A Proposed Solutionfor Security Issues In MANETs

Neha Dixit (Professor)
Dept. of Comp Engg and App
N.I.T.T.T.R
Bhopal, India

Sanjay Agrawal
Dept. of Comp Engg and App
N.I.T.T.T.R
Bhopal, India

Vishal Krishna Singh
Dept. of Comp Engg and App
N.I.T.T.T.R
Bhopal, India

***Abstract*—Mobile Ad hoc Networks (MANET) has become one of the most important technologies in recent years because of the rapid proliferation of wireless devices. A mobile Adhoc network consists of mobile nodes that can move freely in an open environment. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes.This paper provides an introduction to Mobile Adhoc Networks, Routing related issues and overview of security problems for MANETS &some novel solutions are required to make Mobile Adhoc Network secure.**

Keywords: MANET, Wireless Networking, Ad hoc Networks, Secure Routing.

INTRODUCTION

A Mobile Adhoc Network is a group of wireless mobile computers in which nodes cooperate by forwarding packets to one another in order to allow them to communicate beyond direct transmission range. Application such as military conflicts, disaster relief, and mine site operation may benefit from adhoc networking, but it leads toinsecure and unreliable communications. MANETS are more vulnerable to attacks than wired networks due to transparent medium, changes in dynamic network topology, absence of centralized authority and absence of line of defense.

Security is a process that is as secure as its weakest link. So, all the points which are weak should be determined and eliminated to make MANETs safe. Some of the weak points and solutions to strengthen them are considered in this article.

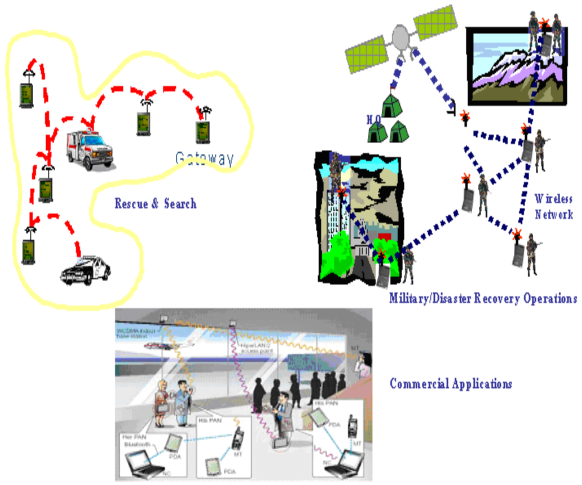

Fig 1. Mobile Ad Hoc Network Applications

Some Important Featuresof MANETs are listedas follows:

- Communication via wireless means.
- No centralized monitoring.
- Dynamic network topology.
- Frequent routing updates.

Advantages of MANETs

- They provide information and services regardless of geographic position.
- Easy to install and maintain.

Disadvantages of MANETs

- Limited resources.
- Limited physical security.
- Lack of authorization facilities.
- Difficulty to detect error prone nodes.

2. ROUTING

Mobile Ad-Hoc networks (MANETS) are by definition peer-to-peer, multi-hop networks, without any existing infrastructure. If the host network wishes to communicate with another network host which is outside its transmission range, it must use intermediate hosts to route the communications. Hence routing functionality needs to be incorporated into the mobile hosts.

In the design of routing protocols for mobile ad-hoc networks, the following are desirable factors: -

(1) *Distributed operation*: - With no central infrastructure, routing must be distributed between the nodes.

(2) *Loop-freedom:* - It avoids route discovery or maintenance processes from going back and forth from node to node.

(3) Reactive attacks versus Proactive attacks: - Are routes to be determined as a source requires it or should a pre-defined current table of routes be distributed amongst nodes? Both approaches are taken in adhoc networks and protocols fall into either of these two categories.

(4) *"Sleep" period operation*: -It is desirable that when a node is not actively participating on a network, i.e., ‘sleep’ state in order to save energy. The routing

protocol should be able to accommodate such periods without majorimpact on operation.

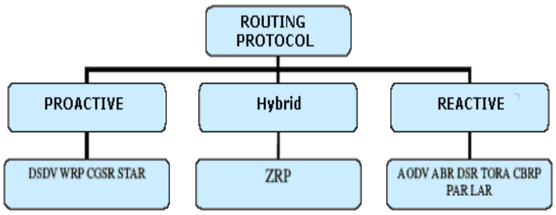

Fig 2 Categorization of adhoc routing protocols

(5) *Unidirectional link supports*: - Due to differences in wireless radio range between devices, routes are notbi-directional. It is an important factor for protocol design which can be later used for the return path. As mentioned, ad-hoc network routing protocols fall into two categories: - Demand driven (reactive) protocols or Table-driven (proactive) protocols.

Proactive protocols seek to leads to decrease in node latency.

These protocols require each node to maintain up-to-date routing tables containing routing information from each node to every other node in the network. E.g. DSDV

Demand-based (Reactive) protocols seek to reduce control overhead andlink usage by constructing routing information only for the source node looking for a route to destinationin the network. When the routehas been discovered and established the process terminates itself. Some form of route maintenance procedure maintains it until either the destination becomes inaccessible. E.g. AODV

2.1 DSDV Protocol Outlined

Destination Sequenced Distance Vector routing is a table-driven routing protocol based on the Bellman-Ford algorithm. Each network node maintains its own routing table in which all destination nodes in the network and the numbers of routing hops are recorded. Routes are given a sequence number to distinguish old routes from new routes. Routing tables are updated periodically throughout the network to maintain consistency. The route with the most recent sequence number (indicating freshness) is used.If routeshave the same sequence number then the one with the smaller hop count is used.

2.2 AODV Protocol Outlined

The Ad Hoc On-Demand Distance Vector (AODV) builds on the DSDV protocol by reducing the required number of broadcasts by creating routes on a source initiated. No list of routes is maintained. When a source node wants to communicate with a destination node, it broadcasts (multicasts, if IPv6 is being used) a route request (RREQ) packet to its neighbors. They will forward it on to their neighbors and so on, until it reaches destination .

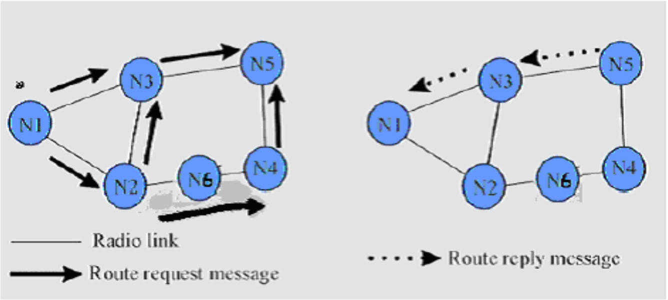

Fig 3 AODV/DSR route discovery, route request message is broadcast, route reply message is unicast

AODV uses sequence numbers to indicate route freshness and to avoid route loops. During the forwarding of RREQ packets the intermediate nodes record in their cached route tables the address of the neighbor from whom the RREQ arrived, hence a reverse path is created. The intermediate node with a fresh route to the destination, responds by unicasting a route reply (RREP) package to the source along the reverse path.

3. SECURITY IN MANETs

When discussing network security in general, two aspects needs to be considered; the security goals and the potential attacks. The security goals includes the functionality that is required to provide a secure networking environment while the security attacks cover the methods that could be employed to break these security services.

3.1 Network Security Goals

In providing a secure networking environment, followings goals are to be implemented:

□ *Confidentiality*: Ensures that the destined receivers can only access transmitted data.Encryption can be classified into two types. Symmetric Encryption, where 2 nodes share a key .Symmetric encryption generally requires less computational resources than public key encryption. Public Key Encryption, here all nodes generate a public\private key pair pubKn/privKn.

□ *Integrity*: Ensures that the data has not been changed during transmission. The integrity can be ensured using cryptographic hash functions along with some form of encryption.

□ *Authentication*: Both sender and receiver of data should be sure of other’s identity. Authentication can be provided using encryption along with cryptographic hashing techniques, digitalsignatures and certificates.

□ *Non-repudiation*: Ensures that parties can ensure the transmission of information by another party without denying it.Itrequires the use of public key cryptography to provide digital signatures.

□ Availability: Ensures that the network security services listed above are available to the destined parties when required. The availability ensuresredundancy, physical protection and other non-cryptographic means.

There are various types of threats or attacks networks can be susceptible to, some of these are given below:

3.2 Attacks

We divide attacks into two types such as passive or active.

1.**Passive attacks**: In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not disrupt communications or cause any direct damage to the network.They can be used to get information for future harmful attacks. Some of the passive attacks are eavesdropping and traffic analysis.

Eavesdropping Attacks: The attackeranalyzes the broadcasting messages to reveal useful information about the network. This attack is also known as disclosure attack. Answers protecting the radio interface from such attacks have been proposed in the literature e.g. spread spectrum communication etc.

Traffic Analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols or initiate thecommunication between nodes. Attackers may use methods likeas traffic rate analysis, and time-correlation. For example, by timinganalysis 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 [1]. 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 communication between the source and destination nodes.

2. **Active Attacks**: These attacks cause unauthorized state changes in the network such as DoS, modification of packets, etc. These attacks are initiated by the nodes with authorization to operate within the current network.Active attacks are divided into four groups: dropping, modification, fabrication, and timing attacks.

Dropping Attacks: Malicious or selfish nodes deliberately drop all packets. These nodes aim to damage the network connection in order to preserve their resources. This attack can help to prevent end-to-end communications between nodes. It could also lower the network performance by making the packets to be resend via new routes to the destination.

An attacker can choose to drop only some packets to avoid being detected bycausing the source node to be unaware of failed links (thus interfering with the discovery of alternative routes to the destination); this is called a *selective dropping attack*.

Modification Attacks: Insider attackers modify packets to damage the network. For example, in the *sinkhole attack* the attacker tries to attract almost allthe traffic from a particular area viacompromised node by making it attractive to one another. It is usefulinthe route discovery process in routing protocols that use advertised information such as remaining energy and nearest node to the destination. This type of attack can be used as a basis for further attacks like *dropping and selective forwarding* attacks.

A black hole attack is like a sinkhole attack that attracts traffic through itself and uses it as the basis for further attacks. It aims to prevent data packets being forwarded to other nodes. This type of attack is hard to detect for a virtual node [4].

Fabrication Attacks: Here the attacker forges network packets. In [5], fabrication attacks are classified into “active forge” in which attackers send faked messages without receiving any related message and “forge reply” in which the attacker sends fake route reply messages in response to genuineroute request messages.

Attackers can initiate frequent packets to cause *denial of service (DoS)*. Example DoS attacks that exploit MANETs’ features are sleep deprivation torture attacks, routing table overflow attacks,flooding attacks, and the like. *The sleep deprivation torture attack* takes a node’s battery power and so disables the node by persistently making service requests of one form or another. This attack was discovered by Stajano et al. [6] who stated that it is stronger in impactthan DoS attacks such as CPU exhaustion. *The flooding attack*, introduced in [7], is another attack against on-demand protocols; here nodes send Route Request messages whensoever they require. The attacker exploits the Route Discovery route by broadcasting many false Route Request messages to a node which is not present.

Another interesting fabrication attack on MANETs is the routing cache poisoning attack [8]. A node can update its table with the routing information in the packets that it hears, even if it is not on the route of the packets. The attacker can poison the routes to a victim node by sending spoofed routing information packets, causing neighboring nodes to update their tables erroneously.

Timing Attacks: An attacker attracts other nodes by causing itself to appear closer to those nodes than it really is. Rushing attacks and hello flood attacks use this technique. *Rushing attacks* [9] occur during the Route Discovery phase.

Rushing attacks can be carried out in many ways: by ignoring delays at MAC layers, by wormhole attacks, or by transmitting packets at a higher wireless transmission power. *The hello flood attack* [10] is another attack that makes the adversary attractive for many routes. The attacker broadcasts many Hello packets with large enough transmission power that each node receiving Hello packets assumes the adversary node to be its neighbor. It can be highly effective in both proactive and reactive MANET protocols.

A further significant attack on MANETs is the collaborative *wormhole attack*. Here an attacker receives packets at one point in the network, passes them to another point in the network by forwarded by multi-hop routes, and then replays them into the network from this final point .Since the packets sent over tunneling are the same as the packets sent by normal nodes, wormhole attacks can be detected by software approaches such as IDS [11].

4. MANETs SECURITY PROBLEM & PROPOSED SOLUTION

As we are aware of that MANETs lack central infrastructure, so many security problems arisesas compared to those that exist in conventional networks. It is comparatively easy for attackers to eavesdrop and gain access to secured data. It is also easier for them to enter or leave a wireless network because no physical connection is required. They attack the network to delete information, inject false data or delete a node. This jeopardizes Manet's security goal of authentication, integrity, availability and non-repudiation. Some of the nodes can cause attacks from inside the network. Most proposed routing methods do not specify ways to protect against such attacks. We give below methods that are a solution to the security problems faced by MANETs

4.1Cryptography

Often, the sender/receiver is an organization. The aim of cryptography is to divide the operation among multiple users in order to get the operation done. In organizations, many security-problems are taken control 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. To avoid a key management problem, only one public key should be made available. The power to sign should then be shared, to avoid abuse and to guarantee reliability.

4.2 Decentralized authentication of new nodes

Two nodes authenticate each other using signed unforgeable certificates issued by virtual trusted CA. Multiple nodes will function collectively as a CA. Authority and functionality of a server collaboratively serve and provide authentication services for k nodes.

4.3 Per-packet and per-hop authentication

A new node has to be initially authenticated by each of its neighbors to join the network. Once that has been accomplished, each data packet sent by the node to its neighboring node is authenticated by using a packet authentication tag. The neighboring node replaces the tag with its own authentication tag and moves the packet to its neighboring node. This next neighboring node checks the tag and the process is repeated iteratively until the packet reaches its destination. Therefore, each packet is authenticated at every hop. The only advantage is it resists to denial of service

(DoS) attacks and man-in-the-middle attack.

4.4 Intrusion detection in Manets

An effective IDS is a key component in securing MANETs. An IDS is introduced to detect possible violations of a security policy by monitoring system activities and responding to those that are apparently intrusive. When an attack is detected in the network, a response can be generated to minimize the damage to the network.

We can classify the different intrusion detection techniques proposed for MANETs which are as follows

Specification-Based Intrusion Detection

One of the most commonly proposed intrusion detection techniques for MANETs is specification basedintrusion detection; here intrusions act asas runtime violations of the specifications of routing protocols. Examples of this method are DSR, OLSR, and AODV

Anomaly-Based Intrusion Detection

This technique profiles the symptoms of normal behaviours of the system, such as CPU usage for programs etc. It detects intrusions as deviations from the normal patterns. Many techniques have been applied for anomaly detection, e.g. statistical approaches, and artificial intelligence techniques like data mining and neural networks.This is important in an environment where new attacks and new vulnerabilities of systems are announced constantly.

Misuse-Based Intrusion Detection

Misuse-Based IDSs compare known attack signatures with current system activities. They are generally preferred by commercial IDSs since they are efficient and have a low false positive rate. The only drawback is that it cannot detect new attacks. The system is only as strong as its signature database and this needs frequent updating for new attacks.

5. CONCLUSIONS

MANETs consists of mobile nodes interconnected by multi hop communications paths or radio links. AMANETs consists of mobile platforms known as nodes, which move at any speed in any direction and organize themselves in any manner. The nodes in the network function as routers, clients and servers. These nodes are limited by power consumption, bandwidth and computational consumption. Because of this unique characteristics and constraints traditional approaches to security are inadequate in MANETs. Traditional authentication, key distribution and intrusion detection methods are often too inefficient to be used in resource constraineddevices in MANETs. In this paper we proposed efficient cryptographic techniques, per packet and per hop authentication anddistributed intrusion-detection system along with its types for addressing the related security issues in MANETs.

References

1. Kong J., Hong X., Gerla M., "A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks", In IEEE MILCOM, 2003

2. 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

3. Hubaux J.-P., Buttyan L., Capkun S., "The Quest for Security in Mobile Ad Hoc Networks", In Proc. of the 2nd ACM Int. Symp.on Mobile Ad hoc Networking & Computing, pp. 146-155, 2001.

Buchegger S., Tissieres C., Le Boudec J.-Y.,"A Test-Bed for Misbehaviour Detection in Mobile Ad-Hoc Networks –How Much Can Watchdogs Really Do?", Mobile Computing Systems and Applications (WMCSA '04), pp. 102-111, 2004

5. Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003

6. Stajano F., Anderson R., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", In Proc. of Int. Workshop on Security Protocols, Springer, 1999

7. Yi P., Dai Z., Zhang S., Zhong Y., "A New Routing Attack in Mobile Ad Hoc Networks", Int. Journal of Information Technology, vol. 11, No. 2, pp. 83-94, 2005

8. Wu B., Chen J., Wu J., Cardei M., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Chapter 12, Springer, 2006

9. Hu Y.-C., Perrig A., Johnson D.B., "Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols", In Proc. of the ACM Workshop on Wireless Security, 2003

10. Karlof C., Wagner D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad Hoc Networks, pp. 293-315, 2003

11. Hu Y.-C., Perrig A., Johnson D.B., "Packet Leashes: A Defence against Wormhole Attacks inWireless Ad Hoc Networks", In Proc. of INFOCOM, 2003