Theory and Practice of Science and Technology
2025, VOL. 6, NO. 6, 11-15
DOI: 10.47297/taposatWSP2633-456902.20250606

Research on Multi-layer Real-time Encryption Transmission Technology Based on 5G Wireless Communication

Wenxin Ge

School of Artificial Intelligence and Electrical Engineering, Guangzhou College of Applied Science and Technology, Zhaoqing, Guangdong, 526072, China

ABSTRACT
With the rapid development of 5G communication technology, extremely high requirements have been put forward for the security of data transmission. Aiming at the 5G network environment, this paper aims to design a multi-layer real-time encryption transmission technology to balance security and real-time performance. Through methods such as literature research, comparative analysis, technical implementation and testing, a scheme for the collaborative work of multi-layer encryption is proposed and verified in a simulated 5G network environment. The results show that this scheme can significantly improve the security and real-time performance of data transmission in 5G networks, providing a strong security guarantee for the widespread promotion of 5G applications.

KEYWORDS
5G wireless communication; Multi-layer encryption; Real-time encryption; Data transmission security; Encryption collaborative work

1 Introduction

1.1 Research background and significance

In recent years, 5G communication technology, with its characteristics of high speed, low latency and large connectivity, has become a key force in promoting the digital transformation of society. From the ultimate network speed experience of smart phones to the extensive applications in fields such as the industrial Internet, autonomous driving, and telemedicine, 5G is reshaping people's lives and the industrial landscape. However, with the explosive growth of data traffic in 5G networks and the continuous expansion of application scenarios, the security issues of data transmission have become increasingly prominent.

The openness of 5G networks, the mobility of wireless terminals, and the complex network architecture make it face various security threats such as APT attacks, DDoS attacks, information eavesdropping, and tampering. In some scenarios with extremely high requirements for security and real-time performance, such as in autonomous driving, a large amount of critical information needs to be transmitted securely and in real-time between vehicles (V2V) and between vehicles and infrastructure (V2I). If the data transmission is attacked or delayed, it may lead to serious traffic accidents. In telemedicine, when doctors perform real-time surgical operations on patients, the secure and timely transmission of data is directly related to the patient's life safety.

Traditional single encryption technologies are no longer sufficient to meet the needs of the 5G era. On the one hand, simple encryption algorithms cannot provide sufficient security in the face of increasingly powerful computing power and complex attack methods. On the other hand, although complex encryption algorithms can enhance security, they will bring high computational overhead and processing delays, affecting the real-time performance of data transmission. Therefore, designing a multi-layer encryption transmission technology that can balance security and real-time performance is of great practical significance for the continuous development and widespread application of 5G communication technology.

1.2 Domestic and foreign research status

In the field of 5G data encryption, scholars at home and abroad have conducted a large number of studies. In terms of physical layer encryption, some studies utilize the inherent characteristics of wireless channels, such as channel fading and noise, to encrypt data by changing signal characteristics. For example, a physical layer encryption method based on artificial noise injection has been proposed. Without affecting the signal quality of the legitimate receiver, artificial noise is added to the transmitted signal to interfere with the reception of eavesdroppers, thereby improving transmission security. However, the performance stability of this method in actual complex environments remains to be further improved.

In terms of network layer encryption, common methods include the IPsec protocol. By encrypting and authenticating data packets at the network layer, the security of data during network transmission is ensured. However, these traditional network layer encryption schemes may face problems such as complex key management and low encryption efficiency in scenarios of large-scale device connections and high traffic transmission in 5G networks.

In addition, some studies focus on application layer encryption, which protects the data of specific applications by implementing encryption functions in application programs. However, this approach often depends on the security awareness and technical level of application developers and lacks systematicness and universality.

Overall, although existing research has achieved certain results in 5G data encryption, there are still deficiencies in balancing security and real-time performance, making it difficult to meet the stringent requirements of diverse 5G application scenarios.

2 Research objectives and contents

2.1 Research objectives

This study aims to design a multi-layer encryption scheme to significantly enhance the security of data transmission in 5G networks, ensuring that data is not stolen, tampered with, or forged during the transmission process. At the same time, real-time factors are fully considered during the encryption process to ensure that encryption and decryption operations do not introduce excessive delays, meeting the extremely high real-time requirements of application scenarios such as autonomous driving and telemedicine.

2.2 Research contents

2.2.1 Research on encryption technologies at different layers

Physical Layer Encryption Technology: Deeply explore methods of encrypting data by utilizing the characteristics of 5G signals. Research involves adjusting parameters such as the amplitude, phase, and frequency of signals, enabling the signals to be correctly demodulated at the legitimate receiver while appearing as noise to eavesdroppers. For example, by using the massive MIMO technology of 5G, specific encoding and modulation of signals transmitted by different antennas are carried out to achieve spatial - dimensional encryption of signals, increasing the difficulty of eavesdropping. Data Link Layer Encryption Technology: Conduct research and selection on block encryption algorithms. Evaluate the applicability of classic block encryption algorithms such as AES and SM4 in the 5G data link layer, considering factors such as the encryption strength, computational complexity of the algorithms, and their compatibility with 5G network protocols. Study how to optimize the implementation of the algorithms to improve the efficiency of encryption and decryption, ensuring the security of data while processing a large number of data packets quickly at the data link layer. Network Layer Encryption Technology: Analyze the feasibility and optimization schemes of implementing encryption at the 5G network layer. Research how to improve traditional network layer encryption protocols, such as IPsec, to adapt to the characteristics of high speed, low latency, and large-scale connections of 5G networks. Explore new key management mechanisms to reduce the complexity and overhead of key management and improve the overall performance of network layer encryption.

2.2.2 Realization of multi-layer encryption collaborative work

Design a multi-layer encryption architecture to ensure seamless connection of encryption technologies at the physical layer, data link layer, and network layer. In this architecture, encryption algorithms at different layers work together in a specific order and according to certain rules, forming an organic whole. For example, physical layer encryption provides preliminary security protection for data, preventing simple signal eavesdropping; data link layer encryption further encrypts data packets to ensure the integrity and confidentiality of data during link transmission; network layer encryption is responsible for the overall protection of data during network transmission.

Through the design of reasonable interfaces and interaction mechanisms, information sharing and collaboration among encryption algorithms at various layers are achieved. For example, the network layer can dynamically adjust the encryption strategy according to the channel state and link quality information fed back by the physical layer and data link layer to adapt to changes in the network environment.

2.2.3 Performance optimization of encryption algorithms

Carry out targeted improvements to the selected encryption algorithms to reduce the encryption and decryption time. Improve the execution efficiency of the algorithms by optimizing the calculation process and adopting hardware acceleration technologies. For example, use dedicated encryption chips or GPUs to accelerate the calculation of the AES algorithm, reducing the occupation of system resources by encryption and decryption operations and thus reducing processing delays.

Use programming technology to implement the designed multi-layer encryption architecture and conduct comprehensive tests in a simulated 5G network environment. By simulating different network topologies, traffic flows, and channel conditions, evaluate the security and real-time performance of the encryption architecture in various scenarios, providing a basis for further optimization.

3 Research methods and technical routes

3.1 Research methods

3.1.1 Literature research method

Systematically review domestic and foreign literature on 5G communication technology, data encryption technology, and related security fields. Sort out the research ideas, methods, and achievements of predecessors in 5G data encryption, analyze the advantages and disadvantages of existing research, and provide a theoretical basis and research ideas reference for this study.

3.1.2 Comparative analysis method

Conduct a comprehensive comparison between the designed multi-layer encryption scheme and existing 5G data encryption schemes. Analyze from multiple dimensions such as security, real-time performance, computational complexity, and key management, clarify the innovative points and improvements of this scheme, and provide directions for the optimization and improvement of the scheme.

3.2 Technical routes

Encryption Technology Screening Stage: Conduct a comprehensive analysis and evaluation of existing encryption technologies, and select suitable encryption algorithms according to the characteristics and requirements of different layers of the 5G network. For example, select signal modulation-based encryption technologies according to the signal processing characteristics of the physical layer, select efficient block encryption algorithms according to the packet processing requirements of the data link layer, and select appropriate network layer encryption protocols according to the routing and transmission characteristics of the network layer. Multi-layer Encryption Architecture Design Stage: Design a multi-layer encryption collaborative work architecture, clarify the interfaces, interaction methods, and collaboration rules among encryption technologies at various layers. Ensure that encryption algorithms at different layers can be organically combined under this architecture to jointly provide security protection for data transmission. Implementation and Testing Stage: Implement the designed multi-layer encryption architecture through programming, and build a test platform in a simulated 5G network environment. The platform includes simulated base stations, terminal devices, and network links, simulating different network loads, channel conditions, and service types. Design rich test cases to comprehensively test the data transmission security and real-time performance of the encryption architecture, and collect and record key indicators such as encryption time, decryption time, and data transmission success rate. Optimization Stage: Optimize the encryption architecture according to the test results. For problems in security and real-time performance, adjust the parameters of the encryption algorithm, improve the architecture design, or optimize the implementation code. For example, if the encryption time is too long, further optimize the calculation process of the algorithm or increase hardware acceleration measures; if the security is insufficient in specific scenarios, adjust the encryption strategy or increase the encryption strength. After multiple rounds of optimization, conduct test verification again until the expected security and real-time performance goals are achieved.

4 Experimental scheme and result analysis

4.1 Experimental scheme

Simulation Environment Construction: Build a simulated 5G network environment, including multiple simulated base stations, terminal devices, and network links. The simulated base stations are responsible for simulating the signal transmission and data processing functions of 5G base stations, and the terminal devices simulate various 5G user devices and application scenarios, such as autonomous driving vehicles and telemedicine devices. The network links simulate the channel characteristics of 5G networks through software, including channel fading and noise interference. Test Case Design: Design a series of rich test cases, covering different network load conditions (such as low load, medium load, and high load) and encryption algorithm combinations. For each test scenario, set specific service traffic types and data transmission requirements, such as real-time video transmission and file transmission. For example, when testing the autonomous driving scenario, simulate the frequent short message transmission during the high-speed movement of vehicles to test the ability of the encryption scheme to ensure real-time performance and security; when testing the telemedicine scenario, simulate the real-time transmission of high-resolution medical images to examine the processing ability of the encryption scheme for large amounts of data. Data Collection and Analysis: During the execution of each test case, collect key data such as encryption time, decryption time, data transmission success rate, and bit error rate. Analyze these data to evaluate the data transmission security and real-time performance of different encryption algorithm combinations under different network loads and service scenarios. For example, judge whether the encryption scheme meets the real-time performance requirements by comparing the decryption times of different test cases; evaluate the protection ability of the encryption scheme for data integrity by counting the data transmission success rate and bit error rate.

4.2 Result analysis

Performance Analysis of Encryption Algorithm Combinations: Analyze the data transmission security and real-time performance of different encryption algorithm combinations. The results show that some encryption algorithm combinations perform well in terms of security, but the encryption and decryption times are long, affecting the real-time performance; while other combinations have good real-time performance but are insufficient in security when facing complex attacks. The optimized multi-layer encryption scheme has achieved a good balance between security and real-time performance and can meet the needs of most 5G application scenarios. Comparative Analysis of Test Scenarios: Compare the results of different test scenarios and find that the network load has a significant impact on the performance of the encryption scheme. Under high load conditions, the real-time performance of some encryption schemes decreases significantly, and the data transmission success rate drops. However, the multi-layer encryption scheme designed in this paper can maintain good stability and reliability under different test scenarios by dynamically adjusting the encryption strategy and resource allocation, effectively improving the security and real-time performance of data transmission. Proposed Improvement Suggestions: Based on the result analysis, propose suggestions for further optimizing the encryption scheme. For example, for the performance problems under high load scenarios, it is recommended to introduce an adaptive resource scheduling mechanism in the encryption architecture to dynamically adjust the computational resource allocation of the encryption algorithm according to the network load; to improve the defense ability against new types of attacks, it is recommended to regularly update the encryption algorithm library and introduce the latest security technologies.

5 Innovations

5.1 Innovation in multi-layer encryption collaboration

For the first time, a scheme for the collaborative work of multi-layer encryption is proposed, organically combining the encryption technologies of the physical layer, data link layer, and network layer. The encryption technologies of different layers collaborate with each other to form a multi-level security protection system. Compared with traditional single encryption technologies, it greatly improves the security of data transmission. Encryption technologies at each layer protect data at different stages according to their own characteristics and advantages, effectively resisting various types of attacks and enhancing the overall security of the system.

5.2 Innovation in real-time performance optimization

When designing the encryption scheme, real-time factors are fully considered, and targeted optimizations are carried out on the encryption algorithm. By improving the calculation process of the algorithm and adopting hardware acceleration technologies, the encryption and decryption times are significantly reduced. At the same time, a dynamic adjustment mechanism is introduced into the multi-layer encryption architecture, and the encryption strategy is adjusted in real-time according to the network status and business requirements, ensuring that the strict real-time requirements of 5G applications are met to the greatest extent while guaranteeing security.

6 Conclusions and prospects

6.1 Conclusions

This study has successfully designed and implemented a multi-layer real-time encryption transmission technology based on 5G wireless communication. Through in-depth research and optimization of encryption technologies at different layers and the careful design of the multi-layer encryption architecture, the collaborative work of encryption technologies has been achieved. Experimental results show that this scheme can significantly improve the security and real-time performance of data transmission in a simulated 5G network environment, effectively resist a variety of security threats, and meet the extremely high security and real-time requirements of application scenarios such as autonomous driving and telemedicine.

However, this study also has certain limitations. For example, in extremely complex network environments, the performance of the encryption scheme may be affected to a certain extent; the defense ability of the encryption scheme against some new and unknown attack methods remains to be further verified.

6.2 Prospects

Future research can be carried out in the following directions: First, further optimize the multi-layer encryption architecture to improve its adaptability and stability in complex network environments. By introducing artificial intelligence and machine learning technologies, realize the intelligent dynamic adjustment of encryption strategies. Second, strengthen the research on new attack methods, continuously update and improve the encryption algorithm library, and enhance the attack resistance of the encryption scheme. Third, explore the combination of this multi-layer encryption technology with emerging technologies such as blockchain to further enhance the security and traceability of data, providing a more solid security guarantee for the development of 5G communication technology.

About the Author

Wenxin Ge, 2567420667@qq.com.

References

[1] Li Xiang, Zhang Yong. Analysis and Protection Strategies of 5G Network Security Threats [J]. Journal on Communications, 2022, 43(8): 156-168.
[2] Wang L, Chen X, Liu Y. Physical-layer Security in 5G Wireless Networks: Challenges and Solutions [J]. IEEE Communications Magazine, 2021, 59 (3): 112-118.
[3] Zhou Ming, Wu Hao. Research on Application of Data Link Layer Encryption Algorithm in 5G Networks [J]. Computer Science, 2023, 50(5): 234-241.
[4] Hu H, Li Z, Zhang M. A Survey on Network-layer Security for 5G Networks [C]//2022 International Conference on Cybersecurity and Communication Networks. IEEE, 2022: 123-128.
[5] Zhao Yang, Sun Ting. Optimization of AES Algorithm Based on Hardware Acceleration and Its Application in 5G Encryption [J]. Application of Electronic Technique, 2022, 48(10): 98-103.
[6] Chen S, Yang Y, Xu X. Cooperative Encryption Mechanism for Multi-layer in 5G Networks [C]//2023 IEEE International Conference on Communications (ICC). IEEE, 2023: 1-6.
[7] Liu Feng, Ma Qiang. Research on Key Management Technology for 5G Networks [J]. Journal of Information Security Research, 2021, 7(7): 632-640.
[8] Wang X, Guo Y, Li S. Real-time Encryption Performance Optimization in 5G-enabled Industrial Internet of Things [J]. IEEE Internet of Things Journal, 2023, 10(12): 11023-11034.
[9] Guo Hua, Chen Jing. Research on 5G Physical Layer Encryption Technology Based on Artificial Noise Injection [J]. Journal of Signal Processing, 2022, 38(9): 1456-1465.
[10] Zhang H, Liu X, Wu J. An Improved IPsec Protocol for 5G Network Security [C]//2022 IEEE Global Communications Conference (GLOBECOM). IEEE, 2022: 1-6.