5G core network security issues and attack classification from network protocol perspective

Hwankuk Kim*
Department of Information Security Engineering
Sangmyung University, 31, Sangmyengdae-gil, Cheonan-si, South Korea
rinyfeel@smu.ac.kr

Abstract

Fifth-generation technology [5G] services commercialized in 2019 have not only provided voice and data communication but also undergone significant structural changes in mobile networks to accommodate Internet-of-things devices, sensitive to latency and reliability, by adopting the latest ICT technologies, such as software-defined networking/network function virtualization, multi-access edge computing, and network slicing. However, this technological evolution poses new security challenges, such as creation of new access paths, owing to its complex inter-operation structures, security downgrading, and limitations in security visibility. To address these issues, research on 5G security threats and security architecture has been actively underway at international standards organizations, communication carriers, and universities. However, security researchers find it difficult to conduct studies on 5G security technology design and application methods owing to the relatively unknown nature of the mobile carrier network. Therefore, in this paper, we analyzed five new security issues for each 5G section, relative to 5G technical advantages, by reviewing previous studies. In addition, we classified cyber attacks against nine network protocols primarily used in the 5G core network. The result of this study is expected to be used as basic data for modeling 5G security threats.

Keywords: 5G security, Internet of things, 5G security technology, Cyber attacks, 5G threats

1 Introduction

The fifth-generation [5G] mobile network is a wireless communication standard technology, established by 3GPP, and its official name defined by the International Telecommunication Union (ITU) is IMT-2020. To respond to the drastic increase in mobile traffic and Internet-of-things (IoT) devices, 3GPP promoted standardization of 5G technology from 2010, as shown in Figure 1, and completed the first stage 5G Release 15 standards in 2018. However, with Release 15, non-standalone (NSA) commercial services (i.e., a structure where user equipment and base stations are based on 5G technology, yet the core network is connected to the 4G core network) have been launched, which provides enhanced mobile broadband [eMBB] services by applying 4G technology and a part of 5G technology. In addition, the second standardization (Release 16) of the standalone (SA) structure reflecting ultra-reliable and low latency communications [uRLLC] and massive machine type communications [mMTC] service requirements is underway, with the aim of establishing standards in the first half of 2020[28].

Until 4G mobile communication, mobile networks have been developed to improve the performance of data transmission speed and the capacity of smartphone devices. However, 5G technology is evolving with the consideration of various new IT technologies to build a mobile network environment that can accommodate the features and service requirements of various IoT devices, ultimately realizing a hyper

Journal of Internet Services and Information Security (JISIS), volume: 10, number: 2 (May 2020), pp. 1-15
DOI: *10.22667/JISIS.2020.05.31.001*

[*]Corresponding author: Department of Information Security Engineering, Sangmyung University, Tel: +82-(0)41-550-5101

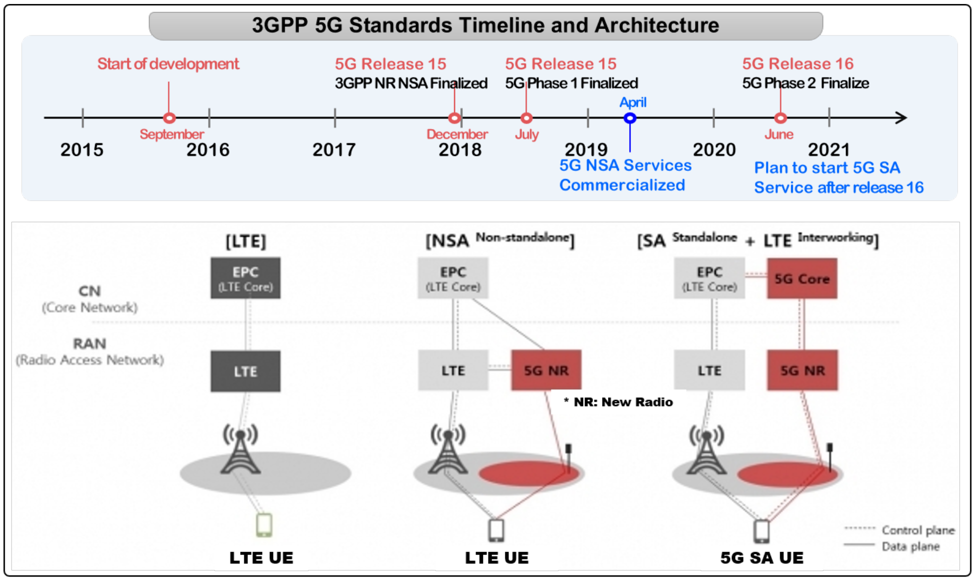


Figure 1: 3GPP 5G Standardization timeline and Architecture

connected society, which utilizes AI and autonomous vehicles. By providing a faster “mobile communication environment,” where there is no difference between wired and wireless networks in terms of data transmission and reception capacity and speed, an “IoT communication environment” can be implemented. Such an environment can offer realistic multimedia content, such as 4K/8K and AR/VR, through new devices, such as AR, VR, drones, and smartphones, while simultaneously ensuring low power consumption in IoT devices and stability of services, even in environments where many devices are connected[27]. ITU-R classified the three major services of 5G mobile network technology into ultra-high speed and large capacity (eMBB), uRLLC, and mMTC, according to each service requirement, such as speed, bandwidth, and latency. The technology aims to provide up to 20 times faster speed, 10 times more IoT device connections, and 10 times shorter low-latency services than 4G mobile communication technology[11]. We divided the technical features of the 5G network by component (i.e., user device,

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)

wireless access network, core network, externally interoperable applications) and summarized them in Table 1(reconstruction based on resources from [28][23][27]). As the main features, 5G techniques selected the software-based architecture, such as cloud-based virtualization technology, network slicing, multi-access edge computing (MEC) support, and service-based interface, by adopting the latest ICT technology to achieve the performance goal of 5G services and provide a flexible and scalable mobile network, according to the business-to-business environment.

5G security threat modeling must precede the design of the 5G core network security technology, and in this study, we intend to classify the methods of 5G network attacks for security threat modeling. While previous studies mainly analyzed the relationship between protected assets and security threats, this paper is meaningful in that it analyzed security issues related to inter-operated 5G technology characteristics in detail and classified attack types from the perspective of network protocols.

Chapter II describes security threats, according to the evolution of 5G network technologies, by analyzing the previous studies of 5G security threats. Chapter III classifies the security vulnerability issues of mobile networks and the types of network-based cyber attacks that are likely to occur in a 5G network and describes new protocol security issues of the SA-based 5G core network. Lastly, Chapter IV concludes this paper with a summary of this study and future research direction.

2 New security threats of the 5G network

2.1 Related Works

Major countries, such as EU, USA, Korea, and China are highly interested in 5G security issues and engage in more fierce competition for the commercialization of 5G services. Therefore, research on 5G security architecture has been underway at the security working group (WG) of ITU-T SG17, 5G PPP (participation by the European Commission, manufacturers, carriers, service providers, and research institutes), as well as 3GPP, an international standardization organization. 5G Working Group of Next Generation Mobile Networks (NGMN), led by mobile communication carriers, handles network slicing and MEC security requirements. The European Telecommunications Standards Institute, network function virtualization security (NFV SEC) WG, mainly handles the security specifications of the NFV platform.

With regard to the 5G security standards as a responsibility of 3GPP SA3, discussions on standards for security architecture, authentication, network slicing security, and subscriber information protection started in 2016. Security standards (TS 33.501) were announced in August 2018 at 5G Release 15[22]. The Release 15 security standards have further strengthened security to address various security issues discovered in the previous generations. The following was introduced for the improved security function: the International Mobile Subscriber Identity (IMSI) information encryption function to protect subscriber information (IMSI user identifier stored in SIM card, etc.,), Security Edge Protection Proxy (SEPP) to solve the Signaling System No.7 (SS7) security issues between roaming domains and to implement the application layer security function between different carriers (i.e., public land mobile network) and the integrated authentication framework (i.e., security anchor function (SEAF)), which can use the same authentication method for 3GPP access and non-3GPP access. SEAF enables devices to be re-authenticated without executing a full authentication method (e.g., AKA authentication), even when they move between different access networks or between different service networks[24][17].

The European Union Agency for Cybersecurity (ENISA) classified 5G network threat types into seven categories, in addition to conducting a long-term evolution (LTE) security threat analysis and then analyzed them as a threat landscape according to the CIA criteria. USA's 5G America analyzed the potential security threats by classifying them into UE/Device, radio access network (RAN) section, edge, core, SGi, and interoperation section, through 5G threat surface research[4].

As part of the EU Horizon 2020 project, the 5G PPP “Enablers for Network and System Security and Resilience (ENSURE)” announced the 5G security architecture and stressed that various vertical ecosystems on each domain, as well as horizontal domain-specific security, should be taken into consideration; additionally, vertical domain security should be considered for this[21][3].

In 2018, the Department for Digital, Culture, Media, and Sport (DCMS) in the United Kingdom announced the research results on 5G security architecture and security requirements through the 5G technology leading strategy. It emphasized that the protection of networks, systems, and services against security threats has become increasingly difficult because the 5G environment provides vertical industrial services by connecting various types of networks and devices, compared to the conventional mobile communication environment. The research suggested four considerations, i.e., end-to-end security, layer-to-layer security, multi-domain security, and security internalization for the implementation and design of secure 5G architecture[25].

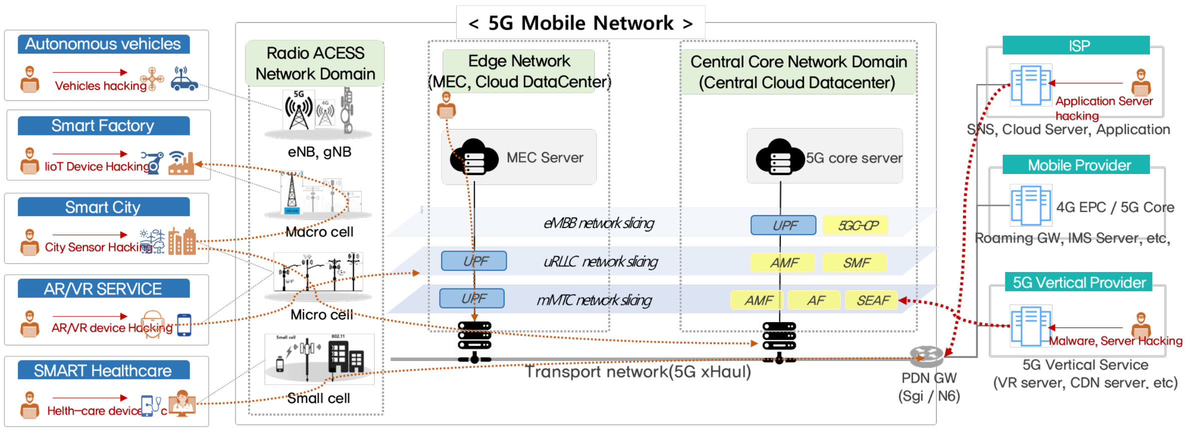
Global 5G communication equipment manufacturers, such as Ericsson[5], Cisco [8], and Huawei[9], have also announced security requirements and architecture models according to changes in 5G technology and have commonly suggested requirements for the design of 5G security architecture, such as a distributed cyber attack defense, flexible and scalable security, automation security, and vertical security, as well as security functions on the control plane and user plane presented by the 3GPP security standard.

Research on mobile network security vulnerabilities has been active. KAIST University[12] in South Korea is a leading group of 4G network security vulnerability research. It developed LTE Fuzzer, which is a checking tool for LTE security vulnerabilities, and announced a number of security vulnerabilities in the radio resource control and/or non-access stratum (RRC/NAS) protocol. In 2018, Oulu University[14] in Finland analyzed the requirements of 5G security threats and response solutions. As the key points, it conducted analysis research on 17 security threats that could occur in the 5G environment and security threats for each attack target (i.e., software defined networking (SDN), NFV, and Channel, Cloud). Ferrag of Algeria University[7] conducted research on the classification of 35 security attacks related to authentication and privacy into 4 categories in the 4G and 5G networks. Xidian University[29] in China, classified 13 security threats by dividing security threats that could occur in the 5G RAN section into physical, control, and service layers and then analyzed security requirements in terms of CIA and access control.

Global IT companies are also actively conducting research on the development of security technologies, such as a 5G firewall. Positive Technology[19][20], which is a global firm that develops a signaling firewall for mobile networks, has been conducting research on security vulnerabilities and developing mobile network security technologies for various protocols, such as the GPRS tunneling protocol (GTP), signaling system no. 7 (SS7), and Diameter. Cisco[8]has analyzed 5G security threats that could occur when building a 5G network and conducted research on the development of response technology products.

2.2 Security issues of 5G network

[Figure 2] summarizes the typical security threats for each section centered around the 5G mobile network. In general, over the mobile traffic path, user equipment is connected to application servers of Internet protocol (IP) service networks (Internet service providers, roaming interoperation between countries, etc.) through a radio access network (RAN) and a core network, providing mobile network functions for mobility management, authentication, billing, etc. Here, because the 5G network is connected to vertical industrial networks, such as automobiles, medicine, factories, and IoT devices, as well as the existing legacy networks (2G, 3G, 4G) and Internet service networks (e.g., SNS, cloud server, etc.), it will create a network connection structure consisting of complex heterogeneous networks, centered around the 5G networks. The complexity of these networks can lead to weak linkages arising from the interconnection



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

Figure 2: 5G Security Threat Landscape

of networks and devices with different security requirements and different levels of security technology applied. Therefore, the biggest security threat is that it can downgrade 5G security. In this section, we describe these security issues by classifying them into five categories.

2.2.1 IoT device security

5G technology is expected to handle high-speed large-capacity traffic, 20 times faster than LTE, and the number of IoT devices connected to 5G networks is expected to grow by 10 times (1 million per unit area). The advantage of 5G is that it can establish a hyper-connected environment that provides mMTC services by allowing a large number of IoT devices to access 5G networks. However, if IoT devices that are vulnerable to security management are infected with malicious code, which triggers large-scale distributed denial-of-service (DDoS) traffic, they may have a direct impact on the 5G network. According to the European ENISA Threat Landscape Report 2018 [26], the size and intensity of DDoS attacks are growing at an alarming pace. In 2016, the first case of an IoT devices-related DDoS attack occurred, and in 2018, a terabyte DDoS attack (1.35 TBps) was targeted against the GitHub server; the level of the DDoS attack has been gradually increasing up to 1.7 terabytes.

Unlike smartphones, designing common security standards and architecture for IoT devices is not easy because industry-specific device types (e.g., smart factory devices, smart city sensors, and CCTV), applications, and supply chain ecosystems are diverse and complex. In addition, as the installation of a high-level security function for low-end IoT devices is difficult, they are vulnerable to tampering because they have weak passwords and old security protection. Therefore, they are more likely to be exposed to vulnerable environments, such as improper access by malicious applications and leakage of subscriber information (IMSI) by man-in-the-middle attacks. Hackers may have access to vulnerable IoT devices and infect them with malicious code to construct a large quantity of IoT botnets and then remotely control them through a C&C server to use IoT devices as a means of attack [8].

2.2.2 5G RAN security

The RAN section is composed of various types of base station equipment (macrocell, microcell, femtocell, etc.). The RAN base station equipment is connected to UE through a wireless communication interface (i.e., Air Interface) and acts as relay equipment, which connects to the 5G core equipment through a wired transmission network. 5G RAN technology has the advantage of allowing various types of wireless access technologies to gain access to the 5G network by accommodating not only 3GPP wireless access technologies (i.e., 2G, 3G, 4G) but also non-3GPP access technologies, such as Wi-Fi and wired Internet. However, as various heterogeneous wireless access and mass IoT device access are allowed, protection of the RAN section is critical. To connect mobile communication services, control signals (movement, authentication, billing, etc.) are exchanged between the UE and the base station (eNB, gNB) equipment of the RAN section and the communication equipment (MME) of the core network. Here, when abnormal control traffic, due to millions of user devices connected to the RAN base stations, are transmitted and received, resilience issues for failures and strengthening the security of small cells for home and business, which are easily accessible, are crucial factors.

The RAN security threat [24] includes a RAN DDoS attack that requests excessive access to wireless resources by a huge number of IoT botnets, infected with malicious code, and a jamming attack on wireless signal channels. The base stations transmit and receive abnormal data, owing to RAN DDoS and radio interference jamming attacks, thus resulting in the exhausting of radio interface resources in the RAN section, which ultimately leads to availability issues, preventing normal data reception. Rogue base station issues allow attackers to launch various types of attacks, such as the interception of user location information, tampering of transmission information, and DDoS attacks between the mobile user and the network through a man-in-the-middle attack, between the mobile UE and the 5G network, using a false base station. Rogue base station issues were continuously raised for 2G, 3G, and 4G legacy networks and various improvements were applied to the 5G security standards. However, if the distribution of small-scale femtocells is accelerated to resolve the shadow area of wireless mobile communications, rogue base station issues can still be raised in cases where attempts by hackers targeting small cells, for which security management is relatively neglected, compared to macro base stations, have increased, such as the security threats of low-end wireless local area networks with the wide spread use of wireless APs.

2.2.3 Decentralized 5G core architecture security

The 5G core network adopts a decentralized core network structure. Until the 4G network, a centralized network structure was adopted, in which traffic signals and data transmission paths were centralized in a central office, up to the 4G core network. However, for the local redeployment of the communication function, the 5G network was decentralized by dividing it into a core network and an edge network. Because the path of control plane and user plane traffic is physically separated, the central office mainly processes control traffic, and user data is processed by cloud-based edge communication centers at local offices. This decentralized core network structure is an efficient structure for providing ultra-low latency services and network slicing services. However, because the protection targets are widely and locally distributed, there are security visibility issues which are tightly interconnected between legacy network (2G, 3G, 4G networks) devices. Therefore, a decentralized response to cyber attacks is inevitable, resulting in a decentralized response to them from a comprehensive perspective.

2.2.4 Software-based Infrastructure security

The 5G network has shifted from hardware-dependent infrastructure to software-based infrastructure [4]. The software-based infrastructure is implemented using 5G communication servers, network equipment, and network slicing services, through SDN and NFV virtualization technology. It provides an independent network slicing service for each uRLLC, mMTC, and eMBB application service by separating a single physical network into multiple virtual networks. Here, instead of dedicated equipment, the network communication function is implemented on a general-purpose x86 server, in the form of a virtualized SW (i.e., Virtual Machine). However, although virtualization technology, which is the core of 5G equipment and service implementation, has advantages in terms of resource efficiency, flexibility, and availability, by sharing physical networks and HW server resources (e.g., CPU, memory), it can be relatively vulnerable to load attacks on physically shared HW resources, unauthorized access to network slicing and shared resources, malicious code distribution through shared resources, and configuration errors for virtualization management SW [8][24][10][16].

(1) SDN/NFV security: SDN technology controls the network delivery function, which has been processed in hardware, by separating the network control function (SDN controller) and traffic delivery function (SDN switch) [5]. Traffic bypass attacks that exploit control protocol vulnerabilities between SDN controllers and switches, unauthorized access between switches and controllers, and resource depletion of SDN systems by DoS attacks can paralyze services. For example, a saturation attack can occur, which exhausts the SDN switch flow table by attacking SDN controllers. In addition, NFV technology implemented on a general-purpose server has a high possibility of security issues, unless hypervisor security, malicious VM migration issues, changes or authentication of applications running on virtualized network functionality, and authorization for networking functions are properly controlled. If there is no protection mechanism in place for authentication and authorization of applications, malicious third party applications can obtain network information from SDN controllers [2][3].

(2) Network slicing security: Network slicing is a new technology introduced to the 5G network. It is a virtual network transmission technology that logically separates traffic for each eMBB, uRLLC, and mMTC service, while using the same physical network. Here, if the network slicing for each service is not properly separated, there is the possibility of attack from one slice to another. For example, an attacker may launch a network slicing resource depletion attack by maliciously overstretching traffic capacity in a network slice dedicated to a specific service, and subsequently, affect other network slices or simultaneously activate specific applications. Without proper encryption applied to the network slice, an attacker could eavesdrop or tamper with data belonging to other slices.

2.2.5 MEC security

MEC refers to the concept of providing services by constructing an application server inside a mobile network, close to the user's device, using a method that goes through the existing mobile communication core internal network and connects to the application server of the Internet service. The combination of the 5G network and the concept of edge computing in MEC has the advantage of providing IoT applications and services, such as telemedicine, autonomous vehicles, factory automation, and IoT sensor data information processing, in real-time without delay. However, because the edge computing server is forward deployed inside the 5G edge network (connected with UPF equipment), a new connection path can be created, which leads to security issues.

In a mobile network, MEC is implemented through cloud and virtualization technology and is expected to operate in an open system running third party applications. Therefore, MEC systems built into the internal network of mobile networks can be the main targets of hackers[10]. For example, MEC can be built as a virtualization platform and MEC applications can run on the same platform as some virtual network functions. If a MEC application is a third party application that is difficult for mobile carriers to control, it can consume virtualized network resources or obtain access to unauthorized sensitive information with inappropriate application programming interface (API) permissions. Furthermore, there is a risk of providing a new attack path for an attacker, who can attempt to launch an attack on edge network functions, such as UPF, which is distributed 5G network internal equipment, by inserting malicious applications[25].

3 Classification of 5G Core Network Protocol Attacks

3.1 Security vulnerability issues of the 5G network

To protect 5G networks and services, security technologies that are different from those of the previous generations must be designed, developed, and operated. To establish and operate a safe 5G network, Ericsson[6] derived the security requirements in the stages of standardization, equipment development, network construction, and service operation. Security requirements and security vulnerability issues for each stage have been summarized in Table x. Because the mobile communication network is composed of a complex ecosystem, it is relatively difficult to solve the associated security vulnerability issues.

Table 2: 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)

First, in the standardization stage, communication protocols and interfaces must be designed safely for the interoperation of networks and systems between countries. Research on the standards of 5G basic security requirements and architecture has been active by international standards bodies and de-facto standard organizations. 3GPP security standards for authentication and key management for mutual authentication between users and networks, signaling messages of the control plane, and data protection of the user plane have been developed to continuously enhance the security of the mobile network. However, because standardization defines the minimum basic security requirements and specifications, there are concerns that vulnerabilities in standard protocols can occur at all times.

Second, manufacturers should develop equipment that meets the security standards and target levels required by standards. For example, security vulnerability issues continuously occur in the stage of equipment implementation because each equipment manufacturer implements different security functions; equipment implemented with SW may contain SW errors or unknown vulnerabilities at the time of equipment implementation can be found over time. However, when the equipment construction is completed, it may take a long time to patch and verify the SW, which leads to supply-chain security issues.

Third, communication carriers must design and build secure networks and services by verifying supply-chain products, to ensure that equipment manufacturers' communication equipment and service applications are implemented to meet security requirements. Nonetheless, configuration setting errors can be present in the process of building networks and services and security issues by third party applications, not by communication carriers, have been continuously raised.

Lastly, in the final stage of service operation, it is crucial to remove security vulnerabilities against highly advanced and intelligent cyber attacks and to restore resilience after cyber breaches. Moreover, the response time required to resolve security issues at each stage can also be a barrier. In other words, because it takes several years to reflect security vulnerabilities of standard protocols in the standards and it takes approximately 6 months or more for SW patches to provide safety verification to address equipment implementation vulnerabilities, it is critical to close the security gap between each stage.

3.2 Classification of network attacks on 5G NSA network

A number of complex standard protocols for mobile networks are used for signal processing, such as user call and data routing, paging, mutual authentication, roaming, and billing. Research on security vulnerabilities in mobile network protocols and cyber attacks that exploit these vulnerabilities has been continuously conducted since the introduction of the 2G mobile network.

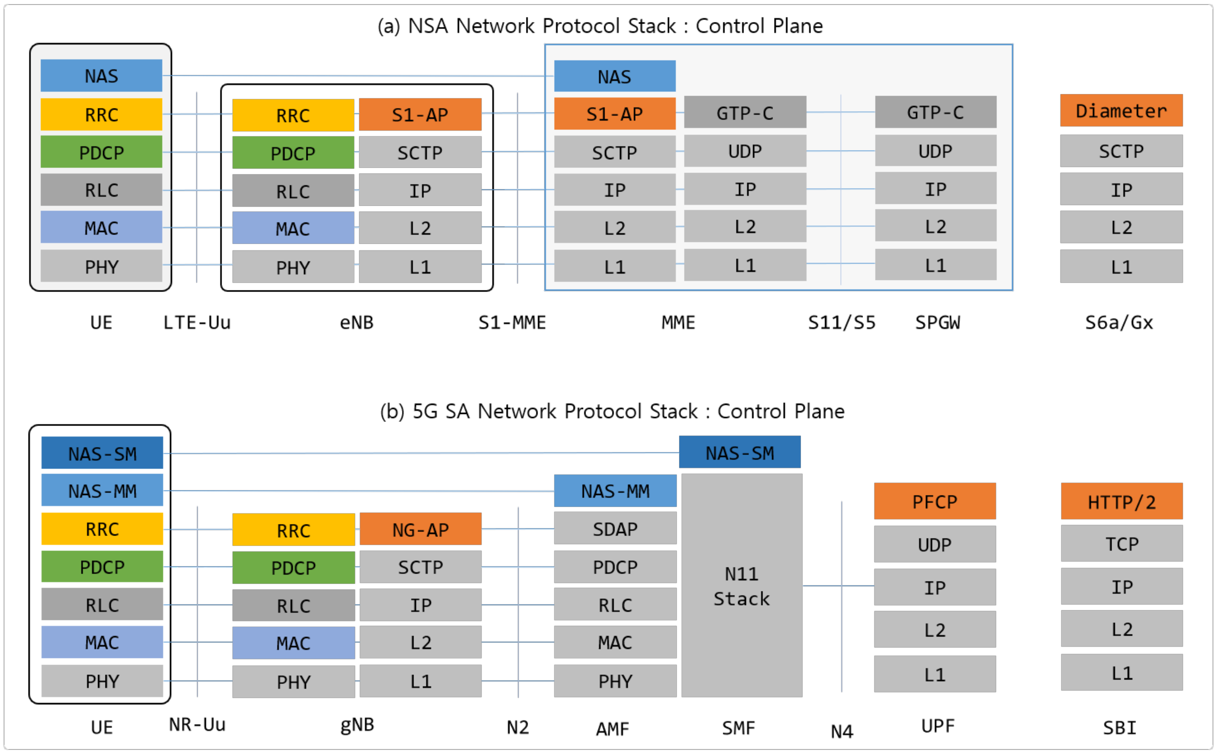


Figure 3: changes of network protocol(control plane)

As described in Section 3.1, because the protocols defined in the standards define only basic security functions, security is not sufficiently considered when designing these protocols. Therefore, although various protocols are interoperated and interacted in mobile communication carrier networks, there are many security vulnerability issues because they are applied differently, according to unique settings and technologies for each communication equipment manufacturer or service area. Because future 5G standards are to be modified by the use of new protocols in the 5G core network, as shown in Figure 3, the greater complexity of interoperation between heterogeneous networks and protocols may require a significantly more complex design and implementation of security technology. Therefore, in this section, we first investigate the attacks on the NSA 5G core network protocols, based on the 4GC EPC core, and then describe the issues for new 5G SA protocols.

Table 3 shows the classification of attack types related to network protocols on 5G core network.

5G security threats classified by ENISA[15] are SPAM, identifier spoofing, location tracking, DoS, subscriber fraud, message intercept, call routing attacks, and infiltration attacks. The most common 5G threats are the following: • Eavesdropping/interception/hijacking: this threat is intercepting into mobile traffic gaining valuable and confidential subscriber information • Fraud: Attackers can use services at the expense of the operator or another subscriber using invalid or hijacked IMSI • Injection of malicious messages: Disrupting sessions and creating DDoS • Subscriber denial of service: this threat is spoofing subscriber IDs to generate malicious messages that cause service disruption for an individual subscriber • Message Modification: this prevent message delivery or allow malicious content delivery, disrupting service • Network DDoS: Malicious, malformed or invalid signalling packets are sent that overwhelm network elements or cause vulnerable elements to fail

Table 3: Classification of 5G Threat based network protocol

Network Domain			UE	Access Network		Core Network						External Network	Ref.
5G NSA Components			Devices	eNb	-	SGW	MME	PCRF	HSS	IMS	PGW	ISP, Roaming	
5G SA Components				gNb	UPF(MEC)	AMF	AMF(SMF)	PCF	AUSF	AF	UPF	Vertical Service	
Control Plane	RRC	DoS		O									[12]
		Spoofing	O	O									
		Location Tracking	O	O									
		Routing Attack	O	O									
	NAS	DoS	O	O			O						
		Spoofing	O				O						
		SPAM	O				O						
	GTP-C	DoS				O	O	O			O		[19] [18]
		Fraud				O	O	O			O		
		Routing Attack		ü		O	O	O			O		
	Diameter	DoS						O	O		O	O	[4] [20] etc
		Routing Attack						O	O		O	O	
		Information Disclosure						O	O		O	O	
		Fraud						O	O		O	O	
	SS7	DoS							O		O	O	[4] [20] etc.
		Faud							O		O	O	
		Location Tracking						O	O		O	O	
User Plane	GTP-U	DoS(GTP-in-GTP)				O	O	O	O				[19] [18] etc.
		Fraud				O	O	O	O				
		Sniffing				O	O	O	O				
	Voice over 5G	SIP Signaling DoS	O		O					O		O	[13]
		SIP Replay Attack	O		O					O		O	
		Location Tracking	O		O					O		O	
	IoT over 5G	IoT Aplication DDoS	O	O	O					O		O	
		IP based attack	O	O	O					O		O	[8][11]

(1) RRC protocol-based attack: The RRC protocol is a control protocol that manages a radio bearer of the L3 layer, related to radio resource establishment, reconfiguration, and release between the UE and radio access network. A study by KAIST[12] announced that, through the RRC protocol attack, attackers are able to launch various attacks, such as subscriber ID tampering, DoS attacks against base stations, and authentication bypass due to vulnerabilities of the baseband chipset of the UE and base station equipment implementation.

(2) NAS protocol-based attack: The NAS protocol is consists of control protocol messages that manage UE authentication, mobility, and the location between the UE and mobile communication core network equipment (MME, AMF/SMF). A study by KAIST[12] announced that, through the NAS protocol attack, attackers are able to launch attacks such as DoS against MME equipment, subscriber identification information leakage, and man-in-the-middle attacks due to vulnerabilities

in standard protocol specification, authentication bypass, and error handling processing errors for communication messages, when implementing the SW of mobile communication equipment.

(3) GTP protocol-based attack: GTP messages are a control protocol related to creating and releasing tunneling inside the core network for IP data transmission. It operates on the user datagram protocol (UDP) and there are GTP-C messages for tunneling session establishment and control in the core network section, GTP-U messages related to data transmission, and messages related to billing. With regard to the section where the GTP is used, control information (GTP-C) messages for GTP tunnel creation, maintenance, and deletion are exchanged between the MME and S-GW sections and the S-GW and P-GW sections. User packets are transmitted through GTP-U tunneling between the base station and base station sections, the base station and S-GW sections, and the S-GW and P-GW sections. GTP prime messages are used to transmit billing information (CDR) in the P-GW and OFCS sections. Because the GTP protocol was introduced with the aim of using it only within the mobile network section, without taking into account the security of encryption and authentication from the initial stage of designing the standards, research results on its vulnerability to hacking attacks have been continuously published. According to studies conducted by Positive Technology[19], GSMA[1], and KISA[18], it is possible to conduct man-in-the middle attacks and DoS attacks against EPC or 5GC core equipment through the forgery of the field values of GTP messages, malformed GTP messages, and spoofing.

(4) Diameter protocol-based attack: The diameter protocol is an IP-based protocol for Authentication Authorization and Accounting and is used to control quality of service policies, such as MME and P-GW equipment, policy server (policy and charging rules function (PCRF)), and subscriber information management (home subscriber server (HSS)). In the 5G NSA core network, it is used in the MME and HSS sections for user authentication, the P-GW and PCRF sections, and the P-GW and online charging system (OCS) sections for billing. Attacks using the diameter protocol include connection hijacking and replay attacks.

(5) SS7 protocol-based attack: The SS7 protocol is primarily used for 2G and 3G; however, this protocol attack is still a threat because, currently, roaming between countries is connected to legacy communication networks. Possible attacks to address the SS7 issues in the 5G standards include SPAM, spoofing, location tracking, subscriber fraud, intercept, DoS, and routing attacks[20][4].

The protocol-based attack on the user plane did not attract much attention, compared to the attack using the signaling protocol on the control plane. Only some DoS and message tampering attacks, using the SIP protocol to connect to the IMS server built inside the carriers to provide VoLTE services in the 4G network, have been announced. However, because various IoT services and voice services are provided in the 5G network, it is expected that DDoS attacks using protocol messages on the user plane will be the primary issue. On the user plane, potential network-based attacks were classified into three types:

(1) GTP-U protocol-based attack: The GTP-U protocol is a tunneling protocol that operates in the user plane by connecting with the GTP-C of the control plane. The typical attack based on the GTP-U protocol is a DoS attack that puts a load on the 5G core equipment through the GTP-in-GTP attack[19]. There is a possibility that an attacker may obtain network and subscriber information, including the tunnel endpoint identifier, by exploiting the vulnerabilities of the GTP protocol. It is also possible to induce a DDoS attack on networks with messages exploiting GTP through IoT botnets.

(2) SIP protocol-based attack: The SIP protocol is a voice signal control protocol used to provide VoIP over LTE services. According to the research results of KISA[13], it was possible for attackers to

conduct protocol based attacks, such as DoS attacks and call hijacking, that exploit SIP messages using various messages, such as INIVTE, which is a call control message of the SIP protocol.

(3) IoT protocol-based attack: In the 5G mobile network, data traffic of IoT devices, as well as data traffic generated by existing smartphones, is expected to increase. For IoT-based DDoS attacks, various types of DDoS are possible on the network protocol stack, such as IoT application protocols (MQTT, SOAP, etc.) and traditional IP attacks (SYN flood, UDP flood, DNS flood, HTTP flood). The main targets of these IoT DDoS attacks are 1) 5G network infrastructure (RAN, core equipment, network slice, memory of physically shared platform, etc.), 2) Internet service application servers connected via 5G network infrastructure, and 3) devices connected to the 5G network[8]. Here, IoT DDoS attack can deplete interconnected network infrastructure resources, thus, resulting in a large-scale service failure.

3.3 5G SA network protocol-based attack issues

The SA 5G core network pursues a service-based infrastructure. Until 4G core network, internal communication functions, service management, and applications were developed under the control of carriers, and interoperation between equipment was possible through the P2P interface. However, for 5G, the interoperation between equipment was unified with HTTP-based web interfaces, and the open API facilitated internal communication service functions and data access for service providers of vertical industry, such as IoT and factory automation. The mobile network section is relatively closed, compared with the IP network, which has served as a high barrier against hackers. However, because the Internet web technology adopted in the 5G SBI architecture is well known to attackers and web application services still have many security vulnerabilities, it can be exploited as attackers' preferred attack methods. In addition, open API security can be a problem by providing API functions, such as SCEF and NEF, to the outside. It is expected that vulnerability management of well-known existing web applications and access control to open APIs will be essential.

The protocols used for 5G signaling and data transmission will also change significantly. Among the network protocols on the control plane, typically, the SS7 and diameter protocols are expected to use HTTP/2, JSON, and REST API. In addition, the GTP-C protocol is expected to be modified to an HTTP-based interface. However, the GTP protocol is likely to be continuously used to interconnect data on the control plane and user plane paths.

In 5G security standards, security functions, such as mutual authentication and encryption of signaling protocols on the control plane, have been improved to address security threats occurring in 2G, 3G, and 4G networks. However, the response standard for protocol-based attacks on the user plane is relatively inadequate. Communication carriers operating 5G networks are concerned whether they can detect the connection of IP traffic transmitted from the user plane path, various types of IoT DDoS traffic passing through 5G networks, DDoS attacks through virtualized network slicing, and abnormal traffic in numerous edge networks.

4 Conclusions

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

This paper summarizes five security issues arising from 5G technical advantages: 1) security issues such as the response to DDoS attacks caused by security vulnerability of IoT devices, 2) RAN failure and small cell security management owing to heterogeneous wireless network access and coverage expansion, 3) visibility for security monitoring and expansion of the protection target owing to the decentralized mobile network structure, 4) dynamic security management and access control caused by the sharing of physical HW equipment regarding virtualization platform and network slicing technology, and 5) security issues related to third-party applications and API reliability and connection paths to internal mobile communication networks, which are caused by applying MEC.

In addition, we classified network protocol-based attacks on the 5G control and user plane paths. Given that network protocol-based attacks on the core network are designed to be basically operated in a closed internal network, issues such as non-encryption, unauthenticated origin of messages, and handling of errors mostly occur. With 5G standards, various security functions, such as SEPP function between domains and IMSI capture prevention, have been enhanced to address these security issues. However, the security standards of 5G networks focus only on protecting signaling on the control plane, and the security functions in terms of integrity and availability of the protocols on the user plane are relatively inadequate. In addition, the SBI interface structure pursued in 5G has become a security issue because it inherits conventional HTTP security vulnerabilities through the use of HTTP and REST API of the IP network.

Finally, research on the classification of 5G security threats has been conducted to categorize security threats primarily focused on targets to be protected. However, this study has a significant contribution as it classifies cyber attacks from the perspective of network protocols operating inside the core network. The analysis performed in this study is expected to be used as basic data for various 5G security equipment design and construction. For future research, we plan to analyze detailed features used for each protocol attack, which is expected to be useful for research on feature engineering for the requirements of 5G security devices and the detection of artificial intelligence-based 5G DDoS attacks.

Acknowledgments

This research was funded by a 2020 Research Grant from Sangmyung University.

References

[1] Securing the 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 and solutions. *IEEE Communications Standards Magazine*, 2(1):36–43, March 2018.

[3] P. Bisson and J. Waryet. 5G PPP Phase1 Security Landscape. Technical report, 5G PPP, June 2017.

[4] ENISA. Signalling Security in Telecom SS7/Diameter/5G. Technical report, ENISA, March 2018.

[5] Ericsson. 5g security - scenarios and solutions. Technical report, Ericsson, 2017.

[6] Errison. A guide to 5G network security. Technical report, Errison, December 2018.

[7] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke. Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and 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.

[11] H. Kim, B. Choi, E. Ko, and S. Park. New security issues and research trends with 5G technology evolution. *Review of Korea Institute of Information Security and Cryptology*, 29(5):7–20, October 2019.

[12] H. Kim, J. Lee, E. Lee, and Y. Kim. Touching the untouchables: Dynamic security analysis of the lte control plane. In *Proc. of the 2019 IEEE Symposium on Security and Privacy (SP'19), San Francisco, California, USA*, pages 1153–1168. IEEE, May 2019.

[13] E. Ko, S. Park, S. Kim, K. Son, and H. Kim. SIP amplification attack analysis and detection in volte service network. In *Proc. of the 2016 International Conference on Information Networking (ICOIN'16), Kota Kinabalu, Malayysia*, pages 334–336. IEEE, January 2016.

[14] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila. *A Comprehensive Guide to 5G Security*. John Wiley & Sons, 2018.

[15] L. Marco and M. Louis. ENISA threat landscape for 5G networks. Technical report, ENISA, November 2019.

[16] A. Nieto, A. Acien, and G. Fernandez. Crowdsourcing analysis in 5g iot: Cybersecurity threats and mitigation. *Mobile Networks and Applications*, 24(3):881–889, 2019.

[17] B. H. Noamen, W. Monica, and J. Christine. An overview of the 3gpp 5g security standard. `https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview` [Online; accessed on February 3, 2020], July 2019.

[18] S. Park, S. Kim, K. Son, and H. Kim. Security threats and countermeasure frame using a session control mechanism on volte. In *Proc. of the 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA'15), Krakow, Poland*, pages 532–537. IEEE, November 2015.

[19] Positive Technology. Threats to evolved packet core (epc) security of 4g network. `https://positive-tech.com/research/epc-research/` [Online; accessed on February 3, 2020], September 2017.

[20] Positive Technology. *SS7 Network Security Analysis Report*, February 2020.

[21] P. Ruuska, O. Mammela, J. Suomalainen, P. Bisson, C. Martins, E. Felix, T. Combe, M. Naslund, H. Englund, S. Phillips, et al. 5G-ENSURE-5G enablers for network and system security and resilience. Technical report, 5G-ENSURE Consortium, November 2016.

[22] G. SA3. Security architecture and Procedures for 5G System. Technical report, 3GPP, July 2018.

[23] Samsung. 5g core vision - revolutionary changes in core with the arrival of 5g. Technical report, Samsung, 2019.

[24] R. Sankar and G. Mike. 5G Security Strategy Considerations The evolution of security in 5G. Technical report, 5G Americas, July 2019.

[25] V. Serdar and et.al. 5G Network Architecture and Security. Technical report, UK DCMS 5G Testbed&Trial WG, December 2018.

[26] A. Sfakianakis, C. Douligeris, L. Marinos, M. Lourenço, and O. Raghimi. Enisa threat landscape report 2018: 15 top cyberthreats and trends. Technical report, ENISA, January 2019.

[27] D. Shin. New world created by 5g: 4th industrial revolution enabler that will include 5g, ai, iot, etc. `https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=82618&bcIdx=20811&parentSeq=20811` [Online; accessed on May 25, 2020], 2019.

[28] M. Shin, S. Lee, S. Lee, J. Lee, and B. Ahn. Trends of 5G network and system standard technology. *TTA Journal*, 184:40–49, 2019.

[29] F. Tian, P. Zhang, and Z. Yan. A survey on c-ran security. *IEEE Access*, 5:13372–13386, June 2017.

Author Biography

Hwankuk Kim received the B.S. and M.S. degrees in Computer Science and Computer Engineering from Korea Aerospace University in 1998 and 2000, and Ph.D. degrees in Korea University in 2017. He worked a researcher at ETRI from 2002 to 2006 and a research team manager at KISA from 2007 to 2020. Currently he is an assistant professor in the Sangmyung University. His research interests include 5G network security, software vulnerability analysis, IoT security and security data analysis.