SECURE NODE LOCALIZATION IN WIRELESS SENSOR NETWORK: A REVIEW

Simarjeet Kaur[1] , Navdeep Kaur [2], Kamaljit Singh[3]
[1]Research Scholar, Deptt of CSE, [2]Associate Professor & Head, Deptt of CSE, [3]Assistant Professor, Deptt of ECE, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India
er.simarjeet@yahoo.in, drnavdeep.sggswu@gmail.com, kamalbhatia.er@gmail.com

ABSTRACT - Wireless Sensor Network (WSN) has achieved researcher's interest worldwide in the last decade. For some applications like environmental monitoring, health monitoring, tracking applications etc., position of node plays a vital role. As wireless sensor networks are deployed in hostile and unattended environment, nodes are prone to various types of attacks like Sybil attack, black hole attack, wormhole attack etc. So security is a main concern in wireless sensor network. Therefore secure localization of nodes is an active area of research. This paper surveys different schemes that have been proposed to find the location of a node securely.

Keywords – wireless sensor network, security, localization

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of hundreds or thousands of sensor nodes which are deployed randomly in harsh environments to monitor physical or environmental conditions. Sensor nodes sense the data and transmit it to the destination nodes. The destination node sends the data to the base station which is connected to the outside world where the data can be collected, processed and analyzed [13]. There are two main components of wireless sensor networks: Sensor Nodes and Base Station (Gateway). A sensor node consists of one or more sensors and a mote. A sensor is a device which senses the information and passes it to mote. A mote consist of processor, memory, battery, Analog to Digital converter for connecting to a sensor and a radio transceiver for forming an adhoc network [13]. A base station links the sensor network to another network [13]. It is also known as sink or gateway. Positioning of Base Station is a very important issue in wireless sensor network as all sensor nodes send their data to base station for further processing and decision making.

Wireless Sensor Networks have been applied in different fields to monitor and sense the environmental conditions owing to the low cost, large scale, densely distributed deployment and self configuration [11]. The sensed data is meaningless without sensor node's location information in many of wireless sensor network applications like environment monitoring, target tracking, traffic monitoring etc. So node must find their location in the network [6]. In these applications gathered information is based on the correct location of the sensor nodes. In addition to these applications, there are also some network operations which require the location of sensor nodes like geographical routing, location aware routing etc [12].

Localization is the process of finding the accurate physical location of a sensor node. Sensor nodes are randomly deployed by an airplane in the area of interest say forest. The most popular technique to find the node's location is Global Positioning System (GPS). When the network contains large number of nodes, this method becomes very costly and energy consuming. So it is difficult to install in every node. A compromised solution is to install GPS receivers in some of the sensor nodes and the rest of nodes could obtain their locations through some localization method. The nodes which are aware of their location are called anchor/beacon nodes. The nodes which use anchor nodes to find their location are called unknown nodes [4].

When Wireless Sensor Networks are deployed in harsh and untrusted environments, sensor nodes are vulnerable to different types of threats and attacks such as sybil attack, wormhole attack, black hole attack etc. so nodes are unable to find their exact location. Specifically for some applications e.g., military applications like battlefield surveillance or environmental applications like forest fire detection, incorrect positions may lead to severe consequences [2]. Therefore secure node localization is an active area of research.

There are two main categories of localization algorithms [5]:

i) Range Based Algorithm
ii) Range Free Algorithm

Range based methods require ranging information (distance or angle) for calculating the coordinates of unknown node. These methods have high localization accuracy but they require more hardware resources.

ISSN: 2229-6913 (Print), ISSN: 2320-0332 (Online)

Range free methods are cost effective alternative that do not require any expensive hardware. These methods estimate the distance between an anchor node and an unknown node by the connectivity information or multihop routing information.

Wireless Sensor Networks are quite different from general wireless networks due to various constraints and highly specific nature of WSNs [13]. Therefore WSNs create many research challenges. Secure localization of sensor is an active area of research in Wireless Sensor Networks.

The remainder of paper is organized as follows: Section II states problem statement. Section III describes schemes for range based and range free secure localization. Section IV provides the conclusion.

II. ATTACKS ON NODES

Localization process can be attacked in many ways.Following are the main types of attacks on the sensor nodes:

Blackhole Attack: In a black hole attack, the attacker drops all or some of the packets received from other nodes in the network. In order to remain ignored, the malicious node keeps sending self generated packets [14].

Wormhole Attack: In a wormhole attack, an attacker receives a packet at one point in the network. Then it tunnels the packet to another location and replays it. This causes the nodes placed in different parts of the network to believe that they are neighbouring nodes[10].

Sybil Attack: Sybil attack is initiated by a malicious node which has virtually multiple identities (IDs). A Sybil node can send message with different IDs [6].

III. PROBLEM STATEMENT

The wireless sensor network is the self configuring type of network in which various sensor nodes are deployed to sense the environmental conditions like temperature, pressure etc. The size of the sensor nodes are very small and generally deployed on the far places due to which it is difficult to replace or recharge battery of sensor nodes. There are many applications of WSNs which are based on the location of the sensor node like target tracking, traffic monitoring etc. In these applications gathered information is based on the correct location of the sensor nodes. The various techniques had been proposed in the literature to find the location of the nodes. These techniques works well when there is no malicious node exists in the network. The performance of these proposed techniques degrades when some malicious nodes exists in the network which are responsible to trigger various types of attacks in the network. So it becomes necessary to develop secure node localization algorithms.

IV. RANGE BASED & RANGE FREE SCHEMES

In this section, survey of various secure localization techniques has been carried out. The following studies have been carried out on the basis of range based classification.

Capkun and Hubaux [15] discussed the issue of positioning in wireless networks in adversarial situation. They suggested a mechanism called Verifiable Multilateration (VM) for position verification. Anchor nodes are called verifiers. This method facilitate secure estimation and confirmation of position of unknown node in the presence of malicious nodes. They have further devised a system for **S**ecure **P**ositioning **I**n sensor **Ne**tworks called SPINE. By using this method nodes are able to locate themselves securely. The limitation of this method is that large number of verifiers are needed to perform verifiable multilateration.

Zhang et al. [18] developed a secure localization scheme called SLS (Secure Localization Scheme) for ultra wide band sensor networks. SLS is more robust than VM but the procedure of SLS is more sophisticated than that of VM and leads to more energy consumption.

Capkun et al. [16] proposed a novel approach to find the location of node in a secure way using the concept of hidden and mobile base station. Moreover by using this method, one can also verify the location of unknown nodes.

He et al. [1] highlighted the need for secure localization and suggested an extension to the existing scheme SLS. The new scheme is called ESLS (Enhanced Secure Localization Scheme). This scheme is tolerant not only against distance reduction attacks but also from distance enlargement attacks and provides more exact location of the nodes.

The following studies have been carried out on the basis of range free classification.

Lazos and Poovendran [7] were the first researchers who proposed a secure range independent localization scheme. They addressed the issue of secure localization in Wireless Sensor Network. The authors proposed a range free localization algorithm SeRLoc that withstand against WSN attacks such as Worm hole, Sybil attack etc. SeRLoc is a distributed algorithm that provides accurate and reliable position information even when there is high possibility of attack. It does not involve any kind of communication among sensors. The simulation results showed that

SeRLoc localizes sensor nodes with higher accuracy, while requiring less reference points and lower communication cost. This algorithm requires extra hardware (sectored antennas) in beacon nodes. It provides no security against attacks on locator's information.

Lazos et al. [9] studied the problem of both location determination and location verification. They proposed an algorithm called Robust Position Estimation (ROPE) that finds the location of sensor node and also verify sensor node's location claim even in the presence of malicious nodes. They introduced a new parameter called Maximum Spoofing Impact (MSI) for calculating the effect of attacks. ROPE is robust against several attacks such as wormhole attack, node impersonation and jamming of transmission. It requires extra hardware (directional antennas) which is inappropriate for low cost WSN.

Lazos and Poovendran [8] proposed a high-resolution range-independent localization scheme called HiRLoc. It achieves high localization accuracy than previously proposed methods by using less hardware resources and without increasing the number of reference points. The scheme is also tolerant against severe security threats in WSN, such as the wormhole attack, the Sybil attack and compromise of network entities. But this scheme increases computational and communication complexity.

Zeng et al. [17] discussed hop count based localization (multihop) and developed a secure hop count based localization scheme called SHOLOC. This is the first secure localization algorithm considering multihop situation. The scheme is resistant to attacks like hop count reduction attack and forging attacks.
Chen et al. [2] investigated the effects of wormhole attack on DV hop based localization scheme in Wireless Sensor Network. To resolve this problem they proposed label based secure localization scheme that expose and oppose wormhole attack by removing the packets delivered through wormhole link. This scheme works efficiently when there is no packet loss in the network and all nodes have same transmission ranges.

V. CONCLUSION

In order to handle security issues in wireless sensor network, various methods have been proposed. This paper focuses on the need of secure node localization and discusses various schemes proposed in the literature. The future research direction of localization schemes possibly is to develop a more secure and robust scheme that can withstand against attacks like wormhole, Sybil and black hole. This approach must also compute location in less time and consumes less energy so that lifetime of the network is prolonged.

REFERENCES

[1] D. He, L. Cui, and H. Huang, "Design and verification of enhanced secure localization scheme in wireless sensor networks," in IEEE transactions on Parallel and Distributed Systems, vol. 20, no.7, 2009, pp.1050-1058.

[2] H. Chen, W. Lou, Z. Wang, J. Wu and Z. Wang, A. Xia, "Securing DV-hop localization against wormhole attacks in wireless sensor networks," in Pervasive and Mobile Computing, Elsevier, 2014, pp. 1-14.

[3] J. Jiang, G. Han, C. Zhu, Y. Dong, N. Zhang, "Secure localization in Wireless Sensor Networks: A Survey," in Journal of Communications, Academy Publisher, vol 6(6), 2011, pp. 460-470.

[4] J. Kuriakose, C. Kuriakose, Amruth V, M. B. Dalsania, M. T. B. Lahori, and S. K. J., "Confiscation of Malicious Anchor Nodes in Wireless Sensor Networks," in Int. J. of Recent Trends in Engineering & Technology, ACEEE, vol. 11, June 2014, pp. 255-266.

[5] J. Kuriakose, S. Joshi, R. V. Raju, and A. Kilaru, "A Review on Localization in Wireless Sensor Networks," in Advances in Signal Processing and Intelligent Recognition Systems, Springer, 2014, pp. 599-610.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in Proceedings of the Third International Symposium on Information Processing in Sensor Networks, April 2004, pp. 259–268.

[7] L. Lazos and R. Poovendran, "SeRLoc: Secure range independent localization for wireless sensor networks," in Proceedings of the 3rd ACM Workshop on Wireless Security, USA, 2004, pp. 21–30.

[8] L. Lazos and R. Poovendran, "HiRLoc: High-resolution robust localization for wireless sensor networks," in IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, 2006, pp. 233 – 246.

[9] L. Lazos, R. Poovendran and S. Capkun, "ROPE: robust position estimation in wireless sensor networks," in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, USA, 2005, pp. 324–331.

[10] M. Jain and H. Kandwal, “A survey on complex wormhole attack in wireless ad hoc networks,” in Proceedings of International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp. 555-558.

[11] N. Bulusu, J. Heidemann, D. Estrin, “GPS-less Low Cost Outdoor Localization for very small devices,” in Personal Communications, IEEE, vol 7(5), 2000 pp. 28-34.

[12] P. Gour and A. Sarje, “Localization in Wireless Sensor Network with ranging error,” in Intelligent Distributed Computing, Springer, 2015, pp. 55-69.

[13] R. K. Tripathi, “Base Station Positioning, Node’s Localization and Clustering Algorithms for Wireless Sensor Networks,” Ph.D. dissertation, Indian Institute of Technology, Kanpur, India, 2012.

[14] S. A. V. Satya Murty, P.G. Namboothiri and K. M. Sivalingam, Y. Xiao, H. Chen, and F. Haizhon Li, “Security Trends and Challenges in Wireless Sensor Network” in Handbook on Sensor Networks, 2010, pp. 357-397.

[15] S. Capkun and J. Hubaux, “Secure positioning in wireless network,” in Journal on Selected Areas in Communications, IEEE, vol. 24, no. 2, 2006, pp. 221–232.

[16] S. Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, “Secure location verification with hidden and mobile base stations,” in IEEE Transactions on Mobile Computing, vol. 7, no. 4, 2008, pp. 470–483.

[17] Y. Zeng, S. Zhang, S. Guo, and L. Xie, “Secure hop-count based localization in wireless sensor networks,” in International Conference on Computational Intelligence and Security, IEEE, Harbin , 2007, pp. 907–911.

[18] Y. Zhang, W. Liu, Y. Fang, and D. Wu, “Secure localization and authentication in ultra-wideband sensor networks,” in IEEE Journal on Selected Areas in Communication, vol. 24, no. 4, 2006, pp. 829–835.