정 보 보 호 학 회 지
제 29 권 제5호, 2019. 10

5G 네트워크 기술 진화에 따른 새로운 5G 보안 도전과제와 해외 보안 아키텍처 연구 동향

김 환 국*, 최 보 민*, 고 은 혜*, 박 성 민*

요 약

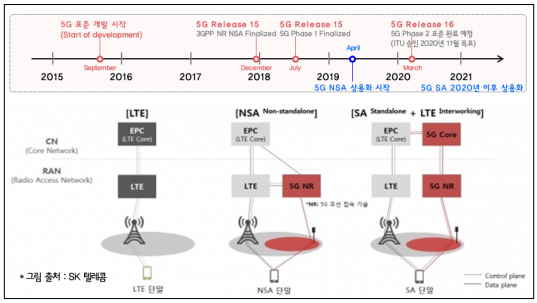
2019년 4월, 4세대 이동통신보다 최대 20배 빠른 속도, 10배 많은 IoT 기기의 연결, 10배 짧은 저지연 서비스를 제공하기 위해 5세대 이동통신이 세계최초로 상용화되었다. 5G 이동통신기술은 고속 대용량의 음성 및 데이터 통신을 제공할 뿐만 아니라 지연 속도와 신뢰성에 민감한 IoT 기기를 수용하기 위해 다양한 최신 기술을 적용하는 기술적 진보가 있었다. 그러나 5G 네트워크 및 서비스가 개방성, 확장성, 유연성을 제공하기 위해 분산 코어 네트워크 구조와 소프트웨어기반 아키텍처(SDN·NFV, MEC, 클라우드 컴퓨팅 등)로의 기술적 변화는 새로운 공격 접근 경로와 네트워크 슬라이싱과 같은 논리적인 계층의 복잡한 보안 가시성 이슈 등 사이버보안관점에서 새로운 도전(Challenges)이 되고 있다. 본 논문에서는 5G 모바일 네트워크의 기술적 변화에 따른 보안도전과제와 해외 5G 보안 아키텍처 연구들을 분석하여 5G 보안 설계 및 운영 고려사항을 고찰하고자 한다.

Ⅰ. 서 론

5G 모바일 네트워크 기술은 3GPP(The 3rd Generation Partnership Project) 표준화기구에서 제정된 5세대 무선통신 표준기술로서 ITU에서 정의하는 정식명칭은 IMT-2020이다.

3GPP는 모바일 트래픽 양 증가, 사물 디바이스 수 증가에 대응하기 위해 2010년부터 5G 기술 표준화를 추진하였고,[그림]과 같이 표준화 로드맵 상 2018년 8월 1차 표준화(Release 15)가 완료되어 4G 기술과 일부 5G 기술이 적용된 eMBB 서비스 중심의 NSA(Non Standalone, 단말기와 기지국은 5G 기술, 코어 네트워크는 4G 코어망 연결) 구조 방식의 상용서비스가 개시되었고, uRLLC와 mMTC 서비스를 반영하기 위한 SA(Standalone) 구조 방식의 2차 표준화(Release 16)는 2020년 상반기 표준 제정을 목표로 진행 중에 있다[1].

이동통신 기술 진화 관점에서 살펴보면 4세대 이동통신까지는 스마트폰을 중심으로 무선 전송 속도와 대용량 성능 향상에 초점을 두어 발전해왔다[2]. 5세대 이동통신 기술은 AI, 자율주행차 등 초연결 사회 구현을 위해 다양한 IoT 기기의 특성과 서비스 요구사항을 수용할 수 있는 모바일 네트워크 환경을 구축하기 위해 다양한 IT 신기술을 고려한 기술적 진보가 진행되어왔다[3]. 즉, 데이터 송·수신 용량과 속도 관점에서 유·무선 간 차이가 없을 정도의 빨라진 “이동 통신 환경”을 제공하여 스마트폰뿐만 아니라 AR, VR, 드론 등 새로운 기기를 통해 4K·8K 및 AR/VR 등 실감형 멀티미디어 콘텐츠들을 제공하고, IoT 기기 사용에 있어 저전력성 및 많은 기기들이 접속하는 환경에서도 서비스의 안정성을



〔그림 1〕 3GPP 5G 표준화 로드맵, NSA vs SA 구조

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019- 0-00793, 국가기간망 사이버공격 사전예방을 위한 지능형 5G 코어망 비정상 공격 탐지 및 대응 기술개발)
* 한국인터넷진흥원 지능형사이버방어R&D팀(rinyfeel@kisa.or.kr; bmchoi@kisa.or.kr; keh@kisa.or.kr; smpark@kisa.or.kr)

〔표 1〕 ITU-R 5G 서비스 주요 특징 및 비교〔3〕

특성	설명	유스케이스	4G	5G	비고
초고속 대용량 통신 (eMBB)	최대 20Gpbs 및 일상적으로 100Mbps 속도가 가능한 '고속성(High Speed)', 1만 배 이상 더 많은 트래픽을 수용 '대용량(High Capacity)	4K,8K, 홀로그램, AR/VR 등	최대전송속도		20배
			1Gbps	20Gbps	
고신뢰 초저지연 통신 (uRLLC)	1ms 이하 "낮은 지연시간(Low Latency)", 이동 간 제로 중단을 실현하는 "높은 안정성(High Reliability)"	자율주행차, 공장자동화,원격 의료 등	전송지연		1/10
			10ms (0.01초)	1ms (0.001초)	
대량연결통신 (mMTC)	$1km^2$ 당 100만 개 기기수용 '고밀집(High Density)', 1개 배터리 10년간 구동 가능한 '고에너지 효율 (High Energy Efficiency)'	스마트시티,스마트빌딩, 물류 등	$1km^2$ 당 기기 연결 수		10배
			10만개	100만개	

보장하는 "IoT 통신 환경"이 본격적으로 구현할 수 있다[3]. ITU-R에서는 5G 이동통신 기술의 3대 서비스로 [표 1]과 같이 속도, 대역폭, 지연시간 등 각 서비스 요구사항에 따라 초고속 및 대용량(eMBB), 고신뢰 및 초저지연(uRLLC), 대량연결통신(mMTC) 세 가지로 구분하고 있다.

[표 2]는 5G 네트워크의 기술적 특성을 구간 도메인별(사용자장치, 무선엑세스 네트워크, 코어 네트워크, 외부연동 어플리케이션)로 구분하여 정리하였다. 주요 특징은 5G 서비스의 성능목표를 달성하고 B2B 비즈니스 환경에 따라 유연하고 확장 가능한 모바일 네트워크를 제공하기 위해 ICT 최신기술을 수용하여 클라우드 기반 가상화 기술, 네트워크 슬라이싱, MEC 지원, 서비스기반 인터페이스 등 소프트웨어기반 아키텍처를 채택하였다[3-6].

본 논문에서는 사이버보안관점에서 5G 네트워크 및 서비스의 기술적 특성에 따른 보안 이슈와 대응기술의 요구사항을 알아보고자 한다. II장에서는 5G 네트워크

〔표 2〕 5G 기술적 특성 및 진화 방향(NIA〔3〕, ETRI〔4〕, 넷마니아즈〔5〕, 삼성 리서치〔6〕 자료를 인용하여 재구성함)

구성요소		현재 4G 기술	5G 기술 진화 (SA 구조 기준)	특징
UE(사용자 장치)		스마트폰, 테블릿 등 개인용 기기 (음성, 문자, 영상, 인터넷 등)	B2B 비즈니스용 IoT 수용 (스마트폰, AR·VR, 드론, IoT 센서 등)	5G 연결 기기 확대
무선 액세스 네트워크	접속 방식	단일 무선 RAT Access (2G, 3G, 4G 별도 구조)	다중 액세스(Multi-RAT access) (Wifi 등 Non-3GPP access 수용)	다양한 유·무선 액세스 기술을 동일한 인터페이스 (One-connectivity)로 통합 제어
	기지국	매크로셀, 펨토셀 등	초고밀도 소형 셀 구축 증가	
	구현 기술	Centralized RAN	Cloud RAN 구조 (기능 분할, 가상화 기술 사용)	
코어 네트워크	물리적 배치	중앙 집중형 단일 코어망(EPC)	분산 클라우드 기반 코어 네트워크 (코어 기능의 지역적 분산화)	분산 에지 클라우드 및 네트워크 슬라이싱 서비스 제공과 MEC 지원이 용이하도록 소프트웨어 기반 구조(SDI)를 채택하여 유연한 코어 네트워킹 기능을 제공하고 3rd Party NF 연동과 어플리케이션을 개방
	전송망	물리적 공유, 단일 네트워크 제공	종단간 네트워크 슬라이싱 (논리적 망 분리)	
	장비형태	물리적 장비 (PNF) 중심 (Physical Network Function)	가상화 NF (SDN/NFV 기술 적용) (Visualization Network Function)	
	인터페이스	Peer-to-Peer I/F Architecture (multiple 인터페이스)	SOA(Service-based I/F Architecture (HTTP2/RESTful)	
	제어신호	CUPS (UP 기능과 CP기능의 분리)	SDN/NFV 기반 CUPS 가속화 (UPF 기능 분산 및 에지 재배치)	
	기능 모듈화	네트워크 컴퓨팅 기능과 데이터 저장 기능이 한군데 처리	무상태(Stateless) 네트워크 기능 (네트워크 기능과 데이터 저장소 분리)	
외부 연동 및 어플리케이션		통신사의 코어망과 외부 GW(SGi 등)를 거쳐 연결	MEC (내부 에지 네트워크 전진 배치)	API 개방화

기술 진화에 따른 보안위협을 살펴보고, III장에서는 3GPP 보안 표준, 5PPP(Public-Private Partnership Programme), 에릭슨, 화웨이 등 해외 5G 보안 아키텍처 연구 동향을 중심으로 5G 네트워크의 보안 요구사항을 분석하여 설명한다. 마지막IV장에서 결론을 제시한다.

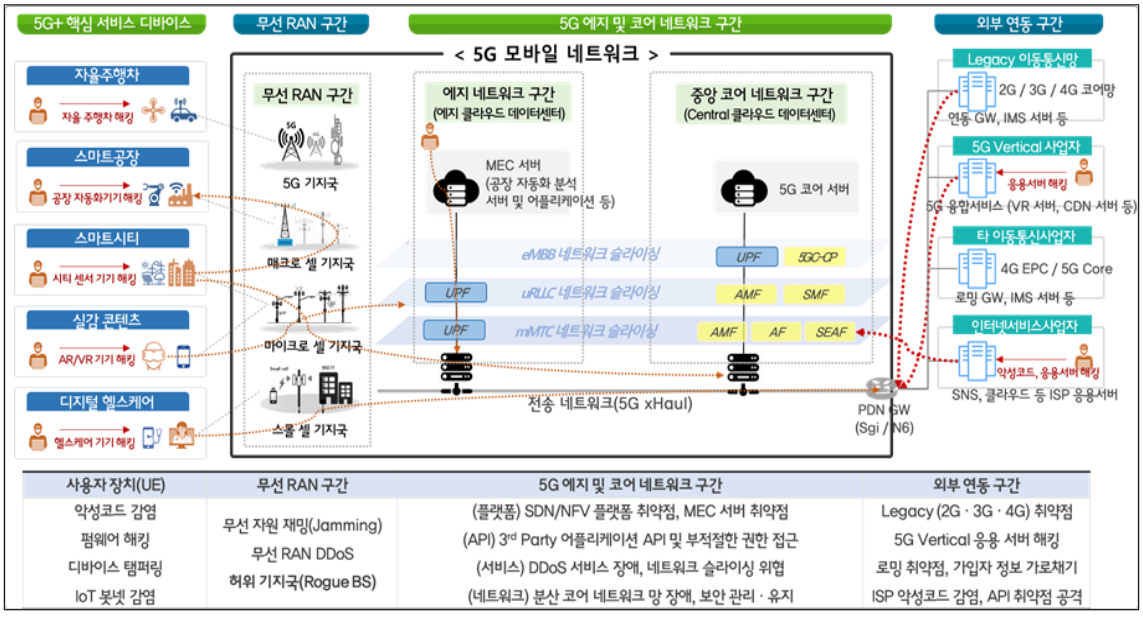
Ⅱ. 5G 기술 특성과 진화에 따른 보안도전과제

앞장에서 살펴본 바와 같이 5G 이동통신기술 이전 세대대비 기술적으로 진일보한 장점을 가진 반면,이 사이버보안관점에서 잠재적 보안위협과 새로운 도전과제를 준다. [그림 2]는 5G 모바일 네트워크를 중심으로 연결되는 각 구간별 대표적 보안위협을 요약하여 도식화 하였다[7]. 일반적으로 모바일 트래픽 경로는 사용자 단말(UE: User Equipment)부터 무선 액세스 네트워크(RAN : Radio Access Network, 기지국)와 코어 네트워크(이동성 관리, 인증, 과금 등을 위한 모바일 네트워킹 기능)를 거쳐 IP 서비스망(인터넷 서비스 사업자, 국가 간 로밍 연동 등)의 응용 서버와 연결된다.

이때 5G 네트워크에 2G, 3G, 4G Legacy 이동통신망과는 인터넷 서비스망(SNS, 클라우드 서버 등)과의 연결뿐만 아니라 타 수직 산업 군(제조, 의료 등)의 네트워크와 IoT 기기들이 상호 연결되는 초연결 네트워크의 복잡성이 증가할 것으로 예상되기 때문에 사이버보안의 위험도 기하급수적으로 증가할 것으로 예상된다. 즉, 5G 네트워크에 연결되는 다양한 기기, 네트워크, 서비스 등이 갖는 다른 보안 요구사항과 수준이 다른 보안 기술들로 인해 취약한 연결 고리가 발생하거나 security downgrading 등으로 인해 5G 네트워크의 전체적인 보안성을 저하 시킬 수 있다는 점이 가장 큰 도전과제가 될 수 있다. 다음 절은 [표 3]에서 요약한 5G

(표 3) 5G 기술적 특성 대비 6가지 보안 과제

단계	5G 네트워크 장점	보안도전과제
사용자장치	IoT 장치 수용	보안 취약한 IoT 장치
무선 RAN	이기종 무선 접속,과 커버러지 확대	무선 RAN 장애, 초소형 스몰셀 보안관리
분산 코어 네트워크	분산화로 모바일 트래피 부하 분산	보호대상 증가/분산과 보안 가시성, Legacy 네트워크·장비와 연동
가상화 및 슬라이싱	물리적 자원의 효율성, 확장성, 가용성	공유 자원 부하와 접근제어 등
MEC 도입	수직산업의 초저지연 서비스의 실시간 제공	3rd APP 신뢰성 및 내부통신망 연결경로
서비스기반 아키텍처	인터넷프로토콜 확대 및 API 개방성	알려진 웹 취약성 상속, 오픈 API 신뢰성



〔그림 2〕 5G 네트워크와 5G+ 융합서비스 연결에 따른 구간별 보안 위협 개요

기술특성과 관련하여 6개 보안 도전과제(Security Challenges)을 상세히 정리하여 설명한다.

2.1. IoT 디바이스 및 DDoS 공격 보안이슈

5G 네트워크는 4G LTE 대비 20배가 빠른 대용량 트래픽을 처리하고 10배의 IoT 장치가 연결될 수 있도록(단위면적당 100만개) 설계 되었다. 5G 네트워크에 연결되는 IoT 기기의 폭발적인 증가는 취약한 IoT 기기가 DDoS 트래픽을 발생시킬 경우 5G 네트워크에 직접적 영향을 주는 위험요소가 될 수 있다. 최근 유럽 ENISA Threat Landscape Report 2018 보고서[8]에 따르면 DDoS 공격 규모와 강도는 대형화 추세이며, 2016년 미라이 악성코드 감염된 IoT 기기가 DDoS 공격을 일으킨 최초 사례가 발생하고, 2018년 GitHub(1.35Tbps) 대상 초당 1 테라급 DDoS 공격이 발생하였으며 최대 1.7 테라급으로 점차 DDoS 강도가 커지고 있다.

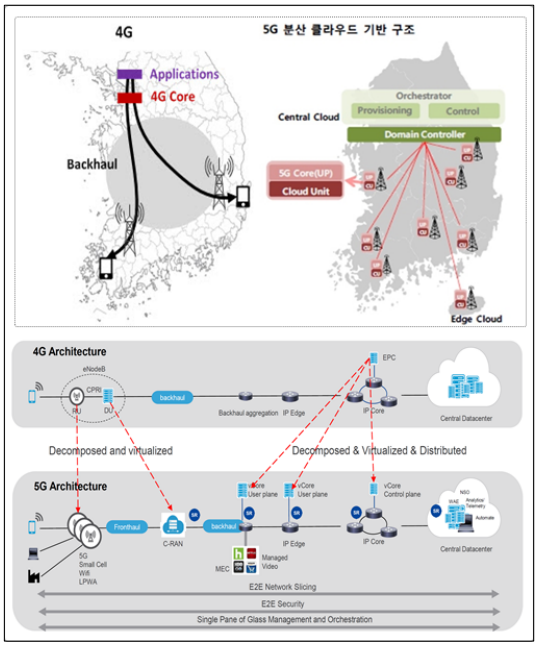
IoT 장치의 보안 이슈는 스마트폰과는 달리 산업 군 서비스별 기기 유형(스마트공장 기기, 스마트시티 센서, CCTV 등)과 탑재 어플리케이션, 공급망 생태계가 다양하기 때문에 공통된 보안 표준이나 아키텍처 설계가 쉽지 않다. 또한 저사양 IoT 기기의 경우 고수준의 보안 기능을 탑재하기 어려워 취약한 패스워드 및 오래된 보안 취약점을 내포한 채 방치되거나 디바이스 템퍼링에 의한 변조에 취약하고 악성 어플리케이션에 의한 부적절한 접근 또는 중간자공격으로 인한 가입자 정보(IMSI) 정보유출 등의 보안위협에 취약한 환경에 노출될 가능성이 상대적으로 높다.

사이버 공격자는 이러한 보안이 취약한 IoT 기기를 공격대상으로 수많은 IoT 기기를 “원격 재부팅” 악성코드에 감염시켜 IoT 봇넷을 구성하여 C&C 서버를 통한 원격제어를 수행하여 IoT 기기를 공격수단으로 활용할 수 있다[7]. IoT DDoS의 주요 공격 대상은 1) 5G 네트워크 인프라(RAN, 코어장비, 네트워크 슬라이스, 물리적 공유되는 플랫폼의 메모리 등), 2) 5G 네트워크 인프라를 경유하여 연결되는 인터넷 서비스의 응용서버, 3) 5G에 연결된 디바이스가 될 수 있으며, 이때 상호 연결된 네트워크 인프라 리소스가 고갈되어 대규모 서비스 장애가 발생 될 수 있다[9].

2.2. 5G 무선 RAN 구간의 보안이슈

무선 RAN 구간은 사용자 단말기와 기지국 간의 무선통신 인터페이스(Air Interface)와 기지국과 5G 코어 장비들을 유선 전송 네트워크(Backhaul)를 통해 연결해 주는 다양한 형태의 기지국 장비(매크로셀 기지국, 마이크로셀 기지국, 초소형 기지국 등)로 구성된다. 5G 무선 RAN 기술은 3GPP 무선액세스 기술(2G, 3G, 4G 등) 뿐만 와이파이, 유선인터넷 등 Non 3GPP 액세스 기술을 수용하여 여러 유형의 무선 접속기술들이 5G 네트워크에 접속할 수 있도록 허용하였다는 장점을 가지고 있다[4].반면 다양한 이종 무선접속과 대량 IoT 기기의 접속을 허용함으로써 무선 RAN 구간의 보호가 중요해졌다. 이동통신 서비스 연결을 위해서는 사용자 장치와 무선 RAN 구간의 기지국(eNB, gNB) 장비와 코어망의 통신장비(MME) 간 제어 신호(이동, 인증, 과금 등)를 교환하게 되는데, 이때 무선 RAN 기지국에 연결되는 수백만의 사용자 장치로 인한 비정상 제어 트래픽이 송수신할 경우 장애에 대한 복원력 이슈와 접근이 용이한 가정용·기업용 스몰셀에 대한 보안 강화가 중요하다.

주요 보안위협[9]은 첫째, 악성코드에 감염된 대량의

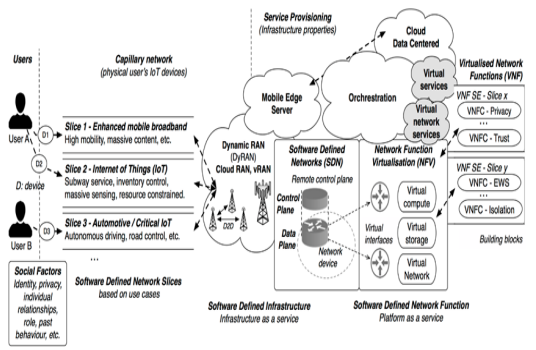


〔그림 3〕 (상) 5G 네트워크의 지역적 분산화(KT 융합기술원), (하) 5G 코어기능의 재배치(시스코, 2018)

IoT 봇넷에 의한 무선 자원에 과도한 접속을 요청하는 무선 RAN DDoS 공격과 무선 신호 채널에 대한 재밍(Jamming) 공격이다. 무선 RAN DDoS와 전파 방해 재밍 공격에 의해 기지국들이 비정상 데이터를 송수신함으로써 RAN 구간의 무선 인터페이스 자원을 고갈시켜 정상적인 데이터 수신을 방해하는 가용성 이슈가 발생될 수 있다. 둘째, 허위 기지국(Rogue Base Station) 이슈로서, 공격자는 허위 기지국을 이용하여 모바일 사용자 장치(UE)와 5G 네트워크 사이에서 중간자 공격을 통해 모바일 사용자와 네트워크 사이에서 사용자 위치 정보 탈취, 전송 정보의 변조, 디도스 공격 등 다양한 공격을 수행할 수 있다. 하위 기지국 이슈는 4G 및 기존 네트워크에서도 지속적으로 제기되어 5G 보안 표준에서 다양한 개선사항이 적용되었음에도 불구하고, 초고밀도 소형셀 구축이 확산될 경우, 보안관리가 취약한 소형셀을 겨냥한 해커들의 해킹으로 통제권이 상실된 상태의 허위 기지국 이슈가 여전히 제기될 수 있다.

2.3. 분산 5G 코어 아키텍처 보안이슈

5G 코어 네트워크의 큰 변화는 4G 코어 네트워크(4G EPC)까지는 중앙국사로 트래픽이 집중되는 중앙집중형 네트워크 구조였으나, 5G 네트워크에서는 통신기능을 지역적으로 재배치하기 위해 코어네트워크와 에지 네트워크를 분리하여 분산화 하였다. 제어 트래픽(Control Plane)과 사용자 데이터(User Plane) 트래픽의 경로가 물리적으로 분리되어 중앙국사에서는 제어 트래픽을 주로 처리하고 사용자 데이터 처리는 지역 국사에 클라우드 기반 에지 통신센터에서 처리 하게 되었다. 이러한 분산 코어 네트워크 구조는 초저지연 서비스, 네트워크 슬라이싱 서비스 제공에는 효율적으로 제공되는 구조이나, 보호대상이 광범위하게 지역적으로 분산화 되기 때문에 보안 가시성 및 보호 수준이 다른 Legacy 네트워크(2G, 3G, 4G 네트워크) 및 장비와 네트워크와의 연결은 공격 대응 관점에서 새로운 도전과제가 될 수 있다.



〔그림 4〕 소프트웨어기반 5G 아키텍처〔11〕

2.4. 가상화 및 네트워크 슬라이싱 보안이슈

5G 네트워크는 하드웨어 종속적인 인프라에서 (그림 4)와 같이 소프트웨어 기반 인프라로 전환이 가속화 되고 있다[4]. 소프트웨어기반 5G 인프라는 5G 통신서버와 네트워크 장비 그리고 네트워크 슬라이싱 서비스를 SDN·NFV 가상화 기술을 통해 실현된다. 즉 하나의 물리적 네트워크를 다수의 가상 네트워크로 분리하여 uRLLC, mMTC, eMBB 응용 서비스별 독립적인 네트워크 슬라이싱 서비스를 제공하고 전용장비 대신 범용 서버 상에 네트워크 통신기능을 가상화 SW (Virtual Machine) 형태로 구현한다. 그러나 5G 장비 및 서비스 구현의 핵심인 가상화 기술은 물리적 네트워크 및 HW 서버 자원(CPU, 메모리 등)을 공유하여 자원의 효율성, 유연성과 가용성 측면에서 장점을 가지고 있으나, 물리적 공유된 HW 자원에 대한 부하공격, 공유자원의 무단 엑세스 및 악성 코드 공격의 전파, 네트워크 슬라이싱 및 공유자원 간 접근제어, 장비 구성설정 결함 및 오류에 상대적으로 취약할 수 있다[7][9][10][11].

첫째, SDN·NFV 보안 이슈로서, SDN 기술은 네트워크 제어 기능(SDN 컨트롤러)과 트래픽 전달(SDN 스위치) 기능을 분리하여 하드웨어적으로 처리되던 네트워크 전달 기능을 소프트웨어로 제어하고 통제하기 위한 기술이다[5]. SDN 컨트롤러와 스위치 간 제어 인터페이스의 프로토콜 및 구성 취약점을 악용하여 트래픽 우회시켜 무결성과 기밀성에 대한 공격, 스위치와 컨트롤러 무단 제어, 자원 고갈 DoS 공격으로 인해 SDN으로 구성된 시스템들을 취약하게 할 수 있다. 예를 들어 SDN 컨트롤러를 공격하여 SDN 스위치 플로우 테이블을 소진시키는 포화 공격이 발생될 수 있다. 또한, 범용 서버 상에 구현되는 NFV 기술은 하이퍼바이저 커널 보안, 악성 가상머신(VM) 마이그레이션 이슈, 가상화된 NF 상에 동작하는 응용 프로그램 간의 신뢰관계, 즉 응용 프로그램의 변경 또는 인증과 네트워킹 기능에 대한

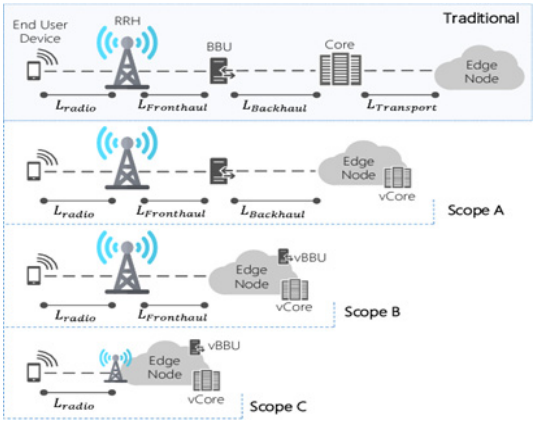
권한 부여 이슈가 중요하다. 응용 프로그램의 인증 및 권한 부여에 대한 보호 메커니즘이 없다면 3rd Party의 악성 응용 프로그램이 SDN 컨트롤러로부터 네트워크 정보를 얻을 수 있다[16][18].

둘째, 네트워크 슬라이싱 보안 이슈로서, 네트워크 슬라이스는 eMBB, uRLLC, mMTC 서비스유형 별 다른 애플리케이션 또는 테넌트를 위해 물리적 동일 네트워크를 논리적으로 분리할 수 있다. 이때 네트워크 슬라이싱을 적절히 격리하지 않으면 공격자가 하나의 슬라이스에서 다른 슬라이스로 공격을 수행 할 가능성이 있다. 예를 들어, 공격자는 특정 서비스 전용의 네트워크 슬라이스에 악의적으로 트래픽 용량을 초과 시켜 다른 네트워크 슬라이스에 영향을 주거나 특정 어플리케이션을 동시에 활성화 시켜 네트워크 슬라이싱 자원고갈 공격을 수행 할 수 있다. 또한 네트워크 슬라이스에 적절한 암호화가 적용되어 있지 않다면 공격자는 다른 슬라이스에 속한 데이터를 도청하거나 변조 할 수 있다.

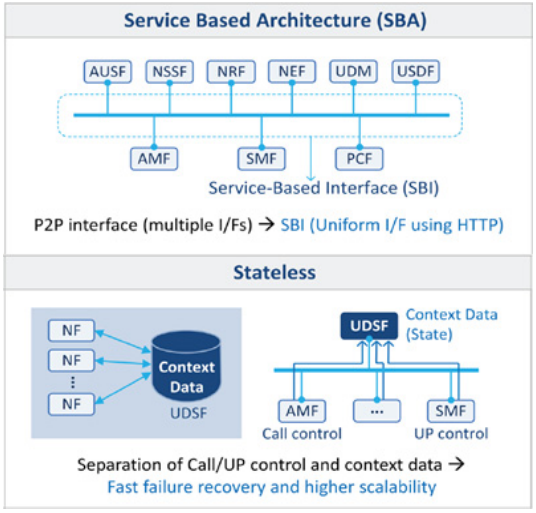
2.5. 다중 액세스 에지 컴퓨팅(MEC) 보안 이슈

다중 액세스 에지 컴퓨팅(Multi access Edge Computing)은 사용자 기기와 가까운 네트워크에서 컴퓨팅을 지원하는 개념을 말하며, 데이터가 수집되는 에지 네트워크에서 데이터를 분석 할 수 있는 장점이 있어 초저지연 서비스를 제공할 수 있다. 특히, 5G 네트워크와 에지 컴퓨팅 개념이 결합됨으로써 [그림5]와 같이 5G 에지 노드(네트워크)에 컴퓨팅 서버를 전진배치 시켜 원격의료, 자율주행차, 공장자동화, IoT 센서 데이터 정보 처리 등 IoT 어플리케이션 및 서비스를 지연 없이 실시간 제공에 장점을 가지고 있다. 반면 에지 컴퓨팅 서버가 5G 에지 네크워크 내부로 전진 배치되거나 새로운 연결 경로가 생기게 됨으로써 발생하는 보안 이슈를 새로운 도전과제가 된다.

특히, MEC 컴퓨팅은 모바일 통신 사업자의 5G 에지 네트워크 내부의 사용자 평면 기능(UPF)과 연결되기 때문에 새로운 연결경로가 생기게 된다. 여기서, MEC 시스템은 클라우드 및 가상화 기술을 통해 구현되고 3rd Party 응용 프로그램 탑재하는 개방형 에코 시스템에서 상호 운영되기 때문에 MEC의 개방성, 이질성과 다양성은 전체 MEC 시스템의 주요 위협이 될 수 있다[10]. 예를 들면, MEC 플랫폼이 가상화 플랫폼으로 구축되어 일부 VNF(Virtual Network Functions)와 동일한 플랫폼에서 MEC 응용 프로그램이 실행될 수 있다. 이때 MEC 응용 프로그램이 모바일 통신 사업자가 통제하기 어려운 3rd Party 응용 프로그램 일 경우, 가상화 네트워크 리소스 자원을 소모하거나 부적절한 API 권한으로 승인되지 않은 민감 정보에 액세스 할 수 있다는 우려가 있다. 또한 공격자는 악의적인 응용 프로그램을 삽입하여 분산된 5G 네트워크 내부 장비인 UPF 등 에지 네트워크 기능에 공격을 시도할 수 있는 새로운 공격 경로를 제공 할 위험이 있다. 즉, MEC와 5G 에지 네트워크 간 경계에서 가상화 된 기능으로 민감한 보안 자산이 손상되면 공격자는 악의적으로 재사용하여 연결을 얻거나 스푸핑, 도청 또는 데이터 조작



(그림 5) 5G에서 MEC 적용 구조[24]



(그림 6) 5G 코어 및 Service based 인터페이스[6]

공격을 수행 할 수 있다[12].

2.6. 서비스기반 아키텍처(SBI) 보안 이슈

5G 코어네트워크는 [그림6]과 같이 서비스기반구조를 지향하고 있다. 즉 4세대 이동통신까지는 B2C 서비스 중심이기 때문에 내부 통신기능과 서비스의 관리, 어플리케이션 개발이 통신사 관리 통제 하에서 주로 이루어지고, 통신 장비 간 연동은 P2P 인터페이스를 통해 가능하였다. 반면 5G는 B2B 서비스를 지향하고 유연한 인터페이스를 제공하기 위해 코어 통신 기능 간의 연동은 HTTP 기반 인터페이스로 통일하고, 내부 통신 기능과 서비스 기능을 IoT, 공장자동화 등 수직산업군의 서비스 제공자(Vertical Service Provider)에게 개방하여 내부 서비스 기능과 데이터 접속을 용이하도록 API 개방화가 가속화 될 것이다.

잘 알려진 인터넷 프로토콜 사용과 API 개방화는 이동통신 프로토콜들이 잘 알려지지 않은 폐쇄 된 특성으로 사이버 공격자들에게 진입 장벽 역할을 했지만 반대로 HTTP와 같은 인터넷 기술은 공격자에게 잘 알려져 있고, 웹 응용서비스가 여전히 많은 보안 취약점을 가지고 있기에 공격자들이 선호하는 공격기법으로 악용 될 수 있다는 점이다. 또한, SCEF, NEF 와 같은 API 기능을 외부에 제공함으로써 새로운 API 보안이슈가 도전과제가 될 수 있다. 즉, 기존 잘 알려진 웹 응용 프로그램의 취약점 관리와 개방형 API에 대한 보안 통제가 중요할 이슈가 될 것으로 보여 진다.

Ⅲ. 해외 5G 보안아키텍처 연구동향 및 보안 고려사항

지금까지 5G 네트워크 기술 변화에 따른 사이버보안 위협 관점에서 도전과제를 살펴보았다. 이번 장에서는 해외 5G 보안 아키텍처 연구동향을 통해 5G 보안이슈를 해결하기 위해 대응기술 측면에서 도전과제(Security Challenges)와 설계 고려사항을 살펴보고자 한다. 현재 5G 보안 아키텍처 연구는 다양한 표준화 기구 및 연구그룹에서 진행되고 있으며, [표 4]는 국내외 4G/5G 보안 연구 내용을 요약하였다. 해외는 2016년부터 3GPP 보안 표준뿐만 아니라 5G PPP(유럽 집행위, 제조사, 통신사, 서비스사업자, 연구기관 참여)의 Security WG에서 5G 보안 아키텍처 연구가 진행 중이다. 이동통신사업자 중심의 NGMN (Next Generation

〔표 4〕 국내외 5G 보안 연구 그룹

연구 그룹		개요	주요 연구 내용
해외	3GPP	Service and System Aspects Security Group (SA3)	보안 아키텍처, RAN 보안인증 메커니즘, 네트워크 슬라싱 보안, 가입자 프라이버시 등
	ITU-T	SG 17 Study Group (‘18년 5G Security 표준화 본격 시작)	데이터 보안, 가상화 보안, 서비스 접근, 데이터 무결성, IoT보안, 인증 등 5G 보안 규격 논의
	5G PPP	EU Horizon 2020 프로젝트 일환 수행 (유럽 공공・민간 파트너쉽, Security WG)	보안 아키텍처, 가입자 프라이버시, 인증 메커니즘 (2018년 5G 보안 백서 발간)
	ETSI	유럽전기 표준협회 (CYBER TC,NFVSEC WG)	NFV 관련된 보안이슈를 주로 다룸 (NFV 보안, 보안 아키텍처, MEC 보안 등)
	NGMN	글로벌 이동통신 사업자(T 모바일, 도이치 텔레콤, 노키아 등) 중심의 차세대 네트워크 모바일 연합	가입자 프라이버시 보호, 슬라이싱 보안, MEC 보안
	ENISA	유럽네트워크정보보호원	LTE, SDN/NFV 등 이동통신망 보안 취약점 연구
	5G Americas	미국 중심 5G기술 연구 그룹 (AT&T,시스코, 노키아, 에릭슨, 퀄컴, 삼성 등)	5G Security 표준 분석, 보안 모델 연구 수행
국내	KAIST	이동통신 보안 취약점 연구	LTE Fuzzer 등 보안 취약점 점검도구 및 다수의 글로벌 수준의 LTE 보안 연구
	KISA	국내 LTE 침해방지기술 원천기술보유 (국내외 특허 등록 30건: 국내 26건, 국제 4건)	과기정통부 정보보호핵심원천기술개발 R&D 사업 “지능형 5G 코어망 비정상 탐지기술개발(‘19-’22)
	윈스	이동통신망 LTE 전용 보안제품 보유	LTE 전용 보안제품(모바일 네트워크 IPS) 보유
	정보보호학회	5G 보안연구회 (순천향대, 국민대, ETRI 등 학계 및 연구소 참여)	5G 네트워크보안이슈 분석, 연구 아이템 발굴 등

Mobile Networks) 5G 워킹그룹에서는 네트워크 슬라이싱, MEC 보안 요구사항을 다루고 있다. ETSI(유럽전기표준협회) NFV SEC (NFV Security) WG에서 NFV 플랫폼의 보안 스펙을 주로 다루고 있다. ITU(SG17)에서 5G 보안에 관한 보안 규격에 대해 본격적으로 논의가 시작되었다[16].

3.1. 5G 보안 아키텍처 설계 시 단계별 고려사항

5G 네트워크, 사용자 트래픽과 서비스를 안전하게 보호하기 위해서는 이전 세대 보안기술과는 차별화된 새로운 보안기술이 설계되고 솔루션이 개발되어 네트워크에 구축되어 운영 되어야 한다. 이를 위해서는 표준화, 장비개발, 네트워크 구축 및 운영의 각 단계별 고려해야할 사항은 [표 5]와 같다[13].

먼저 표준화 단계에서는 국가 간 네트워크 및 시스템의 상호 연동을 위해 통신 프로토콜과 인터페이스가 안전하게 설계가 되어야 한다. 5G 관련된 보안 표준화는 국제표준기구와 사실표준단체에서 5G 기본적 보안 요구사항과 아키텍처에 관한 표준 연구가 활발하게 진행중에 있다. 3GPP 표준에서는 사용자와 네트워크 간에 상호인증을 위한 인증 및 키 관리, 제어 평면(Control Plane)의 시그널링 메시지와 사용자 평면(User Plane)의 데이터 보호를 위한 보안 표준들이 개발되어 모바일 네트워크의 보안성을 지속적으로 강화해 왔다. 그러나 표준화는 최소한 기본적인 보안 요구사항과 스펙만을 정의하기 때문에 표준 프로토콜 상의 취약점이 상시 발생할 수 있다는 우려가 존재한다.

〔표 5〕 단계별 보안 요구사항 및 보안이슈(에릭슨〔13〕 인용하여 재구성)

단계	보안 요구사항	이슈사항
표준화 단계 (Standardization)	국가 간 망의 상호연동을 위해 안전한 통신 프로토콜 설계	표준 프로토콜 취약점 기본적 보안 요구사항·스펙만 정의
장비제조사 개발 단계 (Implementation)	표준에서 요구하는 보안 기준 및 목표 수준에 맞는 장비 개발	장비 구현 취약점 공통 기능을 다르게 구현, SW 오류 등
통신 사업자 구축 단계 (Deployment)	안전한 네트워크 및 서비스 설계와 구축	망 구축 취약점 구성 설정 오류, 오픈소스, 3rd Party SW
서비스 운영 단계 (Operation)	사이버공격에 대한 탐지 및 모니터링, 사고대응 대응 관리	운영 취약점 취약점 대응, 공급망 보안제어 및 보증

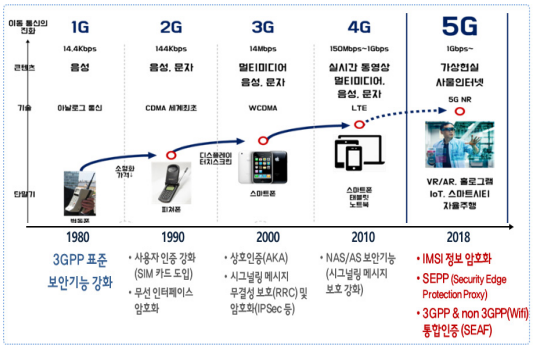
둘째, 장비 개발 제조사들은 표준에서 요구하는 보안 기준과 목표 수준에 맞는 장비를 개발해야 한다. 예를 들어, 각 장비 제조사별로 보안 기능이 다르게 구현되거나 SW로 구현된 장비들이 SW 오류를 내포하거나 장비를 구현 당시 알려지지 않았던 보안 취약점(Unknown Vulnerabilities)이 시간이 지나 지속적으로 발견되는 장비 구현 상 보안 취약점 이슈가 지속적으로 발생한다.

셋째, 통신 사업자는 장비 제조사들의 통신장비와 서비스 어플리케이션들이 보안요구사항에 맞게 구현되었는지 공급망 제품을 검증하여 안전한 네트워크와 서비스를 설계하고 구축해야 한다. 그럼에도 불구하고 네트워크와 서비스를 구축하는 과정에서 구성설정 오류가 존재할 수 있고, 통신 사업자가 아닌 3rd 어플리케이션 등의 보안 이슈는 지속적으로 제기되고 있다.

마지막 서비스 운영 단계에서는 고도화되고 지능화된 사이버공격에 대한 취약점 제거와 침해사고 발생 후 복원력이 중요하다. 또한, 각 단계별 보안 이슈사항을 해결하는데 소요되는 대응조치 시간도 장애요소가 될 수 있으므로, 표준 프로토콜 상의 보안 취약점의 경우 표준에 반영되기까지 수년의 시간이 소요되며, 장비 구현 취약점은 SW 패치부터 안전성 검증까지 약 6개월 이상의 시간이 소요가 되기 때문에 각 단계 간 보안 갭(Security Gap) 줄여나가는 것이 매우 중요하다고 할 수 있다.

3.2. 3GPP 5G 보안 표준화 동향

3GPP 보안 표준은 SA3(Service and System Aspects Security Group)워킹그룹에서 주로 다루고 있으며, [그림 7]과 같이 1세대부터 5세대 이동통신 기술까지 모바일 네트워크 보안이 지속적으로 강화되었다. 2세대 이동통신의 경우 무선 인터페이스 도청 및 메시지 스팸 이슈를 해결하기 위해 무선 인터페이스 암호화 및 SIM 카드가 최초로 도입이 되었고, 3세대 이동통신은 상호인증(AKA) 및 무선자원관리 시그널링 보호기능(RRC 메시지 암호화 등)을 강화해 왔다. 4세대 이동통신은 AS/NAS(Access Stratum/ Non Access Stratum) 보안기능을 통해 시그널링 메시지보안이 지속



〔그림 7〕 3GPP 이동통신 보안 표준화 강화(IT 동아, 5G 통신의 현재와 미래〔2〕 그림을 인용하여 재구성)

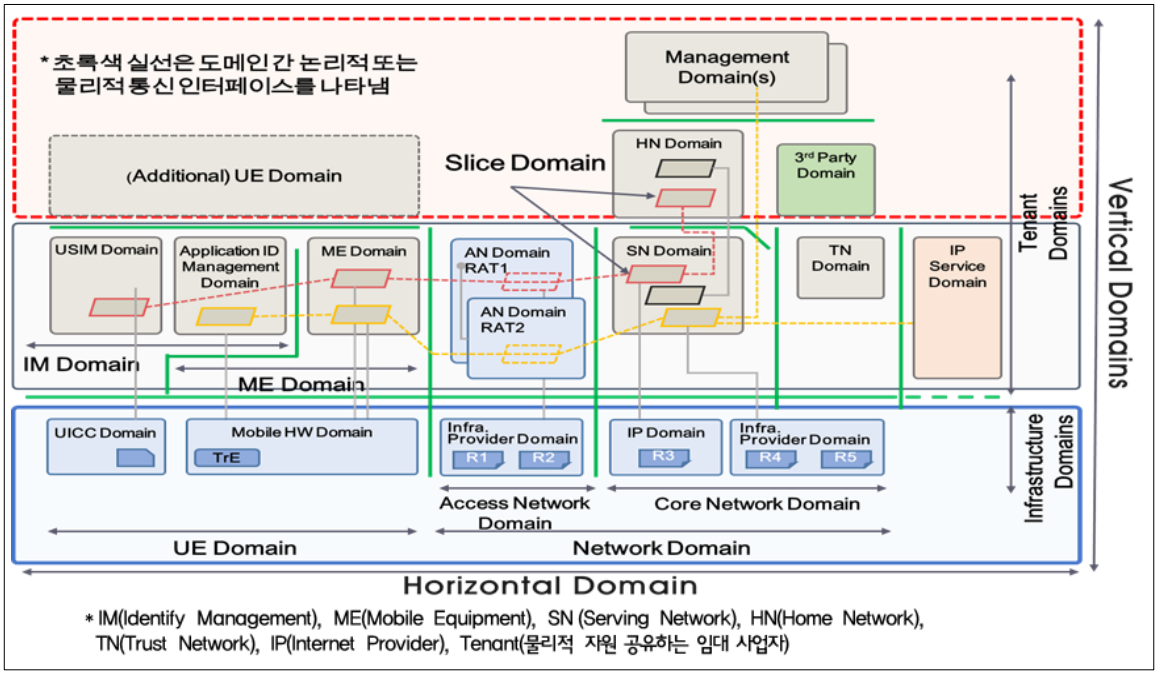
적 강화되었다[14][21][22].

5G 보안 표준은 2016년부터 보안 아키텍처, 인증, 네트워크 슬라이싱 보안, 가입자 정보보호 표준에 대한 논의가 시작되었고, 2018년 8월 5G Release 15에서 보안표준이(TS 33.501) 발표되었다[15]. Release 15 보안 표준에 포함된 주요 보안 기능은 가입자 정보(SIM카드 저장된 IMSI 사용자 식별자 등) 보호를 위해 IMSI(International Mobile Subscriber Identity) 정보 암호화 기능, 로밍 도메인 간 보안이슈였던 SS7(Signaling System No.7) 이슈를 해결하고 서로 다른 통신 사업자(Public Land Mobile Network) 간 어플리케이션 계층의 보안을 구현하기 위한 SEPP(Security Edge Protection Proxy) 기능, 3GPP 액세스와 Non-3GPP 액세스에 동일한 인증방법을 사용할 수 있는 통합인증프레임워크가 도입되었다. SEAF를 사용하면 장치가 서로 다른 액세스 네트워크 간에 이동하거나 서로 다른 서비스 네트워크 사이에서 이동하는 경우에도 전체 인증 방법(예: AKA 인증)을 실행하지 않고 재인증될 수 있다[9].

3.3. 해외 5G 보안 아키텍처 동향 및 고려사항

5G 네트워크와 서비스가 소프트웨어화와 가상화 기술을 통해 분산되고 유연한 아키텍처 특성을 기반으로 새로운 서비스와 기능의 손쉬운 배치가 가능하게 되는 장점을 가지고 있지만, 이는 5G 보안 환경을 더욱 복잡하게 만들기 때문에 현재의 보안 접근 방식으로는 해결하기 어려운 도전과제가 되고 있다. 이에 해외에서는 5G 네트워크 및 서비스에 적합한 보안아키텍처 연구가 진행되고 있다.

2018년 영국 DCMS(디지털 미디어부)는 5G 기술선



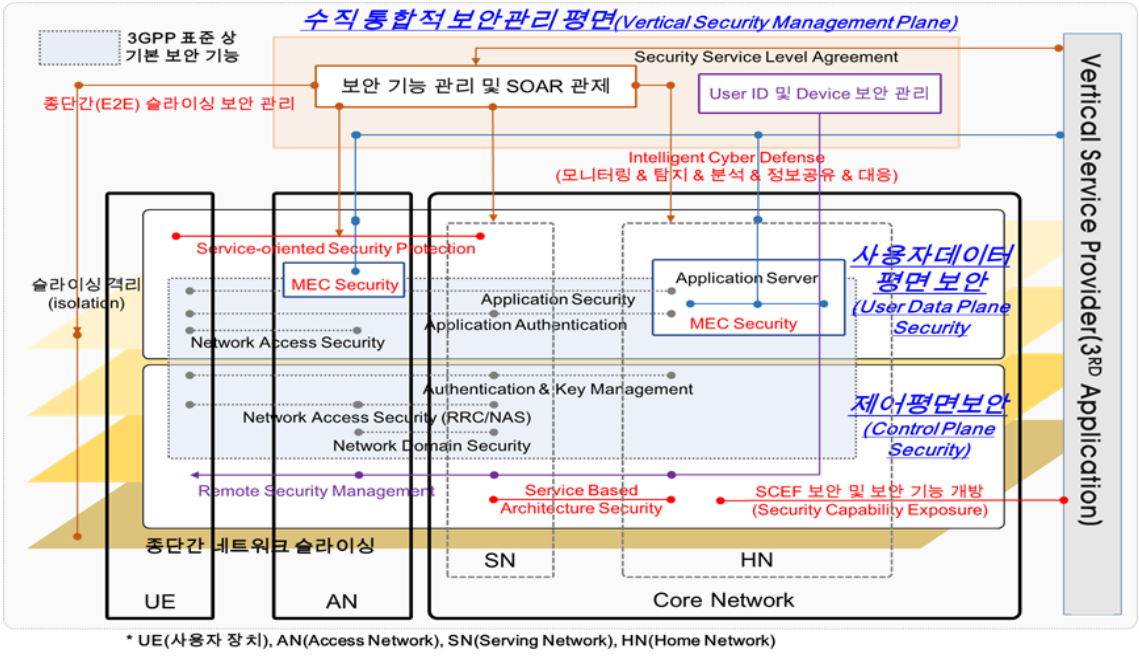
〔그림 8〕 5G PPP 보안 아키넥처 모델〔17〕〔18〕

도전략을 통해 5G 보안 아키텍처와 보안 요구사항에 관한 연구결과를 발표하였다. 주요 내용으로 5G 환경은 이전 이동통신 환경보다 다양한 유형의 네트워크, 장치가 연결되어 버티컬 산업 서비스를 제공하기 때문에 네트워크, 시스템 및 서비스의 보안은 점차 어려워지고 있음을 강조하였고, 안전한 5G 아키텍처 구현과 설계를 위해 4개 고려사항으로 종단 간 보안, 계층 간 보안, 멀티 도메인 간 보안, 보안 내재화를 제시하였다[12].

첫째, 종단 간 보안(End to end security or Horizontal Security)이다. 기존 4G 모바일 네트워크와 마찬가지로 사용자 장치부터 무선 액세스 및 전송 네트워크를 포함하여 코어 네트워크의 종료 지점까지 수평적 통신 경로 상에서 End-to-End 보안을 기본적으로 보장되어야 한다. 5G 네트워크는 이기종 무선접속 방식, 통신 사업자 간 네트워크 (Home Network, Serving Network 등) 장비들이 상호 연결되기 때문에 E2E 보안 설계와 구현이 쉽지 않는 이슈가 존재한다. 예를 들면 표준에서 요구하는 제어 신호(Control Plane)의 기밀성 보장(예, IPSec 적용 등)이 통신 경로 상에 유지되어야 하지만 타 통신 사업자 도메인 간의 연결 과정에서 비보안 연결 구간이 발생하는 지에 검토가 필요하고 어플리케이션 계층에서 E2E 보안 등 다양한 접근방법을 고려하는 것이 중요하다[23].

둘째, 계층 간 보안(Cross-layer Security or Vertical Security)이다. 5G는 분산되고 유연한 특성으로 인해 도메인 경계를 중심으로 하는 보안과 종단 간 보안만으로는 해결하기 어렵다. 예를 들어 5G 네트워크는 물리적인 공유 인프라 상위에서 SDN기반 가상화 네트워크(VNF)를 통해 구현된다. 즉 물리적 HW 장비, 가상화 계층(하이퍼바이저 및 가상머신), 네트워크 슬라이싱, MEC 상의 3rd Party 어플리케이션 계층 같은 수직적 계층(Vertical Layer)으로 구분되고. 경계 중심의 물리적 보안 장비만으로는 다양한 논리적 계층 영역을 모니터링하기 어렵고 각각의 논리적 계층에 적합한 보안 기술이 효과적일 수 있다.

셋째, 멀티 도메인 간 보안(Cross-Domain security)이다. 다양한 도메인 간 상호 운용성은 네트워크, 서비스 및 장비를 포함한 다양한 공급자(사업자) 도메인이 공존함으로써 야기되는 도메인 간 신뢰관계 이슈가 발생 할 수 있다. 예를 들면, 논리적인 네트워크 슬라이싱 기능을 제공하기 위해서는 여러 물리적 도메인(단말, 엑세스 네트워크, 코어 네트워크 등)과 수직적 도메인(장비 제조사, 가상화 솔루션 업체, 3rd 어플리케이션 개발업체 등)에 걸쳐 구현될 수 있고, 이때 각 도메인별



〔그림 9〕 사이버공격 방어 프레임워크(화웨이 5G 보안 모델 그림[19]을 기반으로 재구성함)

로 구축되는 보안 솔루션과 정책을 일정 수준 동일하게 유지하기 위해서는 네트워크 망 사업자, 가상화 솔루션, Vertical Service Provider 등 새로운 공급자 도메인 간의 신뢰할 수 있는 보안 솔루션들 간 상호 연계가 되도록 구현되어야 한다. 각 도메인별 또는 멀티 도메인에 걸쳐 계층 간 보안(Cross-layer Security)가 보장되어야 다른 도메인과 안전하게 작동 할 수 있다.

넷째, 보안 내재화(Security by design)이다. 보안기술은 표준 제정부터 장비 개발과 네트워크 설계 프로세스의 일부로서 초기에 고려되고 배포되어야 한다. 이러한 접근 방식은 시스템이 완전히 구축되어 작동 한 후에는 다루기가 쉽지 않은 잠재적 보안 갭 차이를 최소화 할 수 있다. 특히, SW 개발주기에 대한 빠른 피드백으로 Unknown 취약점 등 잠재적 보안 이슈가 운영 환경까지 피해발생이 확산되는 것을 완화할 수 있는 DevSecOps 적용이 매우 중요하다.

또한 EU Horizon 2020 프로젝트의 일환으로 수행중인 5G PPP “ENSURE(Enablers for Network and System Security and Resilience)” 에서는 5G 보안 아키텍처를 [그림8]과 같이 제시하였으며, 수평적 도메인별 보안뿐만 아니라 각각의 도메인 상에 다양한 수직적 생태계가 고려되어야 하며 이를 위해 수직적 보안(Vertical Domain Security)이 추가적으로 고려되어야 함을 강조하였다[17][18].

예들 들어 사용자 단말 장치(UE) 플랫폼 상에는 HW 제조사의 신뢰보안영역(예, TPM 등), USIM 보안, 응용어플리케이션레벨의 ID 보안, 슬라이스 서비스 보안 등이 수직적으로 존재하여 각기 다른 보안 기능을 일관되게 유지하는 것이 중요하다. 또한 네트워크 도메인(엑세스 및 코어 네트워크)에서 가상화 및 논리적인 슬라이싱 네트워크를 제공해야 하므로 네트워크 도메인 영역에서는 물리적 인프라 도메인(전송망과 물리적 장비)과 Tenant 도메인(가상화 플랫폼 도메인, 3rd Party 도메인 등) 상위에서 논리적 기능과 서비스가 구분되어, Vertical 도메인 간의 보안 메커니즘(상호인증, 엑세스 관리 및 제어, 안전한 시그널링 교환 등)이 작동되어야 한다.

3.4. 운영단계에서 지능형 사이버공격방어 고려사항

이번 절에서는 운영단계에서 지능형 사이버공격대응을 위한 고려사항을 4가지 측면에서 살펴보도록 한다. 에릭슨(22), 시스코(7), 화웨이(9) 등 5G 장비 제조사는 서비스 운영단계에서 보안고려사항을 분산 사이버공격 방어, 유연하고 확장 가능한 보안, 자동화 보안을 공통적으로 제시하고 있다. 예를 들어 [그림9]와 같이 사용자장치(UE) 도메인부터 액세스 네트워크(AN), 코어 네트워크 도메인까지 5G 아키텍처 상에서 논리적인 수직계층(네트워크 슬라이스 서비스와 관련된 Vertical Service Provider)을 포함하여 사각지대 없는 5G 네트워크 및 서비스 기능 보호와 사이버공격 방어 체계를 구축이 필요하다[19].

첫째, 분산 방어(Distributed Security)이다. 모바일 트래픽은 제어 트래픽과 사용자 데이터 트래픽이 분리되어 서로 다른 경로로 여러 도메인을 걸쳐 전송되기 때문에 각 도메인(무선 RAN 구간, 에지 네트워크 구간 등)에서 발생되는 보안위협과 요구하는 보안 수준이 상이하므로 효과적인 사이버 공격 탐지 기능들이 분산되어 배치될 필요가 있다. 예를 들어, 잠재적인 공격 지점에 가까운 위치에서 방어 기능을 배치하고 대응속도를 높이기 위해 Massive IoT DDoS 으로 인한 RAN 과부하 공격 방지는 기지국 또는 에지 네트워크에 공격 탐지 기능을 배치하는 것이 효과적일 수 있다[9].

둘째, 유연하고 확장 가능한 보안(Flexible & Scalable Security)이다. 5G 네트워크 인프라는 물리적인 x86 범용서버를 가상화하여 가상머신상에서 서로 다른 서비스 요구사항에 맞게 통신기능(NFs)들을 동적으로 생성, 확장 제어되고, 3rd Party 서비스 사업자에게 내부 네트워크 기능의 오픈되는 서비스 기반 아키텍처(Service-based Architecture)를 도입하였다[4]. 이때, 각 서비스별 제어평면(Control Plane)과 사용자 데이터 평면(User Plane) 계층별로 3GPP 표준에서 요구하는 기본적 보안기능이 제공되어야 하며, 5G 서비스별 다양하고 복잡한 보안 요구사항을 만족하기 위해 네트워크 슬라이싱 별로 차등화 된 보안 기능의 구성과 호출이 유연하게 적용되어야 한다[22]. 예를 들어 네트워크 슬라이스별로 인증 방법과 암호화를 차등 지원(예, eMBB 서비스는 LTE 유사 수준, 저비용 IoT 센서의 경우 경량 인증, uRLLC 서비스의 경우 빠른 액세스 인증과 강한 암호 기능 제공) 하거나 슬라이스 서비스 별 보안 기능(Service oriented security)을 선택할 수 있어야 한다. 또한, 네트워크 슬라이스 상에서 사이버공격 탐지와 완

화 그리고 슬라이스 간 격리(isolation) 등이 동적으로 모니터링이 되고 통합 관리되어야 한다.

셋째, 자동화된 5G 보안 관리 및 관제(Automated 5G Security) 사이버공격기술은 기존 보안기술을 우회하고 취약한 보안 사각지대를 찾기 위해 점차 정교해지고 자동화되고 있기 때문에 지능형 사이버공격의 대응 속도를 높이기 위해서는 수직 통합적 보안관제의 자동화가 필요하다. 5G 네트워크에서는 멀티 도메인 상에서 논리적 수직적 계층(Cross-layer)에 걸쳐 보안이 다루어지기 때문에 여러 도메인에 걸친 수직 계층 간 보안을 관리하고, 각 논리적 계층의 사이버공격을 모니터링하고 탐지하는 구조가 중요하다. 이때 네트워크 슬라이스별 제공되는 제어평면(Control Signaling) 보안과 사용자 데이터 평면(User Data Plane) 보안과 연계되어 수직적인 계층까지 포괄하는 수직 통합적 사이버 방어 계층이 필요하다. 주요 기능은 각 도메인별 기본적 보안 기능(로그분석 등) 관리뿐만 아니라 다중 도메인에 걸친 네트워크 슬라이싱 보안, 3rd Party 수직적 서비스 사업자에게 개방되는 API 보안, 제로트러스트기반 IoT 기기들의 원격 보안 관리 기능, AI 기술을 활용한 지능형 사이버공격 탐지, 복잡한 보안 가시성 문제를 해결하기 위한 보안 시큐리티 자동 관제 기술(SOAR: Security Orchestration Automation Response) 개념이 포함될 수 있다.

넷째, 제로트러스트기반 보안 모델 적용이다. 제로트러스트 보안 모델(2010, Forrest 리서치)은 글로벌 사이버보안의 최신 화두로서 멀티 클라우드 서비스 연동, 내부자 사이버표적공격 등 내·외부 보호대상의 경계가 허물어지면서 도메인의 경계를 기준으로 보안모델을 설계하는 기존 방식에서 내·외부 구분 없이 접근을 허용하기 전에 시스템, 네트워크에 연결되는 모든 것을 확인하고 검증해야 한다는 신뢰기반의 보안 모델이다. 국내외 발표된 LTE 보안 취약점 이슈들이 결론적으로 경계를 중심으로 신뢰하다고 믿는 도메인(장비, 사용자, API, 메시지 등)로부터 수신되는 악의적인 메시지나 요청들이 검증 없이 또는 한번 인증 후 후속 메시지는 검증하지 않고 허용함으로써 발생되는 다양한 취약성들이 존재하였기 때문에 발생되는 이슈들이 적지 않다. 따라서 다양한 도메인과 논리적 계층 그리고 어플리케이션들이 연결되는 과정에서 검증 후 접속을 허용하고 모든 것에 대한 이상 징후 모니터링을 수행하는 새로운 접근이 필요하다.

Ⅳ. 결 론

지금까지 사이버보안 관점에서 5G 네트워크의 기술적 특성과 진화 방향에 따른 새로운 도전과제를 살펴보았다. 5G 네트워크와 서비스 기술이 다양한 성능 요구사항을 만족하기 위해 최신 IT 기술을 적용하여 효율성, 확장성 등의 장점을 가지게 되었으나, 사이버보안 관점에서 보면 대량의 IoT 장치의 연결성은 사이버공격의 대형화, 분산 소프트웨어기반 코어 아키텍처는 보안 가시성의 복잡성 증가, MEC, 3rd Party 어플리케이션 및 코어 기능의 API 개방화로 인해 새로운 공격 연결 경로와 인터텟 프로토콜 사용으로 인한 기존 보안위협이 상속된 채 운영될 수 있다는 점에서 새로운 도전과제가 되고 있다. 이러한 새로운 도전과제를 해결하기 위해 3GPP, 5G PPP, 5G Americas 등 해외 표준화 기구 및 연구그룹 및 글로벌 장비 제조사들이 5G 보안 강화를 위한 표준화와 5G 보안 아키텍처 연구를 핵심 기술력 확보를 위한 경쟁이 가속화될 것으로 예상된다. 국내에서도 정부, 학계, 산업계에서 5G 보안 기술연구가 금년부터 본격적으로 시작되고 있으나 2020년 SA 방식 5G 표준화(Release 16)가 완성된 이후 상용화가 본격적으로 개시되기 전에 글로벌 기술 경쟁력 확보를 위해 다양한 5G 기술적 특성을 면밀히 분석하고 새로운 보안 문제를 해결하기 위해 복잡한 5G 생태계를 고려한 5G 보안 아키텍처 연구들이 함께 추진되어야 할 시점이라고 생각된다.

참 고 문 헌

[1] 김윤선, “5G 국제표준의 이해”, 삼성 리서치, 삼성 국제표준 백서, 2018.

[2] 이상협, “5G 통신의 현재와 미래”, IT동아(이문규), 4차 산업혁명과 직업의 미래, 2018.

[3] 신동형, “5G가 만들 새로운 세상”, NIA, DNA 플러스, pp.4-11, 2019.

[4] 신명기, 이수환, 이승익, 이종화, 안병준, “5G 네트워크/시스템 표준기술 동향”, TTA, TTA Journal, Vol(184), pp.40-49, 2019.

[5] 손장우, “http://www.netmaniaz.com/kr”, 넷마니

아즈 홈페이지 온라인 문서, 2019.
[6] “5G Core Vision”, SAMSUNG, Technical Report, pp.4-14, 2019.
[7] Michael G., Pramod N., “5G Security Innovation with CISCO” CISO Systems, White Paper, 2018.
[8] Louis M., Andreas S., Cristos D., Louis M., Marco L., Omid R.,“ENISA Threat Landscape Report 2018”, ENISA, pp.47 – 53, 2019.
[9] “The Evolution of Security in 5G” 5G americas, White Paper, pp.18-35, 2018.
[10] Jim H., “5G Security Strategy Considerations”, Jniper, Technical Report, pp.2-9, 2019.
[11] Ana N., Antonio A., Gerardo F., “Crowd sourcing analysis in 5G IoT: Cyber security Threats and Mitigation”, Mobile Networks and Applications, Vol(24), Issues(3), pp.881-889, 2019.
[12] Serdar V. et. al. “5G Network Architecture and Security”, UK DCMS, Technical Paper, pp.19-36, 2018.
[13] “A guide to 5G network security”, Ericsson Oneline White Paper, 2018.
[14] Noamen H., Monica W., Crhistine J., “An overview of the 3GPP 5G security standard”, Ericsson White Paper, 2019.
[15] 3GPP, “Security architecture and procedures for 5G system (TS 33.501)”, 2018.
[16] Ijaz A. Tanesh K., Madhusanka L., Jude O., Mika Y., Andrei G., “Overview of 5G security Challenges and Solutions”, IEEE, Communications Standards Magazine, pp.36-43, 2018.
[17] Rolf B., et. al, “5G Enablers for Network and System Security and Resilience: Security Architecture”, 5G PPP Security WG, pp.15-47, 2017.
[18] Manuel P., Gregorio P., “5G PPP Phase 1 Security Landscape”, 5G PPP Security WG, pp.7-63, 2017.
[19] “5G Security Architecture white paper”, Huawei, White Paper, pp11-14, 2017.
[20] 신상호, “SDN/NFV기반 5G 통신망 인프라의 진화”, NIA AI Network Lab 인사이트 제4호, pp.11-14, 2019.
[21] Ijaz A. Shahriar S. Tanesh K. Jude O., Andrei G., Mika Y., “Security for 5G and Beyond”, IEEE Communications Surveys & Tutorials, pp.4-6, 2019.
[22] Ericsson, “5G Security - Scenarios and solutions”, Ericsson Online white paper, June 2017
[23] Ijaz A., Madhusanka L., Shahriar S., Mika Y., “Design Principles for 5G Security”, A Comprehensive Guide to 5G Security, John Wiley & Sons, pp. 75-98., 2018
[24] Alejandro S. Cristina C., “Edge Nodes Infrastructure Placement Parameters for 5G Networks”, 2018 IEEE Conference on Standards for Communications and Networking, IEEE, p.3, 2018.

〈저자소개〉

김 환 국 (Kim Hwan Kuk)
종신회원
2017년 2월 : 고려대학교 정보보호학과 공학박사
2002년~2006년 : 한국전자통신연구원 정보보호본부 연구원
2007년 ~ 현재 : 한국인터넷진흥원 지능형사이버방어R&D 팀장
2017년 ~ 현재 : TTA 표준화위원회 TC5 사이버보안(PG503) 의장
<관심분야> 5G 보안, IoT SW 취약점 분석, AI 보안 등

최 보 민 (Bomin Choi)
정회원
2012년 2월 : 가천대학교 IT 공학사
2014년 2월 : 가천대학교 전자계산학 공학석사
2014년 5월 ~ 현재 : 한국인터넷진흥원 지능형사이버방어R&D 선임연구원
<관심분야> 5G 보안, 네트워크 보안, 악성코드 분석

고 은 혜 (Eunhye Ko)

정회원

2014년 2월 : 중앙대학교 컴퓨터공학부 졸업

2018년 8월 : 고려대학교 소프트웨어보안학과 공학석사

2014년 ~ 현재 : 한국인터넷진흥원 지능형사이버방어R&D 주임연구원

2017년 ~ 현재 : TTA 표준화위원회 TC5 사이버보안(PG503) 간사

<관심분야> 5G 이동통신망 보안, 네트워크 보안, SW 보안

박 성 민 (Seongmin Park)

정회원

2009년 2월 : 서강대학교 이학·공학사

2015년 2월 : 서강대학교 기술경영대학원 공학석사

2009년 3월~2013년 7월 : LGU+ 코어망개발팀

2013년 8월~현재 : 한국인터넷진흥원 지능형사이버방어R&D 책임연구원

<관심분야> 5G 이동통신망 보안, 네트워크 보안, 융합 보안, 모바일 취약점 분석