

A SURVEY ON 5G MOBILE NETWORKS: THE PERSPECTIVE OF TECHNOLOGY, SECURITY THREATS AND MITIGATIONS

Gambo Junaidu¹, Suleiman Abdullahi², Lawal Idris Bagiwa³

¹Department of Mathematics and Computer Sciences, Faculty of Natural and Applied Science, Al-Qalam University, Katsina, P.M.B. 2137 Dutsin-ma Road, Katsina State, Nigeria.

Junaidu.gambo@gmail.com

²Department of Mathematics and Computer Sciences, Faculty of Natural and Applied Science, Al-Qalam University, Katsina, P.M.B. 2137 Dutsin-ma Road, Katsina State, Nigeria.

abduljby02@gmail.com

³Department of Computer Studies, College of Science and Technology, Hassan Usman Katsina Polytechnic P.M.B. 2052 Katsina State, Nigeria.

lbagiwa@yahoo.com

ABSTRACT

In many telecommunications sectors, safety has today become the main concern as threats can have high impacts. Particularly because the key and enable technology are linked to the 5G network, sensitive information in future wireless networks can travel across all levels. Several accidents have shown that the risk posed by an infected wireless network does not only impact security and privacy issues, but also prevents complicated networking environment dynamics. The sophistication and strength of security threats in recent years has therefore become a global obstacle in identifying or preventing sabotage. This paper provides an extensive list of key and supporting technology used to develop the 5G protection model, network software security, PHY (Physical) layer security, and 5G confidentiality issues from a security and privacy viewpoint. The paper further discusses compliance control and 5G network maintenance. This paper further evaluates the safety precautions and requirements associated with core 5G technology by using separate standardizing bodies and give a concise description of the defense forces for 5G standardization. Moreover, key internationally important initiatives are also discussed in accordance with the safety issues of 5G and beyond. Finally, an open section with the guidelines and obstacles for future studies has been added.

Keywords: *5G, Networks, Security, Threats and Mitigation*

I. INTRODUCTION

5G cellular networks have a great deal of vision based on high data speeds and higher coverage capacity-enhancing rollout, improved service quality (QoS) and incredibly low latency [1]. To supply 5G, new networking, the required facilities, Technologies for service deployment, preparation and distribution is essential. Cloud computing is an effective way to do data, facilities and applications maintenance operators [2]. Mobile technology uses the same principles in a single domain, which can be used by multiple services for greater flexibility. Less Capital Expenditure (CapEx) and availability Expenses for operations (OpEx). The software development of network functions would make networking technologies and networks more portable and flexible. Enables Network Defined Software Networking (SDN). SDN provides networking creativity Abstraction on the one side and network simplification on the other side [3]. The basis for positioning

different networks is Network virtualizing function (NFV)[4]. It Works on a need basis in various network perimeters and Removes the need for the same hardware or service. Network Elasticity is improved by complementary SDN and NFV, simplifying the management and regulation of the network, shake the vendor's obstacle to clear patented solutions and therefore, for future networks, they are considered extremely significant. Network defense for these new innovations and ideas and data anonymity for future networks remains a major problem. From the very beginning, wireless networks were susceptible to security flaws[5]. Wireless networks, cellular phones and wireless in the first wave (1G) illicit copying and masquerading was targeted on the networks. Message in 2G broadband networks of the second wave Spaming was not only normal for overwhelming attacks yet misinformation injection or unwanted broadcasting Knowledge on ads. Wireless in the third (3G) wave IP-based networking allowed networks to migrate Web vulnerability flaws and wireless problems dependencies. The fourth generation (4G) mobile networks also enabled the increasing need for IP-based connectivity. This has contributed to more Landscape of complex and complicated danger. The coming of Wireless networks of fifth generation (5G), security challenge Vectors of greater care will be larger than ever before. It is thus important to highlight the challenges of security which are not only threatening because of the wireless nature but there are mobile networks in the potential technologies for 5G, they're extremely relevant. We emphasize in this paper the Challenges of safety that are ahead of 5G and necessary Security action promptly[1].

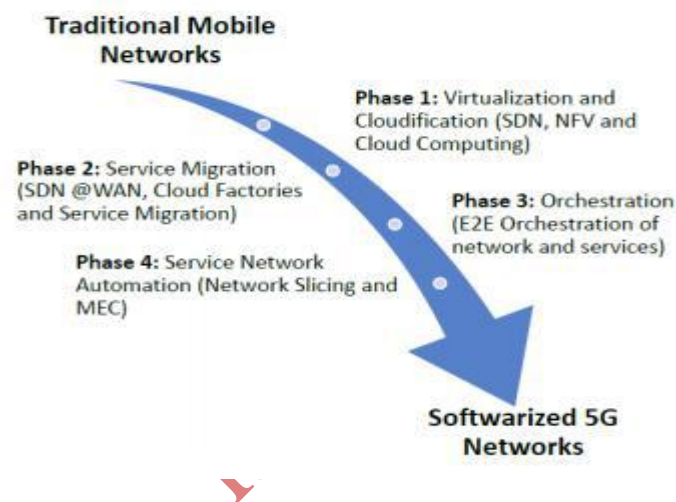


Figure 1: Four phases of Network Transformation towards Network Softwarization in 5G. Source: [6]

II. KEY SECURITY CHALLENGES IN 5G

5G connects critical infrastructure that needs more Safety not only for the critical infrastructure but the security of the entire society. A security, for instance Infringement in online power systems can be disastrous for all systems in the society. We also know that information is critical and what if critical data is corrupted? That's why it is extremely important to study and emphasize 5G network security challenges and the possible overview Might contribute to 5G networks safe solutions[7].

Network Slice (NS) principles for the telecommunications networks[8] and Function Virtualization (NFV), Cloud Computing, Multi-access Edge Computing (MEC). The objective of these activities was to create a modern mobile software network. It will continue to evolve and build new network technologies to meet the need for mobile networks that will develop in the future. The SDN principle is designed to decouple networking interface control and data planes[7]. SDN-based network management and information is located in a logically centralized controller. It also provides an abstract for the control functions and business application layers of the underlying network architecture. NFV offers a new approach to network services growth, deployment and management. In order to act as device instances[9], this definition seeks to separate the network functions from their proprietary hardware. The scalability of the networks on demand will take place in the cloud computing[10]. Slicing of the network increases support for various 5G network traffic classes[11]. In this

modern telecommunication network, the protections, security and privacy have become the main concerns because threats can have high effect[12].

Table I: SECURITY CHALLENGES IN 5G TECHNOLOGIES.

Security Threat	Target Point/Network Element	Effectuated Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS attack	Centralized control elements	✓	✓		✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			✓	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓		✓	
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds		✓		✓	
User identity theft	User information data bases				✓	✓
TCP level attacks	SDN controller-switch communication	✓		✓		
Man-in-the-middle attack	SDN controller-communication	✓		✓		✓
Reset and IP spoofing	Control channels			✓		
Scanning attacks	Open air interfaces			✓		✓
Security keys exposure	Unencrypted channels			✓		
Semantic information attacks	Subscriber location			✓		✓
Timing attacks	Subscriber location				✓	✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Subscriber identity			✓		✓

III. 5G WIRELESS SECURITY STATE OF THE ART

In this part, we will summarize the latest developments including new security technologies in 5G wireless network networks. The cryptography and PLS are two key security solutions. Many new 5G broadband networks applications have initiated significant PLS testing. The majority of PLS analysis is focused on distribution of resources. In a safety-oriented resource assignment system in high density networks is called (UDNs)[3]. The paper reviewed the effect of safety transmission on several aspects of the resource. The major resources are power allocation, relay selection, allocation of frequencies, time and radiation[13]. The unanswered questions and the potential directions of PLS, including intrusion management, dedicated jammer substitution, mobility management protection and heterogeneity management, are addressed. When considering multiple users and SBSs in UDNs, a case study is proposed to cover the cross-layer cooperation scheme in HetNet. Two metrics used as secrecy potential and secrecy outage chance are added to improve the interpretation of the PLS[3].

IV 5G WIRELESS NETWORKS SECURITY SERVICES

The telecoms networks today are commonly divided up into four logical components: radio access network, central network, transportation networks and network interconnection. Each networking section consists of three so-called aircraft, each of which carries a different type of traffic, namely: the signaling control aircraft; the user aircraft carrying payload (actual-) traffic; and the administrative-traffic management of aircraft[14]. All three aircraft are subject to special categories of threats in terms of network defense. The following components characterize the safety of telecommunications networks:

Standardization; a mechanism in which providers, suppliers and other parties set guidelines for the cooperation of networks around the world, this involves the safest way to defend networks and consumers from malicious players[15]. Network architecture; network suppliers design, produce and enforce negotiated specifications in respect of functional network elements and systems that make a functional and stable end network product Network configuration; networks are designed to a specific protection standard during the implementation process that are essential to establish safety criteria and further enhance the network's security and resilience Network configuration and operation; operating processes that enable networks to operate and have specific security levels are heavily dependent on deployment and network operations themselves[16].

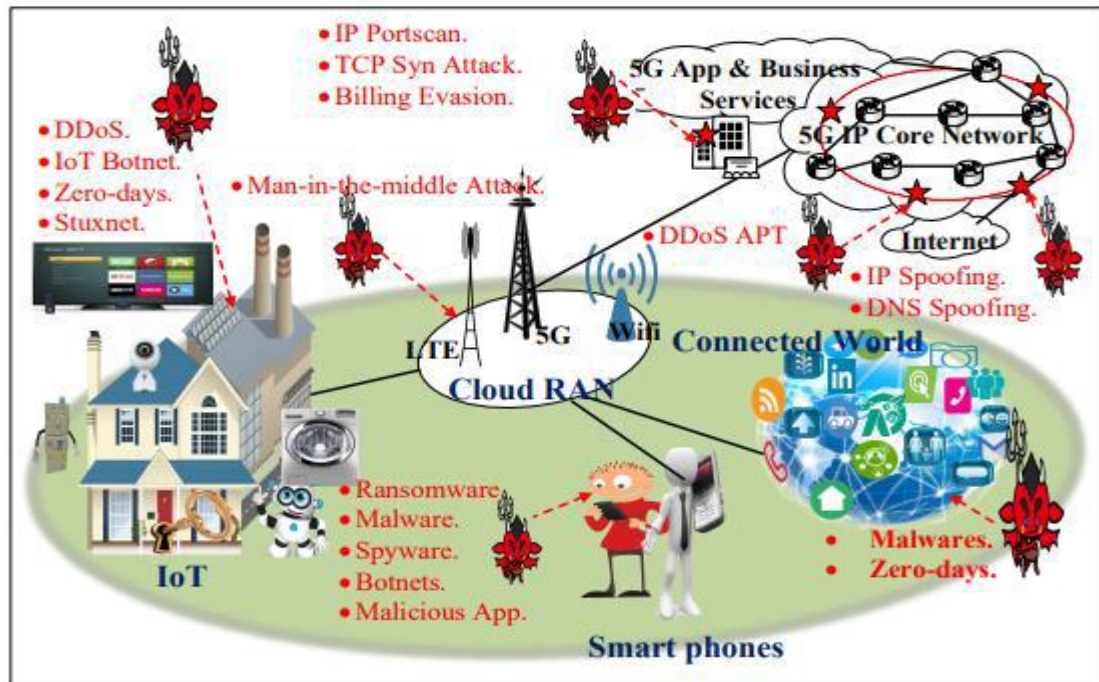


Fig. 2: 5G Security Threat Landscape for several attacks in IoT, smart phones, cloud RAN and connected world. Source: [6]

VI. CONCLUSION

This paper examines many elements of the 5G wireless standard in terms of safety concerns. It examines the nature of the general protocol for defense. In each element, safety considerations are noted. The general protocol design by the 5GPPP gives an overview of the issue. The aspects V2X and IoT emphasize how the general security protocol in these particular vertical services could or would affect execution. Both V2X and IoT aspects can lead to a large number of network nodes, each with numerous threat vectors. In order to reconcile conflicting interests, network is often a service (NaaS) or slicing process. Slicing nevertheless creates a host of additional problems for virtualisation, automation, and insulation assurances. Protection affects both vertical services and dimensional uses at all levels, whether it's about a network and technology or vertical services, and security is a problem even though security is not specifically focused.

REFERENCES

1. Gupta, A. and R.K. Jha, *A survey of 5G network: Architecture and emerging technologies*. IEEE access, 2015. **3**: p. 1206-1232.
2. Ahmad, I., et al., *Overview of 5G security challenges and solutions*. IEEE Communications Standards Magazine, 2018. **2**(1): p. 36-43.
3. Choudhary, G., J. Kim, and V. Sharma, *Security of 5G-mobile backhaul networks: A survey*. arXiv preprint arXiv:1906.11427, 2019.
4. Batalla, J.M., et al., *Security risk assessment for 5G networks: National perspective*. IEEE Wireless Communications, 2020. **27**(4): p. 16-22.
5. Zhang, S., Y. Wang, and W. Zhou, *Towards secure 5G networks: A Survey*. Computer Networks, 2019. **162**: p. 106871.
6. Zikria, Y.B., et al., *5G Mobile services and scenarios: Challenges and solutions*. 2018, Multidisciplinary Digital Publishing Institute.
7. Saha, R.K., P. Saengudomlert, and C. Aswakul, *Evolution toward 5G mobile networks-A survey on enabling technologies*. Engineering Journal, 2016. **20**(1): p. 87-119.

8. Akpakwu, G.A., et al., *A survey on 5G networks for the Internet of Things: Communication technologies and challenges*. IEEE access, 2017. **6**: p. 3619-3647.
9. Singh, S., et al., *A survey on 5G network technologies from social perspective*. IETE Technical Review, 2017. **34**(1): p. 30-39.
10. Panwar, N., S. Sharma, and A.K. Singh, *A survey on 5G: The next generation of mobile communication*. Physical Communication, 2016. **18**: p. 64-84.
11. Xiang, W., K. Zheng, and X.S. Shen, *5G mobile communications*. 2016: Springer.
12. Pérez, M.G., et al., *Dynamic reconfiguration in 5G mobile networks to proactively detect and mitigate botnets*. IEEE Internet Computing, 2017. **21**(5): p. 28-36.
13. Habibi, M.A., et al., *A comprehensive survey of RAN architectures toward 5G mobile communication system*. IEEE Access, 2019. **7**: p. 70371-70421.
14. Geller, M. and P. Nair, *5G security innovation with Cisco*. Whitepaper Cisco Public, 2018: p. 1-29.
15. Mantas, G., et al., *Security for 5G communications*. 2015.
16. Guey, J.-C., et al., *On 5G radio access architecture and technology [industry perspectives]*. IEEE Wireless Communications, 2015. **22**(5): p. 2-5.

*i*Journals