Security in Ad Hoc Network

Bingwen He Joakim Hägglund Qing Gu

Abstract

Security in wireless network is becoming more and more important while the using of mobile equipments such as cellular phones or laptops is tremendously increasing. Due to the unique characteristic of wireless network, unlike wire line networks, to achieve this goal is never a trivial challenge. Mobile ad hoc networks (MANETs) is a special wireless network which does not rely on any fixed infrastructure but depends on the cooperation between each node like a cellular phone in the network. In this essay we discuss the possible attacks in MANETs and briefly discuss the solutions aimed to these problems.

This essay is produced for the course Secure Computer Systems HT2005 (1DT658) of which the lecturer is Björn Victor.

1 Introduction

Wireless networks use radio waves to transmit the signals and exist in basically two different flavors, infrastructure and ad-hoc. In infrastructure mode all traffic is transmitted between the nodes via an access point which controls the network and provides it with the security mechanisms. The most commonly used standard for wireless networks is the 802.11 standard or Wi-Fi which actually is not a standard but a whole family of standards using the same protocol. The security in wireless networks using Wi-Fi consists of WEP, WPA and now recently WPA2 which is basically a finalized version of WPA. WPA was created as an intermediate security system while WPA2 was finalized and tested since the previous system (WEP) contained several serious weaknesses.

Benefits and applications of ad-hoc

Ad-hoc networking doesn't require any access points as opposed to wireless networks in infrastructure mode. This makes them useful in a lot of different applications. It is largely used in military applications and in rescue operations where the existing communication infrastructure has been destroyed or is unavailable, for example after earthquakes and other disasters. But ad-hoc is nowadays also being used in a lot of commercial applications, like mobile phones and PDAs using the Bluetooth protocol, since it is fast and quite easy to setup and doesn't require any extra equipment.

Characteristics and standards of ad-hoc

While the wireless standard 802.11 does support ad-hoc networks, it is very restricted since it doesn't provide routing between the nodes, so a node can only reach the directly visible nodes. Instead protocols like the Ad-hoc On-demand Distance Vector protocol (AODV) or Dynamic Source Routing protocol (DSR) could be used. These routing protocols are so called reactive routing protocols, meaning it establishes a route to a destination only when needed. In contrast the more commonly used routing protocols on the Internet are proactive meaning they will set up routes independently of the traffic in the network. This means that the reactive network is silent until a connection is needed and thus lessens the congestion in the network. DSR is an even more optimized protocol which doesn't require the forwarding computers to have up to date routing tables but includes a list of network addresses in the packet. The protocol also eavesdrops the local network traffic and listens for this routing information included in the packets and adds it to its own routing table.

One of the main goals when designing mobile ad-hoc networks (MANET) where the nodes move around and the topology quickly changes is to protect the network connectivity between the nodes over potentially multi-hop channels. To get multi-hop connectivity you must provide one-hop connectivity through the link-layer (e.g. 802.11) and extend that to multi-hop connectivity through routing and data forwarding protocols in the network-layer (e.g. DSR).

We will discuss about the above issues in the following structure: in chapter 3 we will discuss the passive attacks and active attacks, in active attacks three kinds of attacks – attacks by modification, attacks by fabrication and attacks by impersonation are introduced. In chapter 4 we will give the current security solutions mainly on network-layers, which consist of securing ad hoc route protocols and securing packet forwarding.

2 Attacks

Like all kinds of networks, passive attack and active attack are two kinds of attacks which can be launched against ad hoc networks. The passive attacks only intercept the message transmitted in the network without disturbing the transmission. By doing this, the attacker will be able to analyze the valuable information like network topology to perform further attacks. For example, by eavesdropping and subsequent analyses, the attacker may notice that some particular node is used much more than the others, which means it might be the ‘heart’ of this network. If this node is brought down, the whole network will be out of action as well. Then the attacker can deploy some special attacks to achieve this goal. Unfortunately, this kind of attack in wireless network is impossible to detect due to the nature of wireless network that its medium is air which is widely open to every user within the domain.

The active attacks are carried out by malicious nodes which aim to disrupt transmission among other nodes or selfish nodes which may just want to save their own battery. There are mainly three ways to perform such an attack.

Attacks using modification

Below we briefly talk about several modification attacks against AODV and DSR.

(1) **Redirection by Modified Route Sequence Numbers:**
Protocols such as AODV assign some value to routes to the specific destination to decide the priority. A route with a higher value is preferred. The node may change traffic through itself by advertising a route to a node with a greater value.

(2) **Redirection with Modified Hop Counts:**
Without other metrics, AODV uses the hop count field to determine a shortest path. Malicious nodes can reset the hop count field of the RREQ to zero so that increases the chance that they are included on a newly created route. Similarly, malicious nodes may be not included in the created routes if they set the hop count field of the RREQ to infinity.

(3) **Denial-of-service with Modified Source Routes:**
DSR uses source routes stating routes in data packets. These routes lack integrity checks. So denial-of-service attack can be launched by altering the source routes in packet headers so that the packet can not be delivered to the destination.

Attacks using Fabrication

When a node misrepresent the identity in the network such as by altering MAC or IP address in outgoing packets, spoofing can occur. It can modify the rooting of some nodes then lead to loops in the network which will increase the power consumption greatly.

Attacks using Impersonation

These attacks generate false routing messages which can be difficult to distinguish from invalid constructs.

(1) **Falsifying Route Errors in AODV and DSR:**
In ADOV and DSR, if the destination node or an intermediate node along the active path moves, the node upstream of the link break broadcasts a route error message to all active up stream neighbors. This message causes the corresponding route to be invalid. A denial-of-service attack can be achieved by sending route error messages indicating a broken link on the route, then prevent the source from communicating with destination.

(2) **Route Cache Poisoning in DSR:**
A node overhearing may add the routing information contained in the packet's header to its own route cache. An attacker can exploit this method of learning modify route caches by transmitting packets containing invalid routes in their headers.

3 Solutions

A MANET provides its network connectivity mainly through link-layer protocols and network-layer protocols. Link-layer protocols are used to ensure one-hop connectivity while network-layer protocols extend this connectivity to multiple hops. Thus in order to achieve MANET security there are accordingly two solutions, link-layer security and network-layer security. Link-layer security is to protect the one-hop connectivity between two adjacent nodes that are within each other's communication range through secure protocols, such like the IEEE 802.11 WEP protocol [1] or the more recently proposed 802.11i/WPA protocol [2].

The network-layer security is concerned with securely delivering packets between mobile nodes through multihop ad hoc forwarding. So it tries to ensure that the routing message exchange within the packages between nodes is consistent with the protocol specification and the packet forwarding of each node is consistent with its routing states. Accordingly, the proposals can be divided into two categories: *secure ad hoc routing protocols* and *secure packet forwarding protocols*. In this essay we will mainly discuss about network-layer security.

Secure ad hoc routing protocols

The secure ad hoc routing protocols enhance the existing ad hoc routing protocols, such as DSR and AODV with security extensions. In these protocols, one node signs its routing messages using some cryptographic authentication method like digital signature so that each node can authenticate the legal traffic efficiently and distinguish the unauthenticated message packets from attackers and correct packets. However, there are still chances that an authenticated node has been compromised and controlled by the malicious attacker. Therefore, we have to further ensure that a node obeys the routing protocols properly even it is an authenticated node. In the following, we describe how different types of routing protocols are secured.

Source Routing — For source routing protocols such as DSR, the main challenge is to ensure that none of the intermediate nodes can remove already existing nodes from or add extra nodes into the route. The basic idea is to attach a per-hop authenticator for the source routing forwarder list so that any altering of the list can be detected right away. A secure extension of DSR is Ariadne, which is described in [3].

Distance Vector Routing — For distance vector routing protocols such as AODV, the main challenge is that the information about the routing metric has to be advertised correctly by each intermediate node. For example, if we use hop count as the routing metric, each node has to increase the hop count only by one exactly. A hop count hash chain is used so that none of the intermediate nodes can decrease the hop count in a routing update to achieve benefits, which is described in [4].

Secure Packet Forwarding

The routing message exchange is only one part of the network-layer protocol which needs to be protected. It is still possible that malicious nodes deny forwarding packages correctly even they have acted correctly during the routing discovery phase. For example, a malicious node can join the routing correctly but simply ignore all the packages passing through it rather than forwarding them, known as black hole, or selectively forward some packages, known as grey hole. The basic idea to solve this issue is to ensure that each node indeed forwards packages according to the protocol. Reactive methods should be used instead of proactive methods since attacks on package forwarding cannot be prevented. The core ideas of these solutions are a detection technique and a reaction scheme, which we have not studied too much at present but will study later.

4 Conclusion

In this essay we briefly discussed the attacks in ad hoc network and some solutions on network-layer for these problems. During the study we have learned a lot about wireless networks and ad hoc networks. We have learned the routing protocols such as AODV and DSR used in ad hoc network and learned the solutions such as securing the routing protocol and securing packets forwarding. We have read some papers and searched the net quite a lot.

REFERENCES

[1] IEEE Std. 802.11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 1997.

[2] IEEE Std. 802.11i/D30, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security,” 2002.

[3] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, ACM MOBICOM, 2002.

[4] M. Zapata, and N. Asokan: Securing Ad Hoc Routing Protocols, ACM WiSe, 2002.

[5] H.Yang, H.Luo, F. Ye, S. Lu and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions, IEEE Wireless Communications, February 2002.

[6] K. Sanzgin, B.Dahill, A Secure Routing Protocol for Ad Hoc Networks

[7] Wikipedia