ISSN: 2250-0138 (Online)

A NOVEL APPROACH TO DETECT AND PREVENT WORMHOLE ATTACK IN WIRELESS NETWORKS

SARA ALI[a1] AND KRISHNA MOHAN[b]

[a]Department of CSE Mewar University Gangrar, Chittorgarh, India
[b]Siddhartha Institute of Engineering & Technology, Puttur, India

ABSTRACT

Wireless network have gained immense popularity in the last decade as they provide features like scalability, flexibility, cost effectiveness etc. A major challenge observed with the advent of new technology in wireless network is that of security. As the network is wireless in nature it is exposing the different layers to various security threats and attacks. Our research from various papers finds wormhole attack to be the most dangerous and severe attack taking place at the routing protocols. In this attack one or more than one malicious nodes capture the packet at a certain location and re-transmit it to a remote locate .This attack is considered severe as they do not need to compromise any node as they can effectively use a laptop or any other wireless device to send the packets. Through this paper we have conducted a detailed survey on the wormhole attack, its types and classification. We have also analyzed the existing detection techniques and proposed an algorithm for detection of the attack.

KEYWORDS: Traffic Analysis, VPN, Wireless Network, Wormhole Attack.

With an increase in the Utilization of wireless network a problem of security [Ali and Mohan] is being encountered by various implementers. The network is wireless in nature as there is no definite infrastructure [Bundela & Khare and Ali] which exists for communication between network nodes. There is no requirement for a central access point.

There are various factors which have influenced the popularity of the wireless network, some of them are

- Convenience
- Deployment
- Mobility
- Productivity
- Cost Effectiveness
- Flexibility of Location
- Cost

The network has resulted in an increase in the productivity as the accessibility to the network resources increases [Choi et. al.]. The process of configuration and reconfiguration is simple, cost effective as fast.

The main factors which have played an important role in the growth of the wireless network are convenience, cost effectiveness and ease of integration. These days almost all computers are coming equipped with the technology necessary for the wireless network.

ATTACK CLASSIFICATION IN WIRELESS NETWORKS

The attacks in a wireless network can be classified into two types [Ughade et. al.]

1) Passive Attack

2) Active Attack.

These attacks are classified as mentioned in Figure 1

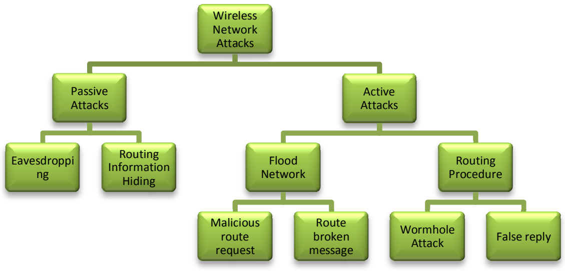

Figure 1: Wireless Attack Classification

Passive Attack

In these types of an attack the node continuously monitors the network and gains information to the sensitive information without being discovered. It monitors the target node till it has gained enough information to launch an active attack.

They are of two types

Eavesdropping and Traffic analysis

Active Attack

After gaining enough information about the network using passive attack the malicious nodes can now launch an active attack. This attack can be established by using a large number of nodes

They are of two types

Routing and Flooding the Network

Our research has leaded us to the conclusion that wormhole attack is the most severe of all.

WORMHOLE ATTACK

The wormhole attack is the most dangerous attack in the network. Two or more collaborating malicious nodes can launch this attack by creating a low latency tunnel and re transmitting the captured packet to different parts of the network. The architecture of the network is such that these malicious nodes can capture packets which are not addressed to these nodes and re transmits the same to the other malicious partner at the other side of the tunnel, this creates an illusion that these nodes are physically very close to each other.

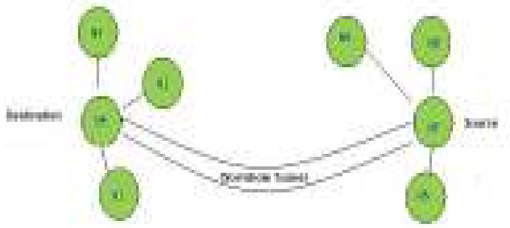

Figure 2: Wormhole Attack

This attacks leads to the disruption in the routing as the nodes get an impression that the link consists of one or two hops as compared to multiple hops. These attacks are thus very dangerous and even difficult to detect as the wormhole tunnels are private in nature and out of bound and hence won't be visible to the network [Marianne et. al.].

The Wormhole and black hole attacks create an illusion of providing the shortest path and results in the entire traffic getting diverted to this route which may lead to Denial of service attack

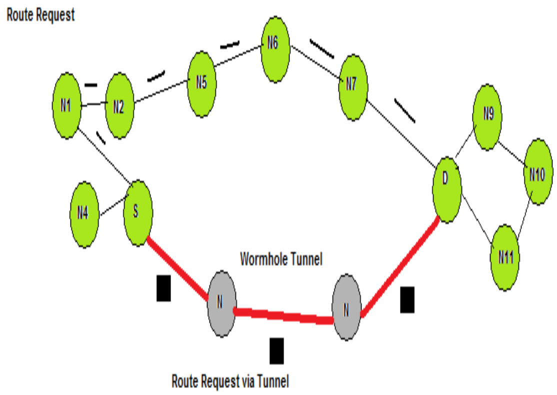

Figure 3: Route Request from Source Node of Destination in presence of wormhole Tunnel

WORMHOLE ATTACK DEPLOYMENT

THE WORMHOLE ATTACK CAN BE DEPLOYED IN THE FOLLOWING MODES.

1) Wormhole using Encapsulation

2) Wormhole using Out-of Band Channel

3) Wormhole using Packet Relay

4) Wormhole using High Power Transmission

Wormhole Using Encapsulation

In this attack one of the malicious nodes at one end of the network hears an RREQ packet and transmits it to the second colluding party at the distant location which is near the destination [Marianne et. al.].The colluding second party on hearing the Re- broadcasted RREQ packet broadcast this packet.

The neighbors of the second party will drop any further legitimate communication request which will arrive on the legitimate path. This has resulted in forming a wormhole network through which the source and destination will communicate. These malicious nodes will prevent the nodes from discovering the legitimate nodes. Let us consider a scenario in which node A tries to send a packet to B by finding the shortest path in presence of two malicious nodes X and Y. When X receives a packet it routes it to Y through the existing path (U-V-W-Z), on receiving the packet Y de-marshals it and rebroadcasts it again. If we notice closely the hop count hasn't increased due to encapsulation. When the RREQ travels from A to B through C-D-E node B has two routes to choose from the first being (A-C-D-E-B) which is 4 hops long and the second route (A-X-Y-B) gives an impression of only 3 hops. Node B will select the smaller route which in reality has 7 hops. Any network using shortest path is vulnerable to these kinds of attacks.

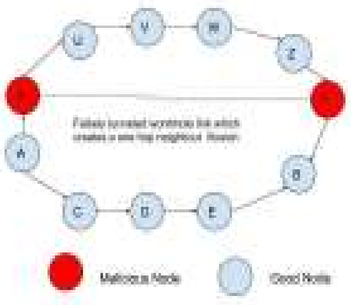

Figure 4: Wormhole Using Encapsulation

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 a channel which is out-of-band between them, when the node X sends a RREQ to Y which is a neighbor 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.

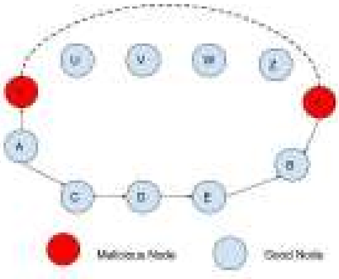

Figure 5: Wormhole Using Out of band channel

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 neighbors. This attack is dangerous as it can be launched even with one node. When large nodes are malicious the neighboring list can be expanded and can be extended to several hops.

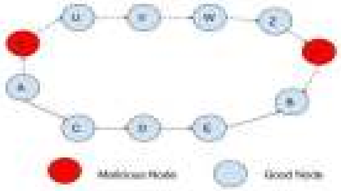

Figure 6: Wormhole Using Packet Relay

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.

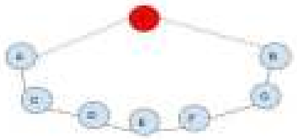

Figure 7: Wormhole Using High Power Transmission

CLASSIFICATION OF WORMHOLE ATTACK

The wormhole attack can be classified into the following types

1) Open Wormhole attack

2) Closed Wormhole Attack

3) Half open wormhole attack.

Open wormhole

In this type of attack the attacker nodes include themselves in header of the RREQ packet followed by the route discovery procedure. These nodes are not hidden in the network but the other nodes will not be aware of the malicious nature of these nodes thinking them to be their direct neighbors.

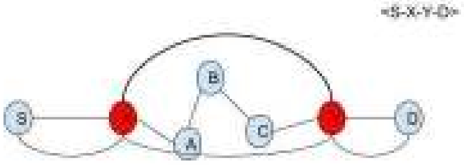

Figure 8: Open Wormhole Attack

Closed wormhole

In this type of an attack the malicious nodes will not modify the packet content; they just tunnel the packet from one end of the wormhole to another and broadcast the packet again

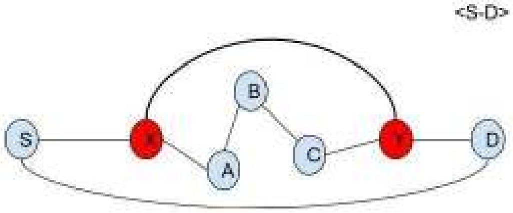

Figure 9: Closed Wormhole Attack

Half open attack

This attack the malicious node at one side of the wormhole does not modify the packet while the node at the other end of the wormhole modifies the packet followed by the route discovery process

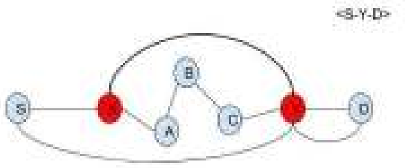

Figure 10: Half Open Wormhole Attack

DETECTION OF WORMHOLE ATTACK

The author in [Hu et. al., 2003 & Jayarekha et. al.] considers the following parameters to detect the wormhole attack

1) Decrease in the length of the path

2) An increase in the end-to-end delay derived from calculating the sum of hop delays despite short path advertisement.

3) Nodes which do not follow the paths advertised may incur delay caused due to some malicious 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 [Mahajan et. al., 2008 & Hu et. al., 2003] are mentioned below.

Length

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

Robustness

The ability of the wormhole to exist and not affecting t its strength despite a certain amount of network topology changes have taken place

Strength

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

Attraction

The metric which displays a decrease in the length of the routing path offered by the malicious wormhole tunnel when small improvements in the correct path results in a decrease in its strength

A BRIEF SUMMARY OF WORMHOLE DETECTION TECHNIQUES

Disadvantages	Advantages	Techniques
Restrict the transmission distance of packet and need the nodes to be tightly synchronized	Both the techniques are employed where strict clock synchronization and global positioning system coordinate all nodes	Distance and location based approach to detect wormhole geographical and temporal
Each nodes needs to be equipped with a special hardware and may result in directional errors	Requires less synchronization.	Directional Antenna
Not always possible to find guard node for particular link.	Guard node or Observer nodes are used to detect the wormhole if one of its neighbor is behaving maliciously	LITEWORP
Guard node uses local broadcast keys which are available only in one hop neighbors.	Approach Uses encryption techniques	Graph Theoretical
	1. Guard nodes are used to inform cluster heads about the attack. 2. No special hardwires are used.	Cluster based detection techniques.

WORMHOLE DETECTION ALGORITHM

VPN

A Virtual Private Network is a technology used to secure the network which creates an encrypted network over a less secure network, when the underlying network fails to do so.

Observer Nodes

Network Nodes which are concerned with monitoring the network performance and detecting any security breaches

Assumptions

1) VPN build on top of it which maintains a record of all nodes present in the network and maintains a malicious list. The system contains observer nodes

which constantly monitor the network at random interval of time.

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

3) All Nodes need to get authenticated by the VPN to enter the network

4) VPN assigns a unique identifier to the node and during the registration phase checks if the node was previously

5) Detected as malicious node and set malicious threshold flag to zero.

6) Once the node enters the network the information is shared with the observer nodes.

7) The observer nodes constantly monitor the network at random time t.

8) Once the node is detected as malicious it is reported to the VPN which assigns a malicious threshold flag

9) This gets incremented whenever the observer nodes report the node to be malicious.

10) When malicious threshold flag is greater than or equal to 1 it is removed from the network and the node

11) With its unique identifier number and IP address gets added to the malicious node list

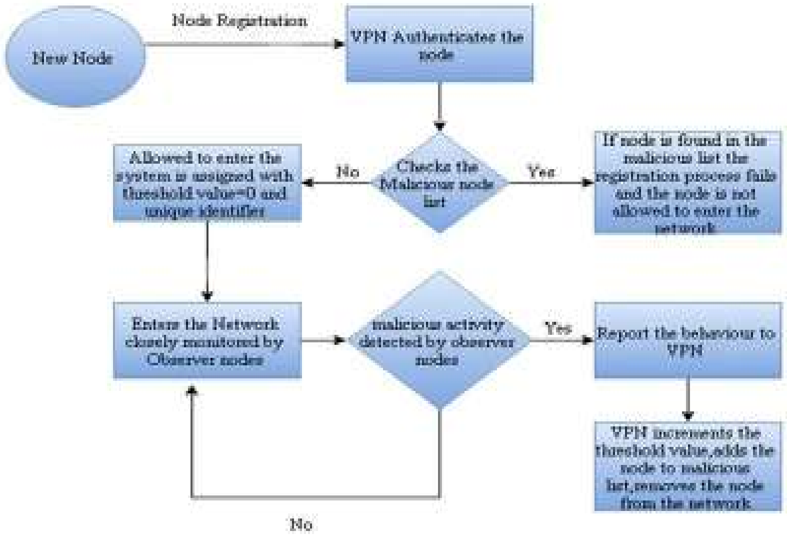
New Node
Node Registration
VPN Authenticates the node
Checks the Malicious node list
No
Yes
Allowed to enter the system is assigned with threshold value=0 and unique identifier
If node is found in the malicious list the registration process fails and the node is not allowed to enter the network
Enters the Network closely monitored by Observer nodes
malicious activity detected by observer nodes
Yes
Report the behaviour to VPN
VPN increments the threshold value,adds the node to malicious list,removes the node from the network
No

Figure 11: Wormhole Detection Algorithm

CONCLUSION

The Algorithm forms an integral part in this paper .It helps the system from harmful attacks and detects the malicious nodes and deletes them from the system when discovered.

Our paper also gives a solution to the traffic problem by keeping a threshold factor in consideration. The VPN helping in improving the authenticity of the system and makes the node passes an entry test before entering into the system. On the whole our paper helps in prevention and detection of the wormhole attacks.

REFERENCES

Ali S. and Mohan S.K., International Journal of Advanced Research in Computer Science Research Paper Enhanced Security Framework for Wireless Networks.

Bundela A.S., Ijesrt International Journal Of Engineering Sciences & Research Technology Literature Survey On Wormhole Attack, Computer Science & Engineering Medicaps Institute of Technology and Management, Indore (M. P.), India.

Khare P. and Ali S., Ijrdet Survey of Wireless Sensor Network Vulnerabilities and its Solution.

Choi M.-K. et. al., "Wireless network security: Vulnerabilities, threats and countermeasures." International .

Ughade S., Kapoor R.K. and Pandey A., An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection

Approach.

Marianne A., Sherif E.-K., Magdy E.-S., “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).

Hu Y.-C., Perrig A. and Johnson D.B., 2003. "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**.

Jayarekha P., Kalaburgi S. and Dakshayini M., "Security and Collaborative Enforcement of Firewall Policies in VPNS.”

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

Hu Y.C., Perrig A. and Johnson D.B., 2003. “Packet leashes: a defense against wormhole attacks in wireless networks,” in INFOCOM.