Protocol Stack based Security Vulnerabilities in MANETs

Jatinder Pal Singh
Research Scholar
RIMT-IET, PUNJAB

Anuj Kr. Gupta
Head of Department, CSE
RIMT-IET, PUNJAB

ABSTRACT

Mobile Ad-hoc network is a temporary network of mobile nodes where mobile nodes communicate with each other through wireless links with no fixed infrastructure & no centralized control. Each mobile node in such a scenario acts as both a router & host. Nodes within each other's radio range communicate directly, while those other nodes that are far apart used as relays. Thus the nodes find a path to the destination node using routing protocols. Minimal configuration & quick deployment make them suitable for emergency situations like war, emergency medical situations etc. Since Mobile Ad-hoc networks lack an infrastructure, they are exposed to a lot of vulnerabilities. In this paper, we present a survey on the protocol stack based security vulnerabilities in MANETs. All these vulnerabilities attempt to affect the overall performance and throughput of the network. The intent of this paper is to classify and explain the security vulnerabilities in the MANET protocol stack.

General Terms

MANETs, MANET Attacks

Keywords

MANETs, DoS, Ad-hoc, Security

1. INTRODUCTION

Wireless networks are usually classified into two broad categories: Infrastructure based network[4] and Infrastructure less network[4]. An Infrastructure-based network is a network that uses fixed infrastructure like access points/gateway to get connected to a new network like Internet or Intranet. For example: Wi-Fi set up in a college where students connect to internet using access points. On the other hand Infrastructure less (ad hoc) network is a network in which mobile nodes communicate with each other through wireless links. For example two laptops with wireless adapter cards can set up an Ad-hoc network. Such an infrastructure less network is also known as MANET, where a temporary network is set up without the aid of any fixed infrastructure or centralized administration. Such a network is developed in 'Ad-hoc' basis without any pre-existing infrastructure & may operate in either stand alone fashion or connected to the Internet.

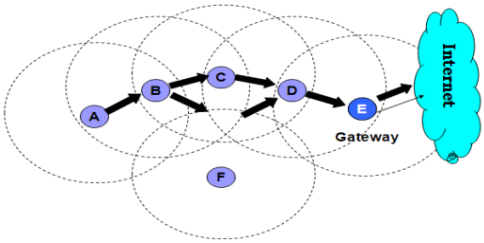

Figure 1: A typical MANET Scenario

1.1 Application of MANETs

Quick and easy deployment makes MANETs useful in wide number of applications some of which are listed below

- Military applications
- Emergency rescue
- Wireless sensor networks

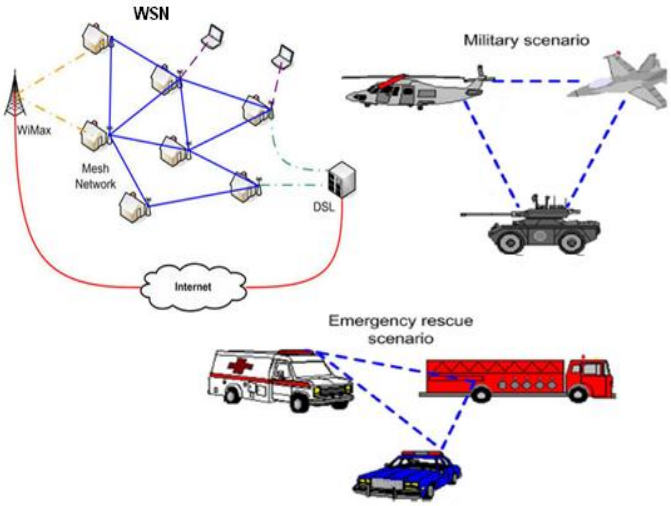

Figure 2: Applications of MANETs

1.2 Merits of MANETs

- No pre-existing infrastructure is required
- Easy to set up at any place.
- Provide access to information and services regardless of geographic position [16].

1.3 Demerits of MANETs

- No authorization facility
- No Physical Security [15].
- Limited resources.
- Time varying topology; changing network topology makes it hard to detect malicious nodes.
- Security protocols for wired network cannot work for MANETs.

The rest of this paper is organized as follows: Next section discusses about the classification of security vulnerabilities[2,5]

as Active/Passive attacks & Internal/External attacks. Section 3, classifies and explain the vulnerabilities according to the MANET Protocol stack. Section 4 discusses the required countermeasures. Section 5 summarizes the paper. Section 6 gives the conclusion and directions for future work.

2. CLASSIFICATION OF SECURITY VULNERABILITIES

Due to lack of security in MANETs and its operation, they are exposed to different kind of security vulnerabilities. Such vulnerabilities in MANET can roughly be classified into two major categories, on the basis of emission and location namely Active/Passive and External/Internal as shown in the Figure below

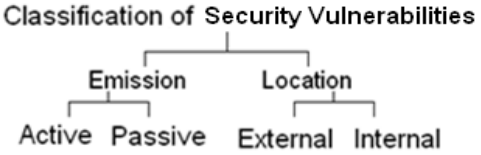

Figure 3: Classification of Vulnerabilities

On the basis of emission, security vulnerabilities can be classified as: Active and Passive Attacks[1, 2].

Active attack: Those attacks which attempt to alter, inject, delete or destroy the data being exchanged in the network. Intention of such an attack is to damage the network or disrupt the network operations. Example: Fabrication or masquerading attacks[1,2], message modifications, message replays and DOS attacks. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks.

Passive attack: Those attacks which attempt to learn or make use of information but do not affect the system resources. Such an attack has no intention to damage the network & network operations because it does not modify the contents of the packets. Example: Eavesdropping, Release of message contents and Traffic analysis. Detection of passive attack[1,2] is very difficult since the operation of the network itself doesn't get affected. This classification on the basis of emission of an attack can further be used to categorize different attacks. Such a classification is mentioned in Table 1 where some of the common attacks are classified as Active or Passive.

On the basis of Location, security vulnerabilities can be of 2 types: Internal and External Attacks[1, 2]

External Attack: Those attacks which are carried out by nodes or group of nodes that do not belong to the network. Such attacks send fake packets in order to interrupt the performance of the network. External attacks try to cause congestion in the network, denial of services [14] and advertising wrong routing information etc [2].

Internal Attack: Those attacks which are carried out by nodes or group of nodes that are actually part of the network. Such attacks are more severe and difficult to detect than external attacks. The wrong routing information generated by compromised nodes or malicious nodes are difficult to identify[6].

Table 1. Classification of Vulnerabilities as Active/Passive attacks

Name of Attack	**Type of Attack (Active or Passive)**
Worm hole, Denial of Service, Black hole, Interference & Jamming, Malicious code, Session hijacking, Impersonation, Routing attacks, DOS	Active Attacks
Eavesdropping, monitoring, Snooping, Selfish misbehavior, traffic analysis.	Passive Attacks

3. PROTOCOL STACK BASED SECURITY VULNERABILITIES

Since attacks on MANETs can come from all directions and target at any node such a nature of MANETs makes them vulnerable to different kind of attacks. According to the layer where they attack we can classify them as layer based attacks. Such protocol stack based security vulnerabilities are mentioned in Table 2 below.

Table 2. Protocol Stack Based Security Vulnerabilities

TCP/IP PROTOCOL STACK	**MANET PROTOCOL STACK**	**SECURITY VULNERABILITIES IN MANET**
Application	Application	Repudiation & Malicious code attacks.
Transport	Transport	Session Hijacking & SYN Flooding attack
Network	Network and Ad-Hoc Routing	Routing, Blackhole, Rushing, Wormhole, Sinkhole, Sybil & Link spoofing attack.
Data Link	Data Link	Selfish misbehavior, Malicious misbehavior & Traffic Analysis
Physical	Physical	Eavesdropping, Jamming & Interference

From the above table we can clearly differentiate between the layers of TCP/IP and MANET, only difference is that in MANET ad-hoc routing is performed at the network layer. For the rest of the section, we have discussed the security vulnerabilities at different layers following the order of the protocol stack. Physical layer vulnerabilities are discussed in Section 3.1, followed by link layer vulnerabilities in Section 3.2; and network layer vulnerabilities in Section 3.3. Transport layer vulnerabilities are discussed in Section 3.4, Application layer vulnerabilities are discussed in Section 3.5.

3.1 Security Vulnerabilities at Physical Layer

The attacks on the physical layer require help from the hardware sources to come into effect, as shown in the below figure, Eve is using the HUB to eavesdrop data communication between Alice and Bob. Examples: eavesdropping, interference, & jamming etc.

3.1.1 Eavesdropping

Secretly listen to a conversation or process of gathering information from a network by snooping[7] on transmitted data is known as Eavesdropping. As show in the below figure, data communication between Alice & Bob is taking place with the help of a Hub, which is being used by Eve to hear/gather the transmitted data. Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information.

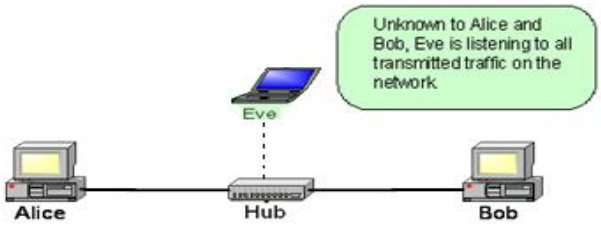

Figure 4: Eavesdropping

3.1.2 Jamming and Active Interference

It's a special type of DOS[14] attack in which a radio signal can be jammed or interfered, which causes the message to be corrupted or lost. In this form of attack, the attacker initially keeps monitoring the wireless medium in order to determine the frequency at which the destination node is receiving signals from the sender. The attacker then transmits signals using the same frequency to send data to the receiver thereby disrupting communications. Frequency hopping is used to overcome jamming.

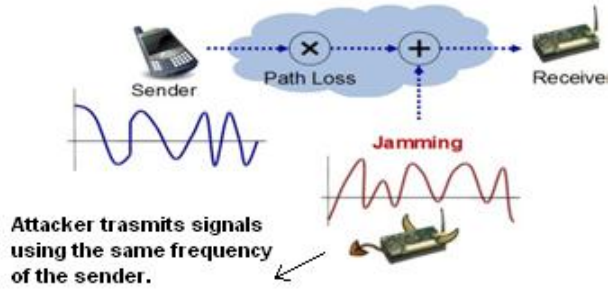

Figure 5: Jamming & Active Interference

3.2 Security Vulnerabilities at Data link layer

The MANET one-hop connectivity among neighbors is maintained by the link layer protocols[17,18], and the network layer protocols extend the connectivity to other nodes in the network. Security Vulnerabilities may target the link layer by disrupting the cooperation of the layer's protocols. The effects can be measured in terms of route discovery failure, energy consumption, link breakage initiating route discovery and so on. The misbehavior of a node can be purely in selfish interest or with malicious intents.

3.2.1 Selfish Misbehavior of Nodes

Attacks under this category concerns with the performance of nodes and do not interfere with the operation of the network. Selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve its resources like conservation of battery power. Dropping attacks[11] can lead to congestion and can prevent end-to-end communications between nodes, if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted,

3.2.2 Malicious Behavior of nodes

Malicious node attacks aims at disrupting the normal operation of network. A malicious node advertises wrong routing information in order to get secure data before the actual route. These nodes receive information that was intended for some other node. A malicious node may advertise fake route request[10], so that other nodes will then direct route replies to the node.

3.2.3 Traffic Analysis

By analyzing the traffic an attacker can reveal some information about the network such as the existence and location of nodes[12], the communications network topology, the roles played by nodes and the like. Then he can use this information to carry out further attacks. Traffic analysis in ad hoc networks may reveal:

- Location of nodes
- Network topology
- Roles played by nodes
- Current sources and destination of communications
- Confidential information about network topology can be derived by analyzing traffic patterns.

3.3 Security Vulnerabilities at Network Layer

The network layer protocols enable the nodes to be connected with another through hop-by-hop [4]. Every individual node in MANETs takes routing decision whether to forward the packet, so it's very easy for malicious node to attack on such a setup. The basic idea behind network layer security vulnerabilities is to inject itself in the active path from source to destination or to absorb network traffic. Some of the most common security vulnerabilities found at this layer are: Routing attack, Black hole attack, Rushing attack, Worm hole attack, Sink hole attack, Link Spoofing attack and Sybil attack.

3.3.1 Routing Attack

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, a malicious node M can inject itself into the routing[11] path between sender S & receiver D. Node M can also divert the data packets exchanged between S and D, which results in significant end to end delay between S and D. The malicious node can disrupt the route discovery process by creating routing loops and overflow routing tables. A special case of Routing Attack is: Routing Table Overflow attack, in which the goal is to create enough routes to prevent new routes from being created.

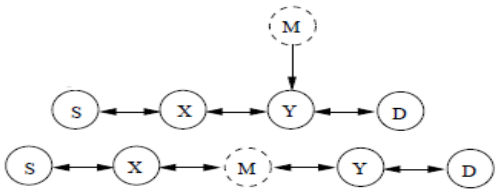

Figure 6: Routing Attack

3.3.2 Black hole Attack

Meaning of black hole is to swallow all the objects. In case of MANETs the malicious node[12] which carries out this attack absorbs all the data. In black hole attack a malicious node falsely replies for route requests without having an active route to the destination. Since this malicious node immediately replies to the RREQ message from the sender with the highest sequence number to settle in the routing table of the victim, the requesting nodes assume that route discovery process is completed and ignore other RREP messages and keep sending packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes.

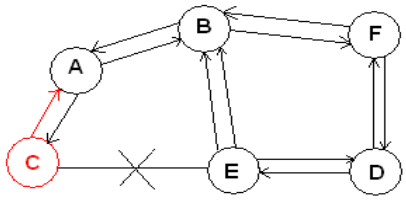

Figure 7: Black Hole Attack

A black hole attack scenario is shown in Figure. 7 where node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the destination by sending a RREP as soon as it receives the RREQ packets. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be consumed or lost.

3.3.3 Rushing Attack

Rushing attacks are mainly against the on-demand routing protocols. This attack is extremely difficult to detect. An attacker on receiving RREQ packet quickly floods the packet throughout the network before other node can react who receive the same RREQ[7, 8]. For example, in figure below the node "4" represents the rushing attack node, where "S" and "D" refers to source and destination nodes. The rushing attack of compromised node "4" quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than do those from other nodes. This result in when neighbouring node of "D" i.e. "7" and "8" when receive the actual (late) route request from source, they simply discard requests. So in the presence of such attacks "S" fails to discover any safe route.

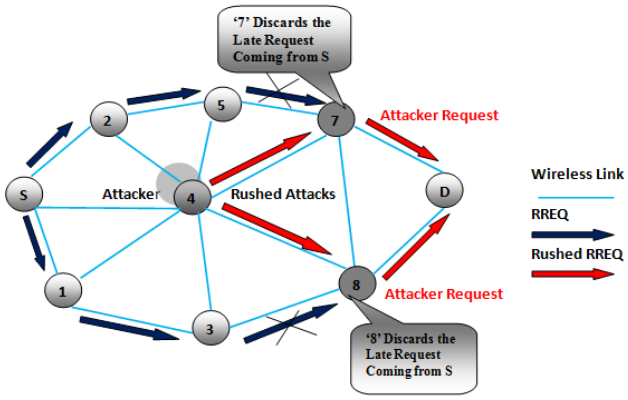

Figure 8: Rushing Attack

3.3.4 Wormhole Attack

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes. For example as shown in figure 9, we assume that nodes A1 and A2 are two colluding attackers[9,10] and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors C and E forward the RREQ as usual. However, node A1, which received the RREQ, forwarded by node C, records and tunnels the RREQ to its partner A2. Then, node A2 rebroadcasts this RREQ to its neighbor H. Since this RREQ passed through a highspeed channel, this RREQ will reach node D first. Therefore, node D will choose route D-H-C-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-H-D that indeed passed through A1 and A2 to send its data.

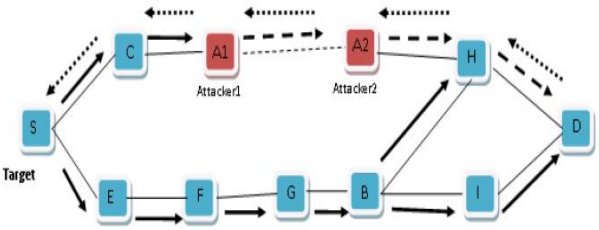

Figure 9: Wormhole Attack

3.3.5 Sinkhole Attack

The attacking node tries to offer a very attractive link: a compromised node tries to attract the data to it from all neighboring nodes. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack. Sinkhole attack in AODV[17,18] protocol attacks the flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate.

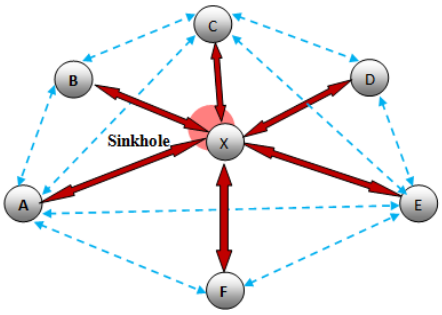

Figure 10: Sinkhole Attack

3.3.6 Link spoofing Attack

In Link spoofing attacks, a malicious node broadcasts or advertises the fake route information[5] to disrupt the routing operation. It results in, malicious node manipulate the data or routing traffic.

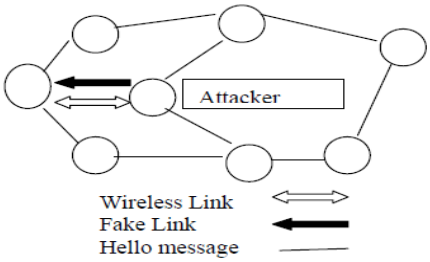

Figure 11: Link Spoofing Attack

3.3.7 Sybil Attack

In this attack, a malicious node produces itself as a large number of nodes instead of single node. Sybil attacker may generate fake identities to represent multiple identities for a malicious node. As shown in the below figure 12, A is connected with B, C and the malicious node, M1. If M1 represents other nodes M2, M3 and M4 (e.g. by using their secret keys) this makes A believe it has 6 neighbors instead of 3).

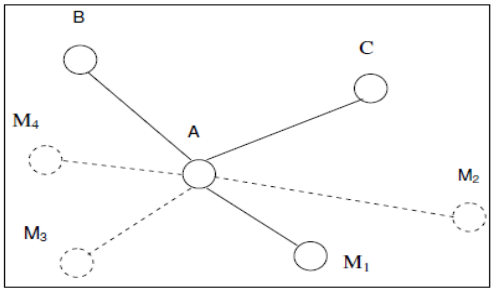

Figure 12: Sybil Attack

3.4 Security Vulnerabilities at Transport Layer

The objectives of TCP-like Transport layer protocols in MANET include setting up of end-to-end connection, end-to-end reliable delivery of packets, flow control, congestion control, clearing of end-to-end connection. Similar to TCP protocols in the Internet, the transport layer in MANET also vulnerable to the SYN flooding attack and session hijacking attack.

3.4.1 Session Hijacking

Session hijacking takes advantage of the fact that most communications are protected at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. E.g. of session hijacking attack [13, 14] is TCP–ACK storm Problem. As shown in the figure below, nodes N1 and N2 have established a TCP connection. An attacker M spoofs the IP address of N2 & injects data into the session of node N1. N1 acknowledges the receipt by sending an ACK packet to node N2. As N2 notices a different sequence number in the received ACK packet from N1, it reissues its last ACK packet to N1 in order to resynchronize. This process repeats over and over, leading to an ACK storm in this way the malicious node impersonates the victim node & continues the session with the target.

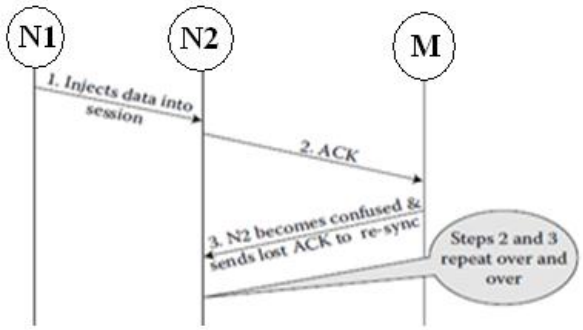

Figure 13: Session Hijacking using TCP-ACK storm

3.4.2 SYN Flooding Attack

The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection. TCP connection between two communicating parties is established through completing three way handshakes [11, 14] which is described in the fig. below. The following are three steps takes place during the three way handshake.

- Step1: Node S sends a SYN packet with a Seq. no P to Node D.
- Step2: Node D transmits to S, a SYN/ACK message, including its own sequence number Q & acknowledgment number P+1.
- Step3: S issues an ACK message (with ack. number Q+1) to D.

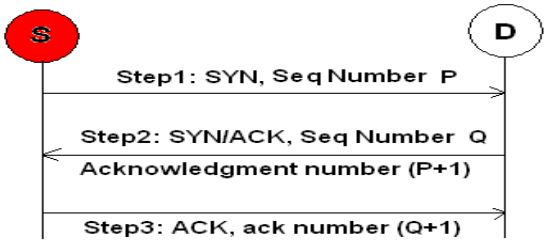

Figure 14: Three-way Handshake Process

In case of SYN flooding attack, Node S initiates a large number

of TCP connections with the victim node D. Node S spoofs the return address of the SYN packets and does not complete step 3 of these TCP connections. Node D, upon receiving the SYN packet from the attacker, issues immediately the SYN–ACK[3] packets to the spoofed address, which often does not exist. D awaits reception of ACK packets (in step 3). A large number of these half-opened connections may overflow the buffer maintained by D. Such a buffer overflow results in "D" not being able to accept any other connection request.

3.5 Security Vulnerabilities at Application Layer

End user applications are accessed by the users with the help of this layer. This end user application needs to be connected with storage devices and applications. Since storage devices are prone to many viruses so security vulnerabilities at this layer are mobile viruses, worm attacks, and repudiation attacks.

3.5.1 Malicious code attacks

Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application. These malicious programs usually can spread themselves through the network and cause the computer system and networks to slow down. Firewall is an effective way to prevent various attacks as well as we Intrusion Detection System[8] to prevent gaining an unauthorized access to a service.

3.5.2 Repudiation attacks

Repudiation refers to a denial of participation[6] in all or part of the communications. Application layer firewalls may take into account in order to provide security. Example of repudiation attack on a commercial system like Flipkart.com online shopping: a person could deny conducting an operation on a credit card purchase or deny any on-line transaction, which is a repudiation attack.

4. COUNTERMEASURES

A variety of security mechanisms have been developed to overcome and avoid these layer based security vulnerabilities. Some of the most common countermeasures[7,8] which we can take into consideration while implementing an Ad-hoc network to avoid these security vulnerabilities are listed in the below Table 3.

Table 3. Countermeasures

Name of the Layer	**Countermeasures**
Application Layer	Firewalls, IDS etc
Transport Layer	Authentication and securing end-to-end or point-to-point communication, use of public key cryptography.
Network Layer	Source authentication and message authentication code (MAC), hashed MAC (HMAC), one-way HMAC Securing routing protocols to overcome impersonation attacks.
Data Link Layer	No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP, WPA
Physical Layer	Using FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum).

5. SUMMARY

Compared to wired networks, MANETs[4] are easy to set up at any place but they are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Classification of these attacks is firstly done on the basis of Emission (Active or Passive) and Location (External or Internal). All the layers in protocol stack suffers from different security vulnerabilities out of which Routing and Rushing attacks at the Network layer are the most vulnerable. Security vulnerabilities discussed above can also be categorized as shown below

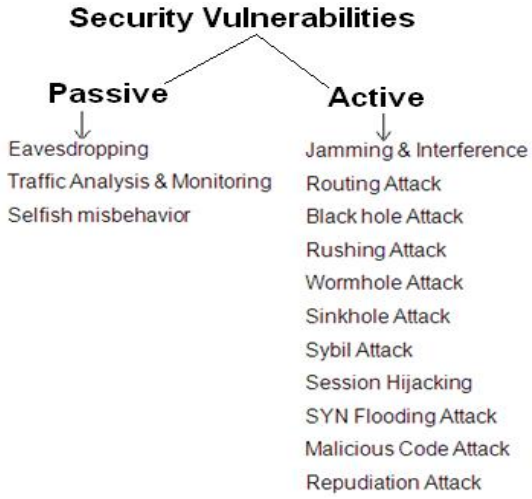

Figure 15: Classification of Security Vulnerabilities

6. CONCLUSION AND FUTURE SCOPE

The field of mobile ad hoc networks is changing and growing rapidly because of its easy and quick deployment. Since it has vast number of applications in different fields, protecting MANETs from different kind of security vulnerabilities should be the key concern. In this paper we have discussed the security vulnerabilities with their countermeasures[7,8]. During the survey, we find that we need a security solution which can handle multiple attacks at a time and most important such solution should be applicable to all type of Table-Driven and On-Demand Routing protocols. Therefore, our aim is to develop secure routing protocols and trust based systems to avoid these security vulnerabilities to disrupt the mobile ad-hoc network operations.

7. ACKNOWLEDGMENTS

I express my sincere gratitude to my guide Mr Anuj Kumar Gupta, for his valuable guidance and advice. Also I would like to thanks all the faculty members and colleagues for their continuous support and encouragement.

8. REFERENCES

[1] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey".

[2] Amitabh Mishra, "SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS" (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook.

[3] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey".

[4] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks".

[5] Kamanshis Biswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network".

[6] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.

[7] Monika, Mukesh Kumar & Rahul Rishi, "Security Aspects in Mobile Ad Hoc Network(MANETs): Technical Review" International Journal of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010.

[8] 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.

[9] N.Shanthi, Dr.Lganesan and Dr.K.Ramar , "Study of Different Attacks on Multicast Mobile Ad hoc Network," Journal of Theoretical and Applied Information Technology.

[10] Hoang Lan and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks", Proceedings of ICNICONSMCL'06, 0-7695-2552-0/06@ 2006 IEEE.

[11] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, Octomber 2002.

[12] Sonja Buchegger and Jean-Yves Le Boudec, "Cooperative Routing in Mobile Ad hoc Networks: Current Efforts Against Malice and Selfishness",In Lecture Notes on Informatics, Mobile Internet Workshop, Germany, Octomber 2002.Springer.

[13] Ping Yi, Yue Wu and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[14] I. Aad and J.P. Hubaux, E.W. Knightly, "Denial of Service Resilience in Ad hoc Networks", Proceedings of ACM MobiCom 2004, Philadelphia, PA, Sep. 2004, pp. 202-215.

[15] W. Lou, W. Liu, Y. Fang: SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks, IEEE INFOCOM, 2004.

[16] T. Bheemarjuna Reddy, I. Karthigeyan, B.S. Manoj, C. SivaRam Murthy."Quality Of Service Provisioning In Ad Hoc Wireless Networks: A Survey of Issues And Solutions. AdHoc Networks", Ad Hoc NetworksVol.4, pp. 83–124.

[17] Anuj K. Gupta, Harsh Sadawarti, & Anil k. Verma, (2011) "Review of various Routing Protocols for MANETs," International Journal of Information and Electrical Engineering, ISSN: 1109-2742, Vol. 1 No. 3, pp. – 251-259.

[18] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma "A Review of Routing Protocols for Mobile Ad Hoc Networks" WSEAS Transactions on Communications, ISSN: 1109-2742, Volume 10 Issue11.