A Survey on Wormhole Attack Detection in Wireless Sensor Networks

Mayur Parmar[1] Manish Sharma[2] Prof. Rajesh Ishwar[3]

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. Sinkhole, 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 cannot work on sensor network because of their limited resources. So new cryptographic measures are needed to protect the sensor nodes. Our proposed method can easily identify real and fake neighbours.

Key words: Wireless Sensor Network, Ad-hoc on demand Distance Vector, Round Trip Time, Round Trip Delay,

I. INTRODUCTION

For example, the packets sent by node an 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.

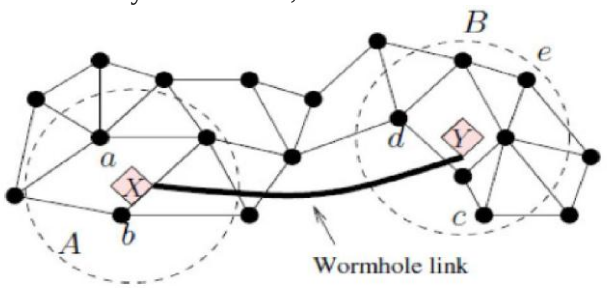

Fig.1: Wormhole Attack

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 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.

a) *Security Goals* When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services:
b) *Confidentiality:* Confidentiality refers to data in transit to be kept secret from eavesdroppers. Here symmetric key ciphers preferred for their low power consumption.
c) *Integrity:* Integrity measures that the received data is not altered in transit by an adversary.
d) *Authentication:* Authentication enables a node to ensure the identity of the peer with which it is communicating.
e) *Availability:* The service should be available all the time.
f) *Data Freshness:* It suggests that the data is recent, and it ensures that no old messages have been replayed.
g) *Non-repudiation:* It denotes that a node cannot deny sending a message it has previously sent.
h) *Authorization:* It ensures that only authorized nodes can be accessed to network services or resources. These goals are not ensured by traditional cryptographic techniques. So new cryptographic measures are needed for sensor network.

II. DETECTING IN WORMHOLE ATTACK

A. *Distributed Intelligent Agent Based System*

The IDS proposed in [1, 2] is based on a distributed intelligent agent-based system. The agents that are hosted by the nodes are capable of sharing their partial views, agree on the identity of the source and expose it. By distributing the agents throughout the network and have they collaborate, we make the system scalable and adaptive. 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. In its configuration, the system model does not include timing assumptions and is characterized by communication between 1-hop and 2-hop neighbors and the use of modern cryptography.

B. *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.

C. *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 neighbor 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. Directional antenna systems are increasingly being recognized as a powerful way for increasing the capacity and connectivity of ad hoc networks. Transmitting in particular directions results in a higher degree of spatial reuse of the shared medium. Further, directional transmission uses energy more efficiently.

D. *Using Message Travelling Time*

An approach towards wormhole detection [5] 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 neighbor numbers. The commutated RTT between two successive nodes and those nodes' neighbor 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.

E. *Multi-Dimensional Scaling Visualization Based Approach*

In [6], 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.

F. *Radio Fingerprinting Approach*

In [7], 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.

G. *Trust Based Solution*

In [8], 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 neighboring node of a source node will have the highest trust level if all the packets sent reach the destination.

III. COMPARISION

Sr.	Methods	Comments
1	Distributed Intelligent Agent Based System	RequireGPS Coordinates of every node
2	Geographical Packet Leashes	Require tightly synchronized clocks
3	Temporal Packet Leashes	Require tightly synchronized clocks.
4	Directional Antenna	Does not require any special supporting hardware
5	Message Traveling Time	Require fingerprinting device
6	Radio Fingerprinting Approach	Require fingerprinting device
7	Trust Based Solution	No hardware requirements, Effectively locate dependable routes through the network

Table. 1: Table of Comparison of different wormhole Attack Method

IV. 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.

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] 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.
[6] 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.
[7] 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
[8] 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.

