Review: Network Security of 5G network

Rahul Chatterjee

December 23, 2021

Review: Network Security of 5G network

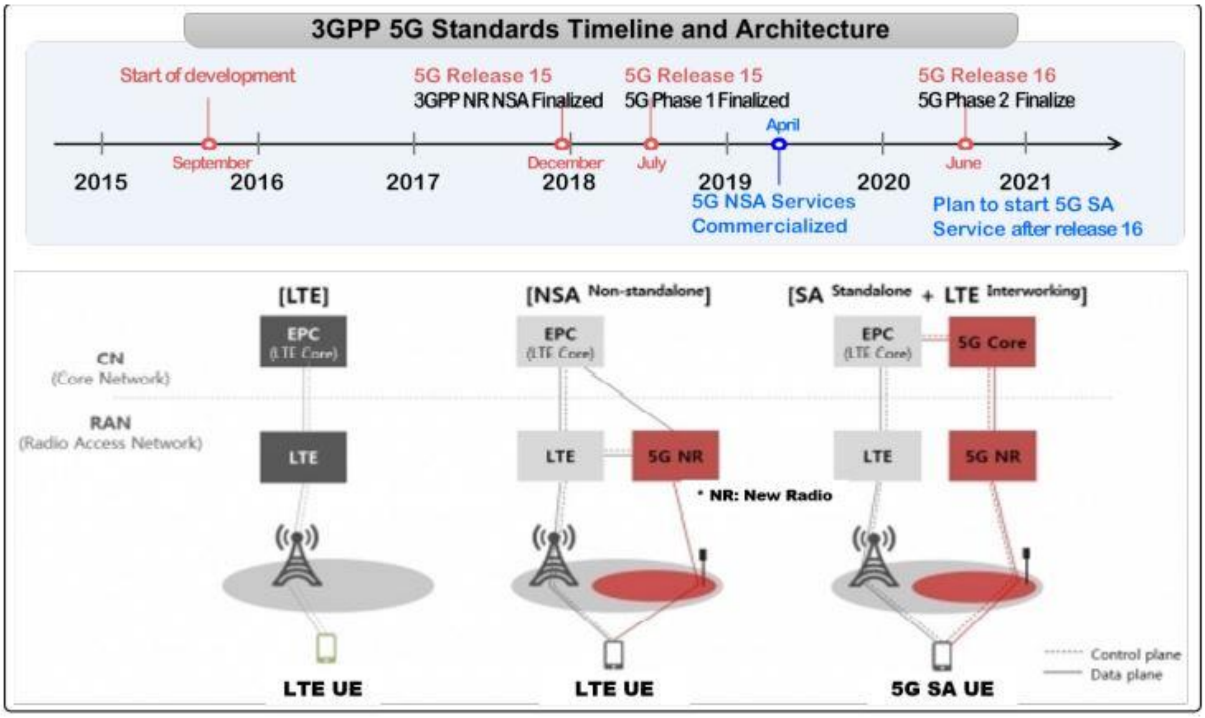
Mr. Rahul Chatterjee
Ph.D. Scholar, Computer Science, and Engineering, National Institute of Technology, Silchar, Assam, India. rahul21_rs@cse.nits.ac.in

Abstract: Fifth-generation technology (5G) was introduced as a commercialized one in 2019 and officially by 3GPP International Telecommunication Union (ITU) is IMT-2020.In 5G, the functionalities are not limited by voice and data, and there has happened a structural change to the internet of things devices, sensitive to latency by 3GPP and reliability. However, this technological evolution poses more challenges than previous, like creating a new access path, following complex interoperation structures, security downgrading, and security visibility-related limitations. Research on 5G security threats and architecture has been actively ongoing at ISO communication carriers and universities to handle such problems. Because of the unknown nature of mobile carrier networks, security researchers find it challenging to research 5G security technology design and application process. Here various security attacks and some security treads have been discussed. It is expected to use the output as basic data for 5G modelling.

Keywords: 5G security,5G security technology, Cyberattacks

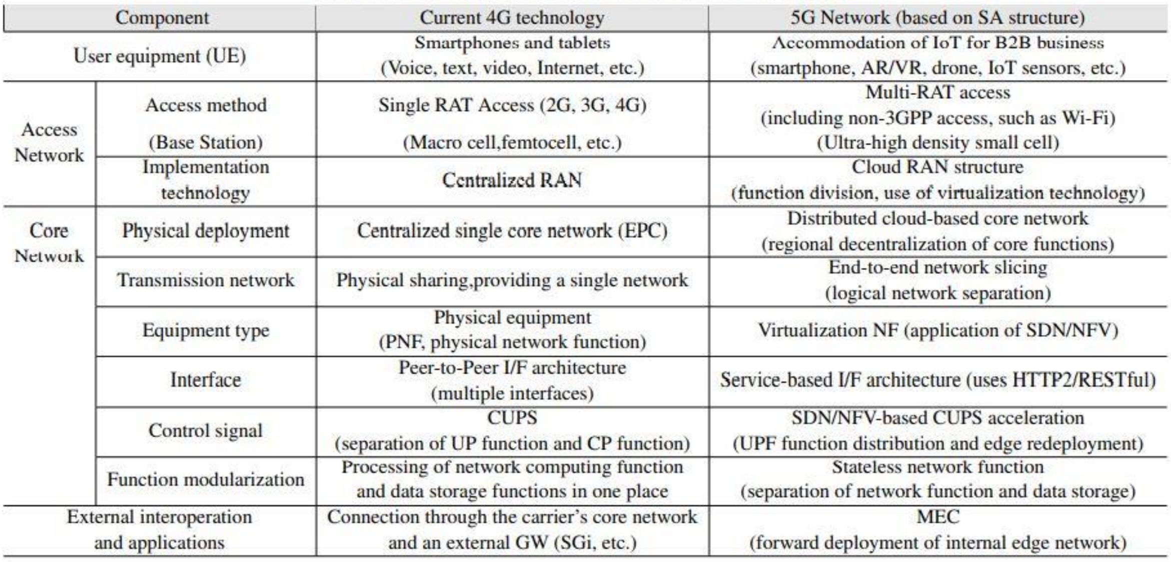
Introduction :

5G mobile network is a standard wireless technology developed by 3GPP, and officially International Telecommunication Union (ITU) is IMT- 2020. 3GPP promoted the first stage standardization of 5G technology from 2010 and completed the first stage of 5G release 15 standards in 2018. The timeline of the architecture is described below.



There is a technological evolution of fifth-generation networks, i.e., from fourth-generation technology to fifth-generation technology. The direction chart of 5G technical is described below.

Table 1: Direction of 5G technological evolution



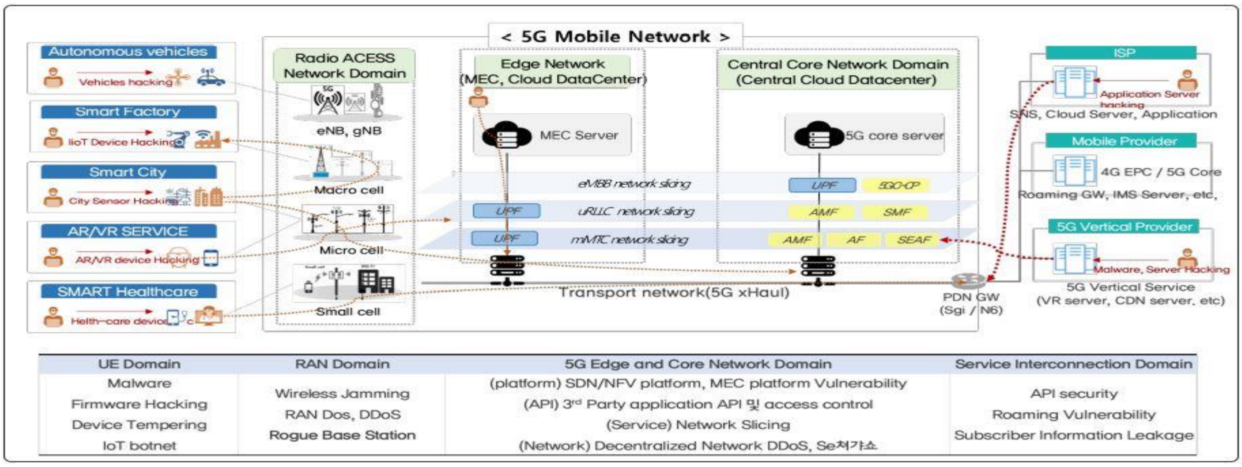
Component		Current 4G technology	5G Network (based on SA structure)
User equipment (UE)		Smartphones and tablets (Voice, text, video, Internet, etc.)	Accommodation of IoT for B2B business (smartphone, AR/VR, drone, IoT sensors, etc.)
Access Network	Access method (Base Station)	Single RAT Access (2G, 3G, 4G) (Macro cell,femtocell, etc.)	Multi-RAT access (including non-3GPP access, such as Wi-Fi) (Ultra-high density small cell)
	Implementation technology	Centralized RAN	Cloud RAN structure (function division, use of virtualization technology)
Core Network	Physical deployment	Centralized single core network (EPC)	Distributed cloud-based core network (regional decentralization of core functions)
	Transmission network	Physical sharing,providing a single network	End-to-end network slicing (logical network separation)
	Equipment type	Physical equipment (PNF, physical network function)	Virtualization NF (application of SDN/NFV)
	Interface	Peer-to-Peer I/F architecture (multiple interfaces)	Service-based I/F architecture (uses HTTP2/RESTful)
	Control signal	CUPS (separation of UP function and CP function)	SDN/NFV-based CUPS acceleration (UPF function distribution and edge redeployment)
	Function modularization	Processing of network computing function and data storage functions in one place	Stateless network function (separation of network function and data storage)
External interoperation and applications		Connection through the carrier's core network and an external GW (SGi, etc.)	MEC (forward deployment of internal edge network)

2. New security threats of 5G network:

Major countries, such as the EU, USA, Korea, and China, are interested in 5G security issues and engage in more intense competition for to taking into a market of 5G services. Therefore, research on the 5G security structure has been underway at the security working group (WG) of ITU-T SG17, 5G PPP, and 3GPP, an ISO. Working Group of 5G Next Generation Mobile Networks (NGMN), by mobile communication carriers, handles network slicing and MEC security requirements. The European Telecommunications Standards Institute, virtualization security for network function (NFV SEC) WG, manages the security specifications of the NFV platform.

2.1 Security issues :

With the increment of functionalities and qualities of the network at 5G, it also faces various security issues. And there are some domains like UE domain, Ran domain,5G Edge and Core network domain, and service interconnection domain. These security issues can be classified into five parts and are described below



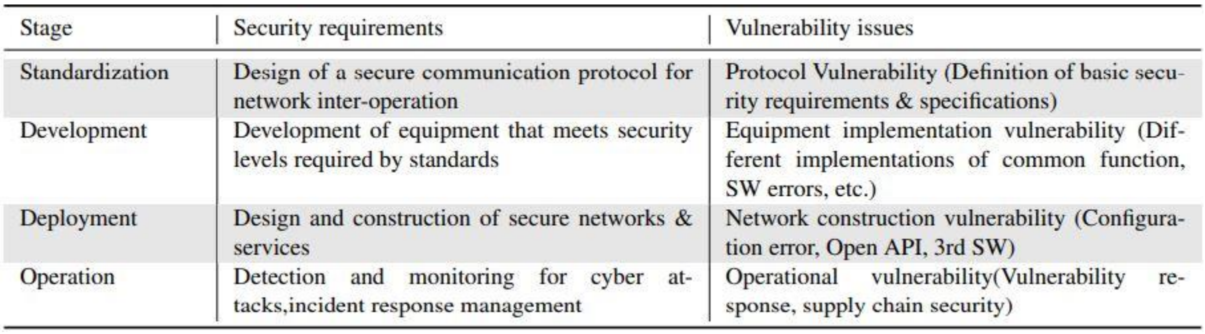
UE Domain	RAN Domain	5G Edge and Core Network Domain	Service Interconnection Domain
Malware Firmware Hacking Device Tempering IoT botnet	Wireless Jamming RAN Dos, DDoS Rogue Base Station	(platform) SDN/NFV platform, MEC platform Vulnerability (API) 3rd Party application API 및 access control (Service) Network Slicing (Network) Decentralized Network DDoS, Se처가소	API security Roaming Vulnerability Subscriber Information Leakage

2.1 IoT device security:

The speed of 5G is expected to be 20 times more than LTE, and the number of connected IoT devices will be more than ten times(1 million per unit area). The main advantage of 5G is that it can make a super-connected environment that provides mMTC services by sensing more IoT devices to access the 5G network. There are more likely to be exposed to vulnerable environments like access by malicious applications and information leakage by man-in-the-middle attacks.

3. Classification of 5G Network protocol Attacks:

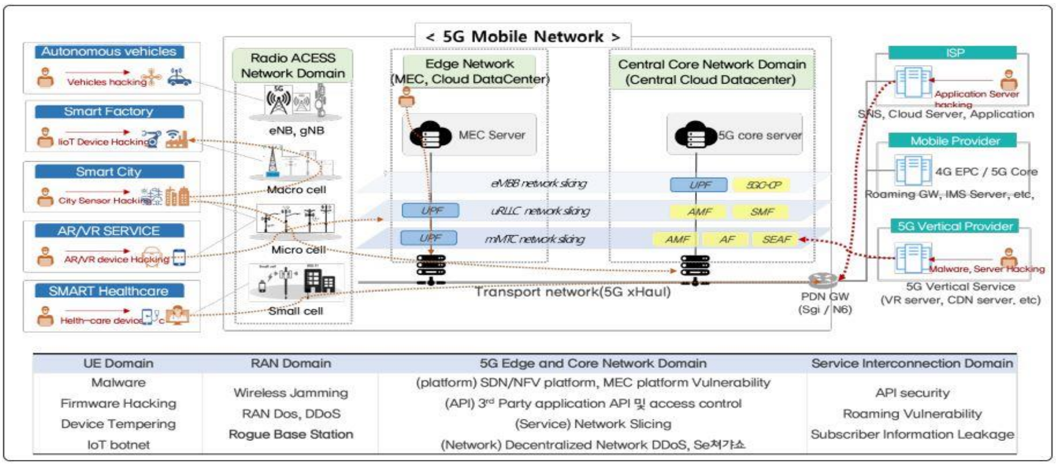
To protect 5G networks and services, we must design some new security technologies from earlier. There are some security requirements and vulnerability issues for each stage to service from standardization.



Stage	Security requirements	Vulnerability issues
Standardization	Design of a secure communication protocol for network inter-operation	Protocol Vulnerability (Definition of basic security requirements & specifications)
Development	Development of equipment that meets security levels required by standards	Equipment implementation vulnerability (Different implementations of common function, SW errors, etc.)
Deployment	Design and construction of secure networks & services	Network construction vulnerability (Configuration error, Open API, 3rd SW)
Operation	Detection and monitoring for cyber attacks,incident response management	Operational vulnerability(Vulnerability response, supply chain security)

4. 5G network protocol-based issues:

The 5G network associates SA service-based infrastructures. Until the 4G core network, internal communication functions, services and applications were developed in the control of carriers, and interoperation between equipment was possible enough through the P2P interface. However, for 5G, the interoperation between equipment was unified with HTTP-based web interfaces. The open API facilitated internal communication service functions and data access for service providers of the vertical industry, like IoT and factory automation. The mobile network section is relatively closer compared with the IP network, which has served



UE Domain	RAN Domain	5G Edge and Core Network Domain	Service Interconnection Domain
Malware Firmware Hacking Device Tempering IoT botnet	Wireless Jamming RAN Dos, DDoS Rogue Base Station	(platform) SDN/NFV platform, MEC platform Vulnerability (API) 3rd Party application API 및 access control (Service) Network Slicing (Network) Decentralized Network DDoS, Se처가소	API security Roaming Vulnerability Subscriber Information Leakage

as a high barrier against hackers. However, because the Internet web technology adopted in the 5G SBI architecture is well known to security attackers and web application services still have many security vulnerability, it can be exploited as the attackers' preferred attack methods. In addition, open API security can be a problem by sharing API functions, such as SCEF and NEF, to the outside. It is expected that vulnerability management of popular existing web applications & access control to open APIs will be essential.
In 5G, standards for security have been improved to address security threats occurring in 2G,3G,4G networks. However, the response standard for attacks on the user plane is relatively not adequate. Communication carriers operating 5G networks are really concerned about whether they can detect the connection transmitted from the user plane path, different types of IoT DDoS traffic passing through 5G networks, DDoS attacks through virtualized slicing networks, and abnormal traffic in numerous edge networks.

5. Conclusion:

The 5G network induced technological advantages by adopting a software-defined infrastructure to accommodate the connection of IoT devices. While 5G Security is an advanced step forward, the inherent risks interconnection prior network continue to grow against a much larger volume of traffic, and it's applications. With its high complexity and many interconnect partners and hubs, IoT traffic can be an especially vulnerable and very attractive target for attackers.

References:

[1] Securing 5g era. https://www.gsma.com/security/securing-the-5g-era/ [Online; accessed on February 3, 2020], 2020.
[2] I. Ahmad, T.Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. Overview of 5g security challenges solution. IEEE Communications Standards Magazine 2(1):36–43, March 2018.
[3] P. Bisson & J. Waryet. 5G PPP Phase Security Landscape. Technical report, 5G PPP, June 2017.
[4] ANISA.Signaling Security in Telecom SS7/Diameter/5G. Technical report, ENISA, March 2018.
[5] Ericsson.5g security - scenarios and solutions. Technical report, Ericsson, 2017.
[6] Morrison.A guide to 5G network security. Technical report, Morrison, December 2018.
[7] M. A. Ferran, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke. Security for 4g & 5g cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network & Computer Applications, 101:55–82, January 2018.
[8] M.Geller and P. Nair. 5G Security Innovation with Cisco. Technical report, CISCO, 2018.
[9] Huawei.5G security architecture. Technical report, Huawei Technologies, November 2017.
[10] H. Jim.5G Security Strategy Considerations. Technical report, Juniper Networks, April 2019.

Rahul Chatterjee ,got his B.Tech. degree from M.A.K.A.U.T.,West Bengal in 2020, now doing Direct PhD from NIT Silchar .And his area of research is Computer Network.