Routing Attacks in Wireless Ad Hoc Networks - A Survey

Joseena M Jose¹, Deepthi P M²

¹Ad Hoc Lecturer, Department of Electronics and Communication Engineering, College of Engineering Trikaripur
²Assistant Professor, Department of Electronics and Communication Engineering, College of Engineering Trikaripur

Abstract: Wireless ad hoc network is a special kind of wireless network with a dynamic topology consist of self organized nodes. The nodes in the networks are randomly and frequently. Due to the self organizing and decentralized capabilities, ad hoc networks are used for a wide range of civilian and military applications. Wireless ad hoc networks are an open environment and it is susceptible to many security attacks due to the inherent features. Attacks in the wireless ad hoc environments are classified under two categories; active and passive attacks. Passive attacker eavesdrop the information transmitted through the networks, and it does not introduced any modifications in the networks. But an active attacker can modify or inject unwanted information in the packets and routing table in the networks. Active attacks are severely affected the network performance. This paper provides an overview of some well known routing attacks in the wireless ad hoc networks.

Keywords: Wireless Ad Hoc Networks, anonymity, security attacks

1. Introduction

Wireless Ad hoc network [1] is a collection of mobile nodes, without a particular infrastructure and centralized authority. Each node in the networks acts as a router and they involved in the network creation, operation and maintenance functions. A wireless transmitter and receiver is attached with each nodes and are communicate with each other by using a set of rules called routing protocols. Usually wireless ad hoc networks use anonymous routing protocols which provide high security to the networks from different types of attacks. Wireless ad hoc networks is an open environment, because of this the network is very much affected by external and internal attacks. So, the security challenges suffered by the ad hoc networks are above than the traditional wireless networks. Inherent features of ad hoc networks such as dynamically changing topology, lack of fixed infrastructure, self organizing capability and decentralized natures make the networks immensely useful of many tactical and civilian applications.

Anonymous routing protocols [2] in ad hoc networks can prevent so many attacks in the networks. But the resource constraint problems in the networks such as limited power efficiency and computational ability of the nodes prevent the development of complex security algorithms and key exchange mechanisms for security. An anonymous routing protocol [3] can handle two major issues such as the route anonymity and location privacy problems. The anonymity concept is defined in terms of either unlinkability or unobservability [4] and they differ in whether security protection covers items of interest or not.

Rest of the paper contains a detailed survey of the security attacks in wireless ad hoc networks. Section 3 provides a conclusion of different security attacks in wireless ad hoc networks.

2. Security Attacks

Security attacks [5] in a network will destroy the successful routing operations or creates Denial of Service (DoS) problems. Attacks in the ad hoc networks are classified in to two; they are the passive and active attacks. A passive attacker just eavesdrops and taps the communication between two nodes. Passive attacker didn’t disturbed operation of the communication channel. But the active attackers can caches some important information related the communication channel. Active attacks are critical in a networks, they can listen information in the channel can also modify them.

A. Flooding Attack or Routing Table Overflow

In flooding attack [6] the attacker node sends enormous route information to the network. This will creates routing table overflow. This flooding of data will destroy the normal routing of the networks.

B. Sleep Depravation

In this attack the attacker node unnecessarily consumed the resources of a node in the network by continually send requests for either existing or non-existing destinations. This will obstruct the normal working of the networks and causes battery and bandwidth wastages.

C. Black Hole Attack

In this attack, the attacker node provides false route replies to the route requests and declared to other node that it has the shortest route to reach destination. If this route has been created then the present active route changes to this new route contains the attacker node. In this situation the attacker node can able to use the information transmitted through the nodes or simply discarded the information contained packets.

D. Impersonation Attack

The attacker node impersonates itself as correct node in the route. This unauthorized node will send incorrect routing information, and masked as some other trusted node.
In this paper, we have analyzed several security attacks in wireless ad hoc networks. Security of the ad hoc networks is very important to maintain the performance of the networks to the expected level. The open environment induces many powerful attacks in the networks. Both passive and active attacks are critical in the wireless environment. The attacker can simply monitor the traffic and also introduced powerful attacks in the networks like introduction of unwanted information to the packet and routing table, modify the packets, create falls routes or discarded the packets. We have overviewed different active and passive attacks and solutions for these attacks for avoiding the adverse effects introduced in the networks. Anonymous routing protocols are very useful to avoid the attacks in the networks to an extent. They conceal the identities of the nodes in the networks, create untraceable routes and there by provides high security in the networks. But the existing anonymous routing protocols are not completely bulletproof from all the security attacks. Researches is still being continued to identify new attacks in the wireless ad hoc networks and security measures against that attacks.

### Conclusion

In this paper, we have analyzed several security attacks in wireless ad hoc networks. Security of the ad hoc networks is very important to maintain the performance of the networks to the expected level. The open environment induces many powerful attacks in the networks. Both passive and active attacks are critical in the wireless environment. The attacker can simply monitor the traffic and also introduced powerful attacks in the networks like introduction of unwanted information to the packet and routing table, modify the packets, create falls routes or discarded the packets.

We have overviewed different active and passive attacks and solutions for these attacks for avoiding the adverse effects introduced in the networks. Anonymous routing protocols are very useful to avoid the attacks in the networks to an extent. They conceal the identities of the nodes in the networks, create untraceable routes and there by provides high security in the networks. But the existing anonymous routing protocols are not completely bulletproof from all the security attacks. Researches is still being continued to identify new attacks in the wireless ad hoc networks and security measures against that attacks.

### References


