Irada Seyidova, Fidan Seyidova
Azerbaijan State Oil and Industry University
irada_seyid@mail.ru, seyidovafidan8@gmail.com

RESEARCH ON 5G MOBILE NETWORK SECURITY TECHNOLOGY

Abstract: The 5G mobile network is a critical infrastructure for building a networked society and enabling the connectivity of all things. The future development of various industries will depend on the rapid advancement of 5G mobile communication technologies. 5G leverages changes and innovations in system architecture and core technologies to achieve network deployment. The technology for safeguarding and ensuring the security of 5G networks is of utmost importance. In the context of the gradual deployment of 5G mobile networks, this thesis primarily focuses on aspects of 5G mobile network security. Technical issues in the network are analyzed, and corresponding technical security measures are explored. References are provided for further technical research and the implementation and deployment of 5G mobile communication networks.

Introduction

5G represents a significant enhancement in the technical realm, promising users faster and more stable communication services. As the next-generation mobile communication network, 5G has garnered widespread attention across all sectors of society. It extensively employs technologies such as ultra-dense networks and Software-Defined Networking (SDN), which offer evident advantages in terms of network speed and stability. The performance of 5G mobile networks has seen substantial improvements in various aspects, including traffic density, end-to-end latency, peak data rates, mobility, the number of connections, and internet speed. It effectively supports the realization of massive device interconnections and differentiated service scenarios, enhancing user experiences.

From the perspective of interacting with network data, 5G can meet the requirements of Triple Play and the Internet of Things (IoT). 5G mobile networks encompass rich functionalities and have broad application areas, thus imposing high demands on network security [1]. 5G mobile networks must establish a more comprehensive, efficient, and energy-efficient communication network and service model to meet security needs in various aspects. 5G must ensure the security of devices within the access network. It employs a unified security management mechanism to provide assurances for device confidentiality and authentication [2].

Forensic Examination Technology for Pseudo-Base Station Attacks in 5G Mobile Communication Networks

The deployment and utilization of 5G mobile communication networks hold the potential to significantly enhance public productivity and improve the lives of residents. However, owing to economic interests, there have been numerous instances of attacks on 5G communication networks. Among the multitude of attacks on 5G mobile networks, the pseudo-base station attack is a typical example. In this attack, malicious actors disguise a pseudo-base station as a legitimate operator's base station, compelling nearby mobile devices to connect to the pseudo-base station. Subsequently, the attackers send malicious text messages, such as phishing links and spam advertisements, to the mobile devices connected to the pseudo-base station [3].

Pseudo-Base Station Structure and Attack Principle

From a production standpoint, there is no unified specification for pseudo-base stations; the external appearance of various pseudo-base stations varies significantly, while most internal modules of pseudo-base stations share a similar structure. A pseudo-base station typically consists of a power supply system,

a transceiver, and a control system. The pseudo-base station employs a user control interface for interaction with the operator. Within the operational interface, parameters such as transmission frequency, power, and information content can be modified and edited [4].

In mobile communication networks, operators typically employ a one-way identity verification method to confirm the legitimacy of mobile access users. In this method, the base station verifies user device information without allowing the user to verify the base station. The one-way authentication vulnerability makes it impossible for users to detect pseudo-base stations. When a pseudo-base station executes an attack, it initially acquires information about the operator's base station cell and, in accordance with the current frequency allocation, maintains the same transmission frequency as that of the operator's base station. This compels mobile devices within its coverage area to connect to the pseudo-base station.

Analysis of Pseudo-Base Station Attacks

Attacks on pseudo-base stations primarily encompass the tracking of user information within the mobile communication network and the dissemination of malicious short messages to network users. The pseudo-base station acquires information such as the operator's trade name, access point, and the signal strength level of surrounding base stations, configuring itself accordingly. Intrusion into the user accounts of mobile communication networks, theft of personal confidential information, and financial details of users have become the targets of a chain attack on the network accounts of pseudo-base stations. The pseudo-base station repeats the relevant steps and can continuously target the network accounts of multiple users [5].

Forensic Examination Technology for Pseudo-Base Station Attacks

Regarding the behavior of pseudo-base stations during an attack, to achieve precise forensic examination, a forensic design for pseudo-base stations based on radio frequency fingerprints can be employed. The process involves collecting the original signal transmitted by the pseudo-base station, recording the collection time and location information, and, after processing with modulation area and waveform shape area modules, extracting the target signal segment from the packet to create a fingerprint.

In the RF fingerprint generation module, the system extracts signal characteristics from the modulation area and waveform shape area to construct the RF fingerprint of the pseudo-base station. This involves computing wavelet changes and non-stationary frequency and phase waveform changes, resulting in changes in both the frequency domain and wavelet domain. Signal shapes in the time domain, frequency domain, and wavelet domain are obtained, and these signal shapes are used for subsequent feature extraction. Frequency-time statistical characteristics of a large number of training bit sequences are computed. Features are ranked based on their importance, combined with envelope amplitude characteristics of the pseudo-base station signal, and selected statistical indicators represent the characteristics of the entire training bit sequence as input vectors for the classifier.

In the forensic examination system processing, it is necessary to compare the collected RF signal fingerprint with the fingerprint of the pseudo-base station. A recognition module is developed, utilizing machine learning algorithms to model the RF fingerprint data of the pseudo-base station. Supervised learning is applied, and a support vector machine classification algorithm is chosen to classify the RF fingerprints according to the pseudo-base station's frequency. For each pseudo-base station, fragments of the training signal M packet sequences are used to generate a multidimensional RF fingerprint and train the classifier. For N pseudo-base stations in the pseudo-base station database, NxM packet sequences are required to train M classifiers. During the forensic examination phase, if the RF fingerprint matches one in the database, the current time and location are added to the database. Otherwise, it is assumed that the RF fingerprint originates from a pseudo-base station that has never been detected [6].

Data Privacy Protection Technology in 5G Mobile Communication Networks Based on Blockchain

A blockchain-based 5G mobile communication network employs a decentralized system structure for data management, effectively mitigating centralized security risks. Utilizing blockchain's tamper-proof and immutable security features, it becomes possible to manage a vast amount of personal data while

ensuring data authenticity. This is achieved by effectively combining blockchain technology with an autonomous database to partition access permissions to data and employing a decentralized approach to manage personal privacy data and associated permissions. Applications must obtain permission to access user data before they can gain access.

After encrypting user data, it is stored in a distributed database outside the blockchain. The user authorizes the application through permission settings, allowing it to modify specific data and recording the granted permissions and data pointers on the blockchain. When the application requests specific data, a data access request is generated and recorded on the blockchain. The network system verifies the application's access rights by checking the blockchain records and signatures. If the authorization requirements for the operation are met, the operation is recorded on the blockchain, and the data is returned to the application through the database. Since the blockchain fully records the application's behavior, users can change data access permissions at any time. In a blockchain-based 5G mobile communication network, transparency and auditability of the data handling process are provided to users. Users can track data, clarify the entire data retrieval and modification process, and ensure data security.

Blockchain's digital signature technology is employed to confirm the integrity and origin of specific data or files and guarantee that data or files have not been maliciously altered [7]. In a blockchain-based 5G mobile communication network, the immutable nature of the blockchain can be utilized to create a blockchain-based user data privacy file signing system.

Blockchain technology ensures that recorded node values cannot be altered. After the system publishes a block containing the root node's value, the file sender uses the corresponding root node value and timestamp to create a signature. When sending the file to the recipient, both the file and its corresponding signature must be sent simultaneously. Upon receiving the file and its signature, the recipient must verify the file's signature [8].

Conclusion

The services of 5G mobile communication networks exhibit diversified and differentiated characteristics, and the network architecture typically represents a new situation of virtualization, cloudiness, and immersion. These changes in network structure have led 5G mobile communication networks to face numerous new challenges in terms of security management and control mechanisms.

Focusing on the investigation of security technologies in 5G mobile communication networks, this article primarily explores the security scheme of the 5G network service segment, analyzes behaviors during pseudo-base station attacks, and investigates user data protection based on blockchain technology. When analyzing the characteristics of pseudo-base station attacks, new attacks involving chain attacks on network account credentials are examined, and a pseudo-base station forensic examination system based on radio frequency fingerprints is discussed.

Blockchain-based security technology for 5G mobile communication networks is still in its early stages of development, and there are many issues that need to be addressed. The integration of blockchain into the security system of mobile communication networks incurs computational overheads, such as encryption and decryption computations and hash computations, which reduce system throughput and increase energy consumption. Given the existing challenges, further research is required [8].

References

[1] Zhu HR, Zhuang X J, Guo S, et al. (2004). Concept of 5G Security. 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] Jin M S, Zhou X P, Ji CH, et al. (2017). Research on the Dynamic Monitoring System of Pseudo-Base Stations. Journal of China Criminal Police College, Vol. 6, pp. 117–119.

[4] Xiao T, Xie C Z. (2018). Analysis of the Working Principle and Control Method of "ft" Base Station. Strategic Emerging Industries of China, Vol. 8, pp. 112.

[5] Li Q. (2015). Implementation of Downlink GSM Receiver. University of Electronic Science and Technology.
[6] Yuan Y., Wang F. Y. (2016). Current State and Development Prospects of Blockchain Technology. Journal of Automation, Vol. 42, No. 4, pp. 481-494.
[7] Shao Q F, Jin C Q, Zhang Z, et al. (2017). Blockchain Technology: Architecture and Progress. Chinese Journal of Computers, pp. 1-20.
[8] Kosba A., Miller A., Shi E, et al. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In: Proceedings of the IEEE Symposium on Security and Privacy (SP), May 23-25, 2016, San Jose, California, USA. Piscataway: IEEE Press, pp. 839–858.

Развитие корпоративной сети для финансовых учреждений

Мамедова Ульвия Музаффар
Сумгаитский Государственный университет
Рашад Мамедов
Азербайджанский государственный университет нефти и промышленности

Аннотация. В современном финансовом секторе корпоративные сети играют ключевую роль. Эти сети оказывают значительное влияние на развитие, эффективность, безопасность и качество услуг, предоставляемых финансовыми учреждениями. В данной статье мы предоставим обзор функционирования корпоративных сетей для финансовых учреждений и обсудим основные принципы и важные вопросы в этой области.
Ключевые слова:безопасность и качество, управление данными, финансовый сектор

Корпоративные сети являются одними из самых значимых активов для финансового учреждения. Управление доступом к привилегиям клиентов и финансовой информации, а также администрирование активов и обеспечение безопасности требуют правильного управления этими сетями. Финансовые учреждения вкладывают значительные средства в функционирование корпоративных сетей, поскольку это помогает им предоставлять качественные долгосрочные услуги и обеспечивает безопасность.

Основные принципы:

• Безопасность: Безопасность является одной из самых важных проблем для финансовыху чреждений в отношении корпоративных сетей. Защита информации и предотвращение нарушений являются необходимыми для обеспечения безопасности финансовой информации клиентов и самого учреждения.

• Производительность и Эффективность: Корпоративные сети для финансовых учреждений должны быть высокопроизводительными и стабильными. Экономия затрат, оптимизация времени и операционная эффективность играют ключевую роль в этом отношении.

• Резервирование: Наличие резервных сетей и хранилищ данных внутри сети является важным для независимой устойчивости к сбоям системы. Резервирование является критическим принципом для финансовых организаций.

• Управление и Мониторинг: Правильное управление и мониторинг корпоративных сетей необходимы для быстрого выявления технических проблем и обеспечения безопасности.

• Обслуживание клиентов: Предоставление высококачественных услуг клиентам является важным для финансовых учреждений. Обеспечение высокого качества и производительности в сетях важно для достижения этой цели.

• Функционирование корпоративных сетей: