International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 02 (March- April, 2018)

A Survey on Localization in Wireless Sensor Networks

Somkumar Varema[1], Prof. Dharmendra Kumar Singh[2]
Department of EC, SVCST, Bhopal, India
[1]verma.sonkumar4@gmail.com, [2]singhdharmendra04@gmail.com

Abstract-Wireless sensor networks (WSNs) have gained researchers' attention in the last several years. Small sensors powered by miniaturized microprocessors are capable of supporting several applications for civil and military domains. Determining the location of sensors is a basic and essential knowledge for most WSN algorithms and protocols including data tagging, routing, node identification, among others. This paper surveys the different algorithms that have been proposed to securely determine the location of a sensor node. By secure, we mean that adversaries cannot easily affect the accuracy of the localized sensors. In other words, the localization algorithm must be robust under several attacks. We provide taxonomy for classifying different secure localization schemes and describe possible attacks that can harm localization. In addition, we survey different secure localization schemes and show how they map to the proposed taxonomy. We also give a comparison between the different schemes, showing the attacks addressed by each.

I. Introduction

In a matter of just few years, WSNs have gained attention from researchers in deferent fields. A WSN consists of a large number of small sensors cooperating to achieve one goal. This helps leveraging several military and civil applications. Since these micro-sensors have limited power and computation, we need special algorithms with low power consumption. WSNs are usually deployed in harsh environments (e.g. Battle fields) and are operating unattended. This makes them more vulnerable to adversary attacks. Knowing a sensor's location is essential for many sensor network applications including surveillance networks and habitat monitoring. Equipping each sensor with a GPS device is too expensive because the number of sensors in a WSN is usually in the order of thousands there are several localization schemes [1] that allow sensors to determine their physical locations in absence of special hardware. Many localization schemes (anchor-based) assume that some special sensors (anchors) know their true physical locations. Other sensors determine an approximate relative location to anchors based on some measurements. However, there are some other schemes (anchor-free) in which there are no anchor nodes. In these schemes, sensors locations are calculated according to some virtual coordinates. We expect that an adversary will try to prevent localization algorithms from working correctly. An adversary may inject malicious data into the network in order to displace sensor nodes. This means that when sensors estimate their locations, a displaced location is calculated. In this paper we survey different algorithms that can fall under such adversary attacks and still get a good estimate of sensors' locations [2].

II. Localization Problem in WSN

Before discussing secure localization problems, it is essential to take a look at some general concepts used in the localization process. Basically, there are two categories of sensor nodes: unknown and anchor nodes. Unknown nodes in the network have no knowledge of their positions and no special hardware to acquire the positions. Anchor nodes, also called beacon nodes, in fact, their positions are obtained by manual placement or additional equipments such as GPS (Global Positioning System). Therefore, unknown nodes can use localization information of anchor nodes to localize themselves. Usually, the localization process can be divided into two steps: 1) information acquisition and 2) position determination.

A. Information acquisition

Roughly speaking, existing localization schemes of WSNs are classified into two categories: range-based schemes [3], [4] and range-free schemes [5], [6]. For range-based localization schemes, the distance or angle information is measured by RSSI (Received Signal Strength Indicator) [7], TOA (Time of Arrival) [8], Time Difference on Arrival (TDOA) [9] and AOA (Angle of Arrival) [10]. For range-free localization schemes, the localization is realized based on network connectivity or other information, which can be obtained by DV-Hop [11], Convex Optimization [12] and MDS-MAP [13].

B. Position determination

Location determination schemes have two categories: 1) terminal-based schemes and 2) infrastructure-based schemes [16]. In terminal-based schemes, the unknown node localizes itself after connecting available information about distances/angles and positions of anchor nodes, the position of an unknown node can simply be computed by trilateration [15], multilateration [17], and triangulation [14]. In infrastructure-based schemes, reference nodes including trusted neighbor nodes, mainly anchor nodes to localize the unknown node. Adversaries can attack localization in both two steps. The goal of the adversary is to make the unknown nodes obtain false positions,

by compromising normal nodes to send false localization information, or pretend to be a legitimate node to forge, modify or replay signals. Thus, security measures are needed to make the estimated positions still correct under attacks.

III.RELATED WORK

Guangyuan Wang in 2017. We propose a novel game based secure localization algorithm for WSNs.They think that the game theory is a powerful approach to make decision under conditions of uncertainty and interdependence. In the paper, they transform the secure localization problem in hostile environments into a game problem. The main research objective is to prevent the malicious reference information and seek an optimized solution [18].

In 2015, Sayyed Majid Mazinani and Mosayeb Safari presented a method discovering the Malicious Anchor Nodes, at first, the anchor nodes (Ai) want other anchor nodes to send their coordinates by sending a message to all nodes on the network. The nodes of Ai obtain their distance from other anchor nodes by using the measurement techniques such as RSSI and compensate this distance with the Euclidean distance of anchor nodes. If this distance is more than Euclidean distance (emax), the anchor nodes was considered malicious, otherwise it will be detected as a benign node. Each node repeats the same strategy for all anchor nodes in the networks and reports their results to base station. After this step, a table was constructed in the base station. Every anchor nodes add a row to this table by starting the calculation of enemy detections. Malicious nodes report the benign nodes as malicious nodes and the malicious nodes as benign nodes. It should be noted as number of malicious nodes that are less than number of benign nodes, the row that the law was not established, should be considered as malicious nodes. For more accuracy in calculations and obtain reliable values for the nodes, which detected benign from this scheme, the following procedure is proposed. The sensor nodes that have 2 or more anchor nodes at the distance of 2**R*, establish the following calculation between every 2 anchor nodes. Details are shown in figure. The sensor node asked the anchor nodes of *A*1and *A*2 to send their coordinates with a message. The anchor nodes send their coordinates to sensor node. So, the sensor nodes obtain the coordinates of 2 anchor nodes and also detect the distance and the angle of them. This data can easily be obtained from the common techniques such as RSSI or AOA [19].

In Parvathy Menon, Associate Prof. Deepa S Kumar and Prof. M Abdul Rahiman gave a method in 2015.A Trust based Position Identification is performed. First phase is location estimation in which the sensor node broadcast its ID to locators which comes in sensor-to locator communication range and those locators perform distance bounding with sensor nodes. Then for every locator trust evaluation value is estimated by sensor node. Trust based Position Identification algorithm contains two phases. First phase is location estimation in which the sensor node broadcast its ID to locators which comes in sensor-to locator communication range and those locators perform distance bounding with sensor nodes. Then for every locator of set LDBs [4], trust evaluation value is estimated by sensor node. If the trust evaluation value is greater than or equal to threshold then it is included within set LTs. If the number of locators within set LTs is greater than or equal to 3 and any 3 locators of set LTs forms an triangle around sensor, then location of sensor node is estimated through Verifiable Trilateration[4]. Otherwise localization fails [20]. Second phase is location verification in which location claim of sensor node is verified by locator through distance bounding.

M. B. Nirmala and A. S. Manjunatha present an enhanced voting based localization scheme in 2015 which includes voting based method, security scheme for authentication and confidentiality, trilateration and bilateration for finding the absolute or relative position estimation of sensor nodes. Section A explains the voting method, section B gives the security scheme, and Section C explains trilateration process [21]. Bilateration process is explained in section D and section E gives the Algorithm for enhanced voting based secure localization scheme and explains the steps involved.

Aashish Singhal and Parul Bansal gave new method called High-Resolution Robust Localization (HiRLoc). In this method, they address the problem of robustly estimating the position of randomly deployed nodes of a wireless sensor network (WSN), in the presence of security threats. They propose a range-independent localization algorithm called high-resolution range independent localization (HiRLoc), that allows sensors to passively determine their location with high resolution, without increasing the number of reference points, or the complexity of the hardware of each reference point. In HiRLoc, sensors determine their location based on the intersection of the areas covered by the beacons transmitted by multiple reference points. By combining the communication range constraints imposed by the physical medium with computationally efficient cryptographic primitives that secure the beacon transmissions, they show that HiRLoc is robust against known attacks on WSN, such as the wormhole attack, the Sybil attack, and

compromise of network entities. Finally, our performance evaluation shows that HiRLoc leads to a significant improvement in localization accuracy compared with state-of-the-art range independent localization schemes, while requiring fewer reference points. It permits sensors to find out their location with high precision even if there are some security threats [22].

Zohreh Sobhanifar and Abolfazl Toroghi Haghighat proposed a new algorithm to find and isolate the nodes which lies about their position in a Wireless Sensor Network (WSN). Also the proposed method enables the sensor nodes to find their location in presence of liar nodes. In the proposed method, a given number of neighbors for all sensors are determined where the number of liars is below a predefined threshold value. The proposed method is evaluated in finding the liars and also the correct location of each node. The minimum error rate on the determination of liars and the location of sensors proves the ability of the algorithm for localization of sensors in the WSNs [23].

S. No.	Title of paper	Author	publication	Remark
1	A Novel Game based Secure Localization Algorithm for Wireless Sensor Networks	Guangyuan Wang, Yongji Ren and Xiaofeng Xu	International Journal of Future Generation Communication and Networking, Vol.10, No.7 (2017).	Author transform the secure localization problem in hostile environments into a game problem[18]
2	Secure Localization Approach in Wireless Sensor Network	Sayyed Majid Mazinani and Mosayeb Safari	International Journal of Machine Learning and Computing, Vol. 5, No. 6, December 2015	distance is more than Euclidean distance (emax), the anchor nodes was considered malicious, otherwise it will be detected as a benign node[19]
3	Security in Wireless Sensor Networks using Trust Based Distance Bounding	Parvathy Menon, Associate Prof. Deepa S Kumar, Prof. M Abdul Rahiman,	IJECS Volume 4 Issue 5 May, 2015	A Trust based Position Identification[20]
4	Enhanced Voting based Secure Localization for Wireless Sensor Networks	M. B. Nirmala, A. S. Manjunatha	I. J. Computer Network and Information Security (ijcnis.2015.12.06) 2015.	Voting based Secure Localization[21]
5	"Secure Localization In Wireless Sensor Networks",	Aashish Singhal, Parul Bansal, Mr. DIWAKER MOURYA,	3rd International Conference on System Modeling & Advancement in Research Trends (SMART), College of Computing Sciences and Information Technology (CCSIT) ,Teerthanker Mahaveer University ,	High-Resolution Robust Localization (HiRLoc)[22]

			Moradabad,2014	
6	,"A NEW SECURE LOCALIZATION APPROACH OF WIRELESS SENSOR NODES INTHE PRESENCE OF MISBEHAVING ANCHOR NODES",	Zohreh Sobhanifar and Abolfazl Toroghi Haghighat	International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol. 4, No.3, June 2014	Algorithm to find and isolate the nodes which lies about their position in a Wireless Sensor Network[23] (WSN)

VI. CONCLUSION

In this survey paper, we've illustrated the importance of securing the localization method in wireless detector networks. We have a tendency to given taxonomy of the different options which will be wont to classify secure localization schemes for wireless detector networks. The taxonomy will be applied to guage the characteristics of a location system required by a specific application or the suitableness of Associate in Nursing existing location system for its application. Further, attacks against localization schemes in WSNs were explained. Then, secure localization schemes appropriate (or doubtless suitable) for detector networks square measure mentioned, mentioning the attacks every of them targets.

REFERENCES

[1] Adel Youssef and Moustafa Youssef. Taxonomy of Localization Schemes for Wireless Sensor Networks. In ICWN, pages 444{450, 2007.

[2] Ananth Rao, Sylvia Ratnasamy, Christos Papadimitriou, Scott Shenker, and Ion Stoica. Geographic routing without location information. In MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking, pages 96{108, New York, NY, USA, 2003. ACM.

[3] S. Zhu and Z. Ding, "A simple approach of range-based positioning with low computational complexity," IEEE Transactions on Wireless Communications, vol. 8, no. 12, December 2009.

[4] M. Heidari, N. Alsindi, and K. Pahlavan, "Udp identification and error mitigation into a-based indoor localization systems using neural network architecture," IEEE Transactions on Wireless Communications, vol. 8, no. 7, July 2009.

[5] S. Lee, E. Kim, C. Kim, and K. Kim, "Localization with a mobile beacon based on geometric constraints in wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 8, no. 7, pp. 5801–5805, December 2009.

[6] H. Chen, Q. Shi, H. Vincent Poor, and K. Sezaki, "Mobile element assisted cooperative localization for wireless sensor networks with obstacles," IEEE Transactions on Wireless Communications, vol. 9, no. 3, March 2010.

[7] P. Bahl and V. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System," in Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 21, 2000, pp. 755–784.

[8] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The anatomy of a context-aware application," in Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, 1999,
pp. 59–68.

[9] L. Girod and D. Estrin, "Robust range estimation using acoustic and multimodal sensing," in Proceedings of the
IEEE/RSJ International Conference on Intelligent Robots and Systems, 2001, pp. 1312–1320.

[10] D. Niculescu and B. Nath, "Ad hoc positioning system (APS) using AoA," in Proceedings of the Twenty-Second
Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, April 2003, pp. 1734–1743.

[11] "Ad hoc positioning system (APS)," in Proceedings of the 2001 IEEE Global Telecommunications Conference of the IEEE Communications Society, vol. 5, 2001, pp. 2926–2931.

[12] L. Doherty, K. Pister, and L. Ghaoui, "Convex position estimation in wireless sensor networks," in Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, 2001, pp. 1655– 1663.

[13] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz, "Localization from mere connectivity," in Proceedings of the 4th International ACM Symposium on Mobile Ad Hoc Networking & Computing, 2003, pp. 201–212.

[14] D. Niculescu and B. Nath, "Ad hoc positioning system (APS) using AoA," in Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, April 2003, pp. 1734–1743.

[15 "Ad hoc positioning system (APS)," in Proceedings of the 2001 IEEE Global Telecommunications Conference of the IEEE Communications Society, vol. 5, 2001, pp. 2926–2931.

[16] A. Ferreres, B. Alvarez, and A. Garnacho, "Guaranteeing the authenticity of location information,"

IEEE Pervasive Computing, vol. 7, no. 3, pp. 72–80, July 2008.
[17] A. Savvides, C.-C. Han, and M. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in Proceedings of the 7th annual international conference on Mobile computing and networking, 2001, pp. 166–179 .
[18]Guangyuan Wang, Yongji Ren and Xiaofeng Xu ," A Novel Game based Secure Localization Algorithm for Wireless Sensor Networks", International Journal of Future Generation Communication and Networking,Vol.10, No.7 (2017).
[19]Sayyed Majid Mazinani and Mosayeb Safari," Secure Localization Approach in Wireless Sensor Network", International Journal of Machine Learning and Computing, Vol. 5, No. 6, December 2015
[20]Parvathy Menon, Associate Prof. Deepa S Kumar, Prof. M Abdul Rahiman," Security in Wireless Sensor Networks using Trust Based Distance Bounding", IJECS Volume 4 Issue 5 May, 2015.
[21] M. B. Nirmala, A. S. Manjunatha," Enhanced Voting based Secure Localization for Wireless Sensor Networks", I. J. Computer Network and Information Security(ijcnis.2015.12.06) 2015.
[22]Aashish Singhal, Parul Bansal, Mr. Diwaker Mourya, "Secure Localization In Wireless Sensor Networks", 3rd International Conference on System Modeling & Advancement in Research Trends (SMART), College of Computing Sciences and Information Technology (CCSIT) ,Teerthanker Mahaveer University , Moradabad,2014
[23]Zohreh Sobhanifar and Abolfazl Toroghi Haghighat,"A New Secure Localization Approach Of Wireless Sensor Nodes In the Presence Of Misbehaving Anchor Nodes", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol. 4, No.3, June 2014.