# A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network

Satyam Shrivastava
Department of Computer Science
MITM, RGPV
Indore, India
Satyamshrivastava89@gmail.com

Sonali Jain
Department of Computer Science
MITM, RGPV
Indore, India
Sonalijain2406@gmail.com

**Abstract- A structure less network is called the mobile ad-hoc network, where all the nodes are independent. In MANET, there is a collection of mobile nodes that from temporary network. Those nodes are act like a host or like a router. The security issue is the main problem of MANET, because many nodes perform many kind of misbehavior. This misbehavior looks like selfishness. We can define the selfishness as, a node use the recourse of other node and preserve the resource of own. This malicious node creates the problem in MANET. In this paper, we define the attacks in MANET.**

**Keywords -** MANET, Security goals, Routing, Attacks.

## I. INTRODUCTION

Wireless cellular system has been in use since 1980's. Access points are present in the wireless system. These access points are required to keep connect, user to wireless system [1]. Mobile nodes in MANET are dynamically located and interconnection between nodes is capable of changing on a continuous basis [2]. There are some characteristics of MANET.

- The communication medium is broadcast and connection of different nodes is wireless.
- The topologies between the nodes are changing continuously.
- Nodes are free to connect to any node.
- Due to the presence of malicious nodes, the performance is decrease [3].

There are some security goals of MANET.

1. Authentication- The authentication means, a user has the access right to use the resource. It is an assurance that the traffic you receive is sent by the legitimate user.
2. Integrity- Integrity is an assurance that the data which is received by the receiver has not been change or modified after the send by the original user.
3. Confidentiality- Confidentiality means that the data is not examined by the non-authorized party.
4. Non-repudiation- This is an authentication service. It is an inability to deny or disavow a transaction. It is an assurance that someone cannot deny something.
5. Access control- It is the prevention of an unauthorized use of a resource.

*Types of routing*

Routing is necessary in MANET, but it create problem and Challenges as compared to the routing in fixed infrastructure [1]. The problem in routing is due to the rapidly changes in the topology of the nodes and the devices. There are two type of routing, proactive and reactive.

In proactive routing, there is a fixed topology and use a single protocol. OLSR and DSDV are the proactive routing protocol.

In reactive routing, there is several protocol are used between the two devices and the type of topology is change according to the condition. AODV and DSR are the reactive routing protocol.

## II. ATTACKS IN MANET

There are mainly two types of attack are present.

1. *Active attack*

The names of some active attacks are Spoofing, Fabrication, Wormhole attack, Denial of services attack, Sinkhole attack, and Sybil attack.

a. *Spoofing*

When a malicious node miss-present his identity, so this way it can alter the vision of sender and sender change the topology [1].

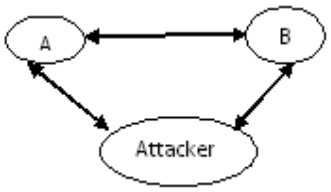


Figure 1. Spoofing Attack

b. *Fabrication*

When a malicious node generates the false routing message. This means malicious node generate the incorrect information about the route between devices [2].

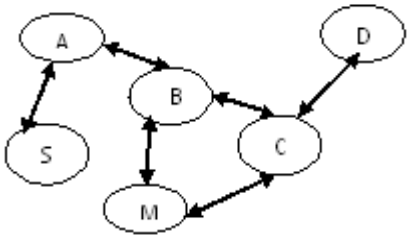


Figure 2. Fabrication Attack

*c. Modification*

Malicious node performs some modification in the routing, so that sender sends the message through the long route. This cause time delay and communication delay is occurred between sender and receiver.

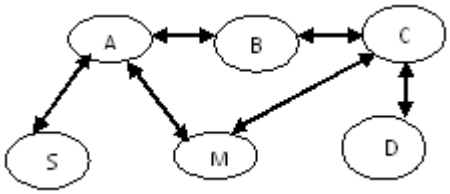


Figure 3. Modification Attack

*d. Wormhole*

Wormhole attack is also called the tunneling attack. An attacker receives a packet at one point and tunnels it to another malicious node in the network. This way beginner assumes that he found the shortest path in the network. This tunnel between two colluding attackers is called the wormhole [1, 2, and 3].

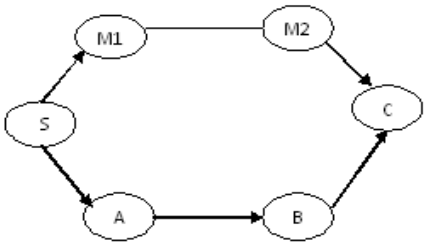


Figure 4. Wormhole Attack

*e. Denial of services*

In this type of attack, malicious node sending the message to the node and consume the bandwidth of the network. The aim of malicious node is to be busy to the network node. This way, if a message from the authorized node will come, then receiver will not receive the message because he is busy and beginner has to wait for the receiver response.


Figure 5. Denial of Services Attack

*f. Sinkhole*

It is a service attack that prevents the base station from obtaining complete and correct information [9]. In sinkhole attack, a compromised node tries to attract the data to it from his all neighboring node. Selective forwarding, modification or even dropping of data can be done by the sinkhole attack [1]

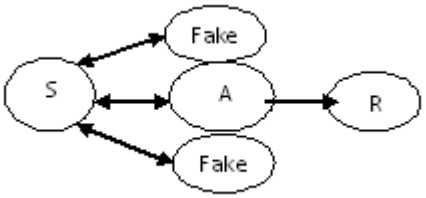


Figure 6. Sinkhole Attack

*g. Sybil*

Sybil attack refers to the multiple copies of malicious nodes. It can be happen, if the malicious node shares its secret key with other malicious nodes. This way the number of malicious node is increased in the network and the probability of the attack is also increased. If we use the multipath routing, then the possibility of choosing a path in the network, those contain the malicious node will be increased [1, 2, 3].

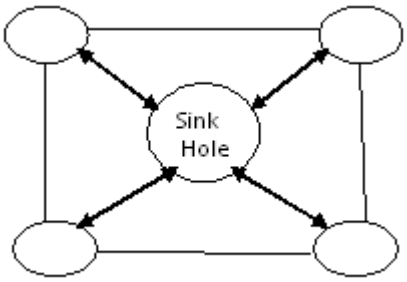


Figure 7. Sybil Attack

*2. Passive attack*

The name of some passive attacks is Eavesdropping, traffic analysis, and Monitoring [1, 2, and 3].

a. *Eavesdropping*

Eavesdropping is a passive attack, which occurred in the mobile ad-hoc network. The aim of eavesdropping is to find some secret or confidential information that should be kept secret during the communication. This confidential information may be privet or public key of sender or receiver or any password.

b. *Traffic analysis*

In this type of attack, an attacker tries to sense the communication path between the sender and receiver. This way attacker found the amount of data which is travel between the route of sender and receiver. There is no alteration in data by the traffic analysis.

c. *Monitoring*

Monitoring is a passive attack in which attacker can see the confidential data, but he cannot change the data or cannot modify the data.

## III. SOME ADVANCE ATTACKS

*a. Black hole attack*

In the black hole attack, attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An attacker use the flooding based protocol for listing the request for a route from the initiator, then attacker create a reply message he has the shortest path to the receiver . As this message from the attacker reached to the initiator before the reply from the actual node, then initiator assume that it is the shortest path to the receiver. So that a fake route is create. Once the attacker has been able to insert himself between the communications node, then attacker may able to do anything with the packet which is send by the initiator for the receiver [13].

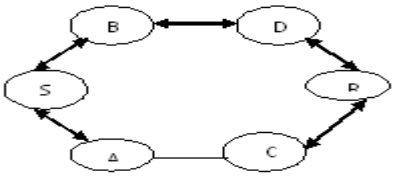


Figure 8. Black hole Attack

*b. Rushing attack*

In rushing attack, an attacker comes between the route of sender and receiver. When sender send packet to the receiver, then attacker intercept the packet and forward to receiver. Attacker performs duplicate suppression mechanism and then sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so that receiver will be busy continuously. This way, it reduces the efficiency of receiver [7].

*c. Replay attack*

It is a network attack in which a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. Suppose node S want to send some data to R. For this S has to prove his identity to R. This way S sends his password to R for identification. At that time, an attacker an intercept the password of S and a presenting itself as S, when asked for the proof of identity. A sends S password read from the last session, which R accepts [8].

*d. Byzantine attack*

A compromised intermediate node work alone or a set of compromised intermediate node works between the sender and receiver and perform some changes such as creating routing loops, forwarding packet through non-optimal path or selectively dropping packet, which result in disruption or degradation of routing services[10].

*e. Location disclosure attack*

Malicious node collects the information about the node and about the route by computing and monitoring the traffic. This way malicious node may perform more attack on the network [12].

## IV. CONCLUSION

Here we map the attacks (active or passive) with the layers [10, 11].

TABLE I

| Attacks | Active Attack | Passive attack | Layer |
|---|---|---|---|
| Spoofing | √ | | Network layer |
| Fabrication | √ | | Multi-layer |
| Modification | √ | | Multi-layer |
| Wormhole | √ | | Network layer |
| Denial of services | √ | | Multi-layer |
| Sinkhole | √ | | Network layer |
| Sybil | √ | | Network layer |
| Eavesdropping | | √ | Physical layer |
| Traffic Analysis | | √ | Data link layer |
| Monitoring | | √ | Data link layer |
| Black hole | √ | | Network layer |
| Rushing | √ | | Multi-later |
| Reply | | √ | Multi-layer |
| Location Disclosure | √ | | Network layer |
| Byzantine | √ | | Network layer |

## REFERENCES


[1] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M. "An Overview Of security Problems in MANET".

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

[3] Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006

[4] Shobha Arya1 And Chandrakala Arya2, "Malicious Nodes Detection In Mobile Ad Hoc Networks", Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-210-212.

[5] YihChun, Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad -Hoc Network Routing Protocols", *WiSe 2003,* September 19, 2003, San Diego, California, USA.Copyright 2003 ACM 1581137699/03/0009

[6] V. Palanisamy1, P.Annadurai2, "Impact of rushing attack on Multicast in Mobile Ad Hoc Network", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009

[7] S. Albert Rabara1 and S.Vijayalakshmi2, "Rushing Attack Mitigation In Multicast MANET (RAM3)", International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 1, No. 4, December 2010

[8] 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)

[9] Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou, "Launching a Sinkhole Attack in Wireless, Sensor Networks; the Intruder Side". Athens Information Technology, 19002 Peania, Athens, Greece.

[10] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, **"**A survey on attacks and countermeasures in mobile ad hoc networks**",** Springer, 2006.

[11] Ms.Supriya and Mrs.Manju Khari, "MANET security breaches: Threat to a Secure communication platform", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012

[12] K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks", *International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.*

[13] Sheenu Sharma, Roopam Gupta, "Simulation study of blackhole attack In the mobile ad hoc networks", Journal of Engineering Science and Technology Vol. 4, No. 2 (2009).