정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

5G 엣지 보안 기술 동향

박 종 근*, 김 영 수*, 이 종 훈*, 장 종 수*, 문 대 성*, 김 익 균*

요 약

1980년대 아날로그 이동전화서비스로 시작된 이동통신 기술은 매 10년을 주기로 빠르게 발전해 오고 있다. 디지털화를 거쳐 모바일 광대역 서비스에 초점을 맞춘 이전 세대와는 달리, 5G 이동통신서비스는 다양한 미래 정보통신 융합서비스의 플랫폼으로서, 산업구조 혁신을 통해 새로운 스마트 비즈니스 모델 및 산업 생태계를 창출하는 4차 산업혁명의 핵심 인프라로 주목받고 있다. 이러한 변화의 흐름속에서 이동통신서비스는 우리 실생활과 더욱 밀접해지고 있으나, 다른 한편으로 이동통신 환경의 취약점을 악용한 사이버 공격 위험에 노출될 가능성도 점차 확대되고 있다. 이런 배경에는 국제전기통신연합(ITU)의 IMT-2020 비전 및 요구사항을 충족시키기 위한 5G 네트워크의 구조적인 변화에 따라 공격접점이 크게 확대되었기 때문이다.

본 고에서는 5G 시대의 도래와 함께 가장 큰 구조적 변화를 겪으며 5G 융합서비스의 핵심 인프라로서 새롭게 주목받고 있는 5G 엣지의 주요 특징을 살펴보고, 5G 엣지에서 제기되고 있는 보안위협과 이에 대한 대응 기술의 동향에 대해 살펴보고자 한다.

Ⅰ. 서 론

우리나라가 작년 4월, 세계 최초로 5G를 상용화한 지도 1년이 훌쩍 지나고 있다. 국내 5G 가입자는 상용화 2개월만인 작년 6월에 100만 가입자를 돌파하였다. 가장 최근에 발표된 과학기술정보통신부의 무선통신서비스 가입자 통계[1]에 따르면 2020년 9월 누적 5G 가입자 수는 924만 8865명에 이른다. 이런 추세대로라면 5G 가입자는 11월에 이미 1,000만명을 돌파한 것으로 추정된다.

국내 5G의 서비스 가입자 수는 크게 증가하고 있으나 한편으로는 5G 이동통신서비스에 대한 가입자의 불만도 제기되고 있다. 이러한 가입자 불만의 주된 이유로는 4G LTE(Long Term Evolution) 대비 고주파수 대역을 사용하는 5G의 특성상 빠른 시간 내에 전국적인 셀 커버리지 확보를 위해 5G 코어망 없이 LTE 코어망 및 기지국(eNB)과 통신이 가능한 5G 비단독모드(NSA; Non-Standalone) 기지국(en-gNB)과 최소한의 LTE 업그레이드를 통해 5G NSA 망을 구축했기 때문이다. 따라서, 5G 단독모드(SA; Standalone)의 네트워크 인프라가 구축되기 전까지는 5G에 대한 가입자의 기대품질(Quality of Expectation)을 만족하는데는 일부분 한계가 있을 수 밖에 없다. 초기 과도기적 상황에서 야기되는 서비스 불만족은 내년부터 5G SA 네트워크가 본격적으로 구축되어 네트워크 슬라이싱을 포함한 다양한 5G 고유의 서비스가 실현되고 셀 커버리지가 점차 전국으로 확대되면 상당부분 해결될 수 있다. 그러나, 이동통신서비스가 고도화되고 우리의 삶에서 차지하는 비중이 높아질수록 악의적 해커나 적성국가 등으로부터 사이버 공격의 표적이 될 가능성은 점차 증가하며, 이에 대한 대응 부족으로 인해 서비스 장애를 비롯한 사용자의 재산과 생명을 위협하는 일을 초래해서는 안된다.

정보보안 측면에서 5G는 사이버 공격의 표적이 될 공격 접점이 크게 증가하였다. 초기 아날로그 이동전화서비스가 디지털화를 거쳐 모바일 광대역 서비스로 발전해 온 것과 달리 5G는 초연결(mMTC)·초저지연(uRLLC)·초고속(eMBB)의 다양한 미래 정보통신 융합서비스 플랫폼을 지향하고 있다. 이와 같은 ITU의 IMT-2020 비전 및 요구사항[2]을 충족하기 위해 네트

본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00952, 5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발)

* 한국전자통신연구원 지능화융합연구소 정보보호연구본부 (책임연구원, queue@etri.re.kr, 책임연구원, blitzkrieg@etri.re.kr, 책임연구원, mine@etri.re.kr, 책임연구원, jsjang@etri.re.kr, 실장, daesung@etri.re.kr, 본부장, ikkim21@etri.re.kr)

워크 인프라에 대한 구조적인 변화가 수반되었으며, 이러한 변화는 이동통신 코어망 보다는 엣지에 집중되어 있다. 여기에서 엣지란 5G 이동통신 네트워크에서 단말과 물리적으로 가까운 기지국부터 지역 또는 광역국사까지의 초기 접속 구간을 말한다.

따라서, 네트워크 구조의 변화로 인해 급증한 공격 접점과 이에 대한 잠재적 보안위협을 식별하고, 점차 고도화되고 지능화되는 사이버 위협에 대응할 수 있는 기술을 확보하는 것은 매우 중요하다.

본 고에서는 5G 시대의 도래와 함께 가장 큰 변화를 겪으며 5G 융합서비스의 핵심 인프라로서 새롭게 주목받고 있는 5G 엣지의 주요 특징을 살펴보고, 5G 엣지에서 제기되고 있는 보안위협과 이에 대한 대응 기술의 동향에 대해 살펴보고자 한다.

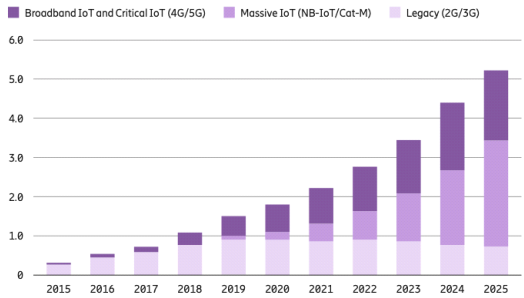
Ⅱ. 5G 엣지 특징

본 장에서는 IMT-2020 비전을 만족하면서 미래 ICT 융합서비스에 유연하고 민첩하게 대응해 나가기 위해 변화된 5G 엣지의 주요 특징을 살펴본다[3-5].

2.1. 접속 환경의 다변화

4G LTE 환경까지는 휴대전화나 테블릿 PC 등 제한된 종류의 단말들이 망에 접속한 반면, 5G 환경에서는 스마트 단말 뿐만 아니라, 센서, 웨어러블 장치, 자동차, 드론, 로봇 등 다양한 종류의 센서와 기기들이 대규모로 연결될 전망이다. 또한 5G NR(New Radio)이나 E-UTRA(Evolved UMTS Terrest- rial Radio Access)와 같은 이동통신 무선망 외에도 무선 LAN, 위성, 유선망 등의 다양한 접속 기술을 통해서도 5G 네트워크로 연결될 수 있다.

물론 4G LTE에서도 LTE Cat-M1이나 NB-IoT (Narrow-band IoT)와 같은 셀룰러 사물인터넷 기술을 통해 복잡도가 낮고 지연에 민감하지 않는 서비스를 대상으로 수많은 센서와 기기들이 이동통신 네트워크와 연결되고 있다. 그러나, 5G는 4G LTE 대비 10배 높은 초연결성, 1ms의 초저지연성, 그리고 99.9999%의 고신뢰성을 바탕으로 실시간 로봇 제어나 자율주행 자동차 등 보다 폭넓고 다양한 기기의 연결로 확대될 전망이며, 이를 바탕으로 스마트공장, 스마트시티, 자율주행차 등 다양한 융합서비스의 실현이 가속화될 전망이다.



〔그림 1〕 셀룰러 사물인터넷 연결수 전망(에릭슨[6])

2.2. 네트워크 소프트웨어화

5G 네트워크 인프라가 기존 세대와 가장 뚜렷하게 차별화되는 변화는 네트워크 소프트웨어화이다. 네트워크 소프트웨어화는 네트워크 장비의 제어부분을 트래픽 전송부분과 분리하여 트래픽 전달 동작을 개방형 인터페이스를 통해 제어하는 소프트웨어 정의 네트워킹(SDN; Software-defined Networking) 기술과 전용 하드웨어 기반 네트워크 장비의 하드웨어와 소프트웨어를 분리하여 네트워크 기능을 범용의 하드웨어 상에서 운용하는 네트워크 기능 가상화(NFV; Network Functions Virtualization) 기술을 바탕으로 한다.

사실상 본격적인 5G의 네트워크 소프트웨어화에 앞서 3GPP(The 3rd Generation Partnership Project)는 Release 14에서 4G EPC에 CUPS (Control and User Plane Separation) 구조를 도입하여 SGW(Serving Gateway)와 PGW (Packet Data Network Gateway)의 제어평면과 사용자 평면을 분리하고, SDN 기술을 바탕으로 중앙집중화된 제어 평면을 통해 분산된 사용자 평면을 제어할 수 있도록 함으로써 유연한 5G 네트워크로의 진화를 준비한 바 있다.

네트워크 소프트웨어화는 물리적인 네트워크 인프라를 마치 프로그래밍하듯이 설계, 구축, 운용, 관리할 수 있는 기술이다. 사실상 앞서 언급한 IMT-2020 비전인 초연결, 초저지연, 초고속의 요구사항을 동시에 만족하는 하나의 네트워크를 구축하기란 불가능하다. 그렇다고 해서 서비스별로 서로 다른 품질특성을 갖는 네트워크를 독립적으로 여러개 구축하여 운용하는 것은 막대한 투자비용과 운용비용 부담을 초래한다.

결국 하나의 물리적인 네트워크 인프라를 가상으로

쪼개어 마치 서로 독립적인 망처럼 사용할 수 있는 네트워크 슬라이싱(network slicing) 기술이 적용되어야 하며, 이를 위해서는 네트워크 소프트웨어화가 필수적이다.

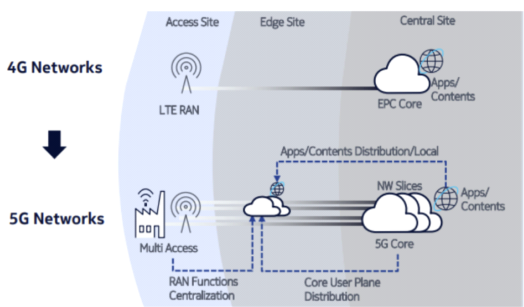
다만, 가상화된 환경에서는 실제 운용되는 물리적인 네트워크 장비보다 더 많은 물리적인 장비와, 가상머신이나 컨테이너 형태의 네트워크 장비가 동시에 운용되기 때문에 관리하거나 보호해야 할 대상과 영역 그리고 복잡도가 크게 증가한다.

2.3. MEC 보편화

MEC(Multi-access Edge Computing)는 사용자의 서비스를 중앙 집중화된 원격의 클라우드가 아닌, 사용자와 물리적으로 가까운 엣지 네트워크에서 클라우드를 이용하여 컴퓨팅 서비스를 제공하는 기술이다. 일반적으로 MEC는 Cloud-RAN이 위치한 셀 사이트나 지역 또는 광역 국사, 서비스 핫스팟 지역, 고객 기업이나 기관의 사내망 등에 위치하면서, 서비스의 지연 시간을 줄이고 위치 기반 맞춤형 서비스를 제공할 수 있는 기술로서 5G의 초저지연·초고속 융합서비스를 실현하는 핵심 기반 기술 중 하나이다.

MEC의 특장점으로는 서비스의 네트워크 지연 시간을 단축하고 백홀(backhaul) 대역폭을 크게 감소시킬 수 있으며, 특정 지역이나 기업별로 맞춤형의 MEC 플랫폼을 구축함으로써 위치기반의 맞춤형 서비스를 제공할 수도 있다. 또한 기지국에서 수집 가능한 무선 액세스 네트워크 상황 정보를 활용하여 실시간 송출 스트림의 품질을 조절하거나 컨텐츠를 캐싱하는 등 맞춤형 고품질 서비스를 제공할 수 있는 것이다.

그러나, 5G 이동통신 네트워크에서 MEC를 통한 원할한 서비스를 제공하기 위해서는 기존 클라우드 서비스와 다른 몇 가지 기술적인 이슈사항을 고려해야 한다.



〔그림 2〕 5G MEC 도입에 따른 서비스 특성 비교(5G Americas[7])

먼저 응용 소프트웨어 또는 이미지의 이동성(mobility)과 이식성(portability)을 고려해야 한다. MEC는 사용자와 물리적으로 가까운 엣지 네트워크에 위치하고 있기 때문에 사용자의 이동성을 전제로 한 이동통신 환경에서는 사용자가 이동함에 따라 MEC 응용의 이동성도 보장해야 한다. 즉, 사용자가 서비스를 제공받는 기존 MEC 서버에서 물리적으로 멀어지면 저지연성을 보장하기 위해 MEC 응용도 사용자와 보다 가까운 엣지 네트워크의 MEC 서버로 응용을 마이그레이션시킬 수 있어야 한다. 마찬가지로 응용이 새로운 MEC 서버로 이동되기 위해서는 MEC 응용이 새로운 MEC 서버에서도 실행될 수 있는 이식성이 보장되어야 한다.

MEC 응용의 이동성으로 인해 MEC 플랫폼에서도 고려해야 할 추가적인 이슈들이 있다. 먼저 MEC 플랫폼은 중앙의 클라우드보다 상대적으로 규모가 작기 때문에 제한된 자원을 효율적으로 관리할 수 있어야 한다. 또한 MEC 서버는 응용의 이동 등을 지원하기 위해 서버간 협업이 이루어져야 한다. 특히, MEC 서버에는 사용자의 식별정보나 서비스 이용 정보 등이 저장되고 처리됨에 따라 민감정보의 유출이나 변조 등의 사이버 위협에 대한 대응도 반드시 뒷받침되어야 한다.

2.4. 분산 네트워크 구조화

5G 네트워크는 네트워크 인프라의 가상화와 더불어 분산 구조화도 본격화될 전망이다. MEC의 확산에 따라 코어망 바깥에 있던 클라우드가 네트워크 인프라 내에도 구축되고, 가상화에 의해 이식성이 뛰어난 소프트웨어 중심의 가상 네트워크 장비와 응용 서비스 등이 클라우드 기지국, MEC, 코어망 등 5G 네트워크 전역에 걸쳐 배치되어 운용될 수 있다.

또한 5G에서 도입된 서비스 기반 구조(Service-based Architecture)에 따라 제어 평면의 각 네트워크 기능은 HTTP 통신이 가능한 곳이라면 서비스 특성에 따라 어디든 자유롭게 배치되어 운용될 수 있다. 여기에서 서비스 기반 구조란 5G 네트워크 기능을 작은 서비스 단위로 세분화하고 세분화된 기능간에는 HTTP 인터페이스를 통해 연동함으로써 네트워크 구조의 유연성과 확장성을 강화하기 위해 도입된 개념이다. 5G

네트워크 구조에서는 5G 코어망의 제어평면이 서비스 기반 구조에 따라 정의되어 있다.

그러나, 네트워크 인프라의 가상화로 인해 늘어난 공격 접점과 관리의 복잡도는 분산 네트워크 구조화로 인해 더욱 가중될 것으로 전망된다.

2.5. 네트워크 슬라이싱

네트워크 슬라이싱은 하나의 물리적인 네트워크를 바탕으로 논리적으로 서로 독립된 복수의 종단간(end-to-end) 네트워크를 제공하는 기술로서, 서로 다른 품질 특성을 요구하는 다양한 5G 융합서비스를 위한 핵심 기술이다. 물론 네트워크 슬라이싱이 5G 엣지에만 국한되는 것은 아니지만, 종단간의 논리적인 네트워크를 제공하기 위해서는 엣지에서의 독립된 네트워크 슬라이싱 제공이 필수적이다.

네트워크 슬라이싱은 아직 널리 운용되지 않은 새로운 개념으로서, 무엇보다도 네트워크 슬라이스에 대한 알려진 위협이나 취약점이 명확하지 않다. 그러나, 네트워크 슬라이스 특성상 하나의 공통 하드웨어 플랫폼 상에서 종단간 서비스를 제공하는 복수의 가상화된 기능이나 응용의 집합으로 네트워크 슬라이스가 구성되기 때문에 서로 다른 네트워크 슬라이스 간의 완전한 격리성 보장이 중요한 이슈로 부각되고 있다.

Ⅲ. 5G 엣지 보안위협 및 대응 기술

5G 엣지 보안 기술은 초연결·초저지연·초고속의 5G 융합서비스에 대한 안전한 이용환경을 보장하기 위해 5G 융합서비스의 품질을 좌우하는 엣지 네트워크를 보호하고, 엣지에서의 보안 위협이 5G 전체 네트워크로 확산되지 않도록 엣지에서 대응하고 해결하기 위한 기술이다.

특히 스마트공장, 자율주행차, 스마트시티 등 5G 핵심 융합서비스의 안전한 이용환경을 제공하기 위해서는 무엇보다도 엣지에서 보안 위협을 신속하게 식별하여 차단하거나 격리시킴으로써 사이버 공격 피해를 최소화하고 코어망과 다른 엣지망으로의 확산을 방지해야 한다.

5G 엣지 보안 기술은 크게 5G 엣지 네트워크 보안 기술, MEC 보안 기술, 인공지능 기반 지능형 보안위협 분석 및 관제 기술로 구분할 수 있다.

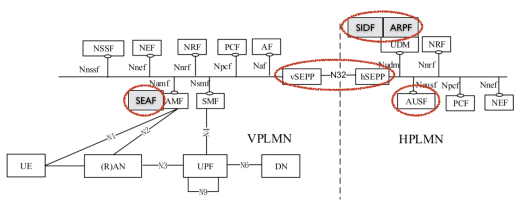
본 장에서는 5G 엣지 보안 기술에 대해 살펴보고, 주요 보안위협과 대응 기술에 대해 정리한다.

3.1. 5G 엣지 네트워크 보안 기술

5G 엣지 네트워크는 초연결·초저지연·초고속의 서비스를 제공받는 모든 단말이 5G 망에 접속하는 연결 접점이자 초저지연 등의 서비스가 제공되는 핵심 인프라이다. 특히, 5G NR 또는 E-UTRA의 이동통신, 무선 LAN, 유선 및 위성통신 등의 다양한 액세스 기술을 통해 수많은 다양한 종류의 센서 및 기기가 연결되는 접점으로서 액세스 환경이 다변화되었다. 또한, SDN/NFV 기술에 기반한 본격적인 네트워크 인프라의 소프트웨어화와 분산 구조로의 변화에 따라 서비스의 품질을 보장하기 위해 코어망의 다양한 네트워크 기능과 응용 서비스가 엣지 네트워크로 집중될 전망이다. 이러한 5G 네트워크 구조의 변화로 인해 5G 엣지 네트워크의 공격 접점과 잠재적 보안위협이 크게 증가하였다.

4G LTE에서의 주요 보안위협에 대한 연구결과에 따르면, 무선 재밍(jamming) 공격, 가입자 식별정보(IMSI; International Mobile Subscriber Identifier) 탈취 공격, 허위 기지국을 이용한 중간자(man-in-the-middle) 공격, 위치추적, 서비스 장애 또는 보안성이 상대적으로 취약한 2G/3G로의 서비스 강등 유도 등 무선 액세스 망의 취약점을 이용한 보안위협이 발표된 바 있으나, 상대적으로 액세스망 보다는 코어망에 대한 경계(perimeter) 보안에 중점을 두어 왔다[7-9].

5G 표준 기술규격을 제정하는 3GPP에서도 이미 알려진 보안 취약점을 해소하기 위해 기존 기술 규격의 보안성을 강화하거나 새로운 기능을 추가하는 등의 노력을 기울이고 있다. 5G에서의 주요 보안 개선사항을 꼽아보면, 가입자 신원정보의 암호화를 통한 보호, 인증 및 키 공유 체계 개선, 무선 구간 사용자 데이터 보호 강화, 서비스 기반 구조 보호 체계, 이동통신 망간



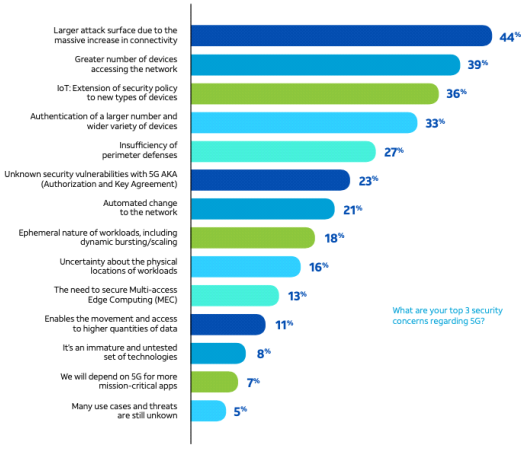
〔그림 3〕 5G 네트워크 구조와 주요 보안 기능

시그널링 보호 체계 강화, 접속망에 비종속적인 통합 인증 체계, 외부 응용서버와의 인증 체계 도입 등을 꼽을 수 있다[9,10].

그러나, 이와같은 3GPP의 보안기술 규격 고도화에도 불구하고, 4G에서의 보안위협 뿐만 아니라 5G 엣지 네트워크의 새로운 잠재적 보안위협이 존재한다. AT&T Cybersecurity가 작년 8월과 9월에 걸쳐, 북미, 인도, 호주, 영국의 500명 이상 규모의 기업을 대상으로 총 704명의 보안담당자에게 설문조사한 결과에 따르면, 우선 응답자의 72.5%가 5G가 보안에 미치는 영향이 높다고 답했다. 또한, [그림 4]와 같이 5G와 관련하여 가장 우려되는 보안위협으로는 초연결에 따른 공격접점의 증가, 대규모 단말의 네트워크 연결, IoT 단말의 연결, 대규모 및 다양한 종류의 단말 인증, 경계 방어의 불충분성 등이 있으며, 이를 통해 5G 엣지 네트워크에 대한 보안 우려가 높다는 것을 엿볼 수 있다.

5G 엣지 네트워크 보안 기술로는 5G 엣지 네트워크의 잠재적 보안위협에 대응하기 위해 무선 액세스 네트워크의 취약점을 분석하고 5G 서비스 품질 특성에 대한 성능저하를 최소화할 수 있는 고성능의 트래픽 분석을 통한 네트워크 기반 실시간 침해위협 탐지 및 차단 기술이 요구된다.

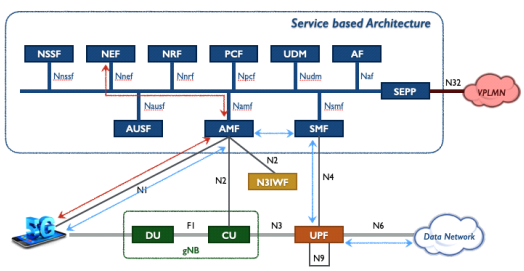
5G는 다양한 융합서비스의 플랫폼으로서 무엇보다도 다양한 사양과 성능의 사물인터넷 연결이 활성화될 전망이다. 사물인터넷 특성상 자원이 부족한 센서 및 기기는 보안 기능을 충분히 갖출 수 없거나 쉽게 공격에 악용될 수도 있다. 따라서, 4G LTE에서와 마찬가지로 봇넷 등 대규모 접속으로 인한 무선 및 클라우드 기지국 자원의 고갈 등 서비스 거부 공격이 발생할 수 있으므로, 이에 대한 대응 기술과 함께 대규모 사물인터넷 인증 및 키 관리 기술과 비정상 배터리 소모 방지 기술 등을 통해 사물인터넷 기기에 대한 대응이 요구된다.



〔그림 4〕 AT&T Cybersecurity의 5G 보안위협 설문결과〔11〕

특히, Cat-M1 및 NB-IoT 기술 등의 초연결 사물인터넷(Massive IoT) 기술은 Release 13에서 본격화된 4G 기술이지만, 두 기술 모두 5G의 초연결성(mMTC) 요구사항을 만족하고 5G NR과의 효과적 공존을 고려하여 진화하는 이유로 GSMA (GSM Association)를 중심으로 5G 기술로 일부 인정받고 있다. 또한 3GPP Release 16에서는 단말의 전력소모 최소화와 함께 이들 기술이 5G 시스템과 통합될 수 있도록 관련 표준 규격의 개발이 이루어졌다[13]. 따라서, Cat-M1 및 NB-IoT의 기술 특성인 Non-IP 데이터의 전송, 시그널링 채널을 통한 간헐적 사용자 트래픽 전송 등을 포함한 셀룰러 사물인터넷 환경에서의 비정상 트래픽 및 공격을 탐지하고 대응할 수 있는 기술이 요구된다.

허위 기지국을 통한 개인정보 유출, 위치 추적 및 중간자 공격 등에 대한 대응 기술도 필요하다. 4G LTE와 달리 5G에서는 허위 기지국을 통한 가입자 식별정보(IMSI) 탈취를 방지하기 위해 단말이 가입자 식별정보를 암호화하여 보내도록 표준 규격을 개선하였다. 그러나, 여전히 시스템 정보 메시지를 전송하는 브로드캐스팅 채널에 대한 보호는 미비하며, 인증을 통한 보안 컨텍스트가 설정되기 이전에는 RRC (Radio Resource Control) 채널에 대한 기밀성과 무결성이 보장되지 않는 취약점이 존재한다. 따라서, 5G 액세스 구간에서의 취약점을 분석하고, 허위 기지국을 이용한 다양한 중간자 공격 등으로부터 사용자를 보호할 수 있는 새로운 보호 매커니즘의 개발이 필요하다. 더 나



〔그림 5〕 5G 초연결 사물인터넷에서의 제어평면 최적화를 통한 데이터 전달 경로

아가 네트워크 기반으로 허위 기지국을 효과적으로 탐지하고 단말이 허위 기지국과 연결하지 않도록 제어하는 기술도 고려할 수 있다.

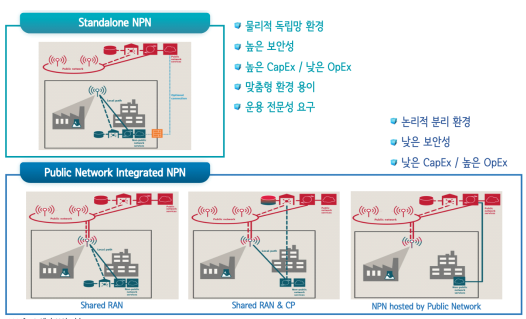
최근 5G 엣지 네트워크와 관련하여 중요하게 대두되는 것 중 하나는 사설 5G 네트워크(Non-Public Networks)이다. 사설 5G 네트워크는 의미 그대로 명확하게 정의된 하나 이상의 사용자 조직을 대상으로 5G 네트워크 서비스를 제공하기 위해 캠퍼스나 공장과 같이 사용자 조직이 지정한 영역 내에 구축된다.

5G-ACIA(5G Alliance for Connected Industries and Automation)에서는 [그림 6]과 같이 사설 5G 네트워크에 대한 4가지 구축 모델을 제안하고 있다. 5G-ACIA의 구축 모델은 크게 격리된 독립형 NPN과 이동통신사업자의 망과 연계된 NPN으로 구분할 수 있다[15].

먼저 완전히 격리된 독립형 NPN은 사용자 조직이 직접 구축하거나 이동통신사가 구축을 대신할 수 있으며, 무엇보다도 물리적으로 독립망 환경이므로 맞춤형의 높은 보안성이 보장되는 것이 특징이다.

이동통신사업자의 망과 연계된 NPN은 다시 기지국 공유형, 기지국 및 코어망 제어평면 공유형, 이동통신사업자에 의한 호스팅형으로 구분된다. 기지국 공유형의 경우, 기지국만 논리적으로 분리되고 나머지는 모두 독립적으로 구축되므로 상대적으로 보안성이 높은 편이나, 기지국 및 코어망 제어평면 공유형과 이동통신사업자에 의한 호스팅형은 단말의 가입정보와 운영정보가 이동통신사업자에 의해 관리되므로 상대적으로 보안성이 낮은 특성이 있다.

사설 5G 네트워크는 스마트공장 등 다양한 B2B 서비스를 위한 네트워크 구축 모델로서 고려된다. 따라서, 사설 5G 네트워크 구축 모델별로 단말의 인증 및 접근 제어, 사설 5G 네트워크와 상용 5G 네트워크와의 연계, 5G LAN 서비스 등과 관련한 보안 취약점을 분석하고 이를 악용한 사설 5G 네트워크에 대한 공격의 탐지 및 대응 기술 개발이 필요하다[16].



〔그림 6〕 5G Non-Public Network 구축 모델

3.2. 5G MEC 보안 기술

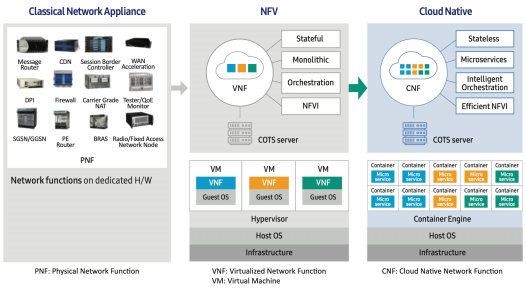
5G MEC는 5G 기반 융합서비스를 실현하는 핵심 인프라로서, NFV 기술을 바탕으로 융합서비스 등을 실행하기 위한 3rd party 응용이 실행될 수 있는 개방형 시스템인 점이 NFV와의 뚜렷한 차이점이다.

일반적으로 개인 사용자를 대상으로 서비스를 제공하는 범용 클라우드 서비스는 서비스 사용자에 대한 인증 및 권한관리, 멀티테넌시(multi-tenancy) 기반의 접근 관리, 클라우드 데이터 유출 방지를 포함한 CASB(Cloud Access Security Broker) 등의 기술을 통해 보안성 확보에 중점을 두고 있다. NFV 기술은 태생적으로 통신사업자 망내에 존재하는 하드웨어 기반의 네트워크 장비를 범용의 하드웨어 상에서 소프트웨어 기반으로 운용하기 위한 기술로서, 일반 사용자의 접근이나 사용이 엄격히 제한되는 것이 특징이다. 따라서, NFV 보안 기술에서는 관리자에 대한 인증 및 권한관리와 통신장비에 저장된 사용자 정보 또는 민감 서비스 데이터에 대한 보호에 중점을 두고 있다.

5G MEC에 대한 주요 보안위협으로는 MEC에 저장된 중요 사용자 또는 서비스 정보를 유출하거나 조작하는 공격, MEC 호스트의 자원을 비정상적으로 고갈시켜 동일 호스트 상에 실행중인 다른 서비스의 장애나 중단을 유발하는 공격, 조작 등 악성코드에 감염된 MEC 응용을 통해 다른 서비스의 장애를 유발하거나 민감한 정보를 유출하는 공격 등을 꼽을 수 있다.

이와 같은 5G MEC 보안위협에 대한 대응 기술로는 가상화된 MEC 플랫폼이나 실행중인 MEC 응용의 보안위협 및 이상행위를 탐지하고 대응하는 기술, 외부에서 공급되는 3rd party 응용의 무결성을 보장하고 취약성을 검증하는 기술이 요구된다[4,5].

5G MEC와 관련하여 대두되는 것은 클라우드 네이티브(Cloud Native) 환경으로의 진화이다. 클라우드 네이티브란 클라우드 컴퓨팅의 장점으로 꼽을 수 있는 유연성, 확장성, 가용성을 극대화하기 위해 응용은 가능한 한 작은 단위인 마이크로 서비스 구조에 따라 개발하고, 개발된 각각의 응용은 가상머신보다 상대적으로 경량화된 컨테이너로 실행하고, 버그의 패치를 포함



〔그림 7〕 클라우드 네이티브 환경으로의 진화(삼성전자 〔18〕)

한 새로운 기능은 자동화를 통해 개발, 통합, 테스트, 배포가 지속적으로 이루어지는 개발 및 운용 접근방법이다. 따라서, 클라우드 네이티브 환경으로의 전환을 통해 빠른 신규 서비스 개발, 지능적 서비스 규모 확장, 배포 자동화, 운영 자동화 등 IT 클라우드의 성공 사례를 추구할 수 있는 장점이 있다[17].

최근 삼성전자와 SK텔레콤은 공동으로 클라우드 네이티브 방식을 기반으로 차세대 5G 클라우드 코어망을 개발한 바 있으며[18,19], 앞으로 5G 네트워크에서 코어망 뿐만 아니라 MEC에서도 클라우드 네이티브 환경으로의 전환이 더욱 가속화될 전망이다. 따라서, 클라우드 네이티브 환경으로 5G MEC 진화에 대비하여 컨테이너에 대한 보안위협과 빈번하게 발생하는 MEC 응용 이미지의 업데이트로 인해 조작되거나 악성코드에 감염된 비정상 이미지가 5G 이동통신 네트워크 내로 유입될 수 있는 보안위협에 대응할 수 있는 기술 개발이 필요하다.

특히, 컨테이너는 호스트의 커널을 공유하는 운영체제 가상화 기술을 기반으로 하기 때문에, 가상화된 이미지의 크기가 작고 빠른 실행이 가능한 장점이 있는 반면, 시스템 가상화 기술을 바탕으로 한 가상머신에 비해 상대적으로 격리성이 취약하여 보안성이 떨어지는 단점이 있다. 따라서, 컨테이너 권한의 임의 조작 방지, 서로 다른 네트워크 슬라이스에 속하는 컨테이너 간 허가되지 않은 네트워크, 파일, 데이터의 접근 탐지 및 차단, 컨테이너의 MEC 호스트 자원 과다 점유 방지 등의 기술 개발이 필요하다[4,5].

3.3. 지능형 보안위협 분석 및 관제 기술

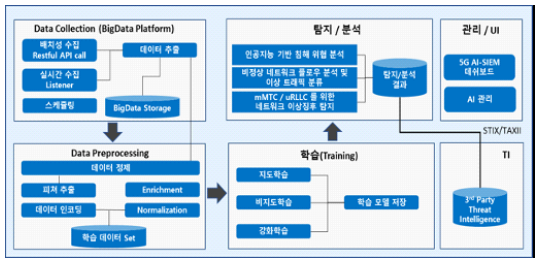
지능형 보안위협 분석 및 관제 기술은 5G 엣지 네트워크와 MEC로부터 실시간 수집되는 보안상황 빅데이터를 기반으로 인공지능 기술을 이용해 보안상황 정보를 종합적으로 분석하여 보안위협을 탐지하고 대응하는 기술이다.

앞서 2장에서 살펴본 바와 같이, 5G 네트워크의 구조적 변화에 따라 공격 접점이 대폭 증가하고 관리해야 할 대상도 크게 증가하였다. 더욱이 실시간으로 수집되는 방대한 네트워크 정보와 보안장비에서 발생하는 이벤트 정보를 통합하여 보안위협을 분석하고 대응하기 위해서는 관제요원 중심의 수동적 분석이 아닌 인공지능 기반의 지능형 보안위협 분석 및 대응이 절실하다. 이를 통해 보안장비 로그에서 발생하는 오탐을 최소화하고, 사전 설정된 임계치 또는 정책 기반의 위협 탐지에서 누락되는 잘 알려지지 않은 위협에 대한 미탐도 최소화할 수 있어야 한다.

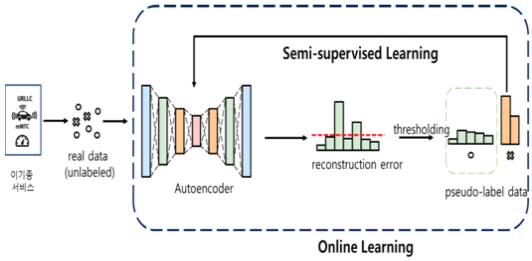
또한, 5G 엣지에서의 보안상황 정보를 종합적으로 모니터링하고, 이를 시각화하여 실시간 보안위협에 대응할 수 있는 관제 시스템이 필요하며, 엣지에서의 보안 위협 정보를 코어망이나 다른 엣지망의 관제 시스템과 상호 공유함으로써 5G 네트워크의 전역적인 관점에서 사이버 위협에 대응할 수 있어야 한다.

지능형 보안위협 분석은 APT(Advanced Persistent Threat) 공격과 같은 알려지지 않은 치명적인 공격에 대응하기 위해 5G 엣지 네트워크와 MEC 플랫폼 및 응용 등으로부터 발생하는 트래픽과 보안 이벤트 간의 연관성을 머신러닝과 같은 인공지능 기법을 이용하여 분석함으로써 보안 성능을 향상시키는 기술이다. 과거에는 이러한 방대한 데이터를 통합하여 분석하기가 어려웠지만 최근 빅데이터 분석 및 인공지능 기술의 발전에 힘입어 지능형 보안 기술을 활용할 수 있게 되었다.

현재까지의 인공지능 기반 지능형 네트워크 침입 탐지 기술은 IP 기반 유선망에서의 침입 탐지를 위해 지도학습 기반 머신러닝 기술을 이용하며, 이를 위해 정상 또는 보안위협 레이블 정보가 포함된 고품질의 학



〔그림 8〕 인공지능 기반 보안위협 분석 및 탐지 구조〔20〕



〔그림 9〕 반지도/비지도 학습 기반 딥러닝 모델의 이상행위 탐지 예시〔20〕

습 데이터가 반드시 필요하다. 다만, 지도학습을 위한 학습 데이터를 생성하기 위해 소요되는 시간과 비용 부담 때문에 보안위협 탐지시스템 개발에 제약이 있으며, 새로운 패턴의 학습 데이터를 반영하기 위한 모델 재훈련 비용도 매우 큰 것이 문제로 지적된다. 따라서, 최근에는 반지도 또는 비지도학습 기반의 머신러닝/딥러닝을 이용한 이상징후 탐지는 보안 업계에서 시급히 확보하고자 하는 실용적인 핵심 기술로 부상하고 있다.

다만, 일반적으로 사이버보안에서의 인공지능 기술은 특정 모델의 선정보다는 수집 데이터의 정의, 데이터셋 수집, 데이터 특성 분석 및 특징값(features) 설정이 성능을 좌우하기 때문에, 무엇보다도 양질의 데이터셋의 확보가 우선되어야 한다.

최근 초연결 스마트 공간에서 사이버 공격에 대한 노출이 증가하면서 이를 보호할 수 있는 인공지능 기반의 시스템과 프로세스의 역할이 증대되면서, 가트너의 2020년 10대 전략기술 트렌드 중 하나로 'AI Security'가 선정된 바 있다. 따라서, 인공지능을 활용한 시스템 보안의 강화, 머신러닝을 이용한 사이버 공격 패턴의 파악, 그리고 인공지능을 악용한 사이버 공격을 예측하는 등 인공지능을 적용한 다양한 보안 기술은 더욱 가속화될 것으로 전망된다[21].

Ⅳ. 결 론

5G 시대의 도래와 함께 주목받고 있는 실감컨텐츠, 스마트시티, 자율주행차, 스마트공장, 디지털 헬스케어 등 실생활과 밀접한 다양한 5G 융합서비스는 사이버 침해시 단순히 이동통신서비스의 장애가 아닌 국민의 재산과 생명을 위협하는 재난으로 이어질 수 있는 측면에서 면밀한 대응이 요구된다. 그러나 종전처럼 코어망의 경계(perimeter)를 중심으로 보안장비를 구축하여 위협에 대응하는 방식만으로는 지능화되고 고도화된 다양한 위협으로부터 네트워크와 서비스를 보호하기에 한계가 있다. 따라서, 5G 인프라의 구조와 서비스 특성의 변화에 따라 새롭게 부각되는 잠재적 보안위협을 식별하고 대응할 수 있는 기술개발 노력이 지속적으로 요구된다.

지난 8월 정부는 '6G 시대 선도를 위한 미래 이동통신 R&D 추진전략'을 발표하면서 고위험 6G 원천기술 확보를 위해 투자하며 설계단계부터 보안을 고려하는 6G 보안 내재화 기술 개발을 병행할 계획을 발표한 바 있다. 굳이 6G가 아니더라도 5G 기술이 지속적으로 발전해 나가고 있는 만큼 네트워크와 서비스를 설계·구축·운용하는 전 단계에 걸쳐 일관되게 '보안 중심 설계(security-by-design)' 원칙에 따라 잠재된 보안위협을 식별하고 이에 대한 대응 기술을 지속적으로 개발하고 적용해 나가야 한다.

참 고 문 헌

[1] 과학기술정보통신부, "(2020년 9월말 기준) 무선통신서비스 가입자 통계", 2020,10.30.

[2] ITU-R Recommendation, M.2083.0, IMT- Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, 2015.

[3] 박종근, "5G 엣지 보안 기술", KRnet 2020, 2020

[4] 박종근, "5G 엣지 보안: MEC 보안을 중심으로", NetSec-KR 2020, 2020

[5] 김영수, 박종근, 이종훈, 장종수, 문대성, 김익균, "5G 환경에서의 MEC 보안위협 및 대응 기술", 정보과학회지, 38권 9호, pp. 16-24, 2020.9.

[6] Ericsson, "Ericsson Mobility Report", 2020.06.

[7] 5G Americas, "The Evolution of Security in 5G", 2018.10.

[8] J. Cichonski, J. Franklin, "LTE Security – How Good is it?", RSA Conference 2015, 2015.04.

[9] 3GPP, TS 33.501, Security Architecture and Procedures for 5G System, V15.3.1, 2018.

[10] 박종근, 김종현, 문대성, 김익균, "3GPP 5G 보안 구조의 특징 및 주요 개선사항", 정보보호학회지, 29권 5호, pp. 21-30, 2019.10.

[11] AT&T Cybersecurity, "AT&T Cyber- security Insights Report: Security at the Speed of 5G",

2019.
[12] 3GPP, TR 33.861, Study on Evolution of Cellular Internet of Things(CIoT) Security for the 5G System, V16.0.0, 2020.
[13] I. Sharp, “5G Standards Developments in 3GPP Release 16 and Beyond”, ATIS Webinar on 5G Standards Development in 3GPP Release 16 and Beyond, 2020.09.
[14] 3GPP TR 33.809, Study on 5G Security Enhancement against False Base Station(FBS), V0.10.0, 2020.
[15] 5G-ACIA, “5G Non-Public Netowrks for Industrial Scenarios”, 2019.7.
[16] 박태근, 박종근, 김기원, “Security Threats and Potential Security Requirements in 5G Non-Public Networks for Industrial Applications”, 한국컴퓨터정보학회논문지, 25권 11호, 105-114, 2020.11.
[17] 박종한, “Cloud Native Platform for Telco”, KRnet 2020, 2020.
[18] Samsung, “Cloud Native 5G Core: Samsung 5G Core Vol.2”, 2020.
[19] 전자신문, “SK텔레콤-삼성전자, 국제 표준 세계 최초 적용 ‘차세대 클라우드 코어망’ 개발”, 2020.11.22.
[20] 이종훈, “5G 엣지 보안위협 분석 탐지를 위한 AI 기술”, 제3회 5G보안 워크숍, 2020.11.
[21] 과학기술정보통신부, “2020년 10대 전략기술 트렌드”, R&D KIOSK, 제69호, 2020.02.

〈저자소개〉

박 종 근 (Jong-Geun Park)
정회원
1997년 2월 : 성균관대학교 산업공학과 학사
1999년 2월 : 성균관대학교 산업공학과 석사
2013년 2월 : 충남대학교 컴퓨터공학과 박사
1999년 3월~2001년 4월 : 국방과학연구소 연구원
2001년 5월 ~ 현재 : 한국전자통신연구원 책임연구원
<관심분야> 이동통신보안, SDN/NFV, 클라우드보안

김 영 수 (Youngsoo Kim)
정회원
1998년 2월 : 성균관대학교 정보공학과 학사
2000년 2월 : 성균관대학교 컴퓨터공학과 석사
2009년 2월 : 성균관대학교 컴퓨터공학과 박사
2012년~2015년 : 충남대학교 컴퓨터공학과 겸임교수
2000년 ~ 현재 : 한국전자통신연구원 책임연구원
<관심분야> 5G 보안, 네트워크 보안, 디지털포렌식, 암호프로토콜

이 종 훈 (Jong-Hoon Lee)
정회원
1999년 2월 : 경북대학교 컴퓨터공학과 학사
2002년 2월 : 경북대학교 컴퓨터공학과 석사
2020년 8월 : 경북대학교 컴퓨터공학과 박사
2002년 ~ 현재 : 한국전자통신연구원 책임연구원
<관심분야> 정보보호, 네트워크 보안, 5G 보안, 인공지능 기반 지능형 위협 탐지, 빅데이터 기반 위협 탐지

장 종 수 (Jongsoo Jang)

정회원

1984년 2월 : 경북대학교 전자공학과 학사

1986년 2월 : 경북대학교 전자공학과 석사

2000년 2월 : 충북대학교 컴퓨터공학과 박사

1998년 ~ 현재 : 한국전자통신연구원 네트워크보안그룹장, 보안응용연구부장, 기술기획연구그룹장/책임연구원

2006년 ~ 현재 : 대검찰청 디지털수사자문위원회 위원

<관심분야> 네트워크 보안, 클라우드 보안, 개인정보보호, 5G 보안

김 익 균 (Kim, Ikkyun)

종신회원

1994년 2월 : 경북대학교 컴퓨터공학과 학사

1996년 2월 : 경북대학교 컴퓨터공학과 석사

2009년 2월 : 경북대학교 컴퓨터공학과 박사

2004년~2005년 : Purdue University 초빙 연구원.

1996년~현재 : 한국전자통신연구원 정보보호연구본부 본부장/책임연구원

<관심분야> 네트워크 보안, 컴퓨터 네트워크, 클라우드보안, 빅데이터 분석

문 대 성 (Moon, Daesung)

정회원

2007년 2월 : 고려대학교 전산학과 박사

2009년 3월~현재 : 과학기술대학원 대학교(UST) 정보보호공학 전공책임교수

2000년 12월~현재 : 한국전자통신연구원 네트워크·시스템보안연구실 실장

<관심분야> 정보보호, 네트워크보안, 5G보안, 인공지능보안