International Journal of Computer Applications Technology and Research
Volume 3– Issue 9, 541 - 546, 2014, ISSN: 2319–8656

Different Types of Attacks and Detection Techniques in Mobile Ad Hoc Network

Mahsa Seyyedtaj
Department of computer, Shabestar branch,
Islamic Azad University, Shabestar,
Iran

Mohammad Ali Jabraeil Jamali
Department of computer, Shabestar branch,
Islamic Azad University, Shabestar,
Iran

Abstract: A Mobile Ad-Hoc Network (MANET) is a collection of mobile nodes (stations) communicating in a multi hop way without any fixed infrastructure such as access points or base stations. MANET has not well specified defense mechanism, so malicious attacker can easily access this kind of network. In this paper we investigate different types of attacks which are happened at the different layers of MANET after that we discuss some available detection techniques for these attacks. To our best knowledge this is the first paper that studies all these attacks corresponding to different layers of MANET with some available detection techniques.

Keywords: Security; Attacks; MANET; Prevention; Routing

1. INTRODUCTION

A MANET contains mobile nodes (stations) that can communicate with each other without the use of predefined infrastructure. There is not well defined administration for MANET. MANET is self organized in nature so it has rapidly deployable capability. MANET is very useful to apply in different applications such as battlefield communication, emergency relief scenario etc. In MANET nodes are mobile in nature, due to the mobility, topology changes dynamically. Due to its basic Ad-Hoc nature, MANET is venerable to various kinds of security attacks [1].

2. SECURITY GOALS FOR MANET

The ultimate goal of the security solutions for MANET is to provide a framework covering availability, confidentially, integrity, authentication and non-repudiation to insure the services to the mobile user. A short explanation about these terms:-

2.1 Availability

ensures the survivability of network services despite denial of service attacks. The adversary can attack the service at any layer of an ad hoc network. For instance, at physical and media control layer it can employ jamming to interfere with communication on physical channels; on network layer it could disrupt the routing protocol and disconnect the network; or on higher layers it could bring down some high-level services (e.g., the key management service).

2.2 Confidentiality

ensures that certain information is never disclosed to unauthorized entities. It protects the network transmission of sensitive information such as military, routing, personal information, etc.

2.3 Integrity

guarantees that the transferred message is never corrupted. A corruption can occur as a result of transmission disturbances or because of malicious attacks on the network.

2.4 Authentication

enables a node to ensure the identity of the peer node with whom it is communicating. It allows manipulation-safe identification of entities (e.g., enables the node to ensure the identity of the peer node), and protects against an adversary gaining unauthorized access to resources and sensitive information, and interfering with the operation of other nodes.

2.5 Non-repudiation

ensures that the origin of a message cannot later deny sending the message and the receiver cannot deny the reception. It enables a unique identification of the initiator of certain actions (e.g., sending of a message) so that these completed actions can not be disputed after the fact [11].

3. TYPES OF SECURITY ATTACKS

3.1 On the basis of nature

3.1.1 Passive attacks

In passive attack there is not any alteration in the message which is transmitted. There is an attacker (intermediated node) between sender & receiver which reads the message. This intermediate attacker node is also doing the task of network monitoring to analyze which type of communication is going on.

3.1.2 Active attacks

The information which is routing through the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also do the task of RREQ (re request) though it is not an authenticated node so the other node rejecting its request due these RREQs the bandwidth is consumed and network is jammed.

3.2 On the basis of domain

3.2.1 External attacks

In external attack the attacker wants to cause congestion in the network this can be done by the propagation of fake routing information. The attacker disturbs the nodes to avail services.

3.2.2 Internal attacks

In internal attacks the attacker wants to gain the access to network & wants to participate in network activities. Attacker does this by some malicious impersonation to get the access to the network as a new node or by directly through a current node and using it as a basis to conduct the attack [12].

4. ATTACKS CORRESPONDING TO DIFFERENT LAYERS IN MANET

First of all let we explain how many layers are there in MANET stack. Basically there are five layers i.e. application layer, transport layer, network layer, Mac layer, & physical layer [3].

4.1 Attacks at application layer

4.1.1 Repudiation attack

Due to repudiation attack deny of participation is happened in whole communication, or in a part of communication [8].

4.1.2 Attack by virus & worms

Attack is done by virus, worms to infect the operating system or application software installed in mobile devices [2].

4.2 Attacks at transport layer

4.2.1 TCP SYN attack (Denial of service attack)

TCP SYN attack is DOS in nature, so the legitimate user does not get the service of network when attack is happened. TCP SYN attack is performed by creating a large no of halt in opened TCP connection with a target node [3].

4.2.2 TCP Session Hijacking

TCP session hijacking is done by the spoofing of IP address of a victim node after that attacker steals sensitive information which is being communicated. Thus the attacker captures the characteristics of a victim node and continues the session with target [6].

4.2.3 Jelly Fish attack

Similar to the blackhole attack, a jellyfish attacker first needs to intrude into the forwarding group and then it delays data packets unnecessarily for some amount of time before forwarding them. This results in significantly high end-to-end delay and delay jitter, and thus degrades the performance of real-time applications. [9].

4.3 Attacks at network layer

4.3.1 Flooding attack (Denial of service attack)

Attacker exhausts the network resources, i.e. bandwidth and also consumes a node's resources, i.e. battery power to disrupt the routing operation to degrade network performance. A malicious node can send a large no. of RREQ (re request) in short duration of time to a destination node that dose not exist in the network. Because no one will replay to these RREQ so they will flood in the whole network. Due to flooding the battery power of all nodes as well as network bandwidth will be consumed and could lead to denial of service [7].

4.3.2 Route tracking

This kind of attack is done to obtain sensitive information which is routed through different intermediate nodes [8].

4.3.3 Message Fabricate, modification

In this kind of attack false stream of messages is added into information which is communicated or some kind of change is done in information [13].

4.3.4 Blackhole attack

In a blackhole attack a attacker node sends fake routing information in the network to claims that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example in an Ad-Hoc on demand distance vector routing (AODV), attacker can send fake RREQs including a fake destination sequence number that is fabricated to be equal or higher than the one contain in the RREQ to source node, claiming that it has a sufficient fresh route to the destination node. This causes the source node to select the route that passes through the attacker node. Therefore all the traffic will be routed through the attacker and therefore, the attacker can misuse the information or sometime discard the traffic [1].

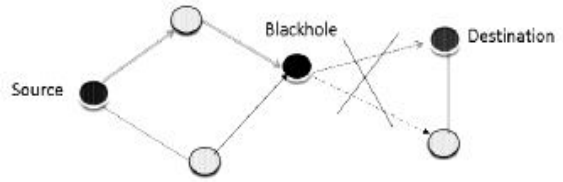

Figure 1. Blackhole attack

4.3.5 Wormhole attack

It is the dangerous one among the all attacks. In this attack, a pair of colluding attackers recodes packets at one location and replays them at another location using a private high speed network [5]. The seriousness of this attack is that it can be launched in all communication that provides authenticity & confidentiality.

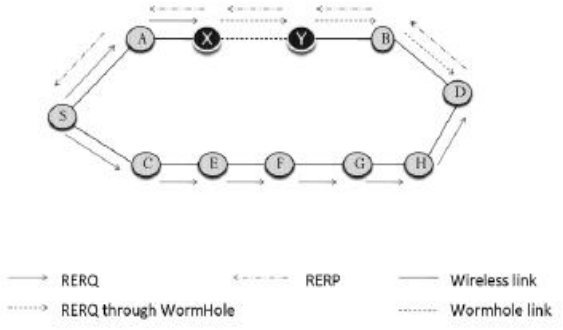

Figure 2. Wormhole attack

4.3.6 Grayhole attack

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are

• Dropping all UDP packets while forwarding TCP packets.

• Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures [8].

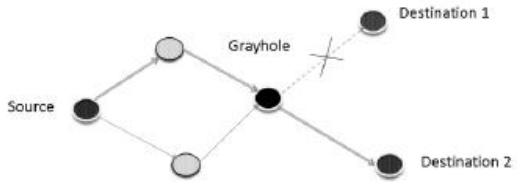

Figure 3. Grayhole attack

4.3.7 Rushing attack

Many demand-driven protocols such as ODMRP, MAODV, and ADMR, which use the duplicate suppression mechanism in their operations, are vulnerable to rushing attacks. When source nodes flood the network with route discovery packets in order to find routes to the destinations, each intermediate node processes only the first non-duplicate packet and discards any duplicate packets that arrive at a later time. Rushing attackers, by skipping some of the routing processes, can quickly forward these packets and be able to gain access to the forwarding group [4].

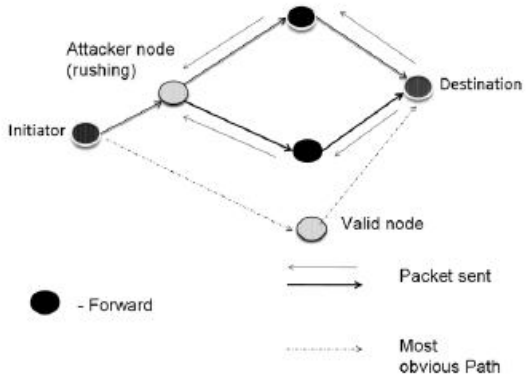

Figure 4. Rushing attack

4.3.8 Link spoofing attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. An attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its multipoint relay node (MPR). As an MPR node, a malicious node can then manipulate data or routing traffic, i.e. modifying or dropping the routing traffic. They can also perform some other types of DOS attacks [13].

4.3.9 Byzantine attack

Byzantine attack can be launched by a single malicious node or a group of nodes that work in cooperation. A compromised intermediate node works alone or set of compromised intermediate nodes works in collusion to form attacks. The compromised nodes may create routing loops, forwarding packets in a long route instead of optimal one, even may drop packets. This attack degrades the routing performance and also disrupts the routing services [8].

4.3.10 Sybil attack

A Sybil attack is a computer hacker attack on a peer-to-peer (P2P) network. It is named after the novel Sybil, which recounts the medical treatment of a woman with extreme dissociative identity disorder. The attack targets the reputation system of the P2P program and allows the hacker to have an unfair advantage in influencing the reputation and score of files stored on the P2P network. Several factors determine how bad a Sybil attack can be, such as whether all entities can equally affect the reputation system, how easy it is to make an entity, and whether the program accepts non-trusted entities and their input. Validating accounts is the best way for administrators to prevent these attacks, but this sacrifices the anonymity of users [10].

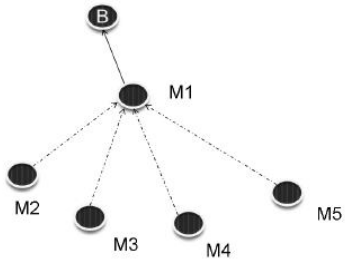

Figure 5. Sybil attack

4.4 Attacks at MAC layer

4.4.1 MAC Denial of service attack (DOS)

At the MAC layer DOS can be attempted as:

There is a single channel which is used frequently, keeping the channel busy around a particular node leads to a denial of service attack at that node.

An attacker node continuously sends spurious packets to a particular network node this leads to drain the battery power of the node, which further leads to a denial of service attack.

4.4.2 Traffic monitoring & Analysis

Traffic analysis is a passive type of attack in nature this kind of analysis is done by attacker to find out which type of communication is going on.

4.4.3 Bandwidth Stealth

In this kind of attack the attacker node illegally stealth the large fraction of bandwidth due to this congestion is happened in the network.

4.4.4 MAC targeted attack

MAC layer plays an important role in every piece of data that is exchanged through several nodes, ensuring that data is collected efficiently to its intended recipient. The MAC targeted attacks disrupt the whole MAC procedure [13].

4.4.5 WEP targeted attacks

The wired equivalent privacy (WEP) is designed to enhance the security in wireless communication that is privacy and authorization. However it is well known that WEP has number of weaknesses and is subject to attacks. Some of them are:-

1. WEP protocol does not specify key management.

2. The initialization vector (IV) is a 24 bit field which is the part of the RC4 encryption key. The reuse of IV and weakness of RC4 help to produce analytic attacks.

3. The combined cure of non cryptographic integrity algorithm, CRC32, with the stream cipher has a security risk [11].

4.5 Attacks at physical layer

4.5.1 Jamming attack (Denial of service attack)

DOS attack is also happened at physical layer. Due to DOS there is denial of services accessed by a legitimate network user. Example is jamming attack.

Due to jamming & interference of radio signals messages can be lost or corrupt. Signals generated by a powerful transmitter are strong enough to overwhelm the target signals and can disrupt communication. Pulse and random noise are most common type of signal jamming [3].

4.5.2 Stolen or compromised attack

These kinds of attacks are happened from a compromised entities or stolen device like physical capturing of a node in MANET.

4.5.3 Malicious message injecting

Attacker inject false streams into the real message streams which is routing through the intermediate nods, due to malicious message injecting the functionality of network is disrupted by the attacker.

4.5.4 Eavesdropping attack

Eavesdropping is the reading of messages and conversation by unintended receivers. The nodes in MANET share a wireless medium and the wireless communication use RF spectrum and broadcast by nature which can easily intercepted with receivers tuned to proper frequency. As a result transmitted messages can be overheard as well as fake messages can be injected into the network [3].

Table1. Attacks corresponding to different layers

MANET Layer	Type of Attack
Application Layer	Repudiation attack, Attacks by virus & worms
Transport Layer	TCP SYN attack (DOS in nature), TCP session hijacking, Jelly Fish attack
Network Layer	Flooding attack, Route tracking, Message Fabricate, modification, Blackhole attack, Wormhole attack, Link spoofing attack Grayhole attack, Rushing attack, Byzantine attack, Sybil attack
MAC Layer	Mac DOS (Denial of service) attack, Traffic monitoring & analysis, Bandwidth stealth, MAC targeted attack, WEP targeted attack
Physical Layer	Jamming attack (DOS in nature), Stolen or compromised attack, Malicious massage injecting, Eavesdropping attack

5. DETECTION TECHNIQUES

There are some schemes which are used to secure the MANET & in the detection of anomalies. Some of these are discussed below:-

5.1 Intrusion Detection Technique

IDS detect different threats in MANET communication There is proposed architecture [1] for IDS which is used by MANET given below:-

In the proposed architecture of IDS for MANET every node participates in the detection process and responds to activities. This detection process is done by detecting the intrusion behavior in the two ways:-

a). Locally

b). Independently

This act is performed by an agent who is known as IDS agent who is inbuilt in all devices (stations). Each node performs detection locally and independently but there is also a situation if a node detects an anomaly but it has not sufficient investigation results to figure out which type of anomaly it is, so it share its result to the other nodes in the communication range and ask them to search this anomaly in their respective security logs to trace out the possible characteristics of that intruder.

There are four functional modules in conceptual model of the IDS:-

5.1.1 Local data collection module

Local data collection module deals with data gathering issues. Data come from various resources through a real time data audit.

5.1.2 Local detection engine

It inspects any anomaly shown in the data which was collected by local data collection modules. This detection engine rely on the statistical anomaly detection technique which distinguish anomaly in the basis of the comparison which is done by taking a deviation between the current observation data and the normal profile (generated on the basis of normal behavior of the system) of system.

5.1.3 Cooperative detection engine

All time it is not possible the attacks which are happened on MANET known to the system (IDS). So there is some need to find more evidence for particular attack, so we have to initiate a cooperative detection process in these circumstances. In cooperated detection process participants will share the information regarding the intrusion detection to all their neighboring nodes. On the basis of information received a node can calculate new intrusion state. In this process they used certain algorithms such as a distributed consensus algorithm with weight. We may assume that the majority of node in MANET are actual (are not attacker nodes) so we can trust the results produced by any of the participants that the network is under attack.

5.1.4 Intrusion response module

When an intrusion is confirmed intrusion response module will response to that. It responses to reinitialize the communication channel. Re-initialization is done such as reassigning the key or reorganizing the network. In reorganization of the network we remove all the compromised nodes. This response varies corresponding to different kind of intrusion.

5.2 Cluster-Based Intrusion Detection Technique [13]

We have discussed cooperative intrusion detection architecture for the ad hoc network in the previous part which has some drawbacks. In cooperative intrusion detection technique there is mechanism of participation of all nodes in detection process which cause huge power consumption for all the participating nodes.

In MANET power supply is limited which may cause some node may behave in selfish way i.e. they are not cooperative with other nodes to save their battery power. So the actual aim is violet in cooperative intrusion detection mechanism. To solve this problem a cluster based intrusion detection technique is used. In this technique MANET can organized into number of clusters. The organization is done in such a way that every node is a member of at least one cluster and there will be only one node per cluster that will take the responsibility of monitoring. In a certain period of time this node is known as cluster head. A cluster contain several node that reside within the same radio range with each other, so when a node is selected as cluster head all the nodes in this cluster should be within 1-hop distance. When a cluster selection process is going on there is the necessity to ensure two things:-

- aFairness.
- Efficiency.

5.2.1 Fairness

Fairness contains two levels of meanings: the probability of every node in the cluster head should be equal and each node should act as the cluster node for the same amount of time.

5.2.2 Efficiency

Efficiency of cluster head selection process means that there should be some method that can select a node from the cluster periodically which has high efficiency. Cluster information is used in cluster based intrusion detection technique. Basically there are four states in the cluster information protocol:-

1. Initial
2. Clique.
3. Done
4. Lost.

At the beginning all nodes are at initial state. In initial state node will monitor their own traffic and detects intrusion behavior independently. There are two steps that we need to finish before we get the cluster head of the network:-

- Cluster computation.
- Cluster head computation.

A cluster is a group of nodes in which every pair of member can communicate via direct wireless link. Once the protocol is finished every node is aware of fellow clique member. Then a node will randomly select from the queue to act as the cluster head. There are two other protocols that assist the cluster to do some validation and recovery which are:-

- Cluster valid assertion protocol.
- Cluster recovery protocol.

5.2.2.1 Cluster valid assertion protocol:-

It is generally used in following two situations

This protocol is used by a node to check if the connection between the cluster head and itself is maintained or not. The node does this task periodically. If connection is not maintained the node will check to see if it belong to another cluster, and if in this situation it also get a negative answer then the node draw a conclusion and will enter into the LOST state and initiate a routing recovering request.

To keeps the fairness and security in the whole cluster a mandatory reelection time out is also needed for the cluster head. If the time out expires, all the nodes switch from DONE state to INITIAL state, thus they begin a new round of cluster head election.

5.2.2.2 Cluster recovery protocol:-

It is mainly used in a case when a node losses its connection with previous cluster head, for a cluster head losses all its connected stations than they enter into LOST state and initiate cluster recovery protocol to elect a new cluster head.

5.3 Misbehavior detection through cross layer analysis [13]

In some cases attacker attacks on multiple layer of MANET simultaneously but they keep the attack stay below the detection threshold so as to escape from detection by the single-layer misbehavior detector. This kind of attack is also called as cross-layer attack. So cross-layer attacks are more threatening to a single-layer detector because they can be easily skipped by the single-layer misbehavior detector. So we have to used some different techniques in these circumstances, this attack scenario can be detected by cross layer misbehavior detector. In this technique the inputs from all layer of MANET stack are combined and analyzed by the cross layer detector. But a problem is arisen here, how to make the cross layer detection more effective and efficient, how to cooperate between single-layer detectors to make the detection process effective. Single-layer detectors deal with attacks to corresponding layers, so we have to take some different viewpoints in these circumstances when a single attack is observed in different layers of MANET. So it is necessary to clubbed out the different results produced by different layers to make a possible solution. There is second thing, we need to find out how much the system resources and network overhead will be increased due to the use of cross layer detector compared with the original single layer detector. Limited battery power of the nodes in MANET is also an issue here, the system and network overhead brought by the cross layer detection should be consider and compared with the performance gain caused by the use of cross layer detection technique.

6. CONCLUSION

In this paper, we try to inspect the security attacks at different layers of MANET, which produces lots of trouble in the MANET operations. Due to the dynamic nature of MANET it is more prone to such kind of attacks. In MANET the solutions are designed corresponding to specific attacks they work well in the presence of these attacks but they fail under different attack scenario.

Therefore, our aim is to develop a multi-functional security system for MANET, which will cover multiple attacks at a time and also some new attacks.

7. FUTURE WORK

This paper can be further extended to give the solutions corresponding to these attacks which we discussed at different

layers of MANET, we can add more detection techniques if it is possible to invent them.

8. REFERENCES

[1] Boora, S. et. al (2011). A Survey on Security Issues in Mobile Ad-Hoc Networks, International Journal of Computer Science & Management Studies, Vol. 11, Issue 2.

[2] Biswas, K. et. al (2007). Security threats in Mobile Ad-hoc Network, Master theses, Department of Interaction & System Design, Blekinge Institute of Technology, Sweden.

[3] Gua, Y. (2008). a dissertation on Defending MANET against flooding attacks by detective measures, Institute of Telecommunication Research, The University of South Australia.

[4] Hu,Y-C. et. al (2003). Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, Proceedings of ACM WiSe 2003, San Diego, CA.

[5] Hu,Y-C. et. al (2006). Wormhole attacks in Wireless Networks, IEEE JSAC, Vol. 24, No. 2.

[6] Ishrat, Z. (2011). Security issues, challenges & solution in MANET, IJCST, Vol. 2, Issue 4.

[7] Khokhar, R. et. al (2008). A review of current routing attacks in Mobile Ad-Hoc Networks, International Journal of Computer Science & Security, Vol. 2, Issue 3.

[8] Mamatha, G. S. et. al (2010). Network Layer Attacks and Defense Mechanisms in MANETS- A Survey, International Journal of Computer Applications, Vol. 9, No. 9.

[9] Nguyen, H. et. al (2006). Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks, International Conference on Mobile Communications and Learning Technologies.

[10] Pandey, A. et. al (2010). A Survey on Wireless Sensor Networks Security, International Journal of Computer Applications, Vol. 3, No. 2.

[11] Rai, P. et. al (2010). A Review of MANETs Security Aspects and Challenges, IJCA Special Issue on "Mobile Ad-hoc Networks".

[12] Sivakumar, K. et. al (2013). overview of various attacks in manet and countermeasures for attacks, International Journal of Computer Science and Management Research, Vol. 2.

[13] Wazid, M. et. al (2011). A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques, International Conference on Computer Communication and Networks CSI-COMNET.