Research on 5G Mobile Communication Network Security Technology

Weishu Zhan$^{1,*}$, Zhen Tao$^{2}$

$^1$ University of Northern Iowa, Cedar Falls, 50618, United States

$^2$ University of bath, bath, BA2 7PD, United Kingdom

*Corresponding Author’s E-mail: zhanw@uni.edu

Abstract. With the infiltration of computer networks in various fields, more and more social and economic activities rely on mobile communication networks. Network attack methods are becoming more and more advanced, resulting in frequent network security accidents, and modern mobile communication network security defense is facing greater threats and challenges. The 5G mobile communication network is an important infrastructure for building a networked society and realizing the interconnection of all things. In the future, the development of various industries will be based on the rapid development of mobile communication technology in 5G. 5G utilizes the changes and innovations in system architecture and core technologies to achieve network layout. The security protection technology and security guarantee mechanism of 5G networks are very important. In the context of the gradual implementation of 5G mobile communication networks, this paper focuses on the security aspects of 5G mobile communication networks, from business slice security, pseudo base station attack behavior analysis, and user privacy protection to its security threats, security needs, and facing Analyzed the technical challenges of the network and researched relevant network security defense technical measures, providing references for the technical research and network implementation and deployment of 5G mobile communication networks.

1. Introduction

5G further improves the user experience from the technical level, and can provide users with faster and more stable communication services. As the next-generation mobile communication network, 5G maintains a high degree of attention to it from all walks of life. In 5G mobile communication networks, ultra-dense networking technology, and SDN technology are widely used, which has obvious advantages in the fluency and stability of communication networks. The performance of 5G mobile communication networks has been greatly improved in many aspects, including traffic density, end-to-end delay, peak rate, mobility, number of connections, and Internet speed. It can effectively support the realization of massive device interconnection and differentiated service scenarios, making the user experience more comfortable. In terms of network data information interaction, it can meet the requirements of triple play and the Internet of Things. 5G mobile communication network has rich functions and wide application fields. Therefore, it has high requirements on network security [1].

On the premise of ensuring voice and data communication services, 5G mobile communication networks need to provide corresponding services for all interconnected industries. The 5G mobile communication network needs to establish a more comprehensive, efficient, and low-energy communication network and service model to meet security needs from multiple aspects, so that many
new service needs can be met. The 5G mobile communication network needs to ensure the security of devices across the access network. It uses a unified security management mechanism to provide security guarantees for device privacy and authentication. Faced with the needs of personal business and vertical industry services, 5G mobile communication networks need to provide differentiated security mechanisms to provide corresponding privacy protection for various types of devices connected to the network [2].

2. Business slice security technology

In order to solve the business demand problem, 5G mobile communication network introduces SDN and NFV into the network architecture, presenting a network structure combining virtual distribution sinking and centralized control. In the 5G mobile communication network structure, the control interface is concentrated on the core network. In order to further reduce the processing delay and backhaul costs of the user plane, the distribution of business characteristics needs sinks, which provides convenience for closer to the user’s block, so that the user Perception is enhanced. During the deployment of mobile communication networks, the focus of security management such as wireless access needs to be migrated to the 5G network user plane for security management and control. In the 5G network structure, a large amount of business processing information is carried by business slices. According to different business characteristics, corresponding security management and control measures need to be provided. During the networking process, it is necessary to focus on the security of the user plane slice of the network [3]. Some core network functions of the 5G mobile communication network use virtual sinking to split the corresponding functions, and the network structure of the virtual core network is semi-open. Facing a large number of interactive and open data scenarios, the network security management layout needs to be transformed from centralized security control to distributed security control.

In the 5G mobile communication network structure, in response to the needs of many terminal types and scene characteristics, the service slice processing method is adopted, and its security has become one of the key contents in the deployment process. When deployed by mobile network operators, public information is encrypted using a unified encryption method under a unified security management framework. For high-value information such as user privacy and security, key information authentication and biometrics are used in combination, or a reliable encryption method from the core network to the wireless node. On the basis of comprehensive consideration of network capacity, signaling, information transmission delay and security strategy, it is necessary to fully consider the network security architecture and policy application after service slicing [4]. 5G mobile communication network service slice security authentication technology scheme is shown in Figure 1. The service slices of 5G mobile networks are mainly divided into voice services, massive services, video services, and low-latency IoT service slices. When the operator authenticates the customer's key information, it is completed in the core cloud; for services that share more information, a unified authentication and security management method is completed at the edge cloud; for low-latency slicing services, these services and customer property With strong correlation, it is necessary to build a personalized key authentication security management mode. On the basis of ensuring low transmission delay, the information encryption algorithm and security management and control layout strategy are independently constructed.
Figure 1. 5G mobile communication network service slice security authentication technical solution

3. 5G mobile communication network pseudo-base station attack forensics technology

The deployment and application of 5G mobile communication networks can bring great convenience to social production and residents' lives. At the same time, due to economic interests, many incidents of attacks on 5G communication networks occur from time to time. Among the many acts of attacking 5G mobile network communications, the pseudo base station is a typical attack. The attacker disguised the pseudo base station as a legitimate base station of the operator, so that the mobile devices of nearby users were forced to access the base station, and then sent malicious text messages such as phishing links and spam advertisements to the mobile devices of the users accessing the pseudo base station [5].

3.1. Pseudo base station structure and attack principle

From the perspective of manufacturing, there is no uniform specification for pseudo base stations, the appearance of different pseudo base stations varies greatly, and most of the internal modules of pseudo base stations have similar structures. The composition structure of the pseudo base station mainly includes the power supply system, the receiving transmitter and the control system. The modules inside the receiver transmitter include duplexer, power amplifier, radio frequency circuit board and antenna. The control system includes a processor main board and an operation control interface inside the pseudo base station. The pseudo base station uses a user control interface to interact with the operator. In the operation interface, you can modify and edit the transmission frequency, power intensity and information content. In order to facilitate the transfer of crime, under normal circumstances, the pseudo base station uses a car battery or a portable power supply for power supply [6].

In the mobile communication network, in order to verify the legitimacy of mobile access users, operators usually adopt a one-way identity verification method, that is, the base station verifies the user information of the access device without letting the user verify the base station. The legitimacy of the identity makes it impossible for the pseudo base station to be discovered by users under the
unidirectional authentication vulnerability. When the pseudo base station performs an attack, it first obtains the information of the operator's base station cell, and according to the current frequency distribution, the pseudo base station keeps the same frequency as the operator's base station's transmission frequency. This forces mobile devices within its radiation range to access the pseudo base station.

3.2. Pseudo base station attack analysis
Pseudo-base station attacks mainly include monitoring the user's information content in the mobile communication network and sending malicious short messages to the mobile communication network user. The pseudo base station obtains information such as the operator brand, access frequency point, and signal strength of surrounding base stations, and configures the pseudo base station according to the obtained operator base station information. Invading mobile communication network user accounts, stealing personal privacy information and user finances has become the target of a chain attack of pseudo base station network accounts. The pseudo-base station network account chain attack process is shown in Figure 2. The pseudo-base station repeats the relevant steps and can continuously attack multiple users' network accounts [7].

![Figure 2. 5G mobile communication network pseudo base station network account chain attack process](image)

3.3. Pseudo base station attack forensics technology
For the attack behavior of the pseudo base station, in order to achieve accurate forensics, a pseudo base station forensic design based on radio frequency fingerprints can be used. Collect the original signal transmitted by the pseudo base station, mark the collection time and location information of this information, and after processing by the modulation domain module and the waveform domain module, extract the target signal segment area from the burst to generate a fingerprint.

In the RF fingerprint generation module, the system extracts signal features from the modulation domain and the waveform domain to construct a pseudo-base station RF fingerprint. We calculate the wavelet change and Fourier change of the transient frequency and phase waveform of the signal, and obtain the changes in the frequency domain and wavelet domain, respectively. We can obtain the waveforms of the transient phase and frequency in the time domain, frequency and wavelet domain, and use these waveforms for subsequent feature extraction. Through calculation, the time-frequency statistical characteristics of a large number of training bit sequences are obtained. The features are ranked according to their importance, combined with the characteristics of the pseudo-base station signal amplitude envelope, and some statistical indicators are selected to represent the characteristics of the entire training bit sequence, as the input vector of the classifier.
When processing the pseudo base station forensics system, it is necessary to compare the collected RF signal fingerprint with the pseudo base station RF signal fingerprint. We design the recognition module, use machine learning algorithms to model the pseudo-base station RF fingerprint data, use supervised learning, and the classification algorithm selects support vector machines to classify the radio-frequency fingerprints to match the pseudo-base station's radio-frequency fingerprints. For each pseudo base station, we use the training signal fragments of M burst sequences to generate a multi-dimensional RF fingerprint and train the classifier. For N pseudo base stations in the pseudo base station database, NxM burst sequences are required to train M two classifiers. In the forensics stage, if the radio frequency fingerprint in the database is the same as the collected fingerprint, the current time and place will be added to the database, otherwise, it is assumed that the radio frequency fingerprint originated from a pseudo base station that has never been discovered [8].

4. 5G mobile communication network privacy data protection technology based on blockchain

The 5G mobile communication network based on blockchain adopts a decentralized system structure to manage data, which can effectively avoid centralized security risks. Using the traceable and non-tamperable security features of blockchain technology, it is possible to manage a large amount of private data and effectively guarantee the authenticity of the data. Effectively combine the blockchain technology and the off-chain database to separate data permissions, and use a decentralized approach to manage personal privacy data and related permissions. Applications need to obtain access authorization before they can access user data.

After encrypting user data, it is stored in a distributed database outside the blockchain. The user authorizes the application through permission settings, allows it to modify certain data, and records the granted permissions and data pointers in the blockchain. When an application accesses a certain data, a data access request is issued and recorded in the blockchain. The network system confirms the access rights of the application by checking the blockchain records and signatures. If the inspection result meets the operation authorization requirements, record the operation in the blockchain and return the data to the application through the database. Because the blockchain completely records the behavior of the application, users can change the data access permissions at any time. In the 5G mobile communication network based on blockchain, for the user, ensure that the data operation process is transparent and auditable. Users can track the data, clarify the complete process of data acquisition and modification, and provide security for the data. The digital signature technology of the blockchain is used to confirm the integrity and origin of a certain data or file, and ensure that the data or file has not been maliciously modified [9]. In the 5G mobile communication network, the immutable nature of the blockchain can be used to construct a user privacy data file signature system based on the blockchain. The user data management system based on blockchain is shown in Figure 3.
Blockchain technology can ensure that the recorded node values cannot be tampered with. After the system publishes the block where the root node value is located, the file sender uses the corresponding root node value and time stamp to construct the signature. When sending a file to the receiving end, you need to send the file and its corresponding signature at the same time. After receiving the file and its signature, the receiver needs to verify the file signature [10].

5. Conclusion
5G mobile communication network services present diversified and differentiated characteristics, and the network architecture tends to be a new situation of virtual distribution, cloudization and sinking. These network structure changes have caused 5G mobile communication networks to face many new challenges in terms of security management and control mechanisms. Aiming at the security technology research of 5G mobile communication network, this paper mainly conducts research on the security layout of 5G network service slice, analysis of pseudo base station attack behavior and network user data protection based on blockchain. In the analysis of the characteristics of pseudo base station attacks, the new pseudo base station attacks of network account chain attacks are studied, and the pseudo base station forensics system based on radio frequency fingerprints is discussed. Blockchain-based 5G mobile communication network security technology is still in the early stages of development, and there are many problems that need to be solved. The introduction of blockchain in the mobile communication network security system causes calculation overheads such as encryption and decryption calculations and hash calculations, which reduces the system's Throughput increases system energy consumption. In view of the current problems, further research is needed.

References
[1] Zhu H R, Zhuang X J, Guo S, et al. 2004 5G Security Vision. Telecommunications Science, vol 11.
[2] Zhao G F, Chen J, Han Y B, et al. 2015 Overview of key technologies in 5G mobile communication networks. Journal of Chongqing University of Posts and Telecommunications, vol 4.
[3] Huang K Z, Jin L, Zhao H. 2015 Research on 5G Security Threats and Protection Technology. Post and Telecommunications Design Technology, vol 6, pp 8-12.
[4] Li H, Fu Y L. 2015 Analysis and Prospect of 5G Network Security Problems. Radio Communication Technology, vol 4, pp 1-7.
[5] Jin M S, Zhou X P, Ji C H, et al. 2017 Research on the pseudo base station dynamic monitoring system. Journal of China Criminal Police College, vol 6, pp 117-119.

[6] Xiao T, Xie C Z. 2018 Analysis of the working principle and management method of "ft base station". China's Strategic Emerging Industries, vol 8, pp 112.

[7] Li Q. 2015 FPGA implementation of GSM downlink receiver. University of Electronic Science and Technology.

[8] Yuan Y, Wang F Y. 2016 Current status and prospects of blockchain technology development. Journal of Automation, vol 42, no 4, pp 481-494.

[9] Shao Q F, Jin C Q, Zhang Z, et al. 2017 Blockchain technology: architecture and progress. Chinese Journal of Computers, pp 1-20.

[10] KOSBA A, MILLER A, SHI E, et al. 2016 Hawk: the blockchain model of cryptography and privacy-preserving smart con-tracts[C]//IEEE Symposium on Security and Privacy (SP), May 23-25, 2016, San Jose, CA, USA. Piscataway: IEEE Press, pp 839-858.