SECURITY SERVICES IN 5G WIRELESS NETWORKS

BIZTONSÁGI SZOLGÁLTATÁSOK AZ 5G VEZETÉK NÉLKÜLI HÁLÓZATOKBAN

ALTALEB, Haya[1]

Abstract

5G wireless networks' innovative design, technologies, and use cases provide new security features and needs. Through unified 5G security standards, shared 5G security principles, and an established 5G security framework, the industry is collaborating to address new security threats posed by 5G architectures, technologies, and services, as well as future security concerns. This article investigates four different forms of security services: authentication (entity authentication, message authentication), confidentiality (data confidentiality, privacy), availability, and integrity. The author evaluated cutting-edge 5G network technologies as well as the New Architectures, Services, and Technologies that will pose security challenges.

Keywords

5G, 5G security challenges, NESAS, "5G Wireless Architecture, Security, and Privacy", Security Services

Absztrakt

Az 5G vezeték nélküli hálózatok innovatív kialakítása, technológiái és használati esetei új biztonsági funkciókat és igényeket kínálnak. Az egységes 5G biztonsági szabványok, a közös 5G biztonsági elvek és a kialakított 5G biztonsági keretrendszer révén az iparág együttműködik az 5G architektúrák, technológiák és szolgáltatások jelentette új biztonsági fenyegetések, valamint a jövőbeni biztonsági problémák megoldásában. Ez a cikk a biztonsági szolgáltatások négy különböző formáját vizsgálja: hitelesítés (entitás-hitelesítés, üzenet-hitelesítés), bizalmas kezelés (adattitoktartás, adatvédelem), elérhetőség és integritás. A szerző értékelte az élvonalbeli 5G hálózati technológiákat, valamint az új architektúrákat, szolgáltatásokat és technológiákat, amelyek biztonsági kihívásokat jelentenek majd.

Kulcsszavak

5G, 5G biztonsági kihívások, NESAS, „5G vezeték nélküli architektúra, biztonság és adatvédelem", biztonsági szolgáltatások

[1] Haya.altaleb@uni-obuda.hu| ORCID: 0000-0002-1442-4037 | Ph.D. candidate Eng., Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

Since the launch of the first generation of mobile technology, many changes have occurred. The 1G period was characterized by briefcase-sized phones and quick interactions between a relatively small number of entrepreneurs. However, the demand for mobile services continued to expand in the years preceding 2G. Pocket-sized phones, SMS, and mobile internet access typified the 3G era. Due to 4G, we have cell phones, app stores, and YouTube. Now that 5G makes new use cases like linked cars, augmented reality, improved video, and gaming, our personal and professional lives are being profoundly revolutionized[1].

According to Ericsson's live 5G networks, there are 125 live 5G Networks in 55 countries around the world, Central & Eastern Europe 19 in 11 countries, and Western Europe 46 in 19 countries[1]. Research trends according to the 4th stage document analysis In 2017, before the 5G network standard was announced, research on general attacks that can occur in 5G networks was mainly conducted. Representatively, in 2017, D Fang et al. conducted a study on wireless network system security among 5G network components. As a result of the study, D Fang et al. conducted eavesdropping and traffic analysis attacks on communication data existing in 5G network base stations, and DDoS (Distributed Denial of Service) attacks, man-in-the-middle attacks and jamming attacks were analyzed and proposed a 5G network wireless architecture that provides flexible authentication as a countermeasure[2]. After that, the 3GPP standard was announced in 2018, and as a result, newly added functions and management compared to the 4G network.

A study on related security requirements was carried out. 2018 As G Arfaoui and others changed to 5G networks, The need for additional security requirements was mentioned[3]. 5G network to derive additional security requirements. Tools for security modeling of work, security design principles, and Security control items were analyzed. Also, I Ahmad et al.Cloud, SDN, the core components of 5G networks, A security problem for NFV was presented [4]. In 2019, possible occurrences on 5G networks linked to threat analysis, attack scenarios, and security solutions proceeded in 2019, RP Jover, etc. By comparing and analyzing the used protocol with the new protocol, Potential attack scenarios in 5G networks, O was analyzed. I Ahmad et al. 5G network Security arises as the environment and new technologies are introduced, analyzed threats, and suggested mitigation techniques.

5G network service was launched in Korea for the first time in the world in April 2019, followed by 5G network service in various countries such as the United States, Europe, China, Japan, and Europe. The market size of the service is expected to increase by approximately 9.4 times in 2023 to $356.5 billion in 2023 compared to 2020 and is expected to increase to $1158.8 billion in 2026, an increase of about 3.3 times compared to 2023.

5G WIRELESS ARCHITECTURE, SECURITY, AND PRIVACY

Cutting-edge technologies are used over 5G networks

Numerous cutting-edge technologies are used over 5G networks to provide new use cases with higher performance needs. Among the most crucial 5G New Radio (NR) technologies created by the 3GPP. Millimeter waves (mm-waves), massive multiple-input, multiple-output (MMIMO), and beamforming are all included in 5G NR are backed [5].

Furthermore, cutting-edge technology such as network function visualization(NFV), software-defined networks (SDNs), device-to-device (D2D) communications, heterogeneous networks (HetNets), and network slicing is also included in 5G. Each is briefly introduced as follows

- 5G New Radio(NR): The NR access technology is constructed for the 5G air interface. There are two frequency ranges, and 5G New Radio will support high data rates and intensive frequency reuse.
- HetNets: In 5G, mm-wave technology is used to increase network performance concerning the data rate as well as the delay. However, one disadvantage of mm-wave transmission is that these signals are more susceptible to interference when passing through physical objects than LTE and Wi-Fi transmissions. 5G makes extensive use of small cells, which have substantially smaller base stations than 4G. HetNets are a characteristic of 5G due to the fact that these tiny cells coexist with the previous robust base stations. With HetNets, 5G may leverage not just the already installed powerful base stations but also small base stations that are energy-efficient.
- D2D: device-to-device communications are described as two nodes communicating directly without going through a base station or a core network they can exist on both licensed and unlicensed spectrum.
- SDNs: This network management technique offers dynamic and programmatically efficient network configuration to provide higher flexibility and easier troubleshooting than traditional decentralized and sophisticated networks.
- NFV: This is an innovative network architecture and software-based network appliances that operate as virtual machines on servers that can replace expensive specialized hardware devices such as firewalls and routers. In high-performance networks, NFVs can offer greater scalability, flexibility, and adaptability at a lower cost than conventional networking solutions.
- Network slicing: Network slicing is a virtual network architecture based on the same concepts as SDN and NFV in a fixed network. As seen in Figure 1, Network slicing enables the construction of several virtual networks for various purposes on top of shared physical infrastructure.

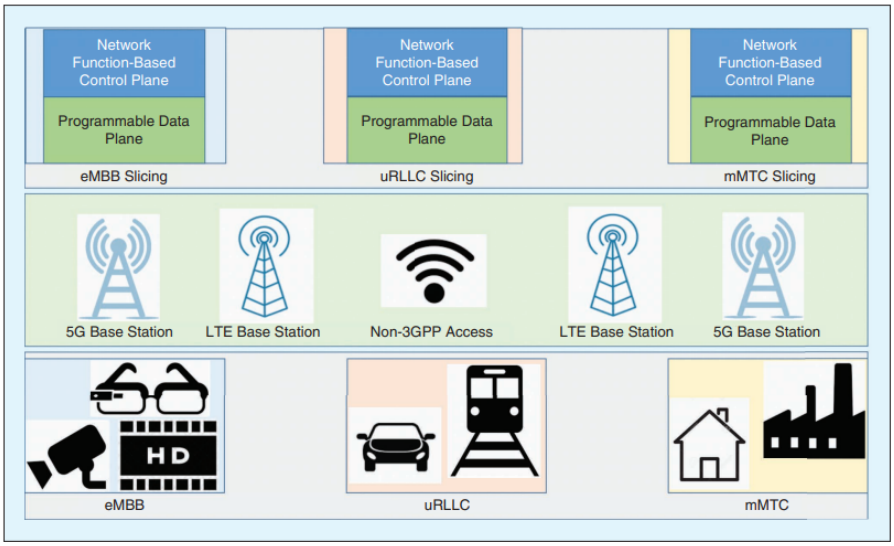

Figure 1: A typical 5G wireless system architecture

Figure 1 describes a basic 5G wireless system design. Different 5G use cases are known as uRLLC, eMBB, and mMTC, respectively. By delivering new access technologies, 5G base stations allow 5G use cases with existing long-term evolution (LTE) base stations and non-Third-Generation Partnership Project (3GPP) connection technologies. The following core network is constructed on the segmentation of the data and control planes to achieve flexible deployment [6]. Moreover, The data plane is configurable, whereas the domain controller is based on network functions. Network slicing could be used to more efficiently manage hardware for a variety of use cases.

The development of new architectures, new technologies, and new applications has brought new challenges to security. On the one hand, 5G has introduced many IT technologies, and asset forms have become more complex and diverse. The application of technologies such as network slicing, edge computing, and network capability opening has brought new challenges. On the other hand, 5G is deeply integrated with vertical industries, and the security requirements have changed from "general security" to "on-demand security."

In order to guarantee the security of 5G networks, the Global System for Mobile Communications (GSMA) has formulated a network equipment security guarantee framework Plan (NESAS) to improve security capabilities through the 5G equipment security assessment. NESAS mainly focuses on large-scale 5G base stations and core network equipment and lacks an assessment mechanism for network operation security, data asset security, etc. The ARMIT model starts from 5G network assets.

Based on the composition and security threats, the security requirements, security capability evaluation index system, and evaluation method applicable to 5G assets and network operation are constructed. A practical reference is provided for equipment companies and operators to conduct security capability evaluation of 5G products, networks, and services[7].

5G Security Architecture

The 5G wireless security architecture is depicted in the following Figure:

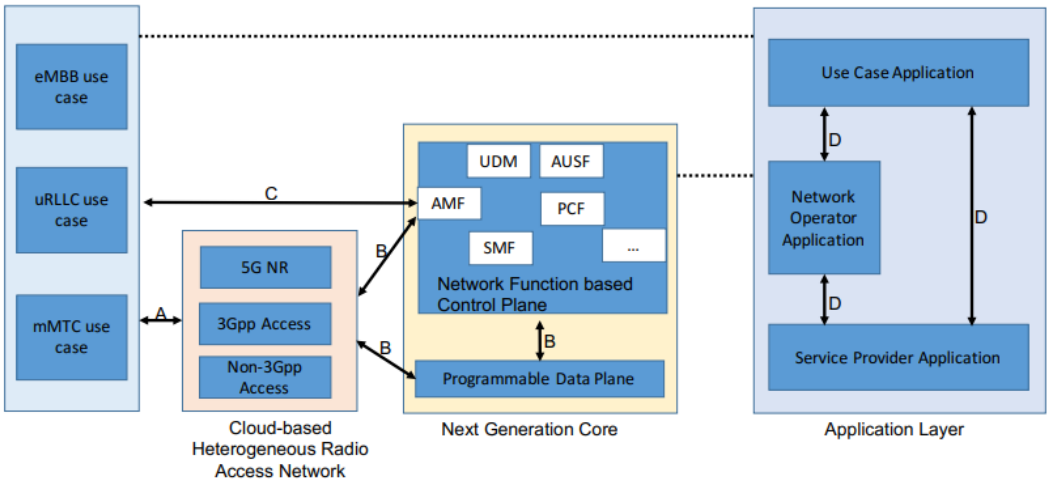

Figure 2:5G security architecture.[2]

eMBB, uRLLC, and mMTC are the classifications for three distinct types of user interface use cases. A cloud-based heterogeneous radio access network is implemented to enable various use cases.

In order to enhance the flexibility and efficiency of next-generation networks, the core network's control plane and data plane are separated, with the data plane being programmable and the control plane being application-specific. The essential network functionalities of the next-generation core's control plane are outlined in TR 23.799.

5G New Architectures, Technologies, and Services Will Bring Security Challenges

Overall, the majority of risks and challenges confronting 5G security are the same as those confronting 4G security. Nonetheless, the added security concerns brought to 5G networks by new architectures, technology, and services must be considered.

Through unified 5G security standards, shared 5G security principles, and an established 5G security framework, the industry is working together to address new security threats posed by 5G architectures, technologies, and services, as well as future security difficulties. In 2020, 111 businesses worldwide (including their subsidiaries) submitted technical specialists to six SA3 meetings to produce the most recent 5G security standards.

The 3GPP SA3 Working Group has formed 42 projects to investigate security vulnerabilities and risks in various 5G scenarios. These programs' findings are increasingly being incorporated into security standards. To assess the security of mobile network equipment development and verification, the GSMA and 3GPP jointly define NESAS[9].

Figure 3: Security issues brought to 5G networks by new architectures, services, and technology must be considered. [8].

Based on expected 5G network threats and critical security solutions, the GSMA 5G Cybersecurity Knowledge Base recommends the security paradigm of shared responsibility and baseline security controls. The 5G security architecture's top-down design principles enable a systematic, dynamic, and adaptive security framework. I believe that 5G cyber security is manageable and provable with these solutions[8].

SECURITY SERVICES IN 5G WIRELESS NETWORKS

In 5G wireless networks, the new architecture, technology, and use cases present encryption techniques and needs. Iwill cover four types of security services in this section: Authentication (entity authentication, message authentication), Confidentiality (data confidentiality, privacy), Integrity, and Availability are the four pillars of information security.

Authentication

Entity authentication and message authentication are the two types of authentication. To combat attacks, 5G wireless networks require both entity authentication and message authentication. Entity authentication ensures that the communicating entity is who it claims to be. Before the two parties connect in legacy cellular networks, mutual authentication between user equipment (UE) and mobility management entity (MME) is implemented. The essential security aspect in the classic cellular security architecture is mutual authentication between UE and MME.

In 4G LTE cellular networks, authentication, and key agreement (AKA) is based on symmetric keys. 5G, on the other hand, necessitates authentication not just between UE and MME, but also between other parties such as service providers. Because the trust paradigm in 5G differs from that in previous cellular networks, hybrid and flexible authentication management is required.

The hybrid and adaptable authentication for UE may be accomplished in three forms: authentication by the network alone, authentication by a service provider alone, or authentication by both the network and the provider together. Due to the exceptionally high data transmission and pretty low latency required by 5G wifi networks, authenticating in 5G is anticipated to be considerably faster than ever before. In addition, 5G's multi-tier design may need a regular handover process and verification between layers.

In [10], "To overcome the challenges of key management in HetNets and to reduce the unnecessary latency caused by frequent handovers and authentications between different tiers. An SDN-enabled fast authentication scheme based on weighted secure-context-information transfer is proposed to improve the efficiency of authentication during handovers and to meet the 5G latency requirement".

To deliver additional security customer services in 5G wireless networks, Message authentication is becoming increasingly critical in 5G wireless networks due to the variety of new applications. Furthermore, with 5G's stricter latency, spectrum efficiency (SE), and energy efficiency (EE) standards, message authentication is facing additional hurdles. [11]proposes an effective Cyclic Redundancy Check (CRC)-based message authentication for 5G to identify both random and malicious errors without increasing bandwidth.

Confidentiality

Privacy and data confidentiality are two features of confidentiality. Data confidentiality secures data transfer against passive attacks by limiting data access to authorized users and banning entry or disclosure to unauthorized entities. Privacy prohibits an attacker from managing and altering information about authorized users, for example, privacy shields traffic flows from any examination.

The traffic patterns can be applied to diagnose sensitive information, such as the location of senders and recipients. Massive data linked to user privacy exists in numerous 5G applications, such as car navigation data, health monitoring data, etc.

Commonly, data encryption is used to safeguard data privacy by prohibiting unauthorized users from obtaining relevant information from broadcasted data. Using a single encryption key owned by the sender and receiver, the symmetric encryption mechanism may be used to encrypt or decrypt data. To convey a password between the sender and

recipient, a reliable key distribution method is necessary. Traditional encryption methods are built on the idea that attackers have limited computational power.

As a result, combating attackers with high computer capabilities is difficult. PLS may offer confidentiality services rather than relying on conventional higher-layer cryptographic techniques [12] against eavesdropping and jammer assaults Aside from 5G internet services, people are beginning to recognize the need for privacy protection services. Because of the massive data connections, privacy service in 5G demands substantially more care than in legacy cellular networks.[13]

Availability

Availability is the extent to which a service is straightforward and used by authorized operators whenever and whenever they request it. 5G's fundamental performance statistic, availability, measures the system's resilience against multiple threats. Availability assault is a common form of active attack.

DoS attacks, which can deny genuine users access to a service, are one of the most significant attacks lying on availability. In addition, by interfering with radio signals, jamming or interference can interrupt the communication links between authorized users. To assure service availability, 5G wireless networks confront a significant problem in preventing jamming and DDoS attacks in the presence of vast numbers of unprotected IoT nodes.

DSSS and FHSS are two conventional PLS methods for availability at PHY. In the 1940s, DSSS was initially applied to the military. In DSSS, a pseudo-noise spreading code is multiplied by the original data signal's spectrum. Without knowledge of the code for spreading pseudo noise, a jammer requires a far greater amount of power to disrupt a valid transmission. For FHSS, a signal is conveyed by rapidly switching between numerous frequency channels via a pseudorandom sequence generated by a shared key between the transmitter and receiver.

To improve 5G SE, dynamic spectrum is employed in D2D communications and the cognitive radio paradigm. Adem et al. [14] noted that the jamming attack could negatively impact the performance of FHSS. A pseudorandom time-hopping spread spectrum is presented to enhance the performance of the probability of interference, the likelihood of switching, and the possibility of error. In addition, adopting resource allocation improves the identification of availability violations [15].

Integrity

Notwithstanding the fact that message authentication certifies the origin of the transmission, there is no protection against message duplication or tampering. 5G wants to enable connectivity at any anytime, anywhere, and in any method, as well as to closely support apps. tied to everyday human life, such as water quality monitoring and transit schedules. Therefore, data integrity is one of the most essential security criteria for specific applications.

Integrity prohibits active assaults from unauthorized organizations from modifying or altering information. Insider malicious attacks, such as message injection or data alteration, can compromise data integrity. Since insider attackers possess legitimate identities, it is challenging in order to identify these attacks.

In use scenarios such as smart meters in a smart grid[16], data integrity service against tampering must be supplied. Associated with voice interactions, the database may be attacked and altered more readily. Mutual authentication can be used to offer integrity services by generating an integrity key.

CONCLUSION

Numerous cutting-edge technologies are used over 5G networks to provide new use cases with higher performance needs. which required Security Services in 5G Wireless Networks and introduce new security features and requirements The application of technologies such as network slicing, edge computing, and network capability opening has brought new challenges. On the other hand, 5G is deeply integrated with vertical industries, and the security requirements have changed from "general security" to "on-demand security." To guarantee the security of 5G networks, the Global System for Mobile Communications (GSMA) has formulated a network equipment security guarantee framework Plan (NESAS) to improve security capabilities through the 5G equipment security assessment. NESAS mainly focuses on large-scale 5G base stations and core network equipment and lacks an assessment mechanism for network operation security, data asset security, etc.

REFERENCES

[1] www.ericsson.com/en/5g, “What is 5G? How will it transform our world? - Ericsson,” *Www.Ericsson.Com*, 2021. [Online]. Available: https://www.ericsson.com/en/5g. [Accessed: 26-Jul-2022].

[2] D. Fang, Y. Qian, and R. Q. Hu, “Security for 5G Mobile Wireless Networks,” *IEEE Access*, vol. 6, pp. 4850–4874, Nov. 2017, doi: 10.1109/ACCESS.2017.2779146.

[3] G. Arfaoui *et al.*, “A Security Architecture for 5G Networks,” *IEEE Access*, vol. 6, pp. 22466–22479, 2018, doi: 10.1109/ACCESS.2018.2827419.

[4] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, “Overview of 5G Security Challenges and Solutions,” *IEEE Commun. Stand. Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[5] C. J. Zhang *et al.*, “Key Technology for 5G New Radio,” *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 10–11, Mar. 2018, doi: 10.1109/MCOM.2018.8316580.

[6] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, “A survey on low latency towards 5G: RAN, core network and caching solutions,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3098–3130, Aug. 2018, doi: 10.1109/COMST.2018.2841349.

[7] “**面向**5G资产的统一安全评测模型与体系构建-【维普官方网站】-www.cqvip.com-维普网.” [Online]. Available: http://www.cqvip.com/qk/72202x/20215/7104512625.html. [Accessed: 26-Jul-2022].

[8] Huawei, “Huawei 5G Security White Paper - Huawei,” 2020.

[9] M. Shatnawi, H. Altaleb, and R. Zoltan, “The Digital Revolution with NESAS

Assessment and Evaluation," *2022 IEEE 10th Jubil. Int. Conf. Comput. Cybern. Cyber-Medical Syst.*, pp. 000099–000104, Jul. 2022, doi: 10.1109/ICCC202255925.2022.9922821.

[10] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," *2016 IEEE Int. Conf. Commun. ICC 2016*, Jul. 2016, doi: 10.1109/ICC.2016.7510994.

[11] E. Dubrova, M. Näslund, and G. Selander, "CRC-based message authentication for 5G mobile technology," *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 1186–1191, Dec. 2015, doi: 10.1109/TRUSTCOM.2015.503.

[12] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015, doi: 10.1109/MCOM.2015.7120011.

[13] O. Auciello, "IEEE Xplore Full-Text PDF_李玲琪 自聚焦 写波导," *Proceedings of the 2011 IEEE International Conference on Robotics and Biomimetics*, 2011. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6420380%0Ahttps://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4405051&casa_token=geFETzjuYooAAAAA:2_Hb4AUCKNIV9SJOGZKpkv8GB_DwIuTU0A4GfMyCc44LIEMKz7OpjKTFzmC8tAmzXW5NfB93iRU%0Ahttps://ieeexplore.ie. [Accessed: 28-Sep-2022].

[14] N. Adem, B. Hamdaoui, and A. Yavuz, "Pseudorandom time-hopping anti-jamming technique for mobile cognitive users," *2015 IEEE Globecom Work. GC Wkshps 2015 - Proc.*, 2015, doi: 10.1109/GLOCOMW.2015.7414043.

[15] M. Labib, S. Ha, W. Saad, and J. H. Reed, "A Colonel Blotto Game for Anti-Jamming in the Internet of Things," pp. 1–6, Mar. 2016, doi: 10.1109/glocom.2015.7417437.

[16] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012, doi: 10.1109/SURV.2012.010912.00035.