ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

A Survey on Wormhole Attack Detection Algorithm

G. Vaishnavi[1], Dr. R. Dhaya[2]

[1] M.E. Computer science and engineering
[1,2]Velammal Engineering College

Manuscript Info

Manuscript History:

Received: 15 September 2015
Final Accepted: 15 October 2015
Published Online: November 2015

Key words:

Wormhole attack, Wireless networks, Security.

Corresponding Author

G. Vaishnavi

Abstract

Wireless sensor networks are the infrastructure- less network which are vulnerable to various routing attacks. This in- turn degrade the performance of the sensor network and information are received by wrong sinks. In this case, the wormhole attack poses a serious threat in compromising sensor nodes and adds new set of malicious nodes to the network. Hence the low latency links are established and packets are replayed between two nodes. To detect and avoid this wormhole attack, various algorithms are presented. This paper emphasis on the study of these algorithms and suggest the best algorithm to detect and avoid wormhole attacks in wireless sensor networks.

INTRODUCTION

In modern days, variety of real-life applications, use WSN. For instance, Environment monitoring, traffic controlling and battle field surveillance. Generally, wireless sensor networks are typically used in open environment where the sensor nodes move freely. Thus these mobile nodes are vulnerable to all kind of network attacks such as Sybil attacks, wormhole attack, flooding attack, sinkhole attack and more. All these attacks disrupt the operation of WSNs and violate basic requirements for secure communications.

Among various attacks, the wormhole attack is very dangerous as this attack involves in connecting two nodes in the network through low latency link which serves as a tunnel between the nodes. This is done by recording the traffic in the network and replaying it in different regions. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where A and B are not themselves within transmission range of each other. Intruder node X merely tunnels control traffic between A and B (and vice versa), without the modification presumed by the routing protocol.

I. SECURITY GOALS FOR WSN

The primary security requirements for WSN are confidentiality, integrity, availability and freshness. In addition to that, authentication, access control, privacy, authorization, non- reputation and survivability are also important.

Confidentiality- Confidentiality is the capability to hide messages from a passive attacker such that every message communicated using the sensor network remains confidential. It is the most important concern in network security. A sensor node should not expose its data to its neighbours.

Integrity- Data integrity is the measure to ensure the consistency of data and to verify that the message has not been altered or changed.

Availability- it is the availability of the resources that can be used by the sensor nodes. The failure of base station or cluster head eventually results in a threat to entire system. Thus data availability has the main importance.

Freshness- in WSN, it should be guaranteed that the sensor nodes must contain the fresh new data and the old data are replayed.

II. WORMHOLE ATTACK

The wormhole attack is a severe threat against wireless networks in which an attacker tunnels the messages received in one part of the network and replays them in a different part, as shown in Figure 1. Once the wormhole link is operated, the attacker analyse the traffic and masquerades the messages at one end and forwards them to the other end selectively, where the packets are retransmitted to hack other parts of the network. Thus nodes resembles like that they are only one or two hops away via the wormhole, even though they are at multiple hops.

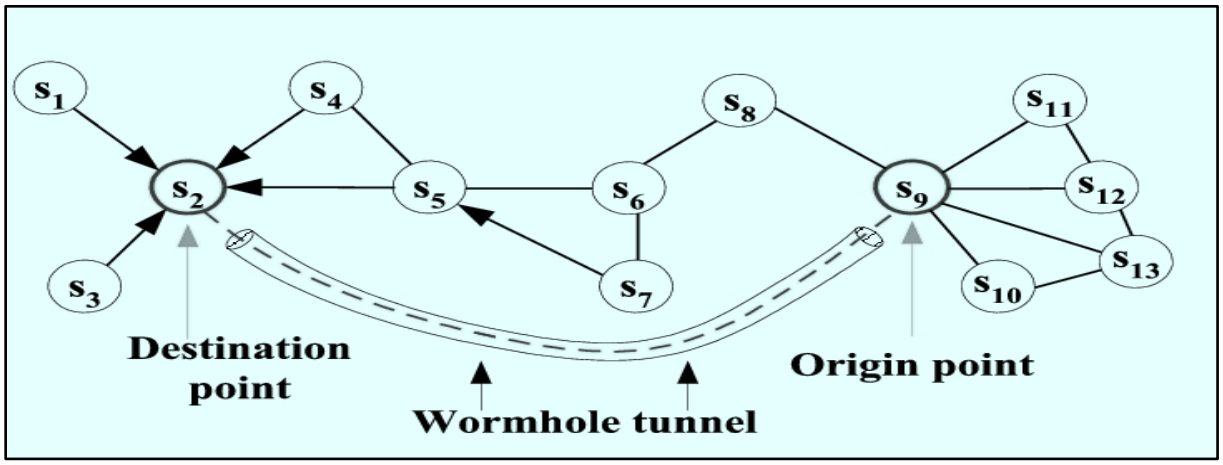

Figure 1: A Model of Wormhole in WSN

As an overall effect, the nodes of two regions seem to be in single region and hence the attacker can compromise the whole network. This is like considering all nodes in one area to be in another area. As a result, the attacker can reduce the overall performance of the wireless sensor network by compromising the integrity between various sensor nodes.

APPROACHES TO WORMHOLE ATTACKS

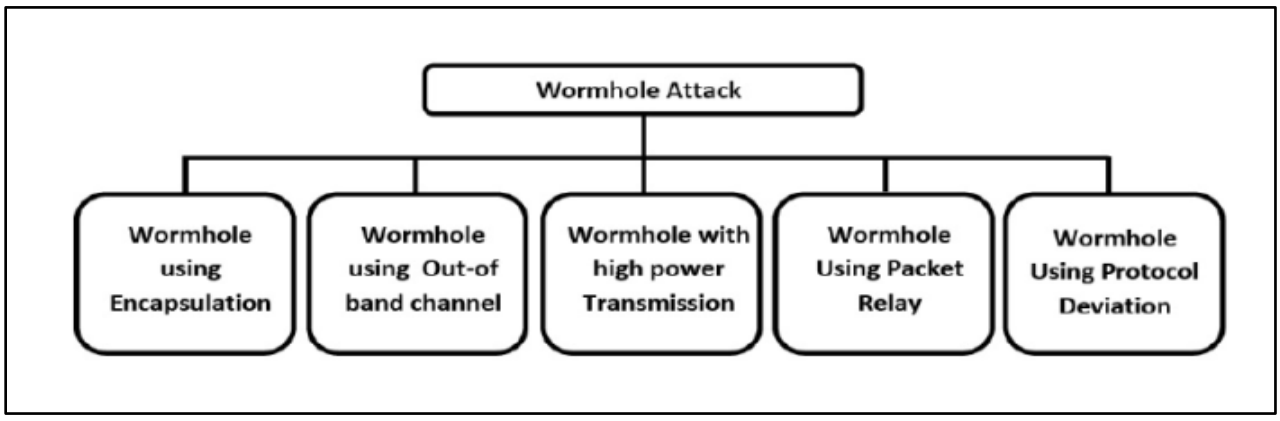

Figure 2: Wormhole attack approaches

Wormhole using Encapsulation:

In encapsulation-based wormhole attacks, several internal nodes present between two malicious nodes. At one wormhole edge point the data packets are encapsulated and packets forward via wormhole link. Since encapsulated data packets do not increase the actual hop count during the traversal through wormhole link. At the other wormhole edge point, the data packets are de- capsulated and broadcast to its neighbours.

Wormhole Using High-quality/Out-of-band Channel:

In this type, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link between the malicious nodes. This type of attack needs specialized hardware capability.

Wormhole Using High-power Transmission Capability:

In this type of attack, there is only one malicious node with high-power transmission capability in the network. It can communicate with other normal nodes from a long distance. When a malicious node receives a RREQ, it broadcasts the request at a high-power level. Any node that receives the high-power broadcast rebroadcasts the RREQ to its neighbours. It can be mitigated if each sensor node is accurately measure the received signal strength.

Wormhole Using Packet Relay:

In this type of attack, a malicious node relays data packets of two distant sensor nodes to convince them that they are neighbours. In Figure (a), sensor node A and B are actually non-neighbouring nodes. Node M1 can relay packets between sensor nodes A and B to make them believe that they are neighbours to each other. As shown in Figure (b), if there are several cooperating malicious sensor nodes, sensor nodes that are multiple hops away from each other can be victims of this attack.

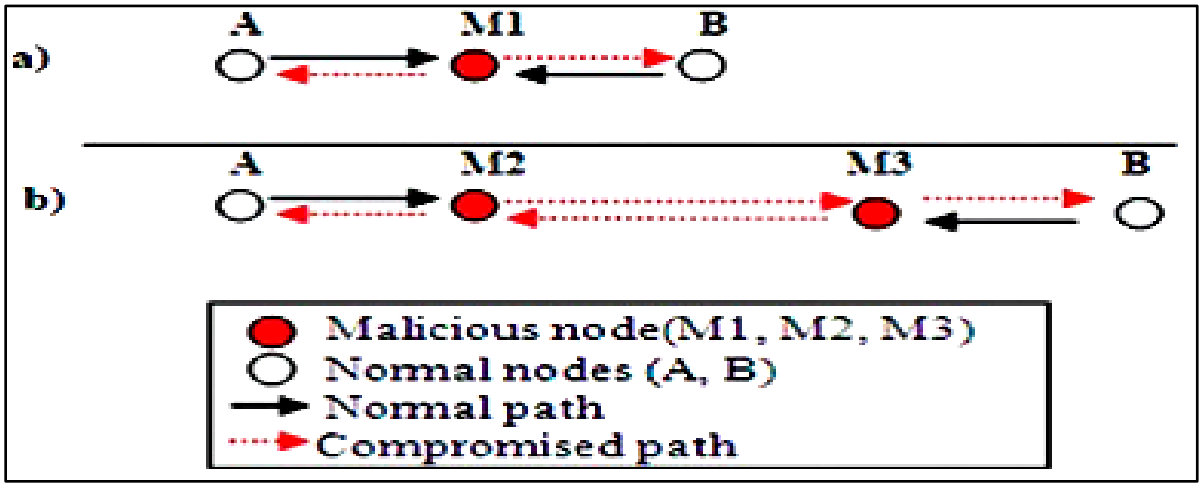

Figure 3: Wormhole using packet relay

Wormhole Using Protocol Distortion:

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. In hop-count-based routing protocols, sensor nodes typically wait for a random back-off time before RREQ forwarding to reduce the number of MAC-layer collisions. In this wormhole mode, a malicious node can create a wormhole by not forwarding RREQs without back-off. The purpose is to let the RREQ packet arrive first at the destination so that the malicious nodes make a part of path to the destination.

III. LITERATURE SURVEY

In this paper, various techniques and algorithms are discussed to detect and prevent wormhole attacks in wireless sensor networks. Every algorithm have their own pros and cons.

a. LOCATION BASED END TO END DETECTION

In the paper [1], the author proposed a lightweight location verification system which performs the location verification using GFM and GFT algorithm. With the help of these algorithms, we can verify the location of sensor nodes which are in- region (application specific). When the attacker is hidden and out of bound, the packet loss in wormhole is unavoidable.

In the same construct, [2] points out the WDI Algorithm to isolate the wormhole based on the hop count of the nodes from source. In this case, there may be miss detection of wormholes which cannot be identified by this approach thus leading to false alarm or removal of incorrect wormhole link which causes distortion in the network through which the attacker may intrude.

b. USING GRAPH STRUCTURE

The authors of [3] have proposed an algorithm for multi hop network where the link information are shared between all the nodes in the cluster. This algorithm is good as it do not involve with specialized hardware but depending upon connectivity information alone may create loopholes as in case of mobile wireless Ad-hoc networks, the connectivity between nodes can change as they move with respect to time and location.

c. TIME BASED APPROACH

The presence of timing based algorithm in [4] appears good when the assumption that the wormhole link remains stable at a particular time is true. This validity is purely depends upon the mobility of nodes in the network. Also the time synchronization factor must hold correct when wormhole links are being detected using this approach. In case, if time synchronization mechanism is not involved, the hop count must be managed between the nodes which results in tedious processing. Hence the statistical analysis method is introduced in [5]. Using this approach, the suspicious links may be found but the confirmation of wormhole cannot be detected as it requires better time constraint for further confirmation of malicious links.

The calculation of round trip time between nodes can improve the detection of wormholes. This is done in the paper [6]. Here, delay per hop value is calculated using the formula RTT/2h where, h is the hop count. It is proved that if RTT value is larger than the hop count, and then there is a chance of prevalence of wormhole in the network. This condition may fail if the message sent through the link is bulky which takes more time to reach the destination. This predominantly increases the RTT even if the link is free from wormhole.

d. LINK STATE ROUTING APPROACH

Using Optimal Link state Routing protocol, the countermeasure for wormholes can be engineered. But, the severity of the attack cannot be reduced even when the confidentiality and authenticity is produced in the network. Thus in paper [7] the authors have presented WP- OLSR, as an extension to the OLSR protocol to combat against the attack. Though time- synchronization and location information are not required, this method surely needs a specialized data- structure which must be taken care always and routed to all the nodes in the network which consumes more energy.

e. IDENTITY BASED APPROACH

In the paper [8] the authors moved a step ahead and introduced an approach to prevent the network from wormhole attack. They used co- operative intrusion detection algorithm to exchange the ID between the nodes in the network. Thus the origin of attack was found. The paper also provides some example ID hierarchy which is stored in hierarchical tree structure. This can create a loophole when the tree becomes complex as the number of node grow in the network. Hence, load balancing has to be produced for better results.

f. LINEAR PROGRAMMING MODEL

Finally, the key management technique came into action to device Linear Programming model to enhance security in the network. In paper [9], the key distribution techniques are considered with Linear Programming to empower the effectiveness of the system proposed. This estimates the input parameter strengths in an attack environment.

The authors of [10] have introduced another interesting concept called DAWN, a distributed algorithm to detect wormhole attacks in wireless network coding systems and ETX (expected transmission count) to stabilize the collaboration between the nodes in the network such that the innovative packets are examined between the nodes and detect the attacker in the network.

Table 1: Summarized approaches and limitations

S. No	APPROACH	ATTRIBUTES TAKEN CARE	LIMITATIONS
1	Location based end to end detection	Sensor location, hop count	Irresistible packet loss when attacker is hidden and the chances of false alarm is high
2	Detection using graph structure	Connectivity information with shortest path algorithm in graph structure	Maintenance of graph structure for mobile nodes are difficult and any nodes can cluster with the cluster head
3	Time based approach	Time synchronization and delay in hop with respect to Round trip time	False alarm is produced when bulky data is sent.
4	Link state routing approach	WP- OLSR algorithm, table maintained for sent and received HELLO message.	Since the table must be distributed among all nodes after each update, the power consumption will be more also it is vulnerable to attack.
5	Identity based approach	Co- operative intrusion detection Algorithm	When the cluster grows, then the node identity structure also grows complex
6	Linear Programming Model	Distributed algorithms and ETX (expected transmission count)	This approach even serves better when unique node identification is provided.

IV. CONCLUSION

Wormhole attacks in wireless sensor network significantly degrade the overall performance and efficiency of the network. In this paper we have discussed various approaches of wormhole attack and many countermeasure algorithms to prevent and detect wormhole attack. On analysing all the above algorithms, the Linear programming model with DAWN and ETX serves as an optimal prevention mechanism for wormhole attack. And collaborating with some unique identification of nodes in the network can make the attacker stay away from the network in future.

REFERENCES

Yawen Wei and Yong Guan, “Lightweight Location Verification Algorithm for Wireless Sensor Network,” IEEE Transaction on Parallel and Distributed Systems, vol. 24, pp: 938-950, 2013.

Yun Wang, Zhongke Zhang and Jie Wu, “A Distributed Approach for Hidden wormhole detection with neighbourhood Information,” Fifth IEEE International conference on Networking, Architecture and Storage, pp:63-72, 2010.

Ritesh Maheshwari, Jie Gao and Samir R Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," in IEEE INFOCOM proceedings, pp:107- 115, 2007.

Jinsub Kim, Dan Sterne, Rommie Hardy, Roshan K. Thomas, and Lang Tong, "Timing-based Localization of In-Band Wormhole Tunnels in MANETs," ACM 978-1-60558-923-7/10/03, 2010.

Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao and Fuxiang Gao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis," in WASE International Conference on Information Engineering, pp:251-254, 2010.

Prasannajit B,Venkatesh, Anupama S,Vindhykumari K, Subhashini S R and Vinitha G, "An Approach towards Detection of Wormhole Attack in Sensor Networks," in First International Conference on Integrated Intelligent Computing, pp:283-289, 2010.

Azeddine Attir, Farid Na¨ıt-Abdesselam, Brahim Bensaou and Jalel Ben-Othman, "Logical Wormhole Prevention in Optimized Link State Routing Protocol," in IEEE GLOBECOM proceedings, 2007.

Anthony McAuley, Kyriakos Manousakis, Dan Sterne, Richard Gopaul, Peter Kruus, "Creating and Maintaining a Good Intrusion Detection Hierarchy in Dynamic Ad Hoc Networks," by the U.S. Army Research Laboratory under the Collaborative Technology Alliance (CTA) Program, Cooperative Agreement DAAD19-2-01-001 1.

Ambika.N, G.T.Raju, "Linear Programming Model of Sensor Network," in International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014.

S. R. Naresh, S. V. Gayathri Soumiya and A.V. Ramprasad, "PROTECTING SOURCE LOCATION PRIVACY AGAINST WORMHOLE ATTACK USING DAWN IN WIRELESS SENSOR NETWORKS," in ARPN Journal of Engineering and Applied Sciences, ISSN 1819-6608, pp: 3844-3849, 2015.