Secure Routing Protocols for Wireless Adhoc Networks

C

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

S. Amutha
P.S.R. Engineering College, India

INTRODUCTION

A mobile adhoc network (MANET) in an autonomous system of mobile routers and associated hosts connected by wireless links. The routers are free to move randomly and organize themselves in an arbitrary fashion. Hence, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion or may be connected to a larger Internet. Sensor networks consisting of sensing, data processing, and communication components are examples of adhoc networks. Due to lack of infrastructure support, each node acts as router forwarding data packets for other nodes.

Ad hoc networks have played an important role in military applications and related research efforts. There are currently two variations of mobile wireless networks: infrastructure networks and infrastructureless networks. The infrastructure networks have fixed gateways and the fixed Base Stations are connected to other Base Stations through wires. Each node is within the range of a Base Station. The other type of wireless network, infrastructureless network, is the MANET. These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in an arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the nodes themselves. The entire network is mobile, and the individual nodes are allowed to move freely. The nodes of these networks function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or in very small devices. The Mobile Ad-hoc Networks are supposed to be used for disaster recovery, battlefield communications, and rescue operations when the wired network is not available(Deng et al., 2002). Mobile Adhoc Networks have a unique set of security challenges which are examined in this article.

BACKGROUND

Routing is a fundamental networking function in every communication system including wireless Ad hoc networks. Routing function can be disrupted by internal or external attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity not involed in the routing of messages. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes. Internal attackers have the capabilities of the strongest outside attacker, as they are legitimate participants of the routing process. Having complete access to the communication link, they can advertise false routing information at will and force arbitrary routing decisions on their peers (Perlman, 1988). One of the most difficult problems to detect in routing is that of byzantine failures. These failures are the result of nodes that behave in a way that does not comply with the protocol. Our analysis focuses only on network-layer threats and countermeasures.

ATTACKS AND COUNTERMEASURES IN MANET

Table 1 summarises the attacks, issues and countermeasures in each layer of the network protocol suite. The main attacks are Modification attacks, Impersonation

DOI: 10.4018/978-1-4666-5888-2.ch140

Table 1. Security Attacks, Issues and Counter Measures on Each Layer in MANETs (Wu et al., 2006, Ramanathan et al., 2002, Yang et al., 2004, Zhou et al., 1999)

Layer	Security Attacks	Security Issues	Countermeasures(Solutions)
Application Layer	Repudiation, data corruption	Detecting and preventing viruses, worms, malicious codes and application abuses	Cooperation enforcement mechanisms, Firewalls, IDS(misuse and anomalies).
Transport layer	Session hijacking, SYN flooding	Authentication and securing end to-end or point-to-point communication through data encryption	Authentication and securing end-to-end communication, use of public cryptography.
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure	Protecting the ad hoc routing and forwarding protocols	Source authentication and message integrity mechanisms to prevent route message modification, Securing routing protocols to overcome black hole, impersonation attacks, wormhole attacks etc.
Data link layer	Traffic analysis, monitoring, disruption of MAC (802.11)	Protecting the wireless MAC protocol and providing link layer security support	Secure link layer protocol like LLSP (Link Layer Security Protocol), WPA (Wi-fi Protected Access)
Physical layer	Jamming, interception, Eavesdropping	Preventing signal jamming denial-of-service attacks	Using Spread spectrum mechanisms

attacks, Fabrication attacks and Lack of Cooperation attacks. The countermeasures include both preventive and reactive mechanisms. Preventive mechanisms include authentication, access control, encryption and digital signatures. Reactive mechanisms include use of Intrusion Detection System(IDS) and cooperation enforcement to detect misuse and anomalies.

SECURE ADHOC ROUTING ATTACKS

Based on this threat analysis and the identified capabilities of the potential attackers, we now discuss several specific attacks that can target the operation of a routing protocol in an ad hoc network (Argyroudis et al., 2005).

1. **Man-in-the-Middle Attack:** In this attack, a malicious node reads and possibly modifies the messages between two parties.
2. **Sybil Attack:** In the Sybil attack, an attacker pretends to have multiple identities. A malicious node can behave as if it were a larger number of nodes either by impersonating other nodes or simply by claiming false identities.
3. **Misrouting Attack:** In the misrouting attack, a non-legitimate node sends data packet to the wrong destination. This type of attack is carried out by modifying the final destination address of the data packet or by forwarding a data packet to the wrong next hop in the route to the destination.
4. **Blackmail Attack:** Blackmail attack causes false identification of a good node as malicious node. An attacker may blackmail a good node and inform other nodes in the network to add that node to their blacklists as well, thus avoiding the victim node in future routes.
5. **Resource Consumption Attack:** In this attack, a malicious node deliberately tries to consume the resources (e.g. battery power, bandwidth, etc.) of other nodes in the network. The attack can be in the form of unnecessary route requests, route discovery, control messages, or by sending stale information.
6. **Routing Table Poisoning:** In this attack, a malicious node sends false routing updates, resulting in sub-optimal routing, network congestion, or network partition.
7. **Rushing Attack:** A malicious node in rushing attack attempts to tamper Route Request packets