International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Routing Attacks in Wireless Ad Hoc Networks - A Survey

Joseena M Jose[1], Deepthi P M[2]

[1]Ad Hoc Lecturer, Department of Electronics and Communication Engineering, College of Engineering Trikaripur

[2]Assistant 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. Usua ad hoc networks use anonymous routing proto provide high security to the networks from differ 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 listens and taps the communication between two nodes. Passive attacker didn't disturbed operation of the cation channel. But the active attackers can catches portant information related the communication 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.

E. Node Isolation Attack

In node isolation [7], the attacker node isolates a given node, and it prevents communication between the particular target node and the other nodes in the network. So other node in the networks didn't get any link information of this target node and cannot establish a route through this node. Other nodes will not know about the existence of this target node.

F. Wormhole Attack

In wormhole attacks [8], the two attacking nodes cooperate between each other. Capturing the routing traffic is down by one node and the captured information is tunneled to the other attacker node present in another point of the network. One high speed private communication link is established between the two attacker nodes. These attacks will forms the topology with their control.

G. Routing Table Poisoning Attack

A routing table contains the information about the routes of the network. In the poisoning attack, the attacker node changes the routing information in the routing table. In this the attacker node inject high sequence number RREQ packet to the table, then the packets having the low sequence number will be discarded, and establishes wrong routes. The creation of non optimal routes, routing loop creation and partitioning of certain network parts are the adverse effect of this attacks.

H.Location Disclosure Attack

Location anonymity has special importance to provide security to a routing protocol. Disclosure of the location of the nodes in the networks may increase the chance of attacks in the networks. The network structure and the location of the nodes in the networks are can explore by the attacker through traffic analysis or monitoring techniques. This attacks compromise the network's privacy requirements.

3. 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 active and passive 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.

I. Rushing Attack

In rushing attack [9] the attacker node sends the route request to the target node before the original route request. The attacker node's route request will reach to the target node first, and it rejects the correct route request from other neighboring nodes.

J. Blackmail

The blackmail attack occurs due to lack of authenticity. In this attack any node can able to corrupt information regarding any other node in the network. A blacklist contains information of perceived intruder nodes is kept by the actual nodes. Blackmail attack is important against routing protocols with malicious node identification mechanisms [10].

Table 1: Different attacks in wireless ad hoc network

Attack	Active/Passive Attack	Security Methods
Eavesdropping	Passive Attack	Using Spread spectrum mechanisms FHSS,DHSS
Jamming	Passive Attack	
Denial of service (DoS) Attacks	Passive Attack	Secure link layer protocol like LLSP using WPA
Misdirecting Traffic	Passive Attack	
Flooding Attack or Routing Table Overflow	Active Attack	Securing routing protocols like SAODV, SAR, ARAN to overcome blackhole, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack
Black Hole Attack	Active Attack	
Location Disclosure Attack	Active Attack	
Wormhole Attack	Active Attack	
Routing Table Poisoning Attack	Active Attack	
Rushing Attack	Active Attack	
Impersonation Attack	Active Attack	

References

[1] C.S.R.Murthy and B.S.Manoj, "*Ad Hoc Wireless Networks"*, Pearson Education, 2008.
[2] S. Corson, J Marker," Mobile Ad Hoc Networking (MANET):Routing Protocol performance Issues and Evaluation Considerations", RFC 2501, January 1999.
[3] Jun Liu, Jiejun Kong, Xiaoyan Hong, Mario Gerla," Performance Evaluation of Anonymous Routing Protocols in MANETs", IEEE Wireless Communications and Networking Conference, 2006. Pearson Education, 2008.
[4] A. Pfitzmann, M. Hansen, "Anonymity,Unlinkability,Undetectability,Unobservability,Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology," Tech. Rep., February 2008.
[5] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability, pp. 10-29, 2001.
[6] P.Yi, Z.Dai, S.Zhang, Y.Zhong., "A New Routing Attack in Mobile Ad Hoc Networks," International Journal of Information Technology, vol. 11, no. 2, 2005.

[7] B. Kannhavong, H. Nakayama, N.Kato, Y.Nemoto and A.Jamalipour, "Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks," Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN' 06), pp. 30-35, June 2006.
[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE journal on selected areas in communications, vol. 24, no. 2, february 2006.
[9] Y.C.Hu, A.Perrig and D.Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego, California, pp.30-40, September 2003.
[10] L. Zhou and Z.J. Haas, "Securing Ad hoc Networks," IEEE Network Magazine, vol. 6, no. 13, pp. 24-30, November/December 1999.