**ISSN: 0975-766X**
**CODEN: IJPTFI**
***Review Article***

***Available through Online***
**www.ijptonline.com**

# A SYSTEMATIC SURVEY OF ROUTING ATTACKS AND COUNTERMEASURES IN WIRELESS NETWORKS

**S.S.Manivannan***
Associate Professor, School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu, India.
*Email: manivannan.ss@vit.ac.in*

*Received on 12-05-2016* *Accepted on 02-06-2016*

## Abstract

Wireless networks plays a vital role in education, entertainment, hospitals and IT parks. People have migrated from wired networks to wireless networks because of the less complexity, easy of deployment and easy to access. At the same time, wireless networks are in secured against variety of attacks such as spoofing attacks, routing attacks, cloning attacks and so on. Routing attacks are more powerful attacks other than any other attacks. Because routing attacks will alter the path of the network packets and can redirect the packets to attacker which can lead to disclose of confidential information that are exchanged between the client and server. In this paper, I have given the complete survey of various routing attacks and countermeasures in wireless networks.

## 1. Introduction

Wireless networks is the sort of PC system that uses remote information associations for interfacing system hubs. Wireless Networking is a technique by which homes, information transfers systems and endeavor the business establishments keep away from the exorbitant procedure of bringing links into a building or as an association between different gear locations. Wireless information transfers systems are by and large executed and directed utilizing radio correspondence.

This execution happens at the physical level (layer) of the OSI model system structure. Illustrations of wireless incorporate mobile phone systems, Wi-Fi neighborhood systems and physical microwave systems. Wireless networks are categorized as Wireless Personal Area Networks, Wireless Local Area Networks, Wireless Mesh Networks, Wireless Metropolitan Area Networks, Global Area Network and Space Networks.

### 2.1 Attacks in Wireless Networks

Wireless networks are very weak against variety of attacks such as Denial of Service, Probing attacks, Surveillance attacks, Impersonation, Man-in-the-Middle and Rogue Access points.

### 2.2 Security Requirements in Wireless Networks

The security requirements of wireless networks can be classified as three levels.

(i) Level I security

(ii) Level 2 security

(iii)Level 3 security

#### 2.2.1 Level I security

The first level of security is focused on cracking the foundation stone of wireless networks .i.e, Wired Equivalent Privacy (WEP). The attacks such as easy access, data tampering, Rougue Access points, masquerading, non repudiation and authentication should be prevented in this level.

#### 2.2.2 Level 2 security

The second level of security is focused on the security attacks not addressed by wired equivalent Privacy. The attacks such as Man-in-the-Middle attack, Cross Site Scripting, SQL Injection attacks should be prevented in this level.

#### 2.2.3 Level 3 security

The third level of security is focused on the elimination of most of the security flaws such WEP and WPA. The attacks such as routing attacks, location disclosure attack, byzantine attacks should be prevented in this level.

## 3. Secure Routing Challenges

The following are the challenges involved in secure routing of network packets.

(i) Wireless medium

(ii) Hostile Environment

(iii) Limited Resources

(iv) Ad Hoc Deployment

(v) Immense Scale

## 4. Routing Attacks in Wireless Networks

### 4.1.1 Grey hole attack

The intermediate nodes involved in the network communication are dropping the data packets selectively or randomly. The intermediate nodes switches its state from normal state to misbehaving state. During the normal state the intermediate nodes are forwarding the packets to other nodes and in the misbehaving state it is dropping the packets.

### 4.1.2 Black hole attack

The router is misdirecting the network packets because the router misbehaves. The malicious router is dropping the packets. It is difficult to detect the malicious router.

### 4.1.3 Worm Hole Attack

In a wormhole attack, an assailant gets parcels at one point in the system, "burrows" them to another point in the system, and afterward replays them into the system starting there. For burrowed removes longer than the ordinary remote transmission scope of a solitary bounce, it is straightforward for the assailant to make the burrowed bundle touch base with preferred metric over a typical multihop course, for instance, through utilization of a solitary long-range directional remote connection or through a direct wired connection to a plotting assailant. It is additionally feasible for the aggressor to forward every piece over the wormhole straightforwardly, without sitting tight for a whole bundle to be gotten before starting to burrow the bits of the parcel.

### 4.1.4 Location Disclosure attack

The intermediate nodes participated in the communication will disclose the locality to the attackers. This will give a chance to steal the information from the intermediate nodes.

### 4.1.5 Rushing attack

At the point when a node send a packet for bundle (RR parcel) to another node in the remote system, if there an aggressor show then he will acknowledge the RR parcel and send to his neighbor with high transmission speed when contrasted with different hubs, which are available in the remote system.

On account of this high transmission speed, parcel sent by the assailant will first reach to the destination hub. Destination hub will acknowledge this RR bundle and dispose of other RR parcels which are come to later. This is known as rushing attack.

### 4.1.6 DDoS attack

Simple denial of service attack is executed by 10 attackers at the same time to attack the particular source. DoS attack is distributed to many attackers.

### 4.1.7 Sybil attack

The Sybil assault in PC security is an assault wherein a notoriety framework is subverted by producing characters in distributed systems. It is named after the subject of the book Sybil, a contextual analysis of a lady determined to have dissociative character issue.

### 4.1.8 Routing Table Overflow attack

Attacker will create the duplicate routing path entries in routing table in order to confuse the genuine senders and receivers.

### 4.1.9 Byzantine Attack

Byzantine attack is an internal failure and normal for a framework that endures the class of disappointments known as the Byzantine Generals Problem.

### 4.1.10 Node Isolation Attack

Out of several nodes participated in the communication, the attacker compromises the particular node and isolate the node. This will cause the routing path disturbance in the network communication.

## 5. Countermeasures

The following Table 5.1 describes the countermeasures against the Top 10 routing attacks in wireless networks.

**Table.5.1 Countermeasures against Routing Attacks.**

| No | Routing Attack | Countermeasures to prevent the Attack |
|---|---|---|
| 1 | Grey hole attack | (i) dividing data packets into k equal parts.<br>(ii) Sending a message to destination containing number of messages.<br>(iii) Broadcasting messages to all neighbors of route.<br>(iv) Setting up a timer until getting number of data packets that destination receives. |
| 2 | Black hole attack | (i) Source node gets vote of one node's neighbors about the maliciousness. |

| | | |
|---|---|---|
| | | (ii) According to the votes of neighbors, starts counter for malicious node in Find Malicious table |
| 3 | Worm hole attack | (i) Physical layer authentication<br>(ii) Graph Theory model |
| 4 | Location disclosure | Secured Traffic Aware Protocol |
| 5 | DDoS Attack | (i) Secure Routing Protocol<br>(ii) Strong Authentication |
| 6 | Sybil Attack | (i) Radio Resource testing<br>(ii) Key pre distribution<br>(iii) Registration and position verification |
| 7 | Routing Table overflow | (i) Secure Routing protocol<br>(ii) Fix the routing table size |
| 8 | Rushing Attack | (i) Modified AODV protocol<br>(ii) Limit the incoming network packets |
| 9 | Byzantine Attack | ODSBR protocol |
| 10 | Node Isolation Attack | Enhanced OLSR protocol |

## 6. Conclusion

Wireless networks are weakly secured against variety of attacks. The routing attacks are severe attacks and create high security violation in wireless networks. The Top 10 routing attacks in wireless networks are discussed and the necessary countermeasures to prevent the routing attacks in wireless networks are also proposed in this survey paper.

## 7. References

1. Ian F. Akyildiz, Xudong Wang and Weilin Wang, “wireless mesh networks: a survey,” Computer Networks, vol. 47, pp. 445-487, Jan.2005.

2. X. Gu and R. Hunt, “Wireless LAN Attacks and Vulnerabilities” In the Proceeding of IASTED Networks and Communication Systems, April 2005.

3. Wong S., “The Evolution of Wireless Security in 802. I1 Networks: WEP, WPA and 802.1 I Standards.” SAN Institute May 20,2003.

4. Y. Hu, A. Perrig, and D. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks,” IEEE INFOCOM, 2002.

5. Kcng H., “Security Guidelines for Wireless LAN Implementation.” SAN Institure ,August 2003

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

7. Karlof, C., & Wagner,. D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks Journal: Special Issue on Sensor Network Applications and Protocols. Vol.1,(p293-315), Elsevier Publications.

8. Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks, IEEE Communications Magazine pp :70-75

9. Naeem,. T & Loo,. K. K. (2009). Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks. International Journal of Digital Content Technology and its Applications: Volume 3, Number 1. pp: 89-90

10. Lee , J. C., Leung, V. C. M., Wong, K. H., Cao, J., & Chan, H. C. B. (2007). Key management issues in wireless sensor networks: current proposals and future developments. IEEE Wireless Communications, pp:76-84

11. Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: a survey. Journal of Information Assurance and Security , pp:31-44

12. E. Ahmed, K. Samad, W. Mahmood, “Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks,” AusCERT2006 R&D Stream Program, Information Technology Security Conference, May 2006.

13. A.Weimerskirch and G.Thonet, “Distributed Light-Weight Authentication Model for Ad-hoc Networks,” Lecture Notes In Computer Science; Vol. 2288, pp. 341 354, 2001.

14. I.Chlamtac, M.Conti, and J.Liu, “Mobile Ad Hoc Networking: Imperatives and challenges,” Ad Hoc Networks, vol. 1, no. 1, pp. 13-64, 2003.

15. Frank Stajano and Ross J. Anderson, “The resurrecting duckling: Security issues for ad-hoc wireless networks,” in Seventh International Security Protocols Workshop, 1999, pp. 172–194.

16. Yih-Chun Hu, David B. Johnson, and Adrian Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), June 2002, pp. 3–13.

17. Chris Karlof David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, Proc. of the IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, May 2003

**Corresponding Author:**

**S.S.Manivannan*,**

**Email:** *manivannan.ss@vit.ac.in*