Master Thesis
Computer Science
Thesis no: MCS-2007:07
22nd March, 2007

Security Threats in Mobile Ad Hoc Network

Kamanshis Biswas and Md. Liakat Ali

Department of
Interaction and System Design
School of Engineering
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

This thesis is submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:

Author(s):

Kamanashis Biswas

E-mail: avrobth@gmail.com

Md. Liakat Ali

E-mail: liakat3026@gmail.com

Advisor:

Rune Gustavsson

E-mail: rgu@bth.se

Department of Computer Science

Department of
Interaction and System Design
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

Internet: www.bth.se/tek
Phone: +46 457 38 50 00
Fax: + 46 457 102 45

Acknowledgements

First and foremost, we would like to express our heartiest gratitude to our honorable supervisor Prof. Dr. Rune Gustavsson for his suggestions, guidance, constant encouragement and enduring patience throughout the progress of the thesis. We would also like to express our sincere thanks to Martin Fredriksson for his advices and all-out cooperation.

Abstract

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. In this thesis, we identify the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer. To accomplish our goal, we have done literature survey in gathering information related to various types of attacks and solutions, as well as we have made comparative study to address the threats in different layers. Finally, we have identified the challenges and proposed solutions to overcome them. In our study, we have found that necessity of secure routing protocol is still a burning question. There is no general algorithm that suits well against the most commonly known attacks such as wormhole, rushing attack etc. In conclusion, we focus on the findings and future works which may be interesting for the researchers like robust key management, trust based systems, data security in different layer etc. However, in short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.

Keywords: *MANET, blackhole, wormhole, DoS, routing, TCP ACK storm, backoff scheme*

Contents

List of Figures

List of Tables

Chapter One

Introduction

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multihop paths through the network to any other node. This idea of Mobile ad hoc network is also called infrastructureless networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly [2].

1.1 Background

Now-a-days, Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self-configuration and self-maintenance capabilities [16]. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless *MANET* presents a larger security problem than conventional wired and wireless networks.

Although mobile ad hoc networks have several advantages over the traditional wired networks, on the other sides they have a unique set of challenges. Firstly, MANETs face challenges in secure communication. For example the resource constraints on nodes in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Secondly, mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Thirdly, static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like *DoS* (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information. Finally, lack of cooperation and constrained capability is common in wireless *MANET* which makes anomalies hard to distinguish from normalcy. In general, the wireless *MANET* is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distribution cooperation and constrained capability [2].

1.2 Related Work

A number of researches are done on security challenges and solutions in Mobile ad hoc network. Zhou and Haas have proposed using threshold cryptography for providing security to the network [18]. Hubaux et al. have defined a method that is designed to ensure equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates [3]. Kong, et al. [8] have proposed a secure ad hoc routing protocol based on secret sharing; unfortunately, this protocol is based on erroneous assumptions, e.g., that each node cannot impersonate the *MAC* address of multiple other nodes. Yi et al. also have designed a general framework for secure ad hoc routing [17]. Deng, et al. have focused on the routing security issues in *MANET*s and have described a solution of ‘black hole’ problem [2]. Sanzgiri, et al. have proposed a

secure routing protocol *ARAN* which is based on certificates and successfully defeats all identified attacks [14].Yang, et al. have identified the security issues related to multihop network connectivity, discussed the challenges to security design, and reviewed the state-of-art security proposals that protect the *MANET* link- and network-layer operations of delivering packets over the multihop wireless channel [16]. In this paper, the emphasis is given only on the link layer and network layer security issues.

1.3 Research Goals

In this thesis, we focus on the overall security threats and challenges in Mobile ad hoc networks *(MANET).* The security issues are analyzed from individual layers namely application layer, transport layer, network layer, link layer and physical layer. This modularity extends the clarity and depicts the original scenario in each layer. The solutions of the current problems are also reported here so that one may get direction. This study provides a good understanding of the current security challenges and solutions of the *MANET*s. In general the following questions are addressed in our thesis:

- What are the vulnerabilities and security threats in MANET? Which level is most vulnerable to attack?
- How the security services like confidentiality, integrity and authentication can be achieved from mobile ad hoc networks? What steps should be taken?
- What are the countermeasures? How the security of the entire system is ensured?
- What are the potential dangers that may be crucial in future?

1.4 Guidance to the Work

The thesis is organized as follows. *Chapter 2* is an overview of the security goals that must be achieved to ensure secure communication in *MANET*. *Chapter 3* presents the security exploits possible in ad hoc network. *Chapter 4* emphasizes on threats imposed in Physical layer. *Chapter 5, 6, 7 and 8* presents the security challenges in Link layer,

Network layer, Transport layer and Application layer respectively. *Chapter 9* focuses on the solutions of the problems described in previous sections. And finally *Chapter 10* offers the concluding remarks and future works. The following two tables, precisely Table 1.1[15] summarizes the attacks and Table 1.2 [16] represents the solutions in each layer in MANET.

Table 1.1: Security Attacks on each layer in MANET

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, eavesdropping

Table 1.2: Security Solutions for MANET

Layer	**Security Issues**
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authentication and securing end-to-end or point-to-point communication through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Data link layer	Protecting the wireless MAC protocol and providing link layer security support
Physical layer	Preventing signal jamming denial-of-serviceattacks

1.5 Our Work

Security should be taken into account at the early stage of design of basic networking mechanisms. In our study, we have identified the security threats in each layer and corresponding countermeasures. The following table summarizes the potential security attacks and the actions that can be taken to prevent the attacks.

Table 1.3: Security threats and countermeasures

Layers	**Attacks**	**Solutions**
Application layer	Lack of cooperation attacks, Malicious code attacks (virus, worms, spywares, Trojan horses) etc.	Cooperation enforcement (Nuglets, Confidant, CORE) mechanisms, Firewalls, IDS etc.
Transport layer	Session hijacking attack, SYN flooding attack, TCP ACK storm attack etc.	Authentication and securing end-to-end or point-to-point communication, use of public cryptography (SSL, TLS, SET, PCT) etc.
Network layer	Routing protocol attacks (e.g. DSR, AODV etc.), cache poisoning, table overflow attacks, Wormhole, blackhole, Byzantine, flooding, resource consumption, impersonation, location disclosure attacks etc.	Source authentication and message integrity mechanisms to prevent routing message modification, Securing routing protocols (e.g. IPSec, ESP, SAR, ARAN) to overcome blackhole, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack etc.
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness etc.	No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP, using WPA etc.
Physical layer	Jamming, interceptions, eavesdropping	Using Spread spectrum mechanisms e.g. FHSS, DSSS etc.

Chapter Two

Security Services

The ultimate goals of the security solutions for *MANETs* is to provide security services, such as *authentication, confidentiality, integrity, authentication, nonrepudiation, anonymity* and *availabilit*y to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. There is no single mechanism that will provide all the security services in *MANETs*. The common security services are described below.

2.1 Availability

Availability is concerned with the (unauthorized) upholding of resources. A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures such as authentication and encryption whereas others require some sort of action to prevent or recover from loss of availability of elements or services of a distributed system. Availability ensures the survivability of network services despite of various attacks. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service [18].

2.2 Confidentiality

Confidentiality ensures that certain information is only readable or accessible by the authorized party. Basically, it protects data from passive attacks. Transmission of sensitive information such as military information requires confidentiality. Release of such information to enemies could have devastating consequences e.g. *ENIGMA*. Routing and packet forwarding information must also remain confidential so that the enemies could never take the advantages of identifying and locating their targets in a battlefield. With respect to the release of message contents, several levels of protection can be identified.

2.3 Integrity

Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted. As with confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message. But, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under integrity service. Thus it addresses both message stream modification and denial of service.

2.4 Authentication

Authentication ensures that the access and supply of data is done only by the authorized parties. It is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function is to assure the recipient that the message is from the source that it claims to be from. Without authentication, an

adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes [18].

2.5 Nonrepudiation

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver. Nonrepudiation is useful for detection and isolation of compromised nodes. When node ***A*** receives an erroneous message from node ***B***, nonrepudiation allows ***A*** to accuse ***B*** using this message and to convince other nodes that ***B*** is compromised.

2.6 Scalability

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network [18]. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system. It is very easy to make an island-hopping attack through one rough point in a distributed network.

2.7 Summary

In this chapter, common security services are described briefly. Still there are other security services which also be considered. For example, authorization that is of concern to certain application. Access control is another one which limits and controls the access to host systems and applications via communication links. One important point is that always there is a tradeoff between security services and achieving a good tradeoff among these services is one fundamental challenge in security design for MANETs.

Chapter Three

Types of Attacks in MANET

The current Mobile ad hoc networks allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Current *MANETs* are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. In this chapter, our focus is on vulnerabilities and exposures in the current ad hoc network. We have classified the attacks as *modification, impersonation, fabrication, wormhole* and *lack of cooperation.*

3.1 Attacks Using Modification

Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct *DoS* attacks by modifying message fields or by forwarding routing message with false values. In *fig. 3.1, **M*** is a malicious node which can keep traffic from reaching ***X*** by continuously advertising to ***B*** a shorter route to ***X*** than the route to ***X*** that ***C*** advertises [14]. In this way, malicious nodes can easily cause traffic subversion and denial of service *(DoS)* by simply altering protocol fields: such attacks compromise the integrity of routing computations. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.

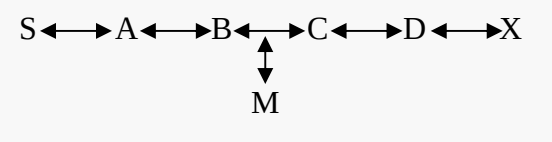

Figure 3.1: Ad hoc network and a malicious node

Consider the following *fig. 3.2*. Assume a shortest path exists from ***S*** to ***X*** and, ***C*** and ***X*** cannot hear each other, that nodes ***B*** and ***C*** cannot hear other, and that ***M*** is a malicious node attempting a denial of service attack. Suppose ***S*** wishes to communicate with ***X*** and that ***S*** has an unexpired route to ***X*** in its route cache. ***S*** transmits a data packet toward ***X*** with the source route ***S*** --> ***A*** --> ***B*** --> ***M*** --> ***C*** --> ***D*** --> ***X*** contained in the packet's header. When ***M*** receives the packet, it can alter the source route in the packet's header, such as deleting ***D*** from the source route. Consequently, when ***C*** receives the altered packet, it attempts to forward the packet to ***X***. Since ***X*** cannot hear ***C***, the transmission is unsuccessful [14].

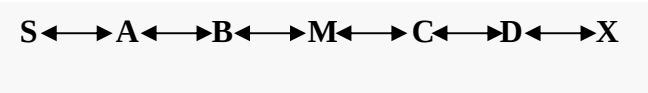

Figure 3.2: Ad hoc network with Dos attack

3.2 Attacks Using Impersonation

As there is *no authentication* of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its *MAC* or *IP address* in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network. Here we have described the scenario in details.

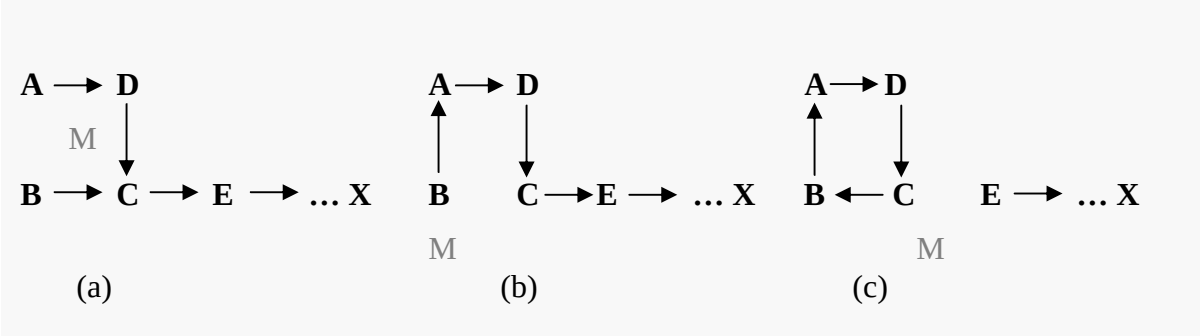

Figure 3.3: A sequence of events forming loops by spoofing packets

In the above *fig. 3.3(a)*, there exists a path between five nodes. ***A*** can hear ***B*** and ***D***, ***B*** can hear ***A*** and ***C***, ***D*** can hear ***A*** and ***C***, and ***C*** can hear ***B***, ***D*** and ***E***. ***M*** can hear ***A***, ***B***, ***C***, and ***D*** while ***E*** can hear ***C*** and next node in the route towards ***X***. A malicious node ***M*** can learn about the topology analyzing the discovery packets and then form a routing loop so that no one nodes in his range can reach to the destination ***X***. At first, ***M*** changes its MAC address to match ***A***'s, moves closer to ***B*** and out of the range of ***A***. It sends a message to ***B*** that contains a hop count to ***X*** which is less than the one sent by ***C***, for example *zero*. Now ***B*** changes its route to the destination, ***X*** to go through ***A*** as shown in the *fig. 3.3(b)*. Similarly, ***M*** again changes its *MAC* address to match ***B***'s, moves closer to ***C*** and out of the range of ***B***. Then it sends message to ***C*** with the information that the route through ***B*** contains hop count to ***X*** which is less than ***E***. Now, ***C*** changes its route to ***B*** which forms a loop as shown in *fig. 3.3(c)*. Thus ***X*** is unreachable from the four nodes in the network.

3.3 Attacks through Fabrication

Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. In *MANET*, fabrication is used to refer the attacks performed by generating false routing messages. Such kind of attacks can be difficult to verify as they come as valid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted [11]. Consider the *fig. 3.1*. Suppose node ***S*** has a route to node ***X*** via nodes ***A***, ***B***, ***C***, and ***D***. A malicious node ***M*** can

launch a denial-of-service attack against ***X*** by continually sending route error messages to ***B*** spoofing node ***C***, indicating a broken link between nodes ***C*** and ***X***. ***B*** receives the spoofed route error message thinking that it came from ***C***. ***B*** deletes its routing table entry for ***X*** and forwards the route error message on to ***A***, who then also deletes its routing table entry. If ***M*** listens and broadcasts spoofed route error messages whenever a route is established from ***S*** to ***X***, ***M*** can successfully prevent communications between ***S*** and ***X*** [14].

3.4 Wormhole Attacks

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers. In the *fig. 3.4*, M_1 and M_2 are two malicious nodes that encapsulate data packets and falsified the route lengths.

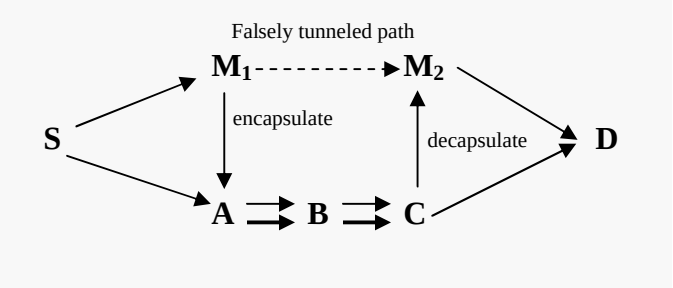

Figure 3.4: Path length spoofed by tunneling

Suppose node ***S*** wishes to form a route to ***D*** and initiates route discovery. When M_1 receives a *RREQ* from ***S***, M_1 encapsulates the *RREQ* and tunnels it to M_2 through an existing data route, in this case {M_1 --> ***A*** --> ***B*** --> ***C*** --> M_2}. When M_2 receives the encapsulated *RREQ* on to ***D*** as if had only traveled {***S*** --> M_1 --> M_2 --> ***D***}. Neither M_1 nor M_2 update the packet header. After route discovery, the destination finds two routes

from ***S*** of unequal length: one is of 5 and another is of 4. If M_2 tunnels the *RREP* back to M_1, ***S*** would falsely consider the path to ***D*** via M_1 is better than the path to ***D*** via ***A***. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

3.5 Lack of Cooperation

Mobile Ad Hoc Networks *(MANETs)* rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a *MANET* gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources. This can endanger the correct network operation by simply not participating to the operation or by not executing the packet forwarding. This attack is also known as the black hole attack and is described briefly in later section.

3.6 Summary

The security of the ad hoc networks greatly depends on the secure routing protocol, transmission technology and communication mechanisms used by the participating nodes. In this chapter, we have focused on the common attacks in *MANET*. The rest of the thesis describes the threats in each layer in the protocol stack and prescribes solution of those attacks.

Chapter Four

Security Threats in Physical Layer

Physical layer security is important for securing *MANET* as many attacks can take place in this layer. The physical layer must adapt to rapid changes in link characteristics. The most common physical layer attacks in *MANET* are eavesdropping, interference, denial-of-service and jamming. The common radio signal in *MANET* is easy to jam or intercept. Moreover an attacker can overhear or disrupt the service of wireless network physically. An attacker with sufficient transmission power and knowledge of the physical and medium access control layer mechanisms can gain access to the wireless medium. Here we will describe eavesdropping, interference and jamming attacks in brief.

4.1 Eavesdropping

Eavesdropping is the reading of messages and conversations by unintended receivers. The nodes in *MANET* share a wireless medium and the wireless communication use the RF spectrum and broadcast by nature which can be easily intercepted with receivers tuned to the proper frequency. As a result transmitted message can be overheard as well as fake message can be injected into the network.

4.2 Interference and Jamming

Jamming and interference of radio signals causes message to be lost or corrupt. A powerful transmitter can generate signal that will be strong enough to overwhelm the target signal and can disrupt communications. Pulse and random noise are the most common type of signal jamming [15].

4.3 Summary

The topology is highly dynamic as nodes frequently leave or join network, and roam in the network on their own will. Again, the communication channel in *MANET* is bandwidth-constrained and shared among multiple network entities. This channel is also subject to interferences and errors exhibiting volatile characteristics in terms of bandwidth and delay. The attacker may take the opportunity of these volatile characteristics.

Chapter Five

Security Threats in Link Layer

The MANET is an open multipoint peer-to-peer network architecture in which the link layer protocols maintain one-hop connectivity among the neighbors. Many attacks can be launched in link layer by disrupting the cooperation of the protocols of this layer. Wireless medium access control (MAC) protocols have to coordinate the transmission of the nodes on the common communication or transmission medium. The IEEE 802.11 MAC protocol uses distributed contention resolution mechanisms which are based on two different coordination functions. One is Distributed Coordination Function (DCF) which is fully distributed access protocol and the other is a centralized access protocol called Point Coordination Function (PCF). For resolving channel contention among the multiple wireless hosts, DCF uses a carrier sense multiple access with collision avoidance or CSMA/CA mechanism.

5.1 Threats in IEEE 802.11 MAC

The IEEE 802.11 MAC is vulnerable to DoS attacks. To launch the DoS attack, the attacker may exploit the binary exponential backoff scheme. For example, the attacker may corrupt frames easily by adding some bits or ignoring the ongoing transmission. Among the contending nodes, the binary exponential scheme favors the last winner which leads to capture effect. Capture effect means that nodes which are heavily loaded tend to capture the channel by sending data continuously, thereby resulting lightly loaded neighbors to backoff endlessly. Malicious nodes may take the advantage of this capture effect vulnerability. Moreover, it can cause a chain reaction in the upper level protocols using backoff scheme, like TCP window management [15].

Another vulnerability to DoS attacks is exposed in IEEE 802.11 MAC through NAV (Network Allocation Vector) field carried in the RTS/CTS (Ready to Send/Clear to Send) frames. During the RTS/CTS handshake, a small RTS frame including the time needed to complete the CTS, data and ACK frames is sent by the sender. All the neighbors of the sender and receiver update their NAV field according to the time that they overheard for transmission duration. The attacker in the local neighborhood is also aware of the duration of the ongoing transmission and he/she may transmit a few bits within this period to incur bit errors in a victim's link layer frame via wireless interference [16].

5.2 Threats in IEEE 802.11 WEP

The first security scheme provided by IEEE 802.11 standards is Wired Equivalent Privacy (WEP). Basically, it was designed to provide security for WLAN. But it suffers from many design flaws and some weakness in the way RC4 cipher used in WEP. It is well known that WEP is vulnerable to message privacy and message integrity attacks and probabilistic cipher key recovery attacks. Now, WEP is replaced by AES in 802.11i. Some of the weakness of the WEP is described below.

- Key management is not specified in the WEP protocol. Lack of key management is a potential exposure for most attacks exploiting manually distributed secrets shared by large populations.

- The initialization vector (IV) used in WEP is a 24-bit field which is sent in clear and is a part of the RC4 leads to probabilistic cipher key recovery attack or most commonly known as analytical attack.

- The combined use of a non-cryptographic integrity algorithm, CRC 32 with the stream chipper is a security risk and may cause message privacy and message integrity attacks.

5.3 Summary

Most of the link layer attacks in MANET are removed by enhancing the existing protocol or proposing a new protocol to thwart such threats. For example, WPA, RSN/AES-CCMP is also being developed to improve the cryptographic strength and enhance security. Still attacks using the NAV field of RTS/CTS frame remains unsolvable and to the best of our knowledge, it remains unclear how to defeat such resource consumption DoS attacks in MANET.

Chapter Six

Security Threats in Network Layer

In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network.

6.1 Routing Protocols

A number of routing protocols have been developed in MANETs. The main target is to provide secure communication and remove flaws in existing protocols. They can be classified into the following categories.

6.1.1 Table-driven

In table-driven routing protocol, *proactive* scheme is used. It means that they maintain consistent up-to-date routing information from each node to every other node in the network. One or more tables are used to store routing information, changes in network topology etc. in order to maintain a consistent network environment. Some common examples are *DSDV (Highly Dynamic Destination-Sequenced Distance Vector routing protocol), DBF (Distributed Bellman-Ford Routing Protocol), HSR (Hierarchical State Routing protocol), OLSR (Optimized Link State Routing Protocol)* etc.

6.1.2 On-Demand

Source initiated on-demand *(reactive)* routing protocol is different from table-driven routing protocol. It creates routes only when asked by the source. The protocol finds the route on demand by flooding the network with *Route Request packets*. Some examples of on-demand protocol are *Admission Control enabled On demand Routing (ACOR), Ant-based Routing Algorithm for Mobile Ad-Hoc Networks, Dynamic Source Routing (DSR), DYnamic Manet On-demand Routing (DYMOR)* etc.

6.1.3 Other Routing Protocols

There are two other types of routing protocol namely Hybrid and Hierarchical. The hybrid routing protocol is a combination of proactive and reactive scheme. On the other hand, the hierarchical protocols contain scalable routing strategies and establish a hierarchy which is followed in the way of ant-trail. *HSLS (Hazy Sighted Link State routing protocol)* and *ZRP (Zone Routing Protocol)* are hybrid protocol whereas *DDR (Distributed Dynamic Routing Algorithm), HSR (Hierarchical State Routing), OORP (OrderOne Routing Protocol)* are examples of hierarchical protocol. Another protocol is also used in MANET which is known as geographical routing protocol. *Geographic routing* refers to a family of techniques to route data packets in a communication network. *ALARM (Adaptive Location Aided Routing - Mines), GPSR (Greedy Perimeter Stateless Routing)* are geographic protocol.

6.2 Network Layer Attacks

A number of attacks in network layer have been identified and studied in security research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow. For example, as shown in the *fig 6.1(a) and (b)* in the next page, a malicious node ***M*** can inject itself into the routing path between sender ***S*** and receiver ***R***.

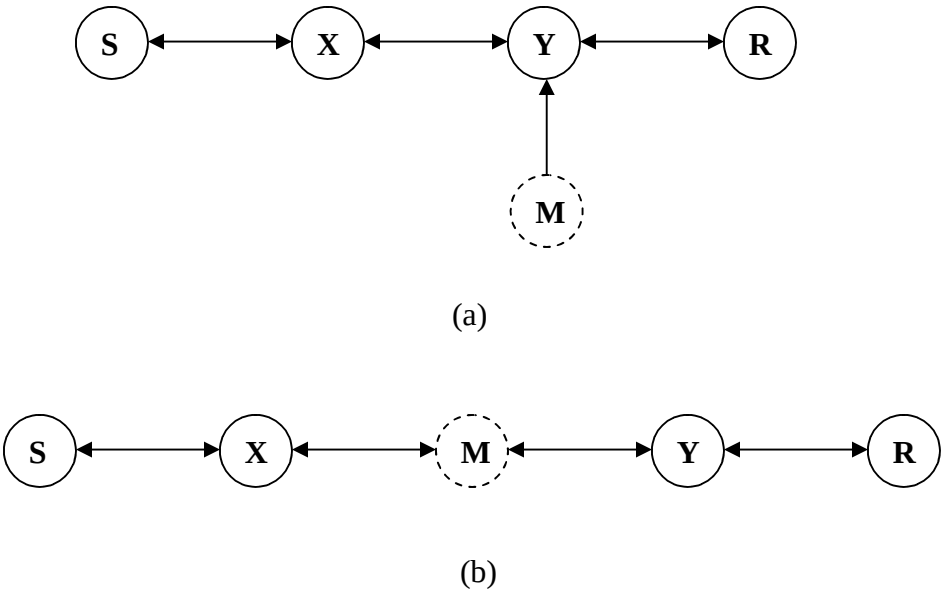

Figure 6.1: Routing attack

Network layer vulnerabilities fall into two categories: routing attacks and packet forwarding attacks [16]. The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocols. The specific attack behaviors are related to the routing protocol used by the MANET.

6.2.1 Routing Table Overflow Attack

This attack is basically happens to proactive routing algorithms, which update routing information periodically. To launch routing table overflow attack, the attacker tries to create routes to nonexistent nodes to the authorized nodes present in the network. He/she can simply send excessive route advertisements to overflow the target system's routing table. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.

6.2.2 Routing Cache Poisoning Attack

Routing cache poisoning attack uses the advantage of the promiscuous mode of routing table updating. This occurs when information stored in routing tables is either deleted, altered or injected with false information. Suppose a malicious node ***M*** wants to poison routes node to ***X***. ***M*** could broadcast spoofed packets with source route to ***X*** via ***M*** itself, thus neighboring nodes that overhear the packet may add the route to their route caches [15].

6.2.3 Attacks on Particular Routing Protocol

There are many attacks in MANET that target the particular routing protocols. This is due to developing routing services without considering security issues. Most of the recent research suffers from this problem. In this section, we will describe about the security threats, advantage and disadvantage of some common routing protocols.

6.2.3.1 AODV

The Ad-hoc On-demand Distance Vector (AODV) routing algorithm is a reactive algorithm that routes data across wireless mesh networks. The advantage of AODV is that it is simple, requires less memory and does not create extra traffic for communication along existing links. In AODV, the attacker may advertise a route with a smaller distance metric than the original distance or advertise a routing update with a large sequence number and invalidate all routing updates from other nodes.

6.2.3.2 DSR

Dynamic Source Routing (DSR) protocol is similar to AODV in that it also forms route on-demand. But the main difference is that it uses source routing instead of relying on the routing table at each intermediate node. It also provides functionality so that packets can be forwarded on a hop-by-hop basis. In DSR, it is possible to modify the source route

listed in the RREQ or RREP packets by the attacker. Deleting a node from the list, switching the order or appending a new node into the list is also the potential dangers in DSR.

6.2.3.3 ARAN

Authenticated Routing for Ad-hoc Networks (ARAN) is an on-demand routing protocol that detects and protects against malicious actions carried out by third parties and peers in particular ad-hoc environment [14]. This protocol introduces authentication, message integrity and non-repudiation as a part of a minimal security policy. Though ARAN is designed to enhance ad-hoc security, still it is immune to rushing attack (described in section 6.2.4.4).

6.2.3.4 ARIADNE

ARIADNE is an on-demand secure ad-hoc routing protocol based on DSR that implements highly efficient symmetric cryptography. It provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two communicating parties. Although ARIADNE is free from a flood of RREQ packets and cache poisoning attack, but it is immune to the wormhole attack and rushing attack.

6.2.3.5 SEAD

Specifically, SEAD builds on the DSDV-SQ version of the DSDV (Destination Sequenced Distance Vector) protocol. It deals with attackers that modify routing information and also with replay attacks and makes use of one-way hash chains rather than implementing expensive asymmetric cryptography operations. Two different approaches are used for message authentication to prevent the attackers. SEAD does not cope with wormhole attacks.

6.2.4 Other Advanced Attacks

In recent researches, more sophisticated and subtle attacks have been identified in MANET. Some protocols also enhanced their services and some other routing protocols are proposed to overcome the attacks. Still it is an area of interest for the security personal. However, the blackhole (or sinkhole), Byzantine, wormhole, rushing attacks are the typical examples which are described below in detail.

6.2.4.1 Wormhole Attack

Wormhole attack is also known as tunneling attack. An attacker creates a tunnel and uses encapsulation and decapsulation to make a false route between two malicious nodes. In section 3.4, we have described wormhole attack in detail.

6.2.4.2 Blackhole Attack

The backhole attack is performed in two steps. At first step, the malicious node exploits the mobile ad hoc routing protocol such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting the packets. In second step, the attacker consumes the packets and never forwards. In an advanced form, the attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected. In this way, the attacker falsified the neighboring nodes that monitor the ongoing packets. In *fig. 6.2*, node 1 wants to send data packets to node 4 and initiates the route discovery process. We assume that node 3 is a malicious node and it claims that it has route to the destination whenever it receives RREQ packets, and immediately sends the response to node 1. If the response from the node 3 reaches first to node 1 then node 1 thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 3. As a result, all packets through the malicious node is consumed or lost [2].

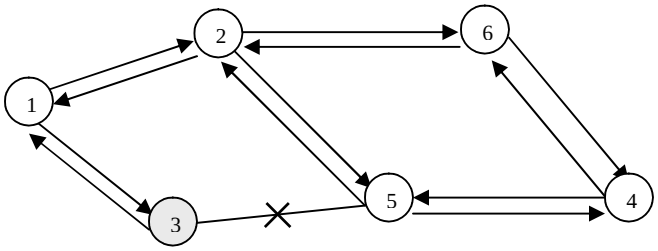

Figure 6.2: The black-hole problem

6.2.4.3 Byzantine Attack

Byzantine attack can be launched by a single malicious node or a group of nodes that work in cooperation. A compromised intermediate node works alone or set of compromised intermediate nodes works in collusion to form attacks. The compromised nodes may create routing loops, forwarding packets in a long route instead of optimal one, even may drop packets. This attack degrades the routing performance and also disrupts the routing services.

6.2.4.4 Rushing Attack

In wormhole attack, two colluded attackers form a tunnel to falsify the original route. If luckily the transmission path is fast enough (e.g. a dedicated channel) then the tunneled packets can propagate faster than those through a normal multi-hop route, and result in the rushing attack. Basically, it is another form of denial of service (DoS) attack that can be launched against all currently proposed on-demand MANET routing protocols such as ARAN and Ariadne [5].

6.2.4.5 Resource Consumption Attack

Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary [2]. The target of resource consumption attack is to send request of excessive route discovery or unnecessary

packets to the victim node in order to consume the battery life. An attacker or compromised node thus can disrupt the normal functionalities of the MANET. This attack is also known as sleep deprivation attack.

6.2.4.6 Location Disclosure Attack

Location disclosure attack is a part of the information disclosure attack. The malicious node leaks information regarding the location or the structure of the network and uses the information for further attack. It gathers the node location information such as a route map and knows which nodes are situated on the target route. Traffic analysis is one of the unsolved security attacks against MANETs.

6.3 Summary

The network layer of the MANET is more immune to attack than all other layers. A good secure routing algorithm can prevent the exploits presented in this chapter. There is no unique algorithm that can prevent all the vulnerabilities. They should be used in cooperation with each other.

Chapter Seven

Security Threats in Transport Layer

The security issues related to transport layer are authentication, securing end-to-end communications through data encryption, handling delays, packet loss and so on. The transport layer protocols in MANET provides end-to-end connection, reliable packet delivery, flow control, congestion control and clearing of end-to-end connection. Like TCP protocol in the Internet model, the nodes in a MANET are also vulnerable to the SYN flooding and session hijacking attacks. In the next sections, threats in transport layer are discussed in detail.

7.1 SYN Flooding Attack

The SYN flooding attack is also DoS attack which is performed by creating a large number of half-opened TCP connections with a target node. TCP connection between two communicating parties is established through completing three way handshakes which is described in the *fig. 7.1*. The sender sends a SYN message to the receiver with a

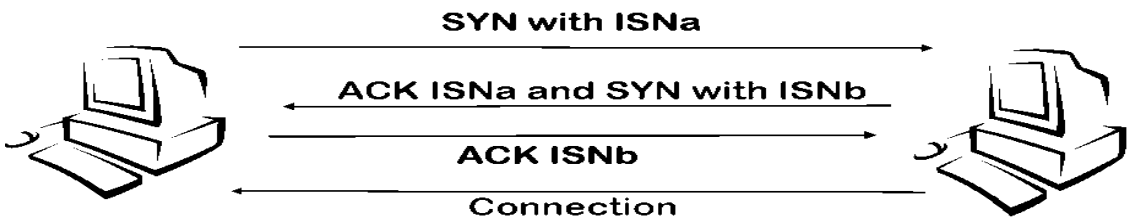

Figure 7.1: TCP Three Way Handshake

randomly generated ISN (Initial Sequence Number). The receiver also generates another ISN and sends a SYN message including the ISN as an acknowledgement of the received SYN message. The sender sends acknowledgement to the receiver. In this way the connection is established between two communicating parties using TCP three way handshakes.

During SYN flooding attack, a malicious node sends a large amount of SYN packets to the target node, spoofing the return address of the SYN packets. When the target machine receives the SYN packets, it sends out SYN-ACK packets to the sender and waits for response i.e. ACK packet. The victim node stores all the SYN packets in a fixed-size table as it waits for the acknowledgement of the three-way handshake. These pending connection requests could overflow the buffer and may make the system unavailable for long time.

7.2 Session Hijacking

Session hijacking is a critical error and gives a malicious node the opportunity of behaving as a legitimate system. All the communications are authenticated only at the beginning of session setup. The attacker may take the advantage of this and commit session hijacking attack. At first, he/she spoofs the IP address of target machine and determines the correct sequence number. After that he performs a DoS attack on the victim. As a result, the target system becomes unavailable for some time. The attacker now continues the session with the other system as a legitimate system.

7.3 TCP ACK Storm

TCP ACK storm is very simple. But to perform the attack, the attacker launches a TCP session hijacking attack at the beginning. After that the attacker sends injected session data as depicted in the *fig. 7.2* and node ***A*** acknowledges the received data with an ACK packet to node ***B***. Node ***B*** is confused as the packet contains an unexpected sequence

number and it tries to resynchronize the TCP session with node ***A*** by sending an ACK packet that contains the intended sequence number. But the steps are followed again and again and results in TCP ACK storm [15].

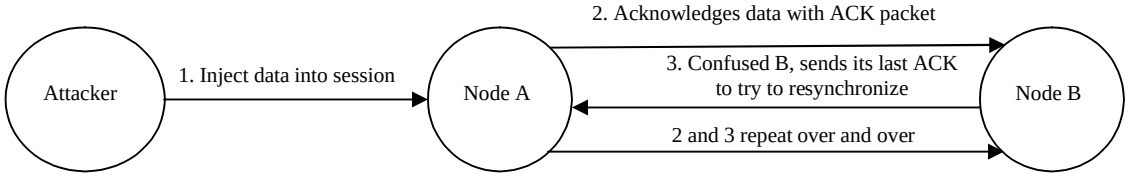

Figure 7.2: TCP ACK Storm

7.4 Summary

MANET has a higher channel error rate when compared to wired network. This is due to TCP does not have any mechanism to distinguish the cause of loss i.e. whether it is done by congestion, random error or malicious attacks. On the other hand, UDP is also immune to session hijacking. It is same over UDP as over TCP, except that the attackers need not to be worried about the overhead of managing sequence numbers and other TCP mechanisms since UDP is connectionless protocol.

Chapter Eight

Security Threats in Application Layer

Applications need to be designed to handle frequent disconnection and reconnection with peer applications as well as widely varying delay and packet loss characteristics [13]. Like other layers application layer also vulnerable and attractive layer for the attacker to attack. Because this layer contains user data that supports many protocols such as SMTP, HTTP, TELNET and FTP which have many vulnerabilities and access points for attackers. The main attacks in application layer are malicious code attacks and repudiation attacks.

8.1 Malicious Code Attacks

Various malicious codes such as virus, worm, spy-wares and Trojan horse attack both operating systems and user applications that cause the computer system and network to slow down or even damaged. An attacker can produce this type of attacks in MANET and can seek their desire information [15].

8.2 Repudiation Attacks

The solution that taken to solve authentication or non-repudiation attacks in network layer or in transport layer is not enough. Because, repudiation refers to a denial of participation in the communication. Example of repudiation attack on a commercial system: a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction [15].

8.3 Summary

Another fundamental problem in MANET is end-to-end security. Heterogeneous network may suffer from various security threats that may increase packet delivery latency, increase packet loss rate and so on. The main security issues involved in application layers are detecting and preventing viruses, worms, malicious codes and application abuses.

Chapter Nine

Countermeasures

Security is a primary concern in MANET in order to provide protected communication between the communicating parties. It is essential for basic network functions like routing and packet forwarding. Network operation can easily be jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design [11]. Hence, a variety of security mechanisms have been developed to counter malicious attacks. There are two mechanisms which are widely used to protect the MANET from the attackers.

- **Preventive mechanism:** In preventive mechanism, the conventional approaches such as authentication, access control, encryption and digital signature are used to provide first line of defense. Some security modules, such as tokens or smart card that is accessible through PIN, passphrases or biometrics verification are also used in addition.

- **Reactive mechanism:** Reactive mechanism uses the schemes like intrusion detection system (IDS), cooperation enforcement mechanisms etc. in MANET. Intrusion detection systems are used to detect misuse and anomalies. Cooperation enforcement such as Nuglets, Confidant, CORE and Token-based reduce selfish node behavior.

9.1 Countermeasures on Physical Layer Attacks

The physical layer of MANET is immune to signal jamming, DoS attack and also some passive attacks. Two spread spectrum technologies can be used to make it difficult to detect or jam signals. Spread spectrum technology changes frequency in a random fashion or spreads it to a wider spectrum which makes the capture of signal difficult. The FHSS (Frequency Hopping Spread Spectrum) makes the signal unintelligible duration impulse noise to the eavesdroppers. On the other hand, DSSS (Direct Sequence Spread Spectrum) represents each data bit in the original signal by multiple bits in the transmitted signal through 11-bit Barker code. However, both FHSS and DSSS pose difficulties for the malicious user while trying to intercept the radio signals. To capture and release the content of transmitted signal, the attacker must know frequency band, spreading code and modulation techniques. Still, there is a problem. These mechanisms are secure only when the hopping pattern or spreading code is unknown to the eavesdropper [15].

9.2 Countermeasures on Link Layer Attacks

The security issues that are closely related to link layer are protecting the wireless MAC protocol and providing link-layer security support. One of the vulnerabilities in link layer is its binary exponential backoff scheme which we described in fifth chapter 5.4 section. But recently a security extension to 802.11 proposed in [10]. The original 802.11 backoff scheme is slightly modified in that the backoff timer at the sender is provided by the receiver in stead of setting an arbitrary timer value on its own. As mentioned earlier, the threats of resource consumption (using NAV field) is still an open challenge though some schemes have been proposed such as ERA-802.11[12]. Finally, the common known security fault in link layer is the weakness of WEP. Fortunately, the 802.11i/WPA [7] has mended all obvious loopholes in WEP and future countermeasures such as RSN/AES-CCMP are also being developed to improve the strength of wireless security.

9.3 Countermeasures on Network Layer Attacks

Network layer is more vulnerable to attacks than all other layers in MANET. A variety of security threats is imposed in this layer. Use of secure routing protocols provides the first line of defense. The active attack like modification of routing messages can be prevented through source authentication and message integrity mechanism. For example, digital signature, message authentication code (MAC), hashed MAC (HMAC), one-way HMAC key chain is used for this purpose. By an unalterable and independent physical metric such as time delay or geographical location can be used to detect wormhole attack. For example, packet leashes are used to combat this attack [6]. IPSec is most commonly used on the network layer in internet that could be used in MANET to provide certain level of confidentiality. The secure routing protocol named ARAN protects from various attacks like modification of sequence number, modification of hop counts, modification of source routes, spoofing, fabrication of source route etc [14]. The research by Deng [2], et al presents a solution to overcome blackhole attack. The solution is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node.

9.4 Countermeasures on Transport Layer Attacks

One way to provide message confidentiality in transport layer is point-to-point or end-to-end communication through data encryption. Though TCP is the main connection-oriented reliable protocol in Internet, it does not fit well in MANET. TCP feedback (TCP-F) [4], TCP explicit failure notification (TCP-ELFN) [4], ad-hoc transmission control protocol (ATCP) [4], and ad hoc transport protocol (ATP) have been developed but none of them covers security issues involved in MANET. Secure Socket Layer (SSL) [9], Transport Layer Security (TLS) [9] and Private Communications Transport (PCT) [9] protocols were designed on the basis of public key cryptography to provide secure communications. TLS/SSL provides protection against masquerade attacks, man-in-middle attacks, rollback attacks, and replay attacks.

9.5 Countermeasures on Application Layer Attacks

Viruses, worms, spywares, trozan horses are the common and challenging application layer attacks in any network. Firewall provides protection against some of these attacks. For example, it can provide access control, user authentication, incoming and outgoing packet filtering, network filtering, accounting service etc. Anti-spyware software can detect spyware and malicious programs running on the system. Still using firewall is not enough because in certain situation the attacker even can penetrate firewall and make an attack. Another mechanism, Intrusion Detection System (IDS) is effective to prevent certain attacks such as trying to gain unauthorized access to a service, pretending like a legitimate user etc. The application layer also detects a DoS attack more quickly than the lower layers.

9.6 Summary

In this chapter we described the countermeasures of the attacks imposed in different layers. Still, there are some attacks such as man-in-middle attack which is known as a multi-layer attack. The countermeasures for this type of attack need to be implemented at different layers. For example, directional antennas [1] are used at the media access layer to defend against wormhole attacks while packet leashes [6] are used for network layer defense.

Chapter Ten

Conclusion

Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of MANET. In this thesis, we have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. The first research question is 'what are the vulnerabilities and security threats in MANET? Which level is most vulnerable to attack?' In our study, we present a variety of attacks (chapter 4-8) related to different layers and find that network layer (chapter 6) is most vulnerable than all other layers in MANET. This isolation of attacks on the basis of different layers makes easy to understand about the security attacks in ad hoc networks. 'How the security services like confidentiality, integrity and authentication can be achieved from mobile ad hoc networks? What steps should be taken?' is the second research question. The answer is that security services can be achieved through following the preventive and reactive countermeasures on the basis of particular attack. The third question is 'what are the countermeasures? How the security of the entire system is ensured?' We focus on the potential countermeasures (chapter 9) either currently used in wired or wireless networking or newly designed specifically for MANET in our study. In addition, we can say that security must be ensured for the entire system since a single weak point may give the attacker the opportunity to gain the access of the system and perform malicious tasks. The final research question is 'what are the potential dangers that may be crucial in future?' Everyday, the attackers are trying to find out the new vulnerability in MANET. Some of those upcoming dangers are described in the next

section but it is sure that the multi-layer or combined attacks will be vital for secure communication in MANET.

10.1 Future Directions

Significant research in MANET has been ongoing for many years, but still in an early stage. Existing solutions are well-suited only for specific attack. They can cope well with known attacks but there are many unanticipated or combined attacks remaining undiscovered. Resource consumption DoS attack is still unclear to the researchers. More research is needed on secure routing protocol, robust key management, trust based systems, integrated approaches to routing security, data security in different level and cooperation enforcement. Existing routing protocols are subject to a variety of attacks that can allow attackers to influence a victim's selection of routes or enable denial-of-service attack. So, necessity of secure routing protocol is inevitable. Cryptography is one of the most common security mechanisms and its strength relies on the secure key management. The public cryptography scheme depends upon centralized CA (Certificate Authority) which is known as a security weak point in MANET. Symmetric cryptography is efficient but suffers from potential attack on key distribution. Hence, efficient key agreement and distribution in MANET is an ongoing research area. Finally, Building a sound trust-based system and integrating it to the current preventive approaches, solution of the node selfishness problem can be considered in future research. Identifying new security threats as well as new countermeasures demands more research in MANET.

References

[1] S. Capkun, L. Buttyan, and J. Hubaux, *"Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks,"* 2003.

[2] H. Deng, W. Li, Agrawal, D.P., *"Routing security in wireless ad hoc networks,"* Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

[3] J.-P. HuBaux, L. Buttyan, and S. Capkun., *"The quest for security immobile ad hoc network,"* In Proc. ACM MOBICOM, Oct. 2001.

[4] H. Hsieh and R. Sivakumar, *"Transport OverWireless Networks,"* Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenovic. John Wiley and Sons, Inc., 2002.

[5] Y. Hu, A. Perrig, and D. Johnson, *"Ariadne: A Secure On-Demand Routing for Ad Hoc Networks,"* Proc. of MobiCom 2002, Atlanta, 2002.

[6] Y. Hu, A. Perrig, and D. Johnson, *"Packet Leashes: A Defense AgainstWormhole Attacks inWireless Ad Hoc Networks,"* Proc. of IEEE INFORCOM, 2002.

[7] IEEE Std. 802.11i/D30, *"Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security,"* 2002.

[8] J. Kong et al., *"Providing robust and ubiquitous security support for mobile ad-hoc networks,"* In Proc. IEEE ICNP, pages 251–260, 2001.

[9] C. Kaufman, R. Perlman, and M. Speciner, *"Network Security Private Communication in a Public World,"* Prentice Hall PTR, A division of Pearson Education, Inc., 2002

[10] P. Kyasanur, and N. Vaidya, *"Detection and Handling of MAC Layer Misbehavior in Wireless Networks,"* DCC, 2003.

[11] P. Michiardi, R. Molva, *"Ad hoc networks security,"* IEEE Press Wiley, New York, 2003.

[12] A. Perrig, R. Canetti, J. Tygar, and D. Song, "*The TESLA Broadcast Authentication Protocol*," Internet Draft, 2000.

[13] R. Ramanathan, J. Redi and BBN Technologies, *"A brief overview of ad hoc networks: challenges and directions,"* IEEE Communication Magazine, May 2002, Volume: 40, page(s): 20-22, ISSN: 0163-6804

[14]K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, *"Secure routing protocol for ad hoc networks,"* In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. 12-15 Nov. 2002, Page(s): 78- 87, ISSN: 1092-1648

[15] B. Wu, J. Chen, J. Wu, M. Cardei, *"A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,"* Department of Computer Science and Engineering, Florida Atlantic University, http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[16] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, *"Security in mobile ad hoc networks: challenges and solutions,"* In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s): 38- 47, ISSN: 1536-1284

[17] S. Yi, P. Naldurg, and R. Kravets, "*Security-aware ad hoc routing for wireless networks,"* In Proc. ACM Mobihoc, 2001.

[18] L. Zhou, Z.J. Haas, Cornell Univ., "*Securing ad hoc networks,"* IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044