Routing Security in Ad Hoc Wireless Networks

Seminar paper of "Internet Security" in WS09/10

Name: Yu Han

Matr.-Nr.: 314029

yhan@cs.tu-berlin.de

Abstract: An Ad Hoc network is a collection of wireless mobile nodes that dynamically form a temporary network. The nodes can communicate with each other without the help of any existing network infrastructure or centralized administration. This technology is primary used for military communication and disaster recovery. Security becomes a very important issue in Ad Hoc network, since its characteristics: open medium, dynamic topology, distributed cooperation, and constrained capability.

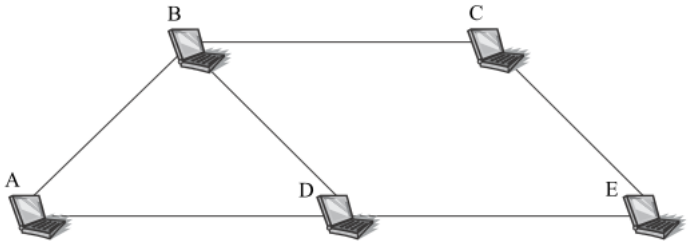

Figure 1 Example of an ad hoc network [3]

1 Introduction

As the cost of wireless equipment has dropped significantly in the past few years, the use of wireless communications becomes more and more popular. Ad Hoc networks are a new paradigm of wireless communication. Using an Ad hoc wireless network has some advantages: easy and speedy deployment, robustness (no infrastructure required), adaptive and self-organizing network. Nodes in traditional wireless networks communicate with a fixed back-bone infrastructure. In contrast, nodes in Ad Hoc wireless network communicate with each other without the use of a fixed network infrastructure.

In Ad Hoc wireless networks, every node operates not only as a host but also as a router. Two nodes can communicate directly if the destination is within the sender's transmission range, or through intermediate nodes if the destination is out of the sender's transmission range.

The Ad Hoc network work based on trust and co-operation between nodes because of the absence of central control. If the node the neighbor is hijacked, the entire network is in danger. So security is a very important issue in Ad Hoc network.

2 Overview of Routing Protocols in Ad Hoc wireless Networks

Routing protocols play a very important role in both the discovery and maintenance of the routes in the network. However the traditional routing protocols can no longer be used in Ad Hoc wireless networks, because of the characteristics of Ad Hoc wireless network.

The major requirements [1] of a routing protocol are (1) minimum route acquisition delay, (2) quick route reconfiguration in the case of path breaks, (3) loop-free routing, (3) distributed routing protocol, (4) low control overhead, (5) scalability with network size, (6) QoS support as demanded by the application, (7) support of time-sensitive traffic, and (8) security and privacy.

There are a number of challenges [1] triggered by the unique characteristics of ad hoc wireless networks. Node mobility affects network topology and may incur packet lost, path disconnection, network partition and difficulty in resource allocation. Wireless nodes are in general resource constrained, in terms of battery power, memory and computing power. Wireless channel has a high bit error rate (10^{-5} to 10^{-3}) compared with wired counterparts (10^{-12} to 10^{-9}). Wireless channel is shared by the nodes in the same broadcast area, thus the link bandwidth available per node is limited, and varies with the number of nodes present in that area. The design of routing protocols should take these factors into consideration.

According to the routing information update mechanism, routing protocols are generally classified into proactive (or table-driven) protocols, reactive (or on-demand) protocols, and hybrid routing protocols. In the next three subsections we will study the important features of each category.

2.1 Proactive Routing Protocols (table-driven)

In proactive protocols, the routes are discovered before been used. The nodes maintain one or more tables in order to store routing and network topology information. If any change in the network, updation has to be made throughout the network.

The advantage of the proactive routing protocol is: when a packet is transmitted, the route will be calculated rapidly through the routing table stored in the node. Nodes exchange routing information periodically, even there is no traffic. Obviously, the disadvantage of proactive routing protocol is potential high overhead.

Destination Sequence Distance Vector (DSDV) is a table-driven routing protocol for Ad Hoc wireless networks. DSDV is based on Bellman-Ford algorithm, which computes shortest paths between nodes using a distributed version of Bellman-Ford algorithm. Each node in the routing table contains a sequence number, which plays an important role in DSDV and used to be avoided routing loops. This is the most newest sequence number known for that destination, and is included in the periodic routing updates. If a node receives an update with a smaller sequence number, the update is ignored. The table will be updated if the node receives a greater sequence number.

2.2 Reactive Routing Protocols (on-demand)

In reactive protocols, the route discovery process is triggered only when a packet to be transferred and the node does know a path to the destination. Once a route has been established, it is maintained until either the destination becomes inaccessible (along every path from the source), or until the route is no longer used, or expired. [4] In this case, reactive routing protocol can reduce the routing overhead, but introduces a delay when the first packet is sent to a host.

A reactive routing protocol has two main functions, route discovery and route maintenance. Representative reactive routing protocols are: Dynamic Source Routing (**DSR**), Ad hoc On Demand Distance Vector (**AODV**), Temporally Ordered Routing Algorithm (TORA), etc.

DSR is a source routing protocol, and each data packet header carries the source-destination path. With this information, loops can be avoided and intermediate nodes know who the next hop for this packet forwarding is. Each node maintains its own route cache that contains routing information. Every node has an expiration time. If the timer expired, the node will be deleted in order to avoid old information.

Ad hoc On Demand Distance Vector (**AODV**): DSR keeps the entire route information in the data packet header, so it may waste bandwidth and degrade performance, especially when the data packet is very small. Ad hoc On-Demand Distance Vector (AODV) Routing tries to improve its performance by maintaining the routing information in each node, so that the data packets do not carry the source-destination path. DSR uses source routing while AODV uses forwarding tables at each node. In AODV, the route is calculated hop by hop. Therefore, the data packet need not carry the total route. That's the difference between AODV and DSR.

AODV saves bandwidth and performs well in a large Ad Hoc wireless network because the data packet does not carry the whole path information. The response time may be large using DSR, if the source node's routing table has no entry to the destination and thus must initiate a route discovery to find a path to the destination before packets transmission.

2.3 Hybrid Routing Protocols

The Ad Hoc network can use the hybrid routing protocols trying to bring the advantage of both proactive and reactive routing protocols together in order to reduce the delay and control overhead (in terms of control packages).

The difficulty of all hybrid routing protocols is how to organize the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption [2].

Examples of hybrid routing protocols are Zone Routing Protocol (ZRP), Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR), etc.

ZRP is the first hybrid routing protocol with both a proactive and a reactive routing component. ZRP divides its network in different zones and each zone operates independently. The intra-zone routing protocol (IARP) is a proactive routing protocol, while the inter-zone routing protocol (IERP) is a reactive routing protocol. Thus, ZRP has two separate routing protocols.

If the source and destination are within a same zone, the route can be calculated from the proactively cached routing table of the source by IARP. Otherwise, the route is discovered with the reactive component IERP using route requests and replies.

3 Security Services and attacks in Ad Hoc Networks

3.1 Security services

Security is an important issue for Ad Hoc wireless network. In order to provide a reliable data transfer over the communication networks and to protect the system resources, the following security services are required.

- **Integrity**: Integrity guarantees the information being transferred is never modified. Data may be modified because of benign failures or malicious attacks on the network.

- **Confidentiality**: Confidentiality ensures that information is never disclosed to unauthorized entities. Confidentiality can be achieved by using encryption techniques so that only authorized entities can understand the information.

- **Availability**: Availability means that the requested services are accessible and useable (without undue delay) whenever needed by an authorized entity.

- **Authentication**: Authentication is a network service that enables a node to indentify the peer node it is communicating with. Without authentication, an attacker could impersonate any node, gaining the control of the network and stealing sensitive information.

- **Non-repudiation**: Non-repudiation ensures that the origin of a message cannot deny having sent the message. This service is useful for detection and isolation of compromised nodes in the network.

To design a secure Ad Hoc wireless network routing protocol has to face the greatest challenge of its features: insecure wireless communication links, dynamic topology, limited bandwidth and battery power and lack of central control.

The majority of existing traditional routing protocols design fails to provide security. The main requirements [1] of a secure routing protocol are: (1) detection of malicious nodes; such nodes should be avoided in the routing process, (2) guarantee of correct route discovery, (3) confidentiality of network topology; if an attacker learns the network topology, he can attack the bottleneck nodes, detected by studying the traffic patters. This will result in disturbing the routing process and DoS, and (4) stability against attacks; the routing protocol must be able to resume the normal operation within a finite amount of time after an attack.

3.2 Attacks in Ad Hoc wireless Networks

Ad Hoc Wireless networks are usually subjected to two kinds of attacks: passive and active attacks. In passive attack, the adversary focuses on disrupting the basic mechanisms of the ad hoc network, such as routing, which are essential for proper network operation, and in active attack, the adversary tries to damage the security mechanisms employed by the network, such as key management schemes or cryptographic algorithms in use.[3]

Passive Attack: In passive attacks, an unauthorized attacker intercepts the data that is being communicated in the network. There is no change to the network data or systems. The goal of the attacker is to gather valuable information about the network. This activity makes detecting and defending against attacks difficult since the attacker doesn't do malicious actions actively.

Active Attack: In active attacks, an attacker must be able to delete messages, modify messages and inject messages into the network. The attacker is not just monitoring on the traffic but is attempting to breach or terminate a service by modifying packets or by sending false information in the Ad Hoc network. Active attacks can be further divided into internal and external attacks:

External Attacks are caused by nodes that do not belong to the network. Such attacks can be defended by using encryption, firewalls and source authentication.

Internal Attacks are caused by compromised nodes that are part of the network. Internal attacks are generally much more severe and hard to detect, because the malicious nodes are already part of the network as authorized parties.

Next we present some important active attacks that easily performed against the Ad Hoc wireless network.

Denial of service (DoS): The DoS attack is attempted to make system failure or services unavailable to its intended users. An Ad Hoc wireless network is vulnerable to DoS attacks due to its dynamic topology and distributed protocols. The classical way to create a DoS attack is to flood any centralized resource so that it no longer operates correctly or crashes.

Impersonation: In impersonation attacks, a compromised node may access to the network, send false routing information, impersonate as some authorized nodes. Strict authentication can be used to stop attacks by impersonation.

Routing table overflow: A malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and prevent the establishment of legitimate routes.

Black hole: In a black hole attack, a malicious node injects false route information replies to the route requests it receives advertising itself as having the shortest path to a destination. The attacker can not only perform a DoS attack by dropping all received packets, but also can collect the activity of nodes in the network.

Location disclosure: An attacker can get locations of nodes or structure of the network using a location disclosure attack. The information gained might reveal which other nodes are adjacent to the target, or the physical location of a node.

Wormhole attack: In the wormhole attack, an attacker receives packets at one node in the network, tunnels them to another node in the network, and resent packets into the network. This tunnel is called “wormhole”. The wormhole can drop packets to cause network disruption or it can selectively forward packets to avoid detection.

Tunneling attack: In a tunneling attack [5], two or more nodes collaborate and exchange encapsulated messages along existing data routes. For example, if a RouteRequest packet is encapsulated and sent between two attackers, the packet will not contain the path traveled between the two attackers. This would falsely make the receiver conclude that the path containing the attackers is the shortest path available.

4 Conclusion

In this paper, we have studied the protocols and the attacks on the Ad Hoc wireless network. The Ad Hoc networks are vulnerable to security attacks. However, we must provide a high degree of security to the security-sensitive applications in ad hoc networks. Therefore, providing a secure network becomes an important task in Ad Hoc wireless network.

Reference

[1] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004.

[2] C. F. Chiasserini, I. Chlamtac, P. Monti, and A. Nucci, "An energyefficient method for nodes assignment in cluster-based ad hoc networks," Wirel. Netw., vol. 10, no. 3, pp. 223–231, 2004.

[3] Amitabh Mishra, Security and Quality of Service in Ad Hoc Wireless Networks, Cambridge University Press, 2008.

[4] Elizabeth, Belding-Royer, 2003, Routing approaches in mobile Ad Hoc networks, in: S. Basagni, M. Conti, S. Giordano, I. Stojemenvoic (Eds), Ad Hoc Networking, IEEE Press Wiley, New York.

[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, A Secure Routing Protocol for Ad hoc Networks, The 10th IEEE Intl. Conf. on Network Protocol (ICNP), Nov. 2002.