NHSEMH - 2023
2nd National Conference on New Horizons in Science, Engineering, Management and Humanities
International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Analysis of Wormhole Attack in Wireless Sensor Networks: A Review

Rakesh Kumar, Ajay Kumar Gupta, Jai Prakash Bhati, Abhishek Kumar
Department of CSE (AI), IIMT Engineering College, Greater Noida, Uttar Pradesh, India

ABSTRACT

Wireless Sensor Networks are a collection of minor sensor nodes. The sensors devices gather the information from the open environment for the use of intended purpose. The WSNs are contaminated from various types of attacks like wormhole attack, blackhole attack, sybil attack, and sinkhole attack. But the wormhole attack is one of most severe attack in WSNs. It creates a tunnel in the network and mislead the data packets. To prevent the sensor network from these attacks a various technique has defined such as watchdog technique, Wormhole Attack Detection Protocol using Hound Packet (WHOP), and Delay Per Hop Indication (DELPHI).

Keywords: WSN, Wormhole Attack, Watchdog, WHOP, DELPHI

I. INTRODUCTION

Wireless sensor networks are the combination of very small tiny devices known as sensors and the main objective of these sensor devices to measure the activities of a particular region where the sensors have deployed. The wireless sensor network is used in various fields like military, hospitals, agriculture, health, and to measure the number of environmental conditions like moisture, temperature, and humidity [1].

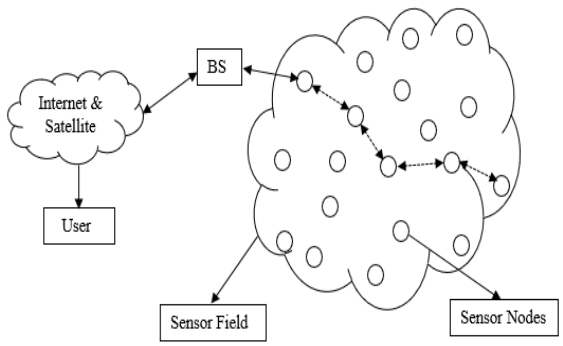

Fig. 1 WSN Architecture

WSN attacks

The Wireless Sensor Networks attacks viewed on security, protocols. It can base on the principle of communication. In Wireless Sensor Network, we can categorize it into two main types.

A. **Active Attack**: The active wants to make changes in the transmitted messages or try to modify it. The attacker can also try to inject its information in the traffic or to disturb the transmission [2].

B. **Passive Attack**: The passive attacks are difficult to trace-out because they only listen to the information. Neither they modify the information nor to exchange it. These attacks are basically supported for the active attack after gaining the information [3].

Security Goals in WSN

The wireless sensor network is not untouched from the various types of attacks. The primary requisites to

supreme the security checks are Availability, Confidentiality, Integrity, and Authenticity. Except these, some other secondary conditions are source localization, self-organization and data freshness [4].

Availability: Availability designates the data should be always on site all time even in case of a contamination. So for this, it is important that the network should be more and more secure.

Confidentiality: Confidentiality should be compulsory from both the sides sender and receiver. There is an important term Secrecy at both the endpoints. The secrecy is of two types, one is forward secrecy and another backward secrecy. In forwarding secrecy, the sender may not be able to retrieve the information after denying the network while in backward secrecy the receiver member node may not be able to access the precedent information afore joining the network. So, secrecy is a consequential thing to maintain between sender and receiver.

Integrity: The data sent by the sender should be modified at the receiver end. The can be modified by the intruder or by an intruder. If the received information is modified then the network should be able to detect the modifications.

Authenticity: Inauthenticity the verification of the sender node is an important thing for the receiver so that any trait node cannot impose any data in the network.

Wormhole Attack

In the wormhole attack, the malicious node has more energy in comparison than the other nodes at the initial level, so it works as a cluster head for the first round. After being a cluster head, it receives the data from all neighbor nodes, then it aggregates the whole data and does not transfer to the base station so the total amount of transmitted data is reduced [5].

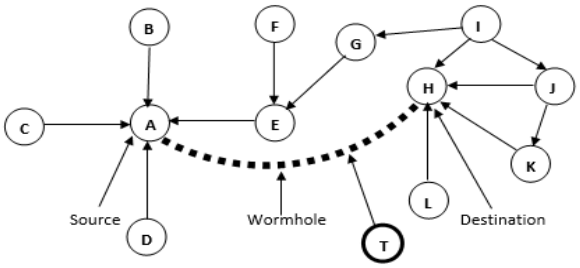

Fig. 2 Representation of Wormhole Attack

WORMHOLE ATTACK MODEL

A. Open Wormhole

In open wormhole attack the malicious node M1, M2 and source and destination nodes are visible while nodes A and B kept hidden. The attackers involved in packet header following the route discovery procedure. The nodes in the network are sensible about the about the beingness of malicious nodes on the path but they would copy that the malicious nodes are direct neighbors [6].

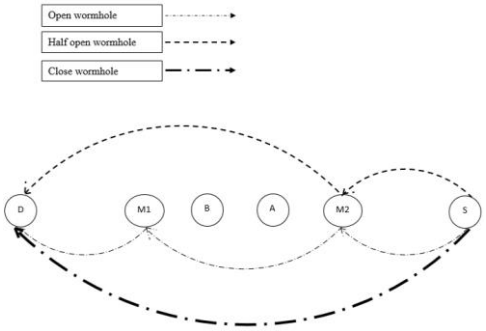

Fig. 3 Representation of Open, Half Open, and Close Wormhole

B. Half-Open Wormhole

The malicious node M1 is near to source node is open while the malicious node M2 node is invisible. The path traversed in this is S-M1-D for transferring the data by source to destination. The malicious does not alter the data of the packet. Alternatively, they normally tunnel the data from one side to another side and it retransmits packets [7].

C. Close Wormhole:

The IDs of all intermediate nodes are hidden between Source and Destination. So, in this way, the Source

node and Destination node feel that they are just one-hop off from each other. Thus, bogus nodes are created [8].

Types of Wormhole Attack

The wormhole attack can be classified on the basis of performance and the number of nodes involved in the simulation.

A. Wormhole using packet encapsulation:

In this scenario, an intruder node hears at one end to RREQ packets and transmits the information to the second end node. After that, the second party node rebroadcasts the RREQ and drops the packets. So, the resultant is that the collaboration of these nodes establishes a packet encapsulation wormhole [9].

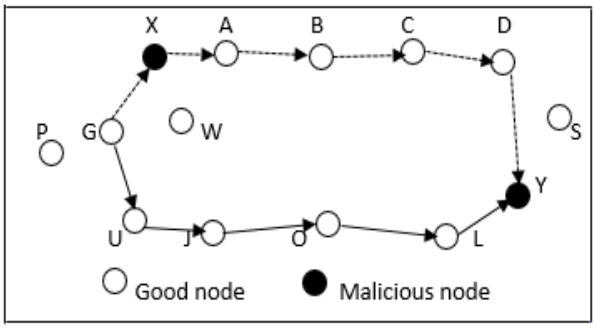

Fig. 4 Wormhole Using Packet Encapsulation

B. Wormhole Using Out-of-band Attack: This takes place due to the high bandwidth energy between the assailed nodes. This link is achieved via long-range direct wireless or wired link. Such type of attack is not easy because it needs some specialized hardware capability [10].

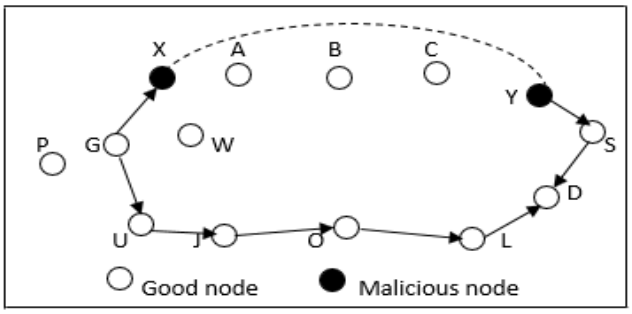

Fig. 5 Wormhole Using Out-of-band

C. Wormhole Using Packet Relay: In Wireless Sensor Networks, such type of attacks can be launched with the help of one or more than nodes. The assailed node transmits the data packets of two faraway sensor nodes to agree them that they are neighbors [11].

D. Wormhole Using High Power Transmission: This type of attack can be done only a single assailed node with a high-power transmission. The assailed node communicates faraway nodes. As the assailed accepts an RREQ, it transmits the request a ta high power level. The receiving node rebroadcasts the RREQ to the destination. Due to this, the assailed have a great chance to initiate a route between the source and sink without the participation of any other assailed node. The chance of occurrence is to be reduced if every sensor node has the ability to measure the received signal strength (RSS) [12].

Schemes to detect the Wormhole Attacks

A. Watchdog technique: With the help of watchdog technique user can traits detect the assailed nodes in the network area. In this scenario, the source node transmits a message to the sink node via an intermediate node. If the intermediate does not transmit the received to sink node, then user declares a malicious node to the intermediate node [13] [18].

The main problem of watchdog approach in leach protocol afore the steady phase and withal used decentralized Intrusion detection method in setup and steady phase [14].

B. Wormhole Attack Detection Protocol using Hound Packet (WHOP): The WHOP protocol was suggested for the wormhole attack detection in AODV protocol. In this methodology, a hound message transmits after discovering the path. The hound packet traverses all the nodes except the nodes are

involved in the path set-up. After receiving the packet by the sender, it launches a hound packet to digest it by its own private key and associate all the information with the hound packet.

But the main problem with the WHOP protocol, the processing of packets is too poor [15].

C. **Delay Per Hop Indication (DELPHI):** In DelPHI wormhole observation user gathers hop count as well as delay information to observe the wormhole detection. In the normal conditions, the delay of a should remain same along each path. But the path traversed via any assailed node should be higher than the normal traversal [16]. This method works only for the checking of wormhole attacks and a delay between the source and sink node [18].

The main restriction of DelPHI mechanism is that it can work for some of the paths tunnelled by wormhole attack, if most of the paths are tunnelled by wormhole attack then it will not work well [13].

D. **Location-Based Approaches:** The main moto behind the location-based approach is to use the geographical id to recognize the assailed nodes. Before transmitting the information, nodes fix a communication time and geographical id and the next receiving node calculate the transmission time to ensure the wormhole attack [17].

E. **Time Calculation Based Approaches:** In this scenario the is a True Link means a direct link among adjacent nodes. The Direct Link takes two steps to detect the wormhole named as rendezvous and validation. The first step is done with timing factor between the nodes but does not exchange any information while the second phase prove that both the nodes are validate to each other. The main downside of this technique is that it operates only on IEEE 802.11 gadgets. So, the True Link technique is planned only for secret attacks.

TABLE 1 Wormhole Attack Detection Techniques

Detection Technique	Necessity/ Analysis
Watchdog Technique	Wrong response, collaboration, incomplete drizzling
WHOP	Works with only private key, packet processing too poor
DelPHI	No need to readjustment, delay as well as hop count is measured
Location Based Approaches	Location of each node, unambiguous solution.
Time Calculation Based Approach	Validation mechanism, operates only with IEEE 802.11 hardware.

II. CONCLUSION

Here we have discussed different types of wormhole attack in wireless sensor networks and detection mechanism for wormhole attacks as well. Each and every detection mechanism has the ability to detect. The watchdog mechanism is a powerful tool for the detection of wormhole attacks in the network. The DelPHI mechanism the user collects the hop count and observe the delay entire network. The WHOP mechanism is used to detect the wormhole attack in AODV protocol but it has constraint of poor packet transmission.

III.REFERENCES

[1]. Taranpreet Kaur et. Al., “DDOS attack in WSN: A survey”, IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), December 23-25, 2016, Jaipur, India.

[2]. Mohamed-Lamin Messai, “Classification of attacks in wireless sensor networks”,

International Congress on Telecommunication and Application 14 University of A. MIRA Begeria, Algeria, 25-23 APRIL 2014.

[3]. Furrakh Shahzad et. al., "A Survey of active attacks on wireless sensor networks and their countermeasures", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 12, December 2016.

[4]. Jitender Grover, et. al., "Security issues in wireless sensor network – A Review", at 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Sep. 7-9, 2016, AIIT, Amity University Uttar Pradesh, Noida, India.

[5]. Siddiq Iqbal et. al., "Comparison of different attacks on leach protocol in WSN", at International Journal of Electrical and Data Communication, ISSN: 2320-2084.

[6]. Nishant Sharma et. al., "Various approaches to aetect wormhole attack in wireless sensor networks", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February-2014, pg. 29-33.

[7]. Dhara Buch et. al., "Prevention of wormhole attack in wireless sensor network", International Journal of Network Security & Its Applications (IJNSA), Vol. 3, No. 5, Sep 2011.

[8]. Priya Maidamwar et. al., "A survey on security issues to detect wormhole attack in wireless sensor network", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012.

[9]. Marianne Azer et. al., "A full image of the wormhole attacks towards introducing complex wormhole attacks in wireless Ad Hoc networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol 1, No. 1, May 2009.

[10]. Monika et. al., "A novel approach for detection and prevention of wormhole attack in Ad-hoc networks", International Journal of Computer Trends and Technology (IJCTT) – Volume4 Issue5-May2013.

[11]. Majid Meghdadi et. al., "A survey of wormhole based attacks and their countermeasures in wireless sensor networks", IETE Technical Review, 28:2, 89-102.

[12]. Shweta Dalke et. al., "Performance analysis of wormhole attack in wireless sensor network using AODV routing protocol", SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) - volume 2 issue 2 Feb 2015.

[13]. Rupinder Singh et. al., "WRHT: A hybrid technique for detection of wormhole attack in wireless sensor networks", Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 8354930, 13 pages

[14]. Mohammad Reza Rohbanian, et.al, "Watchdog-LEACH: A new method based on LEACH protocol to secure clustered wireless sensor networks", at ACSIJ Advances in Computer Science: An International Journal, Vol. 2, Issue 3, No., 2013.

[15]. Amit Rawat et. al., "The effects of various wormhole techniques", International Research of Journal Engineering and Technology (IRJET), Volume: 03 Issue: 12/Dec-2016.

[16]. Hon Sun Chiu et. al., "DelPHI: wormhole detection mechanism for Ad Hoc wireless sensor network", The 1st International Symposium on Wireless Preserve Computing, Phuket, Thailand, 16-18 January 2006.

[17]. Ankit Mehto et. al., "A dynamic hybrid approach for wormhole detection and prevention", 4th ICCCNT 2013 July 4-6, 2013, Tiruchengode, India. IEEE-31661.

[18]. Richa Mudgal et. al., "Study of various wormhole detection techniques in mobile Ad hoc network", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016, 978-1-4673-9939-5/16/$31.00 ©2016 IEEE.