MANET Security Issues and Solutions: A Review

Lalita Nayak[1], Roopal Lakhwani[2]
[1, 2] Department of CSE
[1, 2] Disha Institute of Management & Technology Raipur (C.G.), India

Abstract- *Mobile ad hoc networks as we know are the latest trend in the wireless communication technology. It is because MANET has numerous advantages which makes it most suitable for applications like natural disaster affected areas, military operations, wild life study etc. As it is becoming popular and being use widely the security risk is also growing. We certainly cannot afford to compromise the security of a network life of many people is on the line for example in case of military operations or scenario of any natural disaster area. There are some loophole present in the structure of MANET implementation which if not taken care of properly, can result in vulnerable network. In this paper we have studied various attack and their available countermeasures like Intrusion Detection Techniques. Later we concluded that even after so much of research done in this area still there is chance of enhancement in detection of malicious nodes.*

Keywords- MANET, Intrusion Detection, Blackhole, Security

I. INTRODUCTION

Mobile Ad hoc NETwork (aka MANET) is a collection of moving nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or with the help of intermediate nods. In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. IBM in [cite] has defined term 'self-chop' for MANETs according to their characteristics. These characteristics are self-Configure, self-Heal, self-Optimized and self-Protected.

This paper is divided into 4 major sections, in this first section we will see the basic characteristics of MANET and why it is challenging to implement MANET and design routing protocols for MANETs.

In the next section we will focus our discussion on major security issues on MANET and various types of attacks which are most widely used by the attackers. In section III we will have overview of various security mechanism available to countermeasure different attacks. There are basically two types of IDS available signature based and anomaly based, both have their advantages and disadvantages obviously. It depends on the network that which type of IDS is suitable for a particular network designed for a particular task.

The major challenges in MANET as compared to other wired or infrastructure based network are as follows:

1) Open Communication medium

Since MANET is derived from wireless network it uses wireless medium for communication, which is neither secure nor as reliable as the wired ones. The traffic over the wireless channel is open for other devices so it can be easily tapped. Obstacles like walls, tree etc also affects the available bandwidth of channel.

2) Limited Processing power:

Since nodes used in MANET are usually small in size and do not have very high configuration processors so there is a constrain in processing capacity. If a single node is responsible for computation among multiple nodes (like in cluster based system) the head node exhausts fast as compare to other nodes. Also small processors takes more time to perform heavy calculations which in turn degrades the overall network performance.

3) Limited memory availability:

Nodes in MANET do not have high capacity storage with them because of small size. So the routing protocol must be designed in such a way that it should not keep heavy routing tables stored on the mobile nodes.

4) Limited memory availability:

Nodes in MANET do not have high capacity storage with them because of small size. So the routing protocol must be designed in such a way that it should not keep heavy routing tables stored on the mobile nodes.

5) Communication Overhead:

To communicate among nodes they must share some routing information and to establish path from one node to another these control signals are sent. This traffic is considered as an overhead on the network as they are not data packets. Since the node are moving in nature in MANET the routing information needs to be shared very frequently, this makes communication overhead a serious issue in data transfer.

6) Mobility:

As discussed above, some of the problems in MANET are majorly caused because of mobile nature of the network, so mobility is the biggest advantage of MANET but it is also root cause of several issues of the network.

II. SECURITY ISSUES WITH MANET

So far we have seen some general domain where MANET has major challenges, but another very important aspect of any network is Security. If a network is not secure enough then it is nearly useless as the communication is un-trusted. MANET is considered as less secure as compared to the traditional wired network or infrastructure based networks. There are reasons to justify the above mentioned point, MANET has issues like less processing power and low memory availability. This drawback can make any security system weak, as if one does not have good processing capacity then it is not possible to find the malicious member of the node.

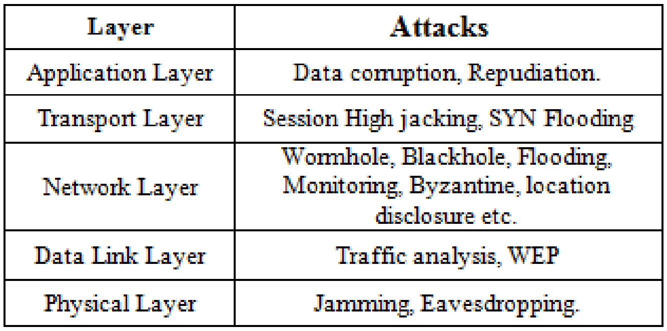
We will see these drawbacks below in brief:

1) Power: As discussed above, some of the problems in MANET are majorly caused because of mobile nature of the network, so mobility is the biggest advantage of MANET but it is also root cause of several issues of the network.
2) Memory: If a node has very small memory to store the data, it makes routing difficult (like for table driven routing protocols) and thus the nodes won't be able to have information of farthest part of the network.
3) Communication Medium: Since the channel is open anyone can intercept the packet. It responsibility of the routing protocol to make the packet un detectable or useless even if they are captured by un authorized node in between the communication.
4) Mobility: As the nodes are mobile and network architecture is changing continuously it is difficult to identify the malicious node. Also the nodes keep going out of the network area and coming back to join it, so trusting an incoming node to be genuine is a challenge for a routing protocol.

Some of the most common attacks in MANET are discussed here, it will us idea of various security loopholes present in the mobile network and how they have been exploited by attackers.

First of all we can divide the attacks on the basis of their target layers, i e in which layer of stack they attacks. It is classified as follows:

Table 1. Classification of Attacks in different layers



Layer	Attacks
Application Layer	Data corruption, Repudiation.
Transport Layer	Session High jacking, SYN Flooding
Network Layer	Wormhole, Blackhole, Flooding, Monitoring, Byzantine, location disclosure etc.
Data Link Layer	Traffic analysis, WEP
Physical Layer	Jamming, Eavesdropping.

As shown in the above Table 1, there are more number of attacks in the network layer. This is because there is always some loophole present in almost every routing protocol designed for MANET. This result has motivated many researchers to design more and more secure routing protocols specially for MANET.

We will discuss in very brief about the network layer attacks and their possible solutions here:

1) Wormhole Attack: This attacks uses tunneling in the network to bypass the designated intermediate nodes in the path. Some countermeasures of this attack includes use of directional antennas, and packet leashes. The concept of packet leashes is very much similar to that of time to live, it restricts the packet to be forwarded for longer distance. But this mechanism requires very tight clock synchronization while implementing. SECTOR is another mechanism used to prevent the network from wormhole attack which does not require clock synchronization it uses one way hash functions and Merkle hash tree instead.

2) Blackhole Attack: SAR is used in general as a secure routing protocol to defend against blackhole attack. This has been one of the most worked domain for researchers to design a secure routing protocol against most generic attack like Blackhole. This attack is based on sequence number, malicious node sends its sequence number as the most optimal one to get part in the communication path, and then later starts dropping all the packets it receives from the source node. It's counter measures include trust based systems, neighbor nodes cooperation, currency like systems etc. There are numerous methods proposed for

defending against blackhole attack. We will see them in little more detail later in this paper.

3) Greyhole Attack: A variation of blackhole attack, which drop packets selectively based on sender node ID. If a malicious node is targeting to a particular source node, it will drop all packets coming from that node. Except that any packet received by malicious node will be forwarded as intended. This makes detection of such attack very difficult because malicious node is not completely inactive like in the case of Blackhole attack.

4) Denial of Service: Denial of service (DoS) attacks are basically attack on availability of any service and it can be launched by one of multiple layers. The network layer, physical layer etc. In this attack the attacker tries to interrupt the service provided by a particular node to the network. The attacker tries to keep the service provider busy in useless task so that the authorized users cannot have their services.

5) Sleep Deprivation Attack: In this attack a particular node is targeted and that is attacked by sending too much packets in very short span of time, this makes target node work very hard to process and forward all those packets. A the end the target node get exhausted as it has wasted its energy on useless packets and the node becomes inactive in the network. This kind of attacks are dangerous if they are performed on articulation point nodes; this results in node isolation and network breakage.

In the next section we will focus on how to detect or prevent such attacks in our network, what are the security mechanisms we have and what are their advantages and limitations if any is there.

III. INTRUSION DETECTION SYSTEM FOR MANET

In general an intrusion detection system is a mechanism to detect any malicious activity in the network, it used in wired networks as well. The IDSs can be broadly classified into two types called 'Signature Based' and 'Anomaly Based'. Signature based IDSs use previously available data to detect the malicious activities in the network. Whereas the Anomaly Based IDSs have predefined network behavior known and they keep eye on the network for suspicious activity. When they find something happening which is out of regular behavior of the network triggers the alarm.

Further each of the IDSs can have more variation depending upon the implementation, for example an IDS can be installed on a single node or multiple nodes collaboratively do the task of detection, in some implementation role of IDS is played by different nodes at different points of time. In this section we will see some of the most successful IDS proposed for MANETs in recent times.

In place of discussing each and every IDS in detail here we have made a table which includes the IDS name, authors, and their working in very brief to make a comparative study among them. (See Table-2)

As we study the table we can infer that every IDS has some specific characteristics and it not the same for all. Some of the IDS are designed for a specific type of network, they can perform better in one particular network but may fail to give their best result in other network environment.

Similarly the IDSs are also sometimes designed specifically for single or may be a set of attacks, for example if an IDS has good detection rate against blackhole attack then it may possible that it won't perform up to same extent in case of one byzantine attack. Some attacks are effectively defended by single detection and on the other hand some requires single detection to make the network more secure

Table 2. Comparison of various proposed IDS

IDS	Protocol	Detection type	Results	Issues
REAct[30]	DSR	Single detection	Reduces the communication overhead but enlarges the identification delay	The binary search method is easily expose audit node's information
NitalMistry*et al.*'s Method[33]	AODV	Single detection	The PDR is improved by 81.811% when network size varying, and rise 70.877% when mobility varying	Rise in end-to-end delay is 13.28% when network size varying, and rise 6.28% when mobility varying
Time based Threshold Detection Scheme[28]	Secure AODV (SAODV)	Single detection	The PDR of SAODV is around 90 to 100% when AODV is around 80%	The end-to-end delay increases when the malicious node is away from source node
Random Two hop ACK and Bayesian Detection Scheme[29]	DSR	Cooperative detection	The true positive rate can achieve 100% when existing 2 witness	The proposed scheme is not efficient when *k* equals to 3, reducing the true positives
Neighborhood based and Routing Recovery[26]	AODV	Single detection	The probability of one attacker can be detected is 93%	Failed when attackers cooperate to forge the fake reply packets
DPRAODV[31]	AODV	Single detection	The PDR is improved by 8085% than AODV when under black hole attack	A little bit higher routing overhead and endtoend delay than AODV
Next Hop Information Scheme[32]	AODV	Single detection	The PDR is improved by 4050% and the number of packets dropped is decreased by 7580% than AODV	Few additional delay
IDS based on ABM[34]	MAODV	Single detection	The packet loss rate can be decreased to 11.28% and 0.1476	Cooperative isolation the malicious node, but failed at collaborative black hole attacks
Redundant Route and Unique Sequence Number Scheme[27]	AODV	Single detection	Verify 75% to 98% of the routes	Attackers can listen to the channel and update the tables for last sequence number

IV. CONCLUSION AND FUTURE WORK

In this paper we studied about importance of Mobile Ad hoc Network in recent time and also discussed about various issues in implementation of MANET. The major issue is security, as users are sharing their sensitive information over the network, and application of MANET is majorly in critical operations like military and rescue operations. There we need message to safe and at the same time reliable because there may be lives on the stake. Also we did study about various attacks and their countermeasures proposed by authors in recent time. We can conclude that designing a single IDS for all type of network and against all type of attacks is near to impossible because of multiple constrains.

In future we will focus on designing an IDS for blackhole attack and will extend the project for greyhole attack as well. We will use anomaly based IDS as it is dynamic and there is no need to maintain signature table on nodes, this avoids the requirement of huge memory on mobile nodes. Also sequence numbers only should not be the only criteria to keep a node in the communication path, so we will find some more attributes for detection of malicious nodes.

REFERENCES

[1] Kozma W, Lazos L: REAct: ResourceEfficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16–18 March 2009 2009.

[2] Mistry N, Jinwala DC, IAENG, Zaveri M: Improving AODV Protocol AgainstBlackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17–19 March, 2010 2010.

[3] Tamilselvan L, Sankaranarayanan V: Prevention of Blackhole Attack in MANET. Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27–30 August 2007 2007.

[4] Djenouri D, Badache N: Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing 2008,8(6):689–704. doi: 10.1002/wcm.v8:6 doi: 10.1002/wcm.v8:6 10.1002/wcm.493 CrossRef (http://dx.doi.org/10.1002/wcm.493)

[5] Sun B, Guan Y, Chen J, Pooch UW: Detecting Blackhole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22–25 April 2003 2003.

[6] Raj PN, Swadas PB: DPRAODV: A Dynamic Learning System AgainstBlackhole Attack in AODV based MANET. International Journal of Computer Science 2009, 2: 54–59. doi: abs/0909.2371 doi: abs/0909.2371.

[7] Jaisankar N, Saravanan R, Swamy KD: A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26–27 March 2010 2010.

[8] Su MY: Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications 2011,34(1):107–117. doi:10.1016/j.comcom.2010.08.007 doi:10.1016/j.comcom.2010.08.007 10.1016/j.comcom. 2010.08.007

[9] AlShurman M, Yoo SM, Park S: Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACMSE'42) , Huntsville, Alabama, 2–3 April 2004 2004