Wormhole Molest Discovery in Wireless Sensor Networks: A Survey

[1]Rahul Amin, [2]Sunip Patel
Assistant Professor
Computer Science & Engineering, SSSRGI, Vadasma, Mehsana, India
[1]rahulnamin84@gmail.com , [2]Sunip_9984@yahoo.com

***Abstract*— Wireless sensor networks have a wide range of potential applications, including security and surveillance, control, actuation and maintenance of complex systems and fine-grain monitoring of indoor and outdoor environments. Sensor nodes have limited transmission power and limited resources. Once they are deployed, they are remotely managed. There are many security attacks possible on sensor network like Jamming. Sink hole, Selective Forwarding, Wormhole, Sybil attack etc. Among all the attacks, wormhole is very dangerous attack because the attacker does not require any cryptographic break to launch the attack. The attacker tunnels the packet from one area to another area, and disturbs the whole routing process. Traditional security algorithm can not work on sensor network because of their limited resources. So new cryptographic measures are needed.**

***Keywords*— security, wormhole, routing, sensor node, tunnel**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are multi hop relaying networks of battery-powered sensory and communication nodes, with potential applications spanning diverse areas including environmental monitoring agricultural production and industrial safety. These networks have many economic and performance advantages over human data gathering. Wireless sensor networks are differ from other ad hoc network in the sense that they are resource limited, they are prone to failure, they are deployed densely, their topology often change and they use broadcast mechanism instead of point to point mechanism

All the applications use intermediate node to send and receive data or can directly send and receive data. Sensor nodes send and receive data through wireless media and thus signals can be received by other nodes also. Broadcast nature requires that data must be sent securely so that no unauthorized node gets the data. Given that the nodes are generally assumed physically remote and unattended, there is a possibility of compromise, with attackers modifying code to adjust device functions, stealing cryptographic keys, or adding external hardware to exploit the network. For example, in a military network, this could be intended to disrupt routing by imitating a sink node or base station, so as to limit connectivity to the genuine base station and thus disguise an offensive operation. Adversary can capture the sensor nodes.

The sensor nodes have limited bandwidth and transmission power. The sensor nodes are unattended after deployment. These limitations make the sensor node more vulnerable to attacks.

The rest of this paper is organized as follows. We first discuss how attacker launch the wormhole attack in Section II, and then define wormhole attack taxonomy in Section III. In Section IV, we describe some existing methods to detect the wormhole attack in wireless sensor network. Section V includes summary of the paper and some open research issues.

II. WORMHOLE BASED ATTACK

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.

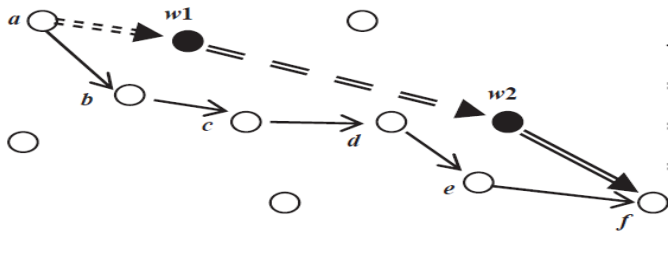

Fig. 1 Wormhole Attack

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. Wormholes are very difficult to detect and can impact on the performance of many network services such as time synchronization, localization and data fusion.

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. A wormhole may also be formed via modification of existing network devices to include this private point-to-point channel. With access to cryptographic key information and deep packet inspection, this active wormhole can obtain additional advantages by attacking network protocols, for example to drop incoming route responses or adjust metrics in forwarded packets.

When activated, key tasks for WSN nodes are to discover their communication neighbors and ultimately form multi-hop routes back to the sink node. If a wormhole succeeds in tunneling routing request messages to the base station and routing dynamics strongly reward shortest paths, then the wormhole will become a preferential link for much of the network, allowing the malicious attacker to compromise availability by dropping selected traffic or suddenly severing the wormhole link.

III. 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.

(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. For example, AODV (Ad hoc On Demand Routing Protocol) fails under encapsulation based wormhole attacks. When a malicious node at one part of the network hears the route request message (RREQ), it transmits this RREQ to the other malicious node at a distant location near the destination. The second malicious node then rebroadcasts the RREQ. The neighbors of the second malicious node then receive the RREQ and drop any further legitimate RREQs that are coming from legitimate multi-hop paths. As a result, the route between the source and the destination include the malicious nodes that form the wormhole. This prevents the sensor nodes from discovering legitimate paths that are more than two hops away.

(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.

(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 along 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.

IV. WORMHOLE ATTACK DETECTION MECHANISM

The wormhole attack problem has received considerable attentions recently. Many countermeasures have been proposed to detect wormholes in wireless ad hoc and sensor networks.

(1) Distributed Intelligent Agent Based System

In [1] 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. One can use this schema to integrate specific detection rules. This scheme is based on a distributed intelligent agent-based system [2]. An IDS agent is installed in all sensor nodes. It runs *independently* from the application, and is capable of detecting intrusions locally based on the data collected by it and by other agents in neighbouring nodes. 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. To avoid drastic flooding over the network caused by broadcasting local detection results, the alarm messages are restricted to a region formed only by the alerted nodes.

(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.

(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.

(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. A set of algorithms are proposed to aggregate the collected evidences, identify colluding nodes, and reconstruct the potential scenarios of wormholes attacks.

(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.

(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.

(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.

(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 latter be used for device identification.

(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.

V. CONCLUSIONS

Wormhole attack in wireless sensor network can disturb the routing process and ultimately degrade network performance. In this paper, we have presented existing wormhole attack types and their detection mechanism. Wormhole detection in a dynamic WSN setting is an open research area. A good research direction for wormhole detection is integration of trust based systems and time or distance bounding wormhole detection techniques.

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.

[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] S. Ozdemir, M. Meghdadi and I. Guler, "A time and trust based wormhole detection algorithm for wireless sensor networks" in 3rd Information Security and Cryptology Conference (ISC'08), pp. 139-142.