Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.29 – 33

RESEARCH ARTICLE

Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks

Nishant Sharma[1], Upinderpal Singh[2]

[1]Department of CSE, Chandigarh Engineering College, India

[2]Department of CSE, CGC College of Engineering, India

[1] nishant3742nis@gmail.com; [2] cgccoe.cse.upinder@gmail.com

Abstract— Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. These small, low-cost, low-powers, multifunctional sensor nodes can communicate in short distances. There is currently enormous research potential in the field of wireless sensor network security. The major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. Among various attacks in wireless sensor networks, In a wormhole attack, a pair of attackers forms 'tunnels' to transfer the data packets and replays them into the network. This paper provides a survey on wormhole attack and its counter measures and a proposed scheme has been described that can detect and prevent wormhole attack in wireless sensor networks.

Keywords— Wireless sensor network; Security; Low latency link; Wormhole attacks; Wireless Sensor Node

I. INTRODUCTION

Wireless sensor networks consist of a large number of tiny sensor nodes that continuously monitors environmental conditions. Sensor nodes perform various significant tasks as signal processing, computation, and network self-configuration to expand network coverage and strengthen its scalability. The sensors all together provide global scenario of the environments that offer more information than those provided by independently operating sensors. They are also responsible for sensing environment and transmission information. Wireless sensor networks are useful in various critical domains such as environment, industry, military, healthcare, security and many others. Usually the transmission task is critical as there is huge amount of data and sensors devices are restricted. As sensor devices are limited the network is exposed to variety of attacks. Traditional security mechanisms are not applicable for Wireless sensor networks as they are usually heavy and nodes are limited. Also these mechanisms do not eliminate risk of other attacks. In the next section II, an introduction about wormhole attack is given, section III describes various models of wormhole attack, section IV discusses various types of wormhole attack, section V presents various mechanisms and techniques to detect and prevent wormhole attack in wireless sensor networks, section VI describes a scheme proposed that can help detect and prevent wormhole attack and finally we conclude in section VII.

II. WORMHOLE BASED ATTACKS

In the wormhole attack, an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. An

attacker situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An attacker could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the attacker on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through if alternate routes are significantly less attractive. This will most likely always be the case when the endpoint of the wormhole is relatively far from a base station.

III. WORMHOLE ATTACK MODEL

Depending on whether the attackers are visible on the route, packet forwarding behaviour of wormhole nodes as well as their tendency to hide or show the identities, wormholes is classified into three types: closed, half open, and open. In the following cases S and D are the source and destination nodes respectively. Nodes M1 and M2 are malicious nodes.

A. Open Wormhole

Source(S) and destination (D) nodes and wormhole ends M1 and M2 are visible. Nodes A and B on the traversed path are kept hidden. In this mode, the attackers include themselves in the packet header following the route discovery procedure. Nodes in network are aware about the presence of malicious nodes on the path but they would imitate that the malicious nodes are direct neighbours.

B. Half-Open Wormhole

Malicious node M1 near the source (S) is visible, while second end M2 is set hidden. This leads to path S-M1-D for the packets sent by S for D. The attackers do not modify the content of the packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet.

C. Close Wormhole

Identities of all the intermediate nodes (M1, A, B, M2) on path from S to D are kept hidden. In this scenario both source and destination feel themselves just one-hop away from each other. Thus fake neighbours are created.

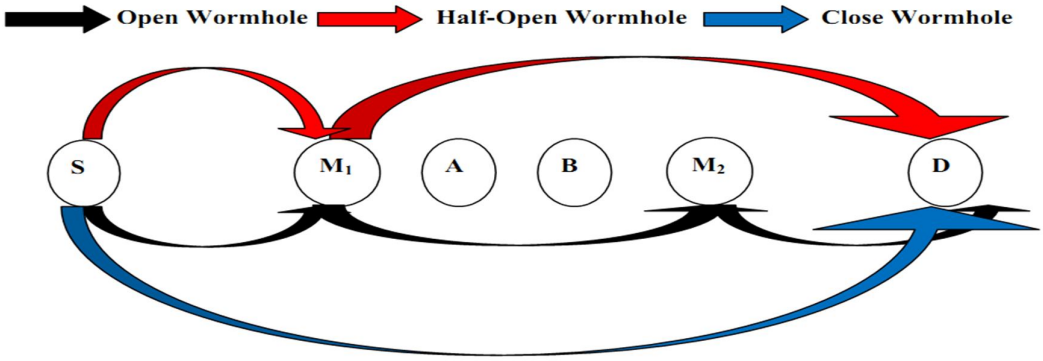

Fig. 1: Representation of Open, Half-Open and Closed Wormhole

IV. TYPES OF WORMHOLE ATTACK

Wormhole attacks can be classified based on implementation technique used for launching it and the number of nodes involved in establishing wormhole into the following types:

A. Wormhole using Packet Encapsulation

In encapsulation-based wormhole attacks, several nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Since encapsulated data packets are sent between the malicious nodes, the actual hop count does not increase during the traversal. Hence, routing protocols that use hop count for path selection are particularly susceptible to encapsulation-based wormhole attacks.

B. Wormhole Using High-quality/Out-of-band Channel

In this mode, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. This tunnel can be achieved, for example, 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.

C. Wormhole Using High-power Transmission Capability

In this type of wormhole attack, 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 an RREQ, it broadcasts the request at a high-power level. Any node that hears the high-power broadcast rebroadcasts the RREQ towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of another malicious node. This attack can be mitigated if each sensor node is able to accurately measure the received signal strength.

D. Wormhole Using Packet Relay

Packet-relay-based wormhole attacks can be launched by one or more malicious nodes. In this attack type, a malicious node relays data packets of two distant sensor nodes to convince them that they are neighbors. This kind of attack is also called "replay-based attack" in the literature.

E. Wormhole Using Protocol Distortion

In this mode of wormhole attack, one malicious node tries to attract network traffic by distorting the routing protocol. Routing protocols that are based on the 'shortest delay' instead of the 'smallest hop count' is at the risk of wormhole attacks by using protocol distortion. This kind of wormhole by itself is harmless and it is also called "rushing attack" in the literature.

V. WORMHOLE ATTACK DETECTION MECHANISMS

This section will describe the important wormhole attack detection mechanisms.

A. Location and Time based approaches

Hu et al. [4] proposed a mechanism, called packet leashes, whose goal is to limit the distance travelled by the packet in the network. They describe two approaches to achieve this goal, one is a space based approach, called as Geographical Leashes which establishes an upper bound on the distance that a packet can travel. Before sending a packet, node appends its current position and transmission time to it. On receiving packet, receiving node computes the distance with respect to the sender and the time required by 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 drawback of this scheme is that, each node must know its own location and all nodes must have loosely synchronized clocks. Because clock synchronization is resource demanding, and, thus, packet leashes have limited applicability in wireless sensor networks.

In Time based approach called as Temporal Leashes the sending node includes in the packet the time at which it sent the packet, ts ; when receiving a packet, the receiving node compares this value to the time at which it received the packet, tr. The receiver is thus able to detect if the packet traveled too far, based on the claimed transmission time and the speed of light.

Alternatively, a temporal leash can be constructed by instead including in the packet an expiration time, after which the receiver should not accept the packet; based on the allowed maximum transmission distance and the speed of light, the sender sets this expiration time in the packet as an offset from the time at which it sends the packet. The drawback of this is that they need highly synchronized clocks.

B. Message Travelling time information based method

Message travelling time information is measured in terms of round trip time (RTT). One way to prevent wormhole attack, as used by Tran et al. [5], Jane Zhen and Sampalli [6], is to measure RTT of a message and its acknowledgement. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node A to Route Reply (RREP) message receiving time from a node B. Node A will calculate the RTT between A and all its neighbours. Because the RTT between two fake neighbours is higher than between two real neighbours, node A can identify both the fake and real neighbours. In this mechanism, each node computes the RTT between itself and all its neighbours. No special hardware is required in this mechanism.

C. Hardware based method

In [7], neighboring nodes are identified by zones where each zones are defined by directional antennas. The zones around each sensor are numbered 1 to *N* clockwise starting with zone 1 facing east. When a sensor node receives a signal from a sensor node for the first time, the sensor node can get the approximate direction of the signal and identify the unknown sensor node by its zone. After that the sensor node cooperates with its neighboring nodes to verify the legitimacy of the unknown node, for example, by checking whether the unknown node is known by the neighboring nodes.

D. Multi-dimensional Scaling-Visualization-based Solutions

Multi-dimensional scaling-visualization of wormhole (MDS-VOW) is adopted in Wang and Bhargava [8] to detect wormhole attacks in WSNs. The approach is based on the observation that the network with malicious nodes has different visualization from that with normal nodes. In this method, the authors first construct the layout of the sensor nodes using MDS. Then the layout of the network can be reconstructed and visualized. In their approach, wormhole attack can be detected by visualizing the anomalies introduced by the attack. In this method, each sensor node estimates the distance to its neighbors using the received signal strength. All sensor nodes send this distance information to the base station (sink), which calculates the network's physical topology based on individual sensor distance measurements. Otherwise it requires that the distance for all node pairs can be obtained by base station (with more power and capacity). If wormhole attackers exist, the shape of the constructed network layout will show some bent/distorted features and detects the wormhole by visualizing the anomalies introduced by the attack.

With no wormholes present, the network topology should be more or less flat, while a wormhole would be seen as a 'string' pulling different ends of the network together. To compensate the distortions caused by distance measurement errors, a surface smoothing scheme is adopted. MDS-VOW then detects the wormhole by visualizing the anomalies introduced by the attack.

*E. Trust Based Method***s**

Wormhole attacks can be detected using the trust information among the sensor nodes [9]. Sensor nodes can monitor the behavior of their neighboring nodes and rate them. In trust-based systems, each source node uses its trust information to compute the most trustworthy path to a particular destination by circumventing intermediary malicious nodes. 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. Similarly, a neighboring node of a source node will have the highest trust level if all the packets sent reach the destination.

F. Hop counting method

The hop count is the minimum number of node-to-node transmissions. This method uses protocol Delay per Hop Indicator (Delphi) [10] proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to determine every available disjoint route between a source and a destination. To identify wormhole, delay time and length of each route are measured and the average delay time per hop along each route is computed. According to this, the route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both modes of wormhole attack; however, pinpoint the location of a wormhole cannot be determined.

G. Localization-based Solutions

Lazos and Poovendran [11] developed a "graph-theoretical" approach to wormhole attack prevention in WSNs. The proposed protocol is based on the use of limited location-aware guard nodes (LAGNs) which are nodes with known location and origination and can be acquired through GPS receivers. LAGNs use "local broadcast keys" that are valid only between immediate one hop neighbors. In the proposed protocol, in order to defy wormhole attackers, a message encrypted with a local key - encrypted with the pair-wise key - at one end of the network cannot be decrypted at another end. The authors propose it to use hashed messages from LAGNs to detect wormholes during the key establishment. A node can detect certain inconsistencies in messages from different LAGNs if a wormhole is present. Without a wormhole, a node should not be able to hear two LAGNs that are far from each other, and should not be able to hear the same message from one guard twice.

H. Secure Neighbor Discovery Approaches

Securely discovering one's neighbors is an effective technique for countering wormhole attacks. Khalil [12] have presented detection and isolation protocol against wormhole attacks. They present a method that can be applied for detecting each mode of the wormhole attack except the protocol deviation. Proposed algorithm has two steps. In the first step, neighboring list of each node is being built. In the second step, a collaborative detection strategy for wormholes is used, where a node monitors the traffic going in and out of its neighbors. The fundamental mechanism used is local monitoring. A sensor node monitors the traffic in and out of its neighboring nodes and uses a data structure for the first and second hop neighbors. This protocol isolates the malicious node and removes its ability to cause future damage.

I. Connectivity-based Approaches

As connectivity is not expected to change frequently in static sensor networks, making connectivity (or topology)-based approaches seems quite practical in this kind of networks. But authors in [13] show that it is impossible for these approaches to detect some wormhole attacks. In [13] and [14], the authors proposed a wormhole detection protocols that use only connectivity information in the connectivity graph. In [14], the proposed approaches are localized and do not use any special hardware or location information for attack detection. The detection algorithm looks for 'forbidden substructures' in the connectivity graph

that should not be present in a legal connectivity graph. They use unit desk graph (UDG) model that have long been used to create an idealized model of multi-hop wireless networks. They run an extra search procedure to determine a critical parameter for the detection algorithm. However, these topology-based approaches alone cannot detect all wormhole attacks in the network.

VI. PROPOSED SCHEME

The proposed scheme is able to detect and prevent wormhole attack in wireless sensor networks. It detects wormhole attack based on location information of nodes and uses Euclidean distance formula which gets the shortest distance between two nodes will improve packet forwarding and make the transmission of packets between nodes more secure and reliable. During route discovery procedure in AODV, routing table is generated at each node which describes the path with less hop counts. This is used by malicious node to attack the sender node and disrupt packet forwarding. For two nodes, with node A with coordinates (x_1, y_1) and node B with coordinates (x_2, y_2), the Euclidean distance is given by $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$. This helps in locating wormhole attack nodes by providing exact location of neighbour nodes with their x-position and y-position and the distance between them when the whole area of sensor nodes follows a grid type pattern. Thus when location information and shortest distance between them is available to the communicating node between them, it does not packets to the malicious nodes and save the packets from being accessed by the malicious attacker.

VII. CONCLUSION

In this paper, wormhole attack has been introduced and various models and types of wormhole attack has been described. Also, various wormhole detection mechanisms and various methods suggested to detect and prevent wormhole attack and mitigate its effects has been discussed. Various methods suggested have their own advantages and disadvantages. Study of these techniques helps in gaining knowledge about various research challenges in wormhole detection and in the design of a more powerful attack countermeasure and finally a proposed scheme has been described to detect and prevent the wormhole attack in Wireless sensor networks.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Commun. Mag.*, Vol. 38, pp. 102-114, 2002.

[2] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *Proceedings of the IEEE Wireless Communications*, Vol. 11, pp. 6-28, 2004.

[3] Dhara Buch and Devesh Jinwala, "Detection Of Wormhole Attacks In Wireless Sensor Network", *Proceedings of Int. Conference on Advances in Recent Technologies in Communication and Computing*, IEEE, 2011.

[4] Y. C. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", *in 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pp. 1976-1986, 2003

[5] Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee and Heejo Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks",*in 4th IEEE conference on Consumer Communications and Networking Conference*, pp. 593 - 598, 2007

[6] J. Zhen and S. Srinivas., "Preventing replay attacks for secure routing in ad hoc networks", *Proc. of 2nd Ad Hoc Networks & Wireless (ADHOCNOW'03)*, pp. 140--150, 2003.

[7] L. Hu and D. Evans. "Using directional antennas to prevent wormhole attacks," *Proceedings of Network and Distributed System Security Symposium*, pp. 131−41, Feb. 2004.

[8] W. Wang and B. Bhargava. "Visualization of wormholes in sensor networks," WiSe '04, *Proceedings of the 2004 ACM workshop on Wireless security*. ACM Press, pp. 51−60, 2004.

[9] S. Özdemir, M. Meghdadi, and Ý. Güler. "A time and trust based wormhole detection algorithm for wireless sensor networks,", *in 3rd Information Security and Cryptology Conference* (ISC'08), pp. 139−4, 2008.

[10] Hon Sun Chiu King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", *International Symposium on Wireless Pervasive Computing ISWPC* ,2006.

[11] L. Lazos and R. Poovendran, "Serloc: Secure range-independent localization for wireless sensor networks,"*Proceeding of the ACM Workshop on Wireless Security*, pp. 21−30, Oct. 2004.

[12] I. Khalil, S. Bagchi, and N.B. Shroff. "MOBIWORP: Mitigation of the wormhole attack in mobile multi-hop wireless networks," *Elsevier Ad Hoc Networks*, Vol. 6, No. 3, pp. 344−62, 2008.

[13] Y.C. Hu, A. Perrig, and D.B. Johnson. "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas of Communications*, Vol. 24, No. 2, pp. 370−80, 2006.

[14] R. Maheshwari, J. Gao, and S.R. Das. "Detecting wormhole attacks in wireless networks using connectivity information," *Proceeding of IEEE International Conference on Computer Communication*, pp. 107−15, May 2007.

