# Threat in Mobile Ad hoc Network (MANET)

Nilesh M. Kadivar

*Dept. of Computer science & Engineering*
*B.H. Gardi College of Engineering & Technology, Rajkot, Gujarat, India*

## 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. 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.***

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

## I. 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 multi hop paths through the network to any other node. This idea of Mobile ad hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly [2].

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 [12]. 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.

## II- Security Attacks on each layer in MANET[11]

| **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 |

**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

**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

**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 favours 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 neighbours to back off 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 back off scheme, like TCP window management

Threats in IEEE 802.11 WEP

1) 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.

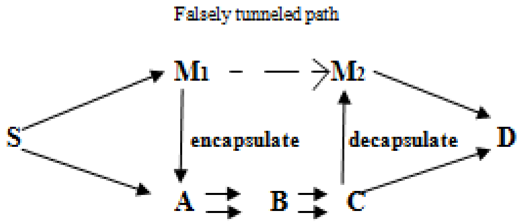
2) The initialization vector (IV) used in WEP is a 24-bit field which is sent in clear and is a part of the RC4 leads to probabilistic cipher key recovery attack or most commonly known as analytical attack.

3)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.

**Wormhole Attack**

Wormhole attack is also known as tunnelling attack. An attacker creates a tunnel and uses

Encapsulation and decapsulation to make a false route between two malicious nodes.



**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 neighbouring nodes that monitor the ongoing packets.

In *fig.*,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

**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.

**Resource Consumption Attack**

Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. 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

**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

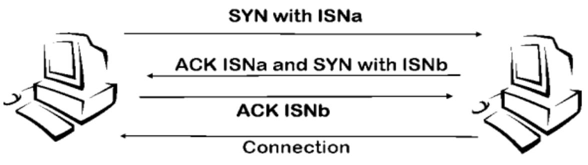
**The SYN flooding attack**

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

this is described in the fig. 7.1. The sender sends a SYN message to the receiver with a 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.

**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

**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

**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

## III-COUNTERMEASURE

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.

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

**2) 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.

| Layers | Solutions |
|---|---|
| Application layer | Cooperation enforcement (Nuglets,Confidant, CORE) mechanisms, Firewalls, IDS etc. |
| Transport layer | Authentication and securing end-to-end or point-to-point communication, use of public cryptography (SSL, TLS, SET,PCT) etc. |
| Network layer | 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 | No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP, using WPA etc |
| Physical layer | Using Spread spectrum mechanisms e.g.FHSS, DSSS etc |

## IV-DISCUSSION

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.

## REFERENCES

[1] H. N.Vyas, W.L.Shekh, D.P., "*Routing security in wireless ad hoc networks,"* Cincinnati Univ., IJEDR, Magazine, Oct. 2011,

[2] H. Deng, W. Li, Agrawal, D.P., "*Routing security in wireless ad hoc networks,"* Cincinnati Univ., OH,USA; IEEE Communications Magazine, Oct. 2002,

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

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

[5] 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

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

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

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

[9] 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

[10]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

[11] 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

[12] 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;