SURVEY ON SECURITY ISSUES IN NETWORK LAYER ACTIVE ATTACKS ON AD HOC WIRELESS NETWORKS

*Prakash Anand and Dr. Rajesh Tiwari

Department of Computer Science & Engineering, R.V.S College of Engineering and Technology, Edalbera, Jamshedpur, Jharkhand India-831012

ABSTRACT

An ad hoc wireless network is a wireless network, comprised of mobile computing devices that use wireless transmission for communication, having no fixed infrastructure. Accordingly, this impedes establishing reliable end to end communication paths and having efficient data transfer. Ad hoc wireless network have different network concerns and security challenges to get the availability of network connectivity, secure communication and reputation management systems which affect the trust in cooperation and negotiation between mobile networking entities. In this survey we consider and security features, challenges and attacks of ad hoc wireless network and we classify the security threats in network layer of Ad hoc wireless network.

Keywords: Ad hoc wireless Networks, Information security. Routing Protocols, Security threats, Trust management,

1. Introduction

1.1 Overview of Ad hoc wireless networks

A wireless ad hoc network is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs are special mobile nodes which have a broadcast radio interface that provide many
advantages such as use of single channel, simpler channel management techniques and ease of supporting mobility. PRNET (packet radio network project sponsored by the defense advanced research project agency DARPA) with combination of ALOHA (ALOHA net utilized single-hop wireless packet switching and multiple access solution for sharing a single channel) and carrier sense multiple access (CSMA) for access to shared radio channel. The radio interface employed the direct sequence (DS) spread spectrum scheme. The system was designed to self organize, self configure, and detect radio connectivity for the dynamic operation of a routing protocol without any support fixed information, error and flow control over the wireless links, reconfiguration of paths to handle path breaks arising due to mobility of nodes and routers, processing and storage capability of nodes and distributed channel sharing. The successful demonstration of PRNET proved the feasibility and efficiency of infrastructure-less networks and their applications for civilian and military purposes. DARPA extended the work on multi-hop wireless network through the survival project radio networks (SURAN) the project that aimed at providing ad hoc networking with small, low cost, low power devices with efficient protocols and improved scalability and survivability (the ability of networks to survive the failure of network nodes and links). Realizing the necessity of open standard in this emerging area of computer communication a working group within the Internet Engineering Task Force (IETF) termed the mobile adhoc networks (MANET) working group was formed to standardize the protocols and functional specification of adhoc wireless networks. The vision of the IETF effort in the MANET working group is to provide improved standardized routing functionality to support self-organizing mobile networking infrastructure. Even though adhoc wireless networks are expected to work in the absence of any fixed infrastructure, recent advances in wireless network architectures reveal interesting solutions that enable the mobile adhoc nodes to function in the presence of infrastructure. Multi-hop cellular networks (MCNS) and self organizing packet radio adhoc networks with overlays are example of such type of networks.

1. Security Requirement of MANET

A security protocol for MANET should satisfy the following requirements.

- **Confidentiality:**
  The data send by the sender must be comprehensively only to he intended (destination node). Though an intruder might get hold of the data being sent, he/she must not be able to derive any useful information out of the data. One of the popular techniques used for ensuring confidentiality in data encryption.

- **Integrity:**
  The data send by the source node should reach the destination node as it was send: unaltered. In other words it should not be possible for any malicious node in the network to tamper with data during transmission.

- **Availability:**
  The network should remain operational all the time. It must be robust enough to tolerate link failures and also capable of surviving various attacks mounted on it. It should be able to provide the guaranteed service whenever an authorized user requires them.
• Non-repudiation:
Non-repudiation is a mechanism to guarantee that the sender of the message and that the recipient cannot deny having received the message. Digital signatures, which function as unique identifiers for each user much like a written signature, are used commonly for this purpose.

1.3 Ad hoc wireless networks challenges and security impact:
Designing a full proof security protocol for wireless ad hoc network is very challenging task. This is mainly because of certain unique of characteristics of adhoc wireless networks, namely, shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among nodes, limited availability of resources and physical vulnerabilities. The details on each above mentioned characteristics causes difficulty in providing security in adhoc wireless networks is given below:

1. Shared broadcast radio channel:
Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in adhoc wireless networks in broadcast in nature and is shared by all nodes in the networks. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

2. Insecure operational environment:
The operating environments where adhoc wireless networks are used may not always be secure. One important application of such networks is in battlefields. In such applications, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

3. Lack of authority:
In wired network and infrastructure –based wireless networks it would be possible to monitor the traffic on the network through certain important central points (such as routers, base stations and access points) and implement security mechanisms at such points. Since ad hoc do not have the central points, these mechanisms cannot be applied in adhoc wireless networks.

4. Lack of association:
Since the networks are dynamic in nature, a node can join or leave the network at any point of time. If no proper authentication mechanism is used for associating nodes with a network an intruder would be able to join in the network quite easily and carry out his/her attacks.

5. Limited resource availability:
Resources such as bandwidth, battery power and computational power (to a certain extent) are scarce in adhoc wireless networks. Hence it is difficult to implement complex cryptographic-based security mechanism in such networks.
6. Physical vulnerabilities:
   Nodes in these networks are usually compact and hand-held in nature. They could get
damaged easily and are also vulnerable to theft.

2. Security threats in Network layer of ad hoc wireless network:

2.1 Classification and types of routing protocols:
Routing protocols for adhoc wireless networks can be classified into several types based on
different criteria.
A classification tree is shown in figure 7a.

2.1.1 Based on the Routing Information Update mechanism:
Adhoc wireless routing protocols can be classified into three major categories based on the
routing information update mechanism. They are:

2.1.1.1 Proactive or table-driven Routing protocols:
In table driven routing protocols every node maintains the network topology information in the
form of routing tables by periodically exchanging routing information. Routing information is
generally flooded in the whole network. Whenever a node requires a path to a destination, it runs
an appropriate path finding algorithm on the topology information it maintains.

2.1.1.2 Reactive or on-demand routing protocols:
Protocols that fall under this category do not maintain the network topology information. They
obtain the necessary path when required by using the connection establishment process. Hence
these protocols do not exchange routing information periodically.
2.1.1.3 Hybrid routing protocols:
Protocols belonging to this category combine the best features of the above two categories. Nodes within a certain distance from the node concerned or within a particular geographical region are said to be within the routing zone of the given node. For routing within this zone a table-driven approach is used. For nodes that are located beyond this zone a table-driven approach is used. For nodes that are located beyond this zone an on-demand approach is used.

2.1.2 Based on the Use of the Temporal Information for Routing:
This classification of routing protocols is based on the use of temporal information used for routing. Since ad hoc wireless networks are highly dynamic and path breaks are much more frequent than wired networks, the use of temporal information regarding the lifetime of the wireless links and the lifetime of the paths selected assumes significance. The protocols that fall under this category can be further classified into two types:

2.1.2.1 Routing protocols using past temporal information:
These routing protocols use information about the past status of the links or the status of links at the time of routing to make routing decisions. For example, the routing metric based on the availability of wireless links (which is the current/present information here) along with a shortest path-finding. The topological changes may immediately break the path making the path undergo a resource-wise expensive path reconfiguration process.

2.1.2.2 Routing protocols that use future temporal information:
Protocols belonging to this category use information about the expected future status of the wireless links to make approximate routing decisions. Apart from the lifetime of wireless links, the future status information also includes information regarding the lifetime of the node (which is based on the remaining battery charge and discharge rate of non-replenishable resources), prediction of location, and prediction of link availability.

2.1.3 Based on the routing Topology:
Routing topology being used in the internet is hierarchical in order to reduce the state information maintained at the core routers. Ad hoc wireless networks, due to their relatively smaller number of nodes can make use of either a flat topology or a hierarchical topology for routing.

2.1.3.1 Flat topology routing protocols:
Protocols that fall under this category make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANS. It assumes the presence of a globally unique (or at least unique to the connected part of the network) addressing mechanism for nodes in an ad hoc wireless network.

2.1.3.2 Hierarchical topology routing protocols:
Protocols belonging to this category make use of a logical hierarchy in the network and an associated addressing scheme. The hierarchy could be based on geographical information or it could be based on hop distance.

2.1.4 Based on the Utilization of Specific Resources:
2.1.4.1 Power-aware routing:
This category of routing protocols aims at minimizing the consumption of a very important resource in the adhoc wireless networks: the battery power. The routing decisions are based on minimizing the power consumption either locally or globally in the network.

2.1.4.2 Geographical information assisted routing:
Protocols belonging to this category improve the performance of routing and reduce the control overhead by effectively utilizing the geographical information available.

2.2 Types of attacks faced by routing Protocols
Attacks on ad hoc wireless networks can be classified into two broad categories, namely, passive and active attacks. A passive attack does not disrupt the operation of the network; the advisory snoops the data exchanged in the network without altering it. Here the requirement of confidentiality can be violated if an advisory is also able to interpret the data gathered through snooping. Detection of passive attack is very difficult since the operation of the network itself does not get affected. One way of overcoming such problems is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overhead.
An active attack attempts to alter or destroy the data being exchanged in the network thereby disrupting the normal functioning of the network. Active attacks can be classified further into two categories, namely, external and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanism such as encryption techniques and firewalls. Internal attacks are from compromised nodes that are actually part of the network. Since the advisories are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.
Figure (7b) shows the classification of the different types of attacks possible in ad hoc wireless networks. The following sections describe the various attacks listed in the figure.
Security attacks

Passive attacks
- Snooping

Active attacks
- MAC layer attacks
- Network layer attacks
- Transport layer attacks
- Application layer attacks
- Other attacks

MAC layer attacks
- Jamming
- Wormhole attack
- Blackhole attack
- Byzantine attack
- Information Disclosure
- Resource consumption attack
- Routing attacks

Network layer attacks

Transport layer attacks
- Session Hijacking

Application layer attacks
- Repudiation

Other attacks
- Denial of service
- Impersonation
- Manipulation of network traffic
- Device tampering

Fig 7b
2.3 Routing table overflow attack:
This attack faces proactive algorithms, which update routing information periodically. To launch this attack, the attacker tries to create routes to nonexistent nodes to the approved nodes present in the network. The attacker can simply send extreme route announcements to overflow the target system’s routing table. The goal is to have enough routes so that creation of new routes is prohibited or the implementation of routing protocol is overwhelmed.

2.4 Routing cache poisoning attack:
Routing cache poisoning attack uses the advantage of the promiscuous mode of routing table updating. This occurs when information stored in routing tables is either deleted, altered or injected with false information. Assume a malicious node M wants to poison routes node to X. M could broadcast spoofed packets with source route to X via M itself, thus neighboring nodes that overhear the packet may add the route to their route caches.

2.5 Routing table poisoning:
The compromised nodes in the networks send fictitious routing updates or modify genuine route update packets send to other uncompromised nodes. Routing table poisoning may result in sub-optimal routing, congestion in portions of the network or even make some parts of the network inaccessible.

2.6 Packet Replication:
In this attack, an advisory nodes replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

2.7 Rushing attack:
On-demand routing protocols that uses duplicate suppression during the route discovery process are vulnerable to this attack[4]. An advisory node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same route request packet can react. Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the advisory nodes as one of the intermediate nodes. hence, the source nodes would not be able to find secure routes, that is, routes that do not include the advisory node. It is extremely difficult to detect such attacks in adhoc wireless networks.

2.8 Attacks on Network layer protocols:
2.8.1 Wormhole attack:
In this attack, an attacker receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network where the packets are resend into the network [1]. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through a single long–range wireless link or even through a wired link between the two colluding attackers. Due to broadcast nature of the radio channel, the attacker can create a wormhole even for packets not addressed to itself. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network. If proper mechanisms are not employed to defend the network against wormhole attacks most of the existing routing protocols for ad hoc wireless networks may fail to find valid routes.

2.8.2 Black hole attack:
In this attack, a malicious node falsely advertises good paths (e.g., shortest path or most stable path) to the destination node during the path finding process (in on-demand routing protocols) or in the route update messages (in table-driven routing protocols). The intension of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node concerned.

2.8.3 Byzantine attack:
Here, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, routine packets on non-optimal paths and selectively dropping packets [2]. Byzantine failures are hard to detect. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be exhibiting Byzantine behavior.

2.8.4 Information Disclosure:
A compromised node may leak confidential or important information to unauthorized nodes in the network. Such information may include information regarding the network topology, geographic location of nodes, or optimal routes to authorized nodes in the network.

2.8.5 Resource consumption attack:
In this attack, a malicious node tries to consume/waste away resources of other nodes present in the network. The resource that are targeted are battery power, bandwidth and computational power which are only limitedly available in the ad hoc wireless networks. The attacks that could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes. Using up the battery power of another node by keeping that node always busy by continuously pumping packets to that node is known as a sleep deprivation attack.
2.9 Other multilayer attacks:

Multi-layer attacks are those that could occur in any layer of the network protocol attack. Denial of service and impersonation are some of the common multi-layer attacks. This section discusses some of the multi-layer attacks in ad hoc wireless networks.

2.9.1 Denial of service:

In this type of attack, an advisory attempts to prevent legitimate and authorized users of services offered by the network from accessing those services. A denial of services (DOS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resources (e.g., an access point) used in the network so that the resource is no longer available to nodes in the network, resulting in the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of ad hoc wireless networks, there exist many more ways to launch a DoS attack in such a network, which would not be possible in wired networks. DoS attacks can be launched against any layer in the network protocol stack [3]. On the physical and MAC layers, an adversary could employ jamming signals which disrupt ongoing transmissions on the wireless channels. On the network layer, an adversary could take part in the routing process and exploit the routing protocols to disrupt the normal functioning of the network. For example, an advisory node could participate in a session but simply drop the certain numbers of packets which may lead to degradation in the QoS being offered by the network. On the higher layers, an advisory could bring down critical services such as key management service.

Some of the DoS attacks are described below:

- Jamming:
  In this form of attack, the advisory initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender. It then transmits signals on that frequency so that error-free reception at the receiver is hindered. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques that overcome jamming attacks.

- SYN flooding:
  Here, an advisory node sends a large number of SYN packets. On receiving the SYN packets, the victim node sends back acknowledgement (SYN-ACK) packets to nodes whose addresses have been specified in the received SYN packets. However, the victim node would not receive any ACK packet in return. In effect, a half-open connection gets created. The victim node builds up a table/data structure for holding information regarding all pending connections. Since the maximum possible size of the table is limited, the increasing number of half-open connections results in the overflow in the table. Hence, even if a
connection request come from a legitimate node at a layer point of time because of the table overflow the victim node would be forced to reject the call request.

-Distributed DoS attack:
A more severe form of the DoS attack is the distributed DoS (DDoS) attack. In this attack, several adversaries that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network.

2.9.2 Impersonation:
In impersonation attacks an advisory assumes the identity and privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances or to disrupt the normal functioning of the network by injecting false routing information into the network. An advisory node could masquerade as an authorized node using several methods. It could by chance guess the identity and authentication details of the authorized node (target node), or it could snoop for information regarding the identity and authentication to the target node from the previous communication, or it could circumvent or disable the authentication mechanism at the target node. A man-in-middle attack is another type of impersonation attack. Here the advisory reads the possibly modifies messages between two end nodes without letting either of them know that they have been attacked. Suppose two nodes X and Y are communicating with each other; the advisory impersonates node Y with respect to node X and impersonates node X with respect to node Y exploiting the lack of third party authentication of the communication between nodes X and Y.

3 Related open research area:
Many researches in wireless ad hoc network are ongoing for many years but still need more to be done. The existing researches aimed to face specific attacks, and they can solve many of them but still vulnerable to others. Also in the field of security resource consumption for different DOS attacks needs to be investigated. More research is required on secure routing protocol, robust key management, trust based systems, integrated approaches to routing security, data security in different level and cooperation enforcement. Current routing protocols are vulnerable to a variety of attacks that can permit attackers to control a victim’s selection of routes or enable denial-of-service attack. Jamming is one of DoS attacks and it can be vanquished using multiple transceivers which can operate in different frequency bands.

References :