ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 2, February 2020

An Overview on Wormhole Attack in Wireless Sensor Networks

Parvathy.K

Assistant Professor, Department of Information Technology, Info Institute of Engineering, Coimbatore, India

ABSTRACT: The wireless sensor network is an emerging technology in the field of communication. Now a days, use of wireless sensor network(WSN) is spreading more rapidly across the world. WSN has found lots of applications in environment monitoring, military applications, health care monitoring, habitat monitoring, etc. Because of these applications WSN is carrying very sensitive information and hence is the target for hackers to get some sensitive information. This technology has many advantages but the security issues have been not given much consideration till now. Due to this neglecting, few loopholes in the security have started to occur such as wormhole attack. In this paper we are going to discuss about wormhole attack, attack model and detection mechanisms.

KEYWORDS:Wormhole Attack , Wireless Sensor Network ,

I. INTRODUCTION

The Wireless Sensor Networks are the network which consist of many number of sensor nodes. These sensor nodes which mainly perform these operations like signal processing, sensor configuration and computation. The sensor nodes which helps to mitigate the environmental condition. The applications used in wireless sensor networks are environment monitoring, military application, healthcare monitoring, habitat and industrial monitoring. Since there are only limited number of nodes, the traditional security is impossible for this kind of networks.

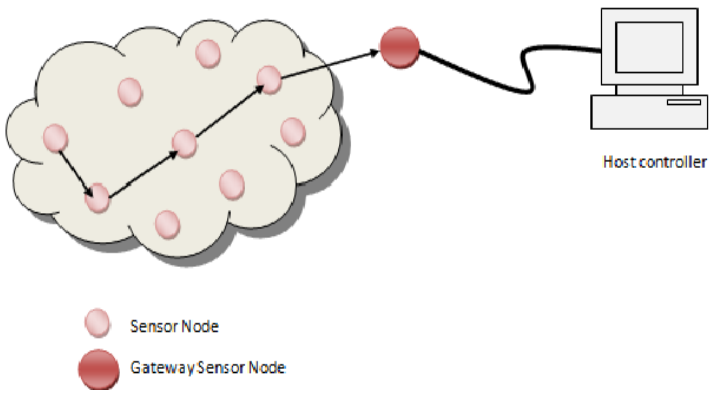


Fig.1.Wireless Sensor Networks

The Architecture of WSN are made up of sensor nodes, base station and the server. The sensor nodes are connected to each other with base station and the server. The nodes which mainly connected to the wireless medium, to communicate to the sensor nodes, base station and server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 2, February 2020

II. WORMHOLE ATTACK

The two nodes which communicate among each other through a link where these link are called as tunnel. During the communication from source to destination, the attacker who get inside the two nodes and create a link i.e., tunnel. The Attacker who capture the packet from the tunnel and send a malicious node through the tunnel.

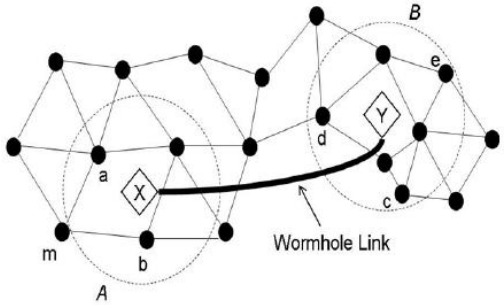


Fig.2.Wormhole Attack

The Wormhole Attack is classified into three types.

- Open Wormhole Attack/Exposed
- Half Open Wormhole Attack
- Closed Wormhole Attack/Hidden

Half Open Wormhole Attack

Malicious node M1 near the source (S) is visible, while second end M2 is set hidden. This leads to path S-M1-D for the packets sent by S for D. The attackers do not modify the content of the packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet.

Open Wormhole Attack/Exposed

Source(S) and destination (D) nodes and wormhole ends M1 and M2 are visible. Nodes A and B on the traversed path are kept hidden. In this mode, the attackers include themselves in the packet header following the route discovery procedure. Nodes in network are aware about the presence of malicious nodes on the path but they would imitate that the malicious nodes are direct neighbours.

Closed Wormhole Attack/Hidden:

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

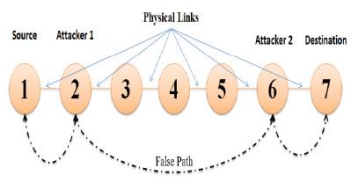
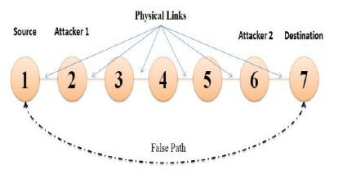
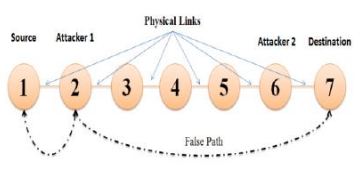
Open wormhole	Closed Wormhole	Half open Wormhole
		

Fig.3.Wormhole Attack Model

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 2, February 2020

III. DETECTION MECHANISM

WSN is spreading faster because of its various applications and hence the need of securing it also increasing. There are lot of algorithms for detection and prevention of the wormhole attack.[2] Detection of wormhole attack is easier task as compare to prevention of wormhole attack. Loads of research is still going on for finding out efficient methods of detection and prevention.[5] Some of the detection methods are mention in the following table.

Table.1.Detection Mechanisms for Wormhole Attack[1][3]4[][5][10][12]

Name of the Method	**Requirements/Commentary**
Geographic and temporal leashes	• GPS coordination of every node; • Loosely synchronized clocks (ms); • Robust, straightforward solution; • Inheritance of general limitations of GPS technology
Packet leashes, end-toend	• GPS coordination of every node; • Loosely synchronized clocks (ms); • Inheritance of limitations of GPS technology
Network visualization	• Centralized Controller; • Works best on dense networks; • Mobility is not studied; • Varied terrains are not studied
Localization	• Location-aware; • use of guard‘ Nodes; • Not readily applicable to mobile networks
Directional antennas	• Directional antennas on all nodes; • Good solutions for networks relying on directional antennas,
Time of flight	• Hardware enabling one-bit message and immediate replies without CPU involvement; • Impractical; • Likely to require MAC-layer Modifications
Connectivity-based Approaches	• Require connectivity information; • Tightly synchronized clocks (ns); • Impractical
End-to-end mechanism	• Requires knowledge of location information; • Loosely synchronized clocks; • This mechanism uses geographic information and authentication method to detect malicious neighbors
Secure eighbour discovery	• Secure eighbour discovery
Connectivity graph	• Connectivity information is required; • To be independent to wireless communication models

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 2, February 2020

IV. CONCLUSION

In this survey we conclude that WSN is spreading widely across all over the area and became the main target for the attackers. Wormhole attack is such one of the serious threats for WSN. It reduces the performance of the sensor network. Presence of two wormholes can attract nearly the network traffic [10]. there are many algorithms and methods being developed to detect and prevent the attack with considering the available sensor network parameters. Hence there is still need to improve the performance of detection and prevention algorithms and efficient use of sensor.

REFERENCES

1.Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d Auriol, Heejo Lee, Sungyoung Lee and Young-Jae Song, ―Achieving Network Level Privacy in Wireless Sensor Networks,‖ Sensors 2010, *10*, pp.1447- 1472.

2. Majid Meghdadi, Suat Ozdemir and Inan Güler, ―A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks,‖ IETE technical review, VOL 28, ISSUE 2, 2011.

3 Xiaopei Lu, Dezun Dong, Xiangke Liao, ―WormPlanar: Topological Planarization Based Wormhole Detection in Wireless Networks,‖ 42nd International Conference on Parallel Processing (ICPP), pp.498 –503.

5 Louazani A., Sekhri L., Kechar B., ―A time Petri net model for wormhole attack detection in wireless sensor networks,‖ International Conference on Smart Communications in Network Technologies (SaCoNeT), pp.1 – 6.

6. Alam M.R., Chan K.S., ―RTT-TC: A topological comparison based method to detect wormhole attacks in MANET,‖ 12th IEEE International Conference on Communication Technology (ICCT), 2010, pp.991 – 994.

7 Ambika, N., Raju, G.T., ―MA WSN — Manifold authentication in wireless sensor network,‖ World Congress on Information and Communication Technologies (WICT), 2012, pp.572 – 576.

8 Shiyu Ji, Tingting Chen, Sheng Zhong, Kak, S., ―DAWN: Defending against wormhole attacks in wireless network coding systems,‖ INFOCOM, 2014 Proceedings IEEE, pp.664 – 672.

9 Dhurandher, S.K., Woungang, I., Gupta, A., Bhargava, B.K., ―E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks,‖ 26th International Conference on Advanced Information Networking and Applications Workshops, 2012, pp.472 – 477.

10 Meenakshi Tripathi, M.S.Gaur, V.Laxmi, ―Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN,‖ The 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN), Procedia Computer Science 19 (2013), pp.1101 – 1107.

11. D.Sheela, Srividhya.V.R, Vrushali, Amrithavarshini and Jayashubha J., ―A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks,‖ International Conference on Computational Techniques and Artificial Intelligence (ICCTAI'2012) Penang, Malaysia.

12. Pushpendra Niranjan, Manish Shrivastava, Rajpal Singh Khainwar, ―Enhancement of Routes Performance in MANET,‖ International ournal of Computer Applications (0975-8887) Vol.42–No.12, March 2012.

13. Zaw Tun and Aung Htein Maw, ―Wormhole Attack Detection in Wireless Sensor Networks,‖ World Academy of Science, Engineering and Technology 46, 2008.