Journal of Intelligent Manufacturing, Vol.1 Iss.1 2025, pp. 10-12
ISSN :3078-4115

Research and analysis of 5G-advanced security

Jinyu Wang Qi Li Juan Guo *

School of Physics and Electronic Engineering, Taishan College, China

*Corresponding author

Abstract: This study focuses on the core challenges and countermeasures of 5G-Advanced network security to ensure secure and reliable communication. The paper first highlights the importance of 5G-Advanced while emphasizing the urgency and complexity of its security issues, while underscoring the research's value in advancing 5G-Advanced applications and enhancing cybersecurity capabilities. The content covers critical security concerns, attack vectors, and defense strategies for 5G-Advanced, establishing a comprehensive framework and logical progression with detailed methodological explanations. In the theoretical review section, the paper introduces fundamental principles and technologies for 5G-Advanced network security, including encryption algorithms and identity authentication. The technical analysis and validation phase examines various security mechanisms through theoretical examination and practical verification under 5G-Advanced environments. The conclusion summarizes key findings, systematically addresses 5G-Advanced security challenges, and proposes future research directions such as algorithm optimization and network protection mechanism design.

Key words:5G advanced, network security, security attack, security defense

1. Introduction

5G Advanced, an upgraded version of 5G technology, offers faster speeds, more connectivity, and lower latency[1][2]. With the advancement of IoT and AI, 5G Advanced has become increasingly vital, but it also brings heightened security concerns[3]. This paper examines the security challenges of 5G Advanced and evaluates the applicability of existing security technologies[4]. The development of 5G Advanced is crucial for meeting people's demand for fast and stable communication[5]. However, as the technology becomes widely adopted, cybersecurity risks are on the rise. As the core infrastructure of future networks, the security of 5G Advanced remains paramount. Currently, we have yet to verify the effectiveness of existing security technologies in 5G Advanced environments. This study aims to explore key security issues and solutions for 5G Advanced by analyzing security threats and attack methods, validating the effectiveness of current security technologies, and identifying effective defense strategies. Investigating 5G Advanced's security challenges is essential for enhancing cybersecurity capabilities. Ensuring the safety and reliability of network communications is critical[6]. The research will clarify the critical security issues faced by 5G Advanced, explore new security mechanisms and technologies, promote the application and development of 5G Advanced cybersecurity, and improve the security and reliability of network communications. The widespread adoption of 5G Advanced has made cybersecurity a focal point in the field of network communications. The significance of this research lies in advancing the application and development of 5G-advanced technologies, enhancing cybersecurity capabilities, and strengthening national cybersecurity infrastructure. By investigating security-related [7] challenges in 5G-advanced systems, we can provide theoretical support and practical guidance for secure communication implementation, thereby contributing to building a safe and trustworthy digital society.

2. Technical analysis and effect verification

technical analysis

Having analyzed common security measures and attack patterns, we now examine how encryption, access control, and authentication technologies ensure network security. Encryption primarily involves symmetric and asymmetric methods. The process converts data into ciphertext through cryptographic algorithms — information that remains unreadable without the corresponding key. Decryption reverses this process. Symmetric encryption uses identical keys for both sender and receiver, offering simplicity but compromising security. Asymmetric encryption employs separate keys, providing stronger confidentiality but slower processing speeds. Authentication verifies user

identity through three methods: 1) Password-based verification (e.g., QQ's PIN system), 2) Physical credential authentication (e.g., mobile verification codes), and 3) Biometric authentication (e.g., fingerprint recognition)[8]. Access control monitors data packets for specific signatures. When packets pass, the system checks them against predefined criteria—allowing qualified ones while blocking unauthorized access. This mechanism effectively protects systems from cyber threats. The effects of these technologies have been fully verified in the 5G era, proving that they can normally protect user security under 5G, but their security has not been fully verified in the 5G-A environment. Below we will verify the security of the above technologies in the 5G-A environment to see whether they can be reflected in the 5G-A environment.

3. Effect validation

First of all, we need to find a 5G-A environment. Recently, Huawei has carried out a 5G-advanced pilot in May Fourth Square, a popular scenic spot in Qingdao[9]. We will verify the effectiveness of existing security technologies under 5G-advanced network there.

Figure 1 Huawei completes 5G-A pilot in Qingdao

To demonstrate encryption technology, we can use Baidu Netdisk's sharing feature as a case study. After sharing files, the service generates a unique download link. To access the files, you must enter the generated password code. Without this key, the files cannot be retrieved. Through repeated experiments, all results consistently showed that passwords are required to retrieve files. This effectively validates that encryption technology remains capable of maintaining robust cybersecurity in 5G-advanced environments.

Figure 2 Baidu web disk link generation and extract code

For identity verification, we can utilize WeChat's login system. When logging in, users can opt to use mobile verification codes sent by the app. After entering the code, they can complete the login process[10]. This represents the second authentication method mentioned earlier – using physical items as verification credentials. Through repeated experiments, all results consistently demonstrated that obtaining verification codes was necessary for successful login, effectively validating the effectiveness of identity verification technology in 5G-advanced environments.

Figure 3 WeChat verification code login

Taking Windows Firewall as an example, access control technology ensures that only data packets authenticated through the firewall's special verification process can be accessed. Data packets failing this validation cannot pass through. Through repeated experiments, it was consistently observed that data must first be permitted to enter the firewall before being accessed. This effectively validates the effectiveness of access control technology in 5G Advanced environments.

Figure 4 Windows firewall

4. Conclusion

This study thoroughly examines the security challenges and defense technologies of 5G-Advanced, validating the effectiveness of encryption, authentication, and access control measures. The research reveals that 5G-Advanced faces multiple security threats requiring enhanced defensive strategies. Furthermore, practical applications have demonstrated significant efficacy in security monitoring, intrusion detection, and key management. Recommendations suggest prioritizing targeted attack types and emerging technologies to improve network security. However, current studies still lack sufficient exploration in specific vulnerabilities and new technology applications, such as inadequate research on privacy breaches and blockchain implementation, along with insufficient validation of existing security technologies. Future research will focus on optimizing security algorithms and network protection mechanisms, including enhancing encryption and authentication security, and developing AI-driven intrusion detection systems through behavioral pattern recognition. Additionally, integrating 5G-Advanced cybersecurity with other domains should be emphasized to ensure the safety and reliability of the network ecosystem.

Reference

[1] Sun Tonglun. Security Research on 5G Network Slicing [J]. Information and Computer (Theoretical Edition), 2019-03-15

[2] Li Gang.5G Technology Research [J]. Information and Computer (Theoretical Edition), 2019-08-15

[3] Zha Xiaoying. Security Research on 5G Network Slicing [J]. Computer Knowledge & Technology, 2021-02-15

[4] Xu Shubin & Gan Zhiwang. Current Status and Development Trends of 5G Security Technologies [J]. Radio Communication Technology, 2020-02-17 11:42

[5] Huang Lijun. Cybersecurity Risk Analysis and Strategy Research for Smart Campus Based on 5G New Technologies [J]. Information Record Materials, 2022-08-01

[6] Zhang Shuhong. Cybersecurity Risk Analysis and Strategy Research for Smart Campus Based on 5G New Technologies [J]. Cybersecurity Technology & Applications, 2023-08-11

[7] Li Xin. Research and Application of 5G Network Security Technology in an Open-pit Mine [J]. Gold, 2023-11-15

[8] Sheng Li. Analysis of 5G Communication Scenarios and Technologies [J]. China New Communications, 2019-05-05

[9] Wang Yuhuan. Research on 5G Security Regulatory Standards System [J]. Information and Communication Technology, 2019-12-20

[10] Song Jinwen. Analysis and Discussion on 5G Airfield Network Security [J]. Popular Science, 2023-ZH