VOL. 10, NO. 13, JULY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

GEOTE LEASHES SECURITY IN MANET

V. Dhanakoti, D. Nivetha and D. Keerthika
Department of Computer Science and Engineering, SRM Valliammai Engineering College, Kancheepuram, India

ABSTRACT

The network which is infrastructure less and connecting a mobile device by wireless is called a Mobile Ad-hoc Network (MANET). Because of its fundamental characteristics like open peer-to-peer architecture, shared wireless medium, stringent resource constraints, highly dynamic network topology, nodes openness to physical capture, etc. MANET becomes vulnerable. An important service for all kind of network communications is its Security. In MANET, security service is not available. So, MANET should improve its security to make the communication confidential. This paper is about different assaults including MANET assaults and its detection schemes which are useful to avoid unwanted assaults.

Keywords: MANET, mobile Ad-hoc network, assaults, detection schemes.

1. INTRODUCTION

Mobile devices are connected by wireless links by help of a self organised system called MANET. The construction cost of MANET is very low. If the nodes are far beyond the communication range then ordinary wireless network is not possible, in this case MANET is used [1]. MANET allows intermediate nodes to pass data transmission. Based on connection of network, MANET is divided into two types single-hop and multi-hop. In source node the recipients are within the transmission range. So the communication session is successfully done through the single-hop transmission.

MANET is also called multi-hop radio networks because, if the recipient is not in the transmission range, then it is connected by intermediate nodes. For low-power the transmission range is limited and node which is outside the range will be routing a message to non-adjacent nodes. Rescue mission, mining operations, vehicle network etc are the applications. Shared wireless medium, stringent resource constraints highly dynamic network topology and open peer to peer architecture are the characteristic of MANET.

Routing of packets is necessary in MANET are divided into proactive routing and reactive routing. proactive protocols [2] are also called as table driven protocols, it possess the node to store the routing information in one or more tables and it should be consistent, the routing information should be up-to-dated for each node [2]. Reactive routing protocols are divided into optimized state routing and destination sequence distance vector.

Reactive protocols also called as source initiated on demand driven protocols. In reactive protocols, the routing table will not be updated periodically. The routed are only created when there is a need by the source node. For example, if a source node sends a packet to destination node, it selects specific path. Even though proactive and reactive protocols are sufficient, there is another type called hybrid protocols. It uses both the techniques of reactive and proactive protocols according to the specified conditions. Hybrid protocol is an optimal one.

When transmission takes place, MANETs are more vulnerable to security assaults in open medium. If security protocol is present, the various assaults can be reduced. The mobile hosts establish dynamic paths among other host to communicate. The dynamic paths will be weak at sometime, assaulter target on the weaknesses.

2. ROUTING IN MANETS

In MANET, mobile node acts as a router, so that overhanging is reduced. If the sender and receiver are within the range they can easily communicate among each other. Otherwise they make use of intermediate nodes for communication. Nodes in MANET have to determine the topology as MANET is unpredictable and dynamic in nature. A node broadcast its presence to other neighbouring nodes. This method is used by the nodes to reach its neighbouring nodes.

Immediate selection of a route without holdup is the main advantage of proactive protocols, but it has some disadvantages also. For routing information large data are maintained with higher capacity and slow action on failures are major disadvantages. Less consumption of capacity and effective route maintenance are the advantages in reactive protocols. But it takes more time to discover routes and excess flooding may also occur while routing. This leads to network congestion which is the major drawback in reactive protocols. In hybrid protocols, their efficiency differ with its number of nodes and their reaction to demand is decided by the amount of traffic in routing.

3. SECURITY ASSAULTS IN MANET AND RESEARCHES

The most important consideration for the basic performance of network is security in mobile ad-hoc network. By the assured security issues which have been met so far, we can achieve availability of network services, confidentiality of the data and integrity of the data. Due to some features like open medium, changing its topology dynamically, lagging of control monitoring and management co-operative algorithms, no clear detecting mechanisms etc. MANET often has some security assaults and threatening.

Passive assault and active assaults are the types of security assaults in MANET.

a) Passive assaults

In network data are snooped without any altering is called passive assault. Confidentiality of the system is affected and decreased by passive assaults. There is no damage or effect caused to system by this assault. So it is very hard to detect passive assaults.

1) Eavesdropping

The confidential information observed by a node can be detected and later used by a malicious node can be detected and later used by a malicious node ears dropper can fetch some important data like location, public key, private key, password etc [3], though it is a wireless medium, communication can be easily interrupted with a receiver tuned with proper frequency. Thus wireless links are easier to tap whereas classified data are ears dropped by tapping communicating lines. As shown in Figure-1.

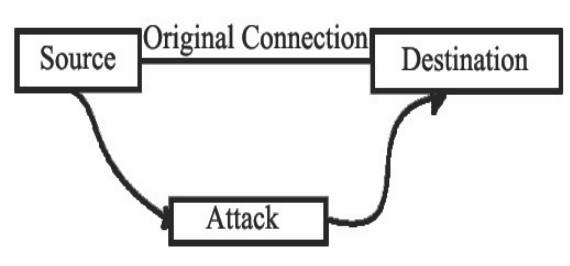

Figure-1. Eaves dropping.

2) Traffic analysis

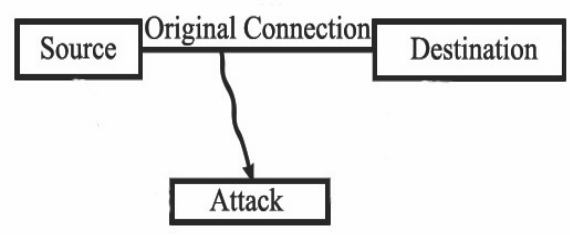

Figure-2. Traffic analysis.

Assaulter analyses the communication track between the sender and receiver. After analysing, assaulter found the data between route of sender and receiver [3]. The processes of intercepting messages are examined to derive information from patterns in communication. This can be implemented even it encrypt the messages and not decrypted. As shown in Figure-2 in network, assaulter can analyse it but cannot participate [3].

b) Active assaults

In active assault, the assaulters will try to change the data which is travelled between sender and receiver. The packets can be altered by the assaulters. Due to the alteration of the packet, it disrupt the usual function in the network. There are several kinds of active assaults. They are wormhole assault, black hole assault denial of service, sinkhole assaults, flooding assault, Sybil assault.

c) DOS assaults

In DOS assault false messages are generated by malicious node that disrupts the operation of network or resources of other nodes are consumed.

d) Wormhole assault

Wormholes assaults are dangerous and harmful to protect against even the information of routing are encrypted, confidential [4]. It can be placed without any knowledge of routing protocols and agreeing nodes [4]. It is easy to expand but really the detection is very hard. In wormhole assault the malicious nodes are sent through wireless link called wormhole link. If the nodes are outside the communication range, it can be communicated through intermediate nodes in a multi-hop way. In network the worms are encapsulated and route lengths are altered. The packets are recorded by a worm at one place and replicate them to another place to end worm. In the network, most of the packets are delivered only through these worms. The networks are connected very efficiently if the assaulter carries the tunnelling truthfully. The assaulter no need to wait for the whole packet to receive, it can send each bit over the wormhole assault, so that delay are minimized. It is assumed that captured packets are minimized and are altered by wormhole assaults. If many number of peer to peer paths are passed over wormhole link, then the wormhole assault will be stronger as shown in Figure-3.

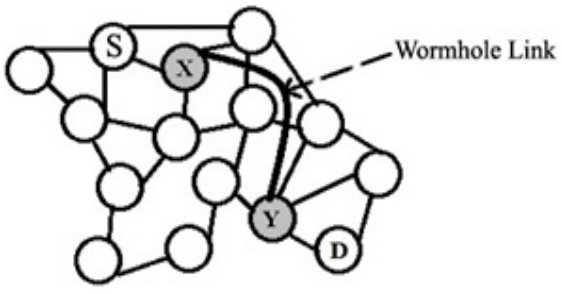

Figure-3. Wormhole assault.

e) Black hole assault

In Figure-4 black hole assault [5], flooding based routing protocol are exploited by a malicious node and destination. Node has a shortest node but before that the reply was sent by malicious node and it creates a bogus route.

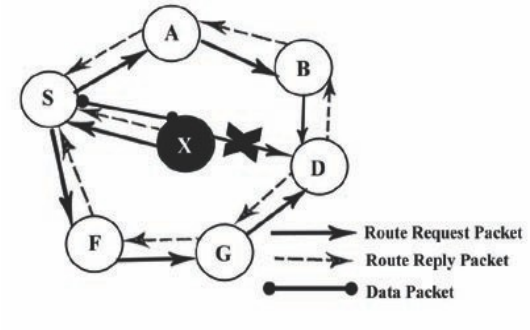

Figure-4. Blackhole assault.

The packets are intercepted by malicious node, so destination node does not receive any packets.

1) Detection/Prevention of Black hole Assault
Various approaches have been proposed to defend against a Black hole assault with their limitations.

f) Grayhole assault

Grayhole assault is an adjunction of black hole assault in which malignant nodes behaviour is considerably unstable. Generally there are 3 types of Grayhole assault [4]. First type is the malignant node may relinquish packets from some nodes but forwards to all other remaining nodes. Second type is, a node may act malignant for particular time but behave normally after some time.

Because of these, detection of this assault is a tough task. It can disturb route discovery and reduce the networks performance.

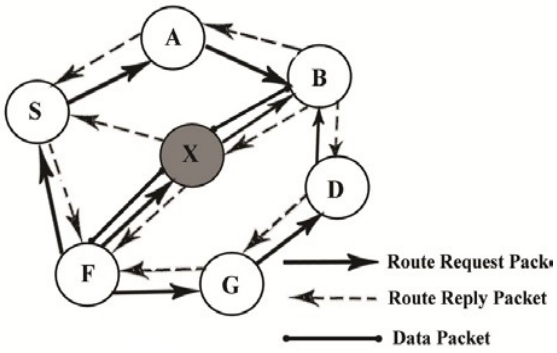

Figure-5. Grayhole assault.

g) Sinkhole assault

As shown in Figure-6 Sinkhole assault, a malignant node sends false routing information and makes itself as a unique node and receives total network traffic. After that it changes the unseen information such as changing and relinquishing of packets to make network difficult.

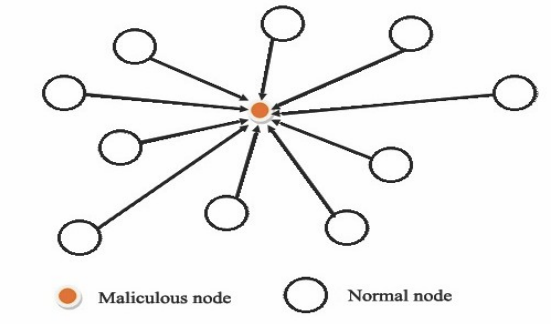

Figure-6. Sinkhole assault.

1) Sinkhole assault detection

Secure aware routing (SAR) protocol finds and prevents these assaults. In SAR, security measures are incorporated in RREQ packet itself. When any node receives this packet it checks whether it can be able to provide such security. If it cans means, then it is sent to next hop otherwise it is dropped. SAR has two security measures trust hierarchy and security capabilities.

h) Flooding assault

In this assault, assaulter aims to cause a failure in a computer system. This is done by provide inputs more than the threshold level so network users may not be able to access critical services or this may even lead to a failure of networking infrastructure [6]. A quick probing assault is one type of flooding assault. It occupies network bandwidth and pick host vulnerabilities by scanning the network within a small period of time [6]. A flooding distributed denial of service (DDOS) assault makes a host or n/w service unavailable by sending useless packets to the pray at the same time [6].

i) Sybil assault

In this, assaulter creates more than one selfhood for the single node. Its main purpose is to cause interruption to acquire more resources information etc. than single nodes ability [7].

It causes damages to ad-hoc network in many ways. For example, assaulter can interrupt the routing of multipath by participating in routing. In Sybil assault, Sybil node detection is difficult [7]. In wireless sensor networks it tries to modify the total average reading outcome by acts as a different node.

As shown in Figure-7, C is malicious node, it creates several selfhoods like A, B, D. A, B, C, D refers the same node but it looks different.

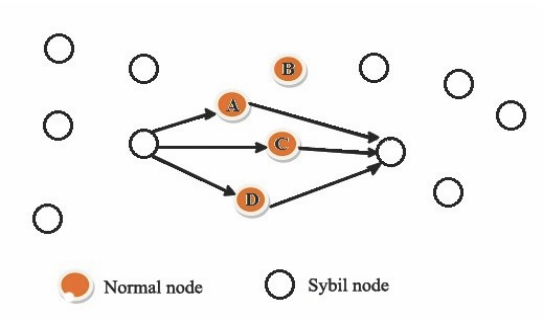

Figure-7. Sybil assault.

1) Sybil assault detection

a) Trusted certification

In this mechanism, centralized authority will provide unique identities for the node. If it fails, whole network will fail.

b) Trusted devices

Network card is associated to all of entities in ad-hoc network but assaulter may invest two or more cards. In trusted devices one network entities is mapped to one network device, so the mapping is one to one. There is no provision to stop this assignment to network devices. The nodes swap their profiles and normal behaviour is estimated using scheme called Barter, which is an admission control system and behaviour based access.

4. RUSHING ASSAULT

It is a DOS assault when assaulter receives a request for route it floods the packet fastly throughout all the nodes to make route discovery process difficult.

As shown in Figure-8, the starter node sends a route discovery to the destination. If RREQ receives the each node of the destination, then if they find any route means, they will have a hop through assaulters node (i.e.) if a neighbour node receives rushed request it will transmit that request alone and discard other request when legitimate request reaches late, it will not be able to discover any routes.

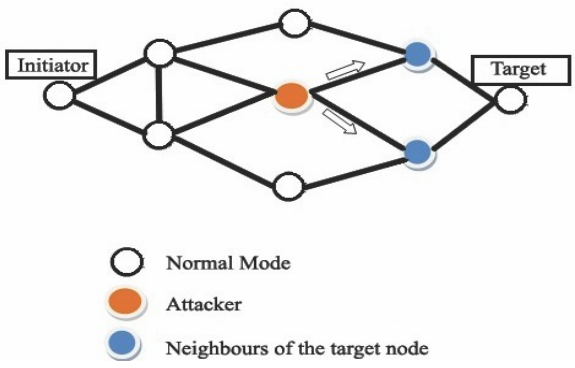

Figure-8. Rushing assault. A. Rushing assault detection.

The mechanism to safeguard against rushing assault is SND, secure path delegation, randomizes path request forwarding. In previous on-demand protocols, when B receives a broadcasted message from A then it considers A as a neighbour node. Standard Neighbour detection replaces the SND which allows to prove that each neighbour node is within the maximum capacity range [8].

Once when a node A forward a RREQ and confirms that node B is neighbour then it signs a Path Delegation message which allows node B to forward that request. When node B confirms node A is within the range then it accepts by signing Accept Delegation message. In On- Demand routing, ROUTE REQUEST messages are forwarded in order to replace the duplicates. It assures that the path which is having low latency is selected among all other paths [8].

5. PROPOSED WORK –GEOTE LEASHES

This technique is the combination of geographical leashes and temporal leashes. In this technique the packets are only accepted if it is from a certain area and the packets received should be within a time stamp. If the timestamp and geographical limit assigned are exceeded then the packets are discarded. The above conditions must be satisfied to find the malicious node. If the conditions are not satisfied then the nodes are considered to be malicious and it is discarded. Let us consider for an example the destination node receiving the packets are not within the timestamp and limit we assume that attacker has got the packet and have made some changes so that the packet is not accepted and considered to be an malicious or infected node.

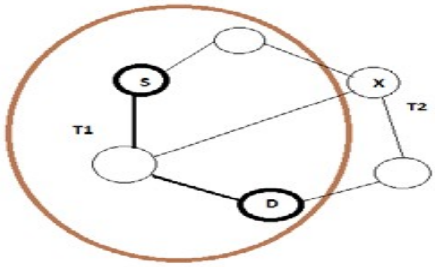

Figure-9. Geote leashes.

In the above Figure-9 sender, receiver and some other nodes are within the geographical limit. Consider the timestamp T1 and T2, T1 be the time stamp assigned for the packets send by the source node and T2 be the timestamp assigned for the packets send by an assaulter. The packets sent by the node x are verified and it is not within a timestamp and geographical limit. So the destination node will assume that packet was sent by an assaulter and it will discard the packet.

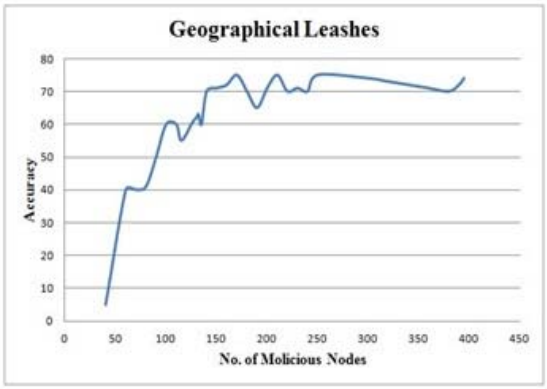

Figure-10. Geographical leashes.

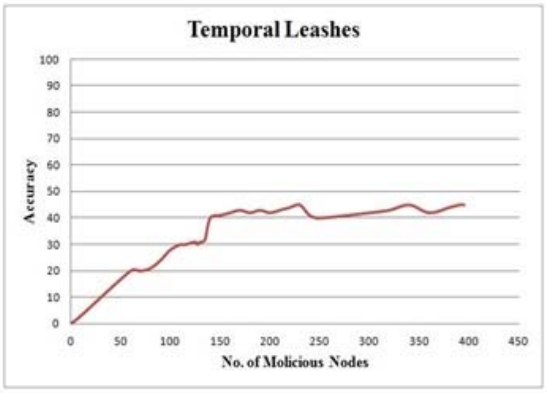

Figure-11. Temporal leashes.

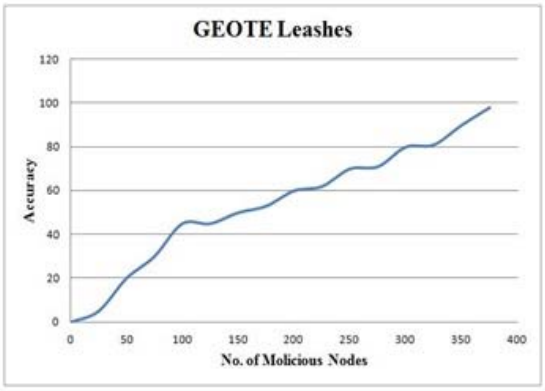

Figure-12. GEOTE leashes.

In the graph, X-axis contains number of malicious nodes and Y-axis contains the accuracy of finding the malicious nodes. In X-axis values are taken in the interval of 50 and 10 in the Y-axis.

In geographical leashes method as show in Figure-10, the first iteration finds 60 nodes as malicious nodes with accuracy of 40.Then in second iteration if finds 100 nodes with an accuracy of 60. In third iteration 192 nodes were found to be malicious with an accuracy of 90. And in final iteration it finds 240 nodes with accuracy of 60. Even though if finds large number of malicious nodes, the accuracy is very low.

In temporal leashes method as show in Figure-11, the first iteration finds 50 nodes as malicious with an accuracy of 20. Then in second iteration it finds 100 nodes as malicious with an accuracy of 30. In the third iteration it finds 195 nodes as malicious nodes with an accuracy of
48. Then in final iteration it finds 230 nodes with an accuracy of 30. In this technique it obtains a large number of malicious nodes, but it also has same drawback of geographical leashes.

In the GEOTE leashes method as shown in Figure-12, during first iteration it finds 50-100 nodes are found to be malicious with an accuracy of 20. In the Second iteration if finds 125 nodes with an accuracy of 32. Then in third iteration it finds 175 nodes as malicious with an accuracy of 48. The following process continuous for the forth coming iterations. Then in the final iteration it finds 360 malicious nodes with an accuracy of 97.99. In this technique the number of malicious nodes found to be more and the accuracy gradually increases. So the performance of GEOTE Leashes is better than the Geographical leashes and Temporal leashes. This is experimented with the help of the following tools: snort and prelude.

In the experimental verification, the results were calculated based on the accuracy of Geographical leashes techniques (GEOTE) and Temporal leashes which is shown in the above graphs.

The outcomes from the GEOTE leashes techniques were found to be higher, when compared to the individual outcome of geographical and temporal leashes. From the above experimental graph it is concluded that GEOTE leashes finds more malicious node than the previous method.

6. CONCLUSION AND FUTURE WORK

MANET is capable of deploying a network. But it is not possible in traditional network infrastructure environment. MANET has still more challenges to overcome. It has vast potential to face those future challenges. But security issues are ignored. In this paper, routing in MANET is discussed in brief and also its security issues. DoS assault the security of the network and disrupt its operations. When there is co-operation in malicious nodes then there will be more damage in networks. Research is carried out especially in black hole and Gray hole assaults of DoS assaults. The main reason for deployment of MANET network is its security features. In this paper the behaviour and challenges of security threats in mobile Ad-Hoc networks with Defence techniques were critically analyzed.

REFERENCES

[1] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, JieYang, and NeiKato. 2013. "Cluster Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Transactions on parallel and distributed systems, Vol.24, No.2.

[2] Huda Al Amri a, Mehran Abolhasana, Tadeusz Wysocki B. 2010. "Scalability of MANET routing protocols for heterogeneous and homogenous networks", Computers and Electrical Engineering.

[3] B. Wu J. Chen J. Wu and M. Cardei. 2006. "A survey on assaults and countermeasures in mobile ad hoc networks", Springer.

[4] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah. 2010. "MANET Routing Protocols and Wormhole Assault against AODV", International Journal of Computer Science and Network Security, Vol.10 No.4, pp.12-18.

[5] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park. 2004. "Black Hole Assault in Mobile Ad Hoc Networks", ACMSE, pp.96-97.

[6] Daniel S. Yeung, Shuyuan Jin and Xizhao Wang. 2007. "Covariance-Matrix Modeling and Detecting Various Flooding Assaults", IEEE Transactions on systems, man and cybertneics part A: systems and humans, Vol.37, No.2.

[7] S. Abbas, M. Merabti, D. L. Jones and K. Kifayat. 2013. "Lightweight Sybil Assault Detection in MANETs", IEEE systems journal, Vol.7, No.2.

[8] L. Tamilselvan and V. Sankaranarayanan. 2008. "Prevention of co-operative black hole assault in MANET", Journal of Networks, pp.13–20.