ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

A Proportional Learning on Sink, Warm Hole Attacks with Prevention Algorithms in Wireless Sensor Networks PLSWHA-WSN

Savitha Devi.M[1], Dr.P.ThangaRaj[2]

Research Scholar, Department of Computer Science, Mother Theresa Women's University, Kodaikkannal, TamilNadu, India[1]

Head of Department, Department of CSE, Bannari Amman Institute of Technology, Sathiyamangalam,TamilNadu, India[2]

ABSTRACT: Wireless Sensor network is a network covers of little cost resource constrained sensor nodes that are collaborating using wireless medium. Equivalent to other technologies, in WSNs there are some substantial issues that should be taken into account. One of that issues is the Intruders, who attacks our resources during the transmission and to overcome this issues, the security has to be tightened to prevent the data transfer. As the wireless sensor nodes are employed in a remote or unfriendly environmental area that is prone to attacks repeatedly, so security is an important and valuable criterion to be considered in WSNs. The researchers have a very big challenges in finding out a solution for preventing the resources from the hackers. This paper is presented to do a Comparative and Wide-range topresent all kinds of Intruders with their attacks and especially the sinkhole attackers and Warmhole attackers are analysed with their attacks of theHeterogeneous Wireless sensor Networks and data loss prevention through various algorithms for securing the data in an efficient manner.

KEYWORDS: Intruders, Attacks, Sink Hole Attacks, Warm Hole Attacks, Heterogeneous Wireless Sensor Networks, Security.

I.INTRODUCTION

Intruders are someone who intrudes on the privacy or property of another without permission.The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system.System must maintain a file that associates a password with each authorized user, so that the data can be accessed only by the concern person. The file can be protected by one of two ways as a.The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password and compares it with the stored value. b. Access control to the password file is limited to one or a very few accounts. Intruder tries in various methods to crack the password, the following techniques are for learning passwords a. Try default passwords used b. Try all short passwords (those of one to three characters) c. Try words in the system's online dictionary or a list of likely passwords d. Collect information about users, such as their full names e.Try users' bike numbers, social safety numbers, and door numbers f. Use a Trojan horse. Intrusions have many causes, such as malware (worms, spyware, etc…), attackers gaining illegal access to systems from the Internet, and authorized users of systems who abuse their privileges or try to gain additional privileges for which they are not authorized.

II.RELATED WORK

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible intrusions (incidents).Intrusion detection system (IDS) is software that automates the intrusion detection process. The primeconcern of an IDS is to detect unwanted and malicious activities.Intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. a.Statistical anomaly detection: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then arithmetictrials are applied to experimental behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior. b.Rule-based detection: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

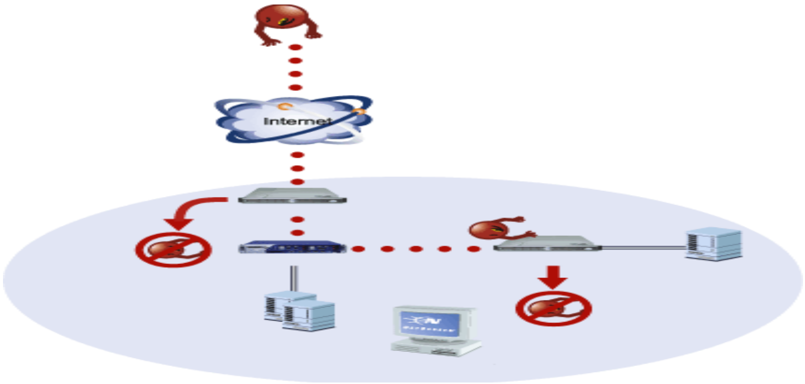

Fig.1 IDS and IPS

The data and the network are attacked by various intruders which has been shown in fig.1. The rule based detection will decide which rule will be applicable to detect the intruders on the path, or network.

c.Password Protection: The front line of defense against intruders is the password scheme. Fundamentally all multiuser systems involve that a user provide not only a name or identifier (ID) but also a password. The password serves to authenticate the ID of the individual logging on to the system. In turn, the ID offers security in the following ways: The ID fixes whether the user is authorized to gain access to a system. The ID determines the privileges accorded to the user. It’s is a dire fact that while every initiative has a firewall, most still agonize from network security problems. Experts are acutely aware of the need for additional caring technologies, and network equipment hawkers are anxious to fill in the gap. Intrusion Prevention Systems have been recognized as cost-effective ways to block malicious traffic, to detect and contain worm and virus threats, to serve as a network observing point, to assist in compliance requirements, and to act as a network sterilizing agent.

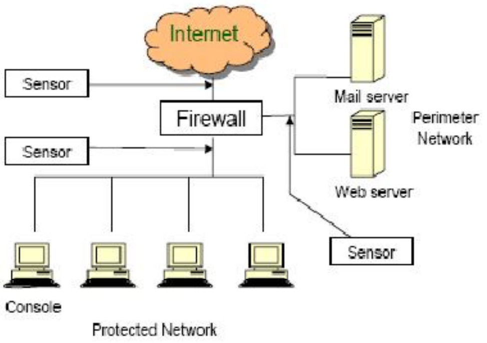

Fig.2 Network Protection

Basically, the intruders are detected through the sensors and protected by the firewall as exposed in the fig.2Intrusion detection systems mainly corrupt their assessments either on Signal (signature-based detection) or Noise (anomaly-based detection). IDS can be categorized on Network-based system, which can concurrently monitor numerous hosts; they can suffer from performance problems, especially with increasing network speeds. Another is Host-based system that can monitor precise applications in ways that would be difficult or incredible in a

Network-based system. While the third is an existence of Hybrid System, this system is the combination of both signature-based and the anomaly-based systems. The following are the approaches for IDS:

a) Signature-based approach: This style is used to detect the identified attacks. It is very active for detecting the attacks without causing an overwhelming figure of incorrect alarms; it can quickly and constantly diagnose the use of a specific attack device. But it has a loophole, that it can only identify the attacks which are defined by its databank.
b) Classification-based approach: This style uses usual and unusual datasets of user behaviour and practices data mining performances to train the IDS system. It creates more accurate in ordering models for IDS as compared to signature-based approaches and thus they are more commanding in detecting familiar attacks. But still they are not accomplish in detecting unknown attacks.

c) Anomaly-based approach: The basic assumption of anomaly detection approach is the attacks that are unlike from regular activities and thus they can be detected by IDS systems that identify these differences. Detection approach can detect unknown attacks also, but still it has an ambiguity. It creates a lot number of false alarms as well as problem in managing fault tolerance. There are a wide variety of dynamic redundancy algorithms for detecting the intruders in the way, in the destination and finding fault tolerance during the transmission.

III. TYPES OF ATTACKS

Classes of attack might comprise passive monitoring of connection, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks proposal attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to edge damage and recover quickly when attacks occur. A Node when it transmit some data it reaches its destination perfectly until it gets some damage through the attackers. The attackers may be denial of services, intrusions, viruses, Flooding attack, Sink hole attack, warmhole attack, etc as shown in fig.3. Also we have protection by firewalls, prevention methods and so on.
There are five types of attack[11]:

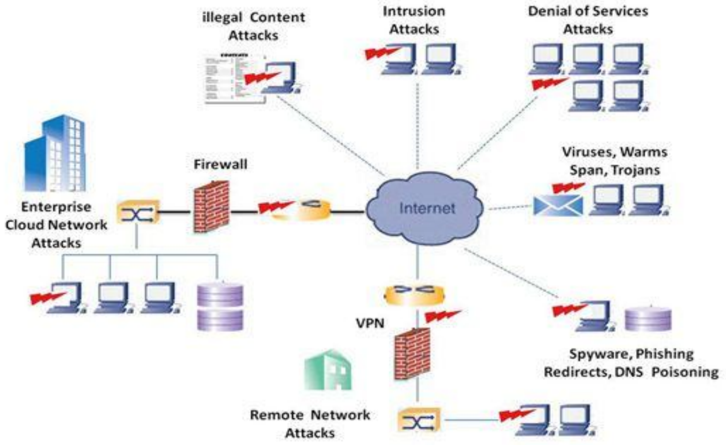
illegal Content Attacks
Intrusion Attacks
Denial of Services Attacks
Firewall
Viruses, Warms Span, Trojans
Enterprise Cloud Network Attacks
Internet
VPN
Spyware, Phishing Redirects, DNS Poisoning
Remote Network Attacks

Fig: 3 Network Attackers

1. Passive Attack monitors unencrypted traffic and aspects for clear-text passwords and sensitive information that can be used in other categories of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encryptedtraffic, and capturing authentication information such as passwords. Passive interception of network operations allows adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

2. Active Attackertries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks comprise attempts to circumvent or break protection features, to introduce

malicious code, and to steal or modify information. These attacks are riding against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks outcome in the disclosure or dissemination of data files, DoS, or modification of data.

3. Distributed Attack covers that the adversary introduce code, such as a Trojan horse or back-door program, to a “trusted” component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks present malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

4.Insider Attack contains someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task

5. Close-in Attack encompasses someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

One popular form of close in attack is social engineering in a social engineering attack, the attacker compromises the network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

Some other attacks are a.Phishing Attack, the hacker produces a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message demanding to trick the user into clicking a link that leads to the fake site. When the user endeavours to log on with their account information, the hacker records the username and password and then tries that information on the real site. b. In Hijack attack, a hacker proceeds over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private data to the hacker by accident. c. In a spoof attack, the hacker adjusts the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rule. d. A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell. e. Exploit attack- In this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability. f. Pass word- An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters.

IV WIRELESS SENSOR NETWORK

Security is a fundamental module of every network design. When planning, building, and operating a network, the importance is a strong security. In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies.The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks.Because they have no Internet connectivity, networks designed in this way can be considered safe from Internet attacks. However, internal threats still exist.

Communication in wireless sensor networks are event driven. Whenever an event triggers wireless sensor nodes generate busty traffic.When the data are transmitted through WSN, it transfer the data with help of base station, transceivers. Here the sensors plays a vital role to reduce the intruders and it identifies the attackers.

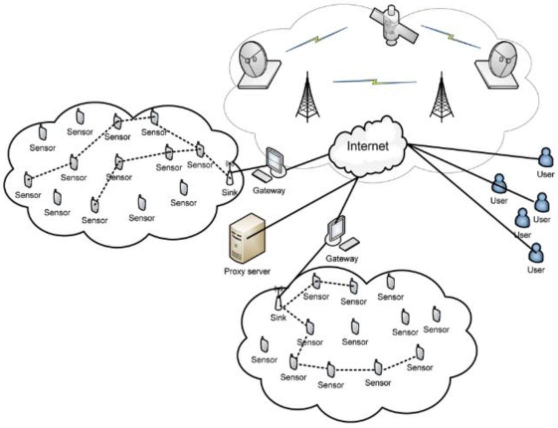

Fig.4 WSN

The main Characteristics of Wireless Sensor Networks requirements are small size, large number, tether-less, and low cost. And the constrained are energy, computation, and communication in small size implies small battery, low cost & energy implies low power CPU, radio with minimum bandwidth and range, ad-hoc deployment implies no maintenance or battery replacement and to increase network lifetime, no raw data is transmitted.

V.COMPARISION OF SINKHOLE AND WARMHOLE ATTACKS

The proportional learning is to identify the intruders during the transmission and to prevent the data from the hackers in heterogeneous WSN.This paper analyses two popular Intruders Prevention Algorithms in WSN. The analysation is comprehensively done for two major attackers, one of two is sinkhole attack in which the attacker are spotted out by novel algorithm and the second one is Warm Hole Attack and detection Algorithm is used to prevent the data and network from the attackers.1.Sink Hole Attack –the authors C.H. Ngai, Jiangchuan Liu, Michael R. Lyu says in a wireless sensor network [1], multiple nodes would send sensor readings to a base station for extrahandling. It is known that such a many-to-one communication is extremelyvulnerable to a sinkhole attack, where an intruder attracts neighbouring nodes with unfaithful routing information, and then executes selective forwarding or alters the data passing through it.

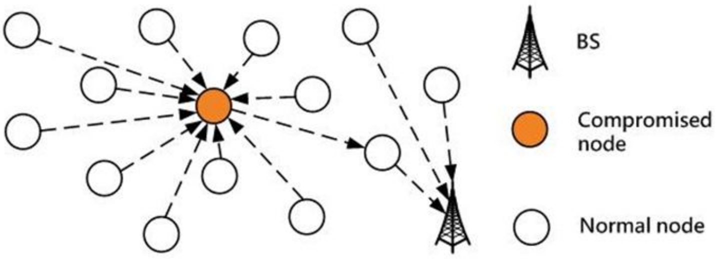

Fig :5 Sink Hole Attacks

A sinkhole attack forms a serious threat to sensor networks, particularly seeing that the sensor nodes are frequently deployed in open areas and of weak computation and battery power.In Sinkhole attack, sometimes the adversary node poses itself as a fake base station (BS) and receives all data of the network. It prevents data from reaching the main BS, or changes the received data and then transfers them to the main BS.

The Authors C.H. Ngai, Jiangchuan Liu, Michael R. LyuSuggested[1] a novel algorithm for spotting the intruder with energy consumption in a sinkhole attack. The algorithm first finds a list of suspected nodes through checking data consistency, and then efficiently identifies the intruder in the list through investigating the network flow information. The algorithm is also robust to deal with multiple malicious nodes that willingly hide the real intruder. The performance of the algorithm is assessed through both numerical analysis and simulations, which confirmed the effectiveness and accuracy of the algorithm. The results also suggest that its communication and computation overheads are reasonably low for wireless sensor networks. In the Algorithm description [2], all network's nodes are similar and distributed randomly in the network. We assume that all network nodes know their location. At the beginning, the BS broadcasts its location to all nodes. The proposed work is appropriated for event driven applications. Whenever a node detects an event, a control packet is sent to the BS using single hop communication. The control packet contains the following information: the unique number of the control packet (id), the transmitter node (Nid), data packet identifier (Pid) and the size of the data packet (Psize).

As analysed in paper [13] After direct transmission of this packet to the BS, the transmitter node, depending on its routing table, sends data packet to its next hop node. The data packet is routed hop by hop until it receives to the BS. When data packet is reached to the BS, the following three situations might be occurred:

1.Data arrive at BS properly: when data arrives at BS, it is
compared to the control packet and the accuracy of the data is determined.

2. Data arrive at BS while manipulated: it means that the
adversary node has changed data en route and transferred them to BS. BS detects this manipulation through comparing the data packet with the original control packet.

3. Data packet never arrives at BS: the adversary node drops
the packet and does not allow it to reach BS. When BS receives the control packet, it waits for a moment to receive the original data packet. Otherwise, it detects the existence of an adversary node in the network.

In cases 2 and 3, the malicious node disrupts the network.

After receiving these twosituationsinthenetwork,it looks forthemaliciousnodesandtriestoremovethem from the networkroutine.Through this algorithm[13]the performance of the simulation parameters referred are Network Radius, number of sensors, energy, data packet size, data packet control. By this method,theamountoflostpacketsdecreases andthe detectionofmalicious andopponent nodestoberemoved from thenetworkoccursmoreexpeditiously.Asthenumber oflostevents is decreased,theenergyconsumptionis reducedtoo.As the part referenced the loss of packets are reduced by using the algorithm to detect the sinkhole attack with the convenience of the energy consumption as a vital role.

2.Warm Hole attack –Mobile ad hoc network applications(Yih-chun Hu , Adrian Perrig , David B. JohnsonYih-chun Hu , Adrian Perrig , David B. Johnson[10])are organized, security emerges as a central requirement. The warmhole attack will confuse the transmission by the tunnel.it will not allow the user to transmit in a right routed path and warmhole attack will intruder in network layer. The wormhole attack, a severe attack in ad hoc networks that is predominantly challenging to defend against. The wormhole attack is imaginable even if the attacker has not compromised any hosts, and even if all communication delivers authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them.The wormhole attack can form a stern threat in wireless networks, expressly against many ad hoc network routing protocols and location-based wireless security systems. For example, most remaining ad hoc network routing protocols, lacking some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. In general mechanism, the packet leashes, for detecting and thus defending against wormhole attacks, and we present a specific protocol, that implements leashes. Also it may arranged in topology networks.

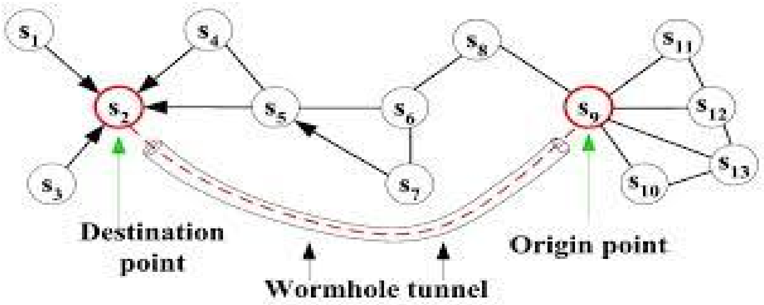

Fig :6WarmHole Attack

Warmhole attack can be launched using several modes. Some of them are a.warmhole using encapsulation b. warmhole out-of-Band channel c. warmhole with high power transmission d. warmhole using packet relay e. warmhole using protocol deviations. Also, several solutions have been proposed for the wormhole attack avoidance like packet leashes, cluster base, hop count analysis and improved DSR protocol. Packet leashes are used as a defense mechanism against wormhole attacks that provide the additional information added to packets to restrict maximum transmission distance of a packet.

5.1Comparisonsof various Techniques of Warmhole Attacks [12]

Techniques	Pros & Cons	Special Hardware	Overhead
PacketLeashes	Temporal leashesare highly efficient. Andare usedwith TIK. They require tighttime synchronization. But geographica lleashes do not require tight time synchronization and increases computation and network overhead.	NO	HIGH
ClusterBasedApproach	Performance of network increases with The increasing number of guard nodes that further increases the probability of detection of worm hole attack But more study has to be done to analyse performance of this algorithm in presence of multiple attacker nodes.	NO	LOW
HopCountAnalysis	Avoiding attacks in this cheme is from The view point of users not of the administrator‟s view point. This scheme MHA when applied with constant boundaries performs better than the loose ones in avoiding attacks.	NO	HIGH
ImprovedDSRprotocol	This technique helps in detecting and Preventing worm hole nodes quickly and easily but does not show major differences between the network parameters compared with the previous one.	NO	LOW

Table : 1

VI. CONCLUSION

Wireless sensor network is a growing field and has many different applications.Most security threats to wireless ad-hoc network are applicable to wireless sensor network.These threats are further complicated by the physical limitations of sensor nodes.Some of these threats can be countered by encryption, data integrity and authentication.Security of wireless sensor network remains an intensive studied field for researchers. In this paper a proportional study have been given about the sinkhole attach and warmhole attack. Existenceofthewormhole nodes in the network is one of the major security difficulties occurred so far. The work is concerned with the comparison of sinkhole attack and warmhole attack with the techniques and modes of wormhole attacks. The major work is to prevent the network from both the attacks in future.

ABBREVIATIONS AND ACRONYMS

[1]. IDS – Intrusion Detection System
[2]. IPS – Intrusion Prevention System
[3]. ID - Identifier
[4]. BS – Base Station
[5]. WSN – Wireless Sensor Network
[6]. Pid – Packet Identifier
[7]. PSize – Packet Size
[8]. Nid – Node Transmitter
[9]. DSR – Dynamic Source Routing

REFERENCES

1. C.H. Ngai, Jiangchuan Liu, Michael R. Lyu "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks", Elsevier volume 30, issue 11-12, 10-September 2007 page 2353-2364 .
2. Cryptography and Network Security Principles and Practices, Fourth Edition, William Stallings, 2005.
3. Computer networks, Andrew S. Tanenbaum. Fourth Edition, 2003.
4. Identity Lifecycle Management, RafalLukawiecki, Strategic Consultant, Project Botticelli Ltd, 2005.
5. Secure Password-Based Cipher Suite for TLS, Michael Steiner University at des Saarlandes and Peter Buhler,ThomasEirich and Michael Waidner.
6. http://www.wikihow.com/Choose-a-Secure-Password.
7.C. Karlof and D.Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," First IEEE International Workshop on Sensor Network Protocols and Applications, May, 2003.
8. Al-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in WirelessSensor Networks: Issues and hallenges," in Proceedings of 8th IEEE ICACT 2006, vol. II, February 20-22, Phoenix Park, Korea,2006, pp. 1043-1048
9. C. K. D. Wagner, "In Secure Routing in Wireless Sensor Networks,"Attacks and Countermeasures.
10.Yih-chunHu , Adrian Perrig , David B. Johnson "Wormhole attacks in wireless networks" (2006)
11. www.computernetworkingnotes.com
12. International Journal Of Research In Computer Applications And Robotics ISSN 2320-7345A Review:Analysis Of Wormhole Attack And Its Detection Techniques.
13. A Novel Algorithm for detecting sinkhole attacks in WSN, International Journal of Computer Theory andEngineering, Vol. 4, No. 3, June 2012.

BIOGRAPHY

Savitha Devi.M is a Research Scholar in Mother Theresa Women's University, Kodaikannel, TamilNadu, India and I thank my university forgivingme theopportunity topresent thisarticle under Network Security.And I am working as an Assistant Professor inPG & Research Department of Computer Science, Don Bosco College, Dharmapuri, TamilNadu, India. I acknowledge our Management for their moral support and encouragement to present the article to enrich the values of Research. The present work is benefited from the input of, my Research Guide Dr.P.Thangaraj, Assistant Professor, Bannari Amman College of Technology, Sathyamangalam, Erode, TamilNadu, India. I would like to thank him, for his valuable assistance to the undertaking of the training shot concise here.