ORIGINAL RESEARCH PAPER | Computer Science | Volume : 6 | Issue : 9 | September 2016 | ISSN - 2249-555X | IF : 3.919 | IC Value : 74.50

A Wormhole Attack Survey in Wirless Networks

KEYWORDS Wireless Networks,Wormhole,malicious nodes

Sara Ali	DR S Krishna Mohan
PhD Research Scholar, Computer Science, Mewar University, Mewar Rajasthan,India Hyderabad, Telangana, India	Research Guide, Faculty of Computer Science, Mewar University, Mewar Rajasthan,India Hyderabad, Telangana, India

ABSTRACT *Wireless networks have gained tremendous importance in the last decade. The users desire to use wireless connectivity regardless of their geographic location. This has led to increase in the treats face by the network. The nodes operating in a mobile network act as both client and intermediate router, as a result the resulting multi-hop communication is not secure.*

Wormhole attack is one of the most serious routing threats launched at the network layer. This attack can be implemented by creating a tunnel at two ends of the network by one or more malicious nodes which disrupts the routing paths in a wireless network. In this paper we try to conduct a detailed study on the wormhole attacks by classifying the attacks and considering different prevention and detection mechanism for the same

Introduction

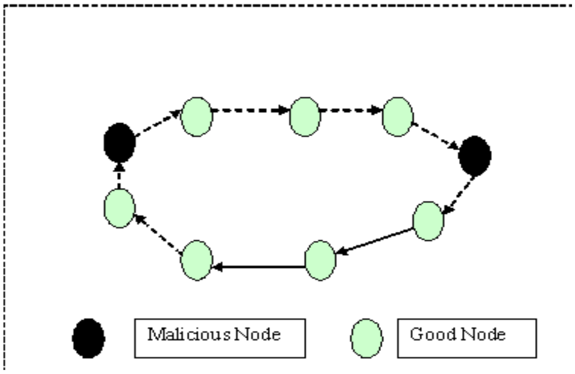
The Wormhole attack[1] is one of the most dangerous and severe security attack and it may result in a significant disruption in the communication across the network ,What makes this attack so dangerous is the fact that it is very easy to implement and difficult to detect in the network.

Two or more malicious nodes [2] can collaborate together to forms a low latency tunnel link and it retransmits them in different parts of the network. The wormhole attack is launched at the network layer [3]. The Architecture of the wireless network allows the malicious nodes to create a wormhole link even for the packets which are not addressed to them by overhearing them and can transmit the same to the other malicious node present at the other end of the network, thereby creating an illusion that these two nodes are physically very close each other. This disrupts the routing as nodes get an impression of a low cost link consisting of 1 or 2 hops as opposed to multiple hops .This attacks are very dangerous and are difficult to detect as these tunnels are private and out of bound and won't be visible to the Wireless Network. These attacks are particularly very dangerous and hard to detect when routing protocols are employed where information like hop count is advertised by the nodes. The attack is launched in 2 phases, in the first phase the malicious nodes tries to attract the legitimate nodes to send data through them, during the second phase the malicious nodes tries to exploit the data in various ways.

Classification of wormhole attacks

Packet Encapsulation attack:

In this type of an attack the malicious node at one end encapsulates the packet being transmitted in the network in order to prevent the network nodes from incrementing the node count. When the packet is received by the other malicious node across the network it will bring the packet to its original state. The figure below indicates such an attack.

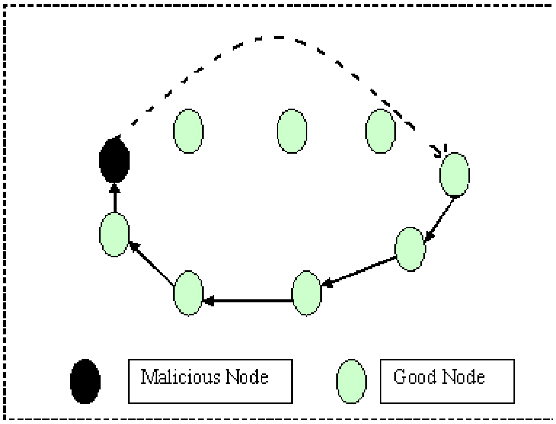


Packet Relay Attack:

In this kind of an attack the two malicious nodes relay the packets which are far apart to each other and give an illusion that the nodes are very close to each other..The figure below indicates such an attack.

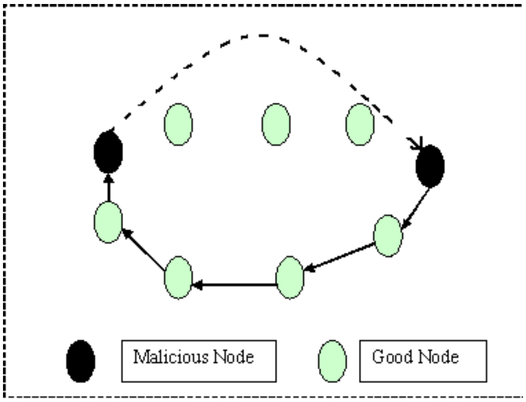
High Power Transmission:

This type of an attack comprises of only one malicious node. This node has a very high transmission power which is used to attract the packets to pass through it.



High Power Transmission:

In this type of an attack the malicious nodes form a wormhole tunnel and advertise it as the shortest path resulting in all communication passing through it. These nodes will advertise the existence of the shortest path between the communicating nodes while making all the communication the take place through this tunnel.



Detecting the Wormhole attacks:

In [4] the author suggests various parameters to be considered to detect the wormhole attacks.

1) A possible symptom can be considered as an abrupt decrease in the path length.

2) If the end-to-end delay calculated by sum of hop delays is increasing in spite of the advertised short path information then a presence of a wormhole can be suspected.

3) Some nodes may not follow the advertised paths but might incur a delay due to some nodes which might be involved in the attacks leading to an increase in the hop delay resulting on an increase in the end-to-end delay in this case a presence of a wormhole can be suspected.

Wormhole detection metrics:

There are various metrics which are used to detect the presence and strength of the wormhole present in the network in [5, 6] the author suggests a few metrics which can be useful in detecting the capacity and capability of the nodes involved in the attack which include length, strength, attraction and robustness

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

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

Robustness: It refers to capability of the wormhole to exist without any change in its strength even after a couple of network topology changes have taken place

Attraction: It refers the metric showing a decrease in the length of the path offered by the wormhole tunnel. in case of a small attraction discrete or small improvements in the regular path may result in decrease in its strength.

References

[1] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), 2002.

[2] Poonam Khare and Sara Ali. "Survey of Wireless Sensor Network Vulnerabilities and its Solution" *International Journal of Recent Development in Engineering and Technology* 2.6 (2014).

[3] Vandana, C. P., and A. Francis Saviour Devaraj. "Evaluation of Impact of Wormhole Attack on AODV." *International Journal of Advanced Networking and Applications* 4.4 (2013): 1652.

[4] 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)

[5] V. Mahajan, M. Natu, A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.

[6] Y. C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in INFOCOM , 2003.