A Literature Review of Security Attack in Mobile Ad-hoc Networks

Priyanka Goyal
Department of Computer Science and Engineering
The Technological Institute of Textile and Science, Bhiwani, Haryana

Sahil Batra
Department of Computer Science and Engineering
The Technological Institute of Textile and Science, Bhiwani, Haryana

Ajit Singh
Department of Computer Science and Engineering
The Technological Institute of Textile and Science, Bhiwani, Haryana

ABSTRACT

Security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets. In this paper, we focus on fundamental security attacks in Mobile adhoc networks. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. However, these solution are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. MANET can operate in isolation or in coordination with a wired infrastructure, often through a gateway node participating in both networks for traffic relay. This flexibility, along with their self-organizing capabilities, are some of MANET's biggest strengths, as well as their biggest security weaknesses. In this paper different routing attacks, such as active(flooding, black hole, spoofing, wormhole) and passive(eavesdropping, traffic monitoring, traffic analysis) are described.

1. INTRODUCTION

In [1, 3, 4, 6] Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network.An adhoc network is self organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. It includes:

1. Military Battlefield
2. Sensor Networks
3. Medical Service
4. Personal Area Network.

Security solutions are important issues for MANET, especially for those selecting sensitive applications, have to meet the following design goals while addressing the above challenges. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET are more prone to malicious attacks. The primary focus of this work is to provide a survey on various types of attacks that affect the MANET behavior due to any reason.

2. RELATED WORK

A MANET is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, in [4,7] many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security. Although a lot of work under progress in this subject particularly routing attacks and its existing countermeasures. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. In this paper, we have discussed current routing attacks in MANET. Some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource constrained in MANET. They still not perfect in terms of tradeoffs between effectiveness and efficiency. Some solutions in [4,7,12] work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol.

The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail.

3. MANET VULNERABILITIES:

A vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

3.1 Lack of centralized management

MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale adhoc network. Lack of centralized management will impede trust management for nodes.

3.2 Resource availability

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative adhoc environments also allow implementation of self organized security mechanism.

3.3 Scalability

Due to mobility of nodes, scale of adhoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

3.4 Cooperativeness

Routing algorithm for MANETs usually assume that nodes are cooperative and non-mailicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

3.5 Dynamic topology

Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

3.6 Limited power supply

The nodes in mobile adhoc network need to consider restricted power supply, which will cause several problems. A node in mobile adhoc network may behave in a selfish manner when it is find that there is only limited power supply.

4. SECURITY GOALS

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self organizing manner. For these reasons, securing a mobile adhoc network is very challenging. The goals to evaluate if mobile adhoc network is secure or not are as follows:

4.1 Availability

Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services.It ensures the survivability of network service despite denial of service attack.

4.2 Confidentiality

Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.[5]

4.3 Integrity

Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

4.4 Authentication

Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

4.5 Nonrepudiation

Nonrepudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

4.6 Anonymity

Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

5. SECURITY ATTACKS

Securing wireless adhoc 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.[4]Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

5.1 Passive Attacks

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.

5.2 Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks.

Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external.

5.2.1 External attacks are carried out by nodes that do not belong to the network.

5.2.2 Internal attacks are from compromised nodes that are part of the network.

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as

impersonation (masquerading or spoofing), modification, fabrication and replication.

6. ACTIVE ATTACKS

6.1 Black hole Attack

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[9] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packet that it receive instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

6.2 Wormhole Attack

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 tunnelled.This tunnel between two colluding attacks is known as a wormhole .In DSR,AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

6.3 Byzantine attack

A compromised with set of intermediate,or intermediate nodes that working alone within network 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 routing services within the network.

6.4 Rushing attack

Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne [14].

6.5 Replay attack

An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions [8].

6.6 Location disclosure attack

An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques [10], or with simpler probing and monitoring approaches [14]. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security.

6.7 Flooding

Malicious nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way. This has especially serious effects on ad hoc networks, since the nodes of these usually possess only limited resources in terms of battery and computational power. Traffic may also be a monetary factor, depending on the services provided, so any flooding which blows up the traffic statistics of the network or a certain node can lead to considerable damage cost.

6.8 Sinkhole

In a sinkhole attack, a compromised node tries to attract the data to itself from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be implemented on Adhoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate.

6.9 Spoofing Attack

In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network. This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node.

6.10 RERR Generation

Malicious nodes can prevent communications between any two nodes by sending RERR messages to some node along the path. The RERR messages when flooded into the network, may cause the breakdown of multiple paths between various nodes of the network, hence causing a no. of link failures.

6.11 Jamming

In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

6.12 Replay Attack

The attacker collects data as well as routing packets and replays them at a later moment in time. This can result in a falsely detected network topology or help to impersonate a different node identity. It can be used to gain access to data which was demanded by replayed packet.

6.13 Sybil attack

The Sybil attack especially aims at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information

6.14 Sinkhole attack

The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.

6.15 Desynchronization attack

In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in network in an end-less synchronization-recovery protocol.

6.16 Overwhelm attack

In this attack, an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.

6.17 Blackmail

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.

6.18 Denial of service attack

Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

6.19 Gray-hole attack

This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

6.20 Selfish Nodes

In this a node is not serving as a relay to other nodes which are participating in the network. This malicious node which is not participating in network operations, use the network for its advantage to save its own resources such as power.

6.21 Man-in-the-middle attack

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with reciever or impersonate the reciever to reply to the sender.

6.22 Fabrication

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 [5].

6.23 Impersonation

Impersonation attacks are launched by using other node's identity,such as IP or MAC address.Impersonation attacks are sometimes are the first step for most attacks,and are used to launch further ,more sophisticated attacks.

7. PASSIVE ATTACKS

7.1 Traffic Monitoring

It can be developed to identify the communication parties and functionality which could provide information to launch further attacks .It is not specific to MANET, other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities.

7.2 Eavesdropping

The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and fake message can be injected into network.

7.3 Traffic Analysis

Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

7.4 Syn flooding

This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.

8. CONCLUSION

In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. On one hand,the security-sensitive applications of an ad-hoc networks require high degree of security on the other hand ,adhoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks.

The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop 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 both known and unknown security threats.

9. REFERENCES

[1] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. /E€€ SlCON '97, Apr. 1997, pp. 197-211

[2] Th. Clausen et al., “Optimized Link State Routing Protocol,” IETF Internet draft, draft-ietfmanet-olsr-11.txt, July 2003.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91

[4] Z. Karakehayov, “Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks,” Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[5] S. Desilva, and R. V. Boppana, “Mitigating Malicious Control Packet Floods in Ad Hoc Networks,” Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[6] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks,” 2002 Int’l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[7] S. Kurosawa et al., “Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method,” Proc. Int’l. J. Network Sec., 2006.

[8] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[9] Jyoti Raju and J.J. Garcia-Luna-Aceves, “ A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless etworks’,” in Proceeding of IEEE ICC, June 2000.

[10] Y-C. Hu, A. Perrig, and D. Johnson, “Wormhole Attacks in Wireless Networks,” IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[11] M. Al-Shurman, S-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad Hoc Networks,” ACM Southeast Regional Conf. 2004.

[12] M. G. Zapata and N. Asokan, “Securing Ad-Hoc Routing Protocols,” Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[13] K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 2002 IEEE Int’l. Conf. Network Protocols, Nov. 2002.

[14] C. Perkins and E Royer, “Ad Hoc On-Demand Distance Vector Routing,” 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.

[15] P. Yi et al., “A New Routing Attack in Mobile Ad Hoc Networks,” Int’l. J. Info. Tech., vol. 11, no. 2, 2005.