Chapter 3

Security Attacks

3.1 Overview

Due to the fact that MANET is a group of nodes that form a temporary network without centralized administration, the nodes have to communicate with each other based on unconditional trust. This characteristic leads to the consequence that MANET is more susceptible to be attacked by inside the network while comparing to other type of networks. Practically, MANET could be attacked by several ways using multiple methods; before going to deeper investigation, it is necessary to classify security attacks within the context of MANET. Recent research on MANET shows that the MANET has larger security issues than conventional networks. Any security solutions for static networks would not be suitable for MANET. Singh et al, discussed several types of attacks that can easily be performed against a MANET. Many researchers define several algorithms for MANETs is well established with many works improving on requirement of networks, each give an overview of some of the difficulties of implementing MANETs.

Therefore, security in MANETs is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats. A MANETs is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

In this chapter we, investigate some of the important attacks might be related to security in MANETs. The end of this chapter, we identified that most of the attacks against ad hoc networks are actually launched. Finally, we conclude this chapter.

3.2 What is Attack?

In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data.
Different attack methods target different vulnerabilities and involve different types of weapons, and several may be within the current capabilities of some terrorist groups.

3.3 Layer Attacks on MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Security means protecting the privacy (confidentiality), availability, integrity and non-repudiation. Security implies the identification of potential attacks from unauthorized access, use, modification or destruction. The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack.

3.3.1. Attacks at Physical Layer Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

3.3.2. Attacks at Data link Layer The data link layer can classified attacks as to what effect it has on the state of the network as a whole. Some of the attacks identified at physical layer include Jamming, Interception, Eavesdropping, Active Interface etc.

3.3.3. Attacks at Network Layer The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic.

Some of the attacks identified at physical layer include Wormhole, Location Disclose, Resource Consumption, Flooding, Black hole, Gray hole, routing attacks etc.

3.3.4. Attacks at Transport Layer Some of the attacks identified at physical layer include TCP/UDP, Session Hijacking, and SYN Flooding etc.

3.3.5. Attacks at Application Layer Some of the attacks identified at physical layer include Repudiation attacks, malicious code attacks, data corruptions attacks etc.

A complete picture of attack types on layers is helpful for the effectively mitigations of these attacks. In figure-3.1 attacks on layers are broadly classified for this purpose

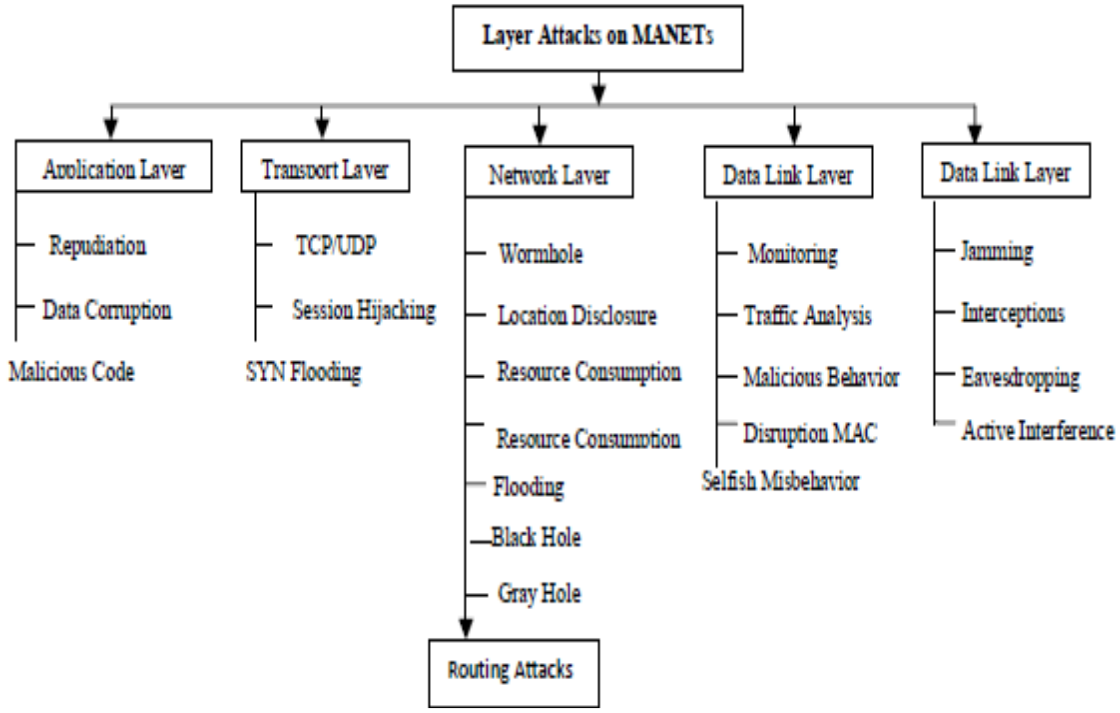

Figure 3.1 Attacks in various layers of MANET [1]

3.4 Other Classification of Attacks

Attacks can also be categorized on the basis of its source, behavior and nodes. Figure-3.2 shows such categorization:

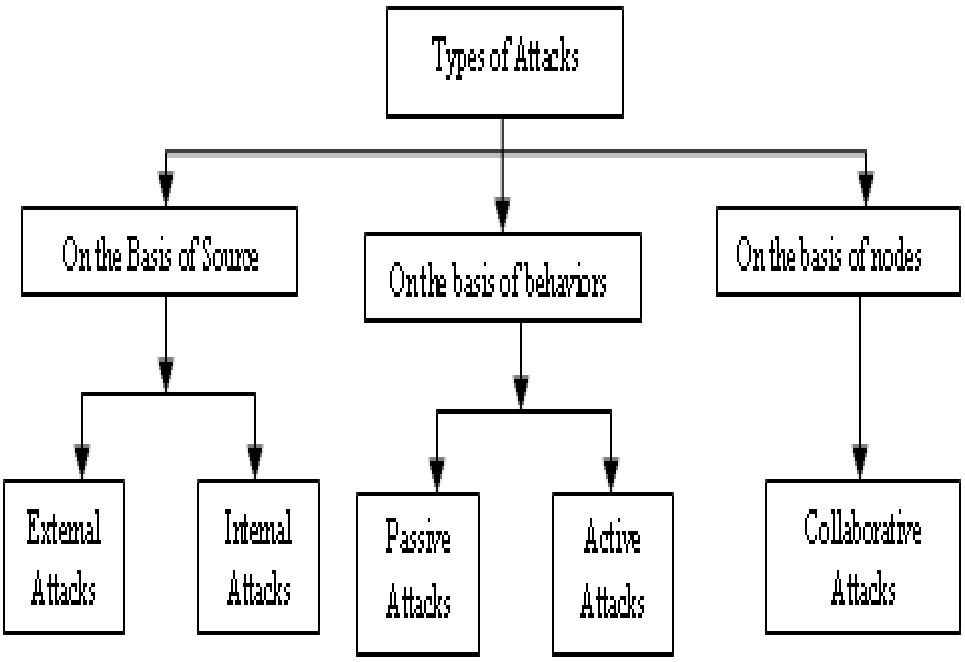

Figure 3.2 Categorization of Attacks in MANETs

3.4.1. On the Basis of Source On the basis of source, attacks can be classified as external and internal attacks. External attacks are caused by the nodes which are not a part of the network. External attackers are the aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks are caused by the nodes which are a part of the network. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

3.4.1.1 Passive Attacks Some important passive attacks are: Snooping Attacks, Eavesdropping Attacks, Traffic Analysis Attacks, and Traffic Monitoring Attacks.

- **Snooping Attacks** Snooping Attack is also known as masquerade or impersonation or spoofing Network attack. In this attack, a single malicious node attempts to take out the identity of other nodes' in the network by advertising false/fake routes. It then attempts to send packets over network with identity of other nodes making the destination believe that the packet is from original source [30].
- **Eavesdropping Attacks** The eavesdropping attacks are serious security threat to a wireless sensor network (WSN) since the eavesdropping attack is a prerequisite for other attacks.
- **Traffic Analysis Attacks** Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security. In this type of attack, an attacker tries to sense the communication path between the sender and receiver. This way attacker found the amount of data which is travel between the route of sender and receiver. There is no alteration in data by the traffic analysis.

- **Monitoring Attacks** Monitoring is another passive attack in which attacker can see the confidential data but he cannot change the data or cannot modify the data.

3.4.1.2. Active Attacks Active attack: Some important passive attacks are: Blackmail, Denial of service attack Fabrication, Gray hole Attacks, Disclosure Attacks, Routing Attacks and Recourse Consumption Attacks.

- **Blackmail Attacks** A black mail attack is relevant against routing protocols that uses mechanisms for identification of malicious nodes and propagate messages that try to blacklist the offender.
- **Denial of service attacks** Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.
- **Fabrication Attacks** The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [31].
- **Gray hole Attacks** a gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. In this attack, an attacker drops all data packets but it lets control messages to route through it [32].
- **Disclosure attacks** Disclosure attacks are aimed at acquiring system-specific information about a website such as software distribution, version numbers, and patch levels. The acquired information might also contain the location of backup files or temporary files [33].
- **Routing Attacks** In Routing Attacks, attackers try to alter the routing information and data in the routing control packet. There are several types of routing attacks mounted on the routing protocol which are intended for disturbing the operation of the network
- **Resource Consumption Attack** In Resource Consumption Attack, a malicious node intentionally tries to consume or misuse of the resources (battery power, bandwidth, and computational power) of other nodes' exist in the network by

requesting excessive route discovery (unnecessary route request control messages), very frequent generation of beacon packets, or by forwarding unnecessary packets (stale information) to that node [34].

3.4.2. On the basis of Behavior A passive attack attempts to retrieve valuable information by listening to traffic channel without proper authorization, but does not affect system resources and the normal functioning of the network. Passive attacks are very hard to detect because they do not involve any alteration of the data. An active attack attempts to change or destroy the system resources. It gains an authentication and tries to affect or disrupt the normal functioning of the network services by injecting or modifying arbitrary packets of the data being exchanged in the network. An active attack involves information interruption, modification, or fabrication.

3.4.3. On the basis of Nodes In these types of attacks, there are numerous nodes involved during the attack. These nodes can be physically existent or not existing at all.
In this chapter we discuss the different attacks related to on the basis of behavior and on the basis of nodes.

Collaborative attacks Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network. Multiple attacks occur when a system is disturbed by more than one attacker, but not necessarily in collaboration. We have study different types of attacks and then provided the definition of collaborative attacks; we are now going to categorize these attacks into two different categories. First: Direct Collaborative Attacks and Second: Indirect Collaborative Attacks.
Here, the attacker nodes are already in existence in the original network or a malicious node joins the network or an internal node is compromised in the network. This kind of collaborative attacks can be referred to as direct collaborative attacks. A Black hole and Wormhole attack belongs to this category.

- 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 [35].

- In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

  The attacker used different non-existent nodes in order to fake other nodes to redirect data packets to malicious node. This kind of collaborative attacks can be referred to as indirect collaborative attacks. A Sybil and Routing table overflow attacks belongs to this category.

  - Sybil attack refers to the multiple copies of malicious nodes. It can be happen, if the malicious node shares its secret key with other malicious nodes. This way the number of malicious node is increased in the network and the probability of the attack is also increased. If we use the multipath routing, then the possibility of choosing a path in the network, those contain the malicious node will be increased [36-37]. The malicious node makes routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

3.5 CONCLUSION

In this chapter we addressed existing potential security threats in MANETs. In this study we found that most of the work on MANET security focused on single layer attacks i.e. active and passive attacks. In the meanwhile some attacks involving multiple nodes have

received little attention since they are surprising and combined attack i.e. collaborative attacks. There have been no proper definition and categorization of these kinds of collaborative attacks in MANETs. Thus, protection of communication system against these types of attacks is a challenging task. Therefore, deep study on collaborative attacks and development of new protocols/algorithms/model to manage these attacks is the need of hour. Development of a multi-fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many known and unknown security threats is also given importance.