A Review on Mobile Ad-hoc Networks (MANET'S) with Attacks Impact

Kanchan Bala

Mtech Student, Department of Computer Science and Engineering, Yadavindra College of Engineering, Punjabi University, Talwandi Sabo, Punjab, India

Arpit bansal

Assistant Professor, Department of Computer Science and Engineering, Yadavindra College of Engineering, Punjabi University , Talwandi Sabo, Punjab, India

Abstract

Mobile Ad-hoc Networks is a wireless network of mobile nodes communicating with each other in a multi-hop fashion without the support of any fixed infrastructure such as base stations, wireless gateways or access points. MANETs enable wireless networking in environments where there is no wired or cellular infrastructure. Due to dynamically changing topology, open environment and lack of centralized infrastructure MANET's are vulnerable to many attacks. So in (MANETs), security is one of the most important concerns. In this paper, we have presented different reviews on MANET with impact of different types of attacks such as Neighbor attack, Ddos attack, and Blackhole attack.

Keywords

Blackhole attack, DDos attack, MANET, Neighbor attack, routing protocols.

1. Introduction

A mobile ad hoc network (MANET) is a spontaneous network that can be established without any fixed infra-structure or a topology. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes *i.e.* nodes within each other's radio range communicate directly via wireless links, while those that are not in each other's radio range use other nodes as relays[1] . The term ad hoc implies that this network is established for a special, often extemporaneous service customized to specific applications. MANETs enable wireless networking in environments where there is no wired or cellular infrastructure; or, if there is an infrastructure, it is not adequate or cost effective [2].

MANETs offer several advantages over traditional networks including reduced infrastructure costs, ease of

establishment and fault tolerance, as routing is performed individually by nodes using other intermediate network nodes to forward packets , this multi-hopping reduces the chance of bottlenecks, however the key MANET attraction is greater mobility compared with wired solutions[3].

1.1 Characteristics of MANET

- The communication medium is broadcast and connection of different nodes is wireless.
- The topologies between the nodes are changing continuously.
- Nodes are free to connect to any node. Due to the presence of malicious nodes the performance is decrease [4].

1.2 Security Challenges & Issues of MANET'S

- MANETs use wireless media for transmission, which introduces security flaws to the networks. Basically any one with the proper equipment and knowledge of the current network topology and the protocols may obtain access to the network. Both active and passive attacks such as impersonation, eavesdrop-ping, message redirection, and traffic analysis, can be per-formed by an adversary.
- In specific scenarios, MANET nodes may be scattered over a large area. Some nodes or network components may be un-monitored or

hard to monitor, and exposed to the physical attacks.

- Because MANETs do not have any central authority, this is a major barrier to security. The security mechanisms employed in wired networks, such as Public Key Management, Node Authentication, and Determination of Node Behavior, are in fact very difficult to achieve without any central administration.
- Ad hoc networks are highly dynamic in nature. Node joins and departures are not predictable. Moreover, network topology is always changing in Ad Hoc networks [5].

1.3 MANET'S Routing Protocols

Routing is necessary in MANET, but it create problem and Challenges as compared to the routing in fixed infrastructure. The problem in routing is due to the rapidly changes in the topology of the nodes and the devices.

There are three type of routing: Proactive, Reactive and Hybrid.

In *Proactive routing,* there is a fixed topology and use a single protocol. OLSR and DSDV are the proactive routing protocol.

In *Reactive routing,* there is several protocol are used between the two devices and the type of topology is change according to the condition. AODV and DSR are the reactive routing protocol [4].

In *Hybrid routing,* they combine features from both reactive and proactive routing protocols, typically attempting to exploit the reduced control traffic overhead from proactive systems while reducing the route discovery delays of reactive systems by maintaining some form of routing table [3]. TORA and ZIP are the hybrid routing protocols.

1.4 MANET vulnerabilities

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

- *Lack of centralized management:* MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network.
- *Resource availability*: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.
- *Scalability:* Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.
- *Cooperativeness:* Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.
- *Dynamic topology:* Dynamic topology and changeable nodes Membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.
- *Limited power supply:* The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.
- *Bandwidth constraint:* Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.
- *Adversary inside the Network*: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

- *No predefined Boundary*:- In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack [5].

2. Types of Attacks

Attacks on MANETs can be classified into two categories: *active* and *passive* attacks.

Active attack

An active attack attempts to destroy the data being exchanged in the network. Active attacks can be divided further into two categories: *external* and *internal* attacks.

External attacks

These are carried out by nodes that do not belong to the network. These attacks can be prevented using standard security mechanisms such as encryption techniques or firewalls.

Internal attacks

These attacks are from compromised nodes that belong to the network.

Passive attack

These attacks affect the network performance without altering the operation of the network [2].

a) Neighbor attack

The goal of the neighbor attack is to disrupt the multicast routes by making two nodes that are in fact out of each other's communication range believe that they can communicate directly with each other. If these two nodes are part of the routing mesh, the join reply packet that they exchange will be lost because there is no actual connection between them. A neighbor attacker violates the routing protocol and does not need to involve itself later in the packet dropping process, since the packets will be lost eventually due to the fake links.

Upon receiving a packet, an intermediate node records its IP in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without recording its IP in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbors (i.e., one-hop away from each other), resulting in a disrupted route [2].

b) Black hole attack

In the black hole attack, attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An attacker use the flooding based protocol for listing the request for a route from the initiator, then attacker create a reply message he has the shortest path to the receiver . As this message from the attacker reached to the initiator before the reply from the actual node, then initiator assume that it is the shortest path to the receiver. So that a fake route is create. Once the attacker has been able to insert himself between the communications node, then attacker may able to do anything with the packet which is send by the initiator for the receiver [4]**.**

c) *Ddos attack*

It is an attack where multiple systems comprised together and target a single system causing a denial of service (DoS). The target node is flooded with the data packets that system shutdowns, thereby denying service to legitimate users. The services under attack are those of the “primary victim”, while the compromised systems used to launch the attack are often called the “secondary victims”.

Current MANETS are basically vulnerable to two different types of DDoS attacks:

- *Active DDoS attack* is an attack when misbehaving node has to bear some energy costs in order to perform the threat.
- *Passive DDoS* attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly.

Nodes that perform active DDoS attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive DDoS attacks with the aim of saving battery life for their own communications are considered to be selfish [5].

3. Different Reviews

S. Parthiban, A. Amuthan, N.Shanmugam, K.Suresh Joseph [2]

In 2012, they present simulation based study of the impact of neighbor attack on mesh-based Mobile Ad-Hoc Network (MANET). The study enables them to propose a secure neighbor detection mechanism (SNDM).A generic detection mechanism against neighbor attack for On Demand Routing Protocols is simulated on Glomosim environment. They arrived at the following conclusions regarding neighbor attack solution. The performance of a small multicast group will degrade seriously under these types of attacks even the solution is available. A large multicast group with a high number of senders and/or a high number of receivers can sustain good performance under these conditions due to more alternative paths in the routing mesh. With respect to attack positions, areas near the senders are the most damaging positions since the original packets are intercepted early, before being duplicated at branch points. However, when the number of attackers is smaller than the number of multicast senders, the mesh center is the strongest attack position, causing the most packet losses.

Geetika, Naveen Kumari [5]

In 2013, they introduce Bottom-up approach, New Cracking algorithm, Prevention algorithm using IDS node for detecting and controlling DDoS attack. As the existing MANET routing protocols, such as Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), do not provide enough security defense capacity.

V.Kaviyarasu, S.Baskaran [6]

In 2014, they focused on mobile ad hoc network's routing vulnerability and analyze the network performance under Distributed Denial of Service MANETS. The resistive schemes against these attacks were proposed for Ad hoc on demand Distance Vector (AODV) routing protocol. The existing intrusion detection system (IDS) was categorized in to two types: Signature based IDS and Anomaly based IDS. The benefit of IDS technique is that it can be able to detect the attack without prior knowledge of attack. In Signature based intrusion detection some of the previously detected patterns or signatures are stored into the data base of the IDS. If any disturbance is found in the network by IDS, it checks it with the previously saved signature. If it matches, then IDS has found the attack. The disadvantage of this system is that if there is an attack and its signature is not in IDS database then IDS cannot be able to detect that attack. To overcome the drawbacks of signature based system, anomaly based IDS were proposed. In this system, first the normal profile of the network is set by the IDS and is taken as a base profile and then is compared with the monitored network profile as shown in Figure 1.1.

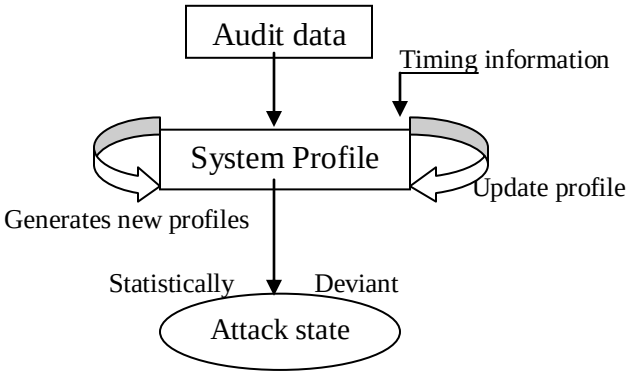

Figure 1.1-Anomaly based Intrusion Detection.

Anomaly based IDS are based on tracking unknown unique behavior pattern of detrimental activity.

The advantages includes:-

1. Helps to reduce the “limitations problem”.
2. Conducts a thorough screening of what comes through.

Along with these, AODV routing protocol is used in normal module, attack module and IDS cases. The Proposed mechanism eliminates the need for a centralized trusted authority which is not practical in Ad-hoc network due to their self organizing nature. The results demonstrate that the presence of a DDoS increases the throughput of the network and also reduces the end to end delay. The proposed mechanism protects the network through a self organized, fully distributed and localized procedure.

M. Mohanapriya, Ilango Krishnamurthi [7]

In 2013, they present a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. They proposed an Intrusion Detection System (IDS) where the IDS nodes are set in promiscuous mode only when required, to detect the abnormal difference in the number of data packets being forwarded by a node. When any anomaly is detected, the nearby IDS node broadcast the block message, informing all nodes on the network to cooperatively isolate the malicious node from the network. It is a light weight solution methodology which is a simple acknowledgement scheme to detect grayhole nodes in

MANET. It can be incorporated with any existing on demand ad hoc routing protocols. By the proposed algorithm, the destination node detects the presence of malicious nodes in the source route and with the help of intrusion detection system the malicious nodes are isolated from the network. Also their IDS nodes will turn into promiscuous listening only in the presence of suspected nodes resulting less energy loss, which makes their method suitable for the resource constrained characteristics of MANET. The proposed technique employs Glomosim to validate the effectiveness of proposed intrusion detection system.

Mayuri Gajera, Sowmya K.S [8]

In 2013, they proposed a secure routing protocol for Ad hoc on demand distance vector (AODV) routing protocol known as Identity-based key management (IKM) which is a combination of ID-based Cryptography and threshold cryptography and authenticates all routing message. They attempt to show how black hole attack is prevented in IKM system. The IKM system uses certificate less approach where each node derives its public key from its network ID and some common shared information. IKM is a secure, lightweight and scalable scheme for MANETs. The system identifies compromised node and prevents from third party attack which may also include trusted third party attack. We also show how the black hole is prevented in the IKM system. Thus they believe that IKM system is very secure system compared to other secure system when black hole attack, third party attack and compromised node is considered.

4. Conclusion and Future work

Mobile ad hoc network is an infrastructure less network due to its capability of operating without the support of any fixed infrastructure. Security plays a vital role in MANET due to its applications like battlefield or disaster-recovery networks. MANETs are more vulnerable compared to wired networks due the lack of a trusted centralized authority and limited resources. There is an urgent need to develop schemes to handle different types of attacks in MANET. In this paper we reviewed the different attacks on MANET'S and methods to prevent and control them and we also state the MANET vulnerabilities and different types of attacks on MANET.

In future, we will enhance MDSR protocol in Hybrid scheme for Controlling Security and Load balancing over MANET.

References

[1] Meghna Chhabra, Brij Gupta, Ammar Almomani, "A Novel Solution to Handle DDOS Attack in MANET", http// www.scirp.org/journal/jis,Vol4,165-179, July 2013.

[2] S. Parthiban, A. Amuthan, N. Shanmugam, K. Suresh Joseph, "Neighbor attack and detection mechanism in Mobile ad hoc networks" International journal of Advanced Computing,Vol.3, No.2, March 2012.

[3] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)",International Journal of Information and Education Technology,Vol.3, No.1,February 2013.

[4] Satyam Shrivastava, Sonali Jain, "A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network" International Journal of Computer Science & Engineering Technology(IJCSET), Vol. 4, No. 03, Mar 2013.

[5] Geetika, Naveen Kumari, "Detection and Prevention Algorithms of DDOS Attack in MANETs", ISSN: 2277 128X, Vol.3, No.8, August 2013@IJARCSSE.ltd.

[6] V.Kaviyarasu1, S.Baskaran2," Security in MANET against DDoS Attack" ISSN:22312803,http://www.ijcttjournal.org,Vol.7,No.1,Jan 2014.

[7] M. Mohanapriya, Ilango Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET", Computers and Electrical Engineering 40 (2014) 530–538, 2013 @Elsevier. Ltd

[8] Mayuri Gajera, Sowmya K.S, "Prevention of Black Hole Attack in Secure Routing Protocol", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2, Issue 6, June 2013, www.ijsr.net.ltd.