Dean&Francis
ISSN 2959-6157

Security analysis of 5G network authentication and key negotiation protocol. Literature review

Longye Wang

Optoelectronics and Information Engineering, Fujian Normal University, Fuzhou, Fujian, 350117, China
Email: U2294502@unimail.hud.ac.uk

Abstract:

This study focuses on the security of 5G network authentication and key negotiation protocols, reviewing existing research findings. It examines the security issues of 5G-AKA and EAP-AKA 'from the protocol's perspective, summarizing formal verification methods and improvement measures. In terms of the integration of emerging technologies, it explores how blockchain and quantum key distribution enhance 5G security and their application progress. The paper highlights the current research's shortcomings in adapting to real-world scenarios and addressing new threats, providing direction for further 5G network security research. This will help solidify the foundation of 5G security and promote its reliable application in critical areas.

Keywords: 5G network, authentication and key negotiation protocols, security analysis, privacy protection, formal verification, man-in-the-middle attack

1. Research Background

1.1 Macro Background

5G technology, with its high bandwidth, low latency, and extensive connectivity, significantly enhances the Internet of Things (IoT), industrial internet, and intelligent transportation, reshaping social and economic production and living models. However, in these scenarios, frequent device interactions and high data value density increase the stringent requirements for network identity authentication and data encryption. Authentication and key negotiation protocols, as the core of 5G security, are crucial for user identity confidentiality, communication data integrity, and service reliability. Meanwhile, the development of quantum computing technology poses a risk of cracking traditional encryption algorithms, intensifying the challenges to 5G network security. Therefore, in-depth research on protocol security and its optimization and upgrade is essential to ensure the stable operation of the 5G ecosystem.

1.2 Research Object and Problem Focus

The research focuses on 5G network authentication and key negotiation protocols (such as 5G-AKA and EAP-AKA') and the application of emerging technologies (such as blockchain and quantum key distribution) in enhancing security. Key issues to address include: vulnerabilities in user identity protection,

ISSN 2959-6157

key security, and message transmission; the compatibility and security mechanism innovation of emerging technologies with 5G networks; and how to respond to emerging threats like quantum computing to enhance the overall security of 5G networks and promote the credible application of technology in critical areas.

2. Research Significance

2.1 Theoretical Significance

This paper systematically reviews the security analysis methods for 5G network authentication and key negotiation protocols, including formal verification and probabilistic model testing. It clarifies how these methods are applied to uncover vulnerabilities and verify security, thereby enhancing the theoretical framework of protocol security analysis. Additionally, it explores the integration of emerging technologies like blockchain and quantum key distribution into 5G security, expanding the boundaries of 5G security research. This work provides a reference for the design of new security protocols and the development of theories for integrating technologies, contributing to the deepening of 5G security theory.

2.2 Practical Significance

In practice, the research findings can precisely identify security vulnerabilities in 5G network authentication and key negotiation protocols, guiding improvements in key management, encryption technology, and verification mechanisms. This ensures user privacy and data security, maintaining the stable operation of 5G networks. It also supports the secure deployment of 5G technology in critical sectors such as healthcare, finance, and industrial control, enhancing industry trust in 5G applications. Furthermore, it explores solutions for future threats, such as quantum computing, providing practical guidance for the long-term security evolution of 5G networks and promoting the healthy and sustainable development of the 5G industry.

3. Research Status

3.1 Security Analysis of 5G Network Authentication and Key Negotiation Protocol

Many studies focus on the security analysis of 5G core protocols. Jia Fan et al. (2021)[12]conducted a security analysis of 5G network authentication and key negotiation protocols, using formal methods to identify potential risks in identity protection and key transmission. Yang Chenglong et al. (2022)[10]used formal verification techniques to analyze 5G network authentication and key negotiation protocols, identifying potential vulnerabilities that could be exploited by attackers during protocol execution. Zhao Lujing (2020)[14]studied the EAP-AKA' protocol, analyzing its security flaws in practical applications to provide a basis for protocol improvements. These studies, from various perspectives, have laid the groundwork for understanding the current security status of 5G authentication and key negotiation protocols, promoting more detailed and comprehensive security analyses.

3.2 Research on Protocol Improvement and Optimization

Scholars actively explore improvement solutions to address protocol shortcomings. Peng Chengwei et al. (2025)[5]formally verified and improved the SAP-AKA secondary authentication protocol, optimizing the protocol process and encryption mechanisms to enhance its resistance to attacks. Xie Zhen (2022)[11]focused on enhancing the security of 5G network authentication and key negotiation protocols, proposing optimization paths that integrate emerging encryption technologies to strengthen key security and the reliability of identity authentication. Liu et al. (2021)[13]designed a new 5G wireless network authentication and key negotiation protocol, optimizing the authentication process and key generation and distribution mechanisms to improve protocol security and efficiency, providing practical references for the iterative upgrade of 5G protocols.

3.3 Exploration of the Application of Emerging Technologies in 5G Security

Blockchain Technology: Su Renze (2024)[2]explored the security of blockchain technology in 5G applications within smart energy networks. By leveraging the decentralized and immutable nature of blockchain, he constructed a secure data sharing and authentication environment, providing insights for enhancing the security of 5G + smart energy scenarios. Xiang Xin (2024)[3]focused on the distributed key management mechanism for blockchain, exploring its application in 5G networks to ensure secure key distribution and storage, thus contributing to the innovation of 5G network key management models. Pratibha Singh et al. (2025)[1]used Event B to formally verify the block-based packet management of blockchain-driven 5G congested networks, validating the feasibility of blockchain technology in 5G network resource management and security assurance. Quantum Key Distribution: Some studies have explored the integration of quantum key distribution with 5G, such as Garima Thakur et al. (2024)

[7], who designed an authentication and key negotiation protocol based on quantum key distribution for 5G applications in satellite communication networks. This protocol leverages quantum properties to enhance key security and resistance to attacks, offering new pathways for 5G wide-area communication security. Although systematic research on the deep integration of 5G and quantum key distribution is still lacking, these explorations lay a solid foundation for future technological integration. Privacy Protection Technology: Li Kaixuan (2024)[4]explored various high-dimensional data release schemes for differential privacy protection, providing a framework for protecting user data privacy in the authentication and negotiation processes of 5G networks, thereby reducing the risk of data leakage while ensuring protocol functionality. Ge et al. (2013)[15]analyzed the security of decentralized encryption schemes for privacy protection, offering theoretical insights for introducing new encryption mechanisms in 5G networks, thus advancing the development of 5G security and privacy protection technologies.

3.4 Research on Security Threats and Attack Responses

To address threats such as man-in-the-middle attacks in 5G networks, Raut Omprakash Jagannath et al. (2024)[6] examined browser man-in-the-middle attacks, outlining attack principles and preventive measures to enhance the security of 5G network terminal access. Elrawy Mohamed Faisal et al. (2023)[9]focused on detecting and classifying man-in-the-middle attacks in 5G private networks of smart grids, proposing strategies to ensure the security of 5G applications in critical infrastructure. Sigurd Eskeland (2024)[8]conducted a cryptanalysis of privacy protection authentication schemes based on the intersection of private sets, providing guidance for optimizing similar privacy protection authentication mechanisms in 5G networks, thus advancing the detailed and in-depth research on 5G network attack responses.

4. Review

4.1 Summary of Research Achievements

Current research has yielded significant results in the field of 5G network authentication and key negotiation protocol security. Hou Junfeng (2004)[16]utilized formal verification and other methods to precisely identify security vulnerabilities in protocols such as 5G-AKA and EAP-AKA', clarifying risks in identity protection and key transmission. In protocol improvements, he proposed multiple optimization schemes from the perspectives of process optimization and encryption mechanism upgrades, enhancing both the security and efficiency of the protocols. In exploring the application of emerging technologies, research on integrating blockchain, quantum key distribution, and privacy protection technologies with 5G security is ongoing, providing new pathways for enhancing 5G security. In addressing security threats, he conducted in-depth analyses and proposed prevention strategies for typical threats like man-in-the-middle attacks, strengthening 5G network security. However, there are still shortcomings in existing research. First, there is a lack of research on practical scenario adaptability; most protocol improvements and technology applications are based on theoretical or simulated environments, and their feasibility and performance in real-world 5G scenarios, such as large-scale IoT high-density access and industrial internet low-latency high-reliability requirements, need further validation.

4.2 Insufficiencies of existing research

However, the research still has several shortcomings. Firstly, there is a lack of studies on the adaptability to real-world scenarios. Most protocol improvements and technology applications are based on theoretical or simulated environments. In the complex and diverse real-world scenarios of 5G (such as high-density IoT access and low-latency, high-reliability requirements in industrial internet), the feasibility and performance of these solutions need further validation. Secondly, the response to emerging threats is insufficient. With the widespread application of quantum computing, the threat of cracking encryption algorithms poses a significant challenge. Current research lacks a comprehensive system for constructing quantum-safe 5G authentication and key negotiation protocols, as well as long-term security mechanisms that integrate multiple technologies. Thirdly, research on the synergy of technology integration is weak. When integrating emerging technologies like blockchain and quantum key distribution with 5G network security, most studies focus on the application of individual technologies, lacking in-depth research on the coordination and complementarity between technologies and the optimization of the overall security architecture.

4.3 Research direction of myself

Based on this, future research can be deepened in three areas: First, enhance the verification of practical scenarios by selecting typical 5G application scenarios (such as smart factories and connected vehicles) to conduct field tests on protocol improvements and emerging technology applications, verifying their security, efficiency, and compatibility in real-world environments; Second, deepen the

ISSN 2959-6157

response to emerging threats by designing quantum secure 5G authentication and key negotiation protocols, integrating quantum key distribution and anti-quantum encryption algorithms to build a security system that resists quantum computing attacks, and studying long-term security evolution mechanisms; Third, promote the integration and collaboration of technologies by exploring a 5G security architecture that integrates blockchain, quantum technology, and privacy computing, leveraging the synergistic advantages of these technologies to enhance the overall security protection level of 5G networks, and laying a solid foundation for the widespread and secure application of 5G technology in critical sectors.

References

[1] Pratibha Singh, Arun Kumar Singh, Girish Chandra. Formal Verification of Blockchain-Driven Packet Management in Congested Networks Using Event B [J]. Expert Systems with Applications, 2025,283.

[2] Su Renze. Application and Security Analysis of Blockchain Technology in Smart Energy Networks [J]. East China Science & Technology, 2024, (12):64-66.

[3] Xiang Aixin. Distributed Key Management Mechanism for Blockchain [D]. Supervisor: Tian Youliang. Guizhou University, 2024.

[4] Li Kaixuan. Research on Multi-Type High-Dimensional Data Publishing Schemes for Differential Privacy Protection [D]. Supervisor: Zhang Hua. Beijing University of Posts and Telecommunications, 2024.

[5] Peng Chengwei, Yang Jinji, Yang Guang. Formal Verification and Improvement of the SAP-aka Secondary Authentication Protocol [J]. Computer Engineering, 2025,51 (06):204-211.

[6] Raut Omprakash Jagannath, Ankit Kumar Jain. Browser-in-the-middle attacks: A comprehensive analysis and countermeasures [J]. Security and Privacy, 2024, 7 (5):

[7] Garima Thakur, Mohammad S. Obaidat, Piyush Sharma, Sunil Prajapat, Pankaj Kumar. An efficient provably secure authentication and key agreement protocol for satellite communication networks [J]. Security and Privacy, 2024, 7 (5):

[8] Sigurd Eskeland. Cryptanalysis of a Privacy-Preserving Authentication Scheme Based on Private Set Intersection [J]. Journal of Mathematical Cryptology, 2024,18 (1):

[9] Elrawy Mohamed Faisal, Hadjidemetriou Lenos, Laoudias Christos, Michael Maria K. Detecting and Classifying Man-in-the-Middle Attacks in Smart Grid Private Area Networks [J]. Sustainable Energy, Grids and Networks, 2023,36;

[10] Yang Chenglong, Yang Jinji, Su Guidian, Guan Jinping. Formal Verification and Analysis of 5G Network Authentication and Key Aggregation Protocol [J]. Computer System Applications, 2022, 31 (12):398-404.

[11] Xie Zhen. Research on Security Enhancement of 5G Network Authentication and Key Agreement Protocol [D]. Supervisor: Ji Xinsheng. Strategic Support Force Information Engineering University, 2022.

[12] Jia Fan, Yan Yan, Yuan Kaiguo, Zhao Lujing. Security Analysis of 5G Network Authentication and Key Agreement Protocol [J]. Tsinghua University Journal (Natural Science Edition), 2021,61 (11):1260-1266.

[13] Liu Tian, Wu Fan, Li Xiong, Chen Chaoyang. A New Authentication and Key Agreement Protocol for 5G Wireless Networks [J]. Telecommunication Systems, 2021,78 (3).

[14] Zhao Lujing. Security Analysis of 5G Network Authentication and Key Agreement Protocol EAP-AKA' [D]. Supervisor: Jia Fan. Beijing Jiaotong University, 2020.

[15] Ge Aijun, Zhang Jiang, Zhang Rui, Ma, Chuangui. Security Analysis of a Privacy-Preserving Decentralized Key Policy Attribute-Based Encryption Scheme [J]. IEEE Transactions on Parallel and Distributed Systems: A Publication of the IEEE Computer Society, 2013,24 (11):

[16] Hou Junfeng. Formal Verification Methods for Security Protocols and Research on Security Protocol Design [D]. Supervisor: Huang Liansheng. Tsinghua University, 2004.