Application of Wireless Sensor Networks in the Sensitive Data Security of Intelligent Data Center under the Big Data Environment

Han Lin1, *, Binxin Weng1, Jianli Pan1, Chaodeng Lin1, Qifan Yang2
1State Grid Info-Telecom Great Power SCI.& Tech. Co., Ltd., Fuzhou, Fujian, 350001, China
2Information and Communication Branch of State Grid Fujian Electric Power Co., Ltd., Fuzhou, Fujian, 350001, China

*Corresponding author e-mail: han_lin@sgit.sgcc.com.cn

Abstract. In the big data environment, wireless sensor networks (WSN) are constantly improving themselves and are widely used in all walks of life. The WSN collects, processes and transmits the information of the sensed object in the monitoring area. In recent years, WSN have also made good progress in environmental change detection, traffic control, and sensitive data security management. The purpose of this article is to study the application of WSN in the security management of sensitive data in the data center under the big data environment. This article first describes the characteristics of WSN, and discusses the security management requirements of sensitive data in WSN based on big data technology. Secondly, it analyzes the problems in the security management of sensitive data and conducts research from different directions. Finally, in response to these problems, the implementation of the WSN in the security management of sensitive data provides some help to solve the problem. Thereby effectively reducing the energy consumption of network nodes, reducing the amount of data transmitted by the network, and extending the life cycle of the WSN. Experimental research results show that the most demanded level in security management is data confidentiality, which is 47.15%, followed by data freshness and data integrity, which are 28.49% and 24.36%, respectively. In summary, it is necessary to increase efforts to improve the security management of sensitive data.

Keywords: Wireless Sensor Network, Sensitive Data, Security Management, Application.

1. Introduction
In the big data environment, WSN have become increasingly mature and have been widely used in various fields [1-2]. The WSN collects, processes and transmits the information of the sensed object in the monitoring area [3-4]. At first, WSN were mainly used in the military field [5-6]. In recent years, WSN have also achieved better development in environmental change detection, traffic control, and sensitive data security management [7-8].
In the research on the application of WSN in the security management of sensitive data in the data center under the big data environment, many domestic and foreign scholars have studied it and achieved good results. Mohamed and Jiang proved that both RSA and ECC can be used. Applied to the WSN of 8-bitCPU, it is proved through experiments that the performance of ECC is obviously better than RSA in the application of WSN [9-10]. Arshad and Erlantz proposed a series of secure synchronization protocols for various situations, such as sender-receiver, multi-hop sender-receiver group synchronization [11-12].

This article first describes the characteristics of WSN, and discusses the security management requirements of sensitive data in WSN based on big data technology. Secondly, it analyses the problems in the security management of sensitive data and conducts research from different directions. Finally, in response to these problems, the implementation of the WSN in the security management of sensitive data provides some help to solve the problem.

2. Research on the Application of WSN in the Security Management of Sensitive Data in the Data Center under the Big Data Environment

2.1. Features of WSN

(1) Widely distributed network nodes
The purpose is to obtain accurate and complete information resources. According to different geographical distribution areas, sensor nodes can collect massive and strong anti-interference information resources. For these information resources, the WSN adopts a distributed processing method, which effectively enhances the total accuracy of the information resources, and at the same time reduces the accuracy requirements for each node. Since there are a large number of redundant nodes distributed in the network, the entire network has a good fault self-repair function. In addition, the massiveness of nodes determines the wide coverage of the distribution area, further reducing the existence of blind spots.

(2) Dynamic
Networking in a complex environment, because the coverage area often encounters a variety of electrical and magnetic environmental interference, coupled with the loss of supply energy can easily cause sensor nodes to fail, therefore, sensor networks must be able to carry out automatic networking, and the nodes can coordinate to complete a certain task.

2.2. The Security Management Requirements for Sensitive Data in the WSN in the Data Center

(1) Data freshness
Even if data confidentiality and integrity are guaranteed, the freshness of each message still needs to be guaranteed. Data freshness means that the data is recent and it is guaranteed that no old information is replayed. This requirement is particularly important when sharing key strategies. The typical shared key needs to be replaced when it expires, but it takes a certain amount of time to transmit the new key to the entire network. In this case, it is easy to be replayed by the adversary. If the sensor node does not know the update time of the new key, the attack can easily interfere with the normal operation of the WSN. The solution to this type of problem is to use time stamps.

(2) Effectiveness
Some changes need to be made to apply traditional encryption algorithms to WSN, but this will cause some additional overhead. Some methods are to sacrifice the security of the algorithm to simplify the code, some methods are to use additional communication to win the security goal, and some methods make strict restrictions on data access or propose some impractical mechanisms (such as a centralized mechanism) to simplify algorithm. But all methods will weaken the effectiveness of WSN.

(3) Self-organization
WSN is a special case of Adhoc network, which requires each sensor node to be highly autonomous, flexible, and capable of self-organization and self-repair in different situations. Since the WSN does not have a fixed infrastructure for management, this inherent characteristic poses a major challenge to the
security of the WSN. Several random key pre-distribution mechanisms have been proposed based on the symmetric cryptographic mechanism. To apply public key cryptography to WSN, an effective public key distribution mechanism is the key. Similarly, distributed sensor networks must have self-organization functions to adapt to multi-hop routing, key management and establishment of trust relationships between sensor nodes. If the sensor network lacks self-organization function, it will be devastating in a hostile environment.

2.3. Security Issues of Sensitive Data

(1) Replay
Replay is similar to the situation where the sound recorded by a tape recorder is replayed. When an illegal user damages the system by recording and replaying a message, this process is replay. An illegal entity wants to become a legal entity for destruction, then he can intercept a valid authentication message and replay it, then it can become a legal entity. The big threat to financial business is replay.

(2) Message tampering
The so-called message tampering is to modify the transmitted message without being noticed, and causing unauthorized consequences. This situation is also very common. For example, the information transmitted in the channel is "authorized user X to access confidential documents". If the message is tampered with "authorized user Y to access confidential documents", then this user Y is an unauthorized user, but once the illegal user has this permission, the consequences are difficult to estimate.

(3) Denial of service
Denial of service is a common DoS (denyofservice). If a normal entity cannot perform its original function normally, or a series of actions of this entity hinder the normal performance of other entities, it is a denial of service. This kind of attack often destroys the entire network, using a large amount of spam resources to exhaust the communication bandwidth or host memory, causing the performance of the entire system to decrease or service interruption. In addition, this active attack can also suppress the flow of communication services or create some false messages trying to destroy the network channel for no reason, so that the relay entity can make routing decisions based on the received messages, which will cause network congestion and cause damage to normal communication.

2.4. Application of WSN in Sensitive Data Security Management

(1) Confidentiality of data
In the case of normal communication throughout the network, each system cannot confirm that illegal users are eavesdropping on the data in the network. For this situation, if some very sensitive data is encrypted, the data will be transmitted in the channel. Relatively safe, even if it is stolen, it cannot be read normally. Because illegal users do not have the decryption key. With the development of science and technology, it is not surprising to decipher the encryption algorithm, so when choosing an encryption algorithm to encrypt data, the encryption algorithm should be chosen with sufficient complexity to eliminate the possibility of deciphering directly from the ciphertext. At the same time, in the process of encrypting sensitive data, the security of data storage is also worthy of attention. This problem can be achieved by using access control methods. For network and various system administrators, users and data can be classified according to different applications and data types, and different access rights can be granted respectively.

(2) Security at the network layer
The main function of the firewall is to effectively prevent illegal external access and prevent the leakage of internal data. Under normal circumstances, the three technologies of channel packet filtering, proxy and state analysis are the key technologies commonly used by firewalls. However, there are only host-based intrusion detection systems, feature-based and abnormal intrusion detection systems, and real-time and non-real-time intrusion detection systems that are very effective. In the network system, digital signature technology can effectively ensure the security and integrity of information. Subsequently, a collaborative intrusion detection technology was proposed, which was proposed to solve the deficiencies of independent intrusion detection. For various illegal intrusions that have
occurred widely, independent intrusion detection technology cannot effectively detect. However, cooperative intrusion detection is different from independent intrusion detection. In the former, each intrusion component will automatically exchange information, and various illegal intrusions can be obtained through the exchanged information, so that the detection can be effectively made.

(3) Security technology of the database management system layer (DBMS)
To be precise, the security of the database depends entirely on the database management system to a certain extent. This is enough to show that the security intensity of the database management system is much higher than the other two levels, because it has a very powerful security mechanism. The DBMS is the last major gate of database security, which means that when the security of the network system layer and the user operating system layer is completely breached, there is still the last security barrier of the DBMS to ensure the security of the database.

2.5. Algorithm
All nodes in the network must periodically calculate and evaluate their own energy information. Because of the wrong energy information, errors in the selection of fusion nodes and packet loss will occur. The energy of a node is usually calculated using the following formula:

\[ E_{te} = E_0 - \frac{E_t}{E_0} \]  \hspace{1cm} (1)

Among them, \( E_0 \) represents the initial energy of the node, and \( E_t \) represents the energy information of the node at time \( t \). According to the interactive data of the activities of each network, the corresponding trade-off value can be obtained by calculation in the following way:

\[ W(A_i) = \frac{NI(A_i)}{TNI} \]  \hspace{1cm} (2)

Among them, represents the sum of the interactive data of all network activities. It is calculated in the following way:

\[ TNI = \sum_{i=1}^{3} NI(A_i) \]  \hspace{1cm} (3)

Through the calculation of these evaluation factors, the value range of the total trade-off of network activities lies in \([0,1]\).

3. Experimental Research on the Application of WSN in the Security Management of Sensitive Data in the Data Center under the Big Data Environment

3.1. Experimental Subjects and Data
This experiment takes the sensitive data security management requirements and application scope of WSN in data as the experimental object. Through actual investigation, it discusses the security management requirements of sensitive data in WSN data and analyzes from different directions. The application scope of WSN in sensitive data security management.

3.2. Data Collection
In this experiment, data was collected through a group survey, and various data were collected and sorted according to the assigned tasks, and the final experimental data was obtained.
4. Experimental Research and Analysis of the Application of WSN in the Security Management of Sensitive Data in the Data Center under the Big Data Environment

4.1. Analysis of the Demand for the Security Management of Sensitive Data in the Data Center by the WSN

This experiment conducted an experimental research on the security management requirements of sensitive data in the data center of the WSN. The experimental research results are shown in Table 1:

| Safety requirement category | Numerical value | Degree of demand |
|-----------------------------|----------------|------------------|
| Data confidentiality        | 0.4715         |
| Data integrity              | 0.2436         |
| Data freshness              | 0.2849         |

As shown in Figure 1, the most demanded level in security management is data confidentiality, which is 47.15%, followed by data freshness and data integrity, which are 28.49% and 24.36%, respectively. In summary, it is necessary to increase efforts to improve the security management of sensitive data.

4.2. Application Analysis of WSN in Sensitive Data Security Management

This experiment conducted an experimental study on the application of WSN in the security management of sensitive data, and compared the scope of its application. The experimental research results are shown in Table 2:

| Safety requirement category | Scope of application |
|----------------------------|---------------------|
| Data Security              | 38.41%              |
| Network Security           | 33.74%              |
| system security            | 27.85%              |
As shown in Figure 2, the most widely used area is data security, which is 38.41%, followed by network security, which is 33.74%, and the last is system security, which is 27.85%. On the whole, the application is not very comprehensive, and further improvements are needed.

5. Conclusion
WSN security is an open and active field. As the application of big data technology becomes more and more extensive, the requirements for data security are getting higher and higher, and there are many security threats to sensitive data. We all need to strengthen prevention and deal with various attacks and other illegal activities to prevent confidentiality. In WSN, sensor nodes developed and designed according to application requirements can collect information on monitoring targets, and at the same time act as intermediate nodes to forward data packets from other nodes to the base station. This article discusses the security management requirements of sensitive data in the WSN based on big data technology. It analyzes the problems in the security management of sensitive data from different directions, and implements the application of WSN in the security management of sensitive data in response to these problems, and provides some help to solve the problem.

References
[1] Tang C, Tan Q, Han Y, et al. An Energy Harvesting Aware Routing Algorithm for Hierarchical Clustering Wireless Sensor Networks [J]. KSII Transactions on Internet and Information Systems (TIIS), 2016 (2): 504 - 521.
[2] Suhag D, Gaur S S, Mohapatra A K. A proposed scheme to achieve node authentication in military applications of wireless sensor network [J]. Journal of Statistics and Management Systems, 2019, 22 (2): 347 - 362.
[3] Hayette B, Boucif A B, Ismail B. A lightweight key management scheme based on an Adelson-elskii and Landis tree and elliptic curve cryptography for wireless sensor networks [J]. Concurrency & Computation Practice & Experience, 2016, 28 (6): 1831 - 1847.
[4] Batra I, Verma S, Kavita, et al. A lightweight IoT-based security framework for inventory automation using wireless sensor network [J]. International Journal of Communication Systems, 2019, 33 (2): e4228.
[5] Khan T, Singh K, Le H S, et al. A Novel and Comprehensive Trust Estimation Clustering Based
Approach for Large Scale Wireless Sensor Networks [J]. IEEE Access, 2019, PP (99): 1 - 1.

[6] He D, Chan S, Yan Z, et al. Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks [J]. IEEE Journal of Biomedical & Health Informatics, 2017, 18 (2): 440 - 448.

[7] Zafar F, Khan A, Suhail S, et al. Trustworthy Data: A Survey, Taxonomy and future trends of Secure Provenance Schemes [J]. Journal of Network and Computer Applications, 2017, 94 (sep.): 50 - 68.

[8] Tan S, Li X, Dong Q. A Trust Management System for Securing Data Plane of Ad-Hoc Networks [J]. IEEE Transactions on Vehicular Technology, 2016, 65 (9): 7579 - 7592.

[9] Mohamed, S, Abdalzaher, et al. Using Stackelberg game to enhance cognitive radio sensor networks security [J]. IET Communications, 2017, 11 (9): 1503 - 1511.

[10] Jiang J, Zhu X, Han G, et al. A Dynamic Trust Evaluation and Update Mechanism based on C4.5 Decision Tree in Underwater Wireless Sensor Networks [J]. IEEE Transactions on Vehicular Technology, 2020, PP (99): 1 - 1.

[11] Arshad M, Ullah Z, Khalid M, et al. Beacon trust management system and fake data detection in vehicular ad-hoc networks [J]. IET Intelligent Transport Systems, 2019, 13 (5): 780 - 788.

[12] Erlantz F, Jorge B, Jon M, et al. A Method for Dynamically Selecting the Best Frequency Hopping Technique in Industrial Wireless Sensor Network Applications [J]. Sensors, 2018, 18 (2): 657.