World Journal of Engineering Research and Technology
WJERT
www.wjert.org
Impact Factor Value: 5.924

ANALYSIS OF DIFFERENT SECURITY ATTACKS IN MANET ON PROTOCOL STACK

***[1]Dr. K. Divya and [2]Dr. B. Srinivasan**

[1]Ph.D Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, India.

[2]Associate Professor, Gobi Arts & Science College, Gobichettipalayam, India.

Article Received on 26/10/2020 **Article Revised on 16/11/2020** **Article Accepted on 06/12/2020**

***Corresponding Author**
Dr. K. Divya
Ph.D Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, India.

ABSTRACT

A MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces In order to make communication among nodes, the nodes dynamically establish paths among one another. The nature and structure of such networks makes it attractive to various types of attackers. In this paper we discuss various types of attacks on various layers under protocol stack. Different types of attacker attempts different approaches to decrease the network performance, throughput. In this paper the principal focus is on routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication. On the basis of the nature of attack interaction, the attacks against MANET may be classified into active and passive attacks. Attackers against a network can be classified into two groups: insider and outsider. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs.

KEYWORDS: MANET, DoS, DSR, AODV.

1 INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. Mobile ad hoc networks are collection of wireless networks, which consists of large number of mobile nodes. Nodes in

MANETs can join and leave the network dynamically. There is no fixed set of infrastructure and centralized administration in this type of networks. Nodes are interconnected through wireless interface. The dynamic nature of such type networks makes it highly susceptible to various link attacks. The basic requirements for a secured networking are secure protocols which ensure the confidentiality, availability, authenticity, integrity of network. Many existing security solutions for wired networks are ineffective and inefficient for MANET environment. As the transmission takes place in open medium makes the MANETs more vulnerable to security attacks. In the presence of security protocol affect of various attacks can be reduced. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the success of MANET communication highly relies on the collaboration of the involved mobile nodes.

In this paper, we discuss some of the existing malicious attacks against MANETs and also the techniques to detect them. These types of attacks consist of replication, modification, or removing information exchanged by other nodes.

A. Vulnerabilities of MANET 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 inadequate physical protection may become malicious node and reduce the network performance.

B. 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

C. Cooperativeness

In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious nodes which disrupt the network operation by changing routing information etc.

D. Lack of clear line of defense

There is no clear line of defense mechanism available in the MANETs; attacks can come from any directions. Attackers can attack the network either internally or externally.

E. 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.

2 Security Attacks In Manets

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network.

The attacks in MANETs are divided into two major types.

- Internal Attacks
- External Attacks

2.1 Internal Attacks

Internal Attacks Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes. The wrong routing information generated by compromised nodes or malicious nodes are difficult to identify. This can be due to the compromised nodes are able to generate the valid signature using their private keys.

2.2 External Attacks

These types of attacks try to cause congestion in the network, Denial of Services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication and producing additional overhead to the network.

External attacks can classify into two categories:

- Passive Attacks
- Active Attacks

2.2.1 Passive Attacks

A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Detection of such type of attacks is difficult since the operation of network itself doesn't get affected. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

2.2.2 Active Attacks

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks.

Active attacks are classified into four groups

- Dropping Attacks
- Modification Attacks
- Sinkhole Attacks
- Fabrication Attacks
- Timing Attacks

2.2.3 Dropping Attacks

Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point.

2.2.4 Modification Attacks

These attacks modify packets and disrupt the overall communication between network nodes. Sinkhole attacks are the example of modification attacks.

2.2.5 Sinkhole Attacks

In sinkhole attack, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node than capture important routing information and uses it for further attacks such as dropping and selective forwarding attacks.

2.2.6 Fabrication Attacks

In fabrication attack, the attacker send fake message to the neighboring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages.

2.2.7 Timing Attacks

In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.

3 Types Of Active Attacks On Various Layers In Protocol Stack

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack.

3.1 Attacks at Physical Layer

The attacks on physical layer are hardware oriented and they need help from hardware sources to come into effect. These attacks are simple to execute as compared to other attacks. They do not require the complete knowledge of technology.

Some of the attacks identified at physical layer include

- Eaves Dropping
- Jamming
- Interference

3.1.1 Eaves Dropping

Eavesdropping can also be defined as interception and reading of messages and conversations by unintended receivers. As the communication takes place on wireless medium can easily be intercepted with receiver tuned to the proper frequency. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. The information may include private key, public key, location or passwords of the nodes.

Classified data can be eavesdropped by tapping communication lines, and wireless links are easier to tap.

3.1.2 Jamming

Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

3.1.3 Active Interference

An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use.

3.1.4 Conservation of battery power

Gaining unfair share of bandwidth. The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources. These attacks exploit the routing protocol to their own advantage. Packet dropping is one of the main attacks by selfish node which leads 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).

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.

- **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.

- **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.

- **Traffic Analysis**

In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self organization in the network, and valuable data about the topology can be gathered.

3.2 Attacks at Network Layer

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 fig 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".

- Black hole attacks
- Rushing Attacks
- Wormhole Attacks
- Sinkhole Attacks
- Replay Attacks
- Link With Holding & Link Spoofing Attacks
- Resource Consumption Attacks
- Sybil Attacks

3.2.1 Black Hole Attacks

In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. On receiving the request the malicious node sends a fake reply with extremely short route. Once the node has been able to place itself between the communicating nodes, it is able to do anything with the packets passing between them.

3.2.2 Rushing Attacks

Rushing attacks are mainly against the on-demand routing protocols. These types of attacks subvert the route discovery process. On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack.

3.2.3 Worm Hole Attacks

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. Wormhole attacks are severe threats to MANET routing protocols. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes.

3.2.4 Sink Hole Attacks

Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complicated. A malicious node tries to attract the secure data from all neighboring nodes.

3.2.5 Replay Attacks

In MANETs, the topology is not fixed; it changes frequently due to mobility of nodes. In replay attack, a malicious node record control messages of other nodes and resends them later. This results in other nodes to record their routing table with stale routes. These replay attacks are later misused to disturb the routing operation in a MANETs.

3.2.6 Link Withholding & Link Spoofing Attacks

In link withholding attack, the malicious node does not broadcast any information about the links to specific nodes. It results in losing the links between nodes. In Link spoofing attacks, a malicious node broadcasts or advertises the fake route information to disrupt the routing operation.

3.2.7 Resource Consumption Attack

In resource consumption attack, a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim. These types of attacks are also known as sleep deprivation attack and mainly occur against the devices that don’t offer any services to the network.

3.2.8 Sybil Attack

In Sybil attack, Sybil attacker may generate fake identities of number of additional nodes. In this, a malicious node produces itself as a large number of instead of single node. The additional identities that the node acquires are called Sybil nodes. A Sybil node may fabricate a new identity for itself or it steals an identity of the legitimate node. Due to presence of duplicate identities the outcome of voting process may vary. Sybil nodes affect the normal operation of routing protocols by appearing itself at various locations in network.

3.3 Attacks at Transport Layer

- Session Hijacking Attacker
- SYN Flooding Attack

3.3.1 Session Hijacking Attacker

Session Hijacking Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc) and other information from nodes.

3.3.2 SYN Flooding Attack

The SYN flooding attacks are the type of Denial of Service (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node. These half opened connection are never completes the handshake to fully open the connection.

3.4 Attacks At Application Layers

Application layer protocols are also vulnerable to many DoS attacks. The application layer contains user data. It supports protocols such as HTTP, SMTP, TALNET and FTP, which provides many vulnerabilities and access points for attackers. Application layers are classified as

- Malicious code attacks
- Repudiation attacks

3.4.1 Malicious code Attacks

Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

3.4.2 Repudiation Attacks

Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks.

4 Security Goals

The goal of system security is to have controlled access to resources. The key requirements for networks are

- Confidentiality
- Authorization
- Integrity
- Non repudiation
- Availability
- Resilience to attacks
- Freshness
- Access Control
- No repudiation

4*.1 Confidentiality*

It protects data or a field in message. It is also required to prevent an adversary from traffic analysis.

4.2 Integrity

It ensures that during transmission the packets are not altered.

4.3 Authorization

It authorizes another node to update information or to receive information.

4.4 Availability

It ensures that services are available whenever required.

4.5 Resilience to attacks

It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

4.6 Freshness

It ensures that malicious node does not resend previously captured packets. Anonymity: this service helps for data confidentiality and privacy.

4.7 Access control

It prevents unauthorised access to a resource.

4.8 No repudiation

No repudiation prevents the source from denying that it sends the packet.

5 CONCLUSION AND FUTURE WORK

Due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks. In this paper, we discuss about how different layers under protocol stack become vulnerable to various attacks. These attacks can classified as a active or passive attacks. Different security mechanisms are introduced in order to prevent such network. In future study we will try to invent such security algorithm, which will be installed along with routing protocols that helps to reduce the impact of different attacks.

REFERENCES

1. Amitabh Mishra, "Security And Quality Of Service In Ad Hoc Wireless Networks" (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook.
2. Akanksha Saini, Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET".
3. C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols".
4. Kamanshis Biswas and M.D. Liakat Ali, "Security Threats in Mobile Ad Hoc Network".
5. K.P. Manikandan, Dr. R Satyaprasad, Dr. Rajasekhararao, "Analysis and Diminution of Security Attacks on Mobile Ad hoc Network", IJCA Special Issue on "Mobile Ad-hoc Networks MANETs", 2010.
6. Kisung Kim and Sehun Kim, "A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks".
7. Mohammed Ilyas, "The Handbook of Ad Hoc Wireless Networks".

8. Pradeep M. Jawandhiya, Mangesh M. Ghonge, "A Survey of Mobile Ad Hoc Network Attacks". International Journal of Engineering Science and Technology, 2010; 2(9): 4063-4071.
9. Panagiotis Papadimitratos and Zygmunt J. Haas, "Securing Mobile Ad Hoc Networks".
10. Sevil¸ Sen, John A. Clark, and Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks".
11. Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey.
12. Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey".
13. Zubair Muhammad Fadlullah, Tarik Taleb, and Marcus Scholar, "Combating against Security Attacks against Mobile Ad Hoc Networks (MANETs)".