INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Wormhole Attack Detection in Wireless Sensor Networks: A Survey

Hinal Patel
S.V.I.T, Vasad, Gujarat, India
Jayna Shah
Assistant Professor, S.V.I.T, Vasad, Gujarat, India

Abstract:
Wireless sensors networks (WSNs) consist of a large number of tiny, spatially distributed, and autonomous devices, called sensor nodes. The nodes are densely deployed. The ad hoc nature of WSNs, their deployment in hostile areas, and their physical interaction with environment, make them vulnerable to several types of security attacks. One of the most important attacks in WSNs is the wormhole attack in which a malicious node receives packets from one location and tunnels them to another location in the network. Wormhole attack can be achieved with the help of several techniques such as packet encapsulation, high transmission power and high quality communication links etc. In this paper, we have surveyed various existing techniques to detect wormhole attack in wireless sensor networks.

Key words*: Wormhole, Tunneling, Security, Malicious node*

1. Introduction

Wireless Sensor Networks offer a unique way of extracting data from hazardous geographical regions where human intervention is extremely difficult, the network is often unattended, and where a specified level of security has to be maintained for each step of the network's operation. We define a sensor network as a network consisting of a set of small sensor devices that are deployed in an ad hoc fashion to cooperate with each other for sensing certain physical phenomenon. Because of the differences in the nature of the works and the constrained resources of WSNs, many solutions that are devised for traditional ad hoc networks will not work for WSNs.

Security in wireless sensor network has a great number of challenges, ranging from the nature of wireless communications, constrained resources of the sensors, unknown topologies of the deployed networks, unattended environment where sensors might be susceptible to physical attacks, dense and large networks, etc.

Section II introduces various attacks on wireless sensor networks. Section II describes description of wormhole attack. Section III describes wormhole attack taxonomy. Section IV describes various existing methods to detect wormhole attack. Finally conclusion is presented in section V.

2. Various Attacks on Wireless Sensor Networks

The various attacks on sensor node are as follows:

2.1. Jamming

Jamming interferes with the radio frequencies of the sensor nodes. Only a few jamming nodes can put a considerable amount of the nodes out of order.

2.2. Selective Forwarding

In this type of attack, an attacker forwards some packets while drop the others.

2.3. Black Hole Attack

In this type of attack, an attacker drops all the packets it has received.

2.4. Hello Flood Attacks
In many routing protocols, nodes broadcast hello messages to announce their presence to their neighbors. If the attacker also advertises a high quality route it can get every node to forward data to it.

2.5. Sybil Attack
A malicious node present multiple identities to the network is called sybil attack. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once.

2.6. Wormhole
In these attacks the adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed. Wormholes often convince distant nodes that they are neighbors, leading to quick exhaustion of their energy resources.

3. Wormhole Attack Description
A malicious node can eavesdrop or receive data packets at a point and transfer them to another malicious node, which is at another part of the network, through an out-of-band channel. The second malicious node then replays the packets. This makes all the nodes that can hear the transmissions by the second malicious node believe that the node that sent the packets to the first malicious node is their single-hop neighbour and they are receiving the packets directly from it.

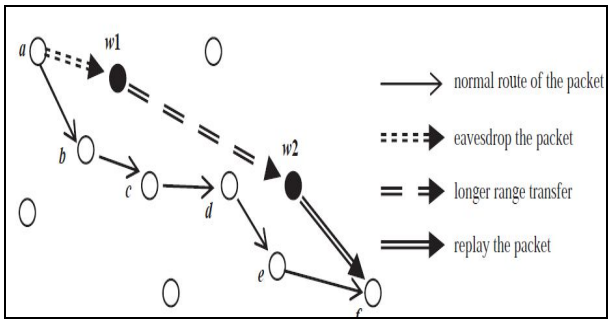

Figure 1: Wormhole Attack

For example, the packets sent by node a in Figure 1 are also received by node w1, which is a malicious node. Then node w1 forwards these packets to node w2 through a channel which is out of band for all the nodes in the network except for the adversaries. Node w2 replays the packets and node f receives them as if it was receiving them directly from node *a*. The packets that follow the normal route, i.e. *a-b-c-d-e-f*, reach node *f* later than those conveyed through the wormhole and are therefore dropped because they do more hops – wormholes are typically established through faster channels. The wormhole attack is one of the most insidious attacks, by which an attacker can severely compromise functionality with only minimal effort and external hardware. In the passive case, the attacker deploys a pair of malicious external devices with directional point-to-point antennas, which tunnel passively intercepted traffic between them over a private low-latency channel, so all messages received at one will be retransmitted at the other, and vice versa.

4. Wormhole Attack Taxonomy
Wormhole attack can be achieved with the help of several techniques such as packet encapsulation, high transmission power and high quality communication links etc.

4.1. Wormhole Using Encapsulation
Several nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Encapsulated data packets are sent between the malicious nodes, so the actual hop count does not increase during the traversal. Routing protocols that use hop count for path selection are particularly susceptible to encapsulation-based wormhole attacks.

4.2. Wormhole Using High Quality Channel
The wormhole attack is launched by having a high quality, single hop, out -of-band link (tunnel) between the malicious nodes. This tunnel can be achieved by using a direct wired link or a long range directional wireless link. This mode of attack is more difficult to launch than the packet encapsulation method since it needs specialized hardware capability.

4.3. Wormhole Using High Power Transmission Capability
Only one malicious node with high power transmission capability exists in the network and this node 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 nodes that hear the high power broadcast rebroadcasts the RREQ towards the destination.

5. Related Work

5.1. Distributed Intelligent Agent Based System

The IDS proposed in [1, 2] is based on a distributed intelligent agent-based system. The goal is to use a generalized IDS (Intrusion Detection System) framework that is lightweight enough to run on sensor nodes and will be able not only to detect that a node has been attacked, but also identify the source of the attack. When a malicious node is found, an alarm message is broadcasted to the network. Each node then makes a final decision based on the detection reports from other nodes.

5.2. Packet Leashes Approach

For the wormhole attack detection, Hu at el. [3] present a general mechanism called packet leashes based on the notions of geographical and temporal leashes. Leash is the information added into a packet to restrict its transmission distance. The geographical leash ensures that the recipient of the packet is within a certain distance from the sender. It requires nodes to be aware of their own location. Every time a node sends a packet, it appends to its header the time of transmission and the location of the sender. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance information to deduce whether the received packet passed through a wormhole or not.

The temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance. It does not require the knowledge of nodes location, but it relies on much tighter clock synchronization in the order of nanoseconds. Every time a node sends a packet, it adds to the header an authenticated timestamp. The receiving node compares this timestamp with its own reception time. Packet transmission distance is calculated as the product of signal propagation time and speed of light. If the estimated distance is too large, it indicates the presence of wormhole.

5.3. Using Directional Antenna

Hu and Evans suggested the method of directional antennas [4]. It is based on the fact that in ad hoc networks with no wormhole link, if one node sends packets in a given direction, then its neighbour will receive that packet from the opposite direction. Only when the directions are matching in pairs, the neighbouring relation is confirmed. It is obvious that each node requires a special hardware: directional antenna.

5.4. Using Digital Investigation

Digital investigation of wormhole attacks in wireless sensor networks is proposed in [5]. An observed WSN is defined to support generation and secure forwarding of evidences regarding sensor nodes behaviour in the network. A set of investigator nodes, called observers, are distributed over the network in charge of monitoring the network topology and datagram forwarding by sensor nodes.

Observer nodes and base stations form together a virtually separate WSN network called an observation network. Communication between observers and the BS may be performed using a frequency band which is not supported by sensor nodes. This is all the more important since the activity of observers should be unnoticeable by sensor nodes, and their detection sensitivity should be higher than the detection of sensor node.

5.5. Using Statistical Analysis

Detecting wormhole attacks in wireless sensor networks with statistical analysis is proposed in [6]. The proposed algorithm consists of three steps: (1) statistic analysis on routing information for wormhole detection, (2) determination of the suspicious wormhole link set and (3) wormhole validation with time constraints. It is based on the on-demand multi-path routings and uses statistical analysis and time constraints to identify the suspected links. It needs neither time synchronization among the sensors nor extra hardware such as directional antenna and GPS. Simulation experiments show that the algorithm can detect the wormhole efficiently and at a high rate of accuracy. In future author is interested in two challenges: the detection of multiple wormhole attacks and a better method for wormhole confirmation.

5.6. Using Message Travelling Time

An approach towards wormhole detection [7] requires two steps: First step is based on the algorithm that uses a hop counting technique as a probe procedure, reconstructs local maps in each node and then uses a “diameter” feature to detect abnormalities caused by the wormholes. Second step is based on round trip time (RTT) and neighbour numbers. The commutated RTT between two successive nodes and those nodes’ neighbour number which is needed to compare those values of other successive nodes. The significant feature of the propose mechanism is that it does not need any specific hardware to detect the wormhole attacks. This mechanism does not require more energy than the normal.

5.7. Multi Dimensional Scaling Visualization Based Approach

In [8], each sensor, nodes estimates the distance to its neighbor using the received signal strength. All sensor nodes send this distance information to the base station, which calculates the network’s physical topology based on individual sensor distance measurements. With no wormholes present, the network topology should be more or less flat. If wormhole attackers exist, the shape of the network layout will show some bent/distorted features and detects the wormhole by visualizing.

5.8. Radio Fingerprinting Approach

In [9], the author has presented an approach to detect wormhole attack using radio fingerprinting. The goal is the detection of device or signal characteristics that form a valid device fingerprint. First the radio signal is received by the fingerprinting device and then converted to its digital form. The signal transient is located and its features are extracted. A set of features form a fingerprint that can later be used for device identification.

5.9. Trust Based Solution

In [10], the author has presented trust based approach to detect the wormhole. Wormhole attacks can be detected using trust information among the sensor nodes. Sensor nodes can monitor the behavior of their neighboring nodes and rate them. Assuming that a wormhole drops all the packets, a wormhole in such a system should have the least trust level and can be easily eliminated. A neighboring node of a source node will have the highest trust level if all the packets sent reach the destination.

5.10. Wormhole Detection using ACK Message Transmission

In [11], all nodes sending reports wait for an ACK message. If nodes do not receive the ACK messages, the next node is wormhole link. The ACK messages must be transmitted between nodes separated by two hops, but cannot be transmitted via the path that the original report is sent on. Since the ACK messages must be sent via other path, the time to live (TTL) is important. The TTL is the maximum number of hops used to transmit the ACK messages. If the ACK messages cannot be delivered to the previous node within the TTL hop limit, a wormhole is detected.

6. Conclusion

Wormhole attack is a severe attack in wireless sensor networks. Among all possible attacks in wireless sensor networks, wormhole attack is very dangerous because it does not require any cryptographic break. We have presented many existing methods to detect the wormhole attack. Integration of time and trust based module to detect a wormhole attack is a good research issue.

7. References

1. Thanassis Giannetsos, Tassos Dimitriou, Neeli R. Prasad "State of the Art on Defenses against Wormhole Attacks in Wireless Sensor Networks" Wireless VITAE 2009: 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory & Electronic Systems Technology, pp. 313-318
2. I. Krontiris, T. Giannetsos, and T. Dimitriou, "Lidea: A distributed lightweight intrusion detection architecture for sensor networks," in SECURECOMM '08: Fourth International Conference on Security and Privacy for Communication Networks, Istanbul, Turkey, September 22- 25 2008.
3. Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks," in Proc. of IEEEINFOCOM, 2003, pp. 1976-1986, vol.3
4. L. X. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proc. IEEE Symp. Network and Distributed System, Security (NDSS 04), San Diego; February 2004.
5. Bayrem TRIKI, Slim REKHIS, and Noureddine BOUDRIGA "Digital Investigation of Wormhole Attacks in Wireless Sensor Networks" Eighth IEEE International Symposium on Network Computing and Applications, 2009, pp. 179-186
6. Zhibin Zhao; Bo Wei; Xiaomei Dong; Lan Yao; Fuxiang Gao; **"**Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis" International Conference on Information Engineering(ICIE), 2010, pp. 251-254
7. Prasannajit B, Venkatesh, Anupama S, Vindhykumari K, Subhashini S R, Vinitha G; "An approach towards Detection of Wormhole Attack in Sensor Networks" First International Conference on Integrated Intelligent Computing (ICIIC), 2010, pp. 283-289.
8. W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks" WiSe'04, Proceeding of the 2004 ACM workshop on Wireless Security , ACM Press, pp. 51-60, 2004.
9. K.B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks" Third International Conference on Security and Privacy in Communication Networks and the Workshops, pp. 331-340, Sep. 2007
10. S. Ozdemir, M. Meghdadi and I. Guler, "A time and trust based wormhole
11. Detection algorithm for wireless sensor networks" in 3rd Information Security and Cryptology Conference (ISC'08), pp. 139-142
12. Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho, A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks Scientific Research on Wireless Sensor Network, March 2013, 5, 33-40