Security Threats in Mobile Ad Hoc Network

Nitesh Chouhan
Assistant Professor, Dept. of Information Technology, MLV Textile & Engineering College, Bhilwara, Rajasthan , India

Abstract-Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET.

Keywords: *MANET, vulnerability, security attacks, peer-to-peer, topology.*

1. Introduction:

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multihop paths through the network to any other node. This idea of Mobile ad hoc network is also called infrastructureless networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly [2].

2. Goals:

In this paper, we focus on the overall security threats and challenges in Mobile ad hoc networks (MANET). The security issues are analyzed from individual layers namely application layer, transport layer, network layer, link layer and physical layer. This modularity extends the clarity and depicts the original scenario in each layer. The solutions of the current problems are also reported here so that one may get direction. This study provides a good understanding of the current security challenges and solutions of the MANETs. In general the following questions are addressed in our paper:

1. What are the vulnerabilities and security threats in MANET? Which level is most vulnerable to attack?

2. How the security services like confidentiality, integrity and authentication can be achieved from mobile ad hoc networks? What steps should be taken?

3. What are the countermeasures? How the security of the entire system is ensured?

4. What are the potential dangers that may be crucial in future?

3. Security measures:

Security Attacks on each layer in MANET:

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping

Security Solutions for MANET:

Layer	Security Issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authentication and securing end-to-end or point-to-point communication through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Data link layer	Protecting the wireless MAC protocol and providing link layer security support
Physical layer	Preventing signal jamming denial-of-serviceattacks

The ultimate goals of the security solutions for MANETs is to provide security services,such as authentication, confidentiality, integrity, authentication, nonrepudiation,anonymity and availability to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. There is no single mechanism that will provide all the security services in MANET.

Security threats and countermeasures:

Layers	Attacks	Solutions
Application layer	Lack of cooperation attacks, Malicious code attacks (virus, worms, spywares, Trojan horses) etc.	Cooperation enforcement (Nuglets, Confidant, CORE) mechanisms, Firewalls, IDS etc.
Transport layer	Session hijacking attack, SYN flooding attack, TCP ACK storm attack etc.	Authentication and securing end-to-end or point-to-point communication, use of public cryptography (SSL, TLS, SET, PCT) etc.
Network layer	Routing protocol attacks (e.g. DSR, AODV etc.), cache poisoning, table overflow attacks, Wormhole, blackhole, Byzantine, flooding, resource consumption, impersonation, location disclosure attacks etc.	Source authentication and message integrity mechanisms to prevent routing message modification, Securing routing protocols (e.g. IPSec, ESP, SAR, ARAN) to overcome blackhole, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack etc.
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness etc.	No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP, using WPA etc.
Physical layer	Jamming, interceptions, eavesdropping	Using Spread spectrum mechanisms e.g. FHSS, DSSS etc.

4. Types of security attacks:

The current Mobile ad hoc networks allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure insuch a network. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand,passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. In this chapter, our focus is on vulnerabilities and exposures in the current ad hoc network. We have classified the attacks as modification, impersonation, fabrication,wormhole and lack of cooperation.

4.1 Attacks Using Modification:

Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct DoS attacks by modifying message fields or by forwarding routing message with false values. In fig. 4.1, M is a malicious node which can keep traffic from reaching X by continuously advertising to B a shorter route to X than the route to X that C advertises[14]. In this way, malicious nodes can easily cause traffic subversion and denial of service (DoS) by simply altering protocol fields: such attacks compromise the integrity of routing computations. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.

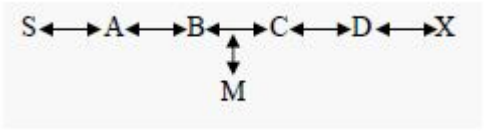

Fig 4.1

Consider the following fig. 4.2. Assume a shortest path exists from S to X and, C and X cannot hear each other, that nodes B and C cannot hear other, and that M is a malicious node attempting a denial of service attack. Suppose S wishes to communicate with X and that S has an unexpired route to X in its route cache. S transmits a data packet toward X with the source route S --> A --> B --> M --> C --> D --> X contained in the packet'sheader. When M receives the packet, it can alter the source route in the packet's header,such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to forward the packet to X. Since X cannot hear C, the transmission is unsuccessful [14].

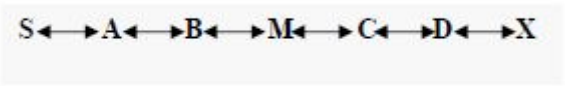

Fig 4.1

4.2 Attacks Using Impersonation:

As there is no authentication of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing.Spoofing is occurred when a malicious node misrepresents its identity in the network(such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network.

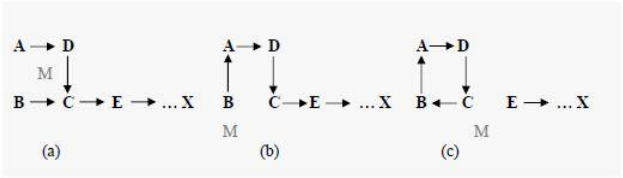

Fig 4.3

4.3 Attacks through Fabrication:

Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages. Such kind of attacks can be difficult to verify as they come as valid constructs, especially in the case of fabricated error messages

that claim a neighbor cannot be contacted [11]. Consider the fig. 4.1.Suppose node S has a route to node X via nodes A, B, C, and D. A malicious node M can launch a denial-of-service attack against X by continually sending route error messages to B spoofing node C, indicating a broken link between nodes C and X. B receives the spoofed route error message thinking that it came from C. B deletes its routing table entry for X and forwards the route error message on to A, who then also deletes its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to X, M can successfully prevent communications between S and X.

4.4 Wormhole Attacks:

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers. In the fig. 4.4, M1 and M2 are two malicious nodes that encapsulate data packets and falsified the route lengths.

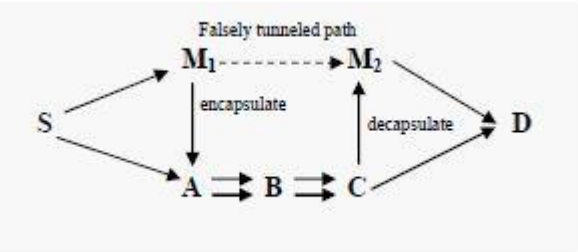

Fig 4.4

Suppose node S wishes to form a route to D and initiates route discovery. When M1

receives a RREQ from S, M1 encapsulates the RREQ and tunnels it to M2 through an

existing data route, in this case {M1 --> A --> B --> C --> M2}. When M2 receives the encapsulated RREQ on to D as if had only traveled {S --> M1 --> M2 --> D}. Neither M1 nor M2 update the packet header. After route discovery, the destination finds two routes from S of unequal length: one is of 5 and another is of 4. If M2 tunnels the RREP back to M1, S would falsely consider the path to D via M1 is better than the path to D via A. Thus,tunneling can prevent honest intermediate nodes from correctly incrementing the metricused to measure path lengths.

4.5 Lack of Cooperation:

Mobile Ad Hoc Networks (MANETs) rely on the cooperation of all the participating

nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets.

But one of the different kinds of misbehavior a node may exhibit is selfishness. A

selfishness node wants to preserve own resources while using the services of others and consuming their resources. This can endanger the correct network operation by simply not participating to the operation or by not executing the packet forwarding. This attack is also known as the black hole attack.

5. Conclusion:

The security of the ad hoc networks greatly depends on the secure routing protocol,

transmission technology and communication mechanisms used by the participating

nodes. In this paper, we have focused on the common attacks in MANET. The rest of

the thesis describes the threats in each layer in the protocol stack and prescribes solution of those attacks**.**

6.References:

[1] S. Capkun, L. Buttyan, and J. Hubaux, "Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks," 2003.

[2] P. Michiardi, R. Molva, "Ad hoc networks security," IEEE Press Wiley, New York, 2003.

[3] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," Internet Draft, 2000.

[4] R. Ramanathan, J. Redi and BBN Technologies, "A brief overview of ad hoc networks: challenges and directions," IEEE Communication Magazine, May 2002, Volume: 40, page(s): 20-22, ISSN: 0163-6804