Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Volume III, Issue II, July 2021

A Review of Security Challenges and Solutions in 5G Network

[1]Sunil Kumar Shah, [2]Snehal Jani, [3]Rinkoo Bhatia, [4]Neeta Nathani
[1]*Ph.D. Scholar, ECE Department,* sunil.shah1@s.amity.edu
[2]*Assistant Professor, Department of Physics,* scjani@gwa.amity.edu
[3]*Assistant Professor, Department of Electronics and Communication Engineering,* rbhatia@gwa.amity.edu
[1,2,3]*Amity School of Engineering and Technology, Amity University Madhya Pradesh, Gwalior, Madhya Pradesh*
[4]*Associate Professor, Department of Electronics and Communication Engineering, Gyan Ganga Institute of Technology and Sciences, Jabalpur, Madhya Pradesh,*
neetanathani@ggits.org

***Abstract*—Fifth Generation (5G) wireless network is a generation of mobile network that is the next evolution of 4G LTE network. The 5G technology is adopted to fulfil the demands of current technology evolution which includes a large growth in data transfer and increasing interest in the Internet of Things (IoT). As 5G network plays very important role in day today lives, it must be very secure to users. The security threats of 5G are growing tremendously due to unmatched increase in number of devices and service. Therefore, security threats which are not developed yet should be visualize on various services, technologies, and increase in user accessibility by the network. This paper framework the 5G network threat and security susceptibility in new technological concept which should be adopted by 5G and come up with either solution of these threats or future guidelines to overcome with those security challenges. When these technology and solution is implemented efficiently, it provides high impact cyber security of 5G network.**

Keyword- 5G, Security, Security challenges, Security solutions, Privacy, SDN security

I. INTRODUCTION

The 5G wireless network provides grate coverage and very high data rates with purposefully improved quality of services (QoS) [1]. With extremely crowded placement of base station , 5G will provide very high reliable and cost-effective broadband access everywhere not only to the cellular hand-held devices, but also to a new devices identify with, Internet of Things (IoT), Machine- to – Machine communication (M2M), and Cyber-Physical Systems (CPSs) [2]. Such improvement implies that 5G network is not a simple additional advancement of 4G as one might naturally think, but an integration of new troublesome technologies to meet increasing demand of user traffic, emerging services, existing and future IoT devices [3]. With all this effectiveness, all aspects of human life will be connected by 5G network, and this indicates the need of tough security mechanism crosswise the entire network segments of 5G network.

The First Generation (1G) mobile networks were liable to suffer from challenges of unauthorised interception, cloning and masking [4]. Message spamming for common attacks, injection of untrue information or broadcasting undesirable marketing information becomes simple in Second Generation (2G) of mobile networks. The main interruption was in the Third Generation (3G) of mobile networks in which IP-based communication permit the transfer of security in internet becomes compulsion and challenges into mobile networks. The security threats becomes further enlarged and difficult in the Fourth Generation (4G) mobile network with the expanded use of IP- based communication which was mandatory for new services and new devices [5]. The amalgam of huge number of IoT devices and the arrangement of new services for examples hospitals, transports, smart home, and surveillance systems in 5G further provoke the security challenges. The security architecture and solutions

used in earlier generation (i.e., 3G and 4G), possibly, will not be enough for 5G networks. The main reason for architecture and new security solutions is the dynamics of technologies and new services in 5G network [6]. This paper studies the highest developments of security in 5G networks. It starts with study of security challenges and its corresponding solutions for the past generation of networks from 1G to 5G.

II. RELATED WORK

The 5G network provides very high data rates and has very low latency due to increase in the density of base station and the capacity the quality of services improved significantly as compare to 4G network [1]. There are number of survey articles which discussed the 5G networks [7], [8]. Software defined networking (SDN) in 5G network for fast authentication, based on weighted security context transfer. The algorithm required for SDN does not required changing existing hardware. This technique simplifies the authentication procedure drastically because of which, latency handover reduces. Software defined networking also provides security which possesses high level of tolerance. Operators can be able to switch ON and OFF the loaded cells if the cell going to reach a certain maximum level according to Scalable Coherent Interconnect (SCI) information which saves more energy. Security challenges solution of 5G network is enabled in SDN to provide non-cryptographic security [9]. By using Reinforcement Learning (RL) algorithm technique, unknown misbehaviours caused by attacks is found which leads to First level-Intrusion Detection Systems (FL-IDS), Second level-Intrusion Detection Systems (SL_IDS), and Security Operation Centre (SOC) to resist against the smart Denial of Service (DoS) threats [10]. As a requirement of fast speed and shrinking the size of cell coverage, the frequency of handover increases. The Distributed IP Mobility Management (DMM), it achieves efficient and fault tolerance solution by excluding centralized network which reduces the distance between a mobile device and its serving network [11]. To protect mobile devices by use of drones and 5G Network from the attack of jamming. The reinforcement learning algorithm can be implemented which allows the 5G system to provide resistance against attackers that probably jam the communications between the static device and mobile [12]. Security threats comes more in existence when there is direct connection between devices. The Device to Device (D2D) communication by eavesdroppers in cellular network which uses portion of spectrum occupied by the cellular users [13].

III. SECURITY IN WIRELESS NETWORKS: FROM 1G TO 5G

Security in wireless communication network is a challenging task due to intricacy in the hidden network. The main change came with the introduction of IP-based communication in wireless network in which large internet-based security challenges immigrate to networks. So, in this section we provide an overview of change in security model from 1G to 5G.

The 1G used Analog signal processing and it was designed initially for the purpose of voice service. The 1G cellular system is also called as Advanced Mobile Phone Services that was first developed by Bell Labs in 1983. Though it was dealing with Analog communication, it was very difficult to provide any efficient security services. This cellular network was not having any encryption, so information was not secured, and it was open to any security challenges. Digital mobile systems were introduced to increase the

efficiency of the limited frequency bands and thus Global System for Mobile (GSM) became most popular cellular communication of 2G network. The 3G cellular network came into demand because of higher data rates as compared to 2G network. 3G cellular systems also introduced new services like video streaming and video chatting. In 3G network more security features were added which was not available in 2G network. Universal Mobile Telecommunication System (UMTS) is 3G cellular technology that was mainly developed by 3GPP. 3GPP requirements combine configuration and secure setup of the base station, secure key management inside the BTS. For secured environment for handling the control plane data and user data. The security of 5G network and system connected through 5G network must be studied from the design phase itself.

TABLE I

SUMMARY OF SECURITY PROGRESSIONS FROM 1G TO 5G

Wireless Network	Security Mechanism Adopted	Security Challenges
1G	No accurate security and privacy is measured	Cell interception, Eavesdropping and no privacy
2G	Encryption based protection is developed	Radio link security, one way authentication, and spamming
3G	Authentication and Key Agreement and two-way authentication technique is adopted	Encryption Keys Security and Roaming security
4G	Introduced 3GPP access security and integrity protection	Not suitable for security of new devices and new services
5G	Introduced new architecture, Security Edge Protection Proxy (SEPP) to protect home gateway between home networks.	To prevent attacks, operators can protect users by using Temporary Mobile Subscriber Identity (TMSI).

IV. CONCLUSION

Wireless communication networks have been emerging from connecting mobile phones in 1G approaching almost all requirement of life in 5G. During this transformation, security levels have equally improved from simple phone tapping to different attacks on mobile devices, services, and network equipment. For integrating IoT and other services into the network, 5G networks uses new technologies such as Advanced Clouded Computing Concept like SDN, Network Function Visualization (NFV), and multiple input multiple output (MIMO) etc. These technologies have their own built-in security challenges and its solution which exist in different parts of the network such as core network, access network and within the technologies which is used in 5G wireless network.

REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016, doi: 10.1109/COMST.2016.2532458.

[2] D. Kutscher, “It’s the network: Towards better security and transport performance in 5G,” Proc. - IEEE INFOCOM, vol. 2016-Septe, pp. 656–661, 2016, doi: 10.1109/INFCOMW.2016.7562158.

[3] J. G. Andrews et al., “What will 5G be?,” IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065–1082, 2014, doi: 10.1109/JSAC.2014.2328098.

[4] J. K. Wey, H. T. Chang, L. F. Sun, and W. P. Yang, “Clone terminator: an authentication service for advanced mobile phone system,” IEEE Veh. Technol. Conf., vol. 1, pp. 175–179, 1995, doi: 10.1109/vetec.1995.504852.

[5] I. Ahmad, T. Kumar, M. Liyanage, J.

Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," 2017 IEEE Conf. Stand. Commun. Networking, CSCN 2017, pp. 193–199, 2017, doi: 10.1109/CSCN.2017.8088621.

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

[7] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," IEEE Access, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[8] C. Sexton, N. J. Kaminski, J. M. Marquez-Barja, N. Marchetti, and L. A. DaSilva, "5G: Adaptable Networks Enabled by Versatile Radio Access Technologies," IEEE Commun. Surv. Tutorials, vol. 19, no. 2, pp. 688–720, 2017, doi: 10.1109/COMST.2017.2652495.

[9] 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, 2016, doi: 10.1109/ICC.2016.7510994.

[10] H. Sedjelmaci, "Attacks detection approach based on a reinforcement learning process to secure 5g wireless network," 2020 IEEE Int. Conf. Commun. Work. ICC Work. 2020 - Proc., 2020, doi: 10.1109/ICCWorkshops49005.2020.9145438.

[11] J. Kim, P. V. Astillo, and I. You, "DMM-SEP: Secure and Efficient Protocol for Distributed Mobility Management Based on 5G Networks," IEEE Access, vol. 8, pp. 76028–76042, 2020, doi: 10.1109/ACCESS.2020.2985448.

[12] X. Lu, L. Xiao, C. Dai, and H. Dai, "UAV-Aided Cellular Communications with Deep Reinforcement Learning against Jamming," IEEE Wirel. Commun., vol. 27, no. 4, pp. 48–53, 2020, doi: 10.1109/MWC.001.1900207.

[13] R. Atat and L. Liu, "On the achievable transmission capacity of secrecy-based D2D cellular networks," 2016 IEEE Glob. Commun. Conf. GLOBECOM 2016 - Proc., pp. 1–6, 2016, doi: 10.1109/GLOCOM.2016.7842047.