An Overview of MANETs: Issues and Security Solutions

Lohit Kumar[a], Vishali Sharma[b]

[a]Student, School of electronics and communication, Lovely Professional University, Phagwara, Punjab, India
[b]Assistant Professor, Department of Electronics and Communication, Lovely Professional University, Phagwara, Punjab, India

Abstract

Mobile ad hoc network (MANETs) are the mobile nodes which are self configured and don't have any fixed infrastructure or pattern of deployment. They don't have any base station or central access point and this is the key feature of MANETs. They work automatically as per the defined routing protocol. The nodes which are in the range of each other communicate directly but the nodes which are not in the range of each other communicate hop by hop. Security in MANETs is the biggest issue. In this paper various issues in MANETs and some security solutions have been discussed.

Key words-Mobile adhoc Networks (MANETs), Malicious Nodes, Routing

1. Introduction

Mobile Ad hoc network (MANET) [1] is a set of mobile devices (nodes) which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver. If two nodes are within the range of each other then they can directly communicate with each other and if the nodes are not within the range of each other then they can communicate with each other using multihop routing. These mobile networks have following features:

- The wireless link between the nodes is highly vulnerable. This is because nodes continuously move which cause frequent breakage of the link.
- The topology of the network is highly dynamic due to the continuous breakage and establishment of wireless link. The nodes continuously move in and out of the range of each other.
- These wireless networks are bandwidth constrained i.e. they have limited bandwidth.
- All nodes depend on battery power which is limited so an energy efficient operation is required.

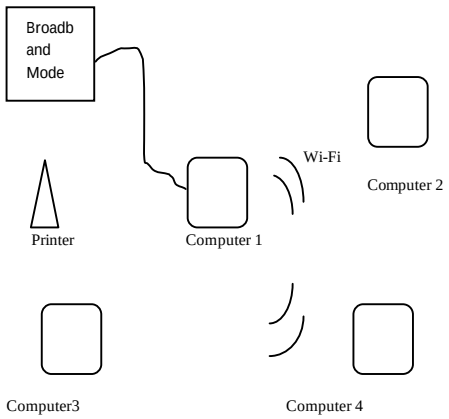


Figure 1: Basic structure of MANET

Ad-hoc networks are basically peer-to-peer multi hop wireless networks where information packets are transmitted from source to arbitrary destination via

intermediate nodes in a forwarded manner. As the nodes move the resulting change in network topology must be known to other nodes so that the previous topology can be updated.

2. Vulnerability of MANETS

2.1 Wireless links*:* The use of wireless links makes the network wide open to attacks such as eavesdropping and active interference. In wireless network attackers do not need any physical access to the network to carry out these attacks.

2.2 Dynamic topology: MANETs nodes are free to leave and join the network at any time. Due to which the network topology changes frequently. Therefore it is difficult to differentiate between the normal behaviour of the network from malicious behaviour in this dynamic environment**.**

2.3 Cooperativeness*:* Routing algorithms of MANETs usually assume that nodes are cooperative and non malicious. As a result a malicious attacker can easily become an important routing agent and destroy the network operations by disobeying the protocol specifications [2].

2.4 Lack of a clear line of defence*:* MANETs do not have a clear line of defence therefore attacks can come from any direction [3]. The boundary that separates the inside network from the outside world is not very clear on MANETs

3. Attacks on MANET

Security in MANETs is one of the biggest issues. The characteristics of MANETs are such that they are inevitable to the attacks. We can classify attacks as passive or active.

3.1 Passive attacks

In passive attacks the unauthorized node tries to find the information about the network. They do not damage the ongoing traffic of the network so detection of this type of attack is very difficult. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard [4].

3.1.1 Snooping: Snooping is unauthorized access to another person's data. Snooping uses software programs to remotely monitor activity on a computer or network device. A snoop server is used to capture network traffic for analysis, and the snooping protocol monitors information on a computer bus to ensure efficient processing [4].

3.2 Active attacks

An active attack destroys the normal functioning of network. Active attacks are of two types internal and external. An internal attack is carried out by nodes which are part of the network. Due to this internal attack is more severe then external attack. External attack is carried out by nodes which are not authorized to the network. This type of attack can be prevented by using firewalls etc.

3.2.1 Wormhole attack: In wormhole attack the malicious nodes receive the packets at one location in the network and tunnel them to another location in the network. Due to this replica of packets is been created.

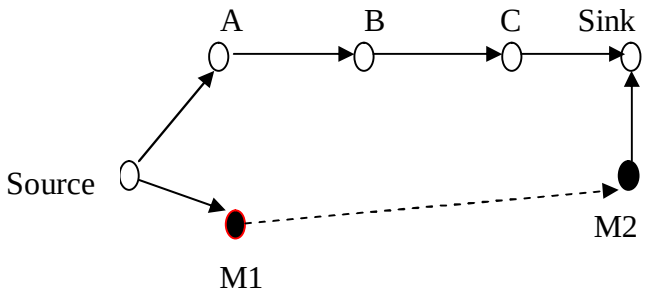


Figure 2: Wormhole Attack

Malicious Node

Tunnel between two malicious nodes

3.2.2 Black hole attack: In black hole attack the attacker listens to the routes and as soon as it receives the request for route to the destination node, it sends the reply to the source node. If the malicious reply reaches the source node before the reply from actual node, a fake route will be created. After this the malicious node will drop all the packets to disturb the whole network

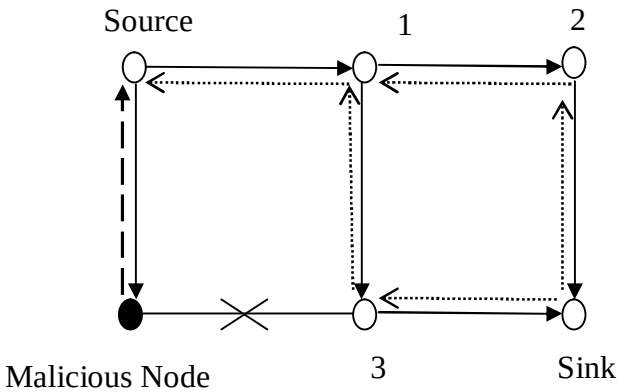
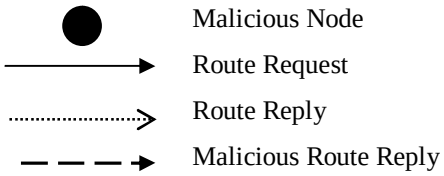


Figure 3: Blackhole Attack



3.2.3 Routing attacks: These are of different types such as routing table overflow, routing table poisoning, and packet replication.

3.2.4 Resource Consumption attack: In this the attacker node tries to waste the resources of other nodes. These resources can be bandwidth and battery power which are limited in the network. Forwarding of stale packet and unnecessary request for route are the different form of attacks.

3.2.5 Information privacy: Any important information of the nodes or network must be protected during the communication process. Such information can contain location of nodes, secret codes etc.

3.2.6 Session hijacking: At first, the attacker spoofs the IP address of target machine and determines the correct sequence number. After that he performs a DOS attack on the victim. As a result, the target system becomes unavailable for some time. The attacker now continues the session with the other system as a legitimate system.[4]

3.2.7 Denial of Service (DOS): In DOS attack the malicious node tries to make the resources of the network unavailable to the authorized user. There are two main forms of DOS attack-one that crash services and the other that flood the services

4. Security Solutions and measures to MANETs

4.1 Secure routing: In this all nodes that are participating in the network must be

authenticated nodes and must follow the routing protocol. Authentication of nodes makes sure that the unauthorized nodes don't take part in the network. Authentication can be provided with the help of symmetric cryptography or public key.

4.2 **Intrusion detection**: An IDS is introduced to detect possible violations of a security policy by monitoring system activities and responding to those that are apparently intrusive. If we detect an attack once it comes into the network, a response can be initiated to prevent or minimize the damage to the system.[2]

4.3 **Confidentiality**: Confidentiality means to keep the data secure from unauthorized user. Data encryption can be done to keep the data confidential.

4.4 **Integrity**: Integrity is the prevention of data from being destroyed by malicious node during transmission process.

4.5 **Availability**: Availability is to keep the network services available to authorized user. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [5].

4.6 **Non-repudiation:** It is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message [6].

5. Conclusion

Random deployment and no centralized access point are the biggest plus points of MANETs. But MANETs have its issues as well where security is the biggest issue. In this papers we have given an overview of MAENTs, discussed some of its issues and security solutions..

References

[1]	C.S.R.Murthy and B.S.Manoj, "Ad Hoc Wireless Networks", Pearson Education, 2008
[2]	K. Sivakumar, Dr. G. Selvaraj "OVERVIEW OF VARIOUS ATTACKS IN MANET AND COUNTERMEASURES FOR ATTACKS", International Journal of Computer Science and Management Research ,Vol. 2 Issue 1 January 2013
[3]	Sanzgiri, K., et al. A secure routing protocol for ad hoc networks, in Proceedings of the 10th IEEE Conference on Network Protocols, 2002.
[4]	Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).
[5]	Lidong Zhou and Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Networks Special Issue on Network Security, November/December 1999.
[6]	Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", 2006 Springer