Overview of Wireless Sensor Network Security Technology

Zili Zeng[1]

[1] Haikou College of Economics, Haikou, Hainan, 571127

Keywords: wireless sensor network; network security; technology

Abstract: With the continuous improvement of science and technology and people's living standards, wireless sensor network technology has gradually been widely used, and provides great convenience for people's living, but with the continuous improvement of the degree of application, wireless sensor network security issues also enters people's field of vision. This paper focuses on analyzing the security requirements of wireless sensor networks (WSN), and analyzes the security technologies of wireless sensor networks from various perspectives, and summarizes and discusses the research direction of sensor network security technologies.

1. Introduction

Wireless sensor network technology is also called WSN (Wireless sensor network). This is a new type of sensor network technology. This network technology has been applied to all aspects of human normal life, and the daily activities of human beings. Inseparable, such as production, life and other activities are inseparable from the support of sensor network technology. The sensor nodes that make up the sensor network are characterized by many types, small size and light weight, low manufacturing cost, and also include wireless communication and monitoring communication. This kind of sensor network technology has been applied to many places, and it is also a new trend in the development of information technology. This technology has broad application in global climate monitoring, national territorial security, medical and health, and traffic information. Prospects.

Wireless sensor networks are composed of a large number of different sensor nodes. The nodes are composed of three parts: wireless communication information module, information processing module, and information sensor module. The development and research of wireless sensor networks based on sensor networks is the improvement of the sensor network and the network itself. The characteristics of the sensor networks are as follows. (1) Generally, large-scale wireless sensor networks require a large number of network nodes. These network nodes have a wide range of distribution, large numbers, small size, and high density. (2) Sensors composed of network nodes have a small size and can adapt to various environments at the same time. (3) The acquisition of information is the main purpose, and the data is used as the center for information transmission. (4) The general communication capabilities of sensor networks are limited by various factors. (5) Each node of the sensor network is subject to restrictions on the use of battery power, information storage capabilities, and information analysis capabilities. (6) Sensor networks generally have very fast topological changes, accompanied by strict self-organization. As mentioned above, the characteristics of a sensor network are also the biggest limitations of wireless sensor networks. Since wireless sensor networks are perfect for sensor network technology, the sensor nodes used are basically the same as the sensor networks. Therefore, the limitations of wireless sensor networks are basically the same as those of sensor networks. These are related to storage hardware and communication hardware. Data analysis is related to transmission and battery power.

2. Wireless Sensor Network Security Issues

The security goal of wireless sensor networks is to solve network availability issues, confidentiality issues, integrity issues, node authentication issues, and freshness issues. Due to the characteristics of the wireless sensor network itself, the implementation of its security goals is different from the general network. When researching and transplanting various security technologies, the following constraints must be further considered [2]: (1) Energy limitation. Nodes are difficult to replace and recharge after deployment, so low energy consumption is a primary consideration when designing security algorithms. (2) Limited storage, operating space, and computing power. The space for sensor nodes to store and run code is very limited, and the computing power of their CPUs cannot be compared with the average computer. (3) Unreliable communication. The instability of wireless channel communication, the conflict of node's concurrent communication [3] and the large delay of multi-hop routing make us to consider the fault tolerance problem when designing the security algorithm, reasonably coordinate the node communication, and minimize the requirement for time synchronization. (4) The physical security of the node cannot be guaranteed. When we conduct security design, we must consider the detection and removal of the captured nodes. We must also limit the spread of security risks caused by the captured nodes to a minimum. (5) The randomness of the node arrangement. Nodes are often randomly placed into the target area, and the positional relationship between the nodes is generally unpredictable prior to deployment. (6) Safety requirements and application related. The application of wireless sensor networks is very extensive, and the security needs of different applications are often different.

3. Attack Methods and Defense Methods

Congestion attack refers to that after the attacker knows the center frequency of the target network communication frequency, the attacker launches a radio wave near the frequency point to perform the interference. The defense method is to detect that the space is under attack, the network node will use a unified strategy to jump to another frequency for communication. Collision attack refers to the enemy sending another packet at the same time when the normal node sends the packet, so that the output signal can not be separated because they are superimposed on each other. The defense method is to use error correction coding to recover the received erroneous data packets, use the channel monitoring and retransmission mechanism to avoid the collision of data packets to the channel requirements, and select the retransmission time of the data packet according to a certain strategy after the conflict. Discarding and greedy destruction means that when a malicious node is used as a normal routing node, a malicious node may randomly drop some packets; in addition, a malicious node may send its own packets with high priority, thus destroying the network. Normal communication. In order to solve this problem, identity authentication mechanism can be used to confirm the legitimacy of the routing node; or use multi-path routing to transmit data packets, so that after a data packet is discarded on a certain path, the data packet can still be transmitted to the destination node. Flooding attack means that the attacker constantly requests to establish a new connection with the neighbor node, thus exhausting the resources used by the neighbor node to establish the connection, so that other legitimate requests to the neighbor node have to be ignored. To solve this problem, you can use the client puzzle technology. Its idea is: before establishing a new connection, the service node requires the client node to solve a puzzle, and the cost of the legal node to solve the puzzle is far less than the cost of solving the problem of the malicious node.

4. Hot Spot Security Technology Research

The current standard for evaluating whether cryptography is suitable for wireless sensor networks is the code length, data length, processing time, and energy consumption of cryptographic algorithms. Compared with the asymmetric key algorithm, the symmetric key algorithm has the characteristics of low computational complexity and low energy consumption [4]. Therefore, it has been regarded as the mainstream cryptographic technology in wireless sensor networks. A ura T et al [5] compared the performance of six popular symmetric key algorithms in wireless sensor networks. The results are shown in Table 2. The comparison results show that MIST Y1 has obvious advantages in key establishment, and there is no obvious advantage in encryption and decryption. A ura T et al. further counted the total number of CPU clock cycles used by various algorithms and found that the Rijndael algorithm uses the largest number of CP U clock cycles, so Rijndael has the highest energy consumption. A ura T et al. finally concluded that the MIST Y1 algorithm has the most advantage on the node equipment with poor performance. Recently, the study of public key algorithms in WSN [7-9] is mainly directed at Rabin's Scheme, NtruEncry pt, RSA and Elliptic Curve Cry ptog ra phy (ECC). The above algorithm was implemented on the Mica2 mote node. The computational speed of the public and private keys, the energy consumed by the signature and authentication, and the energy consumed by the key exchange were compared. It was found that the ECC algorithm has the greatest advantages. This is due to the fact that under the same security strength, the key length required by ECC is the smallest, which reduces the computational load and communication load accordingly. Studies have shown that as long as the appropriate public key algorithm and parameters are selected and the algorithm is optimized to use energy-saving technology at the same time, it is also possible to use public-key cryptography in the WSN. However, most WSN applications still cannot afford the cost of using public key cryptography.

The positional relationship among the nodes in the WSN cannot be determined before deployment, and the network topology is unstable, making the traditional key management technology unable to be effectively applied to the WSN. Due to the advantages of symmetric key algorithms in computational complexity and energy consumption, most key management techniques are based on symmetric key mechanisms. The following is a brief introduction to the current popular key management technologies: (1) Pre-shared key model and non-pre-shared key model. The pre-shared key model means that the shared key between nodes has been determined before the node is deployed. The non-pre-shared key model means that the shared key between nodes is determined through the negotiation mechanism after the node is deployed. The non-pre-shared key model conforms to the characteristics that the relative position of nodes in the WSN can not be predicted before deployment, so it is more suitable for WSN. The key management techniques introduced later belong to the non-pre-shared key model. (2) Probability and certainty. If the key share is successful or not with a calculable probability, it belongs to the probabilistic key management technology. Eschenauer and Gligor first proposed a basic random key pre-distribution protocol. Its basic idea is to establish a large key pool with a capacity of s, and each node has a key in m key pools. As long as any two nodes have the same key, both nodes can establish a secure channel. They proved that there is a computable relationship between s, m and the network connectivity probability p under the condition that the network size and the expected number of neighbor nodes are known. Its advantages are that the key storage pressure of each node is greatly reduced, and it is suitable for key management of large-scale WSNs. The disadvantage is that there is an isolated problem. Key sharing between nodes that require data exchange is not necessarily successful. Later, on this basis, further changes were made to the q-composite random key pre-distribution protocol multiple versions. The deterministic key management technology refers to ignoring physical factors such as channel errors, and it is theoretically possible for two nodes that need to exchange data to generate a shared key. LEAP is a typical deterministic key management technology. The LEAP protocol considers that a single security requirement cannot satisfy all types of communication in the WSN, so a variety of key mechanisms are used. LEAP maintains four keys on each node: an identity key (pre-distribution) that is shared separately with the base station, a group key (pre-distribution) shared with all nodes in the network, a neighbor key shared with neighbor nodes, and Cluster head shared cluster head key. The latter two keys are established through the negotiation mechanism after the node is deployed, and are established using the pre-distribution master key between the nodes that want to share the key. Compared with the random key pre-distribution protocol, the LEAP protocol increases the computational load and memory space requirements of the nodes, but it guarantees that there must be a shared key between nodes that need to exchange data. LEAP is suitable for WSN applications with high security requirements. (3) Isomorphism and Heterogeneity. The above-mentioned key management protocol assumes that all nodes except the base station have the same performance, so their applicable object is the homogeneous WSN. In contrast, Traynor et al. introduced super nodes in random key pre-distribution protocols for heterogeneous WSNs. By storing more keys in the key pool in super nodes, the density needed to be stored on ordinary nodes was further reduced. The number of keys improves network security.

5. Conclusion

Wireless sensor from the entire application situation, because of its stringent requirements in terms of communication information, so the relevant business information and daily exchanges have an important role in the business, so we need to not interrupt the increase in research efforts and research intensity through technology The continuous innovation will increase China's application in wireless sensor network technology, thus promoting the development of China's socialist economy and seeking more and more beneficial benefits.

Acknowledgement

In this paper, the research was sponsored by the School level research project of Haikou College of Economics in 2018(Research on image compression and coding, No. hjkz18-02).

References

[1] Prr JC, PalR N.A functional link artificial neural network for adaptive channel equalization [J]. Signal Processing. 1995.

[2] Pasquale Arpaia, Pasquale Daponte, Domcaico Grmi ald, i et al. Based on Error Reduction for Expermi entally Modeled Sensors [J]. IEEE Trans. on Instrumentation and Measurement. 2002.

[3] Xu Lina. Neural network control [M]. Harbin: Harbin Institute of Technology Press. 1999.

[4] Genetic Algorithm Combining FANN to Accelerate Dynamic Characteristics Compensation of Accelerometers[J]. Chinese Journal of Metrology. 2005.

[5] Lang Weimin, Yang Zongkai, Wu Shizhong, Tan Yunmeng. Research on Wireless Sensor Network Security [J]. Computer Science. 2005.