A Study on Security Concepts in Mobile Ad Hoc Network

P.Ramesh
Assistant Professor,PG & Research Department of Computer Science,Govt. Arts College, Udumalpet,
prmram00@rediffmail.com.

G.Ramya
MPhil., Scholar,PG & Research Department of Computer Science, Govt. Arts College, Udumalpet,
ramyagopalsep13@gmail.com.

----------**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. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wired networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. More recent studies focused on security problems in MANETs. So we discuss security issues in detail and security issues associated with mobile ad hoc networks which are required in order to provide secure communication.

Keywords - Security issues, Security Attacks, Security Goals, and Security Schemes.

---

1. INTRODUCTION

In recent years, the increasing popularity of mobile device, like laptops, PDAs and handled digital devices, has impelled a revolutionary change in the computing world. We need to acquire information and connect to other device whenever and wherever we want. So it is necessary to adopt wireless as the interconnection method. That is how MANET rises. A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. A set of wireless mobile hosts dynamically establish their own network on the fly, without relying on any pre-existing communication infrastructure. But this open network architecture and dynamic network topology are prone to be attacked internally and externally. First of all discuss the security issues and ultimate goal of the security solutions for MANET is to provide security services, such as Availability, Integrity, Confidentiality, Non-repudiation, Authorization, Anonymity, Authenticity.

2. SECURITY ISSUES FOR MANET

Fundamental challenge in security for MANET is to maintain network performance with full security strength, because when more security features are introduced in the network Increases computation, communication and management overhead this can affect the network performance. In this paper, we discuss the security issues[1].

- Secure Multicasting
- Secure routing
- Privacy-aware Routing
- Key management
- Intrusion detection System

2.1 Secure Multicasting

Multicast is a mechanism where any user become the part of multicast group and even send traffic to the multicast users as well as receive traffic, but due to this procedure it can easily fall into denial of service attacks (DoS). There is an architecture usually used to secure multicast traffic that is DIPLOMA. DIPLOMA stands for Distributed Policy enforcement Architecture which is use to protect or secure end user services as well as network bandwidth. Audio and video traffic usually fall into the category of multicast traffic which is usually use by militaries as well as disaster backup plans. There are some of the major responsibilities of DIPLOMA architecture which are given below:

- It gives solution for both sender and receiver whenever they access to the multicast group.
- It also used to limit the bandwidth.
- DIPLOMA integrates with common multicasting routing protocols like PIM-SM and ODMRP.

- It also uses to provide (allocate) network resources in a fair manner during attacks.

2.2 Secure routing

MANET is a self -organized wireless network, due to the fact it has vulnerable attacks that can easily damage the whole network that is why there should be some solutions which works even some of the mobile nodes compromised in the network. One of the primary challenges of secure routing is to provide authentication (trustworthiness) of users in the network. In case of distributed communication environment in MANET, authentication is open and any un-authentic node may be use to compromise routing traffic in order to disrupt the communication. There are some of the major responsibilities of secure routing which are given below:

- It provides assurance that modified and replayed route replies should be rejected in order to avoid fabrication of attacks.
- Routing protocol responsiveness itself provide safety among different routing attacks.

2.3 Privacy-aware and Position based Routing

MANET is a kind of wireless network in which mobile nodes move from one station to another. In this type of network environment routing process among different nodes is important that is why privacy-aware and position based routing is used to avoid route overhead. In case of position based routing mechanism, a mobile node within the MANET network broadcast its position co-ordinates as well as its one-hop neighbours. This information can easily be attacked, so therefore privacy-aware mechanism is together with position based routing in order to provide secure communication. PPBR stands for privacy aware and position based routing in which a mobile node mainly takes pseudo identifiers that are usually dynamic and it is also use to provide end-to-end inconspicuousness to other nodes.

2.4 Key management

Certified Authority (CA) is one of the mechanisms which provide key management, if it is compromised then entire network can easily be
damaged. One of the major functionality of key management and distribution for MANET, it provide solutions for mobility related issues. Discuss the different aspect of key management and distribution for MANET. In the paper, the approach for key management use to solve high mobility issue as well as it provide an efficient method to reduce control overhead also gives an idea how to increase reliability in key management with respect to conventional key management process.

2.5 Intrusion detection System

Intrusion detection system is a complete security solution which provides information about malicious activities in the network, it also uses to detect and report about malicious activities. MANET is also design for route traffic mechanism when there is congestion in the network, faulty nodes as well as topology changes due to its dynamic behaviour. IDS use to detect critical nodes and then analyse its data traffic, critical node also degrade network performance. There are different IDS systems which has some specific features, some of them are given below:

- Cluster based voting
- Neighbour-monitoring
- Trust building for detail description of these IDS system.

3. SECURITY ATTACKS FOR MANET

Securing wireless ad-hoc 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. 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 four types:

- **External Attack:** External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

- **Internal Attack:** Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious that is part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyses traffic between other nodes and may participate in other network activities.

- **Passive Attack:** A Passive attack is a continuous collection of information that might be used later when launching an active attack. For that, the attacker eaves drops packets and analyses them to pick up required information.

- **Active Attacks:** Includes almost all other attacks launched by actively interacting with victims, such as: sleep deprivation torture, which targets the batteries, hijacking, in which the attacker takes control of a communication between two entities and masquerades as one of them jamming, which causes channel unavailability by overusing it.

We discuss type attacks[1]:

3.1 Denial of Service attack

This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will

not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

3.2 Impersonation

If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic.

3.3 Eavesdropping

This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

3.4 Routing Attacks

The malicious node are make routing services a target because it's an important service in MANETs. There are two flavours to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

3.5 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. 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 packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

3.6 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.

3.7. 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.

3.8 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.

3.9 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 receiver or impersonate the receiver to reply to the sender.

3.10 Gray-hole attack

This attack is also known as routing misbehaviour 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. SECURITY GOALS FOR MANETS

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 ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows[1]:

4.1 Availability

Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security issue is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service.

4.2 Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways:

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

4.3 Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of

some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

4.4 Non-repudiation

Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behaviour is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect messages an evidence to notify other nodes that the node sending out the improper message should have been compromised.

4.5 Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

4.6 Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

4.7 Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators .It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

5. Security Schemes

In this part, we discuss several popular security schemes that aim to handle different kinds of attack listed in the previous subsection[2].

5.1 Intrusion Detection Techniques

Intrusion detection is an Intrusion Detection System (or IDS) [3] generally detects unwanted manipulations to systems. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network.

5.1.1Intrusion Detection Techniques in MANET: the First Discussion

The first discussion[3] of general intrusion detection framework in MANET was proposed, which was distributed and cooperative to meet with the needs of MANET. The intrusion detection system every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behaviour locally and independently, which are performed by the built-in IDS agent. However, the neighbouring nodes can share their investigation results with each other and cooperate in a broader range. The cooperation between nodes generally happens when a certain node detects an anomalybut does not have enough evidence to what kind of intrusion it belongs to. In this situation, the node that has detected the anomaly requires other nodes in the communication range to perform searches to their security logs in order to track the possible traces of the intruder.

5.1.2 Cluster-based Intrusion Detection Technique for Ad Hoc Networks

An cooperative intrusion detection for the ad hoc networks in the previous part. However, all of the nodes in this framework are supposed to participate in the cooperative intrusion detection activities when there is such a necessity, which cause huge power consumption for all the participating nodes. Due to the limited power supply in the ad hoc network, this framework may cause some nodes behave in a selfish way and not cooperative with other nodes so as to save their battery power, which will actually violate the original intention of this cooperative intrusion detection[5]. To solve this problem a cluster-based intrusion detection technique is used in this technique a MANET can be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node per cluster that will take care of the monitoring issue in a certain period of time, which is generally called cluster head. A cluster is a group of nodes that reside within the same radio range with each other, which means that when a node is selected as the cluster head, all of the other nodes in this cluster should be within 1-hop vicinity. It is necessary to ensure the fairness and efficiency of the cluster selection process. Here fairness contains two levels of meanings: the probability of every node in the cluster to be selected as the cluster head should be equal, and each node should act as the cluster node for the same amount of time. Efficiency of the process means that there should be some methods that can select a node from the cluster periodically with high efficiency.

5.1.3 Misbehaviour Detection through Cross-layer Analysis

The observe the attack behaviours in the MANET, and [5]find that some smart attackers may simultaneously exploit several vulnerabilities at multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehaviour detector. This type of cross-layer attack will be far more threatening than the single-layer attack in that it can be easily skipped by the single-layer misbehaviour detector. Nevertheless, this attack scenario can be detected by a cross-layer misbehaviour detector, in which the inputs from all layers of the network stack are combined and analysed by the cross-layer detector in a comprehensive way. The authors also present their attempt by working with RTS/CTS input from the 802.11 MAC layer combined with network layer detection of dropped packets.

5.2 Defense Mechanism Against Rushing Attacks in Mobile Ad Hoc Networks

Rushing attack is a new attack that results in denial-of-service. This attack is also particularly damaging because it can be performed by a relatively weak attacker. The initiator node initiates a Route Discovery for the target node. If the ROUTE REQUESTs for this Discovery forwarded by the attacker are the first to reach each neighbour of the target, then any route discovered by this Route Discovery will include a hop through the attacker. That is, when a neighbour of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further REQUESTs from this Route Discovery. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes .Currently proposed protocols choose to forward at most one REQUEST for each discovery, any protocol that allows an attacker to predict which ROUTE REQUEST(s) will be chosen for forwarding at each hop will be vulnerable to some variant of the rushing attack.

5.3 Watchdog and Pathrater

Watchdog and Pathrater are two main components of a system that tries to improve performance of ad hoc networks in the presence of disruptive nodes, the specific working Watchdog determines misbehaviour by copying packets to be forwarded into a buffer and monitoring the behaviour of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not. If the packets that are snooped match with the observing node's buffer, then they are discarded, whereas packets that stay in the buffer beyond a timeout period without any successful matchare flagged as having been dropped or modified. The node responsible for forwarding the packet is then noted as being suspicious. If the number of violations becomes greater than a certain predetermined threshold, the violating node is marked as being malicious. Information about malicious nodes is passed to the Pathrater component for inclusion in path rating evaluation.

Pathrater on an individual node works to rate all of the known nodes in a particular network with respect to their reliabilities. Ratings are made, and updated, from a particular nodes perspective. Nodes start with a neutral rating that is modified over time based on observed reliable or unreliable behaviour during packet routing. Nodes that are observed by watchdog to have misbehaved are given an immediate rating of -100. It should be distinguished that misbehaviour is detected as packet mishandling/modification, whereas unreliable behaviour is detected as link breaks.

6. Manet security problem and proposed solution

MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets or impersonate a node. This violet the networks goal of availability, integrity, authentication and non-repudiation. Compromised nodes can also launch attacks from within a network. Most proposed routing algorithms today do not specify schemes to protect against such attacks. We give below methods that are pertinent for authentication, key distribution, intrusion detection and rerouting in MANET[4].

6.1Cryptography

Often, the sender/receiver is an organization. The goal of cryptography is to split a cryptographic operation among multiple users so that some predetermined number of users so that some predetermined number of users can perform desired operation. In organizations, many security-related actions are taken by a group of people instead of an individual so there is a need for guaranteeing the authenticity of messages sent by a group of individuals to another group without expansion of keys and or messages. To avoid a key management problem and to allow distribution of power, an organization should have one public key. The power to sign should then be shared, to avoid abuse and to guarantee reliability.

6.2 Decentralized authentication of new modes

Two nodes authenticate each other using signed unforgettable certificates issued by virtual trusted CA. Multiple nodes will function collectively as a CA. Authority and functionality of an authentication server is distributed across *k* nodes that collaboratively serve and provide authentication services.

6.3 Per-packet and per-hop authentication

A new node has to be initially authenticated by each of its neighbours to join the network. Once that has been accomplished, each packet sent by the node to its one-hop neighbour is authenticated by the neighbour using a packet authentication tag. The one-hop neighbour then replaces the tag with its own authentication tag and forwards the packet to its neighbour. This next neighbour verifies the new authentication tag as coming from its immediate neighbour and the process is repeated iteratively until the packet reaches its destination. Therefore, each packet is authenticated at every hop. This scheme has the advantage that is resistant to denial of service (DoS) attacks and sessions hijacking attacks such as man-in-the-middle attack.

6.4 Intrusion detection in manet

An effective IDS is an key component in securing MANETs. Two different methodologies of intrusion detectionare commonly used: anomaly intrusion detection and misuse intrusion detection. Anomaly-detection systems are usually slow and inefficient and are prone to miss insider attacks. Misused detection systems cannot detect new types of attack. Hybrid systems using both techniques are often deployed in order to minimize these shortcomings.

7. CONCLUSION

In this paper, we try to inspect the security issues in the mobile ad hoc networks. The mobile ad hoc networks more security problem occurs in routing and data forwarding, so we study this paper about security issues, security attacks, and security goals. We solve the security problem are detect to using techniques such as Intrusion detection, Cryptography, Decentralized authentication of new modes, Per-packet and per-hop authentication.

References

[1] Sachin Lalar, Security in MANET: Vulnerabilities, Attacks & Solutions, *International Journal of Multidisciplinary and Current Research*, Accepted 01 January 2014, Available online 10 January 2014, Vol.2 (Jan/Feb 2014 issue).

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

[3] Jiahong Weng, Security Issues in Mobile Ad Hoc Networks- A Survey.

[4] Rachika Gupta, Mobile Ad hoc Networks (MANETS): Proposed solution to Security Related Issues, *Indian Journal of Computer Science and Engineering (IJCSE).*

[5] Pradeep Rai and Shubha Singh, A Review of 'MANET's Security Aspects and Challenge, *IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.*

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in *Proceedings of ICNP'02,* 2002.

[7] J. Parker, A. Patwardhan and A. Joshi, Cross-layer Analysis for Detecting Wireless Misbehaviour, in *Proceedings of the IEEE Consumer Communications and Networking Conference* (*CCNC 2006*), Las Vegas, Nevada, USA, Jan. 2006.

[8] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks* ((Chapter 30), CRC Press LLC, 2003).

[9] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, *IEEE Networks Special Issue on Network Security*, November/December 1999.

[10] HaoYang, Haiyun & Fan Ye, Security in mobile ad-hoc networks : Challenges and solutions , Pg. 38-4, Vol 11, issue 1 (Feb 2004).