A Literature Survey on Security Issues of WSN and Different Types of Attacks in Network

VarshaGharu
Deptt. of IT, SOIT, RGPV, Bhopal, Madhya Pradesh, India
gharuv27@gmail.com
https://www.rgpv.ac.in

Mahesh Pawar
Deptt. of IT, SOIT, RGPV, Bhopal, Madhya Pradesh, India
mkpawar24@gmail.com
https://www.rgpv.ac.in

Jitendra Agarwal
Deptt. of IT, SOIT, RGPV, Bhopal, Madhya Pradesh, India
jitendra@rgtu.net
https://www.rgpv.ac.in

Abstract - This review work present a gist of security issues related to the WSN network and discusses different types of attacks in the network. Sensor nodes, when deployed to form a network of wireless sensors operating under the control of central authority, namely the base station, are capable of presenting interesting applications due to their ability to be deployed ubiquitously in hostile and ubiquitous environments. But for the same reasons, security becomes a major concern for these networks. The purpose of this paper is to analyze threats to wireless sensor networks and to identify various research efforts to investigate various routing attacks targeting the network layer. A particularly devastating attack is the Wormhole attack, a denial of service attack, where attackers create a low latency link between two points of network. By studying existing Wormhole detection methods, researchers are identifying and delineating key search challenges for detecting wormhole attacks in the network layer.

***Keywords*:** Wormhole; WSN; Blackhole; Manet.

1 INTRODUCTION

A wireless sensor network is a set of nodes organize into a cooperative network. Each node consists of a processing capacity, can contain several types of memory (program, data and ash memories), an RF transceiver (usually with a single omni-directional antenna), a power source (batteries and Solar cells) and accommodate various sensors and actuators. The nodes communicate wirelessly and self-organize often after being deployed in a punctual manner. Systems of 1,000 or even 10,000 nodes are provided. Such systems can revolutionize the way we live and work. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years the world will be covered with networks of wireless sensors with access to them via the Internet. This can be seen as the Internet becoming a physical network. This new technology is exciting with unlimited potential for many fields of application including environment, medical, military, transportation, entertainment, crisis management, homeland defense and smart spaces. Since a wireless sensor network is a real-time distributed system, a natural question is how many solutions from distributed and real- time systems can be used in these new systems.

The main problems that affect the design and performance of a wireless sensor network are: Hardware and Operating System for WSN, Wireless Radio Communication Characteristics, Medium Access Schemes, Deployment, Localization, Synchronization, Calibration, Network Layer, Transport Layer, Data Aggregation and Data Dissemination, Database Centric and Querying, Architecture, Programming Models for Sensor Networks, Middleware, Quality of Service, and Security.

2 ATTACKS IN WSN

The most vulnerable attack in terms of resource depletion in WSN is Denial of Service Attacks (DOS). Denial of service attacks are specific attacks that attempt to prevent legitimate users from accessing networks, servers, services, or other resources by sending unnecessary additional packets and thus preventing legitimate users from accessing services or resources.

2.1. *Black hole attack*

Also known as sink holes occurring at the network layer. It builds an alliance node that seems very attractive in the sense that it promotes zero cost routes for neighboring nodes with respect to the routing algorithm. This results in maximum traffic to these false nodes. Nodes adjacent to these harmful nodes run into huge bandwidth, resulting in contention of resources and destruction of messages

2.2. *Wormhole attack*

In the attack of the wormhole, a pair of horrible nodes first discovers a wormhole on the network layer. All network traffic is tunneled in a particular direction to a remote location, which causes the deprivation of data reception in other parts of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This can cause congestion and retransmission of packets wasting energy from innocent nodes. The attack of the wormhole on the network of wireless sensors [8].

2.3. *Selective forwarding attack*

Selective forwarding is a network layer attack. In this case, an opponent will fit a knot that scrupulously sends some messages and plunges others. This hampers the quality of service in WSN. If the attacker drops all packets, the adjacent nodes become aware and can evaluate it as a fault. To avoid this, the attacker intelligently transmits the selective data. To understand this type of attack is a very tedious job.

2.4. *Flooding*

Flooding also occurs on the network layer. An opponent constantly sends connection requests to the selected node. To reach each request, certain resources are allocated to the opponent by the targeted node. This can result in an effusion of the memory and energy resources of the node that is bombarded.

2.5. *Sybil attack*

This is still a network layer attack. In this case, a horrible node has more than one character in a network. It was originally described as an attack capable of overcoming the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. Sybil's attack is efficient enough to cut other fault tolerance schemes such as disparity, multi-path routing, routing algorithms, aggregation of data, voting, fair allocation of resources and Maintenance of the topology and detection of malfunctions. The false node implies different identities to other nodes of the network and is therefore located in several places at the same time. In this way, it disrupts geographic routing protocols. It can collide with routing algorithms by building many routes from a single node.

2.6. *Node replication attack*

Each sensor node of a network has a unique identifier. This ID can be duplicated by an attacker and is assigned to a new malicious node added in the network. This ensures that the node is in the network and it can lead to various disastrous effects to the sensor network. By using the replicated node, packets passing through the malicious node may be missed, misrouted, or modified. The result is inaccurate packet information, loss of connection, loss of data, and high end-to-end latency. Malicious node can get the authority of sensitive information and therefore can harm the network [10]

3 WORMHOLE ATTACK IN WSN

Wormhole is an attack type in which two attacker nodes create a link calling the worm link from which the two nodes can communicate. These nodes give the illusion that the selected path is the shortest path to get the destination. FIG. 1 shows the general working scenario of the attack of the wormhole on the network of wireless sensors [8].

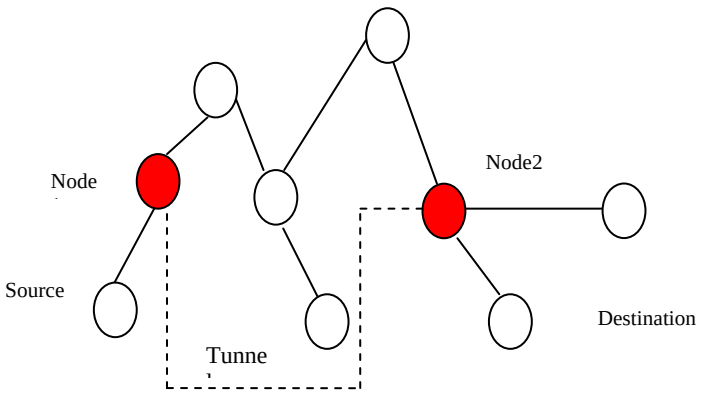

Figure 1: Wormhole Attack

3.1. *Wormhole Attack Model*

Wormhole attack is a network layer attack that can affect the network even without the knowledge of cryptographic techniques implemented. This is why it is very difficult to detect. It is caused by one, two or more numbers of nodes. In the most common type of two completed wormhole, one end tunnels the packets via the worm link and the other end, at the packets reception, replays them at the local area. Number of nodes involved in establishing the wormhole and how to establish it classifies the wormhole in the following types. Wormhole types and patterns are explained here [7].

- Wormhole using Out-of-Band Channel

In this two-end wormhole, a dedicated channel of wide bandwidth out-of-band is placed between the endpoints to create a wormhole link.

- Wormhole using Packet Encapsulation

Each packet is routed through the legitimate path only when it is received by the end of the wormhole, is encapsulated to prevent the nodes in the path from incrementing the hopping counts. The packet is formatted by the second end point.

- Wormhole using High Power Transmission

This type of worm tunnel approach has only one malicious node with a very high transmission capacity that attracts packets to follow the path passing from it.

- Wormhole using Packet Relay Like the previous approach, a single malicious node is required to replay packets between two remote nodes and thus create fake neighbors.
- Wormhole using Protocol Deviation.

The malicious node creates a wormhole by returning packets without retreating unlike a legitimate node and, therefore, increases the possibility that the wormhole path is selected. [7]

The attack of the wormhole can be classified in different ways. Here a few classifications are given below:

- In bound wormhole attack
- Out of bound wormhole attack
- Open wormhole attack
- Half open wormhole attack
- Closed wormhole attack

In the band and out of the band are two other types of wormhole classification. In this way, the attacker builds a tunnel overlay on the existing wireless medium so that it is known as the wormhole attack in the tape. This attack is potentially very harmful and is the most preferred choice for the attacker. On the other hand, the out-of-band uses the different wireless network to perform the attack in the network. In the case of an open attack, the attacking node monitors network RREQ packets, in the presence of malicious nodes in the network, other nodes on the network assume that the malicious node is present on the path and are their neighbors directly. This means that both nodes show their identity in the network.

The Half-Open Wormhole attack is exactly like the open hole but here only one node shows its identity, another hide from the network. Thus, the modification of the packets will be done on one side.

These are third types of wormholes where the attacking node does not balance the data packet. The two nodes are hidden from the node. They listen to network activity and always show the shortest path. When the sender finds his way using an algorithm, then the hidden node response and the sender trap in this scenario.

4 PRIOR APPROACH

[1] In this research work, the authors propose a trusted distance vector routing protocol (T-AODV) to protect the network of wireless sensors from wormhole attacks. The Wormhole attack in WSN can be used to exploit routing communication in the network by an opponent tuning the messages received in a part of the network and replaying them in a different part. A scheme based on confidence AODV proposed to evaluate neighboring trust nodes. The schema reduces overall network delay and improves network performance in the presence of a different number of malicious nodes [1].

[2] In this short review, the security problems and physical assaults were analyzed. The approach consists in classifying and comparing physical attacks their properties such as their strategies and their effects, and finally their associated detection and defense techniques against these attacks to treat them in an independent and exhaustive manner [2].

[3] The study based on the simulation of the authors shows that flooding attacks such as flooding RREQ and hello flood greatly increase the routing overload of the protocol. Road modification attackssuch as the drain hole and the black hole are lethal and seriously affect the efficiency of the packets and reduce the flow to unacceptable ranges [3].

[4] In this research work, the routing safety problems of MANET are discussed. One type of attack, the black hole, which can be easily deployed against the MANET, is described. The percentage of packets received under the proposed method is higher than that of the AODV in the presence of a black hole cooperative attack. The solution is simulated using the global mobile simulator and is found to achieve the required security with minimal delay and overhead [4].

5 PROPOSED METHOD

Wormhole attack detection and prevention is difficult because network is infrastructure less. So here we proposed a link reliability based detection and predecessor base route establishment for wormhole prevention in MANET. In this methodology,

- Send the route request from the source.
- On receiving the route reply, the shortest path value is stored in Lx.
- Send a sample message to the selected path.
- Its acknowledgement is received with distance(Ly), the sample message travelled.
- Then the values Lx and Ly are compared.
- If the values of Lx and Ly mismatched, the link responsible for difference in values is detected.
- After the detection of wormhole, the link watcher node broadcast the wormhole node information to alert all the mobile nodes.
- Those nodes that send data packet through the attacker link, break the connection from predecessor of wormhole nodes and establish the connection from receiver node using local route repair mechanism.

This minimized the overhead of security and provides secure communication between senders to receiver nodes.

6 CONCLUSION

Wireless sensor networks are vulnerable to a wide range of security attacks because of their deployment in an open and unprotected environment. This survey paper presents the major security threats in WSN and also investigates different worm detection techniques, examining various existing methods to discover how they were implemented to detect a worm attack. It has been studied that among the number of techniques discussed, each technique has its own strengths and weaknesses and there is no proper wormhole detection technique that can completely detect all wormhole attacks. Finally, by analyzing the advantages and disadvantages of existing techniques, the challenges of open research in the wormhole detection area are explored.

References

[1] Raja Waseem Anwar, Majid Bakhtiari, AnazidaZainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi,(2015): Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks, International Conference on Smart Sensors and Application, IEEE.

[2] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H.Abdullah, and K. N. Qureshi,(2014):Security Issues and Attacks in Wireless Sensor Network, World Applied Sciences Journal, vol. 30, pp. 1224-1227,.

[3] H. Ehsan and F. A. Khan,(2012): Malicious AODV: implementation and analysis of routing attacks in MANETs, in Trust, Security and Privacy in Computing and Communications (Trust Com), 2012 IEEE 11th International Conference on,, pp. 1181-1187.

[4] M. Medadian, A. Mebadi, and E. Shahri, (2009,): Combat with Black Hole attack in AODV routing protocol," in Communications (MICC), IEEE9th Malaysia International Conference on, pp. 530-535.

[5] C. Karlof and D. Wagner, (2003): Secure routing in wireless sensor networks: Attacks and counter- measures, Ad hoc networks, vol. 1, pp. 293-315.

[6] D. B. J. D. A. Maltz and J. Broch, (2001): "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks, "Computer Science Department Carnegie Mellon University Pittsburgh, PA, pp. 15213-3891.

[7] Dhara Buch, Devesh Jinwala,(2011) Prevention of Wormhole Attack in Wireless Sensor Network, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5.

[8] Saurabh Ughade, R.K. Kapoor, Ankur Pandey, (2014.):An overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach, International Journal of Recent Development in Engineering and Technology, ISSN 2347 - 6435 (Online) Volume 2, Issue4.

[9] Gowrishankar. S, T. G .Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, (2008): Issues in Wireless Sensor Networks, Proceedings of the World Congress on Engineering 2008 Vol I WCE, London, U.K.

[10] Himani Chawla, (2014): Some issues and challenges of Wireless Sensor Networks, International Journal of Advanced Research in Computer Science and Software Engineering 4(7), pp. 236-239.

[11] Priya Maidamwar, Nekita Chavhan, (2012): A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network, International Journal on Ad-Hoc Networking Systems (IJANS) Vol. 2.