Vulnerability and Security of Mobile Ad hoc Networks

ALI GHAFFARI
Islamic Azad University(Tabriz Branch)
IRAN

Abstract:- Mobile Ad-Hoc Networks (MANETs) are becoming increasingly popular as more and more mobile devices find their way to the public, besides “traditional” uses such as military battlefields and disaster situations they are being used more and more in every-day situations. With this increased usage comes the need for making the networks secure as well as efficient, something that is not easily done as many of the demands of network security conflicts with the demands on mobile networks due to the nature of the mobile devices . The concept and structure of MANETs make them prone to be easily attacked using several techniques often used against wired networks as well as new methods particular to MANETs. Security issues arise in many different areas including physical security, key management, routing and intrusion detection, many of which are vital to a functional MANET.

Key-words:- Manet, attack, security, threat, dos

1. Introduction

A mobile ad hoc network is a collection of wireless mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis [1]. There are some unique characteristics of mobile ad hoc networks:

First, the connections between network nodes are wireless, and the communication medium is broadcast. The wireless connection provides the nodes with freedom to move, so the mobile nodes may come together as needed and form a network, not necessarily with any assistance from the cable connections.

Second, unlike traditional wireless networks, mobile ad hoc networks do not have any fixed infrastructure. It is only a collection of self-organized mobile nodes, which are connected through high-variable quality links. Thus, the network topology is always changing. Third, the membership is always changing. The mobile nodes are free to move anywhere, leave at any time and new nodes can enter unexpected. There is no mechanism to administrate or manage the membership.Fourth, the execution environment is insecure and unfriendly. Due to the lack of fixed infrastructure and administration, there are increased chances malicious nodes can mount

attacks. Also, nodes may behave selfishly and result a degradation of the performance or even disable the functionality.

2. Security goals and threats

In mobile ad hoc networks, all networking functions, such as routing and packet forwarding, are performed by the nodes themselves in a self-organizing manner. For this reason, such networks have increased vulnerability and securing a mobile ad hoc network is very challenging. The following attributes are important issues related to mobile ad hoc networks, especially for those security-sensitive applications [1,2]:

- Availability ensures the survivability of network services despite denial of service attack.
- Confidentiality ensures that certain information is never disclosed to unauthorized entities.
- Integrity guarantees that a message being transferred is never corrupted.
- Authentication enables a node to ensure the identity of the peer node it is communicating with.
- Non-repudiation ensures that the origin of a message cannot deny having sent the message.

Because of the nature of ad hoc, it is extremely difficult to achieve the above security goals in mobile ad hoc networks. Threats that mobile ad hoc networks have to face can be classified into two levels: attacks on the basic mechanism and attacks on the security mechanism [3]. The vulnerability of the basic mechanism includes:

- Nodes risk being captured and compromised.
- Algorithms are assumed to be cooperative, but some nodes may not respect the rules.
- Routing mechanisms are more vulnerable.

Vulnerability of the security mechanism includes:

- Public key can be maliciously replaced.
- Some keys can be compromised.
- The trusted server can fall under the control of a malicious party.

3. Security threats for routing protocols

Mobile ad hoc networks are networks with no fixed infrastructure and network functions are carried out by all available nodes, which are highly mobile and have constrained power resources . Consequently, mobile ad hoc network has increased sensitivity to node misbehavior [4,5,6]. There are two sources of attacks related to node misbehavior in mobile ad hoc networks [7]. The first is *external attacker*, in which unauthenticated attackers can replay old routing information or inject false routing information to partition the network or increase the network load. The second is *internal attack*, which comes from the compromised nodes inside the network. Since compromised nodes can be authenticated, internal attacks are usually much harder to detect and can create severe damage.

The goal of an active attack is to disrupt the proper function of the network. This may be achieved by several ways :

- Denial of service:

- Route Disruption (RD): breaking down an existing route or preventing a new route from being established.

- Direct Denial of Service (DDoS): preventing a given node from communicating with any other node in the network.

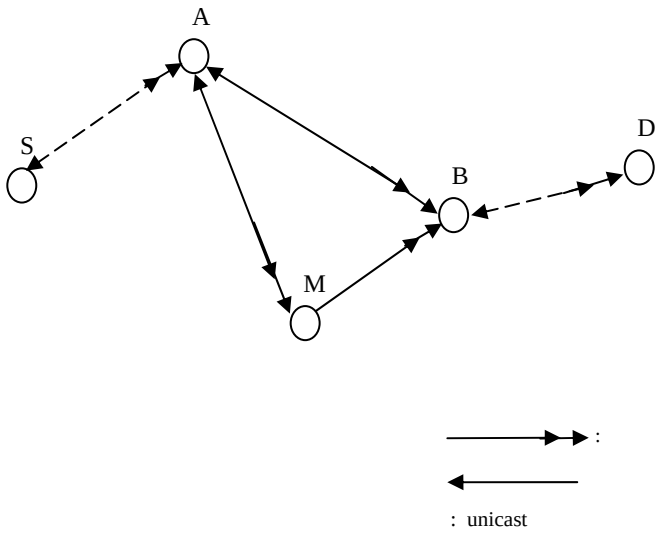
- Resource Consumption (RC): consuming the communication bandwidth in the network or resource at individual node.

- Route Invasion (RI): an attacker adds itself into a route between two nodes and takes control of the route.

Exploits against mobile ad hoc network routing protocols can be classified into modification, fabrication, tunneling attack, denial of service attack, invisible node attack, Sybil attack.

3.1.Modification

Malicious nodes can modify the protocol fields of messages passed among nodes. Such attacks compromise the integrity of routing computation. By altering routing information, an attacker can cause network traffic to be dropped, redirected to a different destination or take a long route to the destination increasing communication delays [7,8]. Using AODV as an example, a malicious node can either increase the *broadcast_id in* RREQ to make the faked RREQ message acceptable, or it can decrease the *hop_cnt* to update other nodes' reverse routing tables. In the network illustrated in Figure 1, a malicious node M can increase the chances it is included on a newly created route from source node *S* to destination node *D* by consistently advertising to *A* a shorter route to *D* than that *B* advertises.



S: source node D: destination node
M: malicious node A, B, M: intermediate node

Figure 1. Redirection with modification

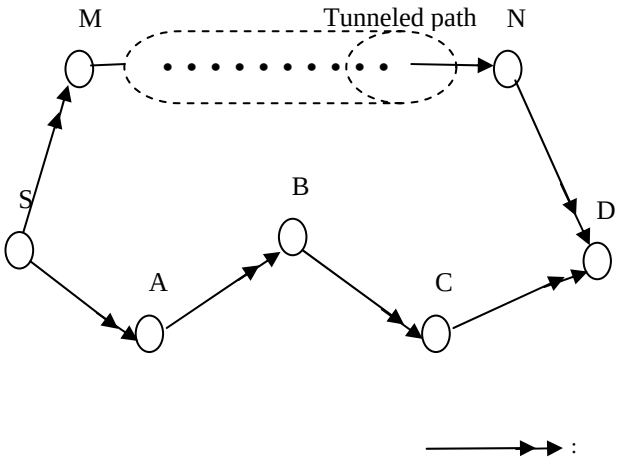
3.2.Fabrication

Fabrication refers to attacks performed by generating false routing messages. Following is an example of an attack launched by sending false route error message. Suppose S has a route to D via nodes A and B, as in Fig. 1. A malicious node M can launch a denial-of-service attack by continually sending route error messages to A spoofing B, indicating a broken link between B and D. A receives the spoofed route error message thinking that it came from B. A deletes its routing table entry for D and forwards the route error message on to

the upstream node, who then also delete its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to D, M can successfully prevent communications between S and D.

3.3.Tunneling attack

Tunneling attack is also called wormhole attack. In a tunneling 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. It is called tunneling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers [8,9,10].



S: source node **D:** destination node **M, N:** malicious node **A, B, C:** intermediate node

Figure 2. Tunneling attack

In Figure 2, M receivers RREQ, and tunnels it to N. When N receives the RREQ, it forwards the RREQ to D as if it had traveled S, M and N. N also tunnels the RREP back to M. By doing this, M, N falsely claim a path between them and fool S to choose the path through M, N (because it has shorter path length).

3.4 Denial of service attack

By saying denial of service attack, we refer to an attack that a malicious node floods irrelevant data to consume network bandwidth or to consume the resources (e.g. power, storage capacity or computation resource) of a particular node. With fixed infrastructure networks, we can control denial of service attack by using "Round Robin Scheduling", but with mobile ad hoc networks, this approach has to be extended to adapt to the lack of infrastructure, which requires the identification of neighbor nodes by using cryptographic tools, and cost is very high.

3.5.Invisible node attack

The attack occurs when an intermediate node M does not append its IP address to the *route record* field of the SRP header. In SRP, the destination node D uses the accumulated *route record* to establish a path between the source node S and itself. The result of the attack is that M becomes "invisible" in the path and S erroneously believes a path exists between D and itself that does not depend on M. If M leaves the mobile ad hoc network, any route maintenance technique will be

unable to notify S that the route is no longer intact because M is "invisible" and it is believed the path does not rely in the existence of M.

3.6.Sybil attack

The Sybil attack refers to represent multiple identities for malicious intent. This can be achieved if the malicious nodes collude and share their secret keys. As illustrated in Figure. 3, A is connected with B, C and the malicious node, M_1. If M_1 represents other nodes M_2, M_3 and M_4 (e.g. by using their secret keys), this makes A believe it has 6 neighbors instead of 3.

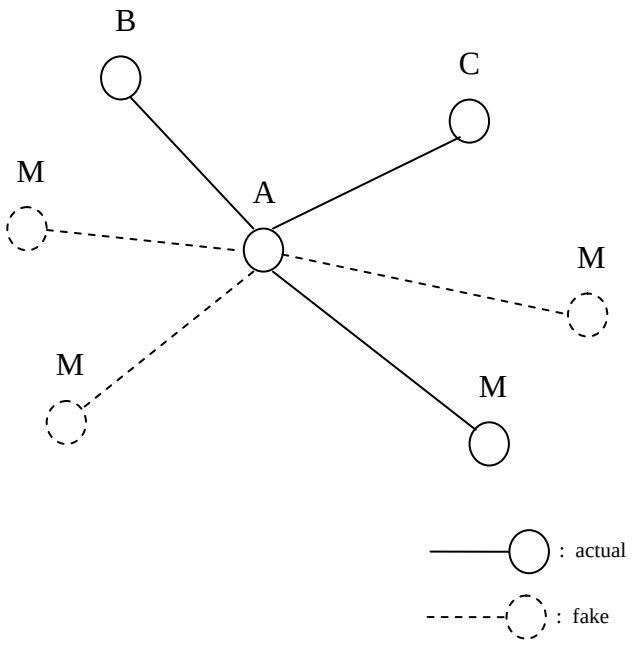


Figure. 3 The Sybil attack

In a mobile ad hoc network that uses multi-path routing, the possibility of choosing a path that contains a malicious node (e.g. M_1) will be largely increased.

4. Deal with tunneling attacks

Tunneling attack can form serious threat in mobile ad hoc network, especially against many routing protocols proposed two possible solutions: a temporal solution and a locational solution. The first one exploits the time taken for each hop, while the second one uses the physical location of the nodes.

5. Conclusion

Table 1 illustrates the different types of attacks, their description and results.

Type of attacks	Description	Results
Modification	Modify the routing message	DoS, take control of the route
Fabrication	Generate false routing messages	DoS, take control of the route
Tunneling attack	Colluding, take advantage of "tunnels"	Take control of the route
DoS attack	Floods irrelevant data, resource consuming	DoS
Invisible node attack	Malicious node becomes "invisible"	DoS
Sybil attack	Colluding, forging of multiple identities	

Table 1. Different types of attacks on mobile ad hoc network routing

Some of the attacks can be achieved by only one malicious node, e.g. modification, fabrication, DoS

attack, invisible node attack, rushing attack and non-cooperation. Other attacks may need two or more malicious nodes to collude with each other, for example, the tunneling attack requires a "tunnel" between the malicious nodes; to launch the Sybil attack, attackers have to share their secret keys.

References:

1. E.M.Belding-Royer and C.K.Toh. A review of current routing protocols for ad-hoc mobile wireless networks. *IEEE Personal Communications Magazine*, pages 46-55, April 1999.
2. C.E. Pekins and p.Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing., *Proceedings of INFOCOM '97*, April 1997.
3. C.C.Chiang, H.K.Wu, W,Liu and M.Gerla, Routing in Clustered Multihop, Mobile Wireless Netwroks with Fading Channel, *Proceedings of IEEE SICON'97*, pp. 197-211, April 1997.
4. S.Murthy and J.J.Garcia-Lana_Aceves, An Efficient Routing Protocol for Wireless Networks, *ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks*, pp. 183-197, October 1996.
5. Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das, Ad Hoc On Demand Distance Vector (AODV) Routing, *IETF Internet draft*, draft-ietf-manet-aodv-12.txt, November 2002.
6. D. B. Johnson and D. A. Maltz, Dynamic source routing in ad hoc wireless networking, in *Mobile Computing*, T. Imielinski and H. Korth, Eds. Norwell, MA: Kluwer, 1996.
7. V. D. Park and M. S. Corson, Temporally-ordered routing algorithm (TORA) version 1: Functional specification, *internet-draft*, draft-ietf-manet-tora-spec-01.txt," August 1998
8. C-K. Toh and George Lin, Implementing Associativity-Based Routing for Ad Hoc Mobile Wireless Networks, Unpublished article, March 1998.
9. R.Dube, C.D.Rais, K.Y.Wang, and S.K.Tripathi, Signal Stability based Adaptive Routing (SSA) for Ad hoc Mobile Networks, *IEEE Personal Communications*, pp. 36-45, Februray 1997.
10. Peng Ning, Kun Sun, How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols, in *Proceedings of the 4th Annual IEEE Information Assurance Workshop*, pages 60-67, West Point, June 2003.