A Review on Different Security Attack in Mobile Ad Hoc Network

Chitra Gupta[1]
[1]Department of Computer Science & Engineering
[1]GITS Gwalior Gwalior, India

Abstract— In MANET security is an important aspect between mobile nodes. Mobile Ad hoc network is an infrastructureless self –organized network without a central coordinator, changes its topology frequently. In absence of any central coordination mechanism manet becomes more vulnerable to cyber-attacks then wired network. In Ad hoc network attacks are classified as active and passive attacks. In this paper, we have presented a survey on worm hole attack in manet. An overview of manet, security goals, their challenges and various types of attack in manet and also present a detailed on worm hole attack in manet.

Key words: Black Hole, Worm Hole, Gray Hole, AODV

I. INTRODUCTION

MANET (Mobile Ad-hoc Network) is a self-organized network, without a central coordinator, and it frequently changes its topology[1] MANET is a set of sensor nodes. Which are without any access point directly communicated with each other [2]. Mobile Ad-hoc Network has no any static organization. All Nodes are communicated with each other using multi-hop or hop by hop mechanism in the network.[3] Mobile Ad-hoc Network is originally inspired by military applications such as battlefield monitoring and border surveillance. Nowadays Mobile Ad-hoc Network can be used in many citizen applications, containing traffic control, healthcare, habitat/environment monitoring and home automation. [4] In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established.fig. of manet is shown below.

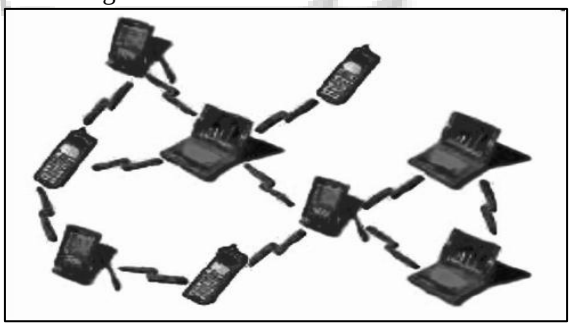

Fig. 1:

Mobile ad hoc network has many attack issue one of them is worm hole attack.

Here we are focusing on a particular kind of attack called wormhole attack which is considered as a severe attack in MANET. Minimum two malicious nodes are required to perform this attack; more than two malicious nodes are also used to perform this attack. In this attack the two malicious nodes resides in the two ends of the network and they form a link between them using an out-of-band hidden channel like wired link, packet encapsulation or high power radio transmission range[5][6]. After they form a tunnel between them as shown in figure 1, whenever a malicious node receives packets it tunnels them to the other malicious node and in turn it broadcasts the packet there. Since the packet is travelling through the tunnel it reaches the destination speeder than other route and moreover the hop count through this path is going to be less so this path is established between the source and the destination [5][7]. Once the path is established between the source and the destination through wormhole link they can misbehave in many ways in the network like continuously dropping the packets, selective dropping the packets, analyzing the traffic and performing Denial of Service attack. Wormhole attacks are divided into two types based on the behaviour of the malicious nodes; they are hidden attacks and exposed attacks. In the former one the malicious nodes do not update the packet header with their identities like MAC address, this keeps the malicious nodes invisible to the outside world but where as in the later one the malicious nodes update the packet header with their identities this makes them look like normal nodes in the network.

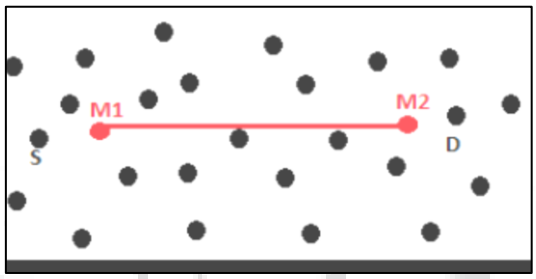

Fig. 2:

S Source
D Destination
M1 Malicious node 1
M2 Malicious node 2
Wormhole tunnel

Fig. 1: Mobile ad hoc network with wormhole link.

In this type of attack, two colluding malicious nodes create a tunnel between them using a private high speed network(s). This attack allows any node to short-circuit the usual flow of a routing information. The attacker at one end collects the data and replays them at the other end using tunnel [8]

II. SECURITY GOALS

The following are five major security goals which require preventing from attacks [2]:

A. Authentication:

Authentication ensures that the communication or transmission of data is done only by the authorized nodes.[5] Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes.

B. Availability:

Availability ensures the services should be available even in the presence of the attacks. Systems should be able to take care of various attacks such as denial of services, energy starvation attacks, and node misbehavior.

C. Confidentiality:

Confidentiality ensures that data should be accessible only to the intended party. No other node except sender and receiver node can read the information. This is implemented through data encryption techniques.

D. Integrity:

Integrity ensures transmitted data is not being altered by any other malicious node.

E. Non-Repudiation:

Non-repudiation ensures that neither a sender nor a receiver should not deny a transmitted message.

III. CHALLENGES IN MANET

A. Power Awareness:

Since the nodes in an Ad-hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements. The significant quality of cluster based routing is that it create dynamic topology those appear in less dynamic. For implementing dynamic hybrid routing scheme, efficient clustering algorithms desined [9].

B. Dynamic Topology:

The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time [9].

C. Quality of Service (Qos)

Providing constant QoS for different multimedia services in frequently changing environment.

D. Multicast Routing:

Designing of multicast routing protocol for a constantly changing MANET environment.

E. Security:

Security in an Ad-hoc network is extremely important in scenarios such as a battlefield. The five goals of security – availability, confidentiality, integrity the network participate equaliy in packets.

F. Distributed Network:

A MANET is a distributed wireless network without any fixed infrastructure

IV. PROTOCOLS FOR MANET [10]

A. Ad Hoc On-Demand Distance Vector Routing (AODV):

It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. When the valid route is not known by the source node, it initializes a route detection procedure by the broadcasting a Route Request (RREQ) to its neighbours. Each node discards Route Requests (RREQs) it has already seen by checking the Broadcast ID and the Sequence Number which had been included into the Route Request (RREQ) .

B. DSR (Dynamic Source Routing):

Determining source routes require accumulating the address of all devices between the source and destination during the finding of a route. The accumulated path info is cached with nodes processing the route finding packets. The learned routes are used to route packets. To accomplish source routing, the routed packets collect the address of all device the packet will traverse.

C. Zone Routing Protocol:

Zone routing protocol combines Proactive protocol features and Reactive protocol features. All nodes within hop distance at most d from a node X are said to be in the routing zone of node X. All nodes at hop distance exactly d are said to be peripheral nodes of node X's routing zone. In Zone Routing Protocol Intra-zone routing involves maintaining state information for links within a short distance from any given node whereas Inter-zone routing involves using a route discovery protocol for determining routes to far away nodes.

V. VARIOUS ATTACKS IN MANET [3]

There are few examples of attacks in MANET (Mobile Ad-hoc Network) routing protocols.

A. Black Hole Attack:

In black hole attack, the routing protocols are used by a malicious node to display itself as the shortest path to the node whose packet they want to the intercept. The attacker catch the traffic destined for another nodes and then select to drop packets to perform different attacks , alternatively use its route as the head phase in a man-in-the-middle (MITM) attack by redirecting the packets to the nodes imagining to bethetarget.

B. Spoofing:

A node may be attempt to take over the unique identity of other node. It then attempts to get every packet destined to the legitimate node, may present false routes. This attack can be disallowed simply by requiring every node to sign every routing message. Signing every information may growth the bandwidth overhead and the CPU operation on every node.

C. Modifying Routing Packets in Transit:

In this node changes its routing knowledge sent by another node. Such operations perform with the intention of misleading other nodes. For example, series no. in the routing protocols such as Ad Hoc On-Demand Distance Vector Routing are applied for representing the cleanness of routes. Nodes can launch attacks by the changing series no. so that new route announcements are unnoticed.

D. Packet Dropping:

A node may promote routes through it to numerous another nodes and may start reducing the received packets rather than promoting them to the another hop which is based on routes promoted. Another difference of this attack is when any node falls packets holding routing knowledge. Such kinds of attack are the case of packet dropping attacks.

E. Wormhole Attack:

In this attack an attacker receives packets from one position and tunnels to other position. When routing messages are tunneled , such tunneling between two colluding nodes is distrupted by routing attack and it is called wormhole.

F. Rushing Attack:

In this case, an adversary can be rush few routing packets towards the target, leading to difficulties with the routing. Among entirely this attack, wormhole attack is the much hard to discover because of it does not want any cryptographic break. Without knowing any secure material am attacker can launch the attack.

VI. WORMHOLE ATTACK

In MANET wormhole refers to an attack on routing protocols in which colluding nodes creates an illusion that two remote regions of a MANET are directly linked through nodes that appear to be neighbors but are actually distant from one another [11][12]. In a wormhole attack, an attacker obtains packets at any one point in the network, "tunnels" them to another point in the network, and then replace them into the network from that point [11][13]. Indeed, a wormhole attack is feasible even when the network infrastructure provides confidentiality and authenticity, and the attacker does not have the cryptographic keys. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multi hop route through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole. However, the wormhole sets the attacker in a most powerful position relative to another nodes in the network, and the attacker could exploit this position in a variety of ways [2]. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node.

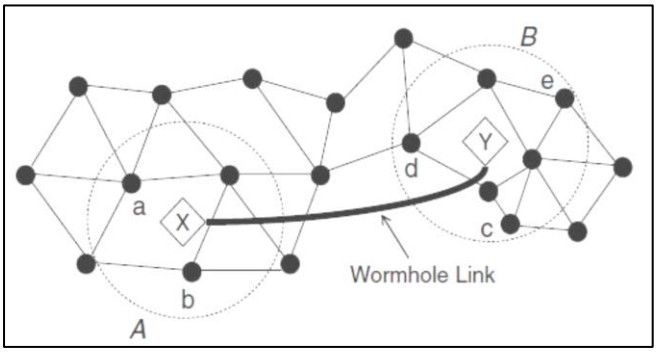

Fig. 3: Wormhole Attack

Fig. 2 shows Demonstration of a wormhole attack where X and Y denote the wormhole nodes connected through a long wormhole link. As a result of the attack, nodes in Area A consider nodes in Area B their neighbors and vice versa [10].

VII. LITERATURE REVIEW

Susheel Kumar et,al 2012[9] in this paper they present a review on worm hole attack I Manet and We can't say one result is applicable to every conditions. so there is select of results obtainable based on cos,need of secure, kind of the network . Implementing more hardware for growing secure may lead good result ,but can be costly , which may affect other networks need. Similarly some network require more security like military area network as compare to just local communication network, it also depending on network type like wireless sensor network have less mobility and can be described in some standard model ,but most of other mobile ad hoc network are of infrastructure less ,in this way we can say the choice of detection method depend upon different situation.

Jyoti Thalor et.al [2013],[11] surveyed the existing approaches which can help to design a new approach for detecting the wormhole attack in Mobile Ad Hoc network. Overall a significant amount of the work has been done on resolving problem of wormhole attack. There is choice of solution available based on cost, need of safety may lead healthier result, but can be expensive, which may disturb other networks need. Similarly some network requires more security like military area network. A standard solution is still lacking, although several very useful solutions applicable to some networks have been described.

Pranjali D. Nikam[2] MANET is a set of Wireless mobile node which is the dynamically moves from one aera to another aera. The presentation of the Mobile Ad-hoc Network and Wireless sensor networks should be degraded. Because of the damage of no. of the packets and disobedience of nodes at the time communication. Mischievous nodes modified packets and drop the packets at the time of document transmission between sources to endpoints. It should change the packets and routing paths in network. Dos attacks, Wormhole attacks, Black hole attacks directly effect on the networks presentation. Always passive attacks on the Mobile Ad-hoc Network. In this paper, we have to do studies on the various classes of attacks on Routing Protocols in Mobile Ad-hoc Network. Here an author shows the MANET is doubtful networks due to its dynamic nature. Few writers use the IDS Method to intrusion finding and also prevention on the network. So this paper is very perfect for implementing and design a novel hybrid protocol or algorithm for recover the prevent and security the malicious nodes.

Bipin N. Patel1[3], in MANET security is very important..in comparison to all attack worm hole is very dangerous because there is no need to require any cryptographic secretand completely disturb the routing process. And presented various existing process to findout wormhole attack in mobile ad hoc networks. No. of result have been proposed to the detect wormhole attack, but still it is an any active search feild.

BaltejKaur Saluja[1], Ad Hoc Networks is an area that is being widely researched nowadays and is a very fast increasing area. Power Control is a major area of rise and also they need to be made more secure. Ad Hoc Networks started to be implemented in the field today in battle_fields and also in disaster struck areas. As time goes by he can see more applications of Ad Hoc Networks various schemes of detection and prevention of the wormhole attack has been

discussed. In wormhole attacks, the detection of adversaries replay for genuine data packets is quite complicated.

VIII. CONCLUSION

MANET (Mobile Ad-hoc Network) is a self-structure network, without a central coordinator, and it frequently changes its topology. Wormhole attacks are significant difficulties that need to be addressed in wireless network secure. In the research community security in ad hoc network gained some popularity. In this paper, present a survey on worm hole attack in manet. An overview of manet, security goals, their challenges and various types of attack in manet and also present a detailed on worm hole attack in manet. Also a review of various researchers is also present in this survey paper.

REFERENCES

[1] Gurjinder Kaur, V.K.Jain, Yogesh Chaba," Wormhole Attacks: Performance Evaluation of On Demand Routing Protocols in Mobile Adhoc Networks" 978-1-4673-0126-8/11/$26.00_c 2011 IEEE 1155.
[2] Pranjali D. Nikam, Vanita Raut, "Attacks Prevention and Detection Techniques In MANET: A Survey" Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 11(Version 2), November 2014, pp.15-19.
[3] Bipin N. Patel1, Prof. Tushar S. Patel2" A Survey on Detecting Wormhole Attack in Manet" Int. Journal of Engineering Research and Application ISSN : 2248-9622, Vol. 4, Issue 3(Version 1), March 2014, pp.653-656 .
[4] Mohini Gupta, Amit Kanungo" A Survey of Different Techniques for Detectionof Wormhole Attack in Wireless Sensor Network" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.
[5] V. Karthik Raju, K. Vinay Kumar, "A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks" 2012 International Conference on Computing Sciences.
[6] Azer, M.A., El-Kassas S.M., Hassan, A.W.F., El-Soudani M.S., "Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a proposed Decentralized Scheme Marianne " IEEE Third International conference on Availability, Reliability and Security, 2008.
[7] Reshmi Maulik, Nabendu Chaki "A comprehensive review on wormhole attacks in MANET" International Conference on Computer Information Systems and Industrail Management Applications (CISIM) 2010.
[8] Gajendra Singh, Amrita Gayakwad, "An Attacker Misbehavior and Security Schemes to Protect MANET: A Survey" International Journal of Advanced Research in Computer Science and Software Engineering; Volume 4, Issue 11, November 2014.
[9] Mr. Susheel Kumar1, Vishal Pahal2, Sachin Garg3," Wormhole attack in Mobile Ad Hoc Networks: A Review"; IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No. 2, April 2012.
[10] Vikas Solomon Abel, "Survey of Attacks on Mobile AdhocWireless Networks" International Journal on Computer Science and Engineering (IJCSE).
[11] Akanksha Gupta, Anuj K.Gupta" Detection and Prevention of Wormhole Attack Using Decentralized Mechanism" International Journal of Latest Trends in Engineering and Technology (IJLTET).
[12] Jyoti Thalor, Ms. Monika, "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review", Volume 3, Issue 2, February 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
[13] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE.

