Security Aspects of Mobile Ad hoc Networks: A Review

Shivani , Munish Katoch
Research scholar, Assistant Professor
Deptt. Computer Science Sri Sai University Palampur

Abstract: The Mobile Ad-Hoc Network is the decentralized network in which mobile nodes can join or leave the network when they want. Due to such unique property of the network malicious node trigger various type of active and passive attacks. The active attacks affected network performance in term of certain parameters. This review paper, various security aspects are reviewed and analyzed in terms of certain parameters.

KEYWORDS:- **MANET, Active-Passive Attacks, Wormhole attack, AODV Routing Protocol.**

INTRODUCTION

A MANET called wireless ad-hoc network and ad-hoc wireless network that usually has a routable networking environment on top of the link layer ad-hoc network. The inherent characteristics of mobile ad-hoc network and dynamic topology in nature [**1**].Due to the mobility connection these network reduce its throughput and increases its mitigate effects of attacks. These network have no fixed routers. The entire network is mobility, and the individual nodes are allowed to move freely anywhere in the network. In this type of network, the terminal may not be able to communicate directly with each other and depends upon third party messages is required to reach its destination [16]. During the communication in MANET, mobile nodes can behave as router or as a host based on multi-hop scenario. Due to MANET architecture, it is gaining more attention for real time applications where a temporary network is required such application scenarios are military application, disaster recovery etc. Providing quality of service is a critical task for any network[15]. Edouard Manet(Mobile advertisement VeriSign vert hoc net) can be described as a wireless meshwork which is a solicitation of heterogeneous mobile River twist and is self-organizing, self-configuring. In this type of meshwork the devices communicate through a wireless medium with each other. The devices in the meshing should cooperate with each other so the packet can be transmitted via intermediate devices when there is no direct course from generator to address. There is no constructor of central controlling authority & a permanent network base in a mobile ad-hoc network. Transfer of packets is done with the help of routing protocols, which help in determining the suitable route from germ to destination for initiating as well as maintaining a connecter between the two. Network topologies are dynamic in nature, due to which there are link breakage and hurly burly in peer to peer connection. An ad hoc mesh is a receiving set network describe by the nonentity of a centralized and fixed infrastructure. In the absence of an infrastructure in ad hoc meshing poses great challenges in the functionality of these networks. Therefore, we refer to a wireless ad hoc electronic network with mobile River nodes as a Mobile Ad Hoc Net. In a Edouard Manet thickening have the potentiality to accept and route traffic from their intermediate client towards the destination. Therefore they can act as both router and hosts. More frequent connection fading and re-tie place an vitality constraint on the mobile knob [2]. As Manet are illustrated by limited bandwidth and node mobility. There are many type of protocol are available in Eduard Manet. Its efficiency of a routing protocol is determined by its barrage fire power consumption of a participating node and routing of traffic into the electronics network [3].

1.1 Classification of Attacks in MANET

The attacks on MANET can be classified on the basis of the source and behavior. On the basis of the source the attacks can be categorized as internal and external, on the basis of behavior the attacks can be either Passive and Active attack [6].

1.1.1 Attack on the basis of the source

In an internal attack on the network the attacker gains unauthorized access and behave as a authorized node. Internal attacks are performed by compromised nodes that are part of the set of connections. Traffic analysis can be done and attacker may participate in the activities of other network.

The external attack is carried out by the nodes which are not part of a network and wants to get access to the network [7]. When these nodes are successful in accessing the network, they disrupt the performance of the whole network by injecting fake packets in the network.

1.1.2 Attack on the basis of the behavior

PASSIVE ATTACKS:-

A passive attack obtains data substitution in the web without disturbing the communicated operation. In this type of attack confidentiality of the network is compromised and these attacks are difficult to detect. Some examples of this type of attack are snooping and eavesdropping. A passive voice plane of attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates the data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from the routed traffic.

ACTIVE ATTACKS:-

An active attack is that attack in which any data or information is inserted into the web so that information and procedyre may impairment. The integrity of the network is compromised in this type of attack. It involves modification, manufacturing and disruption and affects the cognitive operation of the network. Examples of active attacks are spoofing, masquerading [8].Active attacks are very severs attacks on the network that prevent message flow between the nodes. However active attacks are internal or external. Active external attacks can be carried out by out side source that do not belong to the network. Internal attacks are from malicious nodes which are the parts of severe and hard to detect than external attacks. These attacks generate unauthorized access to network that helps the attackers to make change such as modification of packets, DOS, congestion etc.

Active attacks are classified into three types:-

Dropping Attacks:-

Compromised node or selfish node can drop all packets that are not designed for them. Dropping attacks can prevent end-to-end communication between nodes. The malicious router can also accomplish this flak selectively, e.g. by dropping packets for a particular network terminus, at a certain fourth dimension of the day, a package every *n* packets boat or every *t* seconds, or a randomly selected portion of the parcel. This is rather called a **greyhound attack**. If the malicious router Endeavour to drop all packets that come in, the attack can actually be discovered fairly quickly through commons networking tools such as trace route. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding table and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific sentence period or over every *n* packets, it is often harder to detect because some traffic still flows across the network.

Modification attack:-

In a message qualifying attack, an interloper alters packet header addresses to direct a message to a different destination or modify the information on a target machine. These attacks modify packets ans disrupts the overall communication between network nodes. E.g. sinkhole attack.

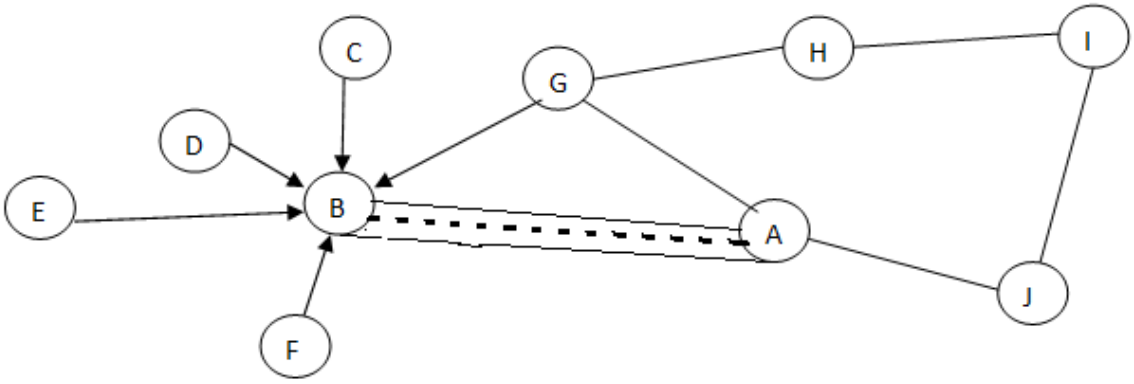
Fabrication Attacks:-

In fabrication attack, the attacker send fake substance to the neighboring nodes without receiving any related message. A **fabrication attack** seeks to create illegitimate information, processes, communications or other information within a organization. Fabricated information is deliberately inserted right alongside authentic data. When a known system is compromised, assaulter may use fabrication technique to addition trustingness, create a false record lead, collect data for illicit use, spawn malicious or extraneous processes. In addition, fabricated data may reduce confidence in genuine data with the affected system [10].

1.2 Worm hole Attack

Wormhole attack is the attack where two nodes that are remote and connected by a tunnel giving an illusion that they are neighbors. Each of these nodes receive route request and topology control messages from the network and send it to the other node via tunnel which will then replay it into the network from there. By using this extra tunnel, these nodes are able to announce that they have the shortest path through them. Once this link is established, the attackers may choose each other as multipoint relays which then lead to an exchange of some topology control messages and data packets through the wormhole tunnel. Since these MPRs ahead defective topology information, it results in distribution of inaccurate topology information throughout the network. On receiving this false information, other knob may send their messages through them for fast delivery. Thus, it prevents honest intermediate nodes from establishing link between the author and the destination. Sometimes, due to this, even a wormhole attacker may fall victim to its own success [3].

In wormhole, a tunnel between two points in the network is creates by an attacker and creates straight link between them as they are straight associated. Here A and B are the two end-points in the wormhole tunnel. A is the germ leaf node and B is the destination node. Node A is presumptuous that here present a direct connection to node B so node A will start transmission using tunnel created by the attacker .This tunnel can be produced by numeral ways including long-range wireless transmission .Wormhole attacker report regarding each packets at one end in the network and tunnels them to other end-point in the network. This attack consists of the security of networks. When a wormhole plan of attack is used against AODV, than all the bundle will be transmitted through this burrow and no other path will be discovered. Every node sends RREQ messages by using its neighbor node list to destination. If the source does not obtain reverse the RREP message from destination inside a stipulated time, it consider the existence of wormhole attack and adds that route to list.



There are two types of wormhole attack:

1.4.1Delay Sensitive

1.4.2 Throughput Sensitive

First is Delay sensitive wormhole attack in which either packets drop or transfer to other route to reach to the destination by malicious node. In throughput sensitive attack, packet dropped by the malicious node [4].

In the wormhole attacks are classified as:

1. **In-band wormhole attack:** It is the attack which require a hidden superimpose above the presented wireless medium
2. **Out-of-band wormhole attack:** It is the attack which requires a hardware guide to connect two colluding nodes.

In-band wormhole attacks are further divided as:

1. Self-sufficient wormhole attack: It is the attack where the attack is restricted to the colluding nodes.

2. Extended wormhole attack: It is the attack where the attack is unmitigated ahead of the colluding nodes. The colluding nodes attack some of its adjacent nodes and attract all the traffic received by its neighbor to pass through them.

In the second type of wormhole attacks, the intrusions are distinguished between **hidden attack**, where the network is unaware of the existence of malicious nodes and **exposed attack,** where the network is aware of the presence of nodes but cannot recognize malicious nodes along with them.

Wormhole attack is one of the most sophisticated and severe attacks in MANEs. In this attack, a pair of colluding attackers record packets at one location to reply them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communication that provide authenticity and confidentiality [5].

There have been recently to protect networks from wormhole attack:

Geographical leashes and temporal leashes:-

Leashes are added to each packet order to restrict distance the packets are allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new trey. A geographical leash is intended to limit the distance between the receiver of a packet. A temporal dence-ace provides an upper bind on the lifetime of a parcel.

Using directional antenna:-

Using directional restricted the direction of signal propagation through air. This is one of the crude ways of limiting packet dispersion [17].

1.3 AODV ROUTING PROTOCOL

AODV stands for Ad-Hoc On Demand Distance Vector routing protocol, On Demand routing protocol are mostly used in Ad-Hoc networks. All the routes are discovered only when needed, and are maintained as long as they are being used. Routes are discover through a route discovery cycle, where by the networks odes are queried in search of a route to the destination node. Each mobile host operates as a specialized router and routes are obtained as needed with little or no reliance on periodic advertisements. Ad hoc on demand distance vector is a reactive, distance vector routing protocol. It uses the sequence numbers to avoid routing loops and indicates the “newness” of routes[18]. It is pure on-demand routing protocol for sending message to destination, it broadcast RREQ message to its immediate neighbors. The neighbors In turns rebroadcast them to their neighbors[19]. Upon receiving the fires RREQ message from the source node, if send a RREP message from the source node following the same reverse path.

AODV developed specially for MANET. It obtains the routes purely on-demand which makes it a very useful and desired algorithm for MANET. AODV use two different operations to find and maintain routes : the route discovery process operation and the route maintenance operation[20]. The broader cast identifier and the source ID are used to detect whether the node has received the route request message previously. It prevents redundant request receive in same node. The source node might girt more then one reply, in which case it will determine later which message will be selected based on the hop counts. When a link break down for example due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable due to the loss of the link. It then creates a route error (RREQ) message which lists all of these lost destination. The lymph node sends the RERR upstream towards the source node. Once the source receive the RERR, it reinitiates route discovery if it still requires route[21].

LITERATURE SURVEY

D. Sasirekha, Dr. N. Radha(2017) The inherent characteristics of Mobile Ad hoc network (MANET) such as dynamic topology, limited bandwidth, limited power supply, infrastructure less network make themselves attractive for a wide spectrum of applications and vulnerable to security attacks. Sinkhole attack is the most disruptive routing layer attack. Sink gob guest nodes attract all the traffic towards them to setup further active agent tone-beginning such as Black hole, Gray hole and wormhole attacks. Sinkhole leaf nodes need to be isolated from the edouard Manet as early as possible. In this paper , an effective

mechanism is proposed to prevent and detect sinkhole and wormhole attacks in Manet. The proposed study detects and punishes the assailant knob using different techniques such as node connivance technique, which classifies a node as an attacker node only with the concord with the neighboring nodes.

Jayrajsinh K. Jadeja, Naren Tada (2013) explained [2] that an ad hoc network is the temporary network which has no fixed infrastructure. It is also called as infrastructure less network. Each mobile node functions as base station and as router forwarding packets for other mobile nodes in electronic network. From all the attacks, wormhole attack is the most dangerous attack. In this attack an attacker confine the packets at one node in the network and forward it to the attacker node through tunnels at a distant location and it is recognized by number of ways like using high power transmission, packet encapsulation, or by using direct antennas. Wormhole attack is so sturdy and detection of this attack is tough. This attack may lead to the attack that is sinkhole attack and wormhole attack. In this paper we are going to review some methods in wormhole detection and investigate the weaknesses and strength of the method**.**

Nishant Sharma , Upinderpal Singh (2014), various approaches [3] to detect wormhole attack in wireless sensor networks 2014 in this paper they described wireless sensor networks is an emerging technology that shows great promise for various futuristic application for both mass public and military, these small, low cost, low-powers, multifunctional sensor nodes can communicate in short distances. There is currently enormous research potential in the field of wireless sensor network is created by the size of sensor network is created by its size of sensors, consequently the processing power, memory and type of task expected from the sensors. Among various attacks in wireless sensor, In a wormhole attack, a pair of attacker from the 'tunnels' to transfer the data packets and replays them into the network. This paper provide a survey on wormhole attack and its counter measures and a proposed scheme has been described that can detect and prevent wormhole attack in wireless sensor network.

Chiu et al , 2006 introduce a simple delay analysis approach, DelPHI [4], which calculates the mean value of the delay per hop for every possible route, based on sender initiation of detection packets, such as route requests (RREQ) and response by the liquidator to every received detection packet. After collecting all answer, the transmitter computes the mean value of the delay per 3 sence of hop for each packet, with the permise that a wormhole would have more hops than its hop count would indicate. The scheme then analyzes computed delays to determine if there is a large difference of opinion between any two of the values. As this scheme does not employment any confidentiality or hallmark service, an attacker can easily deceive the transmitter.

Hu, Y.-C (2006) introduced a packet leash [5] is an approach in which some data is put to restrict the maximum transmission distance of packet. Mainly two ways are there for packet leashes: geographic leash and temporal three. In geographic three, when a node A sends a packet to another node B, the node must contain its location information and sending time into the packet. B can estimate the distance between them. The geographic three computes an upper bound on the distance, whereas the temporal three ensures that a packet has an upper bound on its lifespan. Nodes are temporary synchronized in it. The utmost difference between any two nodes' clocks is surrounded by Δ, and this value should be known to all the nodes. By using system of measurement, each node checks the termination clip in the mail boat and determine whether or not wormhole attempt have occurred. If a mail boat receiving time exceed the expiration time, the packet is discarded.

Conclusion

In this paper, it is concluded mobile ad hoc network is the decentralized type of network in which malicious nodes enter the network and trigger various type of attacks. The selective forwarding attack is the active type of attack in which malicious nodes drop some packets and forward some of the packets. In future, technique will be proposed which isolate malicious nodes from the network

References

[1] Dr. Sasirekha, Dr. N. Radha "Secure And Attack Aware Routing In Mobile Ad Hoc Networks Against Wormhole And Sinkhole Attacks", 5090-5013 2017 IEEE.

[2] Jayrajsinh K. Jadeja, Naren Tada, A Review on Detection of Wormhole Attack in Mobile Ad hoc Networks", A Review on Detection of Wormhole Attack in Mobile Ad-hoc Networks | ISSN: 2321-9939 2013

[3] Nishant Sharma , Upinderpal Singh, "Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 29-33

[4] H.S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," in Proc. International Symposium on Wireless Pervasive computing, Phuket, Thailand, pp. 1-6, 2006.

[5] Hu, Yang, David B Johnson , "Wormhole Attacks in Wireless Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[6] Vrutik shah, and Dr.Nilesh Modi, "Responsive Parameter Based Antiworm Approach to Prevent Wormhole Attack in Adhoc Network", 2014

[7] Rashmi Vijaywargiya , Prof. Kamlesh Chopra "Comparative Study of Various Method of Detection of Wormhole Attack in MANETS, international journal of research in engineering technology and management,ISSN 2347-7539.

[8] Yurong Xu, Guanling Chan, James Ford, Fillia Makedon. F(2007),distributed wormhole attack detection in wireless sensor networks.

[9] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M "An Overview of Security Problem in MANET",International Journal of Advanced Research in Computer Science and mobile computing.

[10] Aarti and Dr. S.S Tyagi "Study of MANETS: "Characterstics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering.

[11] Samiksha Suri" Different methods and approaches for the detection and removal of Wormhole Attack in MANETS ", International journal of Engineering and technical research(IJETR), ISSN:2321-0869, VOLUME-1, Issue-5,July 2013.

[12] J.-P. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," in Proc. ACM Symp. Mobile Ad Hoc Netw. Comput., Oct. 2001, pp. 146–155.

[13] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in Mobile Computing, T. Imielinski and H. Korth, Eds. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181

[14] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in Proc. ACM Workshop Wireless Security, Oct. 2004, pp. 51–60.

[15] Asha and Dr. G. Mahadevan, "An Improvised scheme for cross-layer optimization to support QoS in MANET," in 2017 International conference for convergence in Technology IEEE 5090-4307.

[16] G. Arulkumar and R. K. Gnanamurthy, "Improving Reliability against Security Attacks by Identifying Reliance Node in MANET," in Journal of advance computer networks, vol. 2, no. 2, june 2014.

[17] Aniruddha Bhattacharyya, Arnab Banerjee, Dipayan Bose, Himadri Nath Saha, Debika Bhattacharjee," Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques," .

[18] Kirandeep Kaur ans Parminder Singh, " Comparitive Analysis of AODV ans LEACH Protocol in WSN," in Imperial Journal if Interdisciplinary Research(IJIR) ISSN:2454-1362 Vol. 3, issue-4, 2017.

[19] Rashmi Maulik and Nabendu Chaki," A Study on Wormhole Attacks in MANET," International Journal of Computer Information System and Industrial Management Applications, ISSN 2150-7988, Vol-3(2011), pp. 271-279.

[20] Asma Ahmed, A. Hanan, Izzeldin Osman,"AODV Routin Protocol Working Process," in Journal of Convergence Information Technology(JCIT). Vol-, Nom-2, March.

[21] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre," Black-hole and Wormhole Attack in Routing Protocol AODV in MANET," in ," International Journal of Computer Science, Engineering and Applications, Vol-2, no.-1, feb 2012.