International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# COPY RIGHT

ELSEVIER SSRN



IJIEMR Transactions, online available on 6th Jun 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-06

Title: DETECTION AND PREVENTION OF WORMHOLE ATTACKS IN WIRELESS NETWORK

Volume 08, Issue 06, Pages: 282–287.

Paper Authors

**SARA ALI, DR C. D KUMAWAT**

Mewar University Gangrar, Chittorgarh, India


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# DETECTION AND PREVENTION OF WORMHOLE ATTACKS IN WIRELESS NETWORK

[1]SARA ALI, [2]DR C. D KUMAWAT
[1]PhD Research scholar Dept of CSE ,Mewar University Gangrar, Chittorgarh, India
[2]Professor ,CSE Department ,Mewar University Gangrar, Chittorgarh, India

**Abstract—** Wireless network have is one the most popularly used method of communication. It has gained tremendous popularity since it offers features like flexibility, cost effectiveness, scalability, etc, which has added value to their immense popularity. However the chief challenges being faced by the network are due to security.The networks underlying architecture has exposed it to various attacks .Through our research and by studying various papers we have found "The wormhole attack" to be the most dangerous of them all. The reason for the severity lies in fact that attack is it doesn't need to compromise any network node and any device wireless device like a laptop can be used to send malicious packets. In this paper we conduct a detailed survey on the attack and also analyze various existing detection and prevention techniques and propose an algorithm to detect the attack

**Keywords—**Traffic;Analysis;VPN;Wireless Network;Wormhole Attack;Observer Nodes**;**

## 1. INTRODUCTION

A severe problem faced by various network implementers which effects the utilization of the wireless network is of security [1] .The major advantage of the wireless network is the absence of a basic infrastructure [2] for communication to take place between different network nodes due which a central access point is not required.The increase in the utilization of wireless network has increased the problem of security which is being encountered by various implementers. As the network is has a wireless architecture there is no definite infrastructure [3, 4] for communication between network nodes. The absence of a central access point has exposed the network to various attacks

## 2. ATTACK CLASSIFICATION IN WIRELESS NETWORKS

The network attack classification can be made into the following categories [5]

1) Passive Attack

2) Active Attack.

These attacks are categorized as depicted in Figure

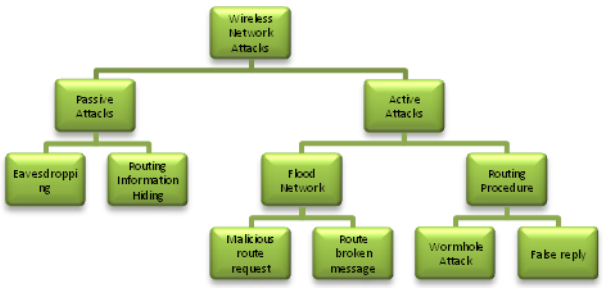



**Figure 1:** Wireless Attack Classification

A. Passive Attack

In passive attack the malicious node monitors the network continuously and collects sensitive information while not being discovered. It monitors the target node continuously till it gains enough data to launch an active attack.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

They are of two types
Eavesdropping and Traffic analysis

B. Active Attack

In active attack after sufficient information has been collected about the network through passive attack the malicious nodes can launch an active attack. The attack can be launched by using a large number of nodes
They are of two types
Routing and Flooding the Network
Through our research we can draw a conclusion that wormhole attack is the most severe of them all.

## 3. WORMHOLE ATTACK

One of the most dangerous attacks in the network is the wormhole attack. Two or more collaborating malicious nodes can initiate the attack by constructing a low latency tunnel and re transmitting the packet to diverse parts of the network. The architecture of the network is such that it has exposed itself to these malicious nodes which capture the packets not addressed to them and re transmits it to the other cooperating malicious node partner at the other end of the tunnel, creating false impression that these nodes are physically very close to each other.

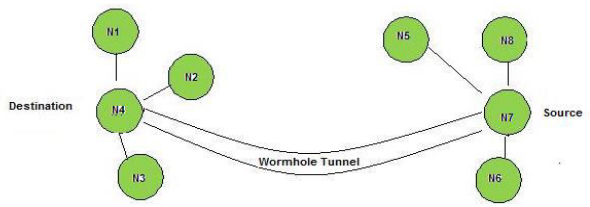



**Figure 2:** Wormhole Attack

These attacks lead to disturbance in the routing as the nodes get an illusion that the link comprises of one or two hops as compared to multiple hops, which may result in packet dropping and flooding. These attacks are thus very dangerous as they are very difficult to detect for the wormhole tunnels are out of bound and private in nature and invisible to the network [5].The Wormhole and black hole attacks create an impression of providing the shortest path and results in the entire traffic getting diverted through this route which may also result in Denial of service attack

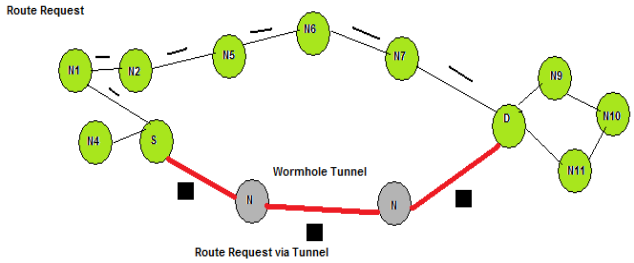



**Figure 3:** Route Request from Source Node of Destination in presence of wormhole Tunnel

## 4. WORMHOLE ATTACK ESTABLISHMENT

The wormhole attack can be categorized in the following categories.

A. Wormhole using Encapsulation
B. Wormhole using Out-of Band Channel
C. Wormhole using Packet Relay
D. Wormhole using High Power Transmission

A. Wormhole Using Encapsulation:

In this type of attack one malicious nodes operates at one end of the network which on receiving a RREQ packet transmits it to the other colluding party present at a distant location which is close to the destination [6,7].The collaborating second party on receiving the broadcasted RREQ packet Re-broadcast the packet.When the neighboring node of the second colluding party receives this packet it drops without any other future legitimate communication request which can arrive through a legitimate path. This results in formation of a wormhole tunnel through which the source and destination will communicate. These malicious nodes will prohibit the other nodes from discovering the rightful nodes. This attack can be by considering a scenario in which node 'A' wants to send a packet to 'B' by discovering the shortest path in presence of two malicious nodes 'X' and 'Y'. On receiving a packet 'X' routes it to 'Y' using the existing path (U-V-W-Z), on receiving the packet 'Y' de-marshals it and re-broadcasts it again. We can notice the hop count hasn't changed due to encapsulation. When the RREQ got transmitted

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

from A to B through C-D-E node 'B' has two path options to choose from the one being (A-C-D-E-B) which contain 4 hops and the second route (A-X-Y-B) which gives an appearance of only 3 hops. Node B will unconsciously select the smaller route which in actuality contains 7 hops. The network implementing shortest path is vulnerable to these kinds of attacks.

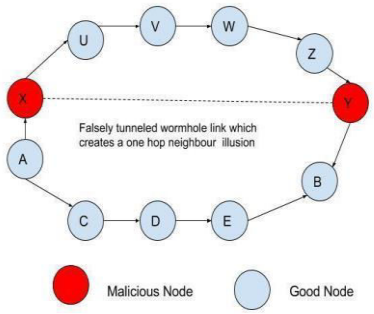



**Figure 4:** Wormhole Using Encapsulation

B. Out of band channel

This mode of attack can be carried forward by using either a direct wired link or long-range directional wireless link. The use of a special hardware makes it more difficult to launch. When two malicious nodes 'X' and 'Y' are present in the network having an out-of-band between them, when node 'X' sends a RREQ request packet to 'Y' which happens to be node 'B' neighbor, when node 'Y' broadcast its packet node 'B' receives 2 RREQ requests A-C-D-E-F-B and A-X-Y-B. The first route is discarded as it appears to be longer and the second is selected.

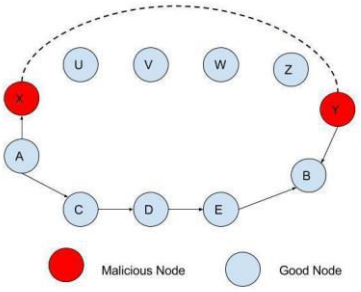



**Figure 5:** Wormhole Using Out of band channel

C. Packet Relay

The malicious node in this mode of attack transmits the packets in between two nodes which are placed at a remote location and establishes them to be neighbors. The attack is very severe and can be launched even with one node. When a large number of nodes are malicious the neighboring list can be expanded and can also get extended to several hops.

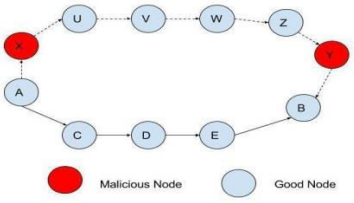



**Figure 6:** Wormhole Using Packet Relay

D. Wormhole with High Power Transmission

The malicious node on reception of a RREQ broadcasts the RREQ at a very high level of power.This ability is not present with any other node. When the node receives a broadcasted packet it re-broadcasts toward the destination.

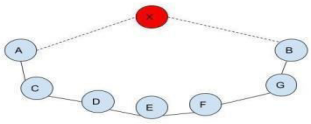



**Figure 7:** Wormhole Using High Power Transmission

## 5. CLASSIFICATION OF WORMHOLE ATTACKS

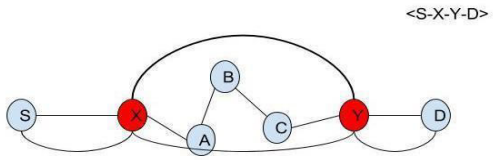
The wormhole attack can be categorized into the following classifications

A. Open Wormhole attack
B. Closed Wormhole Attack
C. Half open wormhole attack.

E. Open wormhole

The attacking nodes in this attack include itself in header of the RREQ request packet following the route discovery process. The nodes are not concealed to the network but the network nodes will not be aware of the malicious nature of these nodes believing them to be their direct neighbors.

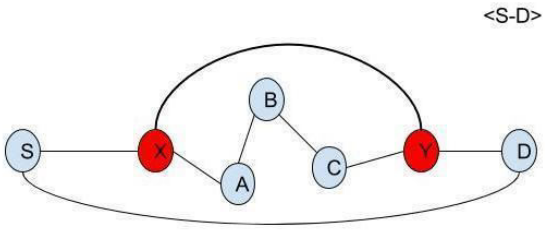
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org




C. **Figure 8:** Open Wormhole Attack

F. Closed wormhole

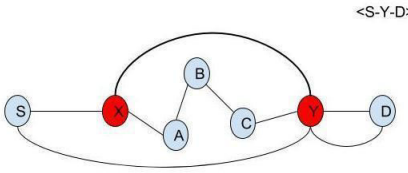
The malicious nodes in this attack will not modify the packet contents; they transmit the packet from one end of the wormhole tunnel to another and re-broadcast the packet again




D. **Figure 9:** Closed Wormhole Attack

G. Half open attack

The malicious node in this attack does not alter the packet at one network end while the node at the other end of the wormhole network tunnel changes the packet followed by the route discovery process




E. **Figure 10:** Half Open Wormhole Attack

## 6. DETECTION OF WORMHOLE ATTACK

The author in [8] considers the following parameters to detect the wormhole attack

1) Reduction in the length of the path

2) An enhancement in the end-to-end delay resulting from calculating the sum of hop delays in spite of short path advertisement.

3) Nodes which not following the paths advertised may be delayed caused by some malicious nodes involved in the attack leading to an increase in the delay in end-to-end routing caused by hop delay.

The various parameters which can be used to sense the presence of wormhole attack and its strength [9, 10] are mentioned below.

H. Length

The difference between the advertised path and actual path is higher then more number of anomalies can be found in our network.

I. Robustness

The capability of the wormhole to be present and not affect its strength in spite of certain changes in the network topology

J. Strength

The consolidated traffic which can be attracted by a node through an incorrect link advertisement made by the malicious nodes.

K. Attraction

This metric represents a decline in the length of the routing path advertised by the malicious wormhole tunnel even through small improvements in the correct path resulting in a decrease in its strength

**Proposed Algorithm**

**VPN**

Virtual Private Network technology is used to secure the network creating an encrypted network on top of a less secure network, when the underlying network fails to do so.

**Observer Nodes**

Network Nodes responsible to monitor the network performance and detect any security breaches

**Cluster**

When a large Network is divided into smaller network spaces it is called cluster which are monitored and controlled by individual cluster heads the Observer nodes

Assumptions

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

1. A Virtual Private Network VPN is build on top of the network .The VPN acts as an administrator which not only maintains a record of nodes present in the network but also maintains a malicious node list. The system contain observer nodes O1...On which are predefined nodes used to continuously monitor the clusters C1...CN network at random interval of time

2. VPN maintains a record of all the malicious nodes monitoring the threshold factor reaching nodes. It also maintains the status of malicious threshold flag.

3. Nodes need to get authenticated by the VPN in order to enter the network
4. VPN assigns an unique id to all the node and during the registration process.

5. Once a node is detected as malicious node the malicious threshold flag is set to zero.
6. When a node enters the network this information is shared with the observer nodes.
7. The observer nodes constantly observe the individual cluster network at a random time‘t’.
8. When the node is detected as malicious using the wormhole detection quantifiers the VPN assigns a malicious threshold flag
9. This flag gets incremented whenever the observer nodes detect a malicious behaviour in the node.
10. When malicious threshold flag reaches a value greater than or equal to 1 it is removed from the network.
11. the node with its unique identifier number gets added to the malicious node list

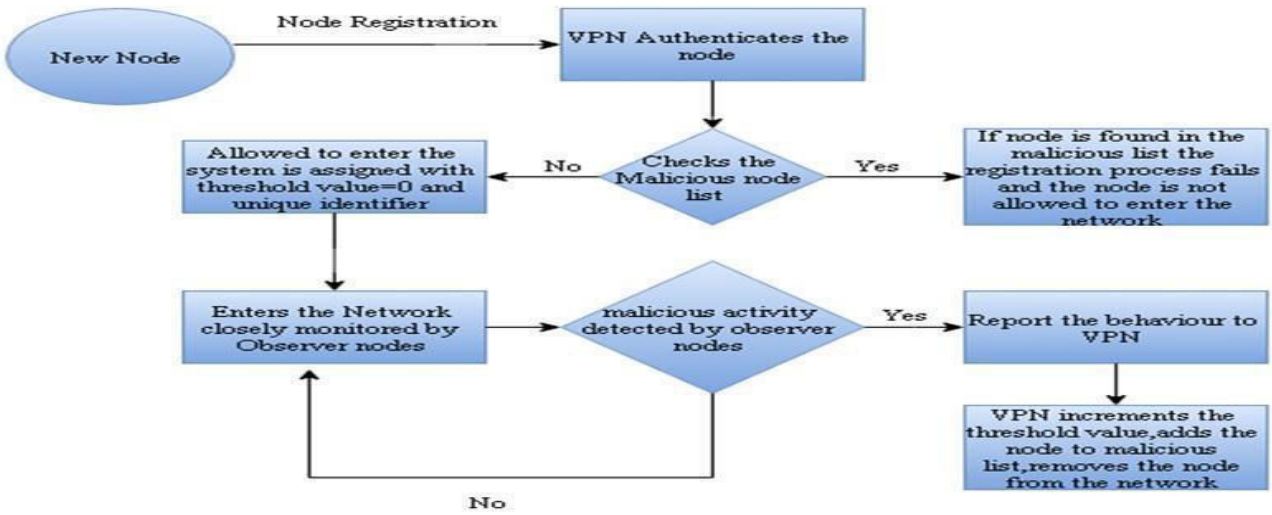



Figure 11: **Wormhole Detection Algorithm**

## 7. CONCLUSION

The Algorithm forms an essential element in this paper .It aids the system in detecting harmful attacks and detects the malicious nodes and removes them from the system after being discovered.Our paper gives an answer to the traffic

problem by keeping a threshold factor in consideration. The VPN helps in improving the accuracy of the system by making the node pass an entry test before it enters the system. On the whole our paper helps in prevention and detection of the wormhole attacks.

## 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

[5] An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach Saurabh Ughade, R.K. Kapoor and Ankur Pandey

[6]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)journal of Multimedia and Ubiquitous Engineering 3.3 (2008).

[7] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks." INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. Vol. 3. IEEE, 2003

[8] Jayarekha, P., Sunil Kalaburgi, and M. Dakshayini. "SECURITY AND COLLABORATIVE ENFORCEMENT OF FIREWALL POLICIES IN VPNS."

[9] V. Mahajan, M. Natu, A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In IEEE Milit

ary Communications Conference(MILCOM), pp. 1-7,2008.

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