Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 9, No. 1, 2024

Internet of Things (IoT) Computer Network Security and Its Remote Control Technology: Key Points and Applications

Kong Cheng

Nanjing Institute of Product Quality Inspection (Nanjing Institute of Quality Development and Advanced Technology Application), Nanjing Jiangsu 210000, China

Abstract: With the development and advancement of science and technology, communication devices have been widely developed and utilized. Among these, internet technology plays a comprehensive role in promoting the development of various industries in its practical application. The Internet of Things (IoT) is a particularly important technological form, significantly enhancing the efficiency of information transmission and sharing, and aiding in the rational implementation of data transmission and information sensing technologies. The security risks of IoT are mainly manifested in three levels: the intelligent perception layer, the access and transmission layer, and the business application layer. In the analysis of this article, the key points and characteristics of IoT computer network security, remote control technology, and computer remote control system structure analysis are mainly elaborated.

Keywords: Science and Technology; Internet of Things (IoT); Remote Control.

1. Introduction

In the development of modern society, to further enhance the efficiency of industry development, it is necessary to actively introduce information technology and strengthen the processing capability of intelligent information. However, to ensure the security of the entire information transmission and sharing, it is also necessary to pay attention to the security of information and remote control capabilities to maximize the value of the information.

2. Internet of Things (IoT)

The IoT is an information system that involves perception, network, and application layers. The perception layer deals with sensing information and is the core of building the IoT, equipped with various types of sensors, smart cards, and related equipment. It can identify and analyze objects and play a role in processing control. The network layer is responsible for information transmission, receiving information collected and recognized by sensors, and processing information through network transmission. The application layer is responsible for information processing in the system, analyzing a large amount of data deeply to mine valuable information content. These three layers coordinate with each other, allowing various objects and devices to form a close association and enhance the effectiveness of information technology [1].

3. Current Status of IoT Computer Network Security

3.1. Communication Security

As the user is the subject of the computer network, there are certain network security issues when the network capacity is limited or there are insufficient communication terminals. For example, network congestion can lead to a large amount of signaling traffic. The current authentication method mainly involves a large number of terminals applying for network connections in a short period of time. Furthermore, the management of encryption keys is relatively complex. After a large number of terminals apply to access the network, a large number of complex protection keys will appear, consuming a lot of network resources during the authentication process. Finally, there are risks associated with transmission security. The main process of information transmission occurs at the network layer. Therefore, encryption algorithms are used to ensure the security of information transmission. However, the use of complex encryption algorithms can lead to communication delays, providing an opportunity for network attackers to find pathways for intrusion and carry out malicious attacks[2].

3.2. Perception Layer Security

The perception layer in the IoT faces certain security issues as it is responsible for information sensing. For example, after RFID is embedded in various items, the items can be passively scanned, located, and tracked immediately. Additionally, there may be interference in processing sensing information. To ensure rational processing, wireless connections are used, leading to strong signal openness and making it easier to suffer from network attacks, resulting in serious network security issues.

4. IoT Computer Network Security Control

4.1. Encryption Mechanism

In network security protection work, rational encryption processing methods are used, such as hop-by-hop encryption and end-to-end encryption. In the application of hop-by-hop encryption technology, the different transmission nodes in the network layer are subject to targeted decryption, encryption, and processing. This has the characteristics of low latency, scalability, and high efficiency. In future processing, the security encryption mechanism can ensure the transparency of the entire encryption process. End-to-end encryption,

mainly based on the type of business, carries out rational encryption processing. Both the exposed locations and endpoints of the information need to be processed accordingly. Generally, to further enhance the encryption level of IoT, hop-by-hop encryption is chosen to ensure the security and reliability of new information without bringing certain encryption risks[3].

4.2. Establishing Privacy Protection Mechanisms

In the process of adopting privacy protection mechanisms, this is a key technical form of security maintenance for the IoT. It can be processed based on authentication mechanisms, encryption mechanisms, and access control. Among them, in the processing of authentication mechanisms, the authenticity and reliability of data information are determined after identifying the data sending end, and some illegal user operations are organized to further enhance the security of data information.

4.3. Security Routing Protocol

IoT routing mainly crosses various types of network forms, and the compliance with security routing protocols has become an important component of security management. It is a form of location protection for each node in the wireless sensor network system. Based on the specific probability of forwarding nodes, data packets are transmitted to specific aggregation node locations. The variable transmission path is not easily attacked, so this processing method can greatly increase security and resilience. It is a security technology that avoids being affected by the external environment and can also be integrated with key encryption technology to achieve centralized processing of transmitted data packets.

5. Computer Remote Control System Structure Analysis

5.1. Main Control Network

In the processing of the main control network, it is first necessary to analyze the control process of the network system, which is also an important basis for network reference. The functional design of the main control network involves two processes: control command and parameter input, which are the operating behaviors of the controlled devices. Feedback information can be displayed centrally. The architecture of the main control network is divided into centralized, decentralized, and hierarchical forms. Different types of structures have different operational difficulties. To enhance the processing effect, it is necessary to combine the operating conditions of the system and make rational security adjustments. However, in actual operation, due to high costs and technical installation difficulties, such technical processing methods cannot facilitate resource sharing of information. In the future, during the processing of decentralized control systems, the stability of the network system will not be easily affected by the controller, and it will be impossible to control and observe the system state. In the processing of hierarchical control structures, it is necessary to strengthen the integration effect between decentralized control structures, and the local control links also need to form a coordinated control mechanism.

5.2. Controlled Network

The construction of the controlled network primarily aims to maintain an effect independent of the main control network. Especially, it needs to be based on network control theory, utilizing software, hardware, and various processing methods to form a comprehensive execution effect, and consistently provide certain control services. In the subsequent processing of a general controlled network, certain data resources will be formed. Or, centered around computer processing, combined with on-site control, data collection, and various control information content, a specific operational form and logic are formed, which can well meet the quality and effectiveness of system operation. In the subsequent security and control processing, maintaining a strong security level and hierarchical processing ensures that the system meets the basic requirements of remote control.

5.3. Communication Protocols

In the design of computer remote control systems, communication protocols are relatively complex, involving mainly IP and TCP protocols. The TCP protocol is a very common basic form in network protocols, with strong security and stability. It is a connection-based protocol that can establish processes between two different terminals, thus realizing the exchange and processing of data. Furthermore, with return notifications and sequence numbers, it greatly enhances the reliability of data transmission. By restoring various data packets to their original data segments, centralized processing of various data information can be achieved. Supporting and utilizing byte stream processing methods enables a more comprehensive replacement of data by various IP-linked sequences, and correspondingly strengthens the overall level of processing.

The adoption of the IP protocol is a method of forming an exchange network based on multiple connection terminals during the connection process. This data transmission method transfers data packets from the source address. The protocol involves several key pieces of information technology. Service type is a parameter information, mainly serving gateways to realize the transmission of specific networks and information. Furthermore, regarding the treatment of time to live (TTL), if data information cannot obtain relevant content during the transmission process, it will reach a time limit and be automatically discarded. In terms of option settings, it involves the targeted selection processing of security, timestamps, and special routing, thereby achieving control and adjustment of information content. With the development and progress of information technology, the overall processing effect is becoming more apparent. Specific verification is needed to enhance the capability of technical processing effectively.

6. Conclusion

In summary, in analyzing the security of the IoT computer network, it is necessary to analyze internet technology from multiple perspectives, and simultaneously strengthen the subsequent processing of remote control technology, thereby ensuring the security of the entire system operation.

References

[1] Yang Haiwei. Analysis of Computer Network Security in Oilfield Internet of Things [J]. Network Security Technology and Application, 2022(09):111-112.

[2] Luo Zhenying. Analysis of Computer Network Security Based on the Internet of Things [J]. Information Recording Materials, 2022, 23(08):17-19.

[3] Lu Shang. Analysis of Computer Network Security Based on the Internet of Things [J]. Network Security Technology and Application, 2022(02):19-20.

[4] Chen Zhenfeng. Preliminary Discussion on the Impact of the Internet of Things on the Development of Computer Network Technology [J]. Science and Technology Wind. 2016 (10):145.

[5] Wang Kan, Jiang Yanyun, Zhang Yi. Big Data Industry Application in the Context of Industrial Internet [J]. Information and Communications Technology. 2017, 11 (4): 15-20.