Research on Wireless Sensor Networks Security Localization Algorithm

Zhihao Zhang, Wenju Liu

Abstract— **The application of wireless sensor networks (WSN) is promising. As one of its core technologies, positioning technology has also developed rapidly. However, the nodes of wireless sensor networks have various limitations, and there are many risks in security, which has become a research hotspot. Attacks on the positioning process and positioning algorithms are undoubtedly a major challenge in the development of positioning technology. In this paper, we introduce several existing security location technologies, common location attack algorithms, and detection methods. And, it is analyzed and compared in detail. Finally, we summarize and look forward to future research hotspots and trends.**

Index Terms—**wireless sensor network (WSN), positioning; security, positioning attack method**

I. INTRODUCTION

Wireless sensor network security localization algorithm and its application research has been one of the hot topics in the current academic field [1]. Also, secure location information is critical for location-based WSN applications [2-4]. When faced with a malicious attack, it is necessary to ensure that the node can detect its correct location. However, after the node is attacked, it may lead to inaccurate location information, and the application related to these locations may have unsafe consequences, so it is important to carry out a secure positioning design. WSN can effectively collect and efficiently transmit data, but the node is limited by various factors such as cost, calculation, storage space, energy, etc., so only a small number of nodes equipped with GPS can be used to sense the position of the node. The positioning algorithm Design is challenging [5-6]. These nodes whose own locations are known by special methods are called anchor nodes, and other nodes need to calculate their positions through these anchor nodes. If the anchor node is attacked or the signal is provided by a malicious node, the positioning of other nodes will be inaccurate, resulting in the entire network becoming unsafe. At present, most sensor network node positioning systems are assumed to be carried out in a safe and friendly network environment, and the security problems that may be encountered during the positioning process are not considered [7]. Therefore, how to design the security mechanism in the wireless mobile network environment, and to respond to possible attacks dynamically and flexibly on the basis of ensuring location information security with reasonable overhead is a research content worthy of attention.

Manuscript received Oct 09, 2018

Zhihao Zhang, School of Computer Science & Software Engineering, Tianjin Polytechnic University, Tianjin, 300387, China

Wenju Liu, Corresponding Author, School of Computer Science & Software Engineering, Tianjin Polytechnic University, Tianjin, 300387, China

II. TYPICAL SECURE POSITIONING ALGORITHM

In order to solve the security problems existing in traditional positioning algorithms, in recent years, domestic and foreign scholars have proposed a number of security positioning algorithms. Typical security location algorithms include SeRLoc [8], HiRLoc [9], ROPE [10], and Liu algorithm [11]. Lazos and Poovendran et al. first proposed the WSN security location algorithm SeRLoc. SeRLoc is a distributed, non-ranging-based, resource-efficient positioning technology. During the positioning process, no additional communication is required between the unknown nodes, and the attack methods such as the hole attack, the Sybil attack, and the node compromise attack have good resistance performance. Although the algorithm can resist wormhole attacks, witch attacks and node capture attacks to some extent. However, when an attacker exploits selective interference to disrupt the transmission of a beacon node, it will be powerless. To this end, Lazos et al. successively proposed the HiRLoc algorithm and the ROPE algorithm.

The HiRLoc algorithm uses a method of passively detecting the position of a node, and no additional communication is required between nodes like the SeRLoc algorithm. The algorithm is also not based on ranging, so it can effectively prevent ranging attacks. In addition, it is highly robust and can resist wormhole attacks, Sybil attacks, and node compromise attacks based on changes in antenna direction and communication distance.

The ROPE algorithm is a composite algorithm that incorporates distance definition techniques. The algorithm divides nodes into Locators and Sensors. Each unknown node in the network shares a pair of keys with each anchor node and stores the key in an unknown node. ROPE can provide position determination and position verification. In addition, the method proposes a new metric called Maximum Spoofing Impact to measure attacks in ROPE. With a small number of reference points, you can still get a very low Maximum Spoofing Impact. ROPE can resist congestion attacks, wormhole attacks, and node captive attacks. ROPE is only suitable for small networks, and performs encryption, XOR, etc. during the positioning process, and requires strict time synchronization.

Liu et al. proposed two kinds of ranging-based detection, resistance and a safe positioning scheme with high robustness. The first option is the Minimum Mean Square Estimation Algorithm (MMSE). The second scheme uses a voting election mechanism to tolerate malicious anchor nodes to locate beacons. The two methods are essentially the same, that is, the beacon of the malicious anchor node is eliminated by

the consistency of the legal beacon. However, the algorithm requires that at least half of the benign nodes are subject to attack, otherwise the security positioning effect will be greatly reduced.

III. COMMON POSITIONING ATTACK METHOD

Attacks on wireless sensor network nodes can be classified into external attacks and internal attacks according to the source. External attacks generally attack by falsifying, tampering, replaying, and blocking messages. The internal attack is an attack carried out after the capture of the node, and it is more difficult to cope because it obtains the key material of the legitimate node. In the existing literature, there are mainly the following types of models for attack location.

3.1 Replay attack

Replay attacks are a relatively simple and common location attack model. The purpose of this attack method is to block the signal transmission between the sender and the receiver. After that, the old information or the same information is repeatedly transmitted. If the attacker can move in the network, the probability that the receiving node obtains the old positioning information will be large. If the unknown node is subjected to a replay attack during the positioning phase and receives incorrect location information, the node will be positioned inaccurately.

3.2 Sybil attack

The Sybil attack is also known as the witch attack. J. Douceur [12] gives the concept and harm of Sybil. In the Sybil attack, an attacker would generally lie that he or she has multiple identities. The attacked node sends a plurality of location reference information to the unknown node to cause the unknown node to locate a large positioning error or even a positioning failure. This type of attack is more destructive to network security positioning. Newsome et al. [13] analyzed the Sybil attack and defense methods in WSN.

3.3 Compromise node attack

A compromise node attack is an internal attack. The attacker captures the sensor node to obtain the wrong location information by acquiring the key of the internal communication of the network. The more serious situation is that if the beacon node is captured, the attacker sends the wrong location information through the beacon node. This may cause the positioning result of the entire network to be affected, resulting in a large positioning error.

3.4 Wormhole attack

The wormhole attack involves establishing a tunnel with little delay between two malicious communication nodes. The attacker continuously receives and replays packets from the other end of the tunnel at one end of the tunnel. Hu et al. [14-15] analyzed the wormhole attack methods in WSN and used Packet Leashes to prevent wormhole attacks. A wormhole attack is the most complex of all attacks. It can disrupt the routing of wireless sensor networks and the packets of the network. This can result in a decrease in the positioning accuracy and communication quality of the wireless sensor network. In fact, the purpose of the wormhole attack is to make two distant nodes mistakenly think that they are neighbors. In the WSN positioning process, if the node location is related to the hop count, there is a high probability of being affected by the wormhole attack.

IV. DETECTION METHOD

Intrusion Detection System (IDS) is another type of network security solution that responds to cyber attacks through detection and feedback. IDS needs to deploy monitoring nodes to collect and record information such as communication parameters and abnormal behaviors. Deploying processing nodes to match and report anomalous data usually requires the network to provide strong support for communication and computing resources. Some scholars have specifically proposed IDS for reducing the overhead of sensor networks, such as cluster-based IDS [16], distributed collaborative IDS [17], reputation-based IDS [18] and so on. In view of the fact that the simple intrusion detection system still lacks response measures to the attack. Pietro proposed an intrusion recovery protocol for unmanaged mobile sensor networks [19] (TMC2013). After the compromised node moves out of the dangerous area, the random value transmitted by the adjacent healthy node can be used to regain the confidentiality of the key material. However, the model set by the institute lacks corresponding application scenarios. Sultana proposed a system combining intrusion detection and event response Kinesis [20] (SenSys2014). Kinesis's innovative idea is to consider the real-time response of abnormal events and the timely recovery of the network, allowing the network to respond to the attack while maintaining normal operation. Because Kinesis's key management mechanism is relatively simple, if there is an internal attack, there is a risk that the security policy will be replaced by the attacker.

Common detections for specialized attacks include replication attack detection, worm attack detection, and witch attack detection. A system that performs node position verification can naturally solve the wormhole attack problem. The well-designed identity authentication system can resist the witch attack of forged identity. However, node location verification and identity authentication are not sufficient to deal with node replication attacks implemented after node capture attacks.

V. COMPARISON AND ANALYSIS

This section compares several security location algorithms and location attack models shown in Table 1. Through analysis, we can find that these algorithms have their own characteristics and scope of application. It can be concluded that there is currently no algorithm that is optimal. Table 1 analyzes and compares several security location algorithms introduced in this paper from the aspects of positioning accuracy, number of beacon nodes, hardware requirements and security methods.

In the traditional non-ranging positioning method, nodes rely on data exchange to sense their position, so the security of data transmission is the focus of this type of method. Some techniques of cryptography can solve some problems, but at the same time increase the communication overhead of the network. With ranging-based positioning techniques, attacks

on such methods can be seen as attacks on hardware that are not easily detected, which poses a challenge to the accuracy of positioning. There is no uniform metric for the several secure positioning techniques described in the table. Starting from the characteristics of wireless sensor networks, these security positioning methods are analyzed and compared only in terms of positioning accuracy, number of beacon nodes, hardware requirements, and security methods used.In Table 1, the various positioning methods affected are classified according to the positioning attack model.

Secure positioning algorithm	positioning accuracy	Beacon node	Hardware requirements	Safety method
SeRLoc	Higher	less	Omnidirectional antenna, Directional antenna	RC5 encryption, One-way hash authentication
HiRLoc	Lower	less	Directional antenna	Global shared key, Hash function authentication
ROPE	Lower	less	Directional antenna	Node shared key pair, One-way hash authentication
Liu	Higher	More	nothing	Key identification technology, Using the same number of hops

Positioning attack model	Affected positioning method
Replay attack	AHLos, RADAR[21], Centroid algorithm, Cricket
Sybil attack	Centroid algorithm
Compromise node attack	RADAR, Cricket, APIT, Centroid algorithm, DV-Hop
Wormhole attack	APIT, DV-Hop

Table 1. Comparison of several typical security location algorithms and location attack models

VI. CONCLUSION

With the widespread deployment and application of wireless sensor networks, the security of wireless sensor network positioning has attracted more and more attention. Location-based services are increasingly being used in people's work and life. In the past, the positioning algorithm design mainly focused on the consideration of the accuracy and energy consumption of the positioning algorithm, and rarely considered security. In response to this phenomenon, this paper first introduces several typical security positioning methods for wireless sensor networks. Subsequently, several common types of positioning attack models and attack detection methods are described. Finally, several typical security location algorithms and location attack models described in the paper are analyzed and compared in detail. With the continuous improvement of positioning accuracy and safety positioning requirements, WSN safety positioning technology will be further developed and will be more and more concerned by scholars [22-24]

REFERENCES

[1] Estrin D, Govindan R, Heidemann J, et al. Next Century Challenges: Mobile Networking for "Smart Dust"[J]. Acm Mobicom, 1999:271--278.
[2] Liu Yunhao, Yang Zheng, Wang Xiaoping, et al. Location, Localization, and Localizability[J]. Journal of Computer Science and Technology,2010, 25(2):274-297.
[3] Liu J, Liu J, Liu J, et al. Semi-supervised deep extreme learning machine for Wi-Fi based localization[J]. Neurocomputing, 2015, 166(C):282-293.
[4] Tsirmpas C, Rompas A, Fokou O, et al. An indoor navigation system for visually impaired and elderly people based on Radio Frequency Identification (RFID)[J]. Information Sciences, 2015, 320(C):288-305.
[5] Ji H R, Irfan M, Reyaz A. A Review on Sensor Network Issues and Robotics[J]. Journal of Sensors, 2015, 2015(6):1-14.
[6] Halder S, Ghosal A. A Survey on Mobility-assisted Localization Techniques in Wireless Sensor Networks[J]. Journal of Network & Computer Applications, 2016, 60:82-94.
[7] Cui Jifeng. Research on Secure Localization in Wireless Sensor Networks[D]. Nanjing University of Aeronautics and Astronautics, 2014.
[8] Lazos L, Poovendran R. SeRLoc: Robust localization for wireless sensor networks[M]. ACM, 2005, 1 (1):73-100.
[9] Lazos L, Poovendran R. HiRLoc: high-resolution robust localization for wireless sensor networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):233-246.
[10] Lazos L, Poovendran R, Capkun S. ROPE: robust position estimation in wireless sensor networks[C]// International Symposium on Information Processing in Sensor Networks. IEEE, 2005:43.
[11] Liu D, Ning P, Du W K. Attack-resistant location estimation in sensor networks[C]// International Symposium on Information Processing in Sensor Networks. IEEE Press, 2005:13.
[12] Douceur J R. The Sybil Attack[C]// International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002:251-260.
[13] Newsome J, Shi E, Song D, et al. The Sybil attack in sensor networks: analysis & defenses[C]// International Symposium on Information Processing in Sensor Networks. IEEE, 2004:259-268.
[14] Hu Y C, Perrig A, Johnson D B. Wormhole attacks in wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):370-380.
[15] Hu Y, Perrig A, Johnson D. Packet leashes:a defense against wormhole attacks in wireless Ad hoc networks[C]//Proceedings of INFOCOM 2003, San Francisco, CA, USA, April 2003.
[16] Su C C, Chang K M, Kuo Y H, et al. The new intrusion prevention and detection approaches for clustering-based sensor networks [wireless sensor networks][C]// IEEE Wireless Communications and NETWORKING Conference. IEEE, 2005:1927-1932 Vol. 4.
[17] Krontiris I, Benenson Z, Giannetsos T, et al. Cooperative Intrusion Detection in Wireless Sensor Networks[C]// Wireless Sensor Networks, European Conference, Ewsn 2009, Cork, Ireland, February 11-13, 2009. Proceedings. DBLP, 2009:263-278.
[18] Bao F，Chen R，Chang M J，et al. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection[J]. Network and Service Management，IEEE Transactions on，2012，9(2): 169-183.
[19] Pietro R D, Oligeri G, Soriente C, et al. United We Stand: Intrusion Resilience in Mobile Unattended WSNs[J]. IEEE Transactions on Mobile Computing, 2013, 12(7):1456-1468.
[20] Sultana S, Midi D, Bertino E. Kinesis:a security incident response and prevention system for wireless sensor networks[C]// Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems. ACM, 2014:148-162.
[21] Bahl P, Padmanabhan V N. RADAR: An In-Building RF-based User Location and Tracking System[C]// INFOCOM 2000. Nineteenth Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. IEEE Xplore, 2000:775-784 vol.2.
[22] Zhang P, Lu J, Wang Q. Performance bounds for relative configuration and global transformation in cooperative localization, ☆[J]. Ict Express, 2016, 2(1):14-18.
[23] Nguyen X L. LOCALIZATION PROBLEM IN SENSOR NETWORKS: THE MACHINE LEARNING APPROACH[C]// 2012.
[24] Tang T, Liu H, Song H, et al. Support Vector Machine Based Range-Free Localization Algorithm in Wireless Sensor Network[M]// Machine Learning and Intelligent Communications. 2017.