Security attacks on mobile adhoc networks

Asst Prof.Anuj Gupta
Department of Computer Science and Engineering,
RIMT-IET,Mandi Gobindgarh, Punjab .
anuj-gupta@hotmail.com

Navjot kaur
Department of Computer Science and Engineering,
RIMT-IET,Mandi Gobindgarh, Punjab.
navjot_ghotra25@yahoo.com

Amandeep Kaur
Department of Computer Science and Engineering,
DAVIET,Jallandhar, Punjab..
amnkhokhar@yahoo.co.in.

Abstract:

A Mobile Ad Ho Network (MANET) is a self organizing, infrastructure less, multi-hop network.

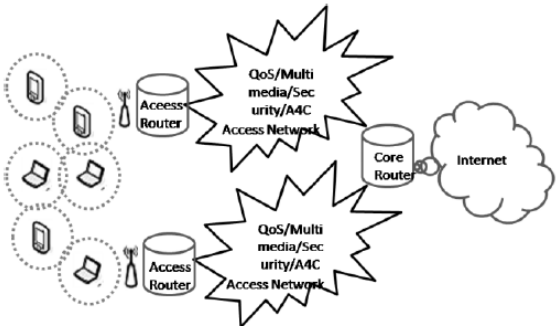


Figure-1 Mobile Ad-hoc Network

The wireless and distributed nature of MANETs poses a great challenge to system security designers. Although security problems in MANETs have attacted much attention in the last few years, most research efforts have been focused on specific security areas, such as establishing trust infrastructure, securing routing protocols. One of the major reasons to address the security aspects in MANETS is the usageof wireless transmission medium, which is highly susceptible or vulnerable to attacks. This paper proposes a way to identify different types of attacks in MANETS.

Keywords:MANET, Survey, Security attacks.

1.INTRODUCTION

A Mobile Ad Hoc Network(MANET) is a network consisting of a collection of nodes capable of communicating with each other without help from a network infrastructure.

The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate.it is a self-configuring network of mobile nodes connected by wireless links the union form an arbitrary topology.The nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably.Applications of MANETs include the battlefield applications,rescue work, as well as civilian applications like an

outdoor meeting, or an ad-hoc classroom. With the increasing number of applications to harness the advantages of Ad Hoc Networks, more concerns arise for security issues in MANETs.To accomplish our goal, we have done literature survey in gathering information related to various types of attacks and solutions, as well as we have made comparative study to address the threats in different layers.

MANET Applications:

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread applications. Typical applications include:

1) Military battlefield. Military equipment now routinely contains some sort of computer equipment. Ad hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarters.

2) Commercial sector. Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

3) Local level. Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a e.g. conference or classroom.

4) Personal Area Network (PAN). Short-range MANET can simplify the inter communication between various mobile devices (such as a PDA, a laptop, and a cellular phone).Tedious wired cables are replaced with wireless connections.Such an adhoc network can also extend the access to the Internet or other networks mechanisms by e.g. Wireless LAN (WLAN), GPRS,and UMTS.

2.SECURITY CHALLENGES IN AD HOC NETWORKS

Major challenges that a routing protocol designed for Ad Hoc wireless networks faces include: mobility of nodes, resource constraints, error-prone channel state, and hidden and exposed terminal problems .

2.1Mobility: the network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes and the addition of new nodes to the network. Disruption in service may occur either due to the movement of the intermediate nodes in the path or due to the movement of the end nodes.

2.2Bandwidth constraints: in wireless networks, the capacity of reception
of data packet. Successful transmission is a four-way exchange mechanism, namely RTS-CTS-Data-ACK.

2.3Exposed terminal problem: refers to the inability of a node to transmit to another node when the wireless channel is not free due to transmission by the nearby transmitting node.

2.4 Resource constraints: battery life and processing power are two essential and limited resources that form the major constraint for the nodes in an ad hoc network. Thus ad hoc wireless network routing protocols must optimally manage these resources.

3.SECURITY OBJECTIVES

In order to assure a reliable data transfer over the communication networks and to protect the system resources, a number of security services are required. Based on their objectives,the security services are classified in five categories:availability,confidentiality, authentication,integrity and nonrepudiation.

3.1 Availability: Availability implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system.

3.2 Confidentiality: Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Confidentiality can be achieved by using different encryption techniques so that only the legitimate communicating nodes can analyze and understand the transmission.

3.3 Authenticity: Authenticity is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

3.4 Integrity: Integrity guarantees that information passed on between nodes has not been tempered in the transmission.Data can be altered both intentionally and accidentally .

3.5 Non-repudiation: Non-repudiation ensures that the information originator can not deny having sent the information. This service is useful for detection and isolation of compromised nodes in the network.

4.ATTACKS ON MANET

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 transmissionof information.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:

1.passive

2.active.

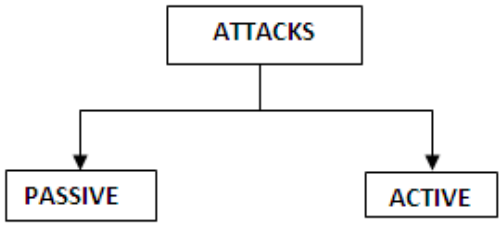


Figure-2 Types of attacks

4.1Passive attacks: In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

4.1.1 Eavesdropping Attacks, also known as disclosure attacks, are passive attacks by external or internal nodes. The attacker can analyse broadcast messages to reveal some useful information about the network. Solutions protecting the radio interface from attacks such as eavesdropping (and jamming) attacks have been proposed in the literature, e.g. spread spectrum communication and frequency hopping .

4.1.2 Traffic Analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols, or seek to provoke communication between nodes. Attackers may employ techniques such as RF direction finding, traffic rate analysis, and time-correlation monitoring. For example, by timing analysis it can be revealed that two packets in and out of an explicit forwarding node at time t and $t+€$ are likely to be from the same packet flow . Traffic analysis in ad hoc networks may reveal:

- the existence and location of nodes;
- the communications network topology;
- the roles played by nodes;

- the current sources and destination of communications; and
- the current location of specific individuals or functions (e.g. if the commander issues a daily briefing at 10am, traffic analysis may reveal a source geographic location).

4.1.3 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.

4.1.4 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.

4.2. Active Attacks: These attacks cause unauthorised state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with authorisation to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group.

4.2.1 Dropping Attacks: Malicious or selfish nodes deliberately drop all packets that are not destined for them.While malicious nodes aim to disrupt the network connection, selfish nodes aim to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes,if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted, new routes to the destination to be discovered, and the like. Unfortunately most routing protocols (DSR is an exception have no mechanism to detect whether data packets have been forwarded or not. However, they can be detected by neighbouring nodes through passive acknowledgement or hop-by-hop acknowledgement at the data link layer.

An attacker can choose to drop only some packets to avoid being detected; this is called a **Selective dropping attack**. Besides data packets or route discovery packets, an attacker can also drop route error packets, causing the source node to be unaware of failed links (thus interfering with the discovery of alternative routes to the destination).

4.2.2 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.

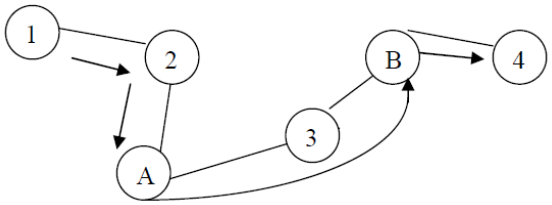


Figure 3: Wormhole attack

4.2.3 Black hole Attack

The blackhole 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. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrong doing.

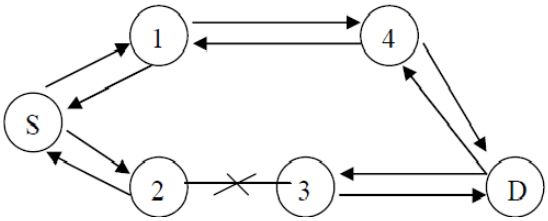


Figure 4: Blackhole attack

4.2.4 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.

4.2.5 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 currentlyproposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne .

4.2.6 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 .

4.2.7 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, or with simpler probing and monitoring approaches . Adversaries try to figure out the identities of communication parties and analyzetraffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security.

4.2.8 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.

4.2.9 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.

4.2.10 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.

4.1.11 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.

4.2.12 Jamming

In jamming, attacker initially keep monitoring wireless mediumin 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.

4.2.13 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.

4.2.14 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

4.2.15 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.

4.2.16 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.

4.2.17 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.

4.2.18 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.

4.2.19Denial of service attack

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

4.2.20 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.

4.2.21 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.

4.2.22 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.

4.2.23 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 .

4.2.24 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.

5 .TECHNIQUES USED TO SECURE MOBILE AD-HOC NETWORKS

In order to provide solutions to the security issues involved in mobile ad-hoc networks, we must elaborate on the two of the most commonly used approaches in use today:

- Prevention
- Detection and Reaction

Prevention dictates solutions that are designed such that malicious nodes are thwarted from actively initiating attacks.Prevention mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non repudiation of routing information. Among the existing preventive approaches, some proposals use symmetric algorithms, some use asymmetric algorithms, while the others use one-way hashing, each having different trade-offs and goals. Prevention mechanisms, by themselves cannot ensure complete cooperation among nodes in the network.

Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. A node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish or malicious. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets. A selfish nodeis unwilling to spend battery life, CPU cycles or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. All protocols defined in this category detect and react to such misbehavior.

Using this as the basis, we describe the following broad classifications:

1. Prevention

using asymmetric cryptography

using symmetric cryptography

using one-way hash chains

1.1Prevention using asymmetric cryptography

Asymmetric cryptographic techniques specify the underlined basic methodology of operation for protocols under this category. A secure wired networks or a similar network is required to distribute public keys or digital certificates in the ad-hoc network. Mathematically speaking a network with n nodes would require n public keys stored in the network.SAODV(an extension to AODV routing protocol) and ARAN are two of the protocols defined in this category.

1.2 Prevention using symmetric cryptography

Symmetric cryptographic techniques are used to avoid attacks on routing protocols in

this section. We assume that symmetric keys are pre negotiated via a secured wired connection. Taking a mathematical approach we see that a network with 'n' nodes would require n * (n + 1) / 2 pair wise keys stored in the network. SAR and SRP are the two protocols that belong to this category.

1.3 Prevention using one way hash Chains

This category defines a one-way hash chain to prevent attacks on routing protocols. They protect modification of routing information. such as metric, sequence number and source route. SEAD and Ariadne fall into this category.

2. Detection and Reaction

Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes.

All protocols in this category are designed such that they are able to detect malicious activates and react to the threat as needed.

Byzantine , CONFIDANT , DSR, CORE and a protocol that uses Watchdog and Pathrater are the few protocols specified in this section.

6. CONCLUSION

In this paper we have presented attacks on mobile adhoc networks. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks.

First we briefly give the introduction of manets.Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention. We then discuss some typical and dangerous security challenges in mobile adhoc networks., most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power. The existence of these security challenges has made it necessary to find some effective security solutions and protect the mobile ad hoc network from all kinds of security risks. We then discuss security objectives of mobile adhoc networks.Then we talk about the main attack types that threaten the current mobile ad hoc

networks. In the end, we discuss several security techniques that can help protect the mobile ad hoc networks from passive and active security threats.

Reference

[1] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, A Survey of Secure Mobile Ad Hoc Routing Protocols, Ieee Communications surveys &tutorials,vol. 10, no. 4, fourth quarter 2008.

[2] Priyanka Goyal , Sahil Batra, Ajit Singh,A Literature Review of Security Attack in Mobile Ad-hoc Networks, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[3] 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.

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

[5] P. Yi et al., "A New Routing Attack in Mobile Ad Hoc
Networks," Int'l. J. Info. Tech., vol. 11, no. 2, 2005.

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

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

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

[9] Yau P.-W., Mitchell C.J., "Security Vulnerabilities in Ad Hoc Networks", In Proc. of the 7th Int.
Symp. on Communications Theory and Applications, pp. 99-104, 2003.

[10] Dr.Sanjeev sofat, Prof.Divya Bansal, Rajinder Kumar*,Secuirty In Mobile Adhoc Networks, Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008)
RIMT-IET, Mandi Gobindgarh. March 29, 2008.

[11] Ali Ghaffari,Vulnerability and Security of Mobile Ad hoc Networks, Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006.

[12] Wenjia Li and Anupam Joshi, Security Issues in Mobile Ad Hoc Networks
- A Survey

[13] Lidong Zhou, Zygmunt J. Haas, Securing Ad Hoc Networks.

[14] Pradip m. Jawandhiya, Mangesh m. Ghonge, dr. M.S.ali, A Survey of Mobile Ad Hoc Network Attacks, Pradip M. Jawandhiya et. al. / International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071

[15] B. Wu *et al.*, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless/Mobile Network Security*, Springer, vol. 17, 2006.

[16] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path," *IEEE Wireless Commun. and Networking Conf. '05*.