ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Survey on Wormhole Attack Modes and Its Prevention in the Wireless Networks

Sara Ali

PhD Research Scholar, Dept. of Computer Science, Mewar University Gangrar, Chittorgarh, India

ABSTRACT: A major challenge faced in the wireless network is security. Since the network is wireless in nature it is exposed and vulnerable to security attacks taking place at various layers. Wormhole attack is one of the most severe attacks on the routing protocols for a wireless network where two or more malicious nodes record a packet at a location and tunnel it to another location, replaying it at the remote location. This attack is challenging to deal with as it is not required for these malicious nodes to compromise any node, they can use a wireless device or a laptop to send packets over a low latency channel.

In this paper we conduct a detailed survey on the wormhole attacks, their classifications, and various modes of launching these attacks. We have focused on a survey of existing detection techniques which are under identification by the researchers.

KEYWORDS: Wireless Networks, WORMHOLE

I. INTRODUCTION

As the usage for the wireless network [1] is increasing a common problem being encountered by various implementers is of security. Most of the Wireless network [2] are infrastructure less network networks and are dynamic in nature. There is no permanent infrastructure for communication to take place between the network nodes; also there is no requirement for a central access point.

Wireless networks are the most widely used technology and are gaining popularity due to features like

- Flexibility of Location
- Cost Effective
- Mobility
- Productivity
- Convenience
- Deployment
- Cost
- Expandability

The network leads to an increase in the productivity as the accessibility increases to the information resources [4].The configuration and reconfiguration is also very simple, less expensive and faster. The major factors which have influenced the growth of the wireless network are cost efficiency, convenience and ease of integration. Most of the computers come equipped with the technology necessary for wireless networks.

II. THREATS TO THE NETWORK

Authentication is the process of actually confirming the identity. It is not a major problem in the wired networks as there is a central point which serves as an authentication point for all the nodes. Any node or device taking part in the communication is identified by a unique address [15] but since WSN is an infrastructure less network, authentication is the first and the major issue for WSN. Lack of authentication gives rise to spoofing attacks in which intruder node sends messages to a node by using the identity of some other legitimate node [17]. The intruder modifies the packet header such that it appears that the packets are coming from a trusted node [17].

Security requirements of wireless

- **Data Confidentiality: It** is concerned with keeping information secure and no leaking any information to the neighbouring nodes.
- **Data Integrity: Data** Integrity is required in the wireless network to certify that the message has not been altered or tampered with.
- **Data Authentication: Data** Authentication is needed to certify the reliability of the message by identifying its origin
- **Data Freshness:** Data freshness is needed to ensure that the data is recent and ensure that no old messages are being replayed in the network
- **Data Availability:** is the measure to determine whether the node can communicate by using the resources available in network.

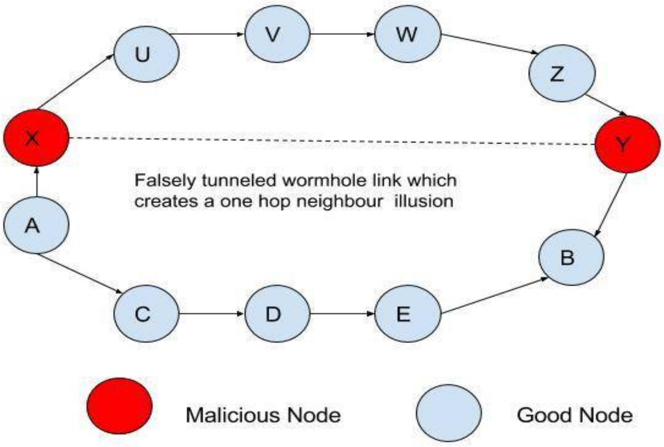
III. **WORMHOLE ATTACK CLASSFICATION**

The wormhole attack can be deployed in the following modes.

- Wormhole using Encapsulation
- Wormhole using Out-of Band Channel
- Wormhole using Packet Relay
- Wormhole using High Power Transmission

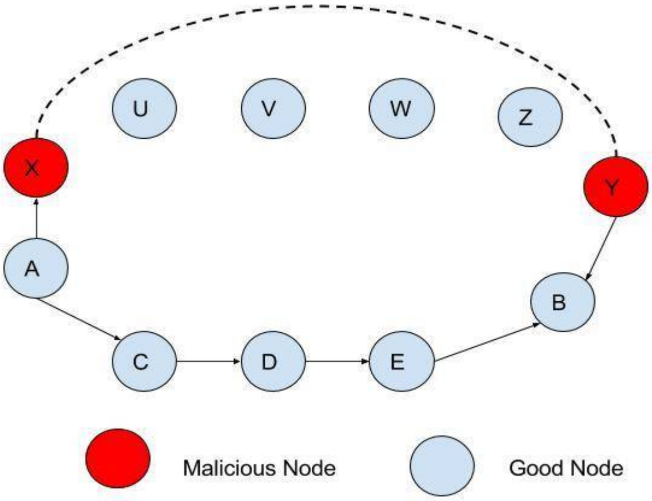
1) Wormhole Using Encapsulation:

In this attack one of the malicious nodes hears a RREQ packet and tunnels it to the collaborating malicious node present at a distant location but close to the destination. This node then re broadcasts the packet, all the neighbouring
In this mode a malicious node at one part of the network and hears the RREQ packet. It tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the RREQ. The neighbours of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multi hop paths. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away. For example, consider Figure 2 [5] in which nodes A and B try to discover the shortest path between them, in the presence of the two malicious nodes X and Y. Node A broadcasts a RREQ, X gets the RREQ and encapsulates it in a packet destined to Y through the path that exists between X and Y (U-V-W-Z). Node Y demarshalls the packet, and rebroadcasts it again, which reaches B. Note that due to the packet encapsulation, the hop count does not increase during the traversal through U-V-W-Z. Concurrently, the RREQ travels from A to B through C-D-E. Node B now has two routes, the first is four hops long (A-C-D-E-B), and the second is apparently three hops long (A-X-Y-B). Node B will choose the second route since it appears to be the shortest while in reality it is seven hops long. Any routing protocol that uses the metric of shortest path to choose the best route is vulnerable to this mode of wormhole attack.


U
V
W
Z
X
Y
A
B
C
D
E
Falsely tunneled wormhole link which creates a one hop neighbour illusion
Malicious Node
Good Node

2) Out of band channel

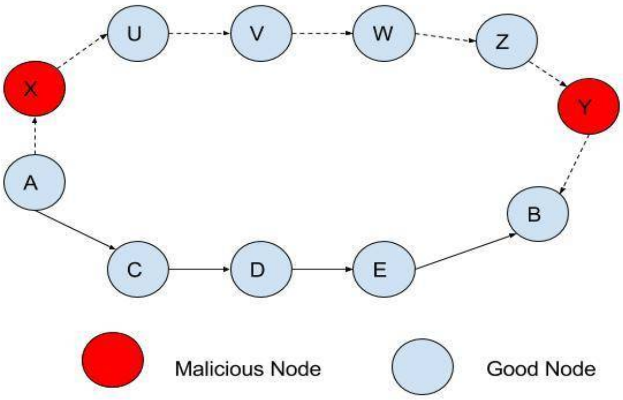
This type of attack can be achieved by using a direct wired link or long-range directional wireless link. It is more difficult to establish as it needs a special hardware. When 2 malicious nodes X and Y are present in the network having an channel which is out-of-band between them, when the node X sends a RREQ to Y which is a neighbour of B, when Y broadcast its packet B receives 2 RREQ A-C-D-E-F-B and A-X-Y-B. The first is rejected as it seems longer and the second is selected.



DOI: 10.15680/IJIRCCE.2016. 0406014

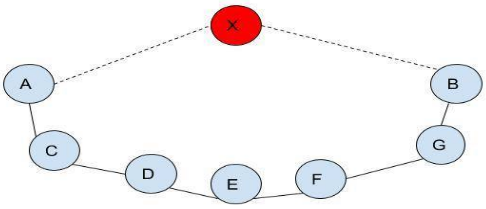
3) Packet Relay

In this type of attack the malicious node transmits the packets between two nodes which are located at a distant location and convinces them to be neighbours. This attack is dangerous as it can be launched even with one node. When large nodes are malicious the neighbouring list can be expanded and can be extended to several hops.



4) Wormhole with High Power Transmission

In this attack when one malicious node receives s a RREQ, it broadcasts the RREQ at a very high power level; this capability is not bestowed to any other node. When the node listens to the broadcast it re-broadcasts toward the destination node.



IV. DETECTION OF WORMHOLE ATTACK

The author in [5] considers the following parameters to detect the wormhole attack

1) Decrease in the path length
2) An increase in the end-to-end delay constructed from calculating the sum of hop delays despite of advertising a short path
3)Certain nodes which do not follow advertised paths may incur delay caused due to some nodes which may be involved in the attack leading to an increase in the delay in end-to-end routing caused by hop delay.

The various metrics which can be used to detect the wormhole attack and its strength [6,7] are mentioned below.

Length: The difference in between the advertised path and actual path is high the more number of anomalies can be observed in our network.

Robustness: The capability of the wormhole to exist and not effect its strength even after a certain amount of network topology changes have taken place

Strength: The total traffic that can be attracted by an incorrect link advertisement made by the malicious nodes.

Attraction: It is a metric which displays a decrease in the length of the routing path offered by the malicious wormhole tunnel when a small attraction or small improvements in the correct path results in a decrease in its strength

V. CONCLUSION

In the current paper we try to analyze the wormhole attack and discuss the various modes of launching the attack. It is one of the most severe attacks that disrupt the network traffic and even the routing protocols. We even try to analyze the various techniques which can be employed to prevent the wormhole attack
Also we discuss the various metrics which can be employed as tools to detect the attack.

REFERENCES

[1]International Journal of Advanced Research in Computer Science Research Paper
Enhanced Security Framework for Wireless Networks Sara Ali DR S Krishna Mohan
[2]Ijesrt International Journal Of Engineering Sciences & Research Technology Literature Survey On Wormhole Attack Avinash S. Bundela Computer Science & Engineering Medicaps Institute of Technology and Management, Indore (M. P.), India
[3]ijrdet Survey of Wireless Sensor Network Vulnerabilities and its Solution
Poonam Khare [1], Sara Ali [2]
[4] Choi, Min-kyu, et al. "Wireless network security: Vulnerabilities, threats and countermeasures." International journal of Multimedia and Ubiquitous Engineering 3.3 (2008).
[5]Marianne Azer,Sherif El-Kassas,Magdy El-Soudani. “A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks ” International Journal of Computer Science and Information Security 1.1 (2009)
[6] V. Mahajan, M. Natu, A. Sethi. “Analysis of wormhole intrusion attacks in MANETS”. In IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.
[7] Y. C. Hu, A. Perrig, and D. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in INFOCOM , 2003.

BIOGRAPHY

Sara Ali is a Research Scholar in the Computer Science, Mewar University GANGRAR, CHITTORGARH. She received Master In IT from IIIT Bangalore .She is currently working as an Associate Professor at Shadan College of Engineering and Technology