A Review on different Types of Active and Passive attacks in MANET

[1]Er. Pankaj,[2]Er. Shikha Verma
Department of Electronics and Communication
LRIET Solan, HP,India

Department of Electronics and Communication
LRIET Solan , HP, India.

Abstract: *In applications with low infrastructural elements, a MANET becomes highly vulnerable to security attacks. These attacks can be active or passive in nature. Active attacker including 'Black-hole', 'Grey-hole' and 'Worm-hole'; can modify, listen and inject messages in communication channel. Whereas, a passive attacker does not alter the information; but secretly listens to valuable information i.e. spoofing. Jellyfish attack is one of the illustrations of a passive attack. Jellyfish conforms to all routing and forwarding protocol specifications. A Jellyfish attacker possesses the property that it is difficult to detect until after the sting. Jellyfish attacker targets closed loops and misguide the packets to adversely affect the network performance. A Jellyfish attack can attack the network in 3-ways Jellyfish-reorder-attack, Jellyfish-periodic-dropping-attack and Jellyfish-delay-variance-attack. In Jellyfish Delay Variance (JFDV) attack, attacker node receives the packets from source side and adds delay while forwarding the packets to receiver.*

Keywords: Jellyfish, MANET, Black-hole, Grey-Hole

I. INTRODUCTION

With the development of network and communication technology, the problem of wired connection is reduced with wireless networks as it has wide perspective and practicability in the area of disaster recovery, defense, emergency situations and special event management. A wireless local area network that uses assigned frequency radio waves rather than wires or physical connections to communicate between networks enabled devices. Every second is crucial in large scale developments and wireless technology elevates the output by providing high mobility of nodes and easier network expansion. It works in two modes named as Infrastructure-based network and ad-hoc networks. Infrastructure mode network is made up of fixed and wired network nodes and gateways, network ser-vices delivered with the help of preconfigured infrastructures. For example, cellular net-works are infrastructure-based networks built from PSTN backbone switches, MSCs, base stations, and mobile hosts. Each node has its specific responsibility in the network, and connection establishment follows a strict signaling sequence among the nodes. However in ad-hoc networks, nodes are not comfortable with the topology of their networks. Instead, they need to discover it on regular basis based on the mechanisms of different protocols. Every node contacts its neighbors using best routes. There are many ways to select the routes like hop count, bandwidth and delay

1.1.1 Characteristics of MANETs

An ad hoc network is a collection of mobile nodes forming an instantaneous network without fixed topology and centralized system. Various Characteristics of MANETs are described as:

Autonomous Behavior: Each mobile node in MANET can act as both host and router exhibiting autonomous behavior.

Multihop Radio Relaying: When any source node and destination node is out of radio range, the MANET is capable of multihop relaying. Multihop routing is a type of communication in which network coverage is larger than the coverage area of single node. Therefore, a node can use other nodes as relays to reach a specific destination.

Less Secure: A Centralized firewall is absent in the network making the ad-hoc network as less stable and secure

Dynamic Topology: The node can join or leave the network at any point of time making the network topology varying continuously.

Less Human Intervention: Mobile and spontaneous behavior of nodes tend to result in minimum human intervention to configure in network.

High User Density: Large numbers of users can get the benefit of the network.

1.2 SECURITY ATTACKS IN MANETs

Attacks against routing protocols can be categorized into internal and external attacks. An external attack initiates from a router that does not participate in the routing process but behaves as trusted router. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls

An internal attack originates from compromised, misconfigured, faulty or malicious routers. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks. Any attack on

Ad-hoc networks can also be categorized as active and passive attacks.

Table 1.1 Attackers at different Layers

Layer	Example of attacks
Application Layer	Repudiation, Data Corruption, Viruses, Worms
Transport Layer	Session Hijacking, SYN Flooding, Jellyfish Attack
Network Layer	Sybil Attack, Black hole Attack, Gray hole Attack, Wormhole Attack, Spoofing, Selfish Misbehavior, Byzantine Attack , Route table overflow
Data Link Layer	ARP Spoofing
Physical Layer	Eavesdropping

In an active attack, the misbehaving node actively disturbs the normal operation of the network with attempts to alter or destroy the data being exchanged in the network. In passive attack the malicious entity only listens to the traffic without disturbing proper operation of the network. An attacker is also able to interpret the data gathered through snooping to violate confidentiality requirement.

1.3.1 Application Layer Attacks

Various attacks that affect application layer are

- **Repudiation Attack**: - A repudiation attack happens when an application or system does not check or track the log user actions. Thus new actions can not be identified and malicious nodes got permission to forge the system. It is the ability of system to deny that specific tasks or actions are performed by them.
- **Data corruption**: - Corruption can affect the communication in various ways. Sometimes a complete file can got deleted. It can either drop all database tables or change the database record.
- **Viruses**: - Virus is a type of software which attack itself to a program and moves ahead through the system by copying itself. Once a virus is executing, it can affect the performance by performing deletion of all files and programs.
- **Worms**: - A system worm spread like a virus but it is independent program rather than hidden inside another program. It is standalone malware which uses computer network to spread itself and relies on the security failures of the target computer system.

1.3.2 Transport Layer Attacks

The following attacks prevail in transport layer

- **Session Hijacking**: - Attack consists of misuse of the web session control mechanism. The mechanism is generally managed for a session token. In any http communication, token is a most common method to identify every user's connection. Web server sends tokens to the client browser after a successful event authentication. The session hijacking attack comprises the session token by stealing or predicting a valid session token to gain unauthorized access to web browser.
- **SYN Flooding**: - In this form of attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYN ACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet. Unless response is obtained from ACK packets, the data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed-size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection. Normally there is a timeout associated with a pending connection, so the half-open connections will eventually expire and the victim node will recover. However, malicious nodes can simply continue sending packets that request new connections faster than the expiration of pending connections.
- **Jellyfish Attack**: - Jellyfish attack affects the network by behaving in three ways named as Jellyfish reorder attack, Jellyfish periodic dropping attack and jellyfish delay variance attack [5]. This type of attack is the main focus in this work.

1.3.3 Network Layer Attacks

Network layer is affected by the following attacks

- **Sybil attack**: - A Sybil attacker can either create more than one identity on a single operating device in order to launch a coordinating attack on network. It can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as trusted node. In Voting based Systems, a Sybil attacker can be use multiple virtual ID's to control the result by rigging the polling process. In Vehicular ad hoc networks, Sybil attacker can create an arbitrary number of virtual non-existent

vehicles and transmit false clue of traffic congestion and divert the traffic.

- **Black hole attack**: - In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. A Black Hole Attack can be carried out in many ways. The classic way is to flood packets in the network so that services provided be intermediate node is no longer available to other participating nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of MANETs, there exist many more ways to launch a Black Hole Attack in such a network. Black Hole Attack attacks can be launched against any layer in the network protocol stack. On the physical and MAC layers, an attacker could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an attacker could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the Quality of Service being offered by the network. On the higher layers, an attacker could bring down critical services by Low Rate Black Hole Attack.

- **Gray hole attack**: - Gray whole attack is an active type of attack, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message by which it takes over the sending packets. Afterwards, the node just drops the packets to launch Black Hole Attack. If neighboring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim of reducing performance of network. This attack is known as Routing Misbehavior attack. A Gray Hole attacker exhibits malicious behavior in different ways. It may drop the coming from certain specific nodes, it may behave maliciously for some time, and then switch to normal behavior. Hence detection of gray hole attack is difficult task

- **Wormhole attack**: - Wormhole attacker node gain the confidentiality of the sender by faking the MAC address from the sender and also by receiving the whole data sent by sender via making a tunnel and by not letting the sender to send data to true destination .

- **Spoofing**: - When an attacker tries to access computer or system by behaving as a trusted source.

- **Selfish Misbehavior**: - Whenever the selfish node feels that packet requires lot of resources, the selfish node does no forward it in the network. Node misbehavior and failures causes isolation problem. However, selfish nodes can still make the communication with all other nodes. Selfish nodes are of three types: No packet forwarding, No participation, Partial packet forwarding with energy saving [6].

- **Byzantine** attack: - Byzantine attack is defined as attack against routing protocol, in which two or more routers conspire to drop, fabricate, modify or misroute packets in an attempt to exploit the routing services. It is an example of internal attack.

- **Route table overflow**: - Attacker attempts to create routes to non-existing nodes and prevents creation of new routes. Proactive protocols are more affected by this attack.

1.3.4 Data Link Layer Attacks

Attack related to data link layer is given below

- **ARP spoofing**: - Address resolution protocol is a protocol used to map IP address to a physical machine. Whenever a host machine wants to find a MAC address for an IP address, it broadcast ARP request. The host machine replies with ARP reply message. Every time a host gets an ARP reply from another host, even though it has not sent an ARP request, it will accept ARP reply entry and updates its ARP Cache. The process of modifying target host, ARP cache with forge entry is known as ARP spoofing.

1.3.5 Physical Layer Attack

Attack affecting physical layer is

- **Eavesdropping: -** An attacker can listen to any wireless network to know what is going on in the network. It first listens to control messages to infer the network topology to understand how nodes are located or are communicating with another. It collects useful information about the network before attacking. It may also listen to the information that is transmitted using encryption although it should be confidential belonging to upper layer applications. Eavesdropping is also a threat to location privacy.

II. RELATED WORK

Avani Sharma et al., (2014), proposed Non-cryptography approach is work basically on delay threshold time. Delay

threshold time was a measure of time interval boundary of all enroute nodes of forwarding data packets. The approach works in two phases, firstly all data packets was analyzed and checked that which particular data among them at delaying the packet at enroute nodes. Any misbehavior during analysis declares the node as an JF node. Then alternate optimum path is chosed with the help of re-routing if the difference between time of current forwarding data packet and their previous sent packet have higher delay than threshold [17].

Preety Dahiya et al., (2016), modifies TCP and AODV system to handle the jelly fish periodic dropping attack, the jellyfish packet reordering attack and the jelly fish delay variance attack. The system uses the E_TCP of the existing system along with the modified AODV routing to get the effective results. In the E_TCP protocol the buffer stores the sequence number and the acknowledgement time while in the NAODV_ETCP protocol the forwarding ratio is stored in buffer [18]

Sukhpal Kaur et al., (2017), presented a tecnnique in order to detect and prevent abnormal behavior of JF attacker node, the proposed scheme aims to work in the following way. When the source node receives the route replies, it will store all the paths in its cache memory. Whole data was sliced in three parts and sent to destination by three different routes. When the destination node will receive the packets, it will compare the number of received packets with the threshold value where the threshold value will be set at 80 percent to the number of packets sent. Detection procedure was initiated on the path containing low threshold value to check the number of packets received and forwarded by each node of that path. If again packet delivery rate of a particular node tends to drop below the threshold value, then that particular node will be detected as malicious. ID of the suspected node will be broadcasted to all the nodes in the paths to prevent communication with that malicious node and thus shall benefit the performance [19].

Sakshi Sachdeva et al., (2017), indicates that the presence of Jellyfish attacker node degrades the performance of network in terms of throughput and end to end delay. A scheme is proposed to detect and prevent JF attacker node from detrioting the network and effectiveness of scheme is evaluated on ns2 simulator. Jellyfish delay variance attack on AODV is analyzed by JFDV detection algorithm that analyzes packet delaying misbehavior of nodes and detects multiple JFDV attacker nodes [20]

III. CONCLUSION

MANET is emerging as a useful technology in mobile computing and have found many applications in different fields. MANET supports various routing protocols, which helps the user to communicate in wireless networks. Due to the decentralized nature and ability of nodes to move freely in any direction, MANET is highly prone to security attacks. Security is major issue in MANETs as it supports dynamic topology and any malicious node can enter the network and affect its normal functioning. Various types of attackers are present that intend to ruin the performance of network. One such attacker that affects the routing protocols is Jellyfish delay variance attack (JFDV). In Jellyfish attack, JF attacker becomes the part of routing mesh and introduces some amount of delay before forwarding the packets. As it behaves more like a normal node, it is very difficult to detect its presence.

IV. FUTURE WORK

This research can be extended by studying the other two types of jellyfish attacks namely Jellyfish periodic dropping attack and Jellyfish reorder attack. This work can also be improved by considering other proactive protocols like OLSR, WRP and hybrid category of protocols like ZRP and ZLSR.

REFERENCES

[1] Avani Sharma, Rajbir Kaur, "Non-Cyrptographic Detection Approach and Countermeasure for JFDV Attack", Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, Scotland, UK, 9-11 Sept-2014, ISBN: 978-1-4503-3033-6

[2] Preety Dahiya, Miss Bhawana, "Design and Implementation of NAODV-ETCP to handle jellyfish attack", International Journal & Engineering Trends and Technology, Vol. 35, No. 7, May-2016, ISSN: 2231-5381

[3] Sukhpal Kaur, Dr. Rajinder Singh, "Detection and Prevention of JFPD attack in MANETs using NBA Technique", Worldwide Journal of Multidisciplinary Research and Development (WWJMRD), Vol. 3, Issue 6, pg. 88-91, 2017, ISSN: 2454-6615

[4] Imad Aad, Jean-Pierre Habaux, Edward W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", IEEE/ACM Transactions on Networking, Vol. 16, Issue 4, pg. 791-802, August-2008

[5] Hoang Lan Nguyen, Uyen Trang Nguyen, "A Study of Different types of attacks on multicast in mobile ad hoc networks", Proceedings of IEEE International Conference on Networking(ICN), pg. 32-46, 2016 ELSEVIER, ISSN: 1570-8705

[6] Pooja Patel B., Patel Manish M., Patel Megha B., "Jellyfish Attack Detection and Prevention in MANET: A Review", International Journal of Advance Research in Engineering, Science & Technology (IJAREST), Vol. 4, Issue 3, pg 361-366, March-2017, ISSN: 2393-9877

[7] Vijay Laxmi, Chhagan Lal, M.S Gaur, Deepanshu Mehta, "Jellyfish attack: Analysis Detection and Counter measure in TCP-based MANET" Journal of

Information Security and Applications (JISA), Elsevier 2014

[8] Sakshi Sachdeva, Parneet Kaur, "Detection and Analysis of Jellyfish Attack in MANETs", IEEE International Conference on Inventive Computation Technology (ICICT), Coimbatore, India, 26-27 Aug-2016.

[9] Sakshi Garg, Satish Chand, "Enhanced AODV protocol for defense against Jellyfish Attack on MANETs", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), Greater Noida, India, 24-27 Sept-2014, ISBN; 978-1-4799-3080-7

[10] Mr. Hepikumar R. Khirasariya, "Simulation Study of Jellyfish Attack in MANET using AODV Routing Protocol" , Journal of Information, Knowledge and Research in Computer Engineering, Vol 2, Issue 2, Oct-2013