International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 6, June-2014, pp: (52-55), Impact Factor: 1.147, Available online at: www.erpublications.com

A Survey of Detection of Wormhole Attacks in Wireless Sensor Network

Priyanka Singh Dabi[1], Khushboo Tunwal[2], Rakhi Khandelwal[3], Divya Acharya[4]
[1234]M.Tech in Computer Science, GWECA, Ajmer, RTU, Kota, Rajasthan, India

Abstract: Wireless Sensor networks are employed in numerous applications which consists high range of self-organizing nodes regarding low cost and low power. Wireless sensor network are easy vulnerable to attack and compromise. There is a need of security in the network because sensor nodes are highly distributed. Wormhole attack is harmful against routing protocol which can drop data randomly or disturbing routing path which is in hidden manner or exposed. In this paper, we surveyed methods to detect and prevent the wormhole attack.

Keywords: Detection, Wormhole Attack, Wireless Sensor Network.

Introduction

Wireless sensor networks are composed of a large number of sensor nodes. These nodes communicate with each other via wireless transmission. We have several unique characteristics to distinguish wireless sensor networks from traditional wireless networks. First, WSNs generally work in unreachable areas with a large number of sensor nodes range in thousands. The resources in terms of memory, energy, communication and computation are limited, so collaborative data in collecting and processing is required to provide reliability and precision. Second, sensor nodes have simple and unreliable hardware, so they are dynamic in nature because number of nodes may expire prior to their expected lifetime. Wireless communication channel compose these networks exposed to various security attacks due to the fast deployment practices, the lack of infrastructure and the hostile deployed environments [1].

These attacks are commonly classified as active and passive attacks. A passive attack captures data without altering the data and normal functionality of the network. The active attacks are further categorized as external and internal attacks. An attack from within the network is an internal attack whereas an attack from a foreign network is an external attack. In the majority of wireless networks, an attacker can easily insert spurious (fake) packets, impersonating another sender. Packets can be recorded and replayed by attacker using eavesdropping on communication [1].

Wormhole attack is one of the severe attacks in Wireless sensor network. In this, wormhole link or tunnel is created and through this high speed link two attackers are connected. Once the link is established, the malicious node can record the data they eavesdrop, forward it to other colluding node and can replay the packets. The tunneling procedure generates an illusion that the two nodes more than one hop away are in the neighborhood of each other. So in the detection and prevention of wormhole attack we have focused on the research done by many researchers using different approaches.

The remaining sections of this paper are organized as follows. Section II consists brief introduction about wormhole attack. In section III we described related work for the detection of wormhole attack. Finally section IV concludes the paper.

Wormhole Attack

Wormhole attack is one of the Denial-of-Service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security. The wormhole attack may be launched by a single or a pair of collaborating nodes. In commonly found two ended wormhole, one end overhears the packets and forwards them through the tunnel to the other end, where the packets are replayed to local area. In case when they only forward all the packets without altering the content, they are helping the network to accomplish transmission faster. But in majority of the cases, it either drops or selectively forwards the packets, leading to the network disruption [2].

Wormhole attack does not require MAC protocol information as well as it is immune to cryptographic techniques, hence not easy to detect. A number of approaches have been proposed for handling wormhole attack. Some approaches used in the detection of wormhole attack and some for the prevention of wormhole attack in the network [2].

Majority of the techniques presented require additional hardware support, time and location based information or may be based on specific routing algorithm.

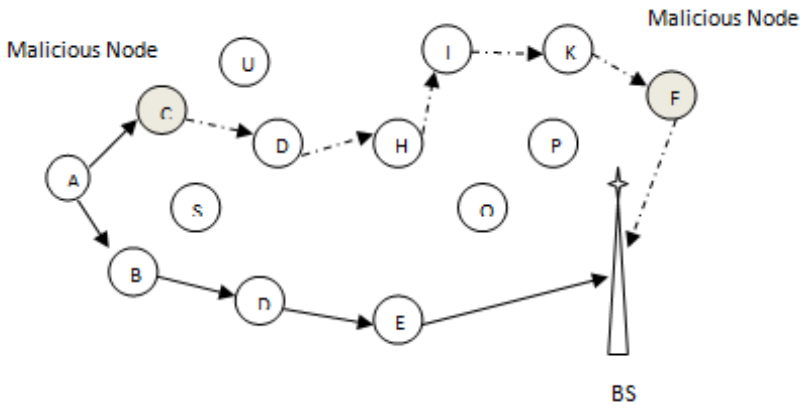

Figure 2: Wormhole Attack

A. Types of Wormhole Attack

Number of nodes involved in establishing wormhole and

the way to establish it classifies Wormhole into the following types.

1) Wormhole using Out-of-Band Channel: In this two-ended wormhole, a dedicated out-of-band high bandwidth channel is placed between end points to create a wormhole link.

2) Wormhole using Packet Encapsulation: Each packet is routed via the legitimate path only, when received by the wormhole end, gets Encapsulated to prevent nodes on way from incrementing hop counts. The packet is brought into original form by the second end point.

3) Wormhole using High Power Transmission: This kind of wormhole approach has only one malicious node with much high transmission Capability that attracts the packets to follow path passing from it.

4) Wormhole using Packet Relay: Like the previous approach, only one malicious node is required that replays packets between two far nodes and this way fake neighbor are created.

5) Wormhole using Protocol Deviation: The malicious node creates wormhole by forwarding packets without backing off unlike a legitimate node and thus, increases the possibility of wormhole path getting selected.

B. Models of Wormhole Attacks

Packet forwarding behavior of wormhole end points as well as their tendency to hide or show the identities, leads to the following three kinds of models. Here, source and destination are represented as S and D respectively. Similarly malicious nodes are represented as M1 and M2.

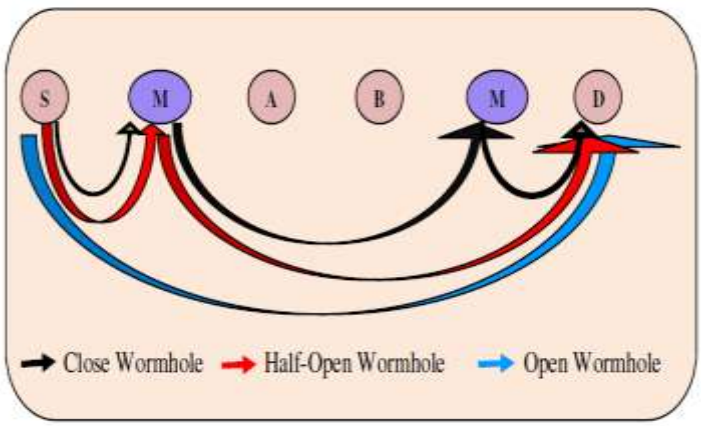

Figure 2: Open, Half-Open and Close Wormhole Attacks

1) Open Wormhole: Source and destination nodes and wormhole ends M1 and M2 are visible. Identities of nodes A and B, on the traversed path are kept hidden.

2) Half-Open Wormhole: Malicious node M1 near the source is visible, while second end M2 is set hidden. This leads to path S-M1-D for the packets sent by S for D.

3) Close Wormhole: Identities of all the intermediate nodes on path from S to D are kept hidden. So the source and destination experience only one-hop away from each other. As a consequence fake neighbors are created.

Detection of Wormhole Attack

A considerable amount of work has been done for the detection/mitigation of wormhole attacks as well as the attackers. The work ranges from proposition of extra and expensive hardware to slight modifications in the network protocols and as well as suggestion of intelligent ways of avoiding or detecting the wormholes. Though some may need extra hardware other might require extra processing and battery life. This section contains a short survey of the approaches proposed [3].

A. Location and Time based Approaches

Hu et al. proposed the used of geographical and temporal packet leashes. In this method either the geographical location (using GPS coordinates) or temporal location (using highly synchronized clocks) is used to limit the distance travelled by the packet in order to avoid the wormhole. This approach is limited by requirement of GPS technology or the time synchronization. Then they proposed connectivity based approaches, which requires connectivity information and need tightly synchronized clocks which seem impractical to achieve [4].

Capkun et al. [5] proposed a method which also needs a specialized hardware and uses end to end packet leashes. The method takes into account the speed of the transmission between the two nodes. They proposed a new protocol named SECTOR, though it doesn't requires clock synchronization though it needs accurate calculation of the distance and needs GPS coordinates of every node. MADB Protocol is used for distance calculation. GPS technology is the limitations of this method.

Baruch et al. [6] proposed the use of time of flight i.e. the round trip time to detect for wormholes. It requires hardware to be enabled to send/receive 1-bit messages without the involvement of CPU. It seems unpractical and seems to require modifications at the MAC Layer.

Khalil et al. proposed LITEWORP; an approach that uses guard nodes which keeps history of all packets. In absence of guard nodes attacks cannot be detected. Khalil et al. again proposed MOBIWORP; which uses loosely synchronized clocks, introduces the concept of centralized authority for global tracking of node positions. MOBIWORP overcome the limitations of LITEWORP [7].

Maheshwari et al. proposed the use of connectivity information among nodes. It is independent to wireless communication models. Hu and Evans proposed the use of directional antennas on all nodes, so in this approach hardware support is required. It is a good approach introduced for networks but is not applicable to other networks. Weichao et al. proposed an end-to-end mechanism, which also needs location information (i.e. GPS) and loosely synchronized clocks are used. It detects anomalies in neighbors. Eriksson et al. proposed True link which is an authentication-based, time-based mechanism. It works only with standard IEEE 802.11 hardware with some backwards compatibility firmware change. Ozdemir et al. proposed TTB, A time and trust based mechanism but it is applied on wireless sensor networks [3].

Tran et al. [8] proposed TTM (Transmission Time based Mechanism), in which all nodes in the path cooperate and attack is detected during route setup stage by computing transmission time between two nodes.

Chen et al. [9] proposed CSB, Conflicting Set Based resistant localization system, takes into account the abnormalities in the message exchanges and a secure localization approached based upon the conflicting set based resistant localization respectively.

Graaf et al. [10] proposed a distributed detection approach for the detection of wormhole attacks, taking into account the ranges of nodes.

A Vani et al. [11] proposed a solution that combines the methods of hop count, decision anomaly and neighbor list count methods for AODV protocol. The process depends upon hierarchical processing of nodes and their neighbors. They used the hop count present in the routing table of nodes, this will require that we need to store two copies of routing table of each node so that to keep track of previous hop counts.

B. Statistical Information based Approaches

Song et al. proposed a statistical analysis approach (SAM) for the detection of wormholes, which is designed for multi-path on-demand routing protocols [3].

Modirkhazeni et al. [12] proposed distributed network discovery approach to mitigate wormhole effect.

C. Graphical and Topological Information based Approaches

Wang et al. [13] proposed a procedure which visualizes the network using Multidimensional scaling (MDS), the network visualization is used for detection of attacks. It takes into account the anomalies introduced into the network by anomalous behavior. A centralized controller is used and is impressive in case of dense networks. Though they do not propose the use of new hardware, but since the algorithm is for WSNs, they do not take mobility into account.

Venkataraman et al. proposed a graph theoretic approach for the detection of wormhole attacks, which is suitable for proactive protocols [3].

Lazos et al. proposed a method in which the nodes are aware of their location which is based on the concept of guard nodes. Location Aware Guard Nodes (LAGN) uses one hop local broadcast keys for secure communication. This approach only consider WSNs, therefore mobility is not taken into account. They again proposed a method in which some nodes (guard nodes) are required to be equipped with GPS locators and directional antennas. The approach uses "local broadcast keys" for secure communication among one another [14].

Conclusion

Wormhole is the kind of attack where intruder can be successful even if the traffic between normal nodes is encrypted; as they only need to replay traffic from one point to another. Numerous approaches being proposed for the detection and isolation of wormhole nodes; each and every one tailored according to facilities/scenarios available for the proposing researchers.

Nowadays, the wormhole attack is a major problem that suffers the wireless sensor network badly. In this report, we focused over the detection and long time prevention in wireless sensor network.

The future work is to detect, isolate and prevent route disruption wormhole attack. Preventing wormhole attack solves the problem of routing the legitimate packets in the dysfunctional way.

References

[1] Bhavneet Kaur, Dr. Sandeep Singh Kang, " The Efficient Prevention of wormhole attack in AODV Routing Protocol in Wireless Sensor Networks" IJSER, Vol. 4, Issue 11, 2013.
[2] Dhara Buch, Devesh Jinwala, "Detection of Wormhole Attacks in Wireless Sensor Network" Proc. Of Int. Conf. on Advances in Recent Technologies in Communication and Computing, 2011.
[3] Zubair Ahmed Khan, M. Hasan Islam, "Wormhole Attack: A new detection technique" IEEE, 2012.
[4] Hu, Y. C.; Perrig, A.; and Johnson, D. B.; , "Wormhole attacks in wireless networks" IEEE Journal on Selected Areas of Communications, Vol. 24, no. 2, pp. 370-80, 2006.
[5] Srdjan Capkun, Jean-Pierre Hubaux, and Levente Buttyan, "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks" Proc. of the 1st ACM workshop on Security of ad hoc and sensor net. , Fairfax, Virginia, October 31, 2003.
[6] Baruch, A.; Curmola, R.; Nita, C.;- Rotaru, Holmer, D.; and Rubens, H.; , "On the survivability of routing protocols in ad-hoc wireless networks" 1st International Conf. on Security and Privacy for Emerging Areas Communications, pp. 327-38, 2005.
[7] Khalil, I.; Saurabh Bagchi, and Shroff, N. B.; , "MOBIWORP: Mitigation of the wormhole attack in mobile multi-hop wireless networks" Elsevier Ad Hoc Networks, Vol. 6, no. 3, pp. 344-62, 2008.
[8] Tran, P. V.; Hung, L. X.; Lee, Y. K.; Lee, S.; and Lee, H.; , "TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks" 4th IEEE Conf. (CCNC-07), pp. 593-8, May 2007.
[9] Honglong Chen, Xice Sun, Zhi Wang, and Wei Lou, "A secure localization approach against wormhole attacks using distance consistency" EURASIP Journal on Wireless Communications and Networking, p.1-11, April 2010.
[10] R. Graaf, J. Horton, R. Safavi-Naini, and I. Hegazy, "Distributed Detection of Wormhole Attacks in WSN" Ad Hoc Networks in Springer book, vol. 28, pp. 208-22, 2010.
[11] A.Vani, D. Sreenivasa Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks" IJCSE, Vol. 3, No. 6, pp. 2377-2384, June 2011.
[12] A. Modirkhazeni, S. Aghamahmoodi, A. Modirkhazeni, and N. Niknejad, "Distributed approach to mitigate wormhole attack in WSN" 7th International Conf., pp. 122-128, 26-28 Sept. 2011.
[13] Weichao Wang , Bharat Bhargava, "Visualization of wormholes in sensor networks" Proc. of the 3rd ACM workshop on Wireless Security, Philadelphia, PA, USA, October 2004.
[14] Lazos, L.; Meadows, C.; Poovendran, R.; Syverson, P.; and Chang, L. W.; , "Preventing Wormhole Attacks on Wireless Adhoc Networks: A Graph Theoretic Approach" IEEE Conf., vol. 2, pp. 1193-1199, March 2005.