International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-6 Issue-3, February 2017

Security Attacks in MANETS (Survey Prospective)

Shaik Noor Mohammad

Abstract: ***Mobile Adhoc Network (MANET) is a dynamic, foundation less Network comprising of agroup of dynamic nodes which communicate with each other. Such networks find application in real-life environment as communication in Battlefields and communication among rescue personnel in disaster affected areas. Recently, mobile ad-hoc networks (MANETs) have gained the attention of research community due to increased adoption of its usage in real life applications. Due to fundamental characteristic of being Adhoc and insecure medium the most challenging job in MANETS is security. In this paper we present a brief survey of security attacks and existing prevention techniques.***

Keywords: Mobile Adhoc Network (MANET), Security, Attacks, Routing, Mobile nodes, Dynamic Topology

I. INTRODUCTION

MANET is an autonomous system of mobile nodes connected through wireless links. It does not have any fixed infrastructure. Here, each intermediary node in the network acts as a router. MANET has useful properties such as adaptability, flexibility and keeps up the availability between devices when a node moves from one point to other. Other property is route discovery to neighbour so that the data packets can be routed from source node to neighbouring node till data reaches destination node.

They have typical features such as inconsistency of wireless links between nodes due to limited energy supply for the mobility of the nodes; the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants. Dynamic Network Topology is another limitation. In MANETs, nodes can add into and leave from the network dynamically and can move independently. Due to such type nature there is no fixed set of topology work in MANETs. The nodes without any physical protection may become malicious node and reduce the network performance. Due to these basic attributes like dynamic topology, wireless medium and limitations in bandwidth they are more exposed to malicious attacks [11]. The researchers are mainly working on establishing the secure and shortest route for nodes to carry data in a dynamic environment with minimum energy, bandwidth and cost [8].

Routing protocols are basically a standard that choose the node behaviour in routing the information from one node to another. Routing protocols are classified as Distance Vector Protocol and Link State protocol. In Distance Vector protocols router maintains information of its neighbours and based on it calculate the cost. One of the Distance Vector routing protocol is AODV.

The topology of the entire network can be built with Link State Protocol for route calculations and choosing the best path. The power and memory consumption of these protocols is more. The examples of these protocols are OLSR and DSR.

The Routing protocols are further classified into three types: Proactive, Reactive and Hybrid. Proactive routing protocol is also known as table driven protocol because here each node maintains routing table periodically. OLSR is an example of proactive routing protocol Reactive routing protocol is known as On-Demand routing protocol because here route is only determined when it is necessary.

DSR and AODV are the examples of it. The combination of Proactive and Reactive routing is called Hybrid routing. First proactive routing is used to collect the unknown routing information and then the reactive routing is used to keep the information when network topology changes. ZRP (Zone Routing Protocol) is one of the examples of hybrid protocols. Researchers are trying to overcome routing and security issues. Out of these issues we focus on security attacks [17].

The rest of the paper is organized as follows, in section 2 we are presenting the various network attacks and their classification. In section 3 art of work have been analyzed as per as prevention of attacks are concerned, and we conclude our paper in section 4

II. TYPES OF ATTACKS IN NETWORK LAYER

Attacks in MANETS are classified as Active and Passive attacks. The attack in which the authorized node (attacker) alters or destroys the data that is to be communicated in the network is called as Active attack. The attack in which unauthorized node gets the data without disturbing the network operation is called as passive attack.

Security issues have been studied in the recent years such as Black hole attack [16], snooping attack, wormhole attack, packet replication, routing table overflow, poisoning attacks, denial of service (DoS) attacks, packet replication, and distributed Denial of Service attacks (DDoS) [17]. Some of the researchers have proposed their ideas on secure routing [13-15] to solve this issue, but the security issue is still a major problem. Classification of attacks can be done on layered basis. Each layer faces different kind of attacks. Table1shows the common attacks on various layers of MANETS.

Manuscript published on 28 February 2017.
* Correspondence Author (s)

Shaik Noor Mohammad, Research Scholar, Department of Electronics & Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences, Sehore, Bhopal (M.P). India.

Table 1 Common attack on MANETs

S. No	Layer	Attacks
1.	Physical layer	eavesdropping, Jamming, interceptions
2.	Data link layer	monitoring , Traffic analysis
3	Network layer	Black hole, Wormhole, Gray hole, Byzantine, message tempering, resource consumption, Flooding, location disclosure attacks
4.	Transport layer	SYN Flooding ,Session hijacking
5.	Multiple layer	man-in-the-middle attack, Denial of Service (DoS)

A. *Black Hole Attack:*

Black hole attack is a type of Denial of service (DOS) attack in MANET. Here one malicious node makes use of routing protocol to claim itself of as the shortest path to the destination node; instead of relaying the data packets to the neighbors it drops them. The Malicious node immediately sends out the fake RREP (Route Reply) to source node whenever it receives the RREQ (Route Request) from source node [9]. The RREP packet of malicious node will be received early by the source node than the RREP packet's of other nodes. Whenever the source node starts transmission of data packets to the destination node in this route the malicious node instead of forwarding data packets it will drop them all. It results in altering the behavior of the routing [16].

B. *Grey Hole Attack:*

Here the malicious node exhibits its fake behavior in multiple ways such as a malicious node will drop all the data packets for the certain time and again it will show its normal behavior by forwarding data packets to the neighboring nodes. It specifically drops the selected data packets for some time and again it starts forwarding data packets to the neighboring nodes [6]. The Grey hole Attack will highly affects the performance of the network.

C. *Worm Hole attack:*

Here an attacker node records packets of one location in the network and tunnels them to another location. This tunneling between two conspiring attackers is referred as a worm hole attack [2]. Routing can be disrupted when routing control messages are tunneled. When a worm hole attack takes place against an on demand routing protocol it prevents the discovery of any other routes other than the route in which worm hole is involved.

D. *Message Tampering:*

In this attack a malicious node will involve in the routing as an intermediate node. It will add (or) delete some bytes of data packets received by it and forward to the destination node. Due to this abnormality or destruction of network takes place.

E. *Byzantine attack:*

Here an intermediate node works alone or a set of intermediate nodes work in collusion and carry out attacks. These attacker nodes create routing loops, forwarding packets through non optimal paths or selectively dropping packets which results in disruption or degradation of routing services.

F. *Flooding Attack:*

Flooding attack can be launched by flooding the network with fake RREQ's (or) data packets leading to the congestion of the network and reduces the probability of data transmission of the authorized nodes [14]. The detection of attack is very hard and it exhausts the network resources.

G. Information Disclosure:

Here authorized node acts as malicious node. It reveals the information regarding the location of node or sometimes structure of network. It gathers the node location information such as route map, passwords, private keys and then plan further attacks. The leakage of information results in catastrophic situation in security sensitive scenarios.

H. Sleep Deprivation (or) Resource Consumption:

Here a malicious node can attempt to consume battery life by requesting excessive routing discovery or by forwarding unnecessary packets to the victim node. Due to wastage of resources the performance of the network degrades.

I). Attacks on Routing:

Here a malicious node will get into the path between the source and destination nodes it then controls the flow of network traffic. These types of attacks can change the behavior of the routing protocol in the network. There are different types of routing attacks as

1. Routing table overflow attack:

This occurs in proactive routing in which updating of routing information takes place periodically. Here the malicious node creates routes between unauthorized node and authorized nodes present in the network. It tries to make the target systems routing table to overflow. The target is to have more routes such that it can prevent creation of new routes.

2. Routing table Poisoning:

Here a malicious node in the network send fake routing updates or modify correct route update the data packets sent to other authorized nodes. This causes congestion in portions of the network, suboptimal routing and makes the network inaccessible.

3. Packet replication:

Here a malicious node replicates the data packets as a result additional consumption of bandwidth and battery power resources takes place. This causes chaos in routing process.

4. Rushing Attack:

Here the aim is to control as much network traffic [12] as possible. The compromised node which receives a RREQ packet from the source node try to distribute the packet early throughout the network before the same RREQ packet reaches the other nodes. Nodes which receive the RREQ packet from the source node consider those packets as duplicates of RREQ packets which are already received through the compromised node and drop (or) discard them.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

As a result whenever source node discovers route the malicious nodes will become as the intermediate nodes of the route. Finding secure routes will become difficult task. Detection of this kind of attacks is very difficult.

5. Route Cache poisoning:

The information regarding known routes can be maintained by each node in route cache. The information in the route cache of the node can be altered or deleted by the malicious node. This is called as route cache poisoning. It results in congestion of some part of network or inaccessibility of some part of network.

III. REVIEW OF LITERATURE

Rutvij H. Jhaveri [1] proposed a MR-AODV protocol which is modification of R-AODV. MR-AODV not only detects the black hole and grey hole nodes but also establishes safe and secure route for data transmission during the route discovery process. When a malicious node is detected the MR-AODV protocol updates the routing table with compromised node entry and rejects RREP. MR-AODV does not forward on reverse path and also it does not require any flag. The source node chooses the shortest fresher for data transmission which was indicated by RREP. After detection of misbehavior, by not forwarding RREP the MR- AODV reduces overhead.

Sanjay K. Dhurandher et al. [2] proposes GAODV protocol which is a modified AODV protocol. Here the presence of black hole can be detected by using significant control packets, CONFIRM, REPLYCONFIRM and CHCKCNFRM are used. The source node broadcasts RREQ message, the intermediate nodes send RREP message to source and then they unicast CONFIRM packet to destination node. To confirm the source node unicast CHCKCNFRM packet to destination and in reply the destination broadcasts REPLYCONFIRM packet only if the destination node receives CONFIRM and the CHCKCNFRM. A malicious node may not have route towards destination node and it cannot send CONFIRM. Thus destination can never generate response to CHCKCNFRM. Therefore Source identifies that the RREP sending node is a malicious node and it will be rejected.

Yudhvir Singh et al. [3] propose a modified DSR protocol for detection and prevention of wormhole nodes in MANET. Here by using route discovery method an alternative path can be selected. When it detects a wormhole node, it transmits the message through the path without disturbing performance of the network. The proposed method detects such malicious nodes and the paths that contain the compromised nodes. They are simply rejected and are not added into the DSR routing table so that these routes are not used in future for communication. G. Indirani et al. [4] proposed a prevention mechanism which is based on DSR algorithm that has two extensions Pathrater and Watchdog. Watchdog module identifies the compromised node by monitoring the node that whether the node is forwarding the packet message to neighboring node or not. If it is doesn't forward the packet message it is considered as compromised node. Pathrater utilizes this information of watchdog module and removes the corresponding route from the routing table and direct another shortest route available to destination by checking its route cache. If no routes are available then the Pathrater will broadcast a Route Request message to achieve a fresh route to destination node.

P. Karthikkannan et al. [5] proposed the sequence number identification method to avoid the black hole attacks in MANET. Here a unique sequence number will be given to each data packet and the recent packet must have sequence number greater than that of pervious packet. During the transmission or arrival of packet the routing table will be updated. Source node initiates transmission by broadcasting RREQ message. After the RREQ reaches the destination node, it initiates a RREP message to source, and RREP keep the previous packet-sequence-numbers which are received from the source node [5]. Similarly an intermediate node which also receives RREQ message will send RREP message to the source node enclosing previous packet sequence number received from the source node. Now if the intermediate node works as a black hole or malicious node then it will send RREP continuously to source node and since it does not have the previous packet sequence number, attacker can be identified easily.

Sapna Gambhir et al. [6] method uses PPN Prime product number for the detection and prevention of compromised node. In this method each will be assigned unique prime number. The Source node broadcasts RREQ to destination and in reply intermediate node willing to send RREP is required to provide also information of its cluster head and product of all prime numbers from destination to source. After receiving the RREP message from intermediate node the source node with the information of its cluster head will divide the PPN with the Node IDs that are stored in neighbor table at cluster head to check whether intermediate node is its reliable node. If PPN is perfectly divisible, then the intermediate node is a reliable node, else it is a compromised node. The cluster head will add it to malicious list and then broadcast it to whole network so that to remove it from the routing table.

Hizbullah Khattak et al. [7] propose to utilize the second ideal route for information packets transmission. He uses hash for avoidance of black and grey hole attacks and to maintain data integrity. Here the author rejects the very first ideal reply and chooses the second nearest RREP message to create a route from source node to destination node. By utilizing the second nearest path for packet transmission, it will be difficult for grey hole or black hole to get the placement in the network. They cannot advertise to the source node that it posses the second nearest to destination node [7]. The hash function can be used in case of presence of many malicious nodes in the network. The source node sends the hash value of message while transmission of data packets to the destination node. Once all the data packets reaches destination node it will check hash vale for equality.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

If both values are equal the there is no attack. If not equal the destination node will broadcast error message. The source node keeps this route in its routing table to avoid transmission of packets in this route in future and again broadcasts the RREQ message.

Al-Shurman et al. [10] proposed two different solutions for the detection of the black hole attack. In the first solution, one route will be selected in terms of shared hops among all received routes. T he source node can recognize the safe route to the destination from the shared hops. The main disadvantage in this approach is to force more delay on the network. In the second approach, each node will store the last-packet-sequence- numbers for the last packet received from each node and the last-packet-sequence-numbers for the last packet sent to each node. Thus the received RREP contains the last-packet-sequence-numbers received from the source node. According to these sequence numbers, the source can detect the malicious RREP.

IV. CONCLUSION AND FUTURE WORK

Security is the main concern in MANETs. Due to their fundamental properties such as dynamic topology, lack of central authority, limited resources and open access medium Wireless ad hoc networks are exposed to being attacked or harmed. These basic attributes introduce new challenges to intrusion detection technology, so it is difficult to achieve security in Adhoc network when compared to wired networks. In this paper, we first briefly summarized the MANET and popular routing protocols in it. Then, types of attacks along with a latest survey of existing solutions are discussed. Different authors have given various approaches for detection and prevention of malicious attack in MANET but every approach has its own limitation. The malicious attack is still an active research area in MANET. In future study includes intend to develop such a security algorithm, which will be installed in header of each node that helps in detection and prevention of malicious attacks.

REFERENCES

1. Rutvij H. Jhaveri, “MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs “, (254-260)2012 Third International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4941-5/12 / 2012 IEEE.
2. Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur , Prashant Khurana,” GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs”,(357-362) 2013 27th International Conference on Advanced Information Networking and Applications Workshops, 978-0-7695-4952-1/13/2013 IEEE.
3. Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak ,“Wormhole Attack Avoidance Technique in Mobile Adhoc Networks”,(283-287) 2013 Third International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4941-5/13/ 2013 IEEE.
4. Indirani, Dr. K. Selvakumar, V. Sivagamasundari, “Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence”, (152-156) Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22, 978- 1-4673-5845-3/13/2013 IEEE.
5. P.Karthikkannan, K.P.Lavanya Priya,” Reduction of Delays in Reactive Routing Protocol for Unobservable Mobile Ad-Hoc Networks”, 2013 IEEE.
6. Sapna Gambhir and Saurabh Sharma,” PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs”, (335-340) 2012 3rd IEEE International Advance Computing Conference (IACC), 978-1-4673-4529-3/12/ 2012 IEEE.
7. Hizbullah Khattak, Nizamuddin, Fahad Khurshid, Noor ul Amin, ” Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash”,(645-648) 978-1-4673-5200-0/13/2013 IEEE.
8. Roopal Lakhwani , Vikram Jain , Anand Motwani , “ Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks”, International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012.
9. Htoo Maung Nyo, Piboonlit Viriyaphol, ” Detecting and Eliminating Black Hole in AODV Routing”, 2011 IEEE, 978-1-4244-6252-0/11
10. Al-Shurman, M. Yoo, S. Park, “Black hole attack in Mobile Ad Hoc Networks”, in Proc. ACM Southeast Regional Conference, pp. 96-97, 2004.
11. Pramod Kumar Singh, Govind Sharma,” An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET”,(902-906) 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 978-0-7695-4745- 9/12/ 2012 IEEE.
12. Zhou L, Chao H-C, “Multimedia Traffic Security Architecture for the Internet of Things” IEEE Network 25(3):29–34. IEEE 2011.
13. Yang H, Lou H, Ye F, Lu S, Zhang L (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 11(1):38–47.
14. S.Nithya, S.Prema, G.Sindhu, " Security Issues & Challenging Attributes in Mobile Ad-Hoc Networks ", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 01 , P.P 1083-1087, Jan-2016
15. Wu B, Chen J, Wu J, Cardei M, “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks” In: Xiao Y,Shen X, Du D-Z (eds) Wireless Network Security. on Signals and Communication Technology. Springer, New York 2007.
16. Marti S, Giuli TJ, Lai K, Baker M, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks” 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, August 2000.
17. Hu Y-C, Perrig A, Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy 2(3):28–39, IEEE 2004.

About the Author:

Shaik Noor Mohammad is a Research Scholar in the Department of Electronics & Communication Engineering at Sri Satya Sai University of Technology and Medical Sciences, Sehore, Bhopal (Madhya Pradesh) India.