A Survey of Attacks and Security Mechanisms in Wireless Networks

P.Suganthi
Assistant Professor
Department of Computer Applications
Sudharsan Engineering College
Pudukkottai.
suganthi.palani@gmail.com

R.Subasree
PG Student
Department of Computer Applications
Sudharsan Engineering College
Pudukkottai.
sree.suba08@gmail.com

K.Vallikkannu
PG Student
Department of Computer Applications
Sudharsan Engineering College
Pudukkottai.
valli5karuppiah@gmail.com

***Abstract* — Any collection of devices or computers connected with each other by means of communication channels to share resources and communicate with other users. An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Security is an essential service for wired and wireless network communications. It must achieve security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. In this paper, we provide a survey on attacks and the security mechanisms to prevent from those attacks. First, we give an overview of different types of attacks and then we present preventive approaches for those attacks.**

***Keywords* —** Networks, Attacks, Security, Prevention.

I. INTRODUCTION

Network is a collection of devices or computers connected with each other by means of communication channels that help the users to share resources and communicate with other users. There are two main types of network commonly known as wired network and wireless network. *Wired Networks* are those networks in which computer devices attached with each with help of wire. The wire is used as medium of communication for transmitting data from one point of the network to other point of the network. *Wireless Networks* means network in which, computer devices communicates with each other without any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with another device, the destination device must lays within the radio range of each other. Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation.

Wireless networks are getting popular due to their ease of use. Consume or user is no more dependent on wires where he or she is, easy to move and enjoy being connected to the network. One of the great features of wireless network that makes it fascinating and distinguishable amongst the traditional wired networks is mobility. This feature gives user the ability to move freely, while being connected to the network. Wireless networks comparatively easy to install then wired network. There is nothing to worry about pulling the cables/wires in wall and ceilings. Wireless networks can be configured according to the need of the users. These can range from small number of users to large full infrastructure networks where the number of users is in thousands. Wireless networks are very useful for areas where the wire cannot be installed like hilly areas.

On the basis of coverage area the wireless network can be divided into the following categories:
a) Personal Area network
b) Local Area Network
c) Wide Area Network

Wireless Network is infrastructure less as it does not require any specialized router to do the routing tasks. Instead, each and every node in Wireless Network acts as a router as well to perform the routing tasks with the dependability on routing protocols. With the advent of Wireless Network, it becomes easier to form a group communication among a set of peer working group for knowledge sharing, confidential information sharing, etc., without the need for any centralized coordinator to establish the communication between the peers of the group. Without a central coordinator, establishing the proof of identity, authentication, leads to the variety of security attacks. However, the characteristics of Wireless Networks pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non- repudiation.

The primary challenge in building a Wireless Network is equipping each device to continuously maintain the information required to properly route traffic. The nodes in Wireless Network can communicate directly if they are in within each other's wireless transmission ranges otherwise they have to rely on some other nodes to transmit messages if the nodes are outside each other's transmission range. Thus, several intermediate hosts relay the packets which are sent by the source host before they reach the destination host, which in turn leads to a multi-hop scenario I.e. each node, will act as a router. The nodes cooperation is very much important for a successful communication. Thus, a Wireless Network has several salient characteristics: dynamic topologies, resource constraints, limited physical security, and no infrastructure.

Routing protocols available for adhoc networks focus on maximization of throughput, network lifetime, reducing network delay, etc., rather than the security issues. Hence, in

recent years much work has been done to improve the protocols in terms of security, energy efficient and other criteria. There may be various updates that are done to the existing routing protocols to prevent from various attacks. The following characteristics of Wireless Network make it difficult to establish security among the node of the network.

a) Shared Broadcast Channel: Data transmitted by a node is received by all other nodes which are directly / indirectly connected by the transmission range of the network. So malicious nodes can easily receive the data sent by other nodes of the network.

b) Mobile operational environment: Nodes of the mobile adhoc network are roaming from one place to the other and are not stable. They are vulnerable to variety of attacks from other mobile nodes.

c) No central control: Since Wireless Network is wireless and infrastructure less; there are no central nodes to authorize the nodes that are coming into the network, forwarding the packets, performing routing activities, etc. Hence there is a higher probability of a malicious node performing the routing decision and forwarding.

d) Lack of authentication: Wireless Network is dynamic and hence nodes those are come in and leave the network dynamically. This provides a way for intruder to come into the network easily and perform various attacks on the network.

e) Scarce resources: Resources such as bandwidth, battery power and computational power are scarcely available which limits implementation of powerful security algorithms.

II. Related Work

There are various methods and algorithms to defend against or to recover from various security attacks. All the proposed methods either modify the existing proposed protocols like AODV, DSR, and DSDV or make use of some additional hardware to improve the security.

Chiu and Lui [1] proposed a two phase mechanism named as DELPHI which made use of both per hop delay and hop count to give a solution to wormhole attack. Phase 1 named as Data Collection involves collecting the delay and hop count metrics from the nodes of the network. Phase 2 named as Data Analysis and detection involves analysing the information collected in phase 1 to detect the presence of wormhole nodes. DELPHI does not work well when all paths are tunnelled.

Attacks were the adversary has full control of an authenticated device and can perform arbitrary behaviour to disrupt the system are referred to as Byzantine attacks [2]. Many Byzantine attacks share some features with the "selfish" node problem for example not forwarding the data packets to others, but the intentions under these two are different. The goal of the selfish node is to reap the benefits of participating in the ad hoc network without having to expend its own resources in exchange. In contrast, the goal of the Byzantine node is to disrupt the communication of other nodes in the network, without regard to its own resource consumption. These cause Byzantine failures which include the omission failures for example crash, failing to receive a request or failing to send a response and the Commission failures for example processing a request incorrectly or sending an incorrect or inconsistent response to a request.

Black Hole attack is a basic Byzantine attack [3] where adversary stops forwarding data packets, but still participates in the routing protocol correctly. As a result whenever the adversarial node is selected as part of a path by the routing protocol, it prevents communication on that path. Most routing protocols are disrupted by Black Hole attacks because they render the normal methods of route maintenance useless.

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [6]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [7].

Gray Hole attack [4], [5] is a special case of black hole attack where an attacker could create a grey hole, in which it is selectively drops some packets but not others, for example forwarding packets but not data packets.

III. Security Attacks

The attacks in wireless networks can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a wireless network.

Security Attacks Classification

- *Passive Attacks* – Eaves dropping, traffic analysis, monitoring
- *Active Attacks* – Jamming, Spoofing, Modification, Replaying, DoS

The attacks can also be classified into two categories, namely external attacks and internal attacks, according the domain of the attacks. Sometimes it is also called as outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged

access rights. Attacks can also be classified according to network protocol stacks. Some attacks could be launched at multiple layers.

TABLE I. : SECURITY ATTACKS ON PROTOCOL STACKS

Layer	Attacks
Application layer	Repudiation, Data corruption
Transport Layer	Session hijacking, SYN Flooding
Network Layer	Wormhole, blackhole, byzantine, flooding, resource consumption, location disclosure attacks
Data link Layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical Layer	Jamming, interceptions, eaves dropping
Multi – layer attacks	DoS, impersonation, replay, man-in-the-middle

Here, we are going to discuss about network layer attacks such as wormhole, byzantine, black hole, grayhole attacks.

a) Wormhole Attack

An attacker receives packets at one location in the network and sends them to another location. Routing is disrupted when routing control messages are tunnelled. This tunnel between two malicious nodes acts as a wormhole which poses a great threat to MANET routing protocols. When a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack always leads to the discovery of routes that includes the malicious wormhole node.

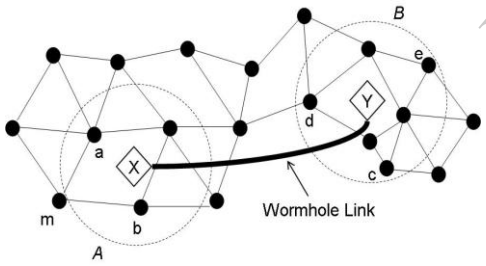

Figure 1: Wormhole Attack

b) Byzantine Attack

Byzantine attack refers to a malicious node creating routing loops, forwarding packets through non – optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

c) Blackhole Attack

In black hole, the malicious node tries to advertise a route to the destination even though the malicious node does not have any valid route. Thus, the black hole attack tries to exploit the mobile ad hoc routing protocol, such as AODV, by advertising route replies to the source node. On grabbing the attention of the source node, the malicious node intercepts the forwarded packets and does not forward it to the destination since it does not have a valid route. Any malicious node suppresses or modifies packets originating only from some nodes but not from all the nodes, which limits other nodes to know about the malicious behavior.

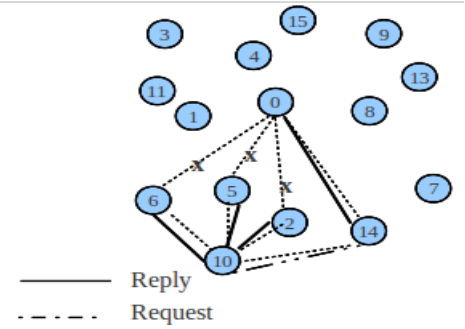

Figure 2: Blackhole Attack

d) Grayhole Attack

A variation of black hole attack s is the grayhole attack, in which nodes either drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). Both types of grayhole attacks seek to disrupt the network without being detected by the security measures in place.

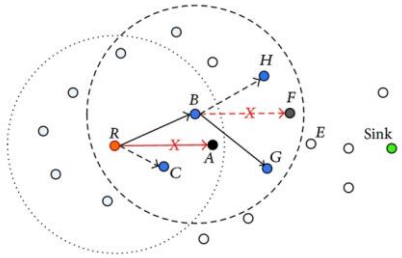

Figure 3: Grayhole Attack

e) Rushing Attack

Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne.

f) Resource Consumption Attack

This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

g) Location disclosure attack

An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against MANET, is unsolved. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track

changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

IV. Security Mechanisms

A variety of security mechanisms have been invented to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of security. As a second line of security, intrusion detection systems and cooperation enforcement mechanisms implemented in wireless network can also help to defend against attacks or enforce cooperation, reducing selfish node behavior.

A) Preventive mechanism

The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions can be used to enhance data integrity in transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well. It is also necessary to consider the physical safety of mobile devices, since the hosts are normally small devices, which are physically vulnerable. For example, a device could easily be stolen, lost, or damaged. In the battlefield they are at risk of being hijacked. The protection of the sensitive data on a physical device can be enforced by some security modules, such as tokens or a smart card that is accessible through PIN, passphrases, or biometrics. Although all of these cryptographic primitives combined can prevent most attacks in theory, in reality, due to the design, implementation, or selection of protocols and physical device restrictions, there are still a number of malicious attacks bypassing prevention mechanisms.

B) Reactive mechanism

An intrusion detection system is a second line of security. There are widely used to detect misuse and anomalies. A misuse detection system attempts to define improper behavior based on the patterns of well-known attacks, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns; Anomaly detection attempts to define normal or expected behavior statistically. It collects data from legitimate user behavior over a period of time, and then statistical tests are applied to determine anomalous behavior with a high level of confidence. In practice, both approaches can be combined to be more effective against attacks. Some intrusion detection systems for wireless network have been proposed in recent research papers.

V. Security Against Attacks

Cryptography algorithms are security primitives, which are widely used for the purposes of authentication, confidentiality, integrity, and non-repudiation. Most cryptographic systems rely on the underlining secure, robust, and efficient key management system. Key management is in the central part of any secure communication, and is the weak point of system security and protocol design. A key is a piece of input information for cryptography algorithms. If the key were released, the encrypted information would be disclosed. The secrecy of the symmetric key and private key must be assured locally. The Key Encryption Key (KEK) approach could be used at local hosts to build a line of defense. Key distribution and key agreement over an insecure channel are at high risk and suffer from potential attacks. In the traditional digital envelop approach, a session key is generated at one side and is encrypted by the public-key algorithm. Then it is delivered and recovered at the other end. In the Diffie-Hellman (DH) scheme, the communication parties at both sides exchange some public information and generate a session key on both ends. Several enhanced DH schemes have been invented to counter man-in-the-middle attacks. In the symmetric approach, the sequence number or a nonce could be included to prevent the replay attack on setting up a session key. In addition, a multi-way challenge response protocol, such as Needham-Schroeder, can also be used. Kerberos, which is based on a variant of Needham-Schroeder, is an authentication protocol used in many real systems including Windows. Key integrity and ownership should be protected from advanced key attacks.

Digital signature, message digest, and hashed message authentication code (HMAC) are techniques used for data authentication or integrity purposes. Similarly, public key is protected by the public-key certificate, in which a trusted entity called the certification authority (CA) in PKI vouches for the binding of the public key with the owner's identity. In systems lacking a trusted third party (TTP), the public-key certificate is vouched for by peer nodes in a distributed manner, such as pretty good privacy (PGP). In some distributed approaches, the system secret is distributed to a subset or all of the network hosts based on threshold cryptography. Obviously, a certificate cannot prove whether an entity is "good" or "bad", but can prove ownership of a key. Mainly it is for key authentication.

A cryptographic key could be compromised or disclosed after a certain period of usage. Since the key should no longer be useable after its disclosure, some mechanism is required to enforce this rule. In PKI, this can be done implicitly or explicitly. The certificate contains the lifetime of validity-it is not useful after expiration. But in some cases, the private key could be disclosed during the valid period, in which case certification authority (CA) needs to revoke a certificate explicitly and notify the network by posting it onto the certificate revocation list (CRL) to prevent its usage. Currently there are three types of key management on Wireless Neworks: the first one is virtual CA approach, the second one is certificate chaining, and the third one is composite key management, which combines the first two.

VI. Conclusions

Security is a fundamental component of every network design. Today Security is an essential activity in all type of communication and transactional processes. We have discussed security issues related to integrated wired and wireless networks. The mechanisms solved many security

issues related to wireless communication but they have not solved them completely. So, we can design a security mechanism by which we can minimize or completely remove many of those attacks. In future, we will propose to design a robust framework that uses minimal public key cryptography to avoid overload on the network and uses shared key cryptography extensively to provide security.

REFERENCES

[1] H.S. Chiu and K.S. Lui, "DELPHI: Wormhole detection mechanism for Ad Hoc wireless networks," In Proc. International Symposium on Wireless Pervasive Computing, Phuket, Thailand, Jan 2006.

[2] Bin Xie and Anup Kumar. "A Framework for Internet and Ad hoc Network Security". IEEE Symposium on Computers and Communications (ISCC-2004), June 2004.

[3] M. Medadian, M.H. Yektaie, and A.M. Rahmani. "Combat with black hole attack in aodv routing protocol in Manet". In Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on, pages 1 –5, Nov. 2009.

[4] A. Patcha and A. Mishra. "Collaborative security architecture for black hole and Gray Hole attack prevention in mobile ad hoc networks". In Radio and Wireless Conference, 2003. RAWCON '03. Proceedings, pages 75 – 78, Aug. 2003.

[5] D.M. Shila, Yu Cheng, and T. Anjali. "Channel- aware detection of gray hole attacks in wireless mesh networks". In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pages 1 –6, 30 2009-dec. 4 2009.

[6] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[7] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006

[8] Webopedia, an Internet Dictionary, http://www.webopedia.com/.