AI Letters

Journal homepage: www.ail.sigmaxplore.com

AI Letters 2, Article ID: 2926, 1–2, April 2025 ISSN 3065-3525

Addressing the Unknowns: A Professional Perspective on the Cybersecurity of 5G Technology

Abu Zahid Md Jalal Uddin[1*], Farzana Akter Shemu[2]

Abstract

Enabling more connectivity for the sake of enhanced mobile broadband, including the Internet of Things (IoT) and digitized logistics, Fifth Generation(5G) has bandwidth and integration security challenges. Hence under heavy loads, the performance of its hardware and many aspects of the data security of users remain unknown. Cybersecurity professionals are still trying to make 5G safe, secure, reliable, and accessible. This paper provides a comprehensive review of the far-reaching security implications of emerging 5G technology on broadband connectivity.

Keywords: 5G, security, wireless, malicious software, legacy vulnerabilities

1. Introduction

Ensuring faster speed, lower latency, and higher capacity than 4G LTE, the 5G wireless technology is widely accepted in the world [1]. 5G offers a speed of 20 gigabits per second (Gbps) which is much faster, like 200 times than LTE's highest speeds [2]. Alongside the value of latency, capacity, coverage, and frequency bands are mostly worthy of commendation in the world. Since 5G connectivity is still being deployed can be vulnerable to security risk. As essential to the digital mobile society utilize a dedicated 5G core to fully leverage 5G's features, such as ultra-low latency and improved network slicing capabilities called Stand-Alone (SA), option 2-shown in Figure 1, is a network that operates independently based on previous generation networks. Side by side, Non-Stand-Alone (NSA) is another deployment model that relies on existing 4G LTE infrastructure while integrating 5G radio access technology to enhance speed and capacity, enabling gradual transition to full 5G capabilities without the need for a completely new network build-out [3]. Since 5G builds upon previous wireless networks, it's currently being integrated with 4G LTE networks.

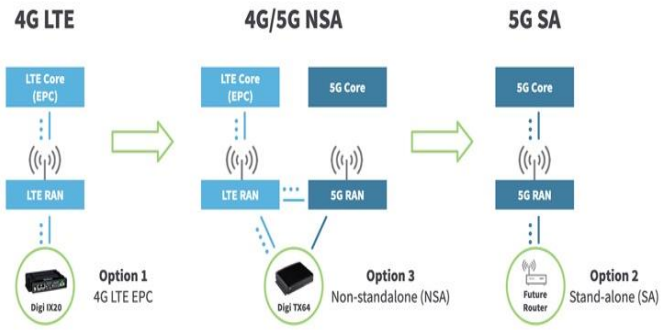

Figure 1. 5G SA and NSA network architecture compared to 4G network [4].

2. Analysis

The highly demanding 5G network architecture is complex. High-speed data transmission of 5G in Millimeter wave (mmWave) is a radio frequency spectrum band that is used in 5G wireless technology to provide high-speed data transmission. 5G high-band delivers the highest frequencies of 5G (24 GHz to approximately 100 GHz), 2 to 6 GHz in mid-band and below 2GHz is low-band coverage also used for 4G LTE [5]. 5G mmWave faces challenges such as high signal attenuation and poor penetration due to shorter wavelengths. These issues limit indoor coverage and require dense infrastructure, like small cells, for effective transmission, making it costly and complex to deploy in urban environments with many physical obstructions.

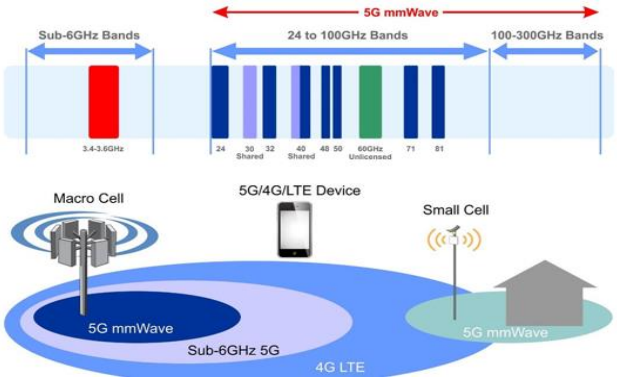

Figure 2. 5G mmWave Bandwidth offering massive covering with capacity

Using the existing 4G infrastructure, the seamless transition and enhanced user experience have come true as shown in Figure 2. Also, many 5G networks utilize Dynamic Spectrum Sharing (DSS) to repurpose 4G bands, allowing operators to provide 5G services alongside 4G [6].

In this way, cyber security specialists are concerned that untrusted components, such as malicious or poorly developed software, which are installed into the infrastructure of 5G, may be inherent in 4G [7]. According to the U.S. General Service Administration (GSA), these kinds of legacy vulnerabilities include Exfiltration risks, Distributed denial-of-service attacks, and Signaling System 7/Diameter challenges that threaten confidentiality also with availability [8]. More other attacks are shown below.

Additionally, The National Security Agency (NSA) in the United States reported the significant security challenge in 5G is multi-tenancy like mobile network operators and the use of shared physical arrangements by multiple cloud infrastructures [9]. The cloud-native 5G networks can deteriorate or be compromised since it is a lucrative target for cyber threat actors, which is a common concern of the NSA [10].

[1] School of Information Technology, Washington University of Science and Technology, Alexandria, VA, USA
[2] Statistics Department, Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur, Bangladesh
* Corresponding Author: Abu Zahid Md Jalal Uddin
E-mail address: abu.student@wust.edu

Received: 23 October 2024; Revised: 3 December 2024; Accepted: 6 December 2024

3. Discussion

Since 5G networks use 4G base stations and network components, it inherits risks of vulnerabilities if they (old equipment) contain them. One major risk arises from purchasing network components, such as base stations and

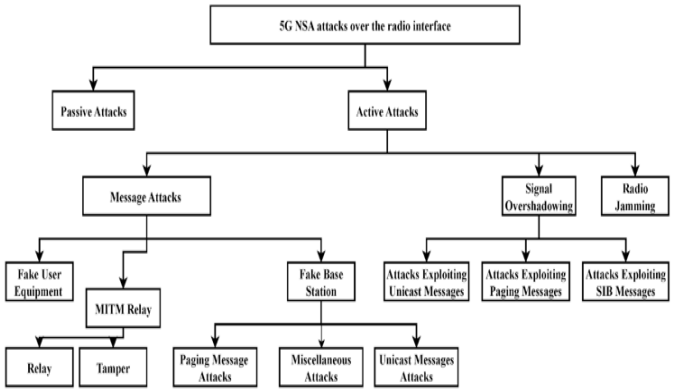

Figure 3. Possible attacks transferring from 4G to 5G NSA Networks shown on the above taxonomy.

routers, from poorly built hardware or suppliers with malign intentions. If vendors or contractors provide substandard or negotiated equipment, confidentiality could be compromised, as unauthorized parties might intercept or manipulate data. The heavy dependency on the existing 4G infrastructure of 5G-NSA architecture, which utilizes 4G LTE for control and signaling while using 5G NR (New Radio) for high-speed data transmission [11]. Alongside, many operators built their networks without safety-security concerns. They apply a security policy when paid customers have started to use it [12]. The White House security review highlighted the safety vulnerabilities of Huawei as a concern rather than spying [13]. Following this, the U.S. government enacted measures to restrict purchasing equipment from the untrusted source of Chinese telecom companies, including Huawei, citing national security risks. In 2020, reports emerged alleging Huawei could exploit security backdoors in its equipment. That allows attackers to gain unauthorized access to sensitive data [13] [14].

Furthermore, the integrity of 5G networks can be undermined by malware-coded software or vulnerabilities in software-defined networking (SDN) and network slicing technologies, which are fundamental to 5G's flexible and scalable architecture [15]. Cybercrooks could exploit these vulnerabilities to tamper with corrupt network data, undermining trust in the system. Then, the availability of 5G services may be impaired if endangered components or software result in service disruptions or denial-of-service (DoS) attacks, especially as 5G networks depend heavily on virtualized systems and cloud infrastructures that are vulnerable to targeted attacks [16].

4. Conclusion

The reliance on 4G infrastructure for 5G deployment introduces critical security concerns that we have already discussed, including the risk of compromised equipment from untrusted suppliers like Huawei, which has been proven. These vulnerabilities threaten the confidentiality, integrity, and availability of the CIA triad of 5G networks, potentially enabling unauthorized access and service disruptions, and undermining trust in advanced telecommunications systems.

To mitigate these security risks, the U.S. must prioritize purchasing equipment from trusted, certified vendors and enforce strict supply chain security protocols [17]. Implement-to-end encryption using protocols like TLS 1.3, deploy network slicing for isolated resources, and utilize advanced firewalls to protect against DDoS attacks, enhancing 5G security and resilience. Enhanced monitoring and security auditing will be crucial to maintaining the durability and trustworthiness of 5G networks as they evolve.

Conflict of Interest Statement

The author declares no conflict of interest.

References

[1] Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila andA. Gurtov, Overview of 5G Security Challenges and Solutions, IEEE Communications Standards Magazine 2, (2018) 36 – 43.
[2] X. Liu, P. Wang, Z. Lan and B. Shao, Biological characteristic online identification technique over 5G network, IEEE Wireless Communications, 22 (2015) 84 – 90.
[3] M. S. Wani, et al., Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy, Journal of Cybersecurity and Privacy 4 (2024).
[4] What is 5G network architecture? (2021, March 19). IIoT Devices and Services for M2M Networking Digi International. https://www.digi.com/blog/post/5g-network-architecture
[5] H. Remmert, "What Is 5G Network Architecture?" Digi.com, Digi International, https://www.digi.com/blog/post/5g-network-architecture. Accessed 6 Nov. 2024.
[6] 5G NR: The Next Generation of Mobile Broadband," 3GPP.
[7] Ancans, Guntis, et al, Analysis of characteristics and requirements for 5G mobile communication systems, Latvian Journal of Physics and Technical Sciences 54.4 (2017): 69-78.
[8] GSA.gov,https://buy.gsa.gov/api/system/files/documents/GSA%20Acquisition%20Guidance%20for%20Procuring%205G%20Technology%20508_0.pdf. Accessed 24 Oct. 2024.
[9] Security Guidance for 5G Cloud Infrastructures, National Security Agency. 2021
[10] Part III: Data Protection. "Security Guidance for 5g Cloud Infrastructures,"Cisa.gov,https://www.cisa.gov/sites/default/files/202302/security_guidance_for_5g_cloud_infrastructures_part_iii_508_compliant.pdf. Accessed 24 Oct. 2024.
[11] Alnaas, Mohammed&Alhodairy,Osama. (2024). Comparison of 5G Networks Non-Standalone Architecture (NSA) and Standalone Architecture (SA). International Journal of Computer Science Engineering Techniques. 8. 2024.
[12] Report on 5G Security Issue (2019), Positive technology
[13] New law bans US gov't from buying tech from Chinese giants ZTE and Huawei". Ars Technica. Archived from the original on 29 May 2019. Retrieved 1 October 2018.
[14] Bishop, Matthew. "Huawei and the U.S. 5G Network: Security Risks and Responses." Journal of Cybersecurity Policy, vol. 3, no. 2, 2020, pp. 143-161.
[15] Zhao, W., et al. "Security Vulnerabilities in the 5G and 4G Integrated Architecture." Cybersecurity Review, vol. 5, no. 2, 2021, pp. 112-128.
[16] Li, Z., et al., 5G Non-Standalone Architecture: Enhancing Deployment Efficiency in Urban Centers., IEEE Transactions on Network and Service Management 18 (2021) 30 – 42.
[17] U.S. Department of Homeland Security, Cybersecurity Risks in 5G Infrastructure, U.S. Government, (2021), www.dhs.gov/5g-security-report.