{N}_{Tmp} = \{2,3,4, \ldots\ldots n_{Max}\}$
II. Initialize Boolean set $B_{Tmp} = \{F_1, F_2, F_3, \ldots\ldots F_{n_{Max}}\}$
III. Initialize $Var = 2$
IV. **Do**
V. Set the index of all the multiples of $Var1$ to True i.e. T occurring between Var^2 and n_{Max} .
VI. $Var = F_{Least}(Var, \mathcal{N}_{Tmp}, B_{Tmp})$
VII. **While** $(Var^2 > n_{Max})$
VIII. $P =$ Set of all indexes of $b_{Indx} \in B_{Tmp} : b_{Indx} = F$

From the above algorithm it is evident that the set P obtained contains all the prime numbers between 2 and n_{Max} . This algorithm is utilized to obtain the probable $P_{Comm\_RSA}^{Prob}$ and $Q_{Comm\_RSA}^{Prob}$ sets required to initialize the commutative RSA algorithm in the $RACP$ for each user considered in the communication plane. The computational complexity of this algorithm is $O(n_{Max} \ln\ln n_{Max})$[12][13].

IV. RASCP - RFID Authentication Based Secure Communication Plane

Let us consider a set of users who would like to communicate securely represented by a set defined as $G = \{g_1, g_2, g_3, \ldots\ldots g_m\}$

Where g_m represents the m^{th} user of the group G.

It is assumed that each user $\mathcal{g}_m \in G$ posses a RFID Tag represented as T^m and an RFID reader. The RFID tags are said to contain data of length L_T^m where m represents the m^{th} user and the users associated tag T^m. The secure communication plane is constructed by adopting the commutative RSA algorithm. To initialization of the commutative RSA algorithm is based on the RFID tag data $RFID_T^m$, used to obtain the parameters $Param\_P_m^{CRSA}$ and $Param\_Q_m^{CRSA}$ using the Sieve of Eratosthenes Prime number generation algorithm. Each member of the group contributes towards the construction of the commutative RSA sets $PARAM\_P$ and $PARAM\_Q$ defined as
$PARAM\_P = \{Param\_P_1^{CRSA}, Param\_P_2^{CRSA}, \cdots, Param\_P_m^{CRSA}\}$ and
$PARAM\_Q = \{Param\_Q_1^{CRSA}, Param\_Q_2^{CRSA}, \cdots, Param\_Q_m^{CRSA}\}$

The algorithm used to construct the $PARAM\_P$ and $PARAM\_Q$ sets is as mentioned below

Algorithm Name: $PARAM\_P$ and $PARAM\_Q$ construction

Input:

I. Group Member Set $\boldsymbol{G = \{\mathcal{g}_1, \mathcal{g}_2, \mathcal{g}_3, \ldots\ldots \mathcal{g}_m\}}$
II. Group RFID Tag Associated with each Group Member $\boldsymbol{\mathcal{g}_m, T^m}$ and its data $\boldsymbol{RFID_T^m}$ and length $\boldsymbol{L_T^m}$

Output:

I. $\boldsymbol{PARAM\_P}$
II. $\boldsymbol{PARAM\_Q}$

Algorithm

I. Initilize $PARAM\_P = \emptyset$ and $PARAM\_Q = \emptyset$
II. For Each group member $\mathcal{g}_m \in G$
III. $\vec{Q}_{Tmp}^m, \vec{P}_{Tmp}^m = Split(L_T^m, RFID_T^m)$
IV. $P_{Comm\_RSA}^{Prob\ m} = GetPrimeSet(\vec{P}_{Tmp}^m)$
V. $Q_{Comm\_RSA}^{Prob\ m} = GetPrimeSet(\vec{Q}_{Tmp}^m)$
VI. $Param\_P_m^{CRSA} = RandSel(P_{Comm_{RSA}}^{Prob\ m}, t)$
VII. $Param\_Q_m^{CRSA} = RandSel(Q_{Comm_{RSA}}^{Prob\ m}, t)$
VIII. $PARAM\_P = PARAM\_P \cup Param\_P_m^{CRSA}$
IX. $PARAM\_Q = PARAM\_Q \cup Param\_Q_m^{CRSA}$
X. End For Each

The function $Split(X, Y)$ represents a splitting function that obtains the most significant bits and least significant bits of the number Y of length X. $GetPrimeSet(X)$ represents a function that uses the Sieve of Eratosthenes Prime number generation algorithm to obtain the prime numbers set within X. $RandSel(X, t)$represents a random element in the set X selection function based on the seed time t. The communication overheads of this algorithm is $m \times 2D$ transmissions where D represents the size of the messages parsed between the m group members.

To construct the commutative RSA secure plane all the m members of the group G require a common $Param\_P_p^{CRSA}$ and $Param\_Q_q^{CRSA}$ to derive their encryption and decryption keys. A time synchronization function φ_T is adopted to ascertain the $Param\_P_p^{CRSA} \in PARAM\_P$ and $Param\_Q_q^{CRSA} \in PARAM\_Q$ amongst the group G. The time synchronization function φ_T can be considered as a $RandSel$ function wherein the seed time is common for all the members $\mathcal{g}_m \in G$. The time synchronization function can be defined as
$\varphi_T(X, t_T) = RandSel(X, t_T)$

Where t_T represents the synchronization seed and $\forall\, \mathcal{g}_m \in G : t = t_T$.

The time synchronization function φ_T is used to obtain $Param\_P_p^{CRSA}$ and $Param\_Q_q^{CRSA}$ defined as
$Param\_P_p^{CRSA} = \varphi_T(PARAM\_P, t_T)$
$Param\_Q_q^{CRSA} = \varphi_T(PARAM\_Q, t_T)$

The encryption and decryptions keys are to be derived from $Param\_P_p^{CRSA}$ and $Param\_Q_q^{CRSA}$ using the following algorithm

Algorithm Name: Encryption and Decryption Key Pair Computation

Input:

I. Group Member Set $\boldsymbol{G = \{\mathcal{g}_1, \mathcal{g}_2, \mathcal{g}_3, \ldots\ldots \mathcal{g}_m\}}$
II. $\boldsymbol{Param\_P_p^{CRSA}}$
III. $\boldsymbol{Param\_Q_q^{CRSA}}$

Output:

I. Encryption Key Pair $\left(\boldsymbol{Param_{N_{\mathcal{g}_m}}^{CRSA}, Param_{E_{\mathcal{g}_m}}^{CRSA}}\right)$
II. Decryption Key Pair $\left(\boldsymbol{Param\_N_{\mathcal{g}_m}^{CRSA}, Param\_D_{\mathcal{g}_m}^{CRSA}}\right)$

Algorithm

I. For Each group member $\mathcal{g}_m \in G$
II. Compute $Param_{N_{\mathcal{g}_m}}^{CRSA} = \left[\left(Param_{P_p}^{CRSA}\right) \times \left(Param_{Q_q}^{CRSA}\right)\right]$
III. Compute $Param_{\phi_{\mathcal{g}_m}}^{CRSA} = \left[\left(Param_{P_p}^{CRSA} - 1\right) \times \left(Param_{Q_q}^{CRSA} - 1\right)\right]$
IV. Select random number using $RandSel(Rnd_{Num}, t) \mid \mathcal{FN}_{GCD}(Rnd_{Num}, Param\_\phi^{CRSA}) = 1$
V. $Param\_E_{\mathcal{g}_m}^{CRSA} = Rnd_{Num}$
VI. Compute $Param_{D_{\mathcal{g}_m}}^{CRSA} = \left[\left(Param_{E_{\mathcal{g}_m}}^{CRSA}\right)^{-1} Mod\left(Param_{N_{\mathcal{g}_m}}^{CRSA}\right)\right]$
VII. Encryption key pair of the $\mathcal{g}_m{}^{th}$ group member is $\left(Param_{N_{\mathcal{g}_m}}^{CRSA}, Param_{E_{\mathcal{g}_m}}^{CRSA}\right)$
VIII. Decryption key Pair of the $\mathcal{g}_m{}^{th}$ group member is $\left(Param_{N_{\mathcal{g}_m}}^{CRSA}, Param_{D_{\mathcal{g}_m}}^{CRSA}\right)$
IX. End For Each

Using the Encryption and Decryption Key Pair Computation algorithm all the group members $g_m \in G$ compute the encryption and decryption key pairs which enable to construct the envisioned secure communication plane. The $RASCP$ discussed eliminates the security arising from key exchange [14], negating key compromise [15] external server maintenance for key management [16] proving the efficiency in creating a secure communication plane.

Let us consider n users of the group G that need to communicate securely and the secure communication group $\bar{G}$ is defined as

$$\bar{G} = \{g_1, g_2, g_3, \ldots \ldots g_n\}$$

Where $n \leq m$ and $\bar{G} \subseteq G$

The secure communication plane consisting of n group members communicate data by using a series of encryption and decryption operations. The commutative nature of the RSA algorithm adopted in the $RASCP$ ensures that the data communicated is encrypted at least once i.e. the original data is encrypted and then only communicated over the plane thereby securing the data. The presence of any colluded users within the group represented by g_c, on intercepting the data would not be unable to determine the level of encryptions and decryption procedures performed on the data prior to his interception. In the case if the user $g_c \in G$ intercepts the data after the first encryption, g_c would not be able to recover the data as the encryption and the decryption keys are not exchanged and are different for each user $g_n \in \bar{G}$ participating in the secure group communication. Let $g_{Sndr} \in \bar{G}$ represents the sender who needs to communicate data X to $g_{Rcv} \in \bar{G}$ in the presence of group member set $\bar{G}$ securely. Let us define a set $\bar{\bar{G}}$ and $\acute{G}$ as follows

$\bar{\bar{G}} = \bar{G} \cap g_{Rcv}$

$\acute{G} = \bar{G} \cap g_{Sndr}$

The algorithm to securely communicate amongst g_{Sndr} and g_{Rcv} is mentioned below

Algorithm Name: Communication over the Secure Plane

Input:

I. Group Member Set $\bar{G}$
II. Group Member Set $\bar{\bar{G}}$
III. Group Member Set $\acute{G}$
IV. Encryption and Decryption Key Pairs of Group Member Set $\bar{G}$
V. Data to be transacted X available with $g_{Sndr} \in \bar{G}$

Output:

I. Data X available with $g_{Rcv} \in \bar{G}$

Algorithm

I. For user $g_m = g_{Sndr} \in \bar{G}$
II. Encrypt the data $Enc_{g_{Sndr}} = \left[X^{Param_{E_{g_{Sndr}}}{}^{CRSA}} Mod\left(Param_{N_{g_{Sndr}}}{}^{CRSA}\right)\right]$
III. $Enc_{Tmp} = Enc_{g_{Sndr}}$
IV. End For
V. For Each user $g_m \in \acute{G}$
VI. Encrypt the data $Enc_{Tmp} = \left[Enc_{Tmp}{}^{Param_{E_{g_m}}{}^{CRSA}} Mod\left(Param_{N_{g_m}}{}^{CRSA}\right)\right]$
VII. End For Each
VIII. For Each user $g_m \in \bar{\bar{G}}$
IX. For the first user
X. Decrypt the data $Dec_{Tmp} = \left[Enc_{Tmp}{}^{Param_{D_{g_m}}{}^{CRSA}} Mod\left(Param_{N_{g_m}}{}^{CRSA}\right)\right]$
XI. End For
XII. Decrypt the data $Dec_{Tmp} = \left[Dec_{Tmp}{}^{Param_{D_{g_m}}{}^{CRSA}} Mod\left(Param_{N_{g_m}}{}^{CRSA}\right)\right]$
XIII. End For Each
XIV. For user $g_m = g_{Rcv} \in \bar{G}$
XV. Decrypt to get final data $X = \left[Dec_{Tmp}{}^{Param_{D_{g_m}}{}^{CRSA}} Mod\left(Param_{N_{g_m}}{}^{CRSA}\right)\right]$
XVI. End For

Using the Communication over Secure Plane Algorithm discussed above the g_{Rcv} is able to receive the data X sent by the user g_{Sndr} using n number of encryption and decryption functions. The algorithm also highlights the fact that the data X to be transmitted is not transmitted in the original form i.e. it is encrypted and transmitted there by securing the data.

The $RASCP$ discussed utilizes the $RFID$ tags available with each group member g_m to construct the secure communication plane. The *RFID* tags are often used for identification and tracking. In $RASCP$ the RFID tags are used both for security provision and identification. As the $RASCP$ adopts multiple encryption and multiple decryptions to securely communicate data the overheads arising from this could be considered as a drawback of the $RASCP$. The $RASCP$ is evaluated with the Secure Lock secure group communication protocol in the subsequent section of this paper.

V. RFID Extended Secure Lock Group Communication Scheme (RSL)

The RSL is a $RFID$ based extended Secure Lock protocol [17]. The RSL protocol considers a central server and a set of group members defined as $G^{RSL} = \{g_1{}^{RSL}, g_2{}^{RSL}, g_3{}^{RSL}, \ldots \ldots g_m{}^{RSL}\}$

The RSL protocol incorporates an asymmetric cryptographic algorithm to provide security. Let the

private and public of a group member ${g_m}^{RSL} \in G^{RSL}$ be represented as $({\mathcal{P}^{RSL}}_m, {\mathcal{S}^{RSL}}_m)$.

The central server also known as the security server establishes a set of $m = |G^{RSL}|$ pair wise relatively prime numbers $\mathcal{N}_1, \ldots, \mathcal{N}_m$ from the $RFID$ tags possessed using the Sieve of Eratosthenes Prime number generation algorithm. These numbers are then assigned to group members ${g_m}^{RSL} \in G^{RSL}$ and are assumed to be public in nature. To establish a secure plane of for communication using the RSL the server computes the following based on the a randomly selected key represented as K^{RSL}

$$\mathcal{L}\mathcal{C}\mathcal{k}^{\mathrm{RSL}} \equiv \mathcal{E}_{{\mathcal{P}^{RSL}}_m}(K^{RSL})\left(mod\ {\mathcal{N}_m}^{RSL}\right)$$

Where $\mathcal{E}$ represents the encryption operation

Using the Chinese remainder theorem the server computes $\mathcal{L}\mathcal{C}\mathcal{k}^{RSL}$. The computed value $\mathcal{L}\mathcal{C}\mathcal{k}^{RSL}$ is considered as the lock for the key $\mathcal{E}_{{\mathcal{P}^{RSL}}_m}(K^{RSL})$ .The resulting message sent by the server is defined as

$${msg^{RSL}}_m = \left(\mathcal{L}\mathcal{C}\mathcal{k}^{RSL}, \{K^{RSL}\}_{K^{RSL}}\right)$$

The group member ${g_m}^{RSL}$ on receiving the message ${msg^{RSL}}_m$ obtains the $\mathcal{L}\mathcal{C}\mathcal{k}^{RSL}$ using the following computations

$$\mathcal{E}_{{\mathcal{P}^{RSL}}_m}(K^{RSL}) = (\mathcal{L}\mathcal{C}\mathcal{k}^{\mathrm{RSL}})\left(mod\ {\mathcal{N}_m}^{RSL}\right)$$

$$K^{RSL} = \mathcal{D}_{{\mathcal{P}^{RSL}}_m}\left(\mathcal{E}_{{\mathcal{P}^{RSL}}_m}(K^{RSL})\right)$$

Where $\mathcal{D}$ represents the decryption operation.

Colluded group members on decryption cannot obtain the lock K^{RSL} selected by the server accurately hence providing for security.

The Chinese remainder theorem utilized by the server provides protection by securing the group membership and group size. The use of the Chinese remainder theorem and asymmetric cryptographic schemes render the RSL group communication scheme inefficient and are not scalable.

VI. Performance Evaluation

This $RASCP$ secure communication mechanism proposed in this paper is compared with the RSL protocol in terms of the computational costs incurred. The computational cost incurred is proportional to the execution time observed. The $RASCP$and the RSL systems were developed using C#.Net on the Visual Studio 2010 Platform. The $RFID$ tags used were of type 0. The $RFID$ readers were integrated into the platform using VC++.Net. To evaluate the $RASCP$ and the RSL secure group communication systems and to observe the computational costs the number of users in the group were varied from 5, 10, 20, 50, 70 and 100 users. The observations were monitored using log files maintained for every operation. The introduction of the $RFID$ tags into the $RASCP$ and RSL can be considered as an overhead that exists in reading the tags and the average time observed in reading the RFID tags when the number of group members are varied from 5, 10,20,50,70 and 100 is as shown in Fig 1. It could be observed that the average of the overheads observed reduces as the number of users increase proving that the induction of the $RFID$ based security systems are scalable in nature and do not affect the responsiveness of the systems. The average time taken to read a $RFID$ tags was found to be about 0.76ms.

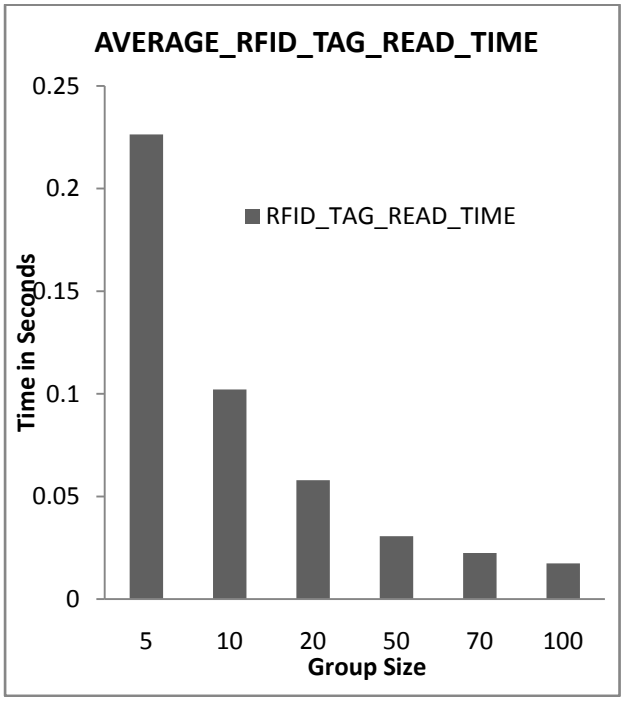


Figure 1 : Average Time Observed in Reading RFID Tags with Varying Number of Group Members

The RSL secure group communication system adopts the RSA Algorithm with a key strength of 1024 [19] bits to incorporate secure transmissions amongst the group members. The $RASCP$ adopts the commutative RSA algorithm to construct a secure communication plane. The RSL relies on a central server for key initialization, distribution using locks and the verifications is carried out by the group members. The experimental evaluation conducted considered the protocol initialization phase as the time taken to verify the group membership and derive the cryptographic keys. The computational overheads observed are as shown in Fig.2. It could be observed that the overheads are reduced by about 99.43% in the initialization phase in the $RASCP$ protocol. The RSL considers a central server and the verification process of the group members. The overheads resulting from the group membership verification process for the RSL scheme is as shown in Fig 3. The $RASCP$ and the RSL group communication protocols adopt cryptographic techniques to construct a secure communication plane.

The overheads arising from the encryption and decryption operations are analyzed for comparisons. The encryption and decryption operations performed using the $RASCP$ and the RSL group communication schemes are compared in terms of the computational complexity exhibited. The results obtained are graphically shown in Fig 4 and Fig 5. Form the figures it is clear that the commutative RSA algorithm adopted in the $RASCP$is computationally less expensive when compared to the RSA cryptographic algorithm adopted in the RSL group communication scheme ye providing security.

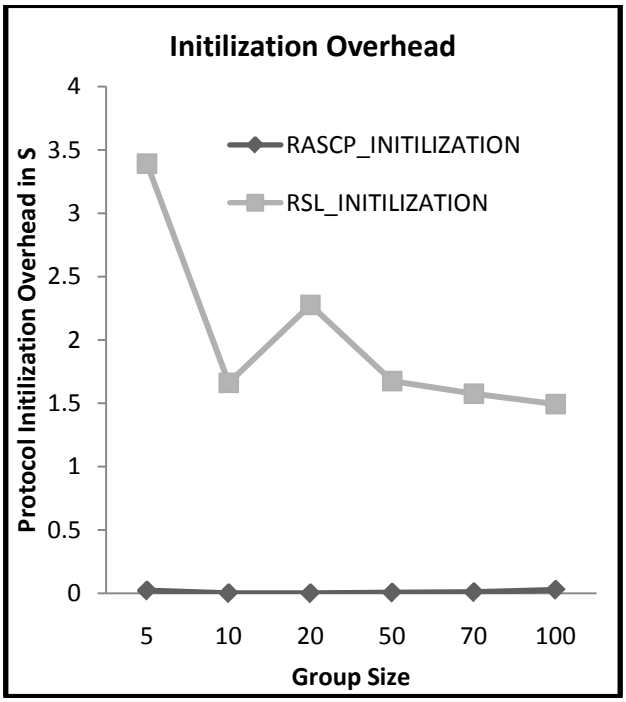


Figure 2 : Average Protocol Initialization Overheads Vs Group Size

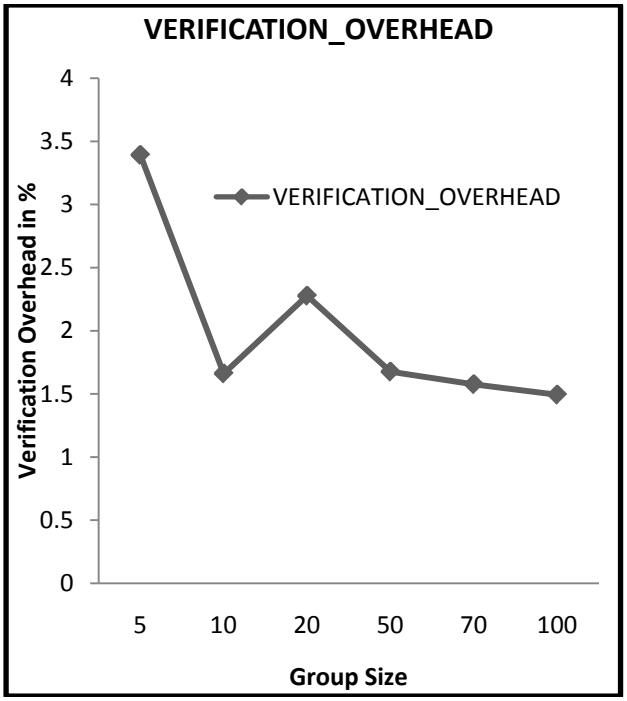


Figure 3 : Verification Overhead in RSL Scheme

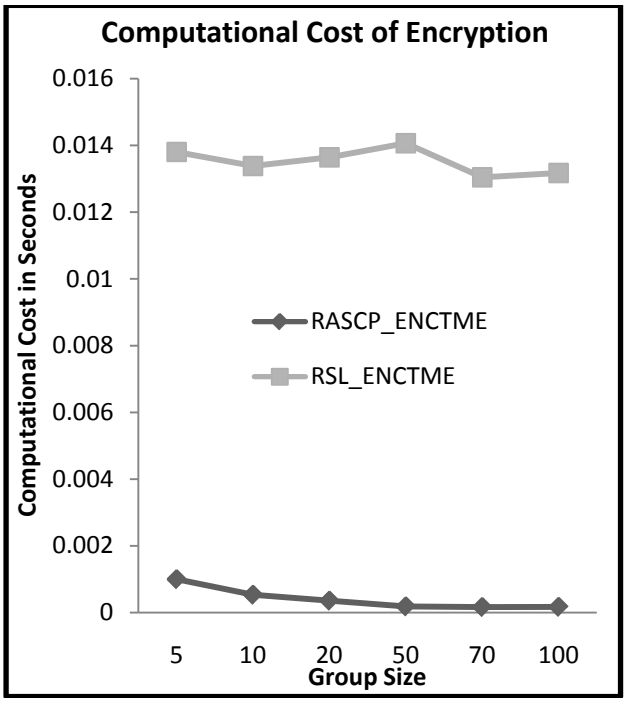


Figure 4 : Computational Analysis of Encryption Operations

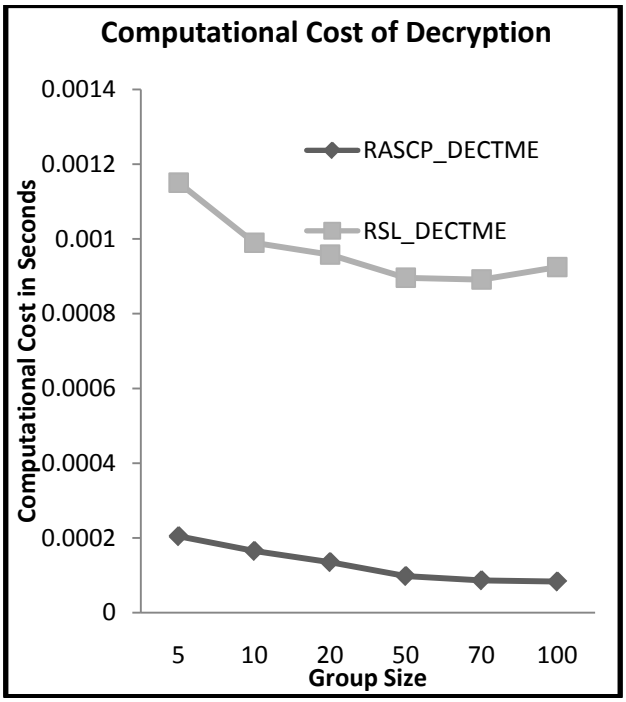


Figure 5 : Computational Analysis of Decryption Operations

The experimental evaluation discussed in this paper prove that the proposed *RASCP* group communication protocol introduced in this paper performs better than the existing *RSL* scheme by reducing the computational overheads and yet providing security of the data transacted amongst the group members.

VII. Conclusion and Future Work

RFID devices are universally used for the purpose of identifications. Many researchers have focused on improving the security of RFID systems in place. This paper introduces a RFID Authentication based Secure Communication Plane (*RASCP*) felicitating secure transmissions amongst group members. The *RASCP* protocol adopts the commutative RSA algorithm to preserve the integrity of the data transacted over the communication plane. The RFID tags are used for the purpose of identification and for protocol initialization. The proposed *RASCP*scheme is compared with the *RSL* secure group communication scheme. The *RASCP* scheme proposed overcomes the drawbacks arising from key distribution, key compromise and external trusted server requirements, yet providing security in the presence of even colluded users. The experimental study conducted proves the efficiency of the proposed *RASCP* over the *RSL* group communication scheme.
The future of the work presented here is to compare the RASCP scheme with other secure group communication schemes using RFID tags.

References Références Referencias

1. IEEE-SA Standards Board,"IEEE Standard for Smart Transducer Interface for Sensors and Actuators—Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats" , IEEE Instrumentation and Measurement Society.IEEE Std 1451.7TM-2010
2. INTERNATIONAL STANDARD"Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) formats" ISO/IEC/IEEE21451-7,First edition 2011-12-15
3. S. Weis, "Security and Privacy in Radio-Frequency Identification Devices," master's thesis, Mass. Inst. of Technology (MIT), May 2003
4. Basel Alomair, Andrew Clark,Jorge Cuellar, and Radha Poovendran,"Scalable RFID Systems: A Privacy-Preserving Protocol with Constant-Time Identification",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. 23, NO. 8, AUGUST 2012,pp 1536 - 1550
5. H. Lee and J. Kim, "Privacy Threats and Issues in Mobile RFID," Proc. First Int'l Conf. Availability, Reliability and Security (ARES '06), Apr. 2006
6. A. Juels, "RFID Security and Privacy: A Research Survey," manuscript, RSA Laboratories, Sept. 2005.
7. D. Molnar and D. Wagner, "Privacy and Security in Library RFID: Issues, Practices, and Architectures," Proc. 11th ACM Conf. Computer and Comm. Security (CCS '04), Oct. 2004.
8. S. Weis et al., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," Proc. First Int'l Conf. Security in Pervasive Computing (SPC '03), Mar. 2003.
9. A. Juels, "Minimalist Cryptography for Low-Cost RFID Tags," Proc. Fourth Int'l Conf. Security in Comm. Networks (SCN '04), Sept. 2004.
10. Y. J. Huang, C. C. Yuan, M. K. Chen, W. C. Lin, and H. C. Teng, "Hardware implementation of RFID mutual authentication protocol," IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1573–1582, May 2010.
11. D. Gries and J. Misra. A linear sieve algorithm for finding prime numbers. Communications of the ACM, 21(12):999–1003, 1978
12. Gabriel Paillard,"A FULLY DISTRIBUTED PRIME NUMBERS GENERATION USING THE WHEEL SIEVE",Parallel and Distributed Computing and Networks, 2005 pp651-656
13. R. Crandall and C. Pomerance. Prime Numbers: a computational perspective. Springer Verlag, 2001
14. Victor P. Hubenko Jr., Richard A. Raines, Rusty O. Baldwin, Barry E. Mullins, Robert F. Mills, and Michael R. Grimaila,"Improving Satellite Multicast Security Scalability by Reducing Rekeying Requirements",IEEE Network • July/August 2007, pp 51-56

15. Bezawada Bruhadeshwar and Sandeep S. Kulkarni,"Balancing Revocation and Storage Trade-Offs in Secure Group Communication ",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 1, JANUARY-FEBRUARY 2011 pp58-73
16. Nathaniel Karst, and Stephen B. Wicker,"On the Rekeying Load in Group Key Distributions Using Cover-Free Families ",2011 IEEE.
17. G. H. Chiou and W. Chen, "Secure broadcasting using the Secure Lock," IEEE Transactions on Software Engineering, vol. 15, no. 8, pp. 929–934, Aug. 1989.
18. Xukai Zou, Mingrui Qi, and Yan Sui."A New Scheme for Anonymous Secure Group Communication",System Sciences (HICSS), 2011 44th Hawaii International Conference.4-7 Jan. 2011.
19. Arjen K. Lenstra, Key length. Handbook of Information Security, Editor-in-Chief, Hossein Bidgoli, pp 617–635.

Global Journals Inc. (US) Guidelines Handbook 2012

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

- 'FARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FARSC" can be added to name in the following manner. eg. **Dr. John E. Hall, Ph.D., FARSC or William Walldroff Ph. D., M.S., FARSC**
- Being FARSC is a respectful honor. It authenticates your research activities. After becoming FARSC, you can use 'FARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 60% Discount will be provided to FARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- FARSC will be given a renowned, secure, free professional email address with 100 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- FARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 15% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- Eg. If we had taken 420 USD from author, we can send 63 USD to your account.
- FARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- After you are FARSC. You can send us scanned copy of all of your documents. We will verify, grade and certify them within a month. It will be based on your academic records, quality of research papers published by you, and 50 more criteria. This is beneficial for your job interviews as recruiting organization need not just rely on you for authenticity and your unknown qualities, you would have authentic ranks of all of your documents. Our scale is unique worldwide.
- FARSC member can proceed to get benefits of free research podcasting in Global Research Radio with their research documents, slides and online movies.
- After your publication anywhere in the world, you can upload you research paper with your recorded voice or you can use our professional RJs to record your paper their voice. We can also stream your conference videos and display your slides online.
- FARSC will be eligible for free application of Standardization of their Researches by Open Scientific Standards. Standardization is next step and level after publishing in a journal. A team of research and professional will work with you to take your research to its next level, which is worldwide open standardization.

- FARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), FARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 80% of its earning by Global Journals Inc. (US) will be transferred to FARSC member's bank account after certain threshold balance. There is no time limit for collection. FARSC member can decide its price and we can help in decision.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

- 'MARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'MARSC" can be added to name in the following manner. eg. Dr. John E. Hall, Ph.D., MARSC or William Walldroff Ph. D., M.S., MARSC
- Being MARSC is a respectful honor. It authenticates your research activities. After becoming MARSC, you can use 'MARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 40% Discount will be provided to MARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- MARSC will be given a renowned, secure, free professional email address with 30 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- MARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 10% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- MARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- MARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), MARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 40% of its earning by Global Journals Inc. (US) will be transferred to MARSC member's bank account after certain threshold balance. There is no time limit for collection. MARSC member can decide its price and we can help in decision.

AUXILIARY MEMBERSHIPS

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJCST for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications

Research letters: The letters are small and concise comments on previously published matters.

5.STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. **Pick a good study spot:** To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. **Think technically:** Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be

sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page

- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to

shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.
- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic

principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.

- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals Inc. (US)

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350