Asia-SAME Transactions on Engineering Sciences, ISSN: 2377-8970
ISBN: 978-1-948012-15-7 https://doi.org/10.7508/aste.01.2020.218.224

Secure Localization Technology of Wireless Sensor Networks Based on Symmetric Cryptography

Zhimin Zhang
Xi'an International University, Xi'an 710000, China
*Corresponding author: 2432132859@qq.com

From 2020 International Conference on Engineering Research, Beijing, China. 12-14 April 2020, Organized by University of Science and Technology Beijing and International Association of Management Science and Engineering Technology (IAMSET).

Abstract: Wireless sensor networks are usually deployed in unattended areas. Wireless communication links are used for data transmission between sensor nodes. The resources of nodes such as calculation, storage, communication and energy are very limited. Information encryption is one of the core contents of information security. In a sensor network, each sensor node senses and collects various information needed by the network in its geographical environment according to its special functions, and transmits this useful information to the monitoring center for further processing in a multi-hop manner through encryption and wireless transmission technologies. Digital signature, identity authentication, password system and other technologies based on encryption technology can effectively maintain information security. It is of great significance to study encryption technology. This paper proposes a new secure location algorithm: symmetric cipher algorithm. This algorithm can effectively suppress malicious attacks of hijacked nodes. Symmetric cipher algorithm has no additional requirements on node hardware and can be used in ordinary wireless sensor networks.
Keywords: Symmetric password, wireless sensor networks, safe positioning.

Introduction

Wireless sensor network (WSN) is usually composed of a large number of inexpensive and low-power sensing devices, which have only limited storage, computing and communication resources [1]. Radio is used as a transmission medium between nodes, and a network is formed in a multi-hop relay mode. The network can realize real-time data acquisition, effective processing and reliable transmission. This sensor network integrates sensor technology, embedded computing technology, distributed information processing technology and communication technology, and can cooperatively monitor, sense, collect and process information of various environments or monitoring objects within the network distribution area in real time [2]. The physical characteristics of the wireless channel itself make the bandwidth of the wireless network generally lower than that of the traditional wired network. Moreover, the collision caused by competing and sharing the

wireless channel is more intense through multi-hop transmission and high-density deployment among sensor nodes, and the problem of exposing and hiding terminals is more prominent [3]. The wireless multi-hop communication mode makes it easier to attack such as signal interference and eavesdropping. The possible capture attacks bring potential security risks of internal attacks to the network. Therefore, how to realize the secure positioning of wireless sensor networks is a very challenging and valuable topic.

Symmetric encryption algorithm

Symmetric cryptographic algorithms are sometimes called traditional cryptographic algorithms. The characteristic of symmetric algorithm is that the encryption key can be deduced from the decryption key, and the decryption key can also be deduced from the encryption key. Generally speaking, the encryption and decryption process of information is determined by the cryptographic system and key. The mathematical functions used for encryption and decryption are called cryptographic algorithms [4]. It is easy to implement. However, only the probability value can be used to measure whether the nodes can share the key and calculate the length of the key path. The degree of network security connectivity is also a probability result. When the network size is large, the sharing probability decreases rapidly. The sink node decrypts each data it receives, aggregates the data according to the corresponding aggregation function, and encrypts the aggregation result before forwarding them (this method requires the sink node to establish a private key with neighboring nodes).

As shown in Figure 1, the keys of both parties are kept confidential, because the confidentiality of the private key system must be based on the confidentiality of the key, not on the algorithm. This ensures the security of the private key encryption algorithm in hardware.

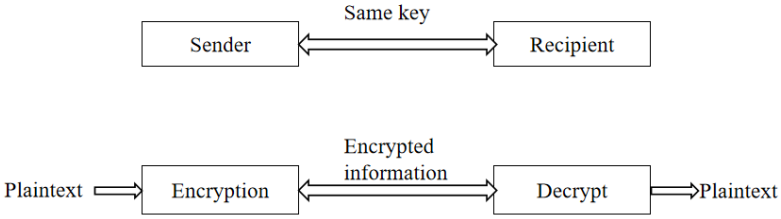

Figure 1. Symmetric encryption

In asymmetric cryptography, the key used to encrypt data and the key used to decrypt data are different, and the other key cannot be derived from one key, so the protection of the key is relatively strong [5]. The security of the encryption method depends on the secrecy of the key, not the secrecy of the algorithm. Therefore, it is not necessary to ensure the secrecy of the algorithm, but the secrecy of the key.

Analysis of node localization technology

Distance-independent location algorithm

The location algorithm without distance measurement does not need to measure the distance or angle information between the unknown node and the anchor node. It estimates the distance between the two nodes through connection information, energy consumption information or the area information of the overlapping area of the anchor node. As we all know, wireless sensor networks usually work in dangerous or hostile environments and have high security requirements, such as military applications. It is necessary to measure the absolute distance or azimuth between the unknown node and the beacon node. This phase is called the ranging phase. Then the actual distance or azimuth information between nodes measured by ranging technology is used to calculate the position coordinates of unknown nodes, i.e. the positioning stage. When the node to be located knows the coordinates of the surrounding three anchor nodes and the angles relative to the three anchor nodes, the unknown node can still determine its own position information under the condition that the distance between the node and the three anchor nodes is unknown [6]. On the one hand, the improved location algorithm makes the location algorithm less vulnerable to attacks from outside. On the other hand, it can design a secure location algorithm to detect attacks and eliminate the attacked nodes or improve the existing security algorithm to make it applicable to wireless sensor network location. In the case of no malicious nodes, the higher the density of two points, the more malicious nodes, and the larger the proportion of failed nodes in the sensor network.

Location algorithm based on distance measurement

The location method based on distance measurement estimates the distance between unknown nodes and anchor nodes, and then combines the location of anchor nodes and the location algorithm to estimate the location. However, the location method without ranging does not need to estimate the distance between the unknown node and the anchor node. Different localization algorithms in sensor networks have different localization ideas, and the security problems they face are also different. When exchanging the received anchor signal strength with the neighbor node, the malicious node maliciously changes its real strength. For example, the malicious node amplifies all signal strengths, making the neighbor node mistakenly believe that the distance from the malicious node to all anchor points is smaller than itself. Considering the influence of environmental factors in wireless sensor networks, this localization algorithm uses signal strength information and actual distance to verify the weighted value of nodes. Therefore, the algorithm can improve the adaptability in different network environments and improve the positioning accuracy. For example, in a public key cryptosystem, an attacker can encrypt any plaintext he chooses using the public key. This attack is a plaintext attack. Since the previous time

synchronization protocols for wireless sensor networks did not consider security issues, attackers can easily launch various attacks against time synchronization protocols [7]. Specific attacks can be divided into two types: external attacks and internal attacks.

Secure localization algorithm for wireless sensor networks based on symmetric cryptography

DES (Data Encryption Standard) decryption process is the opposite of encryption. The key is used in the reverse order of encryption, namely k16, k15, and k1. The encryption system with additive homomorphism is used to aggregate data on ciphertext. The aggregated ciphertext is transmitted to the base station for decryption to obtain the final aggregation result. According to the known propagation speed of the two signals, the time difference is directly converted into distance. However, its power consumption and area cost are much higher than those of the operation unit with folded structure. Therefore, in wireless sensor networks characterized by low cost and low power consumption, it is a very difficult process to manage symmetric cryptographic algorithms, especially for some large and wide-area networks. It is precisely because of these factors that the scope of private key algorithm is restricted. During ranging, unknown nodes must be guaranteed to be within the signal coverage range of anchor nodes. The product of the average distance per hop value and the minimum hop value in the network is used to represent the distance information between the unknown node and the beacon node, and when the unknown node obtains the distance information with three or more distance information to the beacon node, multilateral measurement and positioning are carried out.

In order to save the energy consumption of the whole network, wireless sensor network nodes should reduce the long-distance single-hop transmission as much as possible and change to short-distance multi-hop transmission to save energy. Node sends k bit data packet to another node with distance d, and its energy consumption is [8]:

$$E_{Tx}(d) = E_{Tx-elec}(k) + E_{Tx-amp}(d) \tag{1}$$

$$E_{Tx}(d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2 & d < d_{eo} \\ kE_{elec} + k\varepsilon_{mp}d^4 & d \geq d_{eo} \end{cases} \tag{2}$$

Energy consumption of node receiving k bit data packet is:

$$E_{Rx}(k) = kE_{Rx-elec}(k) = kE_{elec} \tag{3}$$

Where E_{elec} is the energy consumed by the node sending or receiving each bit of data, k is the length of the data packet, and ε_{fs} and ε_{mp} are constants under different amplification models.

Usually, when the coordinate information of the neighboring nodes is known, the distance between the unknown node and the target node is determined. Therefore, external malicious nodes can disguise themselves as anchor nodes

in the network and broadcast fake location messages to the network. The number of keys in the whole network using elliptic curve encryption algorithm is H(n), which is less than DES. the key transmission and update of asymmetric cryptosystems do not require secure information channels. in terms of the number of keys to be distributed, the public key system and the private key system are *n* and *n2*, respectively. the latter is one order of magnitude more than the former and is difficult to distribute and manage. According to this model, by using the distance relation between the unknown node and the anchor node, a rectangular overlapping range can be determined, and the centroid of the overlapping region is the unknown node position. Through information exchange between nodes, each node records the hop distance value to the surrounding beacon nodes and the location information of the beacon nodes for further processing. During pre-distribution, key groups are constructed in units of key fragments, the key groups become a set of key fragments, and the node pairs use the shared multiple key fragments to synthesize a shared key in real time. The process of stopping at anchor nodes to release positioning messages and then moving makes the signal coverage of the two stopping and releasing messages just correspond to a rectangular positioning area group. These clusters constitute the space-time multiplexing allocation of channels. It has advantages in cost and power consumption over distance-based methods. Therefore, it is widely used in wireless sensor networks.

Three spoofing attack nodes are randomly placed in the simulation experiment scene, and the communication range of the attack nodes is the same as that of unknown nodes and beacon nodes, both of which are 10m. Figure 2 shows the average positioning error (curve 1) of the network node when there is no attack, the positioning error (curve 2) of the network node when there is an attack, and the positioning error (curve 3) of the node after the symmetric cryptographic algorithm is adopted. The results show that after the symmetric cipher algorithm is adopted, the average positioning error of nodes is close to the positioning error without attack, and the more beacon nodes, the better the approximation degree.

In data aggregation of static sensor networks, sensor nodes use the same public key to encrypt data, so data can be aggregated on ciphertext using additive homomorphism when transmitted to sink nodes. The distance consistency is used to eliminate abnormal nodes in the positioning reference set, and then the symmetric cryptographic positioning algorithm is used to estimate the coordinates of unknown nodes. When an unknown node obtains distances from 3 or more positioning nodes, trilateration positioning is performed in the third stage. If the channel is busy, the equipment needs to repeat the above process of waiting for a period of time and detecting the channel state until the data can be transmitted. Therefore, the influence of the inserted interference signal on the reception strength of the ranging message signal will be analyzed and discussed in detail below. That is, the positioning stage, in which unknown nodes use Euclidean distances between one or more beacon nodes obtained by the unknown nodes to carry out positioning operation using a specific algorithm, thus realizing the positioning of

unknown nodes. This method reduces the system's requirement for node time synchronization, is relatively easy to implement and has high positioning accuracy, but is still susceptible to multipath and non-line-of-sight propagation. Due to the existence of a large number of anchor triangles around the nodes, ignoring the fact that the nodes are located outside the triangles, the positioning accuracy will not be reduced and the security will be greatly improved.

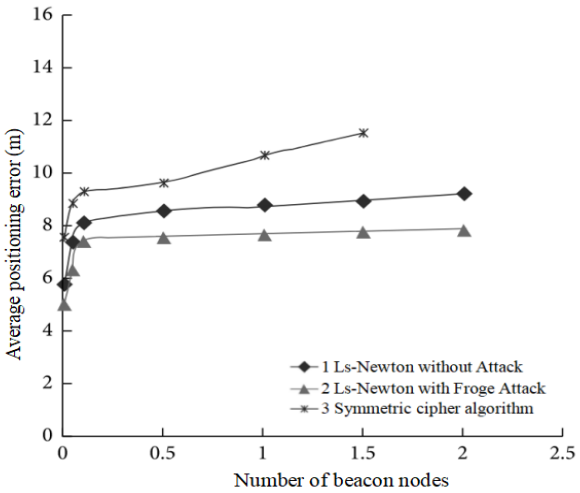

Figure 2. Average positioning error curve with beacon nodes and number

Conclusion

With the continuous maturity and rapid development of technology, people can obtain a large amount of real-time information perceived and measured by objective environment through wireless sensor networks, so the security problem of information data is becoming increasingly serious. In this paper, a new secure location algorithm for wireless sensor networks based on symmetric cipher is proposed. Compared with the common location algorithm, the location error is smaller, and the sharing probability is higher and the key path length is smaller than the existing multi-key sharing scheme under the same node key group length and key strength requirements. Symmetric cryptographic secure localization algorithm can improve the localization accuracy of unknown nodes on the basis of reducing the cost and power consumption of wireless sensor networks. And it can defend against certain camouflage attacks and wormhole attacks.

References

[1] Zhang, D., Han, Z., Wang, X.L. 2016. Lightweight wireless sensor network security authentication protocol based on the cooperation of adjacent areas. Information Communication, (9): 26-27.

[2] Chen, H.L., Wang, Z.B., Wang, Z. 2015. A safe localization method for

wireless sensor networks against wormhole attacks. Journal of Communications, (3): 1-8.
[3] Zhang, Q.H., Xu, X.Z., Zou, Y.L. 2016. Research on roadway personnel positioning technology based on 802.11 n wireless sensor network. China Safety Production Science and Technology, 12 (4): 62-69.
[4] Chen, L.J., Jin, H.B., Mao, K.J. 2016. Security location algorithm for wireless sensor networks against wormhole attacks. Journal of Sensor Technology, (12): 102-107.
[5] Ji, X.M., Zhao, B., Liu, J.H. 2018. Key recovery attack in wireless sensor networks based on symmetric matrix decomposition. Journal of Communications, 39 (10): 87-96.
[6] Zhang, G.P. 2015. The latest research progress of online code distribution in wireless sensor networks. Journal of Zhejiang University of Science and Technology, 33 (2): 219-227.
[7] Gui, Y.H. 2015. Research on safety and energy saving scheme of wireless sensor network for modern agriculture. Journal of Liuzhou Teachers College, 30 (5): 130 + 141-143.
[8] Zhang, Q.K., Gan, Y., Wang, R.F. 2018. Asymmetric group key agreement protocol among clusters. Computer Research and Development, 55 (12): 69-81.