Attacks and Security in MANET

Shabnam Kumari[1], Neetu Sharma[2], Reema[3], Sunita Kumari[4]
[1, 2, 3, 4] Department of CSE
[1, 2, 3] Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India
[4] G.B.Pant Egineering College, Okhla, New Delhi, India

Abstract- *Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications such as building, traffic surveillance, MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability. Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Some of the attacks such as modification, fabrication, impersonation and denial of service attacks are due to misbehavior of malicious nodes, which disrupts the transmission.*

Keywords- MANET, VANET, iMANET, OLSR, DSDV

I. INTRODUCTION

1. MANET:

Mobile Ad Hoc Network (MANET) is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the w ireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure [1]. MANET is a self-configuring infrastructureless network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".

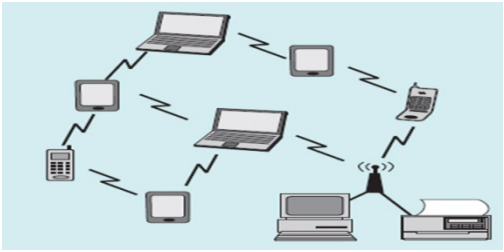

Figure 1. Mobile Ad Hoc Network (MANET).

The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc [2].

The MANET can be used in the applications such as rescue operations, tactical operations, environmental monitoring, conferences, connecting soldiers in battlefields and social or business application such as Public and Personal Area Networks [4]. The weaknesses of ad hoc networks are dynamic topology, lack of infrastructure, exposure of nodes and channels [5].

II. TYPES OF MANET

There are three types of MANET. It includes:

1. **Vehicular Ad hoc Network (VANETs):** VANETs are used for communication among vehicles and between vehicles and roadside equipment.

2. **Intelligent Vehicular Ad hoc Networks (InVANETs):** InVANETs are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

3. **Internet Based Mobile Ad hoc Networks (iMANET):** iMANET are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad-hoc routing algorithms don't apply directly.

III. CHARACTERISTICS OF MANET

Request For Comments (RFC) 2501 document [8] which is published by MANET working group within the IETF describes the main characteristics of MANET which differs from the characteristics of traditional wireless local area networks such as WLANs due to the dynamic and the infrastructureless natures of MANETs [9]. According to the

IETF RFC 2501, MANET has characteristics can be divided into the following:

1. A collection of autonomous terminals means that within a MANET, each mobile node performs its tasks as a router and a host.
2. It contains a dynamic topology which means there are a group of nodes into it that are moving and resulting to a random change rapidly at unpredictable times through the network topology.
3. A distributed operation is contained into it which means that the network's management and control is spread (distributed) in the nodes because of the infrastructure types' absence of which the central control of the network operations is supported.
4. It can be deployed as fast as it could be.
5. Pre-existing infrastructure is independent from it.
6. Bandwidth-constrained, variable capacity links compared with the wired network environment, the capacity of the wireless link itself is relatively small, but also susceptible to external noise, interference, and signal attenuation effects.
7. Self-adapts to the propagation patterns and connectivity.
8. Adapts to mobility patterns and traffic.
9. A limited physical security is contained into it, for example, in the absence of any centralized encryption or authentication. In order to reduce security threats, existing techniques of link security are at most applied into the WLANs and the wired networks.
10. It has an energy constrained operation a laptop or handheld computers are often used batteries to provide power, how to save electricity in the context of depletion of system design is also necessary to consider the point.

III. SECURITY IN MANET

Security remains as a concern in MANET. In general, a MANET is vulnerable due to its fundamental cooperation of open medium, absence of central authorities, dynamic topology, distributed cooperation and constrained capability [15]. A node in the MANET without any adequate protection can become an easy target for attacks. Attacker just needs to be within radio range of a node in order to intercept the network traffic.

There are basically two approaches to securing a MANET:

1. **Proactive:** The proactive approach attempts to prevent security attack, typically through various cryptographic techniques. Most of the secure routing protocols adopt proactive approach to securing routing control messages. The main characteristic of these protocols is the constant maintaining of a route by each node to all other network nodes. The route creation and maintenance are performed through both periodic and event-driven (e.g., triggered by links breakages) messages.

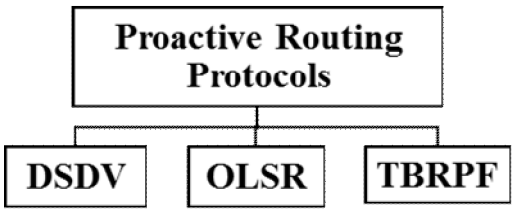

Figure 2. Various Proactive Protocols.

a) **Destination Sequenced Distance Vector (DSDV):** The Destination-Sequenced Distance-Vector (DSDV) protocol [6] is a distance-vector protocol with extensions to make it suitable to MANET. Every node maintains a routing table with one route entry for each destination in which the shortest path route (based on number of hops) is recorded.

b) **Optimized Link State Routing (OLSR):** OLSR protocol [7] is an optimization for MANET of legacy link-state protocols. The key point of the optimization is the multipoint relay (MPR). Each node identifies (among its neighbors) its MPRs. By flooding a message to its MPRs, a node is guaranteed that the message, when retransmitted by the MPRs, will be received by all its two-hop neighbors.

c) **Topology Dissemination Based on Reverse-Path Forwarding (TBRPF):** TBRPF [8] is a link-state routing protocol that employs a different overhead reduction technique. Each node computes a shortest path tree to all other nodes, but to optimize bandwidth only part of the tree is propagated to the neighbors.

2. **Reactive:** The reactive approach finds an attack and reacts accordingly. Most of the secure routing protocols adopt reactive approach to secure data packet forwarding messages. These protocols depart from the legacy Internet approach. To reduce the overhead, the route between two nodes is discovered only when it is needed.

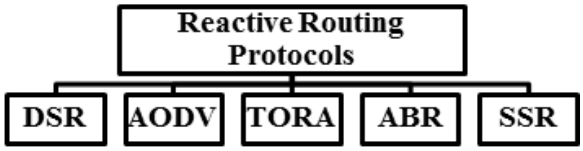

Figure 3. Various Reactive Protocols.

Both approaches has their own merits and suitable for different issues of security in MANET. A complete security solution requires both proactive and reactive approaches.

a) **Dynamic Source Routing (DSR):** DSR is a loop-free, source based, on demand routing protocol [9], where each node maintains a route cache that contains the source routes learned by the node. The route discovery process is only initiated when a source node do not already have a valid route to the destination in its route cache; entries in the route cache are continually updated as new routes are learned. Source routing is used for packets forwarding.

b) **Ad hoc On Demand Distance Vector (AODV):** AODV is a reactive improvement of the DSDV protocol. AODV minimizes the number of route broadcasts by creating routes on-demand [10], as opposed to maintaining a complete list of routes as in the DSDV algorithm. Similar to DSR, route discovery is initiated on-demand, the route request is then forward by the source to the neighbors, and so on, until either the destination or an intermediate node with a fresh route to the destination, are located.

c) **Temporally Ordered Routing Algorithm (TORA):** TORA is another source-initiated on-demand routing protocol built on the concept of link reversal of the Directed Acyclic Graph (ACG) [10]. In addition to being loop-free and bandwidth efficient, TORA has the property of being highly adaptive and quick in route repair during link failure, while providing multiple routes for any desired source/destination pair.

d) **Associativity Based Routing (ABR):** ABR [11] protocol is also a loop free protocol, but it uses a new routing metric termed degree of association stability in selecting routes, so that route discovered can be longer-lived route, thus more stable and requiring less updates subsequently. The limitation of ABR comes mainly from a periodic beaconing used to establish the association stability metrics, which may result in additional energy consumption.

e) **Signal Stability Algorithm (SSA):** SSA [11] is basically an ABR protocol with the additional property of routes selection using the signal strength of the link.

V. ATTACKS IN MANET

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types.

1. **Internal Attacks:** Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes [15, 14]. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes.

2. **External attacks:** These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc [14]. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories:

a) **Passive attacks:** MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic [14, 13].

b) **Active Attacks:** Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks [14, 13, 14].

VI. NETWORK PROTOCOL ATTACKS

Security attacks are also classified on the basis of various layers of the network protocol stack. These can be classified as follows:

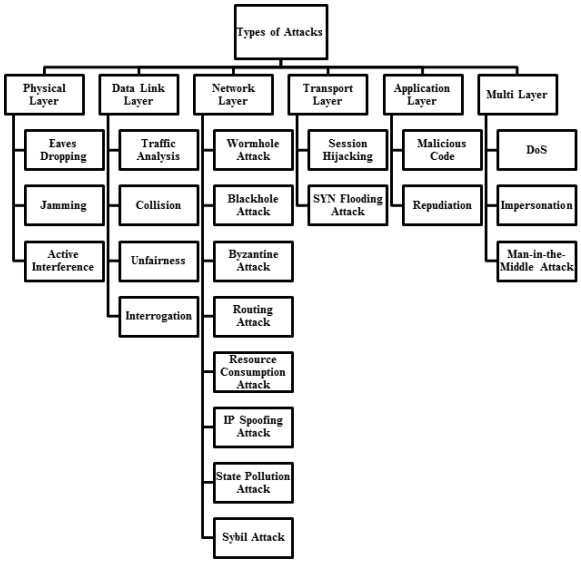

Figure 4. Types of Attacks.

1. Attacks at Physical Layer:

The attacks on physical layer are hardware oriented and they need help from hardware sources to come into effect [14]. These attacks are simple to execute as compared to other attacks. They do not require the complete knowledge of technology. Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

a) **Eavesdropping:** Eavesdropping can also be defined as interception and reading of messages and conversations by unintended receivers [14]. As the communication takes place on wireless medium can easily be intercepted with receiver tuned to the proper frequency.

b) **Jamming:** Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

c) **Active Interference:** An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use [14]

.

2. Attacks at Data link / MAC layer:

The algorithms used in data link layer/MAC layer are susceptible to many DoS attacks. MAC layer attacks can be classified as to what effect it has on the state of the network as a whole [14]. The effects can be measured in terms of route discovery failure, energy consumption, link breakage initiating route discovery and so on.

a) Traffic Analysis [14]: In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self organization in the network, and valuable data about the topology can be gathered.

b) Collision : This is very much similar to the continuous channel attack. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid. A typical defense against collisions is the use of error-correcting codes.

c) Unfairness : Repeated application of these exhaustion or collision based MAC layer attacks or an abusive use of cooperative MAC layer priority mechanisms, can lead into unfairness. This kind of attack is a partial DOS attack, but results in marginal performance degradation. One major defensive measure against such attacks is the usage of small frames, so that any individual node seizes the channel for a smaller duration only.

d) Interrogation : Exploits the two-way request-to-send/clear to send (RTS/CTS) handshake that many MAC protocols use to mitigate the hidden-node problem. An attacker can exhaust a node's resources by repeatedly sending RTS messages to elicit CTS responses from a targeted neighbor node. To put a defense against such type of attacks a node can limit itself in accepting connections from same identity or use Anti replay protection and strong link-layer authentication.

3. Attacks at Network Layer:

The network layer protocols enable the MANET nodes to be connected with another through hop-by-hop [14]. In MANETs every individual node takes route decision to forward the packet, so it's very easy for malicious node to attack on such network.

a) Wormhole attack : An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on- demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

b) Black-hole attack : The black-hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets.

c) Byzantine attack : A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

d) Routing Attacks : There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are described briefly below.

e) Resource consumption attack : This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

f) IP Spoofing attack : In conflict-detection allocation, the new node chooses a random address (say y) and broadcast a conflict detection packet throughout the MANET. Any veto from a node will prevent it from using this address. If the malicious node always impersonates a member that has occupied the same IP address and keeps replying with vetoes, it is called an IP Spoofing attack.

g) State Pollution attack : If a malicious node gives incorrect parameters in reply, it is called the state pollution attack. For example, in best effort allocation, a malicious allocator can always give the new node an occupied address, which leads to repeated broadcast of Duplication Address Detection messages throughout the MANET and the rejection of new node.

h) Sybil attack : If a malicious node impersonates some nonexistent nodes, it will appear as several malicious nodes conspiring together, which is called a Sybil attack. This attacks aims at network services when cooperation is necessary, and affects all the auto configuration schemes and secure allocation schemes based on trust model as well. However, there is no effective way to defeat Sybil attacks.

4. Attacks at Transport Layer:

The objectives of TCP-like Transport layer protocols in WSN include setting up of end-to-end connection, end- to-end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection. Similar to TCP protocols in the Internet, the mobile node is vulnerable to the classic SYN flooding attack or session hijacking attacks [31, 32, 33].

a) Session Hijacking : Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc) and other information from nodes. Session hijacking attacks are also known as address attack which make affect on OLSR protocol.

b) SYN Flooding Attack : The SYN flooding attacks are the type of Denial of Service (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node. These half opened connection are never completes the handshake to fully open the connection.

5. Attacks at Application Layer :

Application layer protocols are also vulnerable to many DoS attacks. The application layer contains user data. It supports protocols such as HTTP, SMTP, TALNET and FTP, which provides many vulnerabilities and access points for attackers.

a) Malicious code attacks : Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

b) Repudiation attacks : Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services.

VII. CONCLUSION

The major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Some of the attacks such as modification, fabrication, impersonation and denial of service attacks are due to misbehavior of malicious nodes, which disrupts the transmission. In the paper we have studied various types of attacks at different layers of models.

REFERENCES

[1] Saleh Ali K. Al-Omari, Putra Sumari, "An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications", Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (J GRAPH-HOC) Vol.2, No.1, March 2010

[2] www.en.wikipedia.org/wiki/Mobile_ad_hoc_network.html

[3] Mohit Kumar, Rashmi Mishra, "An Overview of MANET: History, Challenges and Applications", Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976-5166 Vol. 3 No. 1 Feb-Mar 2012

[4] Sevil ¸ Sen, John A. Clark, "A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad Hoc Networks", Proceedings of the second ACM conference on Wireless network security, 2009

[5] Yian Huang, Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", International journal of computer applications, 2011

[6] http://wirnet.blogspot.in/2009/09/types-of-manet.html

[7] Saleh Ali Alomari and Putra Sumari, "Multimedia Applications for MANETs over Homogeneous and Heterogeneous Mobile Devices"

[8] IETF (1999) RFC 2501 - Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, www.faqs.org /rfcs/rfc-sidx13.html

[9] Hekmat, R. (2006) Ad-hoc Networks: Fundamental Properties and Network Topologies, A book published by Springer.

[10] M.S. Corson, J.P. Maker, J.H. Cernicione, Internet-based mobile ad hoc networking, IEEE Internet Computing 3 (4) (1999) 63–70

[11] C.-F. Chiasserini, R.R. Rao, Pulsed battery discharge in communication devices, in: Proceedings of The Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM _99), August 15–19, 1999, Seattle, WA, pp. 88–95.

[12] I. Chlamtac, A. Lerner, Link allocation in mobile radio networks with noisy channel, in: IEEE INFOCOM, Bar Harbour, FL, April 1986

[13] Rishabh Jain, Charul Dewan, Meenakshi, A Survey on Protocols & Attacks in MANET Routing, IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012 ISSN (Online): 1051 –5138

[14] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Wireless Communications, IEEE In Wireless Communications, IEEE, Vol. 14, No. 5. (06 December 2007), pp. 85-91.

[15] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Wireless Communications, IEEE In Wireless Communications, IEEE, Vol. 14, No. 5. (06 December 2007), pp. 85-91.