International Journal of Engineering Research and General Science Volume 2, Issue 4, June-July, 2014
ISSN 2091-2730

# Detecting Wormhole Nodes in WSN using Data Trackers

Harleen Kaur[1], Neetu Gupta[2]

[1]Research Scholar (M.Tech), ECE, Global Institute of management and Emerging Technology

[2] Asst. Professor, Global Institute of management and Emerging Technology

E-mail- harleen.kaur15@yahoo.com

**Abstract-** Wormhole attack can be destabilizes or disables wireless sensor networks. In a typical wormhole attack, the attacker receives packets at one point in the network and forwards them with a less latency than the network links, and relays them to another point in the network. This paper describes the taxonomy of wormhole attack and presents the several scenarios of wormhole attacks.

**Keywords-** Wireless sensor network, Wormhole detection, Ad hoc network, tunnel, latency, Wireless sensor nodes, malicious node.

## INTRODUCTION

The basic wireless sensor network [1] consists of large number of sensor nodes which are densely deployed over a sensor field. All nodes are connected by radio frequency, infrared, or other medium without any wire connection. This type of network is called wireless sensor network Fig.1.1 is shown below.WSN contains micro-controller, circuit for interface between sensor node and battery, a radio transceiver with antenna for generating the radio waves through which they can communicate and perform operations [2].

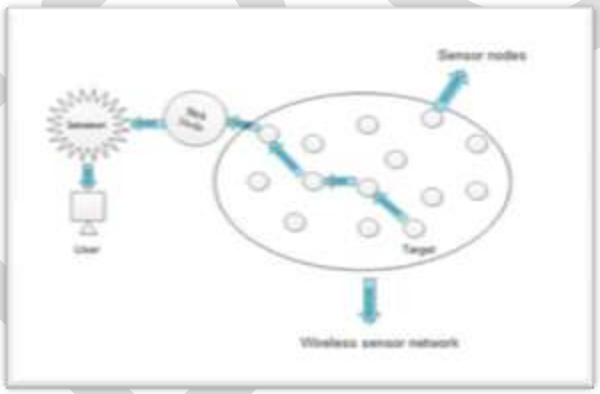


Fig.1.1: General Wireless Sensor Network

With the rapid development in wireless technology, ad hoc network have emerged to attract the attention from industrial and academic research projects. Ad hoc networks are vulnerable to attacks due to many reasons a particularly severe security attack, called the wormhole attack [3], [4], [5]. During the attack [6] an adversary receives packets at one location in the network and tunnel them to another location in the network, where the packets are resent into the network .The remainder of this paper is organized as the following way. Section II gives the taxonomy and basic definition of Wormhole attack. Section III presents survey on wormhole attack. Finally, conclusion is presented in Section IV.

## WORMHOLE ATTACK

In the wormhole attack, an attacker receives packets in one part of the network over a low latency and tunnels them in a different part. The simplest instance of this attack is that single node is situated between two other nodes for forwarding the messages between two of them.

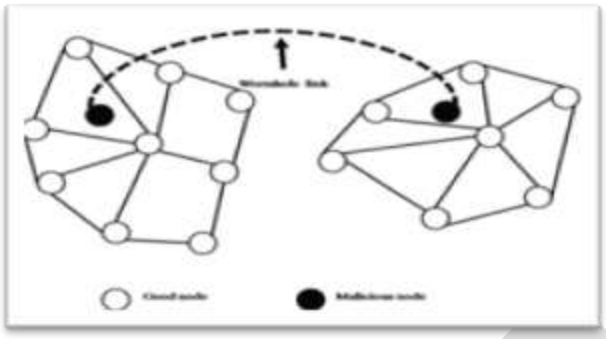

Fig.2.1: Wormhole Attack

Depending on whether the attackers are visible on the route, packets forwarding behavior of wormhole nodes as well as their tendency to hide or show the identities, wormholes are classified into three types: closed, half open, and open as shown in fig.2.2.

1. Open Wormhole

In this mode, nodes (Source(S), destination (D), wormhole ends M1 and M2) are visible and A and B are kept to be hidden. The attacker is aware about the presence of malicious nodes which further include themselves in the packet header to follow the route discovery procedure.

2. Half-Open Wormhole

Malicious node M1 near the source (S) is visible, while second end M2 is set hidden. To tunnel the packets from one side to another over the path S-M1-D sent by S for D, attacker does not modify the contents of the packet and rebroadcasts it.

3. Close Wormhole

Identities of all the intermediate nodes (M1, A, B, M2) on path from S to D were kept hidden. In this scenario both source and destination feel themselves just one-hop away from each other. Thus fake neighbors were created.

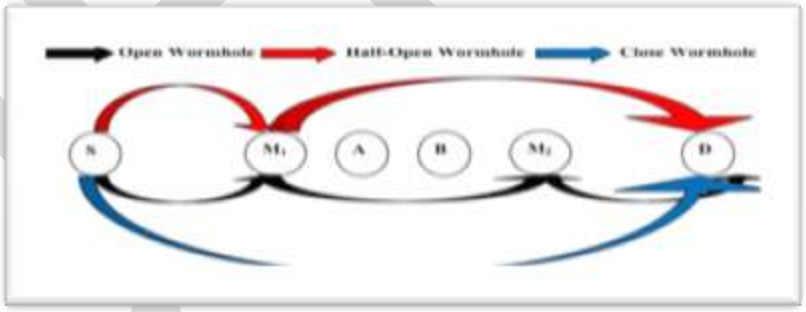


Fig.1.3: Representation of Open, Half-Open and Closed Wormhole

A. Taxonomy of Wormhole Attack

Wormhole attacks can be classified based on implementation technique used for launching it and the number of nodes involved in establishing wormhole into the following types:

1. Wormhole using Packet Encapsulation

Nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Hence, routing protocols that use hop count for path selection are particularly susceptible to encapsulation-based wormhole attacks.

2. Wormhole Using High-quality/Out-of-band Channel

In this mode, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. This tunnel can be achieved, for example, by using a direct wired link or a long-range directional wireless link.

3. Wormhole Using High-power Transmission Capability

In this only one malicious node with high-power transmission capability increases its chance to be in the routes established between source and the destination without the interference of another malicious node. When a malicious node receives an RREQ, it broadcasts the request at a high-power level. Any node that hears the high-power broadcast rebroadcasts the RREQ towards the destination. [11].

4. Wormhole Using Packet Relay

In this attack, one or more malicious node relays data packets of two distant sensor nodes to convince them that they are neighbors. This kind of attack is also called "replay-based attack".

5. Wormhole Using Protocol Distortion

In this mode, one malicious node tries to attract network traffic by distorting the routing protocol. Routing protocols that are based on the 'shortest delay' instead of the 'smallest hop count' is at the risk of wormhole attacks by using protocol distortion.

**LITERATURE REVIEW**

| Ref no. | year | |
|---|---|---|
| [7] | 2005 | A lightweight countermeasure for the wormhole attack, called LITEWORP, which is particularly suitable for resource-constrained multihop wireless networks. Simulation results show that every wormhole is detected and isolated within a very short period of time and packet loss is less when LITEWORP applied. |
| [8] | 2006 | A severe attack in ad hoc network routing protocols and location based that is particularly challenging to defend against. A general mechanism, called packet leashes, for detecting and, thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes. Topology-based wormhole detection is discussed, and shows that it is impossible for these approaches to detect some wormhole topologies. |
| [9] | 2009 | This paper describes different modes and classes with an attack graph that is used to illustrate the sequence of events in each mode. This attack presents as a two phase process launched by one or several malicious nodes. To illustrate this attack's effect we presented the simulation results of two modes of this attack. |
| [10] | 2011 | Routing protocol WHOP for detecting wormhole of large tunnels length without use of any hardware such as directional antenna and clock synchronization. WHOP uses an additional Hound packet and does not require changes in the existing protocol AODV. Our simulation results show that the WHOP is quite excellent in detecting wormhole of large tunnel lengths. |

| | | |
|---|---|---|
| [11] | 2012 | This paper proposes the security emerges as a central requirement as mobile ad hoc network applications are deployed and form a serious threat in wireless networks. It introduces the wormhole attack, enables an attacker with limited resources and no cryptographic material to wreak havoc on wireless networks. It is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. |
| [12] | 2013 | This paper presents simulation results based on packet reception ratio, packet dropped ratio, and throughput and providing higher level security. Routing attack for wireless sensor network and can be implemented by using Mint route protocol to defend against. |
| [13] | 2013 | In this paper alternative path from source to second hop and calculate the number of hops to detect the wormhole. The technique is localized, requires only a small overhead, and does not have special requirements such as location information, accurate synchronization between nodes. |

## CONCLUSION

The intent of the paper is to throw light on the wormhole attacks in WSN. The paper provides a detailed description of the wormhole attack categories and provides a description of the review of the studies about the wormhole attack in different scenarios.

## REFERENCES:

[1] I.Akyildiz, W. Su, Y. Sankara subramaniam and E. Cayirci, "A survey of sensor networks", IEEE Communications, vol. 40(8), pp. 102–114, 2002.

[2] Kashyap Patel and T.Manoranjitham, "Detection of Wormhole attack in wireless sensor network "International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 2 Issue 5, May -2013.

[3] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", in 1st IEEE International Workshop on Sensor Network Protocols and Applications (WSNA), 2003, pp. 113-127.

[4] Y. C. Hu, A. Per rig, and D. B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks", in 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), 2003, pp. 1976-1986.

[5] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", in Network and Distributed System Security Symposium (NDSS), San Diego, 2004.

[6] K. Lee, H. Jeon, and D. Kim, "Wormhole Detection Method based on Location in Wireless Ad-Hoc Networks", in New Technologies, Mobility and Security: Springer Netherlands, 2007, pp. 361-372.

[7] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Network" Proceedings of the 2005 International Conference on Dependable Systems and Networks, 0-7695-2282-3, IEEE 2005.

[8] Yih-Chun Hu,Adrian Perrig ,David B.Johnson, "Wormhole attacks in wireless networks" IEEE Journal on Selected Areas in Communications, Vol. 24, NO.2,February2006, pp. 0733-8716.

[9] Marianne Azer, Sherif El-Kassas,Magdy El-Soudani, "A Full Image of the Wormhole Attacks towards introducing Complex Wormhole Attacks in wireless Ad Hoc Networks ", International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009.

[10] Saurabh Gupta,Subrat Kar ,S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet"IEEE International Conference on Innovations in Information Technology,2011.

[11] Bintu Kadhiwala and Harsh Shah, "Exploration of Wormhole Attack with its Detection and Prevention Techniques in Wireless Ad-hoc Networks", International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012) Proceedings published in International Journal of Computer Applications (IJCA) (0975 – 8887).

[12] Kashyap Patel and T.Manoranjitham, "Detection of Wormhole attack in wireless sensor network"International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 2 Issue 5, May -2013.

[13] Devendra Singh, Kushwaha Ashish Khare, J. L .Rana, "Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET" International Journal of Computer Applications (0975 – 8887), Volume 62– No.7, January 2013