A Review Paper on Network Layer attacks in MANETs

Dhruvi Marsonia[1] Prof. Hardik Patel[2]
[1] P. G. Student (I. T.) [2]Assistant Professor
[1]Shantilal Shah Engineering College, Bhavnagar, Gujarat
[2]Sir Bhavsinhji Polytechnic Institute, Bhavnagar, Gujarat

Abstract—The security issues are the major consideration while implementing Mobile Ad hoc Networks (MANETs). Misbehavior of any node can do serious implications in this kind of dynamic network. A malicious or selfish node wants to preserve own resources along with using the services of other nodes and consumed their resources. Malicious nodes can break the rules and reduce the performance of well-behaved nodes significantly. This paper describes the different attacks and analysis of within Network Layer in MANETs.

Key words: MANETs, Ad Hoc, Security, Robust, Malicious nodes, selfish node etc.

I. INTRODUCTION TO MANETS

The MANET is the collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change speedily and random over time. It is also known as infrastructure less network. MANETs can form stand-alone groups of wireless terminals, but some of these may be connected to some fixed network. Compared to wireless networks in infrastructure mode ad-hoc networking doesn't require any access points. This makes useful in lots of different applications. It is largely used in military applications and in rescue operations where the existing communication infrastructure has been destroyed is possible for two nodes which are not in the communication range of each other, but still can send and receive data from each other with the help of intermediate nodes which can act as routers. This functionality gives another name to ad hoc network as "multi-hop wireless network". There are different routing attacks which appear in network layer during wireless transmission of messages. These attacks are caused by either some internal or external intruders. To accomplish our goal, we have done some methods to gathering information related to various types of attacks and solutions. In this paper we have study different attacks in network layer and also some security issue in mobile ad-hoc network.

II. VULNERABILITY OF MANETS

In a network Vulnerability of Manets is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is weaker than wired network. Some of the vulnerabilities are as follows:

A. Lack of centralized management:

MANET doesn't have a centralized monitor server. The absence of centralized management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes [1].

B. Dynamic Topology:

In MANETs, nodes can join and leave the network dynamically and can move independently. Due to such type nature there is no fixed set of topology works in MANETs. The nodes with poor physical protection may become malicious node and reduce the network performance [2].

C. Resource availability:

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism [1].

D. Limited resources:

The MANETs consists of different set of devices such as laptops, computers, mobile phones etc. All of such devices having different storage capacity, processing speed, computational power etc. This may attracts the attackers to focus on new attacks [2].

E. Scalability:

Due to flexibility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue about security. Security mechanism should be capable of handling a large network as well as small ones [1].

F. Cooperativeness:

Routing algorithm for MANETs usually assume that nodes are cooperative and not a malicious. As a result a malicious attacker can easily become an important routing agent and interrupt network operation by violating the protocol specifications [1].

G. Limited power supply:

The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply [1].

H. Wireless Links:

As the nodes in such networks are interconnected through wireless interface that makes it highly susceptible to link attacks. The bandwidths of wireless networks are less as compared to wired networks, which attracts many attackers to prevent normal communication among nodes [2].

III. SECURITY ATTACKS

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information [9]. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types.

Types of Attack	Characteristics	Example
Passive Attacks	Obtains information without disturbing normal network operation • Difficult to detect	Traffic analysis, traffic monitoring and eavesdropping
Active Attacks	Can be internal (attacker within the network) or external (attacker outside the network) •Can disturb network operation by modifying or deleting information, injecting a false message or impersonating a node	Modification, Impersonation, jamming and message replay

Table. 1: Attack Classification

A. *Passive attacks*

Passive attacks are the attack that does not disrupt proper operation of network .Attackers watch data exchanged in network without altering it. Detection of passive attacks is difficult since the operation of network itself does not get affected. Different type of passive attack as follow:

1) Release of Message Content

Release of Message Content is like an Eavesdropping. Secretly listening to the private conversation of others without their consent

2) Traffic Analysis

Traffic analysis is Monitoring or observes a situation for any changes which may occur over time.

B. *Active attacks*

Active attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks include some modification of data stream or creation of false stream. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication. Different types of Active attacks are as follow:

1) Masquerade

Masquerade is Pretend to be someone one is not. For example bob does not send a message to Alice. But Darth send a message to Alice as that appears by the bob.

2) Replay

Reply is Pretend to Playing again. For Example Bob send a message to Alice but that message capture by Darth and latter reply message to Alice.

3) Modification of Messages

Modification of messages is to Alteration in original message. Some Modification in message as like some data insertion, deletion, modification etc. Message is altered, deployed to produce an unauthorized effect.

4) Denial of Service

Denial of service is an attempt to make a resource unavailable to its intended users.

Some of the Dos Attacks are also listed below.

IV. NETWORK LAYER ATTACKS

Layer	Example Of Attacks
Network Layer	*DoS attacks:* Wormhole, Black hole, Gray hole, Byzantine, Resource Consumption attack, Rushing attack *Information Disclosure selfishness Attack:* selfish node .malicious node

Table. 2: Network Layer Attacks.

A. *Network Layer Attacks*

1) Wormhole Attack:

In this attack two compromised nodes create a tunnel or wormhole hole that linked through a private connection and thus they by-pass the network. This allows the node to short-circuit the normal flow of routing that control by the two attackers [5].The Wormhole attack is a kind of tunneling attack which is extremely dangerous and damaging to defend against even though the routing information is confidential, authenticated or encrypted [4]. It is relatively easy to deploy but exceedingly hard to detect. Usually Wormhole attack is launched by two malicious nodes (worms) connected via a high-speed wired or wireless link called Wormhole link or tunnel. Nodes outside each other's communication range have to communicate via intermediate nodes in a multi-hop way. [4]. The worms can drop delivered messages and acquire statistical data of traffic by investigating message traffic [10]. To minimize delay, the attacker may forward each bit through the Wormhole link without waiting for the entire packet to be received [4].

– *Operation of Wormhole Attack:*

As shown in Figure 1, two malicious nodes X and Y created the Wormhole attack on the MANET. X and Y are connected via a high-speed Wormhole link that tunnels traffic between nodes A and B. when node A want to communicate with node B, normally it takes multiple hops for a packet to travel between them. Though in the attendance of worms X and Y, A and B start believing that they are immediate neighbors. Packets traveling through Wormhole link travel faster to the destination than packets traveling through multiple hops in the MANET. X and Y do not alter the packet header and falsify the route lengths. Packets received by X are replayed through Wormhole link to Y and vice versa. X and Y can now selectively drop data packets or analyze traffic and disrupt the network's communication. Malicious nodes X and Y along with the Wormhole link are not visible in the route; and also the Wormhole attacker is hidden from the higher layers. Therefore, detection of Wormhole attack is exceedingly tough.

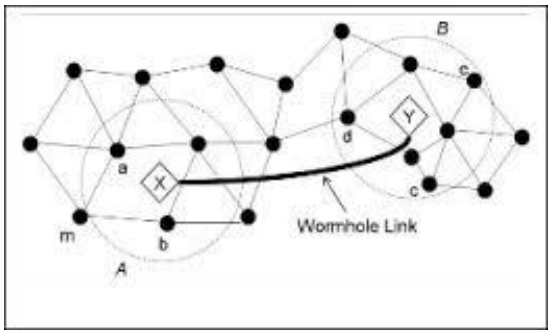

Fig. 1: wormhole Attack

2) Packet Dropping or Black-hole Attack:

Blackhole attack is another type of DoS attack. In mobile ad hoc networks (MANETs), nodes usually cooperate and forward each other's packets in order to enable out of range communication. Saving their own resources or for intentionally disrupting regular communications. This type of misbehavior is generally referred to as packet dropping attack or black hole attack [6].That generates and disseminates fabricated routing information. If the malicious node replies to the requesting node before the actual node replies, a bogus route will be created. Therefore packets are not forwarded to the specified destination node; instead, the malicious node intercepts the packets, drops them and thus, absorbs network traffic [4].

– *Operation of Blackhole Attack:*

An example of Blackhole attack against AODV protocol (Ad-hoc On demand Distance Vector) is shown in Figure 2. [4]. Suppose source S wants to communicate with node D. S initiates route discovery process by broadcasting route request packets (RREQ) to its neighbors. The destination node D or any intermediate nodes having fresh route to the destination can give reply by sending reply packet (RREP) to S. Considering no intermediate nodes have a fresh route to D, they forward request packets towards destination. As X is a malicious node, it doesn't forward the request packet ahead; instead, it falsely replies to S indicating that it has a valid fresh route to D. Thus, reply packet from X reaches to S ahead of reply packets from other neighbors of S. Therefore, S considers sending packets to D via X considering that X has a shortest route to D. Now X absorbs all packets forwarded from S to D. This is how a Blackhole attack is setup.

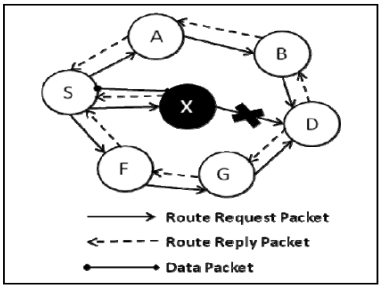

Fig. 2: Blackhole attack

3) Gray-hole attack:

This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability[1].Grayhole attack is an extension of Blackhole attack in which a malicious node's behavior is exceptionally unpredictable[4].

4) Resource Consumption Attack:

In this attack, a malicious node intentionally tries to consume the resources (e.g. battery power, bandwidth etc) of other nodes in the network. The attack can be of various types like unnecessary route requests, route discovery, control messages, or by sending stale information [6].

5) Selfishness Attack:

Cooperation among nodes in Ad- Hoc Networks is an important issue for communication. But some nodes do not cooperate in communication and saves their energy. These nodes are called Selfish nodes. Selfish nodes participate in route discovery stage properly to update their routing table, but as soon as data forwarding stage begins, they drop data packets This malicious node which is not participating in network operations, use the network for its advantage to save its own resources such as power [6, 1].

a) Selfish Misbehavior of Nodes

Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network [2]. It may include two important factors.

i) *Protection of battery power*
ii) *Gaining partial share of bandwidth:* The selfish nodes may reject to take part in the forwarding process or drops the packets purposefully in order to conserve the resources. These attacks use the routing protocol to their own advantage. Packet dropping is one of the main attacks by selfish node which indications to congestion in network. However most of routing protocols have no mechanism to detect whether the packets being forwarded or not except DSR (dynamic source routing) [2].

b) Behavior of Malicious nodes

The main of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighboring nodes. Attacks of such type are fall into following categories.

i) *Denial of Service (DOS):* These types of attacks produced a malicious action with the help of compromised nodes that forms severe security risks. In the presence of compromised nodes, it is very difficult to detect the compromised routing. The compromised route appears like a normal route but leads to severe problems. For example, a compromised node could participate in the communication but drops some packets which lead to degradation in the quality of service being offered by network [2].
ii) *Attacks on Network integrity***:** Network integrity is an important issue, in order to provide secure communication and quality of service in network. There are so many threats which exploit the routing protocol to introduce wrong routing information [2].
iii) *Misdirecting traffic:* 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 owner of the address. A malicious node may advertise fake route request, so that other nodes will then direct route replies to the node [2].

iv) *Attacking neighbor sensing protocols:* malicious nodes advertise fake error messages so that important links interface are marked as broken. This will result in decrease in network throughput and quality of service [2].

– *Operation of malicious nodes*

In such attacks, the attackers can create routing loops to form severe congestion. Different type of attacks are identified which are initiated by malicious node. The malicious node "X" can absorb important data by placing itself between source "A" and destination "D" as shown in Figure-3. "X" can also divert the data packets exchanged between "A" and "D", which results in significant end to end delay between "A" and "D". In this type of attacks attackers attacks against Routing and Path Selection The malicious node can disrupt the route discovery process by creating routing loops and overflow routing tables [2].

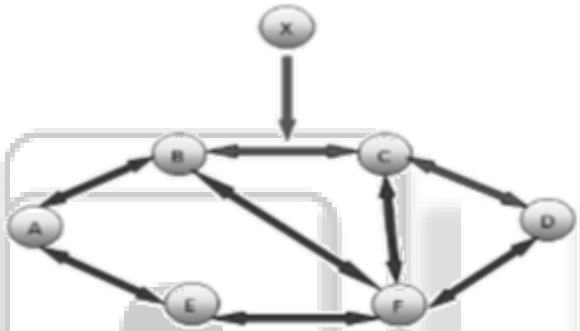

Fig. 3: Malicious nodes

V. CONCLUSION AND FUTURE WORK

Due to dynamic structure of MANETs and having no centralized administration, it makes it more vulnerable to many attacks. It is discussed, the weakness MANETs as well as various active and passive attacks. (There is no significant contribution has been shown in work means what is your finding and what are the solutions)

In future study we will try to invent such intrusion detection system with routing protocols that helps to reduce the impact of different attacks.

REFERENCES

[1] A Literature Review of Security Attack in Mobile Ad-hoc Networks Priyank Goyal, Bhiwani, Haryana, Sahil Batra ,International journal of computer application (0975-8887) volume-9 No 12,November 2010.

[2] Analysis of Different Security Attacks in MANETs on Protocol Stack A Review Gagandeep, Aashima, Pawan Kumar, International Journal o Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[3] Review Report ATTACK Analysis in Mobile Ad HOC Network Based on System Observations Nidhi Saxena1, Iyagpal Yadav, Vipul Saxena International Journal of Advanced Research in Computer Science a Software Engineering 3(7), July – 2013, pp. 618-623.

[4] DoS Attacks in Mobile Ad-hoc Networks: A Survey", Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala," 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE.

[5] Detecting unauthorized and compromised node in mobile ad-hoc network, Nikoskomniuos.

[6] Selfish Node Detection with modified AODV in Ad-Hoc Networks Niyati Shah , Sharada Valiveti , Dr. K Kotecha Institute of Technology Nirma University Ahmedabad, Gujarat, India.

[7] Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks Frank Kargl, Andreas Klenk, Stefan Schlott, and Michael Weber.

[8] P. D. PrzemyslawKazienko, "Intrusion detection systems (ids) part i - (network intrusions; attack symptoms; ids tasks; and ids architecture)," Apr, 2003.

[9] Z. Karakehayov, "Using REWARD to Detect Team Black- Hole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[10] MahdiTaheri, Dr. majidnaderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

