DOI: 10.15849/IJASCA.231130.04

Int. J. Advance Soft Compu. Appl, Vol. 15, No. 3, November 2023
Print ISSN: 2710-1274, Online ISSN: 2074-8523

5G Security, Challenges, Solutions, and Authentication

Yahia Hasan Jazyah

Faculty of Computer Studies, Arab Open University, Kuwait
e-mail: yahia@aou.edu.kw

Abstract

Fifth-Generation (5G) of wireless technology represents a significant leap forward in mobile communication networks. It promises to provide faster speeds, lower latency, and greater network capacity than previous mobile generations, enabling a wide range of new applications, in addition to high standard of security and privacy. 5G networks are designed to support a massive number of devices, including the Internet of Things (IoT) devices, autonomous vehicles, and virtual reality.

5G networks introduce new security challenges and risks. As such, 5G security is a critical component of the technology's deployment, depending on advanced authentication, encryption, and access control techniques in order to protect the confidentiality, integrity, and availability of data and services transmitted over 5G networks. Several works have been done focusing on the 5G and its related topics, but none of them provides deep analysis and clear overview in the field. This work focuses on 5G security issues and highlighting the challenges and proposed solutions, standards, and analysis, in addition to the architecture of 5G network and authentication process of both 4G and 5G.

Keywords: *5G, authentication, privacy, security.*

1. Introduction

Fifth-generation (5G) wireless technology represents a significant evolution in mobile communication networks, providing faster data speeds, lower latency, and greater capacity than previous generations. The key technologies that underpin 5G include massive MIMO antennas [1], millimeter-wave (mmWave) frequencies [2], and software-defined networking.

The high-speed and low-latency capabilities of 5G networks are expected to enable a wide range of new applications, such as smart cities, virtual reality (VR) and augmented reality (AR) [3], and autonomous vehicles. However, the deployment of 5G networks presents new security challenges and risks, and 5G security is a critical challenge of the technology's development.

Received 6 June 2023; Accepted 5 September 2023

In order to ensure the confidentiality, integrity, and availability of data and services transmitted over 5G networks, advanced authentication, encryption, and access control mechanisms are being employed. As 5G continues to be developed worldwide, continued investment in research, development, and security will be crucial to unlocking its full potential.

Advanced authentication and access control mechanisms are used to ensure that only authorized users and devices can access the network and its resources. Robust encryption algorithms are used to protect the confidentiality and integrity of data transmitted over 5G networks, while network slicing enables the creation of different virtual networks that can have their own unique security requirements.

Several works present related subjects about 5G. But this work highlights the security concerns and challenges of 5G, 5G security threats, and types of those threats, proposed solutions to overcome or mitigate such threats, and the required security standards of 5G networks. Then it provides deep details of 5G architecture and how it works, including the security architecture of 5G, in addition to the authentication process of both 4G and 5G, and shows how 5G enhances the process of authentication in comparison to 4G, and highlighting the differences between 4G and 5G in terms of authentication.

The remaining of this article organized as follows: part 2 presents 5G architecture. part 3 presents 5G security architecture, part 4 presents 5G security concerns and its challenges, part 5 presents 5G security threats, part 6 presents security solutions, part 7 presents analysis of security solutions, part 8 presents 5G security standards, part 9 presents Authentication in 4G Networks, part 10 presents open challenges for researches, and finally, part 11 is the conclusion.

2. 5G Architecture

5G architecture [4] refers to the design and organization of all components that form a 5G network. It includes both the core network and the Radio Access Network (RAN) that enables the delivery of high-speed, low-latency communication to a large number of connected devices.

The architecture of 5G network is designed to provide a more flexible, scalable, and efficient network than previous generations of mobile networks. It uses a cloud-native approach with distributed computing and virtualization technologies to provide faster and more reliable communication services.

It is divided into three main components: RAN, the core network, and the edge computing network.

The RAN connects the user equipment (UE), such as smartphones and IoT devices, to the 5G network through the use of small cells and beamforming technologies.

Beamforming is a signal processing technique used in wireless communication systems to enhance the quality and reliability of wireless transmissions. It is focusing radio waves in

a specific direction, instead of broadcasting in all directions, which can lead to interference and signal attenuation.

Beamforming technology [5] uses multiple antennas and complex algorithms to selectively amplify and direct the radio signal towards a specific location. This can increase the range, speed, and capacity of wireless transmissions, as well as improving the reliability of wireless connections in areas with high levels of interference and congestion.

The second component of 5G network is the core network which is responsible for managing the data flow and routing between different devices and applications. It also provides services such as authentication, billing, and quality of service (QoS) control.

The last part is edge computing network that brings compute resources closer to the end user, reduce latency and enable new services such as augmented reality and autonomous vehicles. Figure 1. Shows the architecture of 5G network, where UE is the User Equipment.

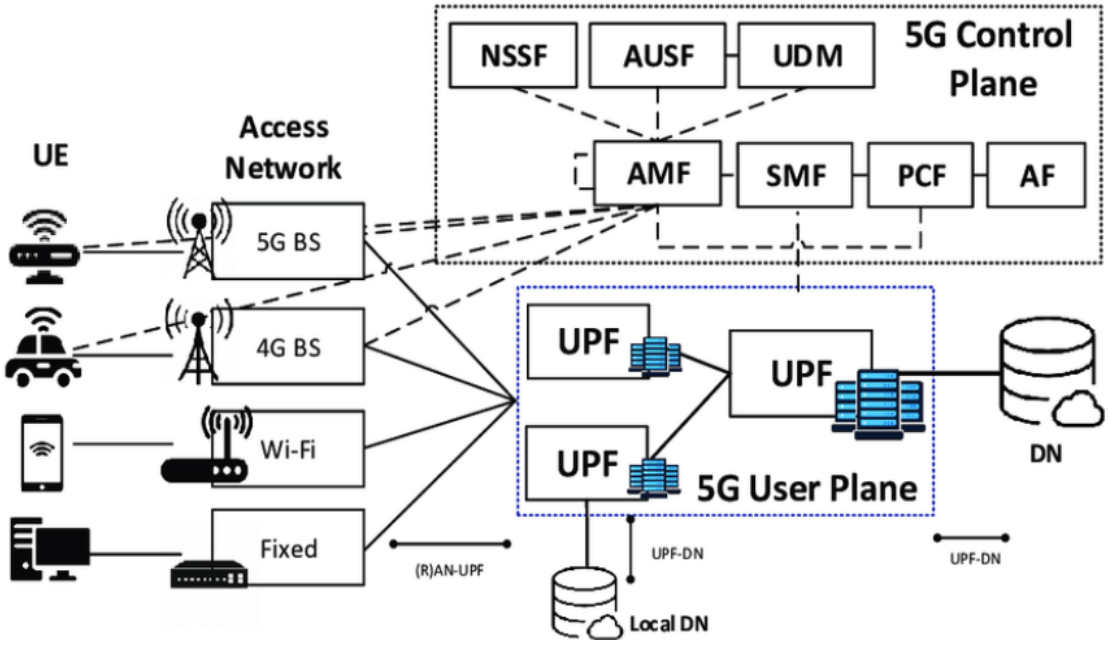

Figure 1. 5G Network Architecture. [6]

AMF is the Core Access and Mobility Management Function, it is responsible for a lot of functions and services, such as: termination of RAN Control Plane interface, Mobility Management, lawful intercept (for AMF events and interface to Lawful Intercept System - LIS), Access Authentication, Access Authorization, Security Anchor Function (SEA) that interacts with the Unified Data Management (UDM) and the UE, receives the intermediate key that was established as a result of the UE authentication process; in case of USIM based authentication, the AMF retrieves the security material from the UDM, Security Context Management (SCM): it receives a key from the SEA that it uses to derive access-network specific keys.

User plane Function (UPF) which provides several functions such as: QoS handling for User Plane, packet routing and forwarding, packet inspection and Policy rule enforcement,

support for interaction with external Data Network (DN) for transport of signalling for Protocol Data Unit (PDU) session authorization/authentication by external DN.

Session Management Control Function (SMF) which provides the following: session management, allocation and management of UE IP address, selection and control of UPF, termination of interfaces towards policy control and charging functions, control of QoS, termination of Session Management parts of Non-Access Stratum (NAS) messages, Downlink Data Notification (DDN), initiator of access node specific Session Management information, roaming functionality, handle local enforcement to apply QoS service level agreement (SLA) to Visited Public Land Mobile Network (VPLMN), charging data collection and charging interface of VPLMN.

Authentication Server Function (AUSF) that Performs authentication processes with the UE
Unified Data Management (UDM), AUSF supports Authentication Credential Repository and Processing Function (ARPF); ARPF stores the long-term security credentials used in authentication for 5G Authentication and Key Agreement (AKA), and storing of subscription information.

Policy Control Function (PCF) that provides support of unified policy framework to govern network behaviour, policy rules to control plane function(s) that enforce them. Application Function (AF) that Requests dynamic policies and/or charging control.

3. Security Architecture of 5G Networks

The security architecture of 5G networks [7] [8] is designed to address the unique security challenges and requirements introduced by the 5G wireless technology. It incorporates various security measures and protocols to protect the network infrastructure, user data, and communication channels. Some of the key components of the security architecture of 5G networks are listed below:

Authentication and Identity Management (AIM). 5G networks use mutual authentication mechanisms to verify the identity of network entities, such as devices, users, and network functions, which helps prevent unauthorized access and protects against identity spoofing attacks.

The authentication process involves the following steps:

1) Initial Authentication: When a device attempts to connect to a 5G network, it initiates an authentication procedure. The UE sends a request to the network, and the network responds by challenging the UE to prove its identity.

2) Authentication Vector Generation: The 5G network generates an Authentication Vector (AV) that consists of a random challenge (RAND) and an expected response (XRES). The AV is unique to the UE and the authentication procedure.

3) Authentication Request: The UE sends an Authentication Request message to the network, including its International Mobile Subscriber Identity (IMSI) or other identifying information.

4) Authentication Response: The network receives the Authentication Request and generates a response based on the AV. It calculates the expected response (XRES) using the UE's authentication key (Ki) and the RAND from the AV.

5) Authentication Confirmation: The network sends an Authentication Response message to the UE, including the XRES and RAND. The UE performs its own calculation of the expected response (XRES) using its authentication key (Ki) and the received RAND.

6) Authentication Result Verification: The UE compares the calculated XRES with the received XRES from the network. If they match, the UE confirms the authenticity of the network. If there is a mismatch, it indicates a potential security threat, and the authentication process may be terminated.

7) Key Derivation: Once the authentication is successful, both the UE and the network derive session keys, such as the encryption key (Kenc) and integrity key (Kint). Those keys are used for securing the subsequent communication between the UE and the network.

Figure 2. summarizes the previous process.

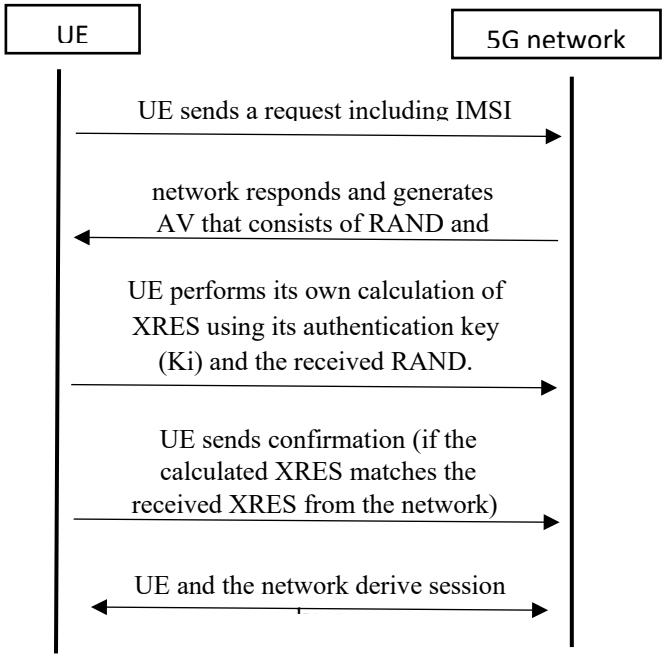

Figure 2. Authentication Process in 5G Networks

Encryption and Privacy. 5G networks employ strong encryption algorithms to secure data transmitted over the air interface and core network. It ensures that the communication

between devices and the network remains confidential and prevents eavesdropping and data tampering.

5G networks use the Advanced Encryption Standard (AES) algorithm, which is a symmetric encryption algorithm. It uses a key length of 128, 192, or 256 bits to encrypt and decrypt data.

5G employs integrity protection mechanisms [9] to ensure that no body tampered with data during transmission. The integrity algorithms used in 5G include Galois/Counter Mode (GCM) and the Cipher-based Message Authentication Code (CMAC). These algorithms verify the integrity of data by adding an authentication tag.

5G introduces network slicing [10], which enables the creation of virtual networks tailored for specific use. Each network slice has its own security requirements and policies to ensure isolation and protect critical services from potential security threats.

5G networks influence virtualization technologies [11] in order to enable efficient resource allocation and flexible network management. Security measures protect the virtualized infrastructure, ensure the integrity and isolation of virtual network functions.

5G enables edge computing capabilities, and bring computation and data storage closer to the network edge. Security mechanisms are implemented to protect edge computing resources and ensure secure processing of sensitive data at the edge.

5G networks incorporate security monitoring tools and techniques to detect and respond to security incidents promptly. Intrusion detection systems, log analysis, and security information and event management (SIEM) systems are used to identify and mitigate security threats.

Security measures are implemented at the network function level to protect against attacks targeting specific network elements. Those measures include access control, secure configuration, and regular security updates for network functions.

5G security architecture adheres to industry standards and regulations by 3GPP and other relevant organizations. It complies with these standards in order to ensure interoperability and consistent security practices across different 5G deployments.

4. 5G Security Concerns and Challenges

The deployment of 5G wireless technology presents new security concerns that must be addressed to ensure the confidentiality, integrity, and availability of data and services transmitted over 5G networks. Some of the main 5G security concerns are:

1. Increased attack surface [12]. Whereas 5G networks are more complex than former generations of wireless technology, and their deployment introduces new attack surfaces that could be exploited by cybercriminals.
2. IoT security [13] [14]. Whereas IoT is expected to play a significant role in the adoption of 5G, and the increased number of connected devices increases the potential attack

environment. Many IoT devices have weak security features, making them more vulnerable to cyberattacks.

3. Network slicing security [10] that enables different virtual networks to be created on the same physical infrastructure, each with its own unique security requirements. Ensuring the security of each network slice can be a challenge.
4. Supply chain security [15]. The global supply chain for 5G technology is complex and involves many different vendors and increase the risk of a compromise in the supply chain that could result in security vulnerabilities.
5. The increased connectivity provided by 5G networks can increase the amount of personal data being collected and transmitted, raising privacy concerns. [16]
6. Network virtualization [11] that the 5G networks will rely heavily on it, which creates new challenges for securing the virtualized environment.
7. As with any network, 5G networks will be vulnerable to insider threats, including employees with access to sensitive information and malicious insiders. [17]

And to address 5G security concerns, ongoing research, development, and investment in 5G security are essential. Additionally, robust authentication, encryption, access control, and monitoring mechanisms are being implemented to protect against potential security threats.

In addition, organizations need to adopt a comprehensive approach to 5G security, including implementing security best practices, conducting regular risk assessments, and collaborating with industry partners to share threat intelligence.

5. 5G Security Threats

The advent of 5G technology promises a revolutionary leap in connectivity and wireless communications, enabling faster data speeds, ultra-low latency, and the seamless interconnection of billions of connected devices. This transformative potential is accompanied by an array of new security challenges that need to be carefully navigated. As the world embraces the era of 5G networks, it becomes paramount to understand and address the distinct security threats that this advanced technology landscape presents.

In this context, exploring the realm of 5G security threats becomes a critical endeavour. From the proliferation of IoT devices to the complex interplay of virtualization and cloud technologies, 5G networks introduce a plethora of vulnerabilities that malicious actors could exploit. Next is a list of potential threats that can appear in 5G networks. [18]

a) Man-in-the-middle attacks [19]. where attackers can intercept and modify data transmitted between devices and the 5G network, compromising the confidentiality and integrity of the communication.
b) Denial-of-service attacks (DoS) [20] [21]. Attackers can overload 5G networks with a large volume of traffic, disrupting communication and causing service outages.
c) Network slicing attacks [10]. Network slicing allows the creation of virtual networks within the 5G infrastructure. Attackers can exploit vulnerabilities in the network slicing technology to gain unauthorized access to the network.

d) Rogue base station attacks [22]. Attackers can set up rogue base stations to intercept and manipulate data, compromise user privacy, and steal sensitive information.
e) IoT device attacks [13] [23]. 5G networks will support a large number of IoT devices, which may have weak security, making them susceptible to exploitation by attackers.
f) Supply chain attacks [15]. The global nature of 5G supply chains can create vulnerabilities that attackers can exploit to introduce malicious code into the network.
g) Insider threats [19]. Employees with authorized access to the 5G network can intentionally or unintentionally compromise the security of the network.
h) Malware and ransomware attacks [24]. 5G networks will enable faster and more efficient delivery of malware and ransomware attacks. With the increased speed and capacity of 5G networks, attackers can launch more powerful distributed denial-of-service (DDoS) attacks, causing significant damage to organizations.
i) Identity theft [9]. 5G networks will rely heavily on digital identity and authentication mechanisms, which can be vulnerable to attack. Hackers can steal or spoof digital identities, allowing them to gain unauthorized access to networks and data.
j) Side-channel attacks [25]. It targets the hardware or software components of a device, rather than the data itself. With the increased use of IoT devices in 5G networks, these attacks can compromise the security of the entire network.

Several measures should be done in order to overcome security issues related to 5G; comprehensive security measures need to be implemented, including encryption, access controls, intrusion detection and prevention systems, and security monitoring and incident response capabilities.

6. 5G Security Solutions

Several security measures should be implemented in order to address the security challenges and threats associated with 5G networks.

Authentication and authorization mechanisms. Strong authentication and authorization mechanisms should be implemented by organizations in order to prevent unauthorized access to networks and devices. This includes using two-factor authentication, multi-factor authentication, and biometric authentication. While these solutions can provide strong security, they can also introduce user friction, which can be a barrier to adoption and usage.

Encryption. It is an essential security measure for protecting data. Strong encryption algorithms should be used to protect sensitive data. On the other hand, encryption can produce latency and processing overhead, which can impact network performance negatively.

Virtual private networks (VPNs) [26]. VPNs can help to protect data as it travels over public networks by creating a secure and encrypted tunnel between two devices.

Network segmentation [26]. it involves dividing a network into smaller subnetworks, which can improve security by limiting the scope of potential attacks. But it can increase network complexity and management overhead.

Intrusion Detection and Prevention Systems (IDPS) [27]. IDPS can detect and prevent attacks by analysing network traffic and identifying suspicious activity. IDPS can generate false positives results, which can be a burden on network administrators.

Security analytics. It involves analysing data from multiple sources to identify potential threats and vulnerabilities. This can help to detect and respond to threats more quickly. However, security analytics requires a significant amount of data processing and analysis, which can affect negatively, network performance.

Threat intelligence [28]. Threat intelligence can be used to stay up-to-date with the latest threats and vulnerabilities in networks. This can help to proactively identify and address potential security risks. But it requires ongoing monitoring and analysis, which can be time-consuming and resource-intensive.

Security testing: Regular security testing and assessments can help to identify and address vulnerabilities in networks and devices.

Security protocols [29]. 5G networks use a variety of security protocols to protect data in transit, including Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Datagram Transport Layer Security (DTLS).

Overall, a comprehensive and layered approach to security is necessary to protect 5G networks and devices from cyber threats.

7. 5G Solution Analysis

5G solution analysis [30] evaluates different 5G technologies and solutions to determine which ones are best suited for a particular service or application. It involves analysing various factors such as speed, capacity, latency, reliability, and cost, as well as considering the specific requirements of the service or application.

The 5G solution analysis involves the following steps:

Requirements analysis that identifies the specific requirements of the service or application, such as speed, capacity, latency, and reliability.

Technology evaluation that evaluates the different 5G technologies and solutions that can meet the requirements of the service or application. It includes analysing factors such as spectrum availability, network architecture, and hardware and software requirements.

Solution comparison that compares the different 5G solutions to determine which one best meets the requirements of the service or application. It involves evaluating the performance, cost, and scalability of each solution.

Risk analysis that assesses the potential risks associated with each solution, such as security vulnerabilities or compatibility issues with existing systems.

Implementation plan where a plan is developed for implementing the chosen 5G solution, including timelines, resource requirements, and testing and validation procedures.

8. 5G Security Standards

Several security standards that are relevant to 5G networks which include:

a) 3rd Generation Partnership Project (3GPP) Security Standard [31] that defines the security architecture and protocols of 5G networks. It includes specifications of encryption, authentication, and access control, as well as guidelines for securing network functions and interfaces.
b) National Institute of Standards and Technology (NIST) Cybersecurity Framework [32], which is a set of guidelines and best practices for managing cybersecurity risk. It includes recommendations for identifying, protecting, detecting, responding to, and recovering from cyber threats.
c) International Organization for Standardization (ISO) 27001 standard [33] that provides a framework for information security management. It includes requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).
d) European Telecommunications Standards Institute (ETSI) Security Standard [34] provides guidelines for securing telecommunications networks. It includes recommendations for securing network functions, interfaces, and user equipment.
e) Global System for Mobile Communications (GSM) Security Standard [35] that provides guidelines for securing mobile networks. It includes recommendations for securing network functions, interfaces, and devices.

9. Authentication in 4G Networks

Authentication mechanisms in 4G-LTE have the following characteristics:

4G networks use the AKA protocol for subscriber authentication [36].

Mutual authentication: Both the UE and the network authenticate each other.

AKA uses authentication vectors, which consist of a random challenge generated by the network and a corresponding expected response calculated by the UE using a shared secret key.

Shared secret key: The UE and the home subscriber server (HSS) in the core network share a secret key, which is used to calculate the expected response for authentication.

The AKA procedure involves multiple steps, including the exchange of authentication vectors, calculation of expected responses, and verification of responses by the network.

4G networks support cryptographic algorithms such as AES.

A. Differences between 4G and 5G Authentication

Key Differences between 4G and 5G with respect to authentication are summarized in table 1.

Table 1. Differences between 4G and 5G in terms of Authentication

Criteria	Difference
Enhanced mutual authentication	5G introduces stronger mutual authentication compared to 4G, providing better protection against various attacks
Complexity	The authentication vectors in 5G are more complex and contain additional information compared to 4G.
Key hierarchy	5G introduces a hierarchical key structure, including a master key (MK), access key (AK), and long-term key (LTK), which provides enhanced security and flexibility
Security algorithms	While 4G networks primarily use AES, 5G supports AES-256 and ECC, which offer stronger cryptographic protection

5G authentication enhances security and introduces advanced cryptographic algorithms, providing a more secure and robust authentication framework compared to 4G.

Figure 3. shows the differences between 4G and 5G in terms of authentication in details.

10. Open Challenges

The deployment and advancement of 5G technology bring several open challenges that need to be addressed. Some of the key open challenges of 5G include:

Network Security: 5G networks introduce new security threats and vulnerabilities due to their complex architecture, increased attack surface, and reliance on virtualization and cloud technologies.

Spectrum Management: whereas efficient spectrum allocation and management are crucial for optimizing 5G network performance.

Interference and Signal Propagation: The higher frequency bands used in 5G networks enable faster data rates but are also more susceptible to interference and signal attenuation due to obstacles. Overcoming challenges related to signal propagation and coverage in urban environments and indoors is essential.

Energy Efficiency: 5G networks are expected to consume more energy than their predecessors due to the increased number of connected devices and data traffic. Developing energy-efficient technologies and optimizing network design to minimize power consumption is an ongoing challenge.

Quality of Service (QoS) and Quality of Experience (QoE): Delivering consistent and high-quality services across network, such as augmented reality, virtual reality, and real-time applications, requires effective QoS and QoE management mechanisms.

		4G Authentication	5G Authentication		
		EPS-AKA	5G-AKA	EAP-AKA'	EAP-TLS
ENTITIES (LOCATED IN)	USER EQUIPMENT (UE)	USIM	USIM		USIM/Non-USIM
	SERVING NETWORK (SN)	MME	SEAF		
	HOME NETWORK (HN)	HSS	AUSF UDM/ARPF/SIDF		
MESSAGE FORMAT	UE <-> SN	NAS	NAS	NAS|EAP	NAS|EAP
	SN <-> HN	Diameter	HTTP-based web APIs		
TRUST MODEL		Shared symmetric key	Shared symmetric key		Public key certificate
UE IDENTITY	UE -> SN	IMSI/GUTI	SUCI/5G-GUTI		
	SN -> HN	IMSI	SUCI/SUPI		
SN IDENTITY		SN id (MCC+MNC)	SN name (5G:MCC+MNC)		
AUTHENTICATION VECTOR GENERATED BY		HSS	UDM/ARPF	UDM/ARPF	N/A
AUTHENTICATION OF UE DECIDED BY		MME	SEAF & AUSF	AUSF	AUSF
HN INFORMED OF UE AUTHENTICATION?		No	Yes	Yes	Yes
ANCHOR KEY HIERARCHY		K_i -> CK+IK -> K_{ASME}	K_i -> CK+IK -> K_{ASME} -> K_{SEAF}	K_i -> CK+IK -> CK'+IK' -> EMSK -> K_{SEAF}	EMSK -> K_{AUSF} -> K_{SEAF}

Figure 3. 4G and 5G Authentication [31]

Privacy and Data Protection: With the proliferation of IoT devices and increased data collection, maintaining user privacy and data protection becomes a challenge. Developing mechanisms for secure data handling, storage, and sharing while adhering to privacy regulations is essential.

11. Conclusion

5G technology presents significant opportunities for innovation and economic growth but also introduces new security challenges. To ensure the successful deployment of 5G networks, it is crucial to prioritize and address the security concerns.

Industry stakeholders, government agencies, and security professionals must work together to establish robust security frameworks and best practices. This includes implementing

strong encryption and authentication mechanisms, securing virtualized and software-defined components.

By adopting a holistic and proactive approach to 5G security, we can reap the benefits of this transformative technology while safeguarding the privacy, integrity, and resilience of our networks and systems.

This article focuses on the 5G security in comparison to 4G-LTE, it is obvious that 5G networks provide higher security and authentication level.

References

[1] Zhang, Yongjian, and Yue Li. "A dimension-reduction multibeam antenna scheme with dual integrated butler matrix networks for low-complex massive MIMO systems." IEEE antennas and wireless propagation letters 19, no. 11 (2020): 1938-1942.

[2] Chiaraviglio, Luca, Chiara Lodovisi, Daniele Franci, Settimio Pavoncello, Elisabetta Merli, Tommaso Aureli, Nicola Blefari-Melazzi, Marco Donald Migliore, and Mohamed-Slim Alouini. "EMF exposure in 5G standalone mm-Wave deployments: What is the impact of downlink traffic?." IEEE Open Journal of the Communications Society 3 (2022): 1445-1465.

[3] Ping, Jiamin, Yue Liu, and Dongdong Weng. "Comparison in depth perception between virtual reality and augmented reality systems." In 2019 IEEE conference on virtual reality and 3d user interfaces (VR), pp. 1124-1125. IEEE, 2019.

[4] Gupta, Akhil, and Rakesh Kumar Jha. "A survey of 5G network: Architecture and emerging technologies." IEEE access 3 (2015): 1206-1232.

[5] Vook, Frederick W., Amitava Ghosh, and Timothy A. Thomas. "MIMO and beamforming solutions for 5G technology." In 2014 IEEE MTT-S International Microwave Symposium (IMS2014), pp. 1-4. IEEE, 2014.

[6] Leyva-Pupo, Irian, Alejandro Santoyo-González, and Cristina Cervelló-Pastor. "A framework for the joint placement of edge service infrastructure and user plane functions for 5G." Sensors 19, no. 18 (2019): 3975.

[7] Arfaoui, Ghada, Pascal Bisson, Rolf Blom, Ravishankar Borgaonkar, Håkan Englund, Edith Félix, Felix Klaedtke et al. "A security architecture for 5G networks." IEEE access 6 (2018): 22466-22479.

[8] Ramezanpour, Keyvan, and Jithin Jagannath. "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN." Computer Networks 217 (2022): 109358.

[9] Yahia Jazyah, "5G Mobile Communication Revolution and its Impact on Life in Comparison to Former Mobile Generations", International Journal of Emerging Technology and Advanced Engineering, volume 13, issue 5, Pages 97-105. May 2023. DOI: 10.46338/ijetae0523_10

[10] Mathew, Alex. "Network slicing in 5G and the security concerns." In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 75-78. IEEE, 2020.

[11] Kitindi, Edvin J., Shu Fu, Yunjian Jia, Asif Kabir, and Ying Wang. "Wireless network virtualization with SDN and C-RAN for 5G networks: Requirements, opportunities, and challenges." IEEE Access 5 (2017): 19099-19115.

[12] Henriques, Joao, Luis Rosa, Andre Gomes, Luis Cordeiro, Konstantinos C. Apostolakis, George Margetis, Constantine Stephanidis et al. "The 5G-EPICENTRE Approach for Decreasing Attack Surface on Cross-Testbeds Cloud-native 5G Scenarios." In 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), pp. 7-12. IEEE, 2021.

[13] Azrour, Mourade, Jamal Mabrouki, Azidine Guezzaz, and Ambrina Kanwal. "Internet of things security: challenges and key issues." Security and Communication Networks 2021 (2021): 1-11.

[14] Masoud, Mohammad, Yousef Jaradat, Ahmad Manasrah, and Ismael Jannoud. "Sensors of smart devices in the internet of everything (IoE) era: big opportunities and massive doubts." Journal of Sensors 2019 (2019).

[15] Zhao, Jingfeng, and Yan Li. "Supply chain security evaluation model and index system based on a 5G information system." Neural Computing and Applications (2021): 1-11.

[16] Khan, Rabia, Pardeep Kumar, Dushantha Nalin K. Jayakody, and Madhusanka Liyanage. "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions." IEEE Communications Surveys & Tutorials 22, no. 1 (2019): 196-248.

[17] Shahbazov, V. "NAVIGATING THE 5G SECURITY LANDSCAPE: REGULATIONS, TECHNOLOGIES, AND FUTURE CHALLENGES." In The 17th International scientific and practical conference “System analysis and intelligent systems for management” (May 02–05, 2023) Ankara, Turkey. International Science Group. 2023. 482 p., p. 397. 2023.

[18] Masoud, Mohammad Z., Yousf Jaradat, and Ismael Jannoud. "On preventing ARP poisoning attack utilizing Software Defined Network (SDN) paradigm." In 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), pp. 1-5. IEEE, 2015.

[19] Yang, Yaoqi, Xianglin Wei, Renhui Xu, Laixian Peng, Lei Zhang, and Lin Ge. "Man-in-the-middle attack detection and localization based on cross-layer location consistency." IEEE Access 8 (2020): 103860-103874.

[20] Kuadey, Noble Arden Elorm, Gerald Tietaa Maale, Thomas Kwantwi, Guolin Sun, and Guisong Liu. "DeepSecure: Detection of distributed denial of service attacks on 5G network slicing—Deep learning approach." IEEE Wireless Communications Letters 11, no. 3 (2021): 488-492.

[21] Bhatia, Deepshikha. "A Comprehensive Review on the Cyber Security Methods in Indian Organisation." International Journal of Advances in Soft Computing & Its Applications 14, no. 1 (2022).

[22] Saedi, Mohammad, Adrian Moore, Philip Perry, Mohammad Shojafar, Hanif Ullah, Jonathan Synnott, Ruth Brown, and Ian Herwono. "Generation of realistic signal strength measurements for a 5G Rogue Base Station attack scenario." In 2020 IEEE Conference on Communications and Network Security (CNS), pp. 1-7. IEEE, 2020.

[23] ALABDULATIF, ABDULLAH. "Potential Security Vulnerabilities of the IEEE 802.15. 4 Standard and a Proposed Solution Against the Dissociation Process." International Journal of Advances in Soft Computing & Its Applications 13, no. 3 (2021).

[24] Reshmi, T. R. "Information security breaches due to ransomware attacks-a systematic literature review." International Journal of Information Management Data Insights 1, no. 2 (2021): 100013.

[25] Al-Shareeda, Mahmood A., Selvakumar Manickam, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J. Alzahrani, Gharbi Alshammari, Amer A. Sallam, and Khalil Almekhlafi. "Chebyshev polynomial-based scheme for resisting side-channel attacks in 5g-enabled vehicular networks." Applied Sciences 12, no. 12 (2022): 5939.

[26] Harmening, James T. "Virtual private networks." In Computer and Information Security Handbook, pp. 843-856. Morgan Kaufmann, 2017.

[27] Sharifi, A. Ahmad, B. Akram Noorollahi, and Farnoosh Farokhmanesh. "Intrusion detection and prevention systems (IDPS) and security issues." International Journal of Computer Science and Network Security (IJCSNS) 14, no. 11 (2014): 80.

[28] Haider, Noman, Muhammad Zeeshan Baig, and Muhammad Imran. "Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends." arXiv preprint arXiv:2007.04490 (2020).

[29] Satapathy, Ashutosh, and Jenila Livingston. "A Comprehensive Survey on SSL/TLS and their Vulnerabilities." International Journal of Computer Applications 153, no. 5 (2016): 31-38.

[30] Ahmad, Ijaz, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. "5G security: Analysis of threats and solutions." In 2017 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 193-199. IEEE, 2017.

[31] Zhang, Xiaowei, Andreas Kunz, and Stefan Schröder. "Overview of 5G security in 3GPP." In 2017 IEEE conference on standards for communications and networking (CSCN), pp. 181-186. IEEE, 2017.

[32] Mylrea, Michael, Sri Nikhil Gupta Gourisetti, and Andrew Nicholls. "An introduction to buildings cybersecurity framework." In 2017 IEEE symposium series on computational intelligence (SSCI), pp. 1-7. IEEE, 2017.

[33] Lukitowati, Risma, and Kalamullah Ramli. "Assessing the Information Security Awareness of Employees in PT ABC Against International Organization for Standardization (ISO) 27001: 2013." Journal of Computational and Theoretical Nanoscience 17, no. 2-3 (2020): 1441-1446.

[34] Hämäläinen, Matti, Tuomas Paso, Lorenzo Mucchi, Marc Girod-Genet, John Farserotu, Hirokazu Tanaka, Woon Hau Chin, and Lina Nachabe Ismail. "ETSI TC SmartBAN: Overview of the wireless body area network standard." In 2015 9th international symposium on medical information and communication technology (ISMICT), pp. 1-5. IEEE, 2015.

[35] Gu, Guifen, and Guili Peng. "The survey of GSM wireless communication system." In 2010 international conference on computer and information application, pp. 121-124. IEEE, 2010.

[36] Borgaonkar, Ravishankar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. "New privacy threat on 3G, 4G, and upcoming 5G AKA protocols." Cryptology ePrint Archive (2018).