Network Security from the Perspective of the Internet of Things

Ang Zhou1,*

1Beijing University of Posts and Telecommunications, Beijing, 100876, China

*Corresponding author e-mail: zhouang1@bupt.edu.cn

Abstract. Networking is one of the new technologies supported by our country's national "125" strategic industry plan, mainly used in medicine, military industry, transportation and other fields. While enjoying the convenient business of the Internet of Things, people also pay more attention to the security of the Internet of Things information system. Therefore, this article mainly discusses security under the perspective of the IoT, and understands the relevant basic theoretical knowledge about the IoT and security on the basis of a large number of documents, and then conceives the security methods under the perspective of the IoT, and the designed method has been tested, and the test results show that the performance of the encryption algorithm in the network security scheme of this article is due to the traditional encryption algorithm. When the encrypted text is 15000 bytes, the encryption time is 40s.

Key words: Internet of Things, Network Security, Security Solutions, Encryption Algorithms

1. Introductions
The Internet of Things uses intelligent detection devices to collect and transmit real-time signals to complete the connection between objects and the Internet [1-2]. The IoT has become an eye-catching frontier of science and technology, and it will have an important impact on the development of social productivity in the 21st century [3-4]. The IoT is also a "great productivity" that will promote the rapid growth of the global economy and society in the future, so it has attracted the attention of domestic and foreign researchers. In the national "Twelfth Five-Year Plan", the concept of "IoT" was first written into the labor report of the Chinese government [5-6]. With the support of our country's national sustainable development strategy, national technological innovation strategy and manufacturing promotion strategy, the IoT has become a major innovation strategy in our country [7-8].

Regarding the research on the IoT, some researchers believe that the IoT has huge growth potential and attractive growth prospects. First of all, the development of the IoT contains endless business opportunities. After decades of continuous development, traditional communication networks can communicate with people anytime and anywhere. However, more applications will require networks to further realize the communication between things and the Internet, which will bring quality to human life variety. By 2020, the ratio of the application of the "IoT" business to human-to-human communication will reach 30:1, and data shows that the value of the IoT business will reach trillions...
of dollars. Secondly, the IoT will have a wider range of applications. The development of the IoT technology is gradually improving, and the accuracy and real-time of its data, as well as the efficiency and accuracy of management, are all inevitable steps in the development of technology [9]. As a new technology, some researchers believe that it will always face some difficulties and challenges. The data transmission process of IoT applications involves uploading data from sensor devices and user instructions. The accuracy of information transmission is directly related to the accuracy of the application. Most of the data transmitted to the IoT contains sensitive content such as user privacy, so it has a close impact on personal privacy and social stability and harmony. In a word, realizing the confidentiality, integrity and identity of IoT data sharing is an important issue to be solved urgently, and it is also a research hotspot [10]. For the security research of the IoT, some scholars have proposed a password-protected user authentication scheme in a hierarchical wireless sensor network environment, but this scheme is easy to crack and cannot meet higher security requirements. In terms of key distribution and management, network-wide pre-distribution models and random key pre-distribution have been continuously proposed in recent years [11]. In summary, the application potential of the IoT is huge, but security problems inevitably arise, and the security problems of the IoT need to be solved urgently.

This article conducts research on network security from the perspective of the IoT, analyzes the architecture of the IoT and the security issues of the IoT on the basis of literature data, and then designs a security solution based on the IoT for the problem, and then tests the design solution. The test results draw relevant conclusions.

2. Research on Cyber Security and IoT

2.1. The Architecture of the IoT

Now, EPCGlobal's IoT architecture is the most representative of the well-known IoT architecture. Its main components are EPC coding technology, EPC tags, EPC readers, ONS servers and EPC middleware [12]. Due to the different capabilities of the IoT system architecture, it can be divided into three levels: the perception level, the lower level used to collect information, and the network level, which also belongs to the middle level grade. The perception level is the application/middle level used for data transmission. Figure 1 shows the architecture diagram of the IoT.
2.2. IoT Security Issues
(1) At the perception level, the security protection of the perception layer is the security of the network itself, because its operation is performed by the wireless sensor network, acquiring the data information of the sensor node, and connecting to the external network through the gateway. The sensor nodes of the IoT generally have limited resources, weak computing power, and rich resources, so relatively large-scale security measures commonly used on the Internet are adopted. Therefore, the perception level must not only meet the security goal, but more importantly, apply the cryptographic mechanism to lighter weights and reduce resource consumption. In general, the perception layer needs to provide specific security solutions based on security requirements such as secure routing, identity verification, intrusion detection, and key management. Perception-level sensor nodes are vulnerable to attacks from other networks. In particular, denial of service can paralyze the entire network. Therefore, the sensor nodes in the wireless sensor network must be able to resist denial of service attacks.

(2) At the network level, the data transmission format is IP datagram, and each IP datagram contains individual information such as TCP, UDP, Internet Control Message Protocol, and Internet Group Message Management Protocol. These IP datagrams are sent directly from one host to another through network transmission technology, making the network layer extremely vulnerable to attackers. End-to-end can also achieve terminal security at the network level, which requires the creation of corresponding key sharing, key management and identity verification mechanisms.

2.3. Security Algorithm
First, define the inverse sequence transformation method as: $R(Q_0, Q_1, Q_2, Q_3) = (Q_3, Q_2, Q_1, Q_0)$, where $Q_i \in Z_{32}^2$, $i=0, 1, 2, 3$ assume that the input plaintext m is $(M_0, M_1, M_2, M_3) \in (Z_{32}^2)^4$, the output ciphertext is $(C_0, C_1, C_2, C_3) \in (Z_{32}^2)^4$, and the round key is $rK_i \in Z_{32}^2$, $i=0, 2, .. 31$. Then the encryption process of SM4 algorithm is:
\[ M_i \in \mathbb{R} = F(M_1, M_{i+1}, M_{i+2}, rK_i) \]
\[ (C_0, C_1, C_2, C_3) = R(M_{32}, M_{33}, M_{34}, M_{35}) \]

3. Cyber Security Solutions from the Perspective of the IoT

3.1. IoT Authentication Method
The IoT only guarantees the legitimacy of network access devices, which means that the collected information requires a strict IoT authentication mechanism, because it only guarantees the accuracy and reliability of the source. Nowadays, in the IoT, many wireless sensors are deployed in no man's land, making the equipment extremely vulnerable to physical damage or intrusion by attackers using illegal identities. Authentication is to determine whether a user is accessing a specific resource and has a specific usage authority, allowing both parties to establish a trust relationship to ensure the reliability of the data at the starting point. If a major relay node is detected during the collaborative data transmission process between sensor nodes, the entire network will face a huge security threat. In addition, although the sensor nodes themselves in harsh environments have passed the certification, physical damage may occur, the operation of the nodes may become unstable, and the accuracy of collected information may be reduced, which is also uncertain. The information collected in this case is not only meaningless, but also affects the judgment of the actual target person. At the same time, the information of the damaged node will consume a large amount of energy of other nodes in the network during the transmission and transfer process, resulting in a waste of resources.

The solution in this paper first performs two-way authentication on the communication part to prevent sensor nodes from accessing forged network system IDs. Two types of random numbers are used in the process of sending sensor node ID information. Even if the ID information is intercepted during the transmission process, it is difficult for an attacker to accurately analyze the sensor node ID information, because two types of random numbers are applied, which effectively resist repeated attacks, and by introducing a backup node, the original faulty sensor can be replaced. Collecting data in time to ensure business continuity. This solution also introduces the early warning mechanism of various alarm information displayed by the sensor node status monitoring device and the terminal base station, which can not only improve the security of the sensor node authentication, but also detect the performance and operating status of the equipment. This greatly improves the reliability of the sensor node data, confirms the accuracy of the collected information, and reduces the consumption of network resources by the transmission of information. The terminal will collect and verify the actual information based on the actual actual information to eliminate the interference of invalid data information. In the case of sensor damage, personnel can also perform various steps to repair the sensor in time to reduce system costs.

3.2. Intrusion Detection Methods
(1) Since the monitoring node and the cluster head node cannot be the same node, the monitoring node can also be the monitored cluster head node. In the static phase, the monitoring node monitors the communication content in real time, and sends an alarm message directly to the base station if a threat is detected. This process is mainly divided into the following processes to complete:

1) Data collection
At this stage, the information collected is messy. The terminal will filter the information before saving to facilitate subsequent analysis. Save the exported valid data in the terminal, and discard it after a period of time or the memory space is exhausted.

2) Application rules
At this stage, the stored data is controlled by standard rules. If the information of a specific rule fails, the number of cancellations will increase by one.
3) Intrusion detection
At this stage, the statistical analysis technique of the intrusion detection system is used to compare the cumulative number of failures with a given random damage limit. If the first is greater than the second, it is considered an invasion. In other words, if the number of abnormal behavior exceeds a certain limit, the monitoring node will consider it an intrusive behavior.

4) Send alarm information.
The monitoring node sends alarm information to the base station.

5) Blacklist management.
After each round, all invading nodes are included in the blacklist, and no longer accept the information sent by the nodes in the blacklist, and the nodes in the blacklist are no longer selected as cluster heads.

(2) Detection rules
Intrusion detection systems usually use three technical tools: pattern matching, statistical analysis, and completeness analysis. This detection system is mainly based on statistical analysis methods. The specific detection rules are as follows:

1) Space rules
If the interval between two consecutive messages monitored by the watch node is not within the default range, it is invalid. In this scenario, this rule is used to detect DoS and snub attacks. In a DoS attack, malicious nodes continuously send cluster head applications to the network, and the time interval between successive application messages is relatively short. In an offensive attack, if some nodes become the target of the attack or cause energy diffusion due to other reasons, the normal information transmission will be insufficient, and the interval between consecutive messages will be very long.

2) Repeat rules
The number of times the same message is sent from the same node must be within a certain range. This rule can detect duplicate and DoS attacks.

3) Unlimited transmission range rule
The intensity of the information sent by the node must be within a certain range, and very strong information is considered a neighborhood flooding attack.

3.3. Key Management Scheme
(1) The security gateway node inserts the remote key management scheme. As a CA, the security gateway node issues certificates to the gateway node and the cluster head node, manages security certificates, and the communication between the gateway node and the cluster head node does not involve the security gateway node. The security gateway node is mainly composed of five parts: the main control panel, the security management module, the key agreement module, the authentication module, and the encryption and decryption module. Among them, the main control panel is the control center. The key agreement module and the authentication module are used to implement key agreement and authentication between nodes, and use the generated key as the encryption and decryption key of the encryption and decryption module. The encryption and decryption module is used to realize the encryption and decryption functions in the data. The security management module mainly performs key management and certificate management on cluster head nodes and gateway nodes. According to whether the gateway node is connected to the IP network to send data to the cloud platform, the WSN mode is divided into offline mode and offline mode. Among them, in the web mode, the gateway node manages the keys and certificates on the nodes in the WSN. In offline mode, the security gateway node selects the gateway node and the cluster head node to form a security
management network. The security gateway node updates the gateway node and cluster head node certificates and the public CA key used for authentication.

(2) In the peripheral key management system, cluster head nodes and ordinary nodes are indistinguishable. The session key between nodes in the area uses the Blom matrix to generate the master key. This model allocates a different key space for each network area, and then assigns each node key to it according to the development information, such as information.

4. Scheme Testing and Evaluation
First test the encryption method and symmetric key algorithm in this article to test the communication efficiency of the secure communication layer. The test time is in seconds, and each indicator is obtained by testing 20,000 times and calculating the average value. Table 1 shows the results of the 128-bit key encryption and decryption test.

| Messenge length/byte | AES_CBC_PKCS5Padding | The algorithm of this article | AES_CTR_PKCS5Padding |
|----------------------|----------------------|-------------------------------|----------------------|
| 15                   | 18                   | 16                            | 18                   |
| 150                  | 18                   | 17                            | 18                   |
| 1500                 | 19                   | 17                            | 18                   |
| 15000                | 20                   | 19                            | 21                   |
| 150000               | 151                  | 40                            | 139                  |

In Figure 2, the x-axis represents the length (in bytes) of the randomly generated text. The y-axis is the average time of each test, in seconds. As shown in the figure, if the text length is about 15 to 15000 bytes, there is not much difference between encryption and decryption time. As the text length increases to 150,000 bytes, the algorithm model in this document has great advantages.
5. Conclusions
This article focuses on the research of network security from the perspective of the IoT. After understanding the relevant theories, design the network security plan from the perspective of the IoT, and test the designed plan. Through the test of the encryption algorithm, it can be concluded that the algorithm of this article There are significant advantages in encryption time.

References
[1] Heinz Weiskirchner, Manfred Bürger. Herausforderungen zur Schließung von IoT Security-Lücken[J]. Elektrotechnik und Informationstechnik, 2019, 136(4-5):a33-a34.
[2] Kudithi T , Sakthivel R . High-performance ECC processor architecture design for IoT security applications[J]. Journal of Supercomputing, 2019, 75(1):447-474.
[3] Schneier, Bruce. IoT Security: What's Plan B?[J]. IEEE Security and Privacy Magazine, 2017, 15(5):96-96.
[4] Rodrigo R C , Javier L , Stefanos G . Evolution and Trends in IoT Security[J]. Computer, 2018, 51(7):16-25.
[5] Zhou L , Niu X , Zhao S , et al. Research on congestion rate of classified storage narrow channel picking system for IoT security[J]. Wireless Networks, 2020:1-17.
[6] Guo C , Li D . IOT security privacy protection mechanism and mechanical structure design simulation optimization[J]. EURASIP Journal on Advances in Signal Processing, 2021, 2021(1):1-14.
[7] Alzubi O A , Alzubi J A , Dorgham O , et al. Cryptosystem design based on Hermitian curves for IoT security[J]. The Journal of Supercomputing, 2020, 76(11):8566-8589.
[8] Yao S , Li Z , Guan J , et al. Stochastic Cost Minimization Mechanism Based on Identifier Network for IoT Security[J]. IEEE Internet of Things Journal, 2020, 7(5):3923-3934.
[9] Aufner P . The IoT security gap: a look down into the valley between threat models and their implementation[J]. International Journal of Information Security, 2020, 19(1):3-14.
[10] Du M , Wang K , Liu Y , et al. Spacechain: A Three-Dimensional Blockchain Architecture for IoT Security[J]. IEEE Wireless Communications, 2020, 27(3):38-45.
[11] Iqbal W , H Abbas, Daneshmand M , et al. An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security[J]. IEEE Internet of Things Journal, 2020, PP(99):1-1.
[12] Sen B . PUF: a new era in IoT security[J]. CSI Transactions on ICT, 2020, 8(2):185-191.