International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

Study of Security for 5G Wireless Communication Network

Shilpa V Swamy[1], Prof. Rashmi R[2]

[1]*Student, Dept. of Information Science and Engineering, RV College of Engineering®, Karnataka,India*
[2]*Professor, Dept. of Information Science and Engineering, RV College of Engineering®, Karnataka, India*

Abstract - *As there is a sudden growth in the high data rate, which is demanded by the subscribers, the need for security of the system is significant. The chances of attacks have raised due to the increase in the amount of handover rates. Network security had been considered as one of the more provocative issues. In order to create a reliable and steady network, Security must be ensured. This paper presents an overview the 5G network architecture of 3GPP. Then, the paper summarizes the security in cloud computing, SDN and NFV. Along with the technological developments which are required to secure the network. Along with that, brief detail about the security services in 5G.*

Key Words: Software Define Network (SDN), Network Function Virtualization (NFV), Denial of Service (DoS), Distributed Denial of Service (DDoS), Eavesdropping, Jamming, Man-in-the-middle (MITM), Internet of Things (IoT), Machine-to-Machine (M2M).

1. INTRODUCTION

When we look at the last decades, the growing in the demand for service and quality assure has been increased as the number of the mobile users have increased drastically[1]. The innovative 5th generation technology is moving towards our prospective telecommunication solution to fulfill the users demand.

With the incorporation of high number of IoT devices like smart hospitals, smart transport, smart appliances etc. and with the new services, the fifth Generation (5G) network is further aggravate the security challenges. The same architectures and the solutions for security which have been used in the previous generation like 3G and 4G will not be enough for providing the security in the evolving 5G network. As the new services and technologies have been incorporated in the 5G, there is a need for new security solutions and architecture[2].

2. OVERVIEW OF 5G SECURITY

This section shows the 5G security architecture and major types of 5G attacks[3].

2.1 5G SECURITY ARCHITECTURE

The 3GPP defined security architecture has six main domains. Below Fig. 1, shows the 5G security architecture defined by 3GPP specifications.

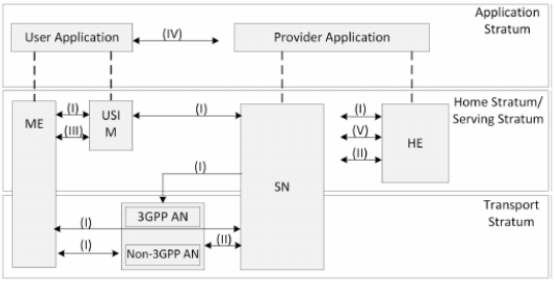

Fig 1: 5G Security Architecture

Network Access Security (I): This consists of the security structures that provides the User Equipment (UE) to get authenticated securely and access the services of network. Access Security comprises of delivering the security environment from secondary Node (SN) to User Equipment (UE).

Network Domain Security (II): This consists of the security structures that provides exchange of signaling and the user plane data securely between the network nodes.

User Domain Security (III): This comprises of the security structure that provides the secured user access to user Equipment (UE).

Application Domain Security (IV): This consists of the security features that provides the provider and user applications to exchange messages securely.

Service Based Architecture (SBA) Domain Security (V): This consists of the security structures for the authorization, registry of the network elements and discovery of network element along with the security for service-based interfaces.

Visibility and Configuration of Security (VI): This comprises of the security structure that provides the user with the information whether the security features are in operation state or not.

2.2 MAJOR ATTACKS IN 5G NETWORK

The As the wireless medium and wireless transmission is involved in the wireless network broadcast, there could be various threats and vulnerabilities in the network. The four major types of attacks include Dos and DDoS, jamming, Man-In-The-Middle (MITM), eavesdropping and traffic analysis in 5G network[5].

These types of attacks are described as below:

DoS and DDoS: DoS assaults will see an attacker draining the network infrastructure. DoS is a security attack that breaches network connectivity. Detection is mainly used for detecting DoS and DDoS attacks. DoS and DDoS would possibly pose a major problem for operators with a large deployment of huge devices in 5 G cellular networks[3].
Jamming: Except for eavesdropping and traffic analysis, jamming can completely disrupt communication between authorized customers. The attacker node can create deliberate interference that can interrupt legitimate users' data transmission. Jamming can often block the connection of registered users to the radio services[2].
MITM: In the attack at MITM, the malicious actor gets hold of the channel of communication among two legitimate parties. MITM intruder can capture, alter and delete the communications of contact between the two legal parties. MITM is an active attack which can be planned to launch at various layers[2].
Eavesdropping and Traffic Analysis: Eavesdropping is a threat that an unintentional receiver uses to encrypt a message from the others. Eavesdropping is a passive attack, since eavesdropping doesn't really affect the basic communication. Eavesdropping is hard to detect because of its passive nature. The encryption of the signals over the radio link is most generally applied to counteract the eavesdropping threat[2].

3. SECURITY CHALLENGES IN 5G NETWORK

3.1 SECURITY IN CLOUD COMPUTING

Cloud computing provides on-demand computing support and information to both small and large companies, thus improving resources available and allowing for greater abstraction mostly on customer side of the underlying mechanisms. Cloud computing's position within 5G mobile network has been a cardinal priority for both industry and academic organizations focused on 5 G and related technology. Most sites for social networking, such as Netflix, Facebook, Twitter and Youtube have also embraced the cloud concept and are growing their ability.

3.2 SECURITY CHALLENGES IN SOFTWARE DEFINED NETWORKING (SDN)

SDN consolidates the systems for network management and enables fully programmable throughout the communication network. However, such disruptive features create chances to crack and hack the network. For example, centralized control would be a great choice for DoS attacks, and it will expose crucial application programming interfaces (APIs) that unintended software can essentially make into the entire network. The SDN controller alters the network traffic in the data route, so that device traffic can be quickly detected.

3.3 SECURITY CHALLENGES IN NETWORK FUNCTION VIRTUALIZATION (NFV)

The NFV has basic security issues for future contact networks, such as integrity, authenticity, confidentiality and non-repudiation. Again, from viewpoint of being used in cellular networks, the existing NFV platforms cannot provide virtualized telecom services with adequate security and isolation. Several of the major challenges that remain with the use of NFV in cellular networks is the interactive nature of Virtual Network Functions (VNFs), which leads to errors in configuration and therefore security breaches.

3.4 SECURITY CHALLENGES IN COMMUNICATION CHANNELS

5G will include complex drone and air traffic control systems, virtual reality powered by the cloud, automated vehicle, smart factories, computer-based robots,e-health and transportation.

The apps therefore require highly secure communication mechanisms that allow more frequent authentication and a much more delicate sharing of data. In turn, many emerging companies, including regional sector providers, mobile network operators (MNOs), and cloud networks, will be involved in these programs.Multiple layers of encapsulated authentications are expected in rather an eco-system, at both network link and service levels, and standard actor authentication is needed.

4. SECURITY SERVICES IN 5G NETWORKS

4.1 AUTHENTICATION

There are two types of authentications: authentication of the entity, and authentication of the message. In 5G wireless networks both entity authentication and message authentication are necessary to handle the previously discussed attacks. Entity authentication is often used to make sure that the entity being communicated seems to be

the one it professes to be. Just when two parties communicate with each other, reciprocal authentication used between user equipment (UE) and the mobility management agency (MME) is introduced in the legacy telecommunications networks.

4.2 CONFIDENTIALITY

There Confidentiality includes two components, namely privacy and data confidentiality. Confidentiality of data helps protect transmission of data from passive attacks by restricting access to data just to meant users and attempting to prevent unauthorized users from accessing or disclosing it. Privacy inhibits the regulating and influencing of legitimate user-related information, for example, privacy involves protecting traffic flows of any intruder analysis.

4.3 AVAILABILITY

The level to which a system is allowing access to any legitimate user whenever and however it is demanded is defined as the availability. Availability assesses how reliable the system is when confronted with numerous attacks and will be a performance measurement factor in 5G. Assault on availability is a standard active attack. DoS assault is one of the big assaults on performance, which may contribute to denial of service access for authorized users.

4.4 INTEGRITY

While message authentication offers confirmation of the message's source, there really is no protection provided toward duplication or message modification. 5G always intends to include connectivity, anywhere or anyhow, and also to support applications tightly linked to social everyday life, like metering for water quality standards and transport planning. In some applications data integrity is one of the key security requirements.

5. CONCLUSION

Wireless networking systems have developed from linking basic 1G cell phones to linking nearly any part of 5G existence. Threat environment has developed similarly through this transition from basic phone tapping to multiple assaults on cell devices, network hardware and utilities. 5G can use emerging technology such as modern cloud infrastructure models, SDN and NFV to bring innovative developments and utilities into the network. These systems have their very own unique protection issues that may change the network security environment still further. Nevertheless, taking into consideration these challenges will minimize the chances of possible privacy and security lapse process from the early designing process to the installation processes.

REFERENCES

[1] Akhil Gupta, Rakesh Kumar Jha and Sanjeev Jain, "Bandwidth Spoofing and Intrusion Detection System for Multistage 5G Wireless Communication Network", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 67, NO. 1, JANUARY 2018 .

[2] Ihsan H. Abdulqadder, Deqing Zou1, Israa T. Aziz1, Bin Yuan, Weiqi Dai, "Deployment Of Robust Security Scheme In SDN Based 5G Network Over NFV Enabled Cloud Environment", DOI 10.1109/TE TC.2018.2879714, IEEE Transactions on Emerging Topics in Computing.

[3] D. Fang and Y. Qian and R. Q. Hu, "Security for 5G Mobile Wireless Networks", IEEE Access, vol. 6, no., pp. 4850–4874, 2018.

[4] Christos Bouras, Anastasia Kollia, Andreas Papazois, "Teaching network security in mobile 5G using ONOS SDN controller", 978-1-5090-4749-9/17, 2017 IEEE.

[5] Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong, "A Survey on Security Aspects for 3GPP 5G Networks", DOI 10.1109/COMST.2019.2951818, IEEE.

[6] M. Agiwal and A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617–1655, third quarter 2016.

[7] Y. Wu and A. Khisti and C. Xiao and G. Caire and K. K. Wong and X.Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 679–695, 2018.

[8] D. Rupprecht and A. Dabrowski and T. Holz and E. Weippl andC. Ppper, "On Security Research Towards Future Mobile Network Generations," IEEE Communications Surveys Tutorials, vol. 20, no. 3, pp. 2518–2542, 2018.

[9] J. Qiao, X. S. Shen, J. W. Mark, Q. Shen, Y. He, and L. Lei, "Enabling Device-to-Device Communications in Millimeter-Wave 5G Cellular Networks", IEEE Communications Magazine, vol. 53, no. 1, pp. 209-215, 2015.

[10] P. K. Agyapong et al., "Design Considerations for a 5G Network Architecture," IEEE Commun. Mag., vol. 52, no. 11, Nov. 2014, pp. 65–75.