방송통신정책연구	RS-2022-00156261

안전한 5G 특화망 도입 및 구축을 위한 보안 고려사항 연구

A study on Security Considerations for the Adoption and Deployment of a Secure 5G Private Networks

유일선

2023. 01.

연구기관 : 국민대학교 산학협력단

과학기술정보통신부 정보통신기획평가원

이 보고서는 2022년도 과학기술정보통신부 방송통신발전기금 방송통신정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 과학기술정보통신부의 공식입장과 다를 수 있습니다.

제 출 문

과학기술정보통신부 장관 귀하

본 보고서를 『**안전한 5G 특화망 도입 및 구축을 위한 보안 고려사항 연구**』의 연구결과보고서로 제출합니다.

2023년 02월

연구기관 : 국민대학교 산학협력단
총괄책임자 : 유일선
참여연구원:

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

안전한 5G 특화망 도입 및 구축을 위한 보안 고려사항 연구

2. 연구 목적 및 필요성

○ 본 과제의 연구 목적 및 필요성은 다음과 같음

- 전 세계 이동통신 네트워크 산업의 표준 기술이 될 5G 네트워크의 주도권 확보를 위한 경쟁심화와 함께 세계 주요국의 5G 특화망에 대한 전용주파수 공급 및 다양한 분야의 서비스 환경 조성
- 5G 특화망은 특정지역(건물, 공장 등)에 한해 사용가능한 5G망으로서, 해당지역에서 도입하고자 하는 서비스에 특화된 맞춤형 네트워크. 독립형 또는 공용 네트워크와 연결하여 구축 가능함
- 과기정통부는 5세대(5G) 특화망 정책방안(´21.1월) 및 공급방안(´21.6월)을 발표하고 4.7㎓/28㎓ 대역 주파수 공급
- 5G 특화망과 관련 정부 정책의 성공을 위한 선제조건으로 보안 기술 연구가 요구됨
- 특히, 국내 5G 특화망 도입 기업 및 관련 기관에게 5G 특화망에 적합한 보안 고려사항을 제시함으로써 안전한 5G 특화망 보안을 체계적으로 구축하도록 지원하는 것이 시급함
- 본 과제에서는 안전한 5G 특화망 도입 및 구축을 위한 보안 고려사항 연구를 통하여 5G 특화망 도입을 계획하는 기업들에게 기술 적용 참조 가이드 및 보안 요구사항들을 도출하는 것을 목표함

3. 연구의 구성 및 범위

○ 본 과제의 구성 및 범위는 다음과 같음

- 국내외 5G 특화망 도입 및 적용 사례 분석 연구
- 5G 특화망 무선 액세스 및 기지국 보안 고려사항 연구
- 5G 특화망 적용 기술 유형 및 기술별 보안 고려사항 연구
- 5G 특화망 도입 기업 보안 고려사항 연구

4. 연구 내용 및 결과

○ 본 과제의 추진 내용은 다음과 같음

- 국내외 5G 특화망 도입 및 적용 사례 분석 연구
  - 5G 특화망 개요 및 현황
  - 5G 특화망 도입 사례
  - 5G 특화망 적용 사례 분석

- 5G 특화망 무선 액세스 및 기지국 보안 고려사항 연구
  - 무선 RAN 구간 보안 위협
  - 5G에서의 허위 기지국 대응 주요 이슈
  - 5G에서의 허위 기지국 공격 대응 방안

- 5G 특화망 적용 기술 유형 및 기술별 보안 고려사항 연구
  - 5G 공통보안 위협
  - 5G 네트워크 구간별 보안 위협
  - MEC 및 네트워크 슬라이싱 기술 및 보안 동향 분석
  - AKMA(Authentication and Key Management for Application)

- 5G 특화망 도입 기업들이 고려해야 할 보안 요구사항 연구
  - 5G 특화망 보안 위협 분석
  - 5G 특화망 도입시 고려해야 할 보안 영향 요소

- 5G 특화망 구축 유형별 보안 고려사항
- 5G 특화망 구성요소별 보안 요구사항

▪ 5G 특화망 보안 고려사항
- 5G 특화망 연결 기기 보안 고려사항
- 5G 특화망 연동 구간 및 네트워크 보안 고려사항
- 5G 특화망 네트워크 통신 장비 보안 고려사항
- 5G 특화망 MEC 및 어플리케이션 보안 고려사항

○ 본 과제에서는 안전한 5G 특화망 도입 및 구축을 위한 보안고려사항 연구를 통하여 5G 특화망 도입을 계획하는 기업들에게 기술 적용 참조 가이드 및 보안 요구사항들을 정리한 4건의 기술 문서 그리고 비SCI논문 1편을 제출함

▪ 기술문서: 4건
- 국내·외 5G 특화망 도입 및 적용사례분석
- 5G 특화망 구축 유형별 및 구성 요소별 보안 고려사항
- 일본 및 유럽의 5G 특화망 보안 고려사항
- 5G 특화망 도입 기업들이 고려해야 할 보안 요구사항 분석

▪ 비SCI논문: 1편
- “5G 특화망의 성공적 정착을 위한 보안고려사항 연구”, 정보기술융합공학 논문지

5. 정책적 활용 내용

○ 국내 실정에 적합한 5G 특화망 보안 고려사항을 제시하여 실질적인 5G 특화망 도입에 기여

○ 5G 특화망 환경의 전반적인 보안 고려사항을 다룸으로써 5G 생태계 활성화에 기여

○ 관련 정책 및 법 개정을 위한 정책 자료로 활용

6. 기대효과

○ 경제·산업적 측면

- 제조업 외 문화예술, 에너지, 교육, 공공분야 등 5G 특화 서비스가 다양한 형태로 제공·발굴됨으로써 국내 5G 산업생태계가 활성화되고 국민의 삶의 질 향상 및 국가경쟁력 강화 등의 다양한 파급효과 기대
- 국내 환경 및 기업에 적합한 5G 특화망 도입을 위한 가이드라인 마련에 활용
- 5G 특화망을 활용한 미래 신산업 육성을 위한 정보보호 핵심원천 기술기획을 위한 기반

○ 사회적 측면

- 5G 특화망 기반 서비스에 대한 위협을 사전에 분석하고 보안 고려사항을 제시하여 이로 인한 사회적 혼란 및 재산 피해를 최소화
- 5G 특화망 도입 및 적용 사례 및 보안 고려사항을 제공하여 5G 특화망 도입을 원하는 사용자에게 보안 필요성을 제고

SUMMARY

1. Title

A Study on Security Considerations for the Adoption and Deployment of a Secure 5G Private Networks

2. Objective and Importance of Research

❍ The Objective and Importance of this project are as follows

- Along with intensifying competition to secure leadership in the 5G network, which will become the standard technology of the global mobile communication network industry, supply dedicated frequencies for 5G private networks in major countries around the world and create a service environment in various fields.

- 5G private network is a 5G network that can be used only in a specific area (building, factory, etc.), and is a customized network specialized for the service to be introduced in that area. Build stand-alone or connected to public network.

- The Ministry of Science and ICT announced the 5th generation (5G) private network policy plan (January, ´21) and supply plan (June, ´21) and suplied 4.7Ghz/28Ghz band frequencies.

- Security technology research is required as a prerequisite for the success of 5G private networks and related government policies.

- In particular, it is urgent to support the systematic establishment of safe 5G private network security by presenting security considerations suitable for 5G specialized network to domestic 5G specialized network introduction companies

and related organizations.

- Therefore, this task aims to derive technology application reference guides and security requirements for companies planning to introduce 5G private networks through research on security considerations for the introduction and establishment of safe 5G private networks.

3. Contents and Scope of the Research

❍ The composition and scope of this project are as follows

- Domestic and overseas 5G private network introduction and application case analysis study
- Research on 5G private network radio access and base station security considerations
- 5G private network applied technology types and security considerations for each technology
- Research on security considerations for companies introducing 5G private networks

4. Research Results

❍ The contents of this project are as follows.

- Domestic and foreign 5G private network introduction and application case study
  - 5G private network overview and current status
  - 5G private network introduction case
  - 5G private network application case analysis

- Research on 5G private network radio access and base station security considerations

- Security threats in the wireless RAN section
- Key issues in dealing with false base stations in 5G
- Countermeasures against false base station attacks in 5G

▪ Research on technology types applied to 5G private networks and security considerations for each technology
- 5G Common Security Threats
- Security threats by 5G network section
- MEC and network slicing technology and security trend analysis
- AKMA (Authentication and Key Management for Applications)

▪ Research on security requirements to be considered by companies introducing 5G private networks
- 5G private network security threat analysis
- Security impact factors to be considered when introducing 5G private networks
- Security considerations for each type of 5G private network construction
- Security requirements for each 5G private network component

▪ 5G private network security considerations
- Security considerations for devices connected to 5G private networks
- 5G private network linking section and network security considerations
- 5G private network network communication equipment security considerations
- 5G private network MEC and application security considerations

❍ In this task, through research on security considerations for the introduction and establishment of a safe 5G private network, four technical documents were prepared that summarized the technology application reference guide and security requirements for companies planning to introduce a 5G private network. In

addition, one non-SCI thesis was submitted.

- The technical documents : 4
  - Domestic and foreign 5G private network introduction and application case analysis
  - Security considerations by 5G private network construction type and component
  - Security considerations for 5G private networks in Japan and Europe
  - Analysis of security requirements to be considered by companies introducing 5G private networks
- Non-SCI Papers : 1
  - "Study on Security Considerations for Successful Settlement of 5G private Network", Journal of Information Technology and Applied Engineering(JITAE)

5. Policy Suggestions for Practical Use

○ Contributing to the introduction of a practical 5G private network by presenting 5G private network security considerations appropriate to the domestic situation

○ Contribute to vitalizing the 5G ecosystem by addressing overall security considerations in the 5G private network environment

○ Use as policy data for related policy and law revision

6. Expectations

○ Economic and industrial aspects

- Various types of 5G-private services, such as culture/art, energy, education, and public sectors, in addition to manufacturing, are provided and discovered, activating the domestic 5G industrial ecosystem and expected to have various ripple effects such as improving the quality of life of the people and strengthening national competitiveness. Used to prepare guidelines for introducing 5G private networks suitable for domestic environment and businesses

- Foundation for planning core source technology for information protection to foster future new industries using 5G private networks

❍ Social aspect

- Preliminary analysis of threats to 5G private network-based services and presenting security considerations to minimize social disruption and property damage
- Increase security needs for users who want to introduce 5G private networks by providing cases of introduction and application of 5G private networks and security considerations

CONTENTS

제 1 장 국내외 5G 특화망 도입 및 적용 사례 분석 연구

제 1 절 5G 특화망 개요 및 현황

1. 5G 특화망 개요

본 장에서는 5G 특화망에 대한 정의 및 현황을 살펴보기 위해서 특화망에 대한 기본 개념에 대해서 우선적으로 살펴보고자 한다.

최근 국내외 5G 기술 도입의 확산으로 LTE 망으로 제공하지 못하는 5G 만의 높은 전송 속도, 낮은 지연시간, 넓은 대역폭을 산업계에서 활용하고자 하는 요구가 증가하고 있다. ITU-R에서 정의하고 있는 5G 기술의 요구사항은 다음을 만족시켜야 한다. 첫째, 1Gbyte의 컨텐츠를 10초에 다운로드 할 수 있어야 한다. 이를 위해 5G 기지국에서는 TDD 무선 기술을 채용하고 있다. 두 번째는 1km2 반경 내 최대 100만개의 사물과 연결할 수 있어야 한다. 이는 기존 LTE에서 제공하던 20Mhz 의 대역폭과 비교하여 5G 망에서는 1GHz의 대역폭을 제공하고 있다. 세 번째는 1ms 의 최소 지연시간을 보장해야 한다. 이를 위해 5G 기지국은 CU와 DU를 분리되었고, MEC를 활용하는 구조가 제안되었다.

이런 특성들을 잘 활용할 수 있는 서비스 또한 출시될 것으로 기대되고 있다. 스마트 공장으로 대표되는 제조, 생산 서비스 뿐만 아니라 교통, 수송, 에너지, 자원 등의 산업에도 활용될 것으로 보인다. 또한 5G 기술을 산업계에 적극적으로 융합시킬 수 있는 맞춤형 네트워크로서 5G 특화망은 특정지역 서비스에 특화된 서비스를 제공한다. 5G 특화망은 사설망, 지역망, 기업망, NPN 등으로도 불리는데 국내에서는 과학기술정통부에서 “이음5G” 라는 명칭으로 정의하고 관련 정책 및 전략을 추진 중에 있다.

<표 1-1> 에 비교되어 있는 바와 같이, 기존 5G 망은 특정 사업자가 할당받은 주파수를 통해 전국 단위 대규모 네트워크를 구축하여 대국민 서비스를 제공하는 반면, 5G 특화망은 수요기업 또는 사업자가 건물이나 시설 등 제한된 범위 내에서 5G 서비스를 적용하기 위해 기업 맞춤형으로 무선 네트워크 구축이 가능하다.

<표 1-1> 5G 이동통신과 특화망 비교

구 분		5G 이동통신	5G 특화망
서비스 시장 측면	서비스 범위	전국	토지/건물
	사업자 수	소수(3개)	다수
네트워크 구축 측면	주파수 이용	전국적 주파수 사용	지역적 공동사용
	주파수 수요	경합성 높음	경합성 낮음
	설비 투자 규모	대규모 투자 필요	소규모 투자 가능
통신망 이용 측면	주 공급자	이동통신 사업자	수요기업·기관(자가망 형태)
	주 사용자	이동통신 가입 소비자(개인·기업)	수요기업·기관 및 서비스 이용 고객
	주요용도	음성, 데이터 등 전송	다양(수요기업·기관 활용형태에 따라)

자료: 과학기술정통부·KCA, 5G 특화망 가이드라인(2021)

수요기업은 행정적 신청절차를 통해 4.7GHz, 28GHz 대역의 특화망 주파수를 지정 또는 할당받아 다양한 분야에서 특화망 통신 네트워크를 구축할 수 있다.

2. 5G 특화망 구축 현황

국내에서는 '22년부터 이음5G 1호 기간통신사업자로서 네이버 클라우드가 성남시 분당 소재 사옥인 '1784'에 ARC 플랫폼 브레인리스 로봇 제어를 위해 5G 특화망을 적용했다. ARC 로봇 '쿠키'는 본체 내 프로세서 탑재를 최소화하고, 클라우드망으로 중앙 서버와 실시간 연결해 AI 기반으로 각종 데이터를 처리하고 제어한다. 또한 건물 내 수백대의 로봇이 데이터를 공유하며 이용자에 필요한 정보를 동시에 공유하며 자율주행 경로를 실시간으로 제어한다. 이를 통해 빌딩 내 이용자들에게 택배, 음식물 배달, 수거 등 서비스를 제공한다. 1784에는 자율주행로봇인 '쿠키' 뿐아니라 얼굴인식을 통한 시설 이용 시스템 '클로바 페이스사인', '네이버웍스 앱'을 통한 온도, 조명, 환기, 식음료 주문 등 다양한 서비스를 제공하고 있다.

LG CNS는 5G 특화망을 LG이노텍 구미2공장에 구축하고 있다. 인공지능 비전 카메라를 통한 불량품 검사와 무인 운반차량 운용, 작업자에게 가상현실(VR), 증강현실(AR) 도면 제공 등의 서비스를 제공할 계획이다. LG CNS 또한 기간통신사업자로서 LG이노텍 등을 통해 확보한 경험을 바탕으로 스마트 팩토리 사업을 다양화할 예정이다.

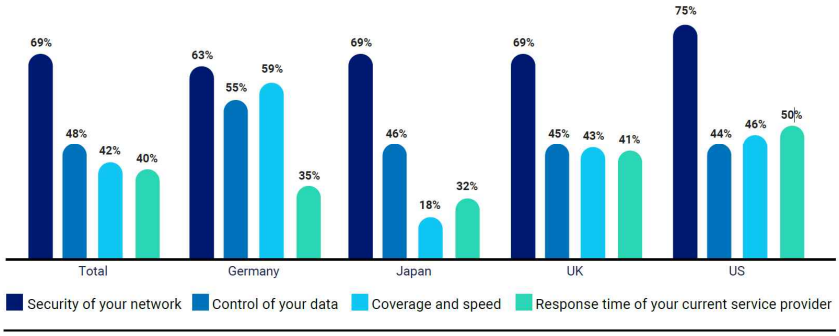
SK네트웍스서비스는 센트럴 창원공장 내에 5G 특화망을 구축한다. 자율이동로봇(AMR) 운용으로 공장물류를 자동화하고, 디지털트윈 기반 공장 관리, 관제 서비스로 실시간 제조공정을 모니터링하고 시뮬레이션하여 유연한 생산체계를 구현하고 있다.

해외에서는 ‘20년부터 독일과 일본, 영국 등이 5G 특화망을 구축하기 시작했다. 독일의 제조사 보쉬는 ’20년 8월 로이틀링겐에 위치한 자사 반도체 공장에 5G 특화망 구축을 시작하고 11월부터 운영하기 시작하였다. 3.7~3.8GHz 대역을 사용하고 단독모드 망을 갖추었으며, 공장 내 무인 이동로봇(AGV)과 고정형 제조설비 연결 및 자동화를 통한 스마트 팩토리를 구축하였다. 또한 독일 항공사 루프트한자 항공기 정비계열사인 루프트한자 테크닉은 ‘20년 2월 함부르크에 있는 항공기 격납고에서 3.7GHz 대역을 사용, 단독모드 망을 갖춘 5G 특화망을 운영하기 시작하였다. 이를 통해 기술자들은 대용량의 CAD 데이터를 현장에서 모바일로 빠르게 다운받을 수 있고, 고해상도 가상 및 증강현실 기술을 사용하여 항공기 동체에서 더욱 정밀하게 작업할 수 있다. 격납고 뿐만 아니라 항공기 동체 내부에서도 끊김 없는 네트워크 사용이 가능하여 루프트한자의 전반적인 유지보수 운영에 통합되어 사용되고 있다.

일본의 IT기업 후지쯔는 ‘21년 3월 일본 오야마 공장에서 5G 특화망 운영을 시작하였다. 4.7GHz 대역의 단독모드와 28GHz 대역의 비단독모드 방식으로 네트워크를 구성하였다. 4.7GHz 대역은 광범위한 제어가 필요한 AGV 자율주행 시스템에 도입했고, 28GHz 대역은 대용량 이미지 및 영상의 고속 전송이 필요한 AI 작업 이미지 검수 시스템에 적용하였다. 또한 ’21년 3월 도쿄도립대학은 도쿄 미나미 오사와 캠퍼스와 히노 캠퍼스에 5G 특화망 운영을 시작하였다. 28GHz 대역을 사용하고 비단독모드 방식을 통해 실내 부분서비스를 시작으로 4.7GHz 대역을 통한 광역 커버리지를 구축하였다.

영국의 경우 ‘21년 2월 케임브리지 와이어리스와 화웨이는 케임브리지 사이언스 파크에 5G 특화망을 구축하였다. 사이언스 파크 내 5G 사설망은 테스트베드 용도로 사용되며, 혁신 기업들이 5G 관련 융합서비스를 테스트하는데 사용하고 있다. 또한 ’18년 3월 리버풀 켄싱턴 지역에서 ‘리버풀 5G 크리에이트’ 프로젝트의 일환으로 지역사회를 위한 헬스케어, 사회 복지 등 시민들을 위한 5G 서비스를 위해 5G 특화망 테스트운영을 시작하여 ‘20년 1월 종료하였다. 이런 사례들을 통해 430만 파운드(한화 68억)를 추가지원 받았으며, ’22년 3월까지 추가로 테스트운영을 연장하였다.

[그림 1-1] 국가별 기업들의 5G 특화망 구축 고려사항



자료: NTT, Private 5G: rising adoption collides with CIOs' security concerns, White paper(2022)

참고로 [-1] 과 같이 일본 최대 통신사인 NTT에서 '22년에 국가별로 기업들이 5G 특화망 구축시 어떤 부분들을 고려하는지에 대한 조사를 진행하였고, 보안성이 가장 큰 고려사항으로 나타났다. 이로인해 대부분의 5G 특화망이 테스트베드 형태로 구축되었다.

제 2 절 5G 특화망 도입 사례

1. 5G 특화망 적용 구조 분석

5G 이동통신 기반 제조업 고도화를 추진하는 협업체인 5G ACIA 에서는 특화망 구축 방식에 따른 4가지 시나리오를 제시한다.

첫 번째인 독립형 전개 모델은 특화망이 5G 인프라 및 기타 MEC 등을 모두 독립적으로 구축하여 높은 수준의 보안 및 안정성을 제공할 수 있는 형태이다. 두 번째, 무선 액세스 공유 모델은 5G RAN 부분을 상용 이동통신망과 함께 운용하는 방식을 말한다. 세 번째는 무선 액세스 및 제어부 공유 모델로 5G RAN 외에 제어부를 상용 이동통신망과 함께 운용하여, 공중망의 네트워크 제어를 따른다. 네 번째는 이동통신사 호스팅 방식으로 5G 특화망 트래픽을 공중망을 통해서 전달받는 방식을 말한다. 특화망은 업체나 사업자들 전용의 자체 전용망을 구축할 수 있는 기술로, 구축을 원하는 업체나 사업자가 4가지 시나리오 중 적절한 방식을 선택하여 서비스를 제공할 수 있다.

<표 1-2> 5G 특화망 4가지 시나리오

네트워크 유형		설명
독립형	1. 독립형 전개 모델 (Deployment as isolated network)	독립적인 5G 기지국과 5G 핵심설비(게이트웨이, 이용자 DB 등)를 자체 구축
공용 네트워크와 연결	2. 무선 액세스 공유 모델 (Deployment with shared RAN)	Private 5G RAN 장비를 공용 네트워크를 운용하는 MNO와 공유
	3. 무선 액세스 및 제어부 공유 모델 (Deployment with shared RAN & control plane)	기지국 공유 모델의 RAN 뿐만 아니라 네트워크 제어부 (control plane)도 MNO와 공유. MNO가 실질적인 네트워크의 제어를 수행
	4. 이동통신사 호스팅 방식 (NPN deployed by public network)	Private 5G 운용 구역 내에서 발생하는 모든 5G 트래픽을 외부의 공중망 사업자에게 전송한 후, private 5G 트래픽은 private 5G 운용자에게 보내는 방식

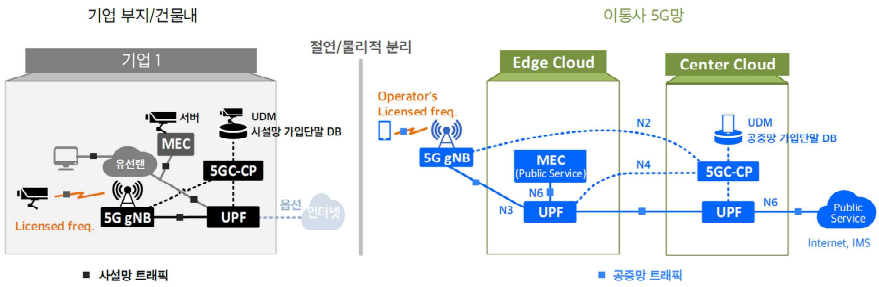
자료: 5G-ACIA, 5G Non-Public Networks for Industrial Scenarios, White Paper(2019)

(1) 독립형 전개 모델

독립형 전개 모델은 기업 등이 소유한 무선망과 코어망을 구성하여 5G 특화망을 구축하는 방식이다. 해당 그룹이나 기업의 가입자만 전용으로 5G 특화망 서비스를 사용할 수 있다. 독립형 5G 특화망은 PLMN 식별자와 특화망 식별자가 결합된 정보를 참조하여 구분된다. 여기서 PLMN 식별자는 이동통신망을 식별하는 정보이고, 특화망

식별자는 글로벌하게 유일한 값 또는 PLMN 내부에서 유일한 값이다. 독립형 전개모델은 [그림 1-2] 와 같이 기업 또는 그룹 소유의 특화망을 통하여 5G 특화망 서비스를 제공하며, 서비스의 특성을 고려하여 하나 또는 하나 이상의 네트워크 슬라이스로 분리하여 서비스를 제공할 수 있다. 여기서 5G 특화망 운영자는 일반적으로 해당 기업 또는 이동통신 사업자일 수 있으며, 5G 장비 제조업체가 운영자인 경우도 있다.

[그림 1-2] 독립형 전개 모델



자료: Netmanias, Private 5G Networks 구축 방안(2019)

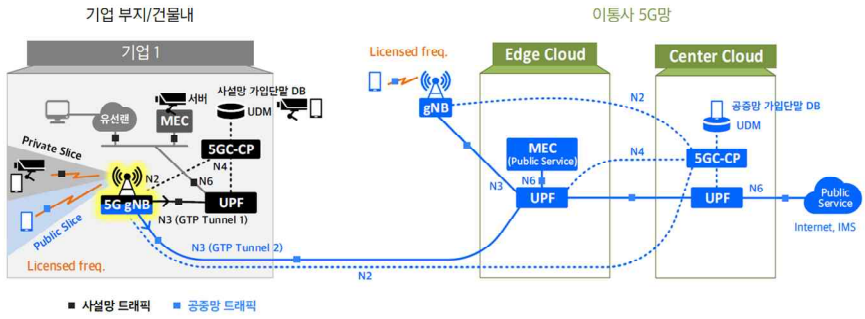
- 보안 : 사설망이 공중망과 물리적으로 분리되어 있어 완벽한 데이터 보안 제공
- 초저지연 : 단말과 응용 서버간 네트워크 지연이 수ms이내이기 때문에 URLLC 응용 서비스 구현 가능
- 서비스 장애 : 이동통신사의 서비스 장애와 무관하게 독립적으로 대응
- 구축비용 : 다른 모델에 비해 가장 비용이 높음

(2) 무선 액세스 공유 모델

무선 액세스 공유 모델은 이동통신사의 무선망과 특화망의 코어망을 결합한 형태로 기업 등의 허락을 받은 단말만 5G 특화망 서비스를 받을 수 있다. 무선 액세스 공유 특화망은 PLMN 식별자를 참조하여 네트워크를 선택하고 그룹 식별자를 참조하여 CAG 셀을 선택한다. 여기서 그룹 식별자는 3GPP NPN 표준에서 CAG 식별자를 의미한다. CAG는 CAG 셀의 식별자로서 5G 특화망에 접속하는 그룹을 식별하는 정보이다. 무선

액세스 공유 모델은 [그림 1-3] 과 같이 기업 등에 존재하는 기지국만 특화망과 공중망간에 공유된다. Private 슬라이스에 속한 단말들의 데이터 트래픽은 기업 내 전용 UPF로 전달되며, Public 슬라이스에 속한 단말들의 데이터 트래픽은 이동통신사 엣지 클라우드에 있는 UPF로 전달된다. 즉, 기업 내 기기 제어 데이터 등과 같은 특화망 트래픽은 기업 내에서만 머무르며, 전화와 인터넷과 같은 공중망 서비스 트래픽은 이동통신사 망으로 전달된다. 여기서 Private 슬라이스는 5G 특화망 구축 기업 등에서만 사용하는 네트워크 슬라이스를 의미하며, 3GPP 표준에서 정의되었다.

[그림 1-3] 무선 액세스 공유 모델



자료: Netmanias, Private 5G Networks 구축 방안(2019)

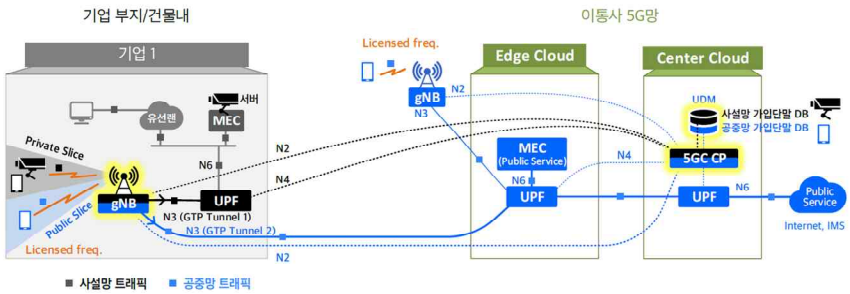
기지국이 논리적으로만 분리되어 있으나 무선망 레벨에서 특화망 내 데이터 정보를 수집하는 것은 거의 어려워 기업 내 특화망 데이터 트래픽 보안도 우수하다고 볼 수 있다. 특히 코어망이 기업 내에 따로 구축되어 있어, 특화망 단말들의 가입정보와 운영 정보가 사내에 저장, 관리되므로 기업 외부에 유출되지 않는다. 기업 내에 UPF와 MEC가 위치하여 초저지연 통신을 제공하고 URLLC 응용 서비스 구현이 가능하다.

(3) 무선 액세스 및 제어부 공유 모델

무선 액세스 및 제어부 공유 모델은 이동통신사의 무선망 및 코어망을 공유하는 형태로 기업 등의 허락을 받은 단말만 5G 특화망 서비스를 받을 수 있다. 무선 액세스 및 제어부 공유 특화망은 PLMN 식별자를 참조하여 네트워크를 선택하고 그룹

식별자를 참조하여 CAG 셀을 선택한다. 여기서 그룹 식별자는 3GPP NPN 표준에서 CAG 식별자를 의미한다. CAG는 CAG 셀의 식별자로서 5G 특화망에 접속하는 그룹을 식별하는 정보이다. 무선 액세스 및 제어부 공유 모델은 [그림 1-4] 와 같이 기업 등에 존재하는 기지국과 이동통신사 공중망 내 코어망 중 CP와 UDM이 공유된다. 특화망과 공중망 간에 기지국, CP, UDM은 논리적으로 분리되며, UPF와 MEC는 물리적으로 분리된다. Private 슬라이스에 속한 단말들의 데이터 트래픽은 기업 내 전용 엣지 클라우드에 있는 UPF로 전달되며, Public 슬라이스에 속한 단말들의 데이터 트래픽은 이동통신사 엣지 클라우드에 있는 UPF로 전달된다. 즉, 기업 내 기기 제어 데이터 등과 같은 특화망 트래픽은 기업 내에서만 머무르며, 전화와 인터넷과 같은 공중망 서비스 트래픽은 이동통신사 망으로 전달된다.

[그림 1-4] 무선 액세스 및 제어부 공유 모델



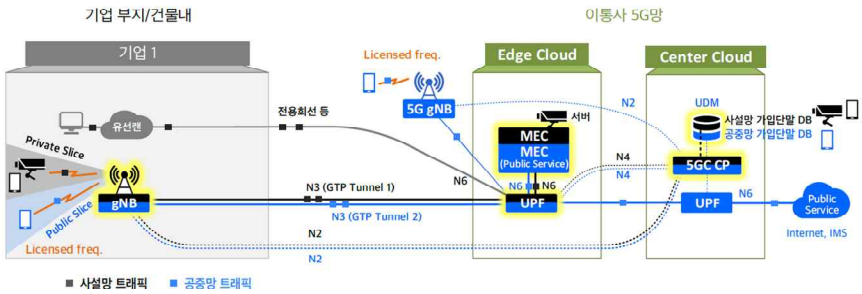
자료: Netmanias, Private 5G Networks 구축 방안(2019)

기지국이 논리적으로만 분리되어 있으나 무선망 레벨에서 특화망 내 데이터 정보를 수집하는 것은 거의 어려워 기업 내 특화망 데이터 트래픽 보안도 우수하다고 볼 수 있다. 다만 특화망 단말들의 가입정보와 운영 정보가 사내가 아닌 이동통신사 망에 저장, 관리되므로 보안상 우려사항이 존재한다.기업 내에 UPF와 MEC가 위치하여 초저지연 통신을 제공하고 URLLC 응용 서비스 구현이 가능하다.

(4) 이동통신사 호스팅 방식

이동통신사 호스팅 방식은 이동통신 사업자가 소유한 무선망과 코어망에 네트워크 슬라이싱을 적용하여 5G 특화망 서비스를 제공한다. 이동통신사 호스팅 방식은 S-NSSAI 또는 S-NSSAI와 DNN이 결합한 정보를 참조하여 선택된다. 여기서 S-NSSAI는 네트워크 슬라이스를 선택하는 정보이며, DNN은 DN을 표시하는 이름으로서 단말이 요청한 서비스 네트워크 이름을 표시한다. 일반적으로 하나의 네트워크 슬라이스는 다수의 DNN을 포함할 수 있다. 5G 공중망은 이동통신사업자가 소유하고 운영하는 망이며, 면허 주파수를 사용하므로 기본적으로 특화망 서비스와 공중망 서비스를 제공하는 절차는 동일하다. 공중망 기반 5G 특화망은 기업 등이 전용으로 사용하는 Private 슬라이스를 통해 5G 특화망 서비스를 제공하며, 협약한 서비스의 특성을 고려하여 다수의 네트워크 슬라이스를 생성할 수 있다. 단말은 PLMN 레벨의 기본 인증과 네트워크 슬라이스 레벨의 추가 인증을 통과하면 5G 특화망 서비스를 받을 수 있다.

[그림 1-5] 이동통신사 호스팅 방식



자료: Netmanias, Private 5G Networks 구축 방안(2019)

기업 내에는 기지국만 구축하고 엣지 클라우드 및 코어 클라우드는 이동통신사에 존재한다. 특화망과 공중망이 5G 망 전체를 논리적으로 분리하여 공유한다. 기업 내에는 기지국 밖에 없기 때문에 기업 내 특화망 단말과 LAN 단말간 트래픽 전달 경로가 없다. 데이터 트래픽이 이동통신사 에지 클라우드에 있는 UPF 까지 올라갔다가

전용회선 등을 통해 다시 기업 내로 내려와야하기 때문에, 기업과 이동통신사 에지 클라우드간 거리에 따라 네트워크 지연 문제가 발생할 수 있다. 또한 특화망 단말의 트래픽이 기업을 벗어나 공중망까지 전달되므로 데이터 트래픽 보안에 우려가 발생한다. 또한 특화망 단말들의 가입정보와 운영 정보가 사내가 아닌 이동통신사 망에 저장, 관리되므로 보안상 우려사항이 존재한다.

살펴본 5G 특화망 구축방식에 따른 4가지 시나리오를 종합해보면 독립구축, 일부공유, 전부공유 등 3가지로 압축할 수 있는데 이때 3가지 구성방식의 특징을 살펴보면 다음과 같다.

먼저 독립구축은 내부 5G 특화망 운용 전담인력 구성이 가능한 기업에 적합한 모델이다. 기지국과 코어망, MEC를 사업장 내 별도로 구축하여 전송지연·성능 등을 향상시키고 보안성을 제공하는 사업장 특화된 네트워크를 구축할 수 있다. 따라서 데이터 저장·관리에 민감한 사업장에 적합한 방식이다.

두 번째 일부공유는 5G 특화망 사업장 내 기지국과 코어망의 UP, MEC를 특화망 서비스 플랫폼으로 구축하는 모델이다. 이동통신사 코어망의 CP를 공유하기 때문에 코어망 구축 및 운영, 유지보수 비용 부담이 완화될 수 있다.

세 번째 전부공유는 5G 특화망 사업장 내 기지국만 설치하는 모델이다. 이동통신사 코어망 전부를 활용하기 때문에 보안성이 떨어지지만 중소 규모의 경제성 있는 특화망 구축이 가능하다. 또한 이동통신사와의 거리에 따라 데이터 트래픽 지연이 발생할 수 있다.

<표 1-3> 5G 특화망 구축 방식별 특성

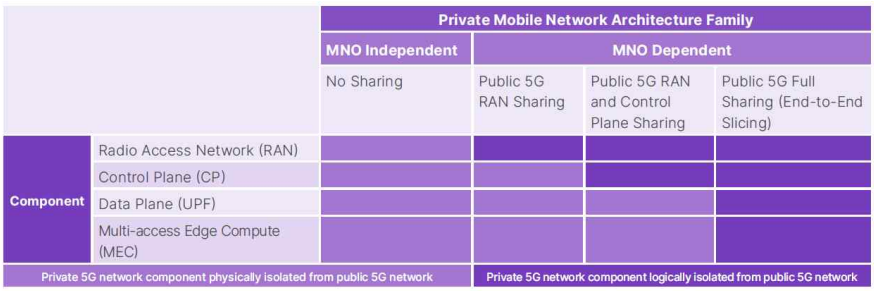
구 분	데이터 관리	유지보수 인력	비용절감	보 안	정기 사용료	QoS보장	서비스 지연 최소화
5G코어 독립구축	◎	◎	△	◎	◎	◎	◎
5G코어 일부공유 (CP한정)	○	△	○	○	○	○	◎
5G코어 전부공유	△	△	◎	△	△	○	△

자료: 과학기술정통부·KCA, 5G 특화망 가이드라인(2021)

2. 5G 특화망 구축 사례 분석

5G 특화망은 기업별 요구사항을 만족하면서 자체적으로 관리와 제어가 가능한 기술이다. 이는 이동통신사가 아닌 일반 기업들이 공공 5G 인프라와 서비스를 독립적으로 구축할 수 있는 기회를 가지게 되었다고 볼 수 있다. 기업들이 5G 특화망을 구축할 때 선택 가능한 이동통신사에 독립적인 모델 또는 의존하는 모델은 [그림 1-6] 과 같이 네트워크 구성 요소들을 얼마나 공유하는지에 따라 구분된다.

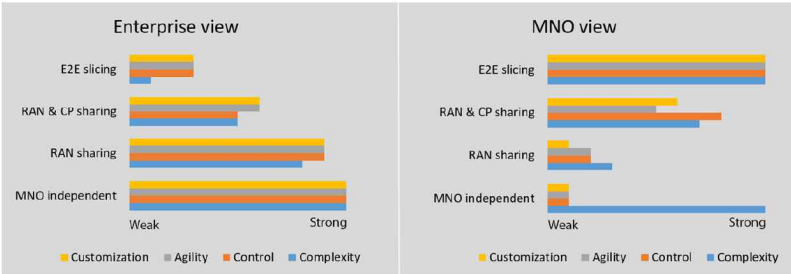
[그림 1-6] 5G 특화망 구성요소와 구축 모델별 관계



자료: Fortinet, Securing 5G Private Mobile Network, White paper(2021)

따라서 공중망 네트워크 리소스에 대한 의존도는 [그림 1-7] 과 같이 기업들과 이동통신사 모두의 복잡성과 유연성, 그리고 제어가능성에 영향을 미친다. 이러한 영향도는 기업과 이동통신사에 따라 다를 수 있지만, 5G 특화망을 구축하려는 기업이 특화망 모델을 선택할 때 매우 중요한 요소로 작용한다.

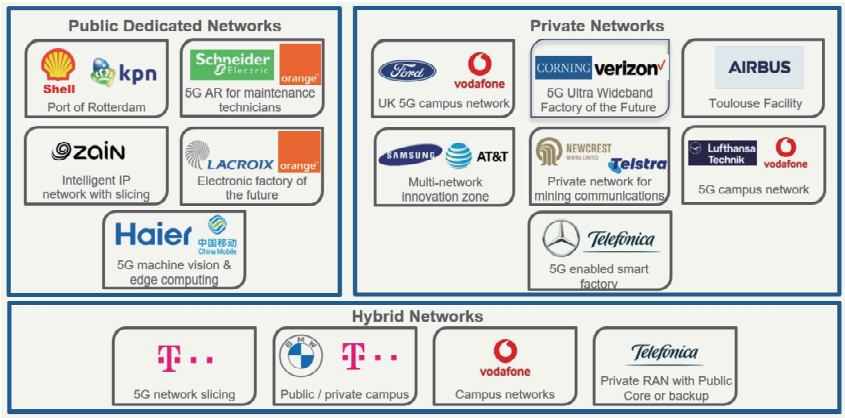
[그림 1-7] 기업과 이동통신사의 5G 특화망 구축 모델별 특성 영향도



자료: Fortinet, Securing 5G Private Mobile Network, White paper(2021)

특히 해외에서는 기업별로 5G 특화망 구축 모델을 다르게 운영하는 것으로 조사되었다. GSMA에서 조사한 자료에 의하면 '18년 11월 네덜란드의 글로벌 정유회사인 Shell은 로테르담 소재 항만 화학 정유 공장설비에서 설비 유지보수를 위해 이동통신사에 의존도가 높은 이동통신사 호스팅 방식을 사용한 특화망을 테스트하였다. 반면 독일의 에어버스, 루프트한자, 벤츠 등에서는 독립형 전개 모델을 사용한 특화망을 구축하였다. 그리고 독일의 BMW 등에서는 공유 모델을 사용한 특화망을 구축하였다.

[그림 1-8] 5G 특화망 적용 모델별 구축 사례



자료: GSMA, 5G IoT Private & Dedicated Networks for Industry 4.0(2020)

또한 해외 특화망 구축사례를 활용 목적, 서비스 분야 등을 고려하여 1) 기업 내

사업장의 자체 수요를 위한 통신망 구축, 2) 특화망 시장 공략, 3) 새로운 유형의 기간 통신사업 확보, 4) 혁신을 위한 연구개발 분야 등 4가지 유형으로 분류할 수 있다.

(1) 기업 내 사업장의 자체 수요를 위한 통신망 구축

독일의 경제기술부 산하 BNetzA는 '19년 11월부터 3.7~3.8GHz 대역의 특화망 주파수 할당 절차를 시작하였다. 또한 '21년 1월부터 26GHz 대역의 특화망 주파수 할당 절차를 개시하였다. 이에 자동차 제조기업인 BMW는 독일 정부부처의 지원을 받아 3.7~3.8GHz 대역의 특화망 주파수 면허를 획득하였다. 이를 통해 자국 통신 SW 업체인 M3connect 및 Stäubli WFT 와 연구 컨소시엄을 구성하였으며 Industry 4.0 표준 구현을 위하여 3개년 프로젝트를 수행하고 있다. BMW 그룹의 Industry 4.0 솔루션은 조립 알고리즘 분석, VR 기능을 활용한 실시간 3D 환경 및 시나리오 조성, 스마트 운송 로봇, 유통 경로 연결 등을 포함한다. 또한 그룹 최대 규모의 공장인 바이에른 주 딩골핑 공장 부지에 M3connect가 5G 특화망을 구축하고, Stäubli WFT는 자율 이동이 가능한 운송 솔루션의 개발 및 생산을 담당하였다. BMW는 딩골핑 공장을 5G 특화망 테스트베드로 활용하여 장기적으로 전세계 모든 자사 공장에 5G 망을 구축할 계획이다.

독일의 국영 항공사 루프트한자의 자회사인 루프트한자 테크닉은 3.7-3.8GHz 대역 특화망 면허를 확보하여 함부르크 기지 내 항공기 격납고 및 엔진 공장에 5G 단독모드 방식의 특화망을 구축하였다. 또한 Vodafone과 협업하여 기지 내 루프트한자 항공기 격납고 8,500㎡를 커버하는 5G 단독모드 방식의 특화망을 구축하고, 5G 통신을 활용한 고해상도 AR·VR 기술을 통해 빈 항공기 동체에서 3D 객실 설계 데이터를 시각화하고, 이를 통해 구성 요소 확인 및 변경사항을 조정할 수 있는 환경을 구성했다. 그리고 노키아와 협업하여 기지 내 엔진 공장에 5G 단독모드 방식의 특화망을 구축하고, 영상 스트리밍을 통하여 실시간으로 엔진 메카닉과 협업하거나 원격으로 부품을 검사하는 등 민간 항공기 고객의 엔진 원격 검사 서비스 제공하였다.

[그림 1-9] 독일 루프트한자의 5G 특화망 구축 사례

자료: Lufthansa Technik, Lufthansa gets spectrum licence, deploys Nokia private 5G for remote engine checks(2020)

영국의 통신청 Ofcom은 ’19년 12월부터 3.8~4.2GHz 대역과 1800MHz 대역, 2300MHz 및 24.25~26.5GHz 대역의 특화망 주파수 할당 절차를 시작하였다. 이에 영국 전역의 21개 항구 및 Hams Hall 소재의 철도 화물 터미널을 보유·운영 중인 영국항만연합은 Business Radio 면허 77개, 고정 링크 25개, Shared Access 중출력 면허 7개 등 총 205개의 무선 면허를 확보하고 ‘21년 4월 Verizon Business와 계약을 체결하여 사우스햄프턴 항구에 5G 특화망을 구축하였다. 기존 네트워크를 단일로 통합함으로써 복잡성을 줄이고 터미널 통신의 안정성과 보안성 개선을 목표로, 5G의 특성을 활용한 새로운 기술 어플리케이션과 실시간 분석을 활용하여 향후 디지털 전환을 준비할 계획이다.

(2) 특화망 시장 공략

일본 총무성은 4.6~4.8GHz, 28.2~29.1GHz을 5G 특화망 주파수 대역으로 공급하고 있는데, 28.2~28.3GHz 면허 신청 접수를 ‘19년 12월에 개시하였으며, ’20년 12월에 주파수 대역을 확장하였다. 이에 일본의 장비 제조 및 정보 시스템 구축 업체인 후지쯔는 토치기현 오야마시와 가나가와현 가와사키시에 28㎓ 대역의 5G 특화망 주파수 면허를 확보하였다. ‘20년 3월에 주파수 면허를 취득한 후 자사 공장 부지에 5G 특화망을 구축하여 고화질 영상을 활용한 보안 시스템 검증 등을 수행하였다. ’20년 10월에는 고객사의 디지털화 가속을 위한 개인 무선 관리 서비스 및 개인 무선 클라우드

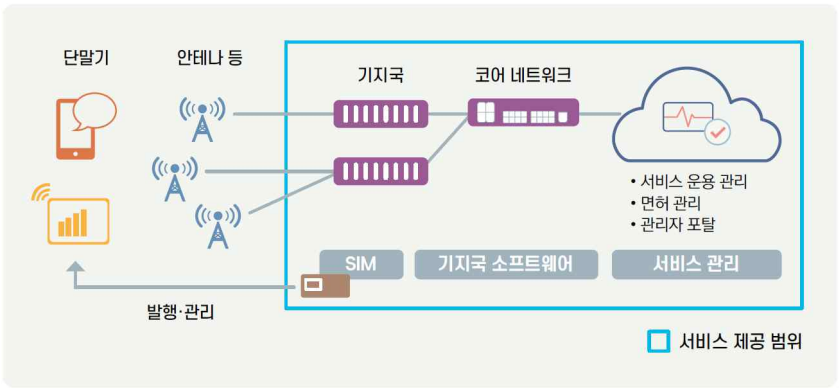
서비스 개시하였으며, 5G 특화망을 활용한 자영용 무선 시스템의 PoC, 면허 신청, 전파 측정, 설계 및 구축, 유지 보수 등 개인 무선 관리 서비스를 원스톱 서비스로 제공하고 있다.

[그림 1-10] 일본 후지쯔의 5G 특화망을 통한 개인 무선 관리 서비스 사례

출처: Fujitsu(2020), お客様のDXを加速するローカル5Gのサービスを提供開始

후지쯔는 기지국 및 코어 네트워크 SIM에 의한 통신 기능과 원격 감시, 장애 발생 시 기본 지원 등 서비스 관리 기능 제공하는 개인 무선 클라우드 서비스도 제공하고 있는데, 14개 기업과 5G 특화망 파트너십 프로그램을 위해 가와사키시 소재의 후지쯔 협력 연구소에 5G 특화망을 구축하고, 파트너 기업의 활용사례 창출과 솔루션 개발에 협력하고 있다.

[그림 1-11] 일본 후지쯔의 5G 특화망을 통한 개인 무선 클라우드 서비스 사례



출처: Fujitsu(2020), お客様のDXを加速するローカル5Gのサービスを提供開始 재구성

일본의 NEC(일본전기) 또한 ‘20년 11월 지자체 및 기업을 대상으로 5G 특화망 컨설팅, 통합(integration), 유지 관리 서비스를 개시하였다. 이를 위해 가와사키시 소재의 5G 특화망 연구소에 4.8GHz 대역 로컬 5G 무선국을 구축하고 고객사와의 공동창출(Co-creation)을 통해 5G 특화망 구축 사례를 적용하였다.

[그림 1-12] 일본 NEC의 5G 특화망 서비스 목록

기획·검증			설계·도입		운용감시·보수	
기획	요건정의	검증	시스템 설계	시스템 도입	운용감시	보수
컨설팅(consulting) 서비스			통합(intergration) 서비스		관리(managed) 서비스	
요건정의 지원 서비스 전파조사 서비스 5G 단말 검증 서비스 가치 검증 서비스			로컬 5G 구축 서비스 무선면허 취득 지원 서비스		운용 서비스 5G 코어 클라우드 서비스 기기 구독 서비스	

출처: NEC(2020), NEC, ローカル5Gをサービス型で提供開始

또한 일본의 기기 생산업체인 일본무선은 ‘21년 6월 나가노 사업소 부지 내에 4.7GHz 대역의 5G 특화망 주파수 면허를 확보하고, 해당 대역을 활용하는 5G 단독모드 방식의 제품 개발 및 실용화를 위해 활용할 계획이며, 향후 5G 특화망 관련 사업의 전개를 계획하고 있다. 특히 ’ 20년 12월에는 부지 내에 4.7GHz 대역의 6개 기지국을 개설하여 테스트에 활용하였다.

그리고 미국의 Verizon Business는 ‘20년 10월 노키아와 협력하여 유럽 및 아태지역 소재의 글로벌 기업대상으로 5G 특화망 플랫폼을 출시하였다.

(3) 새로운 유형의 기간통신사업 확보

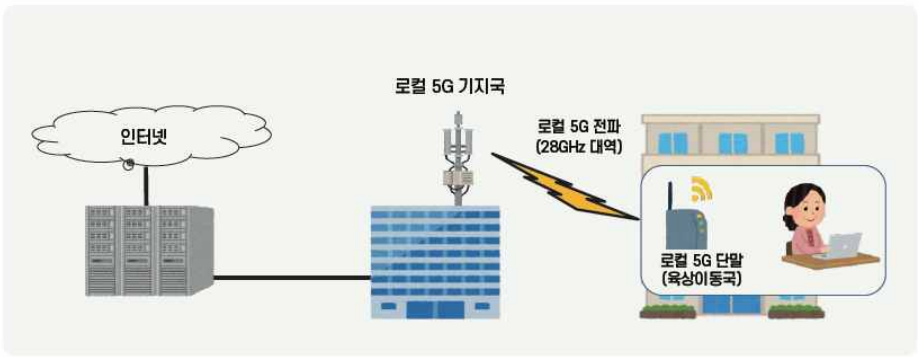
영국의 네트워크 사업자인 Dense Air는 지자체, 기업, MNO 등을 대상으로 통신사 중립적인 자체 스몰 셀 네트워크 운영하였다. Dense Air는 3.8-4.2GHz 대역 38개 및 2.3GHz 대역 15개 주파수 면허를 획득하였으며, 영국 외에도 아일랜드, 벨기에, 포르투갈, 뉴질랜드, 호주 등에 주파수 자원을 획득하였다.

Dense Air는 이동통신사에 중립적인 자체 스몰 셀 네트워크 인프라를 구축하고 4G 및 5G 모바일 네트워크의 고밀도화 및 확장 서비스를 제공하였으며, 여러 이동통신사

및 특화망이 함께 커버리지 및 용량을 보완할 수 있도록 하였다. 특히 아일랜드의 더블린 시의회와는 '18년 초부터 LTE 및 미래 5G 연결을 위한 대규모 인프라 프레임워크를 마련하고자 협력하고 있다. 또한, '19년 10월에는 더블린 소방대(Dublin Fire Brigade)와 협력하여 비상 대응 팀의 지휘 차량에 스몰 셀을 배치하고 지휘관이 드론을 통해 실시간으로 공중 시야를 확보하고 최초 대응자와 비디오 스트리밍을 지원하는 방법을 시연하였다.

일본의 도카이(東海) 지역 케이블 TV 및 광대역 사업자인 CNCI는 나고야시 히가시구 및 니시구에 28GHz 대역의 5G 특화망 주파수 면허를 확보하였다. '21년 가을에는 아파트 등 공동 주택과 사무실 빌딩을 무선으로 연결하는 로컬 5G 인터넷 서비스를 개시하였다. 5G 특화망 기지국과 서비스 건물 내의 모바일 라우터 기능을 가진 5G 특화망 단말을 28GHz 대역 주파수로 연결하고, 사용자들은 유무선 LAN을 통해 PC 또는 스마트폰으로 인터넷 서비스를 이용할 수 있도록 구성하였다.

[그림 1-13] 일본 CNCI의 5G 특화망을 통한 인터넷 서비스 사례



출처: 東海総合通信局(2020), CNCIに対して「ローカル5G」無線局の免許を付与

영국 도싯(Dorset)주의 Bournemouth, Christchurch 및 Poole 지역 지방 의회인 BCP Council는 Business Radio 면허 7개, CSR(Coastal Station Radio) International 면허 1개 및 1.8GHz 대역 및 3.8-4.2GHz 대역 Shared Access 면허 6개를 확보하였다. 또한 33만 파운드의 매칭펀드와 100만 파운드의 지역 성장 기금을 할당하여 Bournemouth의 Lansdowne 지역에서 5G 어플리케이션 및 장비 테스트가 가능하도록 한 파일럿

프로젝트인 Dorset Smart Place Pilot를 ‘19년 12월부터 ’ 21년 3월까지 진행하였다.

특히 Landsdowne 지역 내 IoT망 구축, 무료 공공 Wi-Fi 제공 등으로 신규 투자, 고용 및 혁신을 도모하고 도싯주의 로컬 제조업체가 실제 환경에서의 테스트를 통해 5G 기계의 생산을 가속할 수 있도록 지원하였다. 또한 BCP 위원회는 Smart Place Pilot 프로젝트를 지원하기 위한 투자 계획인 Dorset Smart Place Investment Plan을 ‘20년 5월부터 ’ 21년 4월까지 추진하여 최대 10억 파운드의 투자를 유치하고, 향후 5~7년간 도싯주 지역에 스마트 플레이스를 구축할 계획이다. 뿐만 아니라 38만 파운드의 지역 성장 기금을 할당받아 기가비트 광섬유, 5G 솔루션, 장소 기반 데이터 인사이트 시스템, 장소 기반 통합 어플리케이션 등 4개 프로그램에 대해 비즈니스 모델 및 재정 모델, 시스템 구조·네트워크 계획 등을 개발하였으며, 6개의 신뢰 가능한 투자자를 비롯한 파트너들과 후속 논의를 진행하면서 BCP 지역에 신규 중립 호스트(neutral host) 광섬유 네트워크 구축을 고려중이다.

(4) 혁신을 위한 연구개발 분야

도쿄도립대학은 미나미오사와 캠퍼스 및 히노 캠퍼스에 4.7GHz 및 28GHz 대역의 5G 특화망 주파수 면허를 확보하였다. ‘19년 12월에는 미래의 도쿄 전략 비전의 일환으로 캠퍼스 내에 로컬 5G 환경을 조성하고, “스마트 도쿄” 실현을 목표로 5G 연구 및 실증 실험의 촉진을 도모하였다. 이를 위해 4.7GHz 및 28GHz 대역의 특성을 조합하여 2개 캠퍼스를 아우르는 약 49만㎡ 부지를 효율적으로 커버하는 일본 최대 규모 5G 특화망 환경을 구축하였다. 또한 ’ 21년 1월부터는 5G 특화망 환경을 활용한 연구 프로젝트를 개시하였다.

그리고 규슈공업대학은 28GHz 대역의 5G 특화망 주파수 면허를 보유한 통신사업자 QTnet과 연계하여 대학 캠퍼스 내에 5G 특화망을 구축하였다. 참고로 일본 지자체인 효고현은 4.7GHz 대역의 5G 특화망 주파수 면허를 확보하여 현립 공업기술센터에서 5G 특화망을 활용한 스마트팩토리 등 시연 컨텐츠를 제공하였다.

[그림 1-14] 일본 도쿄도립대학 캠퍼스 내 5G 특화망 환경

출처: 関東総合通信局(2021), 国内最大規模となるローカル5G無線局免許を付与

[그림 1-15] 일본 도쿄도립대학 5G 특화망 환경을 활용한 연구 사례

프로젝트 분류	분류 설명 및 추진 중인 프로젝트 테마
사회구현형 연구	새로운 라이프스타일에 대한 제안이나 사회적·공공적 가치 창조를 통하여 주민들의 삶의 질 향상을 불러오는 등 Society 5.0 실현으로 이어지는 응용 연구, 사회실현이 기대되는 연구 • AR 게임으로 즐겁게 단독 이동을 지원하는 AI 휠체어 시스템의 사회 구현
도전형 연구	기업이 추진하기 어려운 미래 과제 해결에 이바지할 도전적인 기초 연구, 과학기술 발전이나 변혁을 가져올 이노베이션의 핵심이 될 가능성을 지닌 연구 • 통신 자원의 이용 효율 극대화를 목표로 한 모바일 네트워킹 • L5G(Local 5G) 네트워크를 이용한 차세대 멀티 모달 센싱

출처: 東京都立大学(2020), 東京都立大学において、ローカル５Ｇ事業を開始 재구성

독일에서는 도르트문트 공과대학교, 슈투트가르트 대학교, 쾰른 공과대학교, 카이저슬라우테른 공과대학교, 아헨 라인 베스트팔렌 공과대학교 IT 센터 등 5개 대학에서 3.7~3.8GHz 대역 및 26GHz 대역의 주파수 면허를 확보하였다. 또한 영국은 셰필드 대학교, 링컨 대학교, 사우샘프턴 대학교, 워릭대학교 WMG (Warwick Manufacturing Group)의 대학에서 3.8-4.2GHz 대역의 주파수 면허를 확보하였다.

독일 작센 주의 에너지, 기후 보호, 환경 및 농업부 산하 환경농림지질청(LfULG)은 3.7-3.8GHz 대역 특화망 주파수를 확보하고, '19년 6월 Köllitsch 소재의 교육 및 실험 농장에 5G 테스트 필드를 마련, 디지털 농업 및 농촌 지역 분야에서 5G

커넥티비티의 이점을 연구하였다. 또한 작센 주의 simul+ Innovation Hub는 (1) 농림업에서의 5G 테스트 필드, (2) 스마트 농업 및 임업 기술, (3) 환경 기술 및 지속가능성, (4) 자연 및 기후 보호, (5) 디지털 빌리지 및 스마트 교외 지역 등 5개 주제를 중점 연구 분야로 삼고 특화망 주파수를 활용하여 여러 가지 기술적 시도들을 진행하였다.

3. 5G 특화망 요소 기술 분석

5G 특화망을 구축하기 위한 요소 기술로서 스몰셀, vRAN, 네트워크 슬라이싱, MEC 등 4가지 기술에 대해 분석한다.

(1) 5G 특화망 구축을 위한 스몰셀 기술

스몰셀(Small Cell)이란 기존의 수 km의 영역을 가지는 광역 기지국이 아닌 작은 출력만을 이용하여 기존보다 작은 영역을 가지는 기지국을 의미한다. 5G는 단순 최대 전송 용량 증대와 더불어 사용자가 어디에 있더라도 안정적으로 서비스를 제공해야하며, 사용자가 요구하는 다양한 서비스를 제공해야 하는 사용자 체감 전송률에 대한 요구사항도 하나의 중요한 요구사항이다. 전송 용량 증대를 위해서는 셀의 크기를 줄여 단위 면적당 셀을 더 많이 배치하는 스몰셀 기술이 제안되었다. 5G는 앞서 말했듯이 전송 용량 증대를 위해 스몰셀 구조를 기본 이동망 구조로 가정하고 있고, 이러한 스몰셀 기반의 5G 망은 대용량 데이터 전송 기능, 끊김 없는 품질을 보장하면서 다양한 서비스를 수용하므로 요구되는 서비스의 특성에 따라 동적으로 무선 자원의 할당 및 이동통신망의 구성을 가능하게 한다. 이러한 스몰셀의 장점을 활용하여, 5G 특화망 구축 시 음용지역 해소, 높은 수준의 통신 품질을 제공할 수 있다.

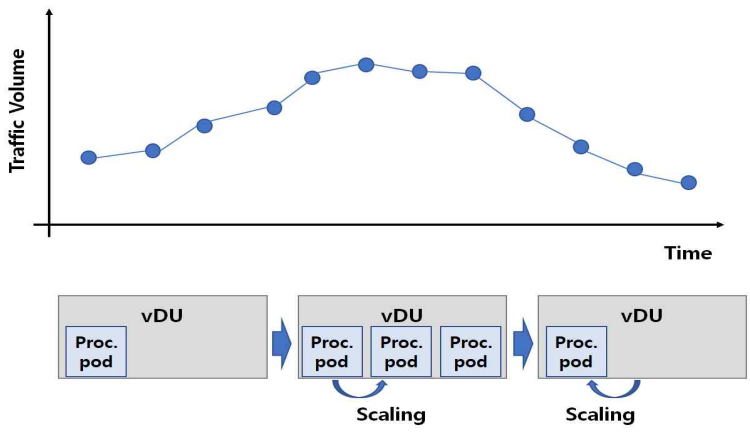
(2) 5G 특화망 구축을 위한 vRAN 기술

기존 RAN (Radio Access Network) 기능은 PNF (Physical Network Function)으로 구현되어 벤더에 종속적으로 개발되었다. 최근 통신 기능들을 가상화 기술을 이용해 소프트웨어화 하여 지능적이고 효율적으로 망을 운영할 수 있는 vRAN(Virtualized

RAN) 기술이 개발되고 있다. 여기서 나아가 최근에는 클라우드 컴퓨팅 기술을 적용하는 클라우드 네이티브 기술을 도입하고 있다. 클라우드 네이티브는 클라우드의 이점을 최대로 활용할 수 있도록 애플리케이션을 구축하고 실행하는 기술을 말한다. 기존 시스템에서의 어플리케이션은 클라우드의 이점을 잘 활용하지 못했다면, 마이크로서비스 아키텍처를 채택하고 컨테이너, 쿠버네티스와 같은 기술과 도구, 서비스 매쉬, 불면 인프라 등을 도입하여 개발자 생산성, 비즈니스 민첩성, 확장성, 가용성 및 비용 절감 효과를 높일 수 있다. 이로 인해 빌드와 테스트를 자동화할 수 있고, 배포가 가능해지고, 단단한 서비스의 구성 요소와 변화에 민첩한 시스템을 구축할 수 있게 된다.

〔그림 1-16〕는 vRAN의 동적 스케일링 기법을 보여준다. 그림에서 볼 수 있듯이, 컨테이너로 구성된 Pod을 사용자의 트래픽 요구가 많아지는 시간에 복사하여 증가시킴으로 리소스를 효율적으로 관리 할 수 있다. 따라서 기업에서는 5G 특화망 구축에 필요한 투자를 절감할 뿐 아니라, 최신 통신 기능을 손쉽게 업데이트 하고, 사용자 요구에 맞는 자원할당을 할 수 있기 때문에, 운용비용도 절감할 수 있다.

[그림 1-16] vRAN의 동적 스케일링 기법



자료: Samsung, Virtualized RAN-vol.2, White paper(2021)

(3) 5G 특화망 구축을 위한 네트워크 슬라이싱 기술

5G Network Slicing 기술은 물리적으로 하나의 망을 논리적으로 구분하여 가상의 독립망을 생성해 주는 기술을 말한다. 이를 통해, 서로 다른 어플리케이션들에게 그들에 QoS에 맞는 전용망을 구축하는 것을 도울 수 있다. 이러한 물리적인 인프라의 설정을 통해 사용자가 사용자만의 네트워크를 가진 것처럼 가상의 네트워크를 제공할 수 있게 된다. 가상화된 네트워크 자원 풀에서 서비스에 따른 자원을 할당받는 것으로써, 신규 서비스 도입 시 물리적인 네트워크 없이도 빠르게 서비스를 제공 가능하고, 한정된 자원을 효율적으로 활용할 수 있어 CAPEX(Capital expenditures) 절감에 유용하다. 이에 따라 각각의 서비스에 맞는 네트워크를 구성해서 자원을 효율적으로 사용할 수 있게 되고, 하나의 서비스는 다른 서비스의 영향을 받지 않고 운영된다. 이러한 Network Slicing 기술을 5G 특화망 인프라 구축과 연계하여 서비스 수준 협약에 맞는 5G를 구축한다.

(4) 5G 특화망 구축을 위한 MEC 기술

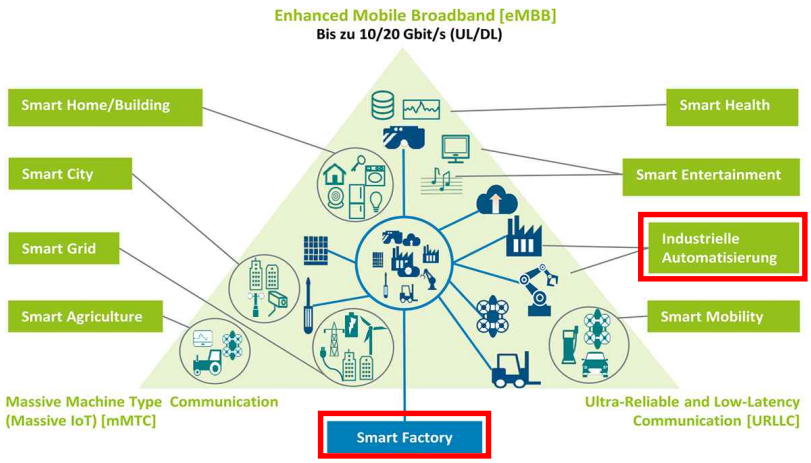
MEC(Mobile Edge Computing)은 무선 기지국에 분산 클라우드 컴퓨팅 기술을 적용하여 다양한 서비스와 캐싱 콘텐츠를 이용자 단말에 가까이 위치시킴으로써 코어망의 혼잡을 완화하는 기술이다. MEC는 어플리케이션 개발자나 콘텐츠 제공자들에게 모바일 네트워크 에지에서 IT서비스 환경과 클라우드 컴퓨팅 능력을 제공한다. 특히 어플리케이션들에게 초 저지연과 대용량 대역폭 제공, 실시간으로 네트워크에 접근하는 것을 가능하도록 하고, 사용자는 내가 보유한 단말기 가까운 곳에서 서비스가 처리되므로 빠른 속도의 서비스를 경험할 수 있고 사업자는 데이터를 기존보다 먼 거리까지 전송하는 비용을 절감할 수 있다. 또한 무선 기지국에 분산 클라우드 컴퓨팅을 위치시켜 신규 비즈니스 모델, 새로운 서비스 카테고리 등이 가능한 인프라를 만들어줌으로써 해당 로컬 목적에 효율적으로 대처할 수 있게 한다. 따라서 5G 특화망에서 생성된 데이터를 목적에 따라 가공하고 분석할 수 있으며, 특화망 서비스 목적에 따른 최적화를 수행할 수 있다.

제 3 절 5G 특화망 적용 특성 분석

1. 5G 특화망 제조・생산 서비스 적용 특성 분석

5G 특화망 적용 특성을 분석하기 위해 5G 적용이 가능한 다양한 분야들 중 제조 및 생산 서비스 분야에 대한 5G 특화망의 활용 형태를 제시한다.

[그림 1-17] 제조・생산 서비스에 대한 5G 특화망 적용 특성



자료: Industrial ethernet book, 5G on test bench for Industry: What’s possible in the future?(2021)

5G 특화망이 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있지만, 자동화된 제조・생산 설비에는 초고속과 저지연 특성이 필수적이다. 특히 스마트 공장은 제품의 기획부터 판매까지 모든 생산과정을 정보통신기술로 통합해 최소 비용과 시간으로 고객 맞춤형 제품을 생산하는 첨단 지능형 공장이며 산업 기밀 정보들이 데이터 내에 그대로 포함될 수 있다. 따라서 5G 특화망을 활용하되 유연한 확장성과 높은 보안성을 갖춘 모델을 선택해야 한다. 앞서

언급했던 4개 시나리오 중 이에 가장 적합한 특성을 가진 5G 특화망 모델은 독립형 전개 모델이라고 할 수 있다.

<표 1-4> 제조·생산 서비스에 적합한 5G 특화망 적용 모델

서비스	커버리지	SI 비용	구축비용	보안성	QoS 보장	최소지연보장	모델
제조생산	Low	High	High	High	High	High	독립형 전개 모델

(1) 5G 특화망을 적용한 스마트 공장

기존 자동화 설비의 IoT 데이터는 게이트웨이로부터 5G 특화망을 통해 중앙 서버로 전송이 가능하다. 최소 지연 보장 기능을 적용하여 설비별 자동화된 단위 장비의 상태 및 제어 데이터를 주변 설비 및 인프라와 연계하여 최적화 할 수 있다. 작업자 단말로 무선 링크를 통해 알림 메시지를 전달하는 등 스마트 공장 구현에 있어 보다 확장성과 보안성이 뛰어난 무선 환경을 제공한다.

제조과정에서 고화질 이미지 분석 기반 실시간 작업 확인 및 작업자의 AR글래스를 통한 영상기반 원격 작업지시, 3D VR·AR 도면 기반 작업자 기술지원 시스템 등 현장에서의 데이터 라이브러리 열람 및 업로드가 가능하다. 무인 운반 시스템(AGV)의 경우 5G네트워크의 정밀 포지셔닝 기술이 더해져 기존 유도선을 따라 이동하는 AGV의 이동한계를 극복한 원격 위치제어가 가능하다.

제조설비의 라인 증축에 있어 밀리미터파 기반의 무선링크로 구성한다면 별도의 유선공사 및 생산라인 중단 없이 설비 증설이 가능하며 외부 수요환경에 맞는 빠른 설치·변경 가능한 생산 환경 구현이 가능하다. 타 지역의 공장간 또는 본사 관제시스템과의 5G 특화망을 연동하는 경우 유선 기간통신사업자의 전용회선 임대를 통해 구현하다. 이 경우 5G 특화망으로부터 실시간 수집되는 정보를 공장·제조설비의 3D 모델에 적용한다면 CPS(Cyber Physical System) 또한 구축 가능할 것이다.

[그림 1-18] 5G 특화망 적용된 제조·생산 서비스

자료: Bosch Press, Bosch puts first 5G campus network into operation(2020)

⑵ 5G 특화망을 적용한 스마트 조선

조선 산업을 친환경적이고 스마트화하기 위해서 5G 특화망을 적극 활용할 수 있다. 야드 영역 내 작업자의 웨어러블 디바이스와 기존 자동화 설비에서 발생하는 데이터를 5G 특화망을 통해 수집하고 디지털 트윈 플랫폼 내 3D 모델링 정보와 결합하여, 가상 조선소를 구현할 수 있다.

또한, 작업자의 스마트 헬멧 등 웨어러블 기기를 통해 작업장 내 안전사고를 예방하고 AR·VR 등을 활용한 3D 설계정보의 전송 및 원격 작업지시가 가능하다. 또한 블록 조립 공장에는 원격 제어 가능한 용접로봇을 도입하는 등 디지털 공법으로의 전환이 가능하다. 5G 코어망을 조선소 내 구축하고, 설계도면과 같은 보안성이 요구되는 기업의 주요 디지털 정보를 On-Site MEC 솔루션을 통해 직접보관·관리함으로써 기업 경쟁력을 확보할 수 있고, ESG경영이 주요 화두인 만큼 조선소 내 작업자의 노동환경 개선 및 안전 확보 측면에 있어 핵심 인프라가 될 것이다.

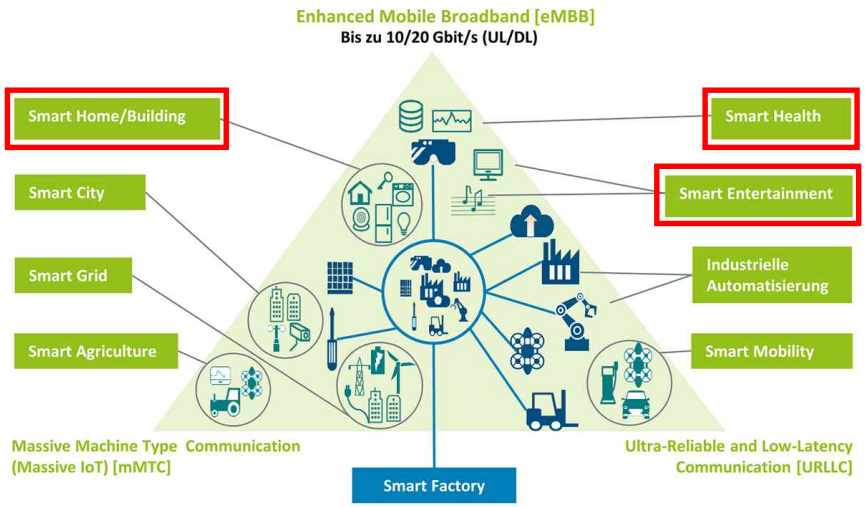
(3) 5G 특화망을 적용한 스마트 건설

건설 현장에서 작업자의 스마트 헬멧으로부터 주요 공정에 대한 고화질 영상 기록을 중앙서버로 전송하고 이동동선 및 현재 위치를 모니터링하여 현장 관리 및 작업자의 안전을 확보할 수 있다. 현장소장 및 감리는 특화망 전용 단말 또는 AR 글래스를 통해 BIM(Building Information Modeling) 설계와 2D 도면과 같은 대용량 이미지·문서 등 현장에서의 데이터 라이브러리 열람 및 업로드가 가능하다. 공사 중장비에 5G 단말을 연동하여 초저지연 기반의 원격제어가 가능한 작업환경을 구성하고, 나아가 중앙서버의 BIM 설계 모델과 현장에서 5G 특화망을 통해 수집되는 다양한 형태의 정보를 결합시키면 디지털 트윈(Digital Twin)기반의 가상 건설현장 구현도 가능하다.

2. 5G 특화망 공공·인빌딩 서비스 적용 특성 분석

5G 특화망 적용 특성을 분석하기 위해 5G 적용이 가능한 다양한 분야들 중 공공 및 인빌딩 서비스 분야에 대한 5G 특화망의 활용 형태를 제시한다.

[그림 1-19] 공공·인빌딩 서비스에 대한 5G 특화망 적용 특성



자료: Industrial ethernet book, 5G on test bench for Industry: What's possible in the future?(2021)

5G 특화망이 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있지만, 자동화된 공공·인빌딩 설비에는 초고속 특성이 필수적이다. 또한 스마트 병원 등 의료서비스를 제공하기 위해서는 도심 뿐 아니라 도서산간 지역에도 통신이 가능해야하고 수술 등 생명에 직결되는 통신 서비스를 위해서는 QoS 보장 및 초저지연 특성도 필요하다. 따라서 5G 특화망을 활용하되 QoS 보장과 넓은 커버리지를 갖춘 모델을 선택해야 한다. 앞서 언급했던 4개 시나리오 중 이에 가장 적합한 특성을 가진 5G 특화망 모델은 무선 액세스 공유 모델이라고 할 수 있다.

<표 1-5> 공공·인빌딩 서비스에 적합한 5G 특화망 적용 모델

서비스	커버리지	SI 비용	구축비용	보안성	QoS 보장	최소지연보장	모델
공공인빌딩	High	High	Mid	High	High	High	무선 액세스 공유 모델

(1) 5G 특화망을 적용한 스마트 병원

병원 내 스마트 의료서비스 도입을 위해서 5G 특화망을 적극 활용할 수 있다. 의료진은 IoT 장비(웨어러블 기기 등)를 활용한 모니터링을 통해 환자의 건강 정보에 대한 연속적인 관리 감독이 가능하며, 질병의 패턴과 순간적인 변화를 실시간으로 전송·공유하여 빠른 대처 및 진단·치료가 가능하다. 또한 다양한 의료기기로부터 발생하는 IoMT(Internet of Medical Things)데이터를 특화망을 통해 중앙서버로 전송함으로써 의료장비의 상태 추적, 원무·행정·진료 프로세스 개선 등 병원의 운영 효율성 및 의료 서비스 품질향상이 가능하다. 환자의 각종 샘플이나 방사선 사진, 의약품 등을 옮기는 천장 레일형 이동 로봇의 경우 특화망의 정밀 위치측위 기술 등을 적용해 이동성의 제약없는 자율원격제어 주행이 가능해진다. 무력감에 빠지기 쉬운 환자나 고령자에게는 활동적인 행동을 할 수 있도록 동기 부여가 가능한 가상·증강현실 콘텐츠를 스마트 디바이스를 통해 제공할 수 있으며, 전염병 등으로 인하여 병실 방문이 어려울 경우 가상현실 기술(VR·MR)을 통해 방문객의 면회가 가능하다.

(2) 5G 특화망을 적용한 스마트 캠퍼스

대학 내 융복합 연구 환경 및 첨단 교육 제공을 위해 5G 특화망을 적극 활용할 수 있다. 독립구축 모델 또는 일부 공유 모델을 활용하여 직접 운영할 경우 관계 교수진들과 학생들의 참여를 통해 네트워크 엔지니어링 및 운영 전반의 실무경험을 쌓을 수 있다. 5G 특화망을 기반으로 교내 진행되고 있는 자율주행, 드론 등의 ICT 융·복합 연구 과제들에 대한 테스트 베드로서 활용할 수 있습니다. 또한 코로나와 같은 정상 수업 진행이 어려운 환경에서 특화망 단말체계를 확보하고 5G 브로드캐스트(Broadcast) 기술을 적용하여 고화질 스트리밍 기반의 캠퍼스 내 시·공간 제약 없는 원격강의 수강환경을 실현시킬 수 있다. 아울러 대용량의 융합현실(XR) 콘텐츠를 전송받거나 360° 매트릭스 뷰 실습실을 구축하여 학생들에게 보다 효과적인 몰입·참여형 교육기회 제공이 가능하다.

[그림 1-20] 5G 특화망 적용된 공공·인빌딩 서비스

자료: Nokia, Sendai city improves tsunami preparedness with connected drones(2019)

(3) 5G 특화망을 적용한 스마트 오피스

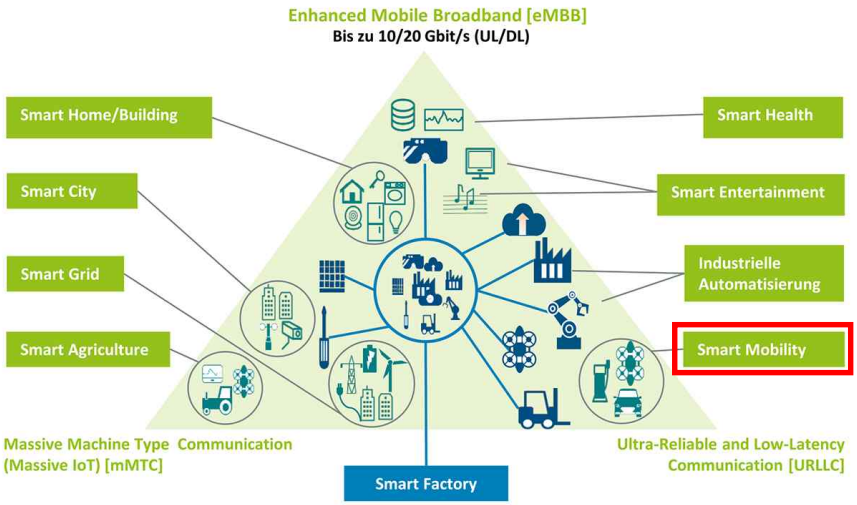
업무 효율 향상 및 스마트 사옥관리 등을 위해 5G 특화망을 적극 활용할 수 있다. 사옥 보안 및 운영관리 측면에서 영상정보 처리기기(CCTV)를 감시구역 및 주차 관제 설비 등에 적용함으로써 고화질의 영상 데이터를 중앙서버로 실시간 전송시킬 수 있다.

공조설비, 조명, 전력기기 등의 IoT 센서로부터 발생하는 데이터는 게이트웨이와 5G 특화망을 통해 중앙서버로 연결이 가능하다. 이를 통해 빌딩 자동제어 솔루션, 지능형 에너지 절감 등을 기대할 수 있다. 업무환경에 있어 유선 LAN 환경을 5G 특화망으로 대체하여 외부망과 분리된 내부 업무환경을 구축할 수 있고, 무선화된 모바일 오피스 환경도 구축할 수 있다. 외부 인터넷망 연동 필요시 네트워크슬라이싱 기술 등을 적용하여 논리적으로 분리된 업무망 환경 또한 구현 가능하다.

3. 5G 특화망 교통·수송 서비스 적용 특성 분석

5G 특화망 적용 특성을 분석하기 위해 5G 적용이 가능한 다양한 분야들 중 교통 및 수송 서비스 분야에 대한 5G 특화망의 활용 형태를 제시한다.

[그림 1-21] 교통·수송 서비스에 대한 5G 특화망 적용 특성



자료: Industrial ethernet book, 5G on test bench for Industry: What's possible in the future?(2021)

5G 특화망이 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있지만, 자동화된 교통·수송 설비에는 초저지연

특성이 필수적이다. 자율주행과 같은 교통 자동화에는 운전자 및 보행자의 안전이 필수적이며, 차량이 이동할 수 있는 전국 지역에 서비스를 제공할 수 있어야하기 때문에 서비스 커버리지가 넓어야 한다. 또한 공공재의 특성상 구축비용과 SI 비용이 크지 않아야 한다. 따라서 구축비용을 최소화하는 5G 특화망을 활용하되 최소 지연 보장과 넓은 커버리지를 갖춘 모델을 선택해야 한다. 앞서 언급했던 4개 시나리오 중 이에 가장 적합한 특성을 가진 5G 특화망 모델은 무선 액세스 및 제어부 공유 모델이라고 할 수 있다.

<표 1-6> 교통·수송 서비스에 적합한 5G 특화망 적용 모델

서비스	커버리지	SI 비용	구축비용	보안성	QoS 보장	최소지연보장	모델
교통수송	High	Mid	Low	Low	High	High	무선 및 제어부 공유 모델

(1) 5G 특화망을 적용한 스마트 공항

공항을 이용하는 고객 및 공항 인프라 운영, 관리 측면에서 5G 특화망을 적극 활용할 수 있다. 터미널 내 실감 미디어 콘텐츠, 방역 안내 로봇 서비스 외 실시간, 출국장 및 보안검색 지역 등에 대용량 및 이동성이 보장된 공항 특화 서비스 구현이 가능하다. Airside 내 다양한 용도의 자율운행 차량 제어 및 등화 시설 등의 시설물 관리, 유선 공사 없는 고화질 지능형 CCTV 추가 증축, 스마트 헬멧을 활용한 작업자 안전관리 등이 가능하다. 독립구축 모델 또는 일부 공유 모델을 활용하여 직접 운영할 경우 항공기 격납고를 이용하는 항공사 및 상업시설 입주사 등을 대상으로 5G 서비스 상품을 제공할 수 있다.

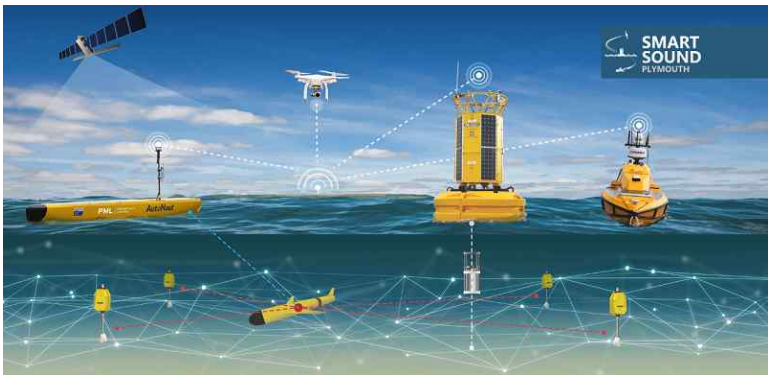
[그림 1-22] 5G 특화망 적용된 스마트 공항 서비스

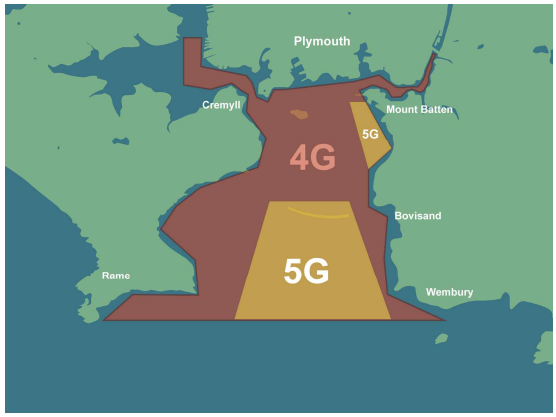
자료: Lufthansa Technik, Lufthansa gets spectrum licence, deploys Nokia private 5G for remote engine checks(2020)

(2) 5G 특화망을 적용한 스마트 항만

항만 인프라 운영, 관리 측면에서 5G 특화망을 적극 활용할 수 있다. 안벽 영역의 크레인 내 고화질 카메라와 센서를 이용하여 원격에서 크레인의 양하 및 적하 제어가 가능하며 별도의 유선 공사 없이 구현할 수 있다. 이송영역에서는 AGV(Automated Guided Vehicle) 등과 같은 자동 운반차량의 이동제어·관리가 가능하다. 야드 영역에서는 야드 크레인의 실시간 원격제어와 스마트 헬멧 등을 활용한 작업자의 안전관리, 지능형 CCTV를 통한 보안 관제 서비스 등을 구현할 수 있다. 독립구축 모델 또는 일부 공유 모델을 활용하여 직접 운영할 경우 항만 내 입주하고 있는 선사, 하역업체 등을 대상으로 5G 서비스 상품 또한 제공이 가능하다.

[그림 1-23] 5G 특화망 적용된 스마트 항만 서비스



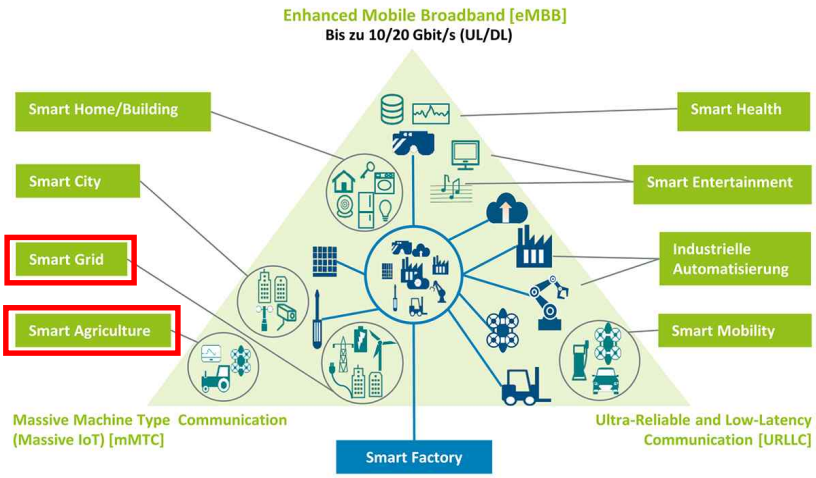


자료: Smart sound plymouth, Vodafone, Plymouth city council and Plymouth marine laboratory announce use cases for world's first 5G marine focused testbed(2022)

4. 5G 특화망 에너지·자원 서비스 적용 특성 분석

5G 특화망 적용 특성을 분석하기 위해 5G 적용이 가능한 다양한 분야들 중 에너지 및 자원 서비스 분야에 대한 5G 특화망의 활용 형태를 제시한다.

[그림 1-24] 에너지·자원 서비스에 대한 5G 특화망 적용 특성



자료: Industrial ethernet book, 5G on test bench for Industry: What's possible in the future?(2021)

5G 특화망이 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있지만, 자동화된 에너지·자원 설비에는 초연결 특성이 필수적이다. 집집마다 들어가는 전기 계량기와 넓은 발전소에는 수많은 5G 특화망 기기들이 적용될 것이다. 또한 수많은 기기들로부터 발생하는 에너지 자원 데이터를 처리하기 위해서는 고성능의 기지국과 코어망을 갖춘 모델을 선택해야 한다. 앞서 언급했던 4개 시나리오 중 이에 가장 적합한 특성을 가진 5G 특화망 모델은 이동통신사 호스팅 방식이라고 할 수 있다.

<표 1-7> 에너지·자원 서비스에 적합한 5G 특화망 적용 모델

서비스	커버리지	SI 비용	구축비용	보안성	QoS 보장	최소지연보장	모델
에너지자원	High	Low	Low	Low	Low	Low	이동통신사 호스팅 방식

(1) 5G 특화망을 적용한 스마트 발전소

5G 기반 설비의 원격 모니터링, 제어 등을 위해 5G 특화망을 적극 활용할 수 있다. 설비 순찰로봇 및 CCTV의 고화질의 영상 데이터와 IoT 센서로부터 발생하는 기존 발전 계통 및 환경설비 정보를 IoT 게이트웨이와 5G 특화망을 통해 중앙서버로 전송이 가능하다. 또한 실시간 수집되는 영상 데이터와 IoT 센싱 데이터를 결합함으로써 주요 발전 및 송전 설비에 대한 실시간 원격 모니터링, 장애 설비의 실시간 절체가 가능하다. 나아가 발전소 내 주요 계통 설비를 3D 모델링하고 5G 특화망을 통해 수집되는 다양한 형태의 정보를 결합시킴으로써 디지털 트윈(Digital Twin)기반의 가상 발전소를 구축하여 발전소의 가동효율 높이고 장애 예측 및 사전 예방 활동을 수행할 수 있다.

[그림 1-25] 5G 특화망 적용된 에너지・자원 서비스

자료: Im-mining, Sandvik and Nokia team up to offer miners LTE and 5G networks(2018)

제4절 요약

본 장에서는 5G 특화망 도입 사례 분석 결과를 종합하고 도입된 사례를 바탕으로 서비스별로 어떤 형태의 특화망 모델이 좀 더 적합한지를 논의하고자 한다. 5G 특화망이 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있다. 하지만 실시간성이나 복잡성, 유연성, 그리고 제어가능성 등 각 서비스에 필수적인 요소들은 5G 특화망이 제공하는 특성과 부합하여 다른 서비스와 차별화된다.

첫 번째로 자동화된 제조·생산 설비에는 초고속과 저지연 특성이 필수적이다. 5G 특화망을 활용하되 유연한 확장성과 높은 보안성을 갖춘 모델을 선택해야 하며, 4개 시나리오 중 독립형 전개 모델이 제조·생산 서비스에 가장 적합한 5G 특화망 모델이다.

두 번째로 자동화된 공공·인빌딩 설비에는 초고속 특성이 필수적이다. 또한 스마트 병원 등 의료 서비스를 위해서는 QoS 보장 및 초저지연 특성도 필요하다. 5G 특화망을 활용하되 QoS 보장과 넓은 커버리지를 갖춘 모델을 선택해야 하며, 4개 시나리오 중 무선 액세스 공유 모델이 공공·인빌딩 서비스에 가장 적합한 5G 특화망 모델이다.

세 번째로 자동화된 교통·수송 설비에는 초저지연 특성이 필수적이다. 자율주행과 같은 교통 서비스를 위해서는 서비스 커버리지가 넓어야 하며 구축비용과 SI 비용이 크지 않아야 한다. 구축비용을 최소화하는 5G 특화망을 활용하되 최소 지연 보장과 넓은 커버리지를 갖춘 모델을 선택해야 하며. 4개 시나리오 중 무선 액세스 및 제어부 공유 모델이 교통·수송 서비스에 가장 적합한 5G 특화망 모델이다.

네 번째로 자동화된 에너지·자원 설비에는 초연결 특성이 필수적이다. 수많은 기기들로부터 발생하는 에너지 자원 데이터를 처리하기 위해서는 고성능의 기지국과 코어망을 갖춘 모델을 선택해야 하며, 4개 시나리오 중 이동통신사 호스팅 방식이 에너지·자원 서비스에 가장 적합한 5G 특화망 모델이다.

<표 1-8>에서 4가지 서비스 군에 대해 어떤 5G 특화망 모델이 가장 접합한지 요약해 놓았다. 하지만 반드시 해당 서비스에 대해 적합 모델의 5G 특화망을 구축해야하는 것

은 아니다. 모든 기업이나 사업자들이 모두 동일한 환경에서 서비스를 제공하는 것은 아니며, 개별적인 서비스 환경의 특성을 잘 살펴서 어떤 방식으로 5G 특화망을 구축할 것인지에 대한 의사결정이 필요하다.

<표 1-8> 5G 특화망 서비스별 적합 모델

서비스	커버리지	SI 비용	구축비용	보안성	QoS 보장	최소지연보장	모델
제조생산	Low	High	High	**High**	High	High	독립형 전개 모델
공공인빌딩	High	High	Mid	Mid	**High**	High	무선 액세스 공유 모델
교통수송	High	Mid	Low	Low	High	**High**	무선 액세스 및 제어부 공유 모델
에너지자원	**High**	Low	Low	Low	Low	Low	이동통신사 호스팅 방식

제 2 장 5G 특화망 도입 기업들이 고려해야 할 보안 요구사항 연구

제 1 절 5G 특화망 보안 위협

1. 5G 특화망 보안 위협 분석

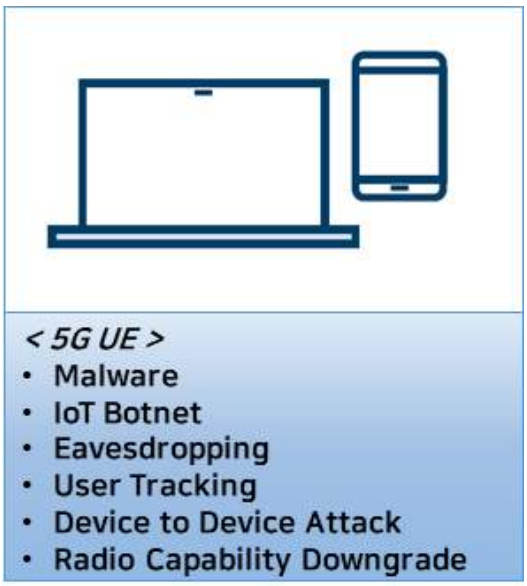
5G 특화망의 기본인 5G SA 표준은 이전 세대 이동통신에 비해 많은 보안적인 사항이 향상되었음에도 불구하고, 여전히 보안위협은 존재한다.

5G 특화망을 이루는 주요 요소별로 보안위협 사항을 살펴보겠다.

(1) 5G 특화망 단말 보안 위협 사항

먼저, 5G 특화망에 접속할 수 있는 단말의 종류는 다양하기 때문에 단말 간 적용된 보안 수준이나 장비 제조사의 제품 제조 시 고려된 보안 수준이 또한 천차만별이다. 이런 상황에서 보안이 허술한 단말이 악성코드에 감염이 되면 봇넷, 사용자의 민감정보 유출, 사용자 위치추적이 될 수 있다. 그리고 특정취약점에 의해 악성코드에 감염된 기기가 주변의 동일한 보안취약점을 가진 기기로 악성코드를 점염시키는 공격 또한 가능하다.

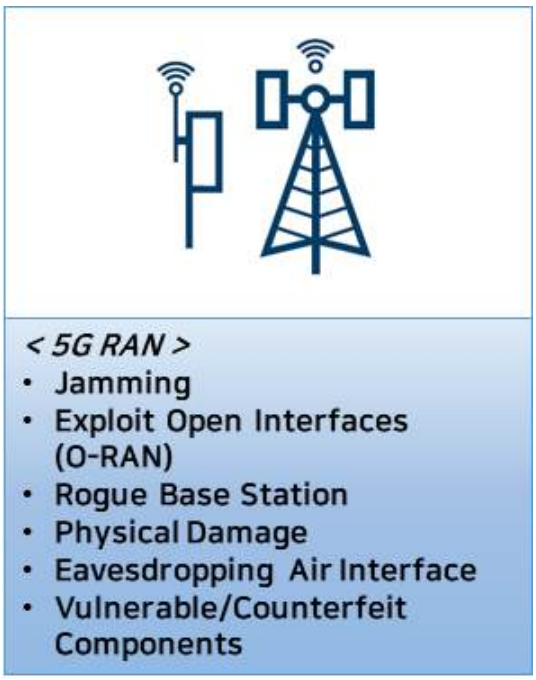
[그림 2-1] 5G 특화망 단말 보안위협 사항



⑵ 5G 특화망 기지국 보안 위협 사항

통신 기지국에 필요한 인터페이스, 운영체제 등을 개방형 표준으로 구축하는 Open RAN (O-RAN) 사용이 확대될 것으로 예상된다. 하지만 O-RAN의 인터페이스가 취약하게 제작되었을 경우, 악의적인 공격자의 주요 공격 대상이 될 것이고 이로 인해 기지국의 정상적인 운영이 방해받을 수 있다. 그리고, 가짜 기지국 (Rogue Base Station)으로 인해 중간자 공격 (Man-In-The-Middle Attack)이 발생할 수 있다. 기지국은 물리적인 장비이기 때문에 물리적인 공격으로 인해 파손될 수 있으며, 보안이 취약한 소프트웨어, 부속품으로 인해 장비의 보안에 위협이 될 수 있다.

[그림 2-2] 5G 특화망 기지국 보안위협 사항

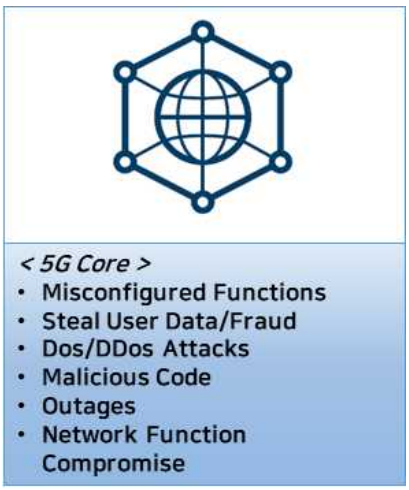


(3) 5G 특화망 코어 보안 위협 사항

코어의 NF 설정이 잘못되어 보안위협이 발생할 수 있다. 5G 보안표준에 따라 하지 못할 경우, 거부되어야할 통신 패킷이 정상 처리가 되는 등 해킹 공격에 악프로 토콜에서 요구하거나 갖추어야 하는 설정이 있으나, 이에 대한 설정을 제대로 용될 수 있다. 그리고, 코어를 운영하는 소스코드가 보안취약점을 존재하거나 해킹 공격으로 인해 공격자에 의해 장악된 NF에 의해 다른 NF가 해킹공격 받는 보안위협이 있을 수 있다. 코어에는 사용자 정보가 저장되어 있기 때문에 관리가 허술할 경우 단말 인증 등에 사용되는 주요 정보 등이 유출 또는 남용될 수 있다. 그 뿐 아니라, 정전 또는 DoS, DDoS 와 같은 서비스 거부 공격에 대한 대비가 필요하다.

[그림 2-3] 5G 특화망 코어

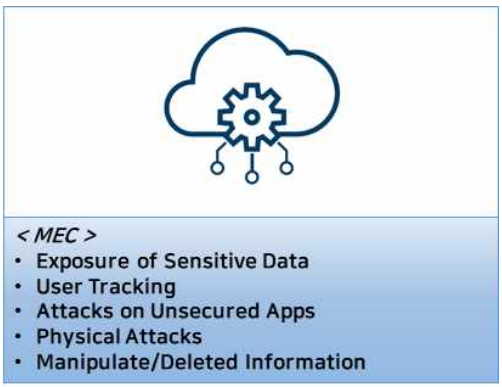
보안위협 사항



(4) 5G 특화망 Mlulti-access Edge Computing (MEC) 보안 위협 사항

MEC에 설치된 보안에 취약한 애플리케이션에 의해 민감정보가 유출되거나 사용자의 사용이력이 노출될 수 있으며, 저장된 정보가 변경·삭제될 수 있다. 그리고 MEC 서버에 대한 물리적 관리 소홀로 인해 파손이 될 경우 서비스 중단 등의 문제가 발생할 수 있다.

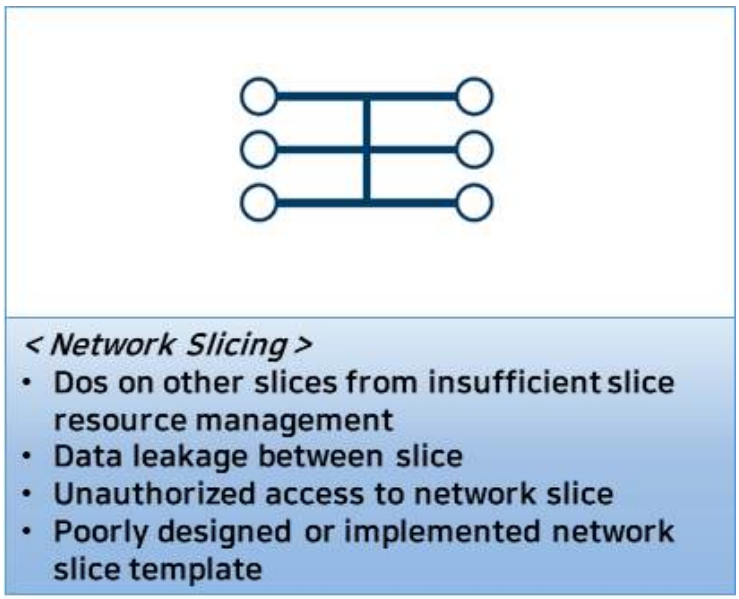
[그림 2-4] 5G 특화망 MEC 보안위협 사항



(5) 5G 특화망 네트워크 슬라이싱 보안 위협 사항

슬라이스 리소스 관리가 적절하게 이루어지지 않아 다른 슬라이스 서비스에 문제가 발생할 수 있고, 슬라이스 간 격리가 되지 않아 슬라이스에서 다른 슬라이스로 비정상적인 접근으로 인해 데이터 유출이 발생할 수 있다. 이와 같이 보안적으로 제대로 설계되지 않은 슬라이스 템플릿으로 사용으로 인해 문제가 계속 반복되어 나타날 수 있다.

[그림 2-5] 5G 특화망 네트워크슬라이싱 보안위협 사항

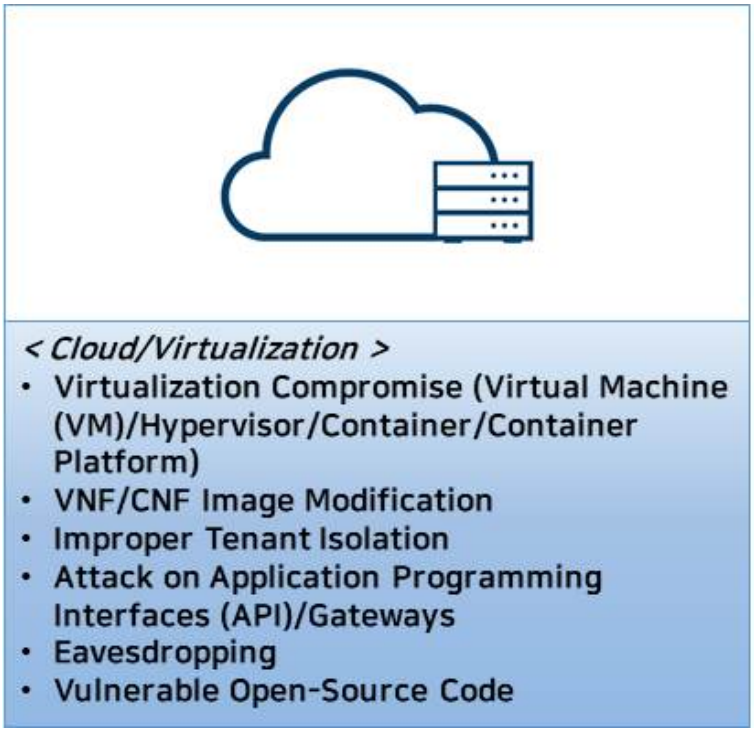


(6) 5G 특화망 클라우드/가상화 보안 위협 사항

가상화 머신 (Virtual Machine, VM), 하이퍼바이저 (Hypervisor), 컨테이너 (Container) 등과 같은 가상화 솔루션의 보안취약점이나 오픈소스 코드의 보안취약점을 악용하여 해킹공격이 될 수 있고, Virtualized Network Function (VNF) / Cloud Network Function (CNF) 이미지의 관리 소홀로 인해 해킹공격으로 변경이 될 수 있으며, 잘못 설계된 클라우드의 멀티테넌트로 인해 특정 기업의 데이터가 공유환경을 이용하는

다른 기업에 노출될 위험이 있다. 가상화 모듈간 통신에 이용되는 Application Programming Interface (API) 의 설계가 잘못되어 해킹공격의 창구로 이용될 수 있다.

[그림 2-6] 5G 특화망 클라우드/가상화 보안위협 사항

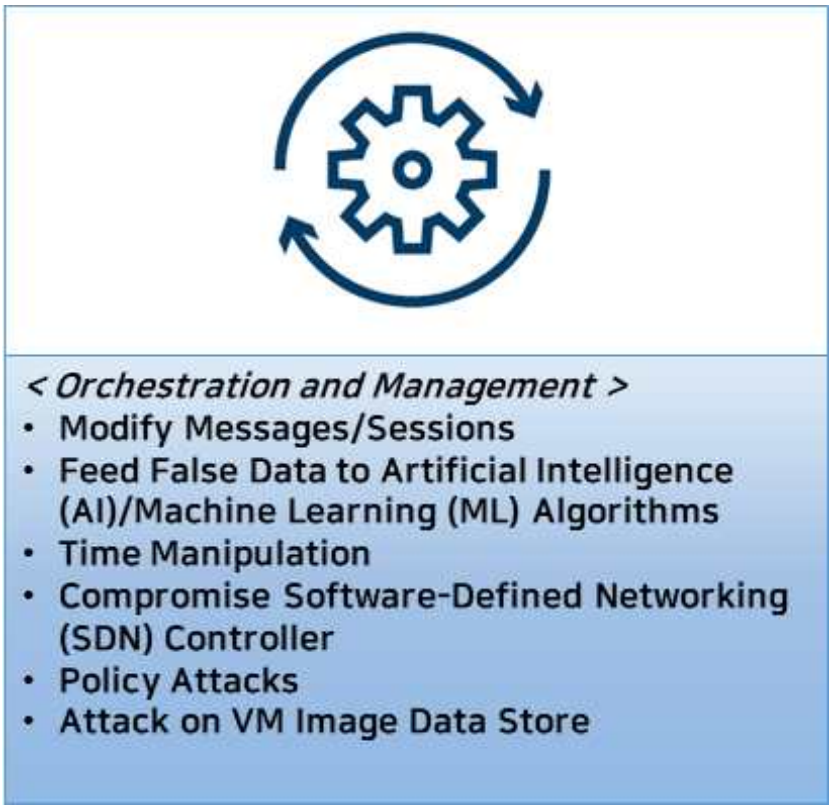


(7) 5G 특화망 운영 관리 보안 위협 사항

5G 특화망에는 MEC를 통해 Artificial Intelligence (AI) / Machine Learning (ML)이 사용이 확대될 것인데 안전하지 않은 알고리즘 사용으로 인해 학습데이터의 조작, 악의적 샘플 삽입 등 AI 운영에 영향을 줄 수 있는 공격이 발생할 수 있다. 그리고 5G 특화망의 운영에서 발생하는 각종 시스템 메시지 등을 조작하여 제대로 된 모니터링을 방해하는 해킹공격이 발생할 수 있으며, 시스템 간 일괄적인 시간 동기화가 제대로 이루어지지 않아 해킹사고 및 비정상적 서비스 장애 발생 시 대처에 대한

혼선을 유발할 수 있다. 그리고 SDN 컨트롤러의 해킹공격으로 인해 운영 네트워크 전체의 혼돈 및 정상적인 운영을 방해할 수 있다. 그리고 가상화 이미지 저장소의 관리 및 주요 시스템에 접속하는 단말 접근 시 인증·권한 관리가 제대로 되어있지 않을 경우, 해킹공격에 주요한 경로가 될 수 있다.

[그림 2-7] 5G 특화망 오케스트레이션 및 운영·관리 보안위협 사항



제 2 절 5G 특화망 도입시 고려해야 할 보안 영향 요소

1. 5G 특화망 활용분야

5G는 초고속(eMBB), 초저지연(uRLLC), 초연결(mMTC) 서비스 비전 달성을 통해 개인의 이동전화 및 멀티미디어 서비스 뿐만 아니라 산업환경 전체를 혁신하고 공공 서비스의 차원을 높일 수 있는 4차 산업혁명의 핵심 인프라이다. 따라서, 수요기업이나 사업자가 건물・시설・토지 등 제한된 범위 내에서 5G 서비스를 적용하기 위해 기업 맞춤형으로 무선 네트워크를 구축할 수 있는 5G 특화망은 전 산업분야에서 기업의 도입이 점차 활성화될 전망이다.

[그림 2-8] 5G 특화망 활용분야

자료: 과학기술정보통신부/한국방송통신전파진흥원, 5G 특화망 가이드라인, 2021

5G 특화망은 기업이나 기관의 규모 및 전문성 여부와 관계없이 수요기업 및 제3자(SW・SI기업, 중소통신사, 장비벤더사)에게 이용 및 구축의 기회가 제공되며, 전문성이

부족한 비통신 수요기업에게도 정부로부터의 유효한 정보 지원을 제공받을 수 있는 특징을 갖는다. 따라서, [그림 2-8]과 같이 스마트 공장을 도입하는 제조업 뿐만 아니라 문화・예술, 에너지, 교육, 의료, 보안, 스마트시티, 건설, 관광, 교통 등 다양한 분야에서 5G 특화 서비스가 다양한 형태로 제공・발굴됨으로써 국내 5G 기반 산업 생태계가 더욱 활성화될 전망이다.

2. 5G 특화망 도입 및 활용 효과

건물・시설・토지 등 제한된 범위 내에서 고속 무선 통신 환경을 제공하는 기술로서 무선 인터넷(WiFi)이 5G 특화망과 비교 검토될 수 있다. [그림 2-9]는 5G 대비 유선(TSN), 4G LTE, Wi-Fi 통신 방식에 대한 주요 특징을 비교한 것이다.

[그림 2-9] 통신 방식별 특징 비교

특성	유선 (TSN)	4G (LTE-adv.)	Wi-Fi (802.11ax)	5G
이동성	X	O	O	O
전송지연	1ms	20~60ms	2ms~200ms	1ms
QoS보장	O	O	X	O
최고전송속도	10 Gbps	1 Gbps	1.2 Gbps	20 Gbps
최대연결기기	-	100,000/km^2	-	1,000,000/km^2
에너지효율	-	1x		100x
설치·유지보수	복잡	단순	단순	단순

자료: 관계부처 합동, 5G 기반 스마트공장 고도화 전략(안), 2019

기업 입장에서는 4G LTE나 5G 특화망과 같은 이동통신 네트워크 도입에 있어서 구축(CAPEX) 및 운영비용(OPEX)과 이동통신 기술에 대한 전문 인력 확보의 어려움 측면에서 정부의 지원이 있다고 하더라도, 보다 익숙하고 비용 부담이 적은 Wi-Fi 기반의 기업망 구축을 고려할 수도 있다. 그러나, Wi-Fi 기술은 비면허 대역(2.4GHz, 5GHz, 6GHz)을 이용함으로써 인접지역의 AP(Access Point)로부터 혼・간섭 영향을 받을 수

있으며 간헐적 끊김 현상 등 서비스 품질(Quality of Service) 보장이 어렵기 때문에 실시간 원격제어 등 저지연, 고품질의 서비스 환경 구축을 위해서는 Wi-Fi가 아닌 5G 적용이 필요하다. 일례로 스마트공장 환경에서 Wi-Fi 도입시 한계점은 다음과 같다.

[그림 2-10] 스마트공장 내 WiFi(802.11ax) 도입시 한계점

무선기반 스마트공장 솔루션		5G가 아닌 Wi-Fi 도입 시 제약사항
다기능 협동 로봇		• 공장 내 좁은 공간에서 **사람과 로봇의 협동작업** 과정에서 **QoS 미보장 시**, 사람-기계 충돌 등 산업재해' 발생 가능 * 국내 산업용 로봇에 의한 재해는 연평균 41.4명(산업안전보건연구원 '16)
네트워크 슬라이싱 기반 원격 제어		• 스마트공장 내 다양한 서비스(자율주행, 산업용 로봇 제어, Massive IoT)를 동시에 제공하는 경우, **특정 서비스에 과부하가 발생할 경우 타 서비스에 영향** 가능 * 5G는 네트워크슬라이싱 기능으로 서비스별 독립적 N/W 할당
자율주행 물류운송		• 모바일 로봇 여러 대가 동시에 안정적으로 움직일 수 있도록 끊임없이 제어해야 하나 **인터넷 끊김 시 충돌** 가능

자료: 관계부처 합동, 5G 기반 스마트공장 고도화 전략(안), 2019

결국 기업이 5G 특화망을 도입할 때 얻을 수 있는 효과는 이동통신사업자의 상용 5G 네트워크의 관여없이 기업이 필요로 하는 맞춤형 5G 사설망을 구축할 수 있으며. 이를 통해 기업 내 작업장의 안전환경을 개선하고 작업공정을 첨단화할 수 있으며, 5G 기반의 고품질 서비스를 제공함으로써 비용을 최적화하고 생산효율성을 증대할 수 있다. 또한 기업간 B2B 사업 영역 확대는 물론 신산업 활성화를 도모함으로써, 궁극적으로 기업의 디지털 대전환(Digital Transformation)의 혁신을 추구할 수 있다.

[그림 2-11] 기업의 5G 특화망 활용 효과

자료: 과학기술정보통신부/한국방송통신전파진흥원, 5G 특화망 가이드라인, 2021

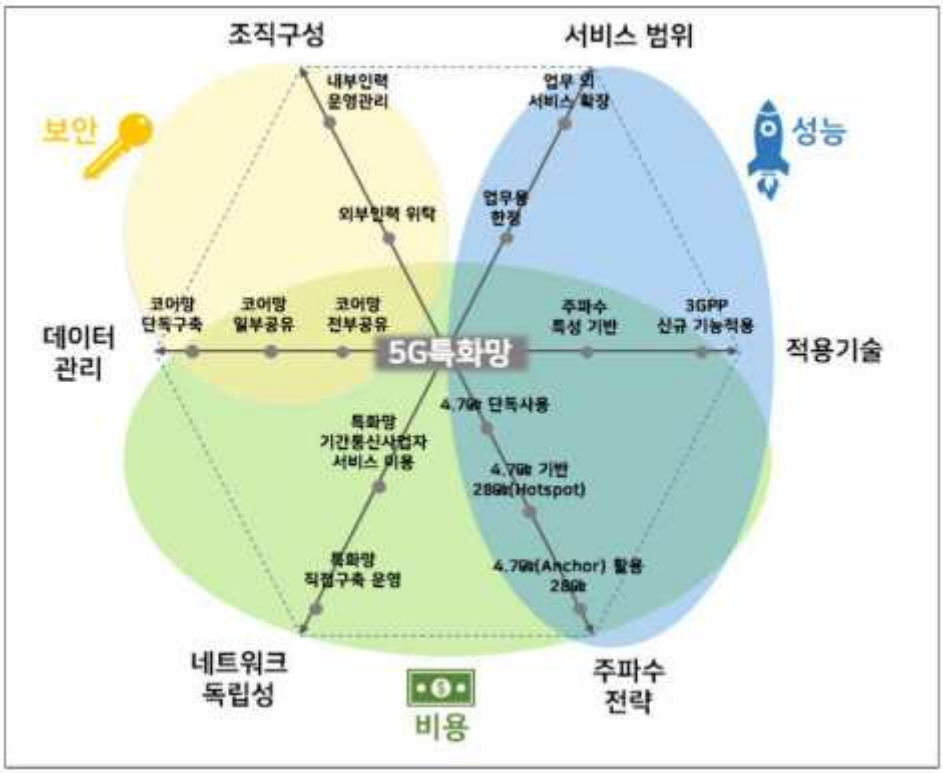
3. 5G 특화망 도입시 보안 영향 요소

『5G 특화망 가이드라인』에 따르면, 5G 특화망을 도입하는 기업이 사업장 내에서 5G 네트워크를 구축하고 특화망 서비스를 이용하는데 있어 비용적 측면, 성능적 측면, 보안적 측면에서의 평가요소를 구분하여 제시하고 있다. 따라서, 사업장 내에서 구현하고자 하는 서비스 및 요구사항 우선순위에 따라 특화망의 구축 및 이용하는 형태가 달라질 수 있기 때문에 특화망 구축 전 충분한 자가진단이 이루어지도록 권고하고 있다.

[그림 2-12]은 5G 특화망 가이드라인에서 제시하는 5G 특화망 도입시 비용, 성능, 보안 측면에서의 평가요소를 도식화 한 것으로서, 보안적 측면에서 살펴보면 '데이터 관리'와 '조직 구성'에 따라 특화망의 보안 수준이 영향을 받을 수 있음을 알 수 있다.

'데이터 관리' 측면에서는 특화망으로부터 발생하는 데이터가 기업의 중요 데이터로서 사업장 내 전담인력을 통해서만 관리되어야 하는지, 또는 사업장 외 별도 장소에서 저장·관리되어도 무방한지에 대한 고려가 필요하다. 만일 데이터를 외부에 저장·관리가 어려운 민감한 중요 데이터인 경우 독립된 UPF를 포함한 5G 코어망을 사업장 내에 단독으로 구축하고, 독립된 5G 코어망에 대한 전담 인력이 관리·운영하는 것이 바람직하다. 이와 반대로 데이터를 외부에 저장·관리하는 것이 허용되는 경우에는 특화망 기간통신사업자의 UPF를 포함한 5G 코어망을 일부(제어평면, Control Plane) 공유하거나 전부를 공유·연동하는 방안을 채택할 수 있다.

[그림 2-12] 5G 특화망 도입시 비용, 성능, 보안 측면에서의 평가요소



자료: 과학기술정보통신부/한국방송통신전파진흥원, 5G 특화망 가이드라인, 2021

‘조직 구성’ 측면에서는 기업의 내부 인력을 통해 5G 특화망을 구축하고 운영할 수 있는 여력이 있는 기업은 네트워크의 기획단계부터 설계, 시공 과정에 있어서 5G 특화망을 직접 구축하고 검증함으로써, 기업의 시설, 조직 및 서비스 특성에 최적화된 맞춤형 네트워크를 구축·운영할 수 있으며, 보안적인 측면에서도 기업의 특성에 맞는 보다 강화된 보안성을 갖출 수 있는 장점이 있다. 반대로 여러 여건상 기업이 자체적인 5G 특화망 구축 및 운영 조직을 구성하기 어려운 경우 5G 특화망 기간통신사업자 등 외부 전문기관에 위탁하여 5G 특화망을 구축하고 운용할 수도 있다.

제 3 절 5G 특화망 구축 유형별 보안 고려사항

1. 사설 5G 망 구축 유형별 보안 특성

5G 특화망 서비스를 위한 네트워크의 구성은 크게 단말, 기지국을 포함한 액세스망(RAN), 코어망으로 구분할 수 있으며, 최근 5G에서의 초저지연・초고속・초연결 서비스 특성을 고려하여 액세스망을 포함하는 엣지 네트워크에는 MEC를 구성할 수도 있다.

일반적으로 5G 네트워크는 이동통신사업자의 상용 서비스(public 5G service)를 위한 구축 모델과는 별도로 기업이나 기관이 제한된 사용자만을 대상으로 제한된 서비스를 제공하기 위한 사설 5G 네트워크(private 5G 또는 non-public 5G network)의 구축도 가능하다. 대표적으로 5G-ACIA(5G Alliance for Connected Industries and Automation)에서 제시한 사설 5G 네트워크 구축을 위한 4가지 모델을 들 수 있다. 5G-ACIA에서 제시한 4가지 구축 모델로는 독립형 사설 5G 네트워크(Standalone non-public network), 무선 액세스 공유형 사설 5G 네트워크(Shared radio access non-public network), 무선 액세스 및 제어평면 공유형 사설 5G 네트워크(Shared radio and control plane non-public network), 무선 액세스, 제어평면 및 사용자 평면 공유형 사설 5G 네트워크(Shared radio, control and user plane non-public network)가 있으며, 이 4가지 구축 모델의 특징을 간략히 도식화하면 [그림 2-13]과 같다.

독립형 사설 5G 네트워크는 이동통신사업자의 상용망과는 완전히 독립적으로 격리된 5G 구축 모델이다. 선택적으로 상용망과 방화벽(firewall)을 두고 연결성을 보장할 수도 있지만, 기본적으로 물리적・논리적으로 독립된 환경을 제공함으로써 높은 보안성을 갖는 것이 특징이다.

무선 액세스 공유형 사설 5G 네트워크는 이동통신사업자의 상용망 중 무선 액세스 네트워크(RAN)만을 공유하여 구축하고, 그 외 코어망의 제어평면과 사용자 평면 그리고 모든 네트워크 자원은 이동통신사업자 상용망과 별도로 자체적으로 구축하는 방식이다.

[그림 2-13] 사설 5G 네트워크 구축 모델

자료: 5G-ACIA, Security Aspects of 5G for Industrial Networks, 2021

이때 기업의 사설 5G 망 내의 데이터는 논리적인 사설망 경계 내에서 유지된다. 기술적인 관점에서 이동통신사업자에게 독립형 사설 5G 네트워크와 무선 액세스 공유형 사설 5G 네트워크 간의 차이는 없다. 다만, 기업 입장에서는 이동통신사업자와 공유하는 기지국이 기업 가입자(단말)의 인증 데이터나 사용자 평면 보안 키에 대한 가시성(visibility)을 가지기 때문에 이 구축 모델에 대한 보안성을 함께 고려해야 한다.

무선 액세스 및 제어평면 공유형 사설 5G 네트워크는 이동통신사업자와 무선 액세스 네트워크와 코어망의 제어 평면을 함께 공유하는 모델이다. 다만 사용자 평면은 기업의 사설망 내부에 완전히 독립적으로 구성되어 있기 때문에 기업의 사설 5G 서비스 데이터는 논리적인 사설 5G 망 경계 내에서 유지되며 사용자 데이터에 대한 보안성을 제공할 수 있다. 그러나, 사설 5G 망 내의 단말은 코어망의 제어평면이 공유되어 있어 이동통신사업자로부터 가입자 관리를 제공받게 된다. 따라서 특정 가입자 그룹에만 접속을 허용하는 CAG(Closed Access Group) 기능을 통해 사설 5G 망 내의 단말에 대한 인증 및 접근제어 기능을 함께 고려할 수 있다. 3GPP 규격에서는 CAG 식별자(32bit의 CAG ID로서, CAG ID는 한 개의 PLMN 내에서 고유한 값을 가짐)를 방송하는 셀을 CAG 셀이라고 부르며, CAG 셀은 CAG 접속과 이동통신사업자망 접속을 모두 허용하는 셀 또는 CAG 접속만을 허용하는 CAG-only 셀일 수 있다. 일반적으로 단말은 CAG가 Allowed-CAG-List에 포함돼 있지 않더라도 수동 CAG 선택 기능을 통해 접속을 시도할 수 있다. CAG 선택은 단말에서 NAS 프로토콜에 의한 이동통신사업자(PLMN) 선택 과정을 통해 자동 PLMN 선택을 통한 CAG 선택과 수동 PLMN 선택 과정을 통한 CAG 선택이 모두 가능하다. 따라서, 이동통신사업자(PLMN) 선택과정에서 NAS는 검색된 CAG가 접속 가능한 CAG인지 판단하고 접속이 기능하면 이 CAG를 선택한다.

마지막으로 무선 액세스, 제어평면 및 사용자 평면 공유형 사설 5G 네트워크는 모든 사설 5G 네트워크 기능은 이동통신시업자의 망 내에서 호스팅되고, 사설 5G 망 내의 모든 기업 데이터는 이동통신사업자의 공용 네트워크 및 네트워크 장비를 통해 라우팅 된다. 바로 이전 모델과 마찬가지로 본 구축 모델의 경우에도 모든 기업의 단말이 이동통신사업자로부터 가입자 관리를 제공받게 된다. 따라서, 본 구축 모델의 경우에도 CAG 기능을 통해 사설 5G 네트워크 내의 단말에 대한 인증 및 접근제어 기능을 제공할 수 있다.

사설 5G 망 구축 유형은 5G-ACIA에서 제시한 사설 5G 네트워크 구축을 위한 4가지 모델을 기반으로 다양하게 정의될 수 있다. 대표적으로 국내 네트워크・통신 전문 컨설팅 그룹인 넷매니아즈(netmanias.com)는 5G-ACIA의 구축 모델을 보다 세분화하고 각 나라별 구축 사례를 종합하여 총 10개의 구축 모델과 모델별 장・단점을 제시한 바 있다.

[그림 2-14] 기업의 사설 5G 구축 모델

자료: Netmanias.com, https://www.netmanias.com, 2019

2. 5G 특화망 구성 방안

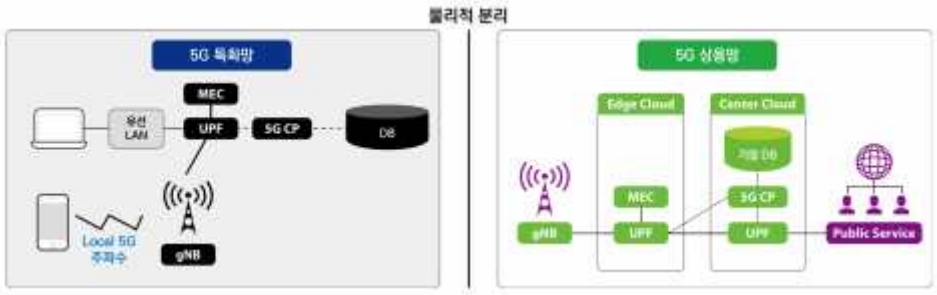
5G 특화망 구축 유형도 5G-ACIA에서 제시한 사설 5G 네트워크 구축을 위한 4가지 모델을 기반으로 5G 특화망 환경에 맞게 다양하게 정의될 수 있다. 나성욱(2021)은 국가 및 공공부문에 적용될 수 있는 방안으로 5G 특화망 구축 모델을 구분하고, 이동통신사업자의 상용망을 활용하는 정도에 따라 (1) 상용망과 완전분리된 특화망 구축 모델, (2) 상용망의 일부 자원을 공유하는 특화망 구축 모델, (3) 상용망을 활용한 특화망 구축 모델로 구분하여 총 6개의 구축 모델로 제시한 바 있다.

또한, 과학기술정보통신부와 한국방송통신전파진흥원이 발간한 ‘5G 특화망 가이드라인’에 따르면, 5G 특화망의 코어망 구축 방식에 따라 크게 3가지 구축 모델을 제시하고 있다. 본 절에서는 5G 특화망 가이드라인에 제시된 3가지 구축 모델인 5G 코어 독립구축 모델, 5G 코어 일부 공유 모델, 그리고 5G 코어 전부 공유 모델에 대해 정리하기로 한다.

먼저 5G 코어 독립구축 모델은 4.7GHz 대역 또는 28GHz 대역의 5G 특화망 전용 주파수를 이용하여, 기관이나 기업 내부에서 유선 LAN이나 Wi-Fi를 구축하는 것과

같이 5G 특화망을 맞춤형으로 설계·구축할 수 있는 방안이다. 이 경우 특화망은 기관·기업이 직접 구축하고 운영할 수도 있으며, 5G 장비 벤더나 기간통신사업자 등에게 위탁하여 구축하고 운영할 수도 있다.

[그림 2-15] 5G 코어 독립구축 모델



자료: 나성욱, 한국에서의 특화망 활용방안, 2021

장점

- 상용 이동통신서비스 면허 대역 주파수가 아닌 5G 특화망 전용 주파수 사용
- 단말과 응용 서버 간의 네트워크 지연이 수 ms 이내로서, 초저지연 서비스의 실현 용이
- 5G 특화망 서비스 데이터가 외부로 유출되지 않음
- 이동통신사업자 또는 기간통신사업자의 국사로 연결되는 광케이블 링크 불필요

단점

- 5G 무선 액세스, 코어망, MEC 플랫폼 등 모든 특화망 네트워크 노드를 직접 구축하기 위한 설계 및 구축 비용 부담
- 독립적으로 구축한 5G 특화망을 운용 관리하기 위한 전문 인력, 조직 및 운영 노하우 확보 필요
- 보안 고려사항
- 특화망과 이동통신사업자의 상용망이 물리적으로 완전히 분리되어 있어 완벽한 데이터 보안 확보

- 5G 특화망 가입자 정보, 인증 정보 및 서비스 이용 패턴 등의 중요 정보가 외부로 유출될 염려가 없음

5G 코어 일부 공유 모델은 이동통신사업자 또는 5G 특화망 기간통신사업자의 5G 코어망의 일부인 제어 평면(Control Plane)을 공유함으로써 5G 코어망의 구축 및 운용 부담을 경감시킬 수 있는 모델이다. 단, 기업의 특화망 사업장 내에 무선 액세스(기지국) 장비와 5G 코어의 서비스 데이터 처리를 위한 UPF 장비, MEC 서버 등의 플랫폼은 독립적으로 구축해야 한다.

[그림 2-16] 5G 코어 일부 공유 모델

자료: 나성욱, 한국에서의 특화망 활용방안, 2021

장점

- 상용 이동통신서비스 면허 대역 주파수가 아닌 5G 특화망 전용 주파수 사용
- 단말과 응용 서버 간의 네트워크 지연이 수 ms 이내로서, 초저지연 서비스의 실현 용이
- 5G 특화망 서비스 데이터가 외부로 유출되지 않음
- 5G 코어망(제어평면)의 구축 및 운용 유지보수 부담이 일부 완화됨

단점

- 5G 무선 액세스, 코어망 UPF, MEC 플랫폼 등 일부 특화망 네트워크 노드를 직접 구축하기 위한 설계 및 구축 비용 부담

- 독립적으로 구축한 5G 특화망을 운용 관리하기 위한 전문 인력, 조직 및 운영 노하우 확보 필요
- 이동통신사업자 또는 특화망 기간통신사업자와의 코어망 제어평면 연결 구축 필요 및 정기적 비용 발생

보안 고려사항

- 특화망과 이동통신사업자의 상용망이 물리적·논리적으로 분리되어 있어 서비스 데이터에 대한 보안 확보
- 5G 특화망 가입자 정보, 단말 정보, 인증 정보 및 서비스 이용 패턴 등의 기업 운영 정보가 이동통신사업자 또는 특화망 기간통신사업자의 서버에 저장되므로 추가적인 보안성 확보 방안 고려 필요

5G 코어 전부 공유 모델은 5G 특화망 사업장 내에는 무선 액세스(기지국) 장비만을 설치하고 특화망 기간통신사업자로부터 5G 코어장비의 전체(제어평면과 사용자 평면)를 공유하여 서비스로써 이용하는 방식이다. 따라서, 중소 규모의 사업장 등이 5G 코어 장비의 구축 부담을 줄일 수 있기 때문에 경제적인 특화망 구축 모델로서 고려될 수 있는 장점이 있다. 단, 기간통신사업자의 중앙 클라우드 영역에 위치하는 5G 코어 장비는 타 기업의 특화망 서비스와 함께 공유되어 운용될 수 있으므로 보안성에 상대적으로 취약한 점도 있다.

[그림 2-17] 5G 코어 전부 공유 모델

자료: 나성욱, 한국에서의 특화망 활용방안, 2021

장점

- 상용 이동통신서비스 면허 대역 주파수가 아닌 5G 특화망 전용 주파수 사용
- 5G 코어망의 구축 비용 부담이 없는 경제적인 구축 모델
- 이동통신사업자 또는 기간통신사업자의 전문 운용 서비스를 통한 운용 유지보수 부담이 크게 완화됨

단점

- 5G 특화망 서비스 데이터가 외부로 유출될 수 있음
- 단말과 특화망 기간통신사업자의 클라우드에 위치하는 응용 서버 간의 네트워크 지연에 따라 초저지연 서비스의 실현 가능성 검토 필요
- 이동통신사업자 또는 특화망 기간통신사업자와의 코어망 연결을 위한 광케이블 연결 필요 및 정기적 서비스 이용요금 등 운용 비용 발생

보안 고려사항

- 특화망 내 단말의 서비스 데이터가 이동통신사업자 또는 특화망 기간통신사업자망까지 전달되므로 서비스 데이터에 대한 보안 확보
- 5G 융합서비스 플랫폼인 MEC도 외부 망에 위치하고 다른 특화망 이용 기업과 공유된 자원을 활용할 수 있으므로 서비스 데이터에 대한 보안 확보 및 악성 코드 감염 등에 대한 보안성 확보 방안 검토 필요
- 5G 특화망 가입자 정보, 단말 정보, 인증 정보 및 서비스 이용 패턴 등의 기업 운영 정보가 이동통신사업자 또는 특화망 기간통신사업자의 서버에 저장되므로

추가적인 보안성 확보 방안 고려 필요

상기 3가지 5G 특화망 구축 모델의 장점, 단점 및 보안 고려사항을 정리하면 다음의 그림과 같다. 보안적인 측면만을 고려했을 때에는 완전한 독립형 5G 특화망을 설계·구축하는 것이 가장 바람직한 모델이다. 그러나, 기업의 규모나 특화망 적용 사업장의 물리적, 지리적, 환경적 특성, 5G로 연결되는 단말 및 서비스의 특성 등을 종합적으로 검토하여 아래 그림에서 제시된 데이터 관리, 유지보수 인력, 비용, QoS, 서비스 지연시간 등을 보안과 함께 종합적으로 검토하여 5G 특화망 구축 모델을 결정하여야 한다.

[그림 2-18] 5G 특화망 구축 모델별 특성 비교

구 분	데이터 관리	유지보수 인력	비용절감	보 안	정기 사용료	QoS보장	서비스 지연 최소화
5G코어 독립구축	◎	◎	△	◎	◎	◎	◎
5G코어 일부공유 (CP한정)	○	△	○	○	○	○	◎
5G코어 전부공유	△	△	◎	△	△	○	△

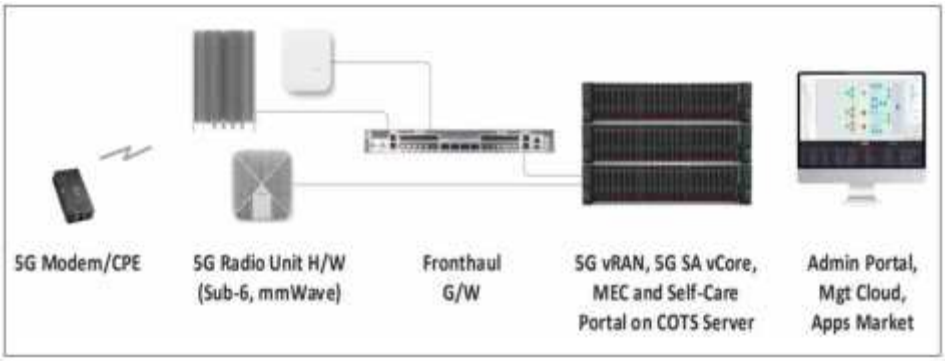
※ ◎ : 매우우수 또는 매우필요, ○ : 우수 또는 필요 , △ : 보통

자료: 과학기술정보통신부/한국방송통신전파진흥원, 5G 특화망 가이드라인, 2021

제 4 절 5G 특화망 구성요소별 보안 요구사항

앞서 기술한 바와 같이, 5G 특화망 서비스를 위한 네트워크의 구성은 크게 단말, 기지국을 포함한 액세스망(RAN), 코어망으로 구분할 수 있으며, 최근 5G에서의 초저지연·초고속·초연결 서비스 특성을 고려하여 액세스망을 포함하는 엣지 네트워크에는 MEC를 구성하여 보다 다양한 융합서비스를 제공할 수도 있다. 본 절에서는 주요 네트워크 구성 요소별 보안 요구사항에 대해 정리한다.

[그림 2-19] 5G 특화망 토탈 솔루션(예시)



자료: 과학기술정보통신부/한국방송통신전파진흥원, 5G 특화망 가이드라인, 2021

1. 5G 특화망 단말 보안 요구사항

5G 특화망의 단말은 스마트폰, 태블릿, 신규 설비에 5G 모뎀을 적용하거나, 사업장 내의 기존 설비의 경우에는 CPE(Customer Premises Equipment) 또는 모바일 라우터 형태로 5G 특화망과 연동할 수 있다.

단말 내 SIM(Subscriber Idenity Module) 또는 eSIM(embedded SIM)을 내장하고 가입자 식별변호를 부여함으로써 코어망에서 단말의 인증 및 관리 기능을 구현할 수 있다. 단, 관리해야 할 단말 및 가입자의 규모가 늘어날 경우에는 별도의 SIM 관리 솔루션 도입을 고려해야 한다.

[그림 2-20] 5G 특화망 주요 단말 형태

자료: 과학기술정보통신부/한국방송통신전파진흥원, 5G 특화망 가이드라인, 2021

5G 특화망을 이동통신사업자 또는 특화망 기간통신사업자와 완전히 분리·독립된 네트워크로 구축하지 않은 경우에는 앞서 2절에서 제시한 바와 같이 특정 가입자 그룹에만 접속을 허용하는 CAG(Closed Access Group) 기능을 통해 5G 특화망 내의 단말에 대한 인증 및 접근제어 기능을 함께 고려해야 한다.

특히 5G 특화망 환경에서 민감한 기업정보나 서비스 정보가 유통되는 경우에는 보다 강화된 단말 보안이 고려되어야 한다. 예를 들어, 기업 설비가 아닌 스마트폰이나 태블릿을 통해 5G 특화망에 접속하는 경우, 단말에 삽입된 SIM 또는 eSIM 만으로 사용자를 인증하고 망에 접속할 수 있는 권한이 주어지기 때문에, 사용자 인증 등과 같이 2차 인증 방식의 도입도 적극 검토할 수 있다.

더욱이 5G 라우터나 5G 에그 등과 같이 5G 모뎀을 탑재하지 않은 다른 단말이 5G 특화망에 접속할 수 있도록 허용하는 단말의 경우, 실질적으로 5G 특화망에 접속하는 단말은 5G 라우터나 5G 에그가 아니라, 여기에 접속하는 스마트폰, 노트북 또는 IoT 장비들이 될 수 있다. 따라서, 실제 접속하는 단말에 대한 인증보다는 5G 라우터나 5G 에그 등에 대한 단말 인증만으로 5G 특화망에 접속할 수 있는 권한을 부여할 수 있으므로 다단계 인증 방식 등을 도입함으로써 비인가된 단말이 5G 라우터 등을 통해 기업의 특화망에 접속할 수 없도록 해야 한다.

[그림 2-21] 4G 대비 5G 무선 구간에서의 암호화 및 무결성 요구사항

	5G (TS 33.501)	4G (TS 33.401)
NAS Integrity	Mandatory	Mandatory
NAS Confidentality	Optional+	Optional
RRC Integrity	Mandatory	Mandatory
RRC Confidentiality	Optional+	Optional
UP Integrity	Optional	Forbidden
UP Confidentiality	Optional+	Optional

☆ Optional+: Optional to use, but should be used whenever regulations permit

자료: 박종근 외, 5G 보안 구조의 특징 및 주요 개선사항, 2019

5G 네트워크는 망과 단말 사이의 상호인증 절차가 성공적으로 마무리되면 단말과 망 사이에 주고받는 시그널링 메시지와 사용자의 서비스 데이터를 보호하기 위한 기밀성 및 무결성 보호 절차가 진행된다. 5G 단말과 5G 코어망의 AMF(Access and Mobility Management Function) 사이의 시그널링 프로토콜인 NAS(Non-Access Stratum), 5G 단말과 5G 기지국 사이의 시그널링 프로토콜인 RRC(Radio Resource Control) 그리고 사용자 데이터 트래픽(User Plane)에 대한 기밀성 및 무결성 요구사항을 3GPP에서는 [그림 2-21]과 같이 정의하고 있다.

4G LTE에서는 NAS와 RRC 시그널링 메시지에 대한 무결성 보호만을 강제사항으로 정의하였으며, 사용자 데이터에 대한 무결성 보호는 정의되지 않았다. 사실상 무결성 보호는 패킷 크기와 함께 무엇보다도 단말과 기지국에서 무결성 검증을 위한 부하가 증가하는 부담이 매우 크다. 그러나, 5G에서는 사용자 데이터 전송에 대한 무결성 보호 기능을 강제사항은 아니지만 선택사항으로 명시함으로써 무선 접속 환경에서의 데이터 위·변조가 우려되는 민감한 서비스 환경에서는 가급적 사용자 데이터에 대한 무결성도

보호하도록 권고하여 데이터 보호 체계를 강화하였다. 또한 암호화를 통한 시그널링 데이터 및 사용자 데이터의 기밀성 보호 체계에 있어서도 4G LTE에서와 같이 단순 선택사항으로 권고하기 보다는 특별한 제약사항이 없는 한 암호화를 사용하도록 한층 강화된 데이터 보호 체계를 정의하고 있다.

따라서, 5G 특화망을 도입하는 기업에서는 5G 특화망에 접속할 단말을 선정할 때 이와 같은 무선 구간에서의 시그널링 데이터 및 사용자 데이터에 대한 기밀성과 무결성 보장 여부를 반드시 고려해야 한다. 즉, 민감한 데이터나 중요 정보를 유통하는 단말의 경우에는 반드시 시그널링 데이터 및 사용자 데이터에 대한 기밀성과 무결성을 보장하도록 하고, 이를 위해 충분한 시스템 자원을 갖춘 단말을 선정해야 한다. 더욱이 기밀성과 같이 암호화 수준을 강화할수록 제한된 시스템 자원을 갖춘 단말에서는 서비스 처리 속도의 저하를 초래할 수 있으므로 일률적인 기밀성 및 무결성을 강제하기 보다는 기업의 5G 특화망 환경, 서비스 요구사항. 데이터 보안 요구사항 등을 종합적으로 검토하여 안전한 단말 보안 환경을 설계·구축할 수 있어야 한다.

2. 5G 특화망 네트워크 보안 요구사항

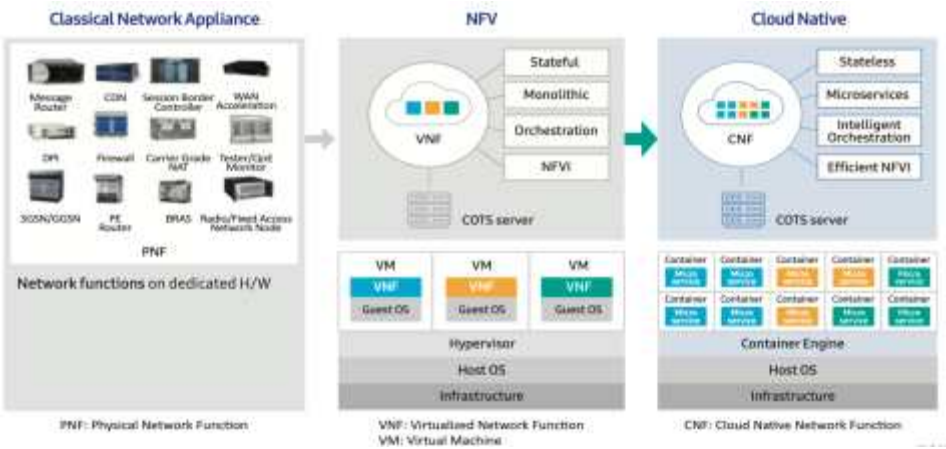
5G 네트워크의 가장 큰 변화 중 하나는 SDN(Software-defined Networking)/ NFV(Network Functions Virtualization) 기술을 바탕으로 한 가상화를 통해 네트워크 소프트웨어화를 꼽을 수 있다. 4G LTE부터 이동통신사업자는 CUPS(Control and User Plane Separation) 접근법에 따라 제어 평면은 가상머신 형태의 가상화를 도입하여 유연한 이동통신망 구현을 적용한 바 있다.

가상화를 통해 이동통신망을 보다 유연하고 서비스에 동적으로 프로그래머블한 구조적 이점을 추구한 반면, 보안적인 측면에서는 가상화에 따른 공격 접점(attack surface)의 증가 뿐만 아니라 물리적 자원 공유에 따른 완전한 격리 환경의 보장이 어려운 취약점이 존재한다. 예를 들어, SDN/NFV 인프라 및 관리 플랫폼 공격을 통한 서비스 장애, 자원 고갈, 민감정보의 탈취 등의 위협이 발생할 수 있으며, 가상화된 네트워크 장비 이미지의 조작이나 악성코드 감염에 의한 서비스 장애 또는 중요 정보의 유출도 발생할 수 있다. 더욱이 네트워크 슬라이스간 불완전한 격리로 인해 네트워크 슬라이스 간 공격이나

부채널 정보를 이용한 보안 정보의 유출 등도 가상화에 따른 잠재적인 보안 위협으로 고려될 수 있다.

더욱이 5G 네트워크 장비의 가상화가 무선 액세스(RAN)는 물론 코어망까지 적용되고 있으며, 가상화 방식도 가상머신(virtual machine)을 운용하는 시스템 가상화 방식에서 클라우드 네이티브(cloud native) 기반 컨테이너를 운용하는 운영체계 가상화로 진화하고 있는 점도 고려해야 한다. 이미 삼성전자는 클라우드 네이티브 방식을 기반으로 차세대 5G 클라우드 코어망을 개발한 바 있다. 클라우드 네이티브 기반의 가상화 환경에서의 보안 고려사항은 다음 절에서 다시 살펴보기로 한다.

[그림 2-22] 5G 네트워크 장비의 구조 진화



자료: 삼성전자, Cloud Native 5G Core, 2020

5G 특화망 구축시 높은 보안성이 요구되는 경우에는 도입되는 네트워크 장비에 대한 네트워크 보안 인증 획득 여부를 고려할 수 있다. 5G 특화망 도입시 고려해야 할 대표적인 보안 인증제도는 CC(Common Criteria) 인증, 보안적합성 검증, KCMVP(Korea Cryptographic Module Validation Program)을 꼽을 수 있다.

CC 인증 제도는 정보보호 제품에 대한 국제적인 신뢰성 확보 및 국가통신망 정보보호 수준 제고를 위한 목적으로 시행되는 제도로서, 정보보호제품 평가·인증 수행규정,

제품군별 보호 프로파일(PP; Protection Profile)을 기준으로 인증을 수행한다. 대표적인 대상 제품군으로는 방화벽, IPS(Intrusion Protection System). DDoS 대응장비, 접근 통제 등 20종의 보안제품 및 솔루션이 주요 인증 대상이다.

보안적합성 검증은 국가정보통신망의 보안 수준 제고를 위해 국가·지자체·공공기관이 도입하는 정보보호시스템, 네트워크 장비 등 보안 기능이 탑재된 IT 제품의 안전성을 검증하는 제도로서, 국제 CC인증 제품 및 L3 이상 네트워크 장비, SDN(Software-Defined Networking) 등 가상화 제품이 주요 대상이다. 최근에는 보안적합성 검증 제도를 생략하기 위한 제도로서 보안기능 확인서 제도가 시행되고 있으며, 이는 공인된 시험기관으로부터 '국가용 보안요구사항' 만족 여부를 검증하는 방식이다.

KCMVP 검증제도는 행정기관 등 국가·공공기관 정보통신망에서 소통되는 자료 중 비밀로 분류되지 않은 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도로서, 검증 대상이 되는 암호모듈은 소프트웨어, 하드웨어, 펌웨어 또는 이들을 조합한 형태가 모두 대상이 될 수 있다.

[그림 2-23] 5G 특화망 도입시 고려해야 할 네트워크 보안 인증제도

대 상	인 증	담당부처·기관	관계법률
방화벽, IPS, DDOS대응장비, 접근통제 등 20종 보안제품·솔루션	CC인증	과기부, ITSCC	국가정보화법
국제CC인증 제품 및 L3이상 네트워크 장비, 가상화(SDN) 제품 (국가·지자체·공공기관 한)	보안적합성검증	국정원, 국가보안기술연구소	전자정부법
암호화모듈 (국가·지자체·공공기관 한)	KCMVP	국정원, 국가보안기술연구소	전자정부법

자료: 과학기술정보통신부/한국방송통신전파진흥원, 5G 특화망 가이드라인, 2021

기업이 5G 특화망을 구축하고 외부 인터넷과의 연동이 필요한 경우에는 CC 인증을 받은 보안제품·솔루션을 도입함으로써 해킹 등의 보안위협 등으로부터 기업의 5G

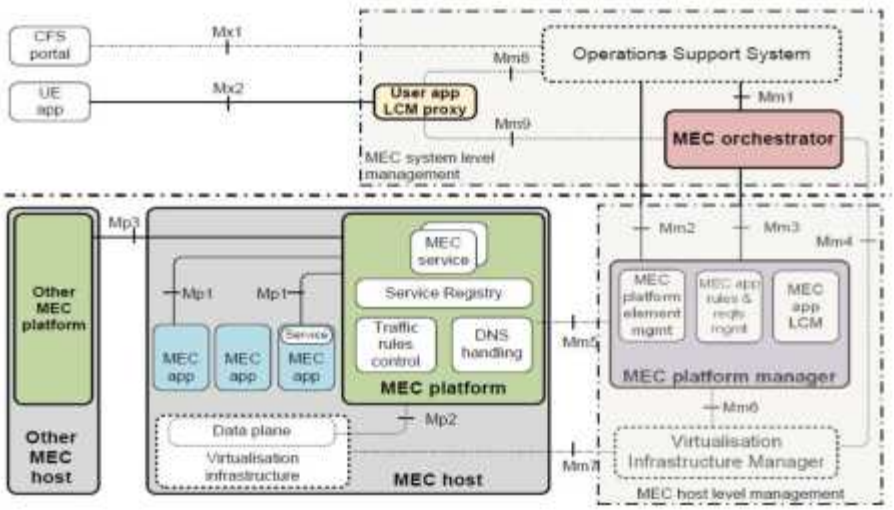
특화망을 보호할 수 있다.

또한, 국가, 공공기관 및 지자체의 경우 5G 코어장비 등 가상화 장비에 대한 보안적합성 검증은 물론 단말~서버 간의 암호화 적용시 KCMVP 검증필을 받은 암호모듈을 반드시 적용해야 한다.

3. 5G 특화망 MEC 보안 요구사항

5G MEC는 5G 기반의 융합서비스 특히 초저지연, 초고속과 같은 서비스를 실현하기 위한 핵심 인프라로서, NFV 기술을 바탕으로 융합서비스 등을 실행하기 위한 3rd party 응용이 실행될 수 있는 개방형 시스템이다. 특히, 기업이 맞춤형 서비스로 구축하는 5G 특화망에서는 데이터 보안성을 고려하여 서비스 플랫폼이 외부 클라우드 등에 위치하기보다는 특화망 내에 구축하는 것이 바람직하다.

[그림 2-24] 5G MEC 시스템 구조



자료: F. Giust, et.al., Multi-Access Edge Computing: An Overview of ETSI MEC ISG, 2017

5G MEC 플랫폼에 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, 악성코드에 감염된 MEC 응용을 통해 다른 서비스의 장애를 유발하거나 민감한 정보를 유출하는 공격 등을 꼽을 수 있으며, 이는 5G 특화망에 구축되는 MEC에서 동일하게 발생할 수 있는 잠재적 보안 위협으로 고려될 수 있다. 따라서, 5G MEC 보안위협에 대응하기 위해 가상화된 MEC 플랫폼이나 실행중인 MEC 응용의 보안위협 및 이상행위를 실시간 탐지하고 대응할 수 있는 보안 기술의 적용 뿐만 아니라, 외부에서 공급되는 MEC 응용의 무결성을 보장하고 취약성을 검증할 수 있는 보안 기술의 도입을 고려해야 한다.

특히 최근 대두되고 있는 클라우드 네이티브 기반의 가상 환경은 기존 가상머신을 이용한 시스템 가상화 환경보다 자원의 격리성(isolation)이 상대적으로 취약한 것이 특징이다. 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 가상머신 보다 상대적으로 경량화된 컨테이너로 실행하고, 버그의 패치를 포함한 새로운 기능의 업데이트는 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 5G 이동통신 환경에서도 동일하게 추구할 수 있는 장점이 있다.

앞서 2절에서도 언급한 바와 같이, 삼성전자에서도 클라우드 네이티브 기반의 5G 클라우드 코어망을 개발하여 제품화한 바와 같이, 5G 네트워크 장비 및 MEC 환경의 클라우드 네이티브도의 전환은 가속화될 전망이다. 따라서, 클라우드 네이티브 환경으로 5G 특화망 MEC 플랫폼 도입에 대비하여 컨테이너에 대한 보안위협과 빈번하게 발생하는 MEC 응용 이미지의 업데이트로 인해 조작되거나 악성코드에 감염된 비정상 이미지가 5G 특화망 내로 유입될 수 있는 보안위협에 대응할 수 있는 보안 기술 체계를 고려해야 한다.

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 보안 기술 도입을 고려해야 한다.

제 3 장 5G 특화망 보안 고려사항

제 1 절 5G 특화망 연결 기기 보안 고려사항

5G 특화망은 기업이 구축하는 모바일 네트워크로 다양한 사용자 단말이 연결될 수 있다. 업무용 PC, 모바일 기기, IoT 기기, 5G 중계 게이트웨이 등이 5G 특화망에 연결될 수 있기 때문에 각 기기의 특성에 맞는 보안 고려사항 적용이 필요하다.

<표 3-1> 5G 특화망 연결 기기 유형

구 분	설명
모바일 기기	· 노트북, 스마트폰, 테블릿 등 5G 특화망에 접속하는 모바일 기기
IoT 기기	· CCTV, 산업용 IoT 기기 등 5G 특화망을 구축하는 기업에 사용되는 IoT 기기
5G 중계 게이트웨이	· 이동통신사업자 기지국과 5G 연결기기 간 중계해주는 장비로서 5G 무선통신과 와이파이 또는 에그 장치

IoT 기기의 경우 성능 제한이 있을 수 있기 때문에 고수준의 보안 기능을 탑재하기 어렵기 때문에 취약한 패스워드, 오래된 보안 취약점을 가진 채 방치되어 변조에 취약하고 악성 어플리케이션에 의한 부적절한 접근, 중간자공격으로 인한 가입자 정보(SUPI) 정보 유출 등 취약한 환경에 노출될 가능성이 높다.

본 절에서 공통적으로 적용할 수 있는 보안 고려사항으로 인증 및 접근통제, 패스워드 및 암호화 등을 설명한다.

5G 특화망에 연결되는 기기를 보호하기 위한 공통적인 보안 고려사항으로는 인증 및 접근통제, 패스워드 관리, 암호화 및 키관리, IoT 플랫폼 보안, 5G 통신망 연결 기기 인증 및 보안 관리를 수행하여야 한다.

<표 3-2> 5G 특화망 보안 고려사항

연결 기기 보안 고려 사항	인증 및 접근통제	어플리케이션 보안특성에 부합된 단말 인증 프로토토콜 적용 및 역할기반의 엄격한 접근통제가 고려되어야 함. 인증정보는 반드시 보호되어 저장되어야 함
	안전한 패스워드 관리	패스워드 보호 정책이 수립 및 시행되어야 함
	암호화 및 키관리	어플리케이션 보안특성에 부합된 암호화 알고리즘 및 키 관리가 적용되어야 함
	IoT 플랫폼 보안	임베디드 IoT 운영체게 보안 및 안티바이러스 설치・운영, 주기적인 소프트웨어 갱신・보안 패치 관리, 시큐어 코딩 적용 확인 등 IoT 연결 기기의 플랫폼을 위한 통합 보안이 적용되어야 함
	5G 연결 IoT 기기 등록, 인증 관리	연결 IoT의 식별 및 등록, 상호인증, 운영상태 관리가 적용되어야 함
	5G 중계 게이트웨이 보안	IoT 중계 게이트웨이 장비의 인증 및 펌웨어 보안이 시행되어야 함
연동 구간 및 네트 워크 보안 고려 사항	네트워크 보호	비정상 트래픽 대응 보안장비 및 5G 전용 네트워크 보안 솔루션이 구축되어야 함. 또한, 비인가 접속 차단을 위해 상호인증과 접근통제가 적용되어야 하고, 네트워크 전송 데이터 보호를 위해 최소한 기밀성과 무결성, 인증이 적용되어야 함
	기업 내부 네트워크 연동 구간 보호	기업 내부 네트워크에 대한 외부 연결을 제한하고, 기업 내부 네트워크를 세분화 및 분리하여 기업 내부 시스템을 보호함. 또한, 분리된 내부 네트워크 영역간 데이터 이동시 영역간 네트워크 연동 구간을 안전하게 보호되어야 함
	네트워크 슬라이싱 보호	네트워크 슬라이스간 물리적 논리적 격리가 필요하고, 네트워크 기능간 접근통제가 요구됨
네트 워크 통신 장비 보안 고려 사항	물리적 접근통제	주요 5G 통신장비 배치 구역을 통제구역으로 설정하고, 이에 대한 물리적 접근시도를 탐지・차단하기 위한 보안 솔루션이 적용되어야 함
	5G 통신장비 보안	5G 통신장비에 대한 주기적인 취약점 점검, 장비보호를 위한 보안 솔루션 구축 및 운영, 장비 관리자에 대한 인증 및 접근통제가 적용되어야 함
	SDN/NFV 가상화 인프라 보안	가상자원(가상 PC, 가상 스토리지, 가상 SW)을 위한 관리방안 수립 및 운영, 가상자원 접근을 위한 인터페이스 및 API의 주기적인 보안취약점 점검,

		악성코드로부터 가상환경 보호, SDN 컨트롤러 보호를 위해 가상화 인프라 보안장비를 도입
	5G 공급망 보안	외주 개발 및 오픈소스 SW 업데이트 보안 관리 체계를 수립해야 함. 안전한 경로(White List 방식 안전한 경로 상 IP, URL)를 통한 보안 패치와 보안 패치 후 안전성과 보안성 테스트를 수행해야 함
MEC 및 어플리케이션 보안 고려사항	MEC 플랫폼 보안	클라우드 인프라와 NFV 기술을 기반으로 가상 머신 보안, 컨테이너 보안 등 가상화된 보안 솔루션을 구축해야 함. 또한, MEC 소프트웨어 보안을 위해 VNF 소프트웨어 패키지에 대한 서명(발행자)과 검증(수신자), 서명검증 등을 적용해야 하고, 상호 원격 재해 복구를 제공함으로써 MEC 서비스 장애관리를 제공해야 함
	MEC 연동 구간 보안	MEC 연결 API 보호를 위한 보안솔루션 도입 및 MEC 연동구간 보안관제 적용을 통해 MEC 연동 구간을 보호함
	MEC 어플리케이션 보안	MEC 어플리케이션 보호를 위해 엄격한 어플리케이션 인증 및 통신채널 보안, 어플리케이션간 접근통제, 감사 및 모니터링을 도입해야 함
	MEC 데이터 보호	MEC 데이터 보호를 위해 데이터 자신 식별, 데이터 위변조 및 유출 방지, 개인정보 및 민감 데이터 비식별 조치, 저장 데이터 보호를 적용해야 함

1. 인증 및 접근통제

- 5G 단말 인증 프로토콜 : 5G특화망은 탑재된 어플리케이션에 보안 요구사항을 만족하도록 구축되어야 한다. 따라서, 1차인증 필수 인증 프로토콜인 5G AKA/ EAP-AKA’가 어플리케이션의 보안 요구사항을 만족하지 못할 경우, 이를 대체하도록 2차 인증을 도입하거나, 1차인증에서 EAP 계열의 강력한 인증 프로토콜(예: EAP-TLS)을 도입하는 것이 바람직하다.
- 인증정보 보호 : IoT 기기를 도입 시 비밀번호, PIN 번호 등 인증정보 저장 시에 평문으로 저장하지 않고 보안 강도가 높은 일방향 해시함수 사용, DB 접속과 같은 인증정보가 필요한 경우 암호화하여 저장되는지 확인하여야 한다.
- 역할기반 접근통제 : 사용자 단말 및 IoT 기기의 특성과 사용자의 역할을 식별하여

역할별로 권한을 관리하는 정책을 수립하여야 한다. 관리자 권한이 일반 사용자에게 부여되지 않도록 하여야 하며, 중요 기능의 접근 및 사용을 할 경우에는 사용자 인증 후 허가된 관리자 및 사용자로 제한하는 접근통제 수단을 제공해야 한다.

- 관리자 인증 : IoT 제품의 설정과 제어 등의 관리 서비스나 민감정보에 접근 시에는 반드시 인증을 수행하여야 하며, 반복된 인증 시도에 대해서 횟수 제한 등 인증을 제한하는 기능을 제공해야 한다.
- IoT 기기 관리자 및 특수권한 관리 : 관리자 및 특수 목적을 위해 사용하는 계정 및 권한은 최소한으로 부여하고 계정 및 권한 할당 시에는 책임자의 승인을 포함한 인가 절차 수립하여야 한다. 또한, 특수 목적을 위해 부여한 계정 및 권한을 식별하고 목록을 관리하여야 하며, 최소한 Multi-Factor 인증 방식을 적용하여야 한다.

2. 안전한 패스워드 관리

- 안전한 패스워드 설정 : 정부가 가이드하는 안전한 비밀번호 기준에 따라 패스워드의 복잡도와 변경 주기에 따라 패스워드 생성 및 변경 관리를 하여야 한다.
- 패스워드 보호 정책 수립 : 패스워드 저장 시 암호화, 패스워드 입력 시 마스킹 처리, 일정 횟수 이상 패스워드 오류 시 접근제한 등의 패스워드 보호 정책을 수립하여야 한다.
- 초기 설정 비밀번호 변경 : IoT 기기를 최초 도입 단계에서 초기 인증정보 변경하는 단계를 가져야 한다. 제조사 배포한 초기 패스워드 및 단순한 패스워드 설정에 대해서 보안성이 높은 패스워드로 변경하도록 IoT 기기 초기 인증 후 사용자에게 인증정보를 변경하는 수단을 제공해야 한다.

3. 암호화 및 키관리

- 안전한 암호 알고리즘 사용 : 보안 강도가 낮은 암호 알고리즘을 사용하는 경우 데이터에 대한 암호문을 복호화할 수 있는 가능성이 존재한다. 따라서 안전하게 데이터를 보호하기 위해 국내에서 권고하는 암호 알고리즘을 사용하거나 일정 보안 강도 이상이 암호키 길이를 가진 암호 알고리즘을 사용하여야 한다.

- 안전한 암호화키 관리 방안 수립 : 안전하게 암호키가 생성되지 않을 경우에는 암호화된 데이터에 대한 기밀성이 보장되지 않으므로 안정성이 검증된 암호키를 생성해야 한다. 따라서 암호화 키를 관리, 생성 및 안전한 보관을 위해 정책 수립과 키 관리 기술 적용하여야 한다.

4. IoT 플랫폼 보안

- 불필요한 오픈 접근 포트 제거 : 제품 개발 시 디버깅용 오프 포트(예, JTAG 등), 사용하지 않는 서비스 포트 등을 제거하여야 한다.
- 펌웨어 및 소프트웨어 위변조 방지 : 악성코드를 펌웨어에 추가하여 배포하는 공격 등 펌웨어 위변조 방지를 위한 서명 검사 등 임베디드 플랫폼 위변조 방지 기술 적용하여야 한다.
- 임베디드 IoT 운영체제 보안 : 방화벽 기능 설정, 불필요한 서비스 제거, 기본 공유 폴더 제거, 비인가 저장장치 연결 시 접근 제한 등을 설정하여야 한다.
- 주기적인 소프트웨어 업데이트 및 보안 패치 관리 : 5G 연결 기기들의 버전 업데이트 주기를 고려하여 주기적인 패치 관리를 하여야 한다. 또한, 안전한 업데이트를 위해 신뢰할 수 있는 업데이틀 서버를 통해서 업데이트가 수행되어야 한다.
- 안티바이러스 설치 및 운영 : 코드 감염경로 유입을 차단하기 위해 권장 백신 SW 사용, 악성 프로그램 실행방지 등 조치하여야 한다.
- 주기적인 취약점 점검 : 안티바이러스 점검 등 기기의 보안성 검증 및 보안 조치 수행하고 미조치 시 통신망 접속 제한을 하여야 한다.
- 시큐어 코딩 적용 확인 : 기업용 IoT 기기 및 플랫폼 도입 시 소프트웨어 개발보안 가이드, IoT 제품 개발 시 보안 가이드를 참고하여 안전하게 구현되었는지 또는 IoT 보안인증획득 제품 도입을 고려하여야 한다.

5. 5G 연결 IoT 기기 등록, 인증 관리

- 5G 특화망 연결 IoT 기기 식별 및 등록 : 기기 위변조 방지를 위해 유일성, 불변성 특성을 가진 기기 고유 식별자 (SUPI, MAC Address 등)를 활용하여 해당

기기를 유일하게 식별하고 등록 관리하여야 한다.

- IoT 기기 상호 인증 : 5G 통신망에 연결 시에는 기기와 기기, 기기와 게이트웨이, 기기와 5G 통신 서버 간 상호 인증 기술 적용하여야 한다.
- IoT 기기 보안 관리 : IoT 기기 운영상태를 주기적으로 관리 서버에 전송하여 IoT 기기 플랫폼에 대한 관리가 이뤄져야 한다.

6. 5G 중계 게이트웨이 보안

- IoT 중계 게이트웨이 인증 관리 : IoT 기기 게이트웨이(무선 AP, 에그 등) 유일한 식별정보(IP주소, MAC 주소, UICC 등) 활용하여 5G 통신망에 연결되는 중계 게이트웨이 장비 인증을 수행해야 한다.
- 게이트웨이 펌웨어 보안 : 펌웨어 변조 및 악용에 대응하기 위한 전자서명 적용, 안전한 업데이트 및 업데이트 시 관리자 인증 등 수행하여야 한다. 펌웨어 파일에는 부트로더, 설정파일, 키 파일, 소스코드, 서명 값 등이 포함되어 있으므로 공개된 역공학 도구를 통해 분석되지 않도록 적절한 수준의 펌웨어 보호 기법을 적용하여야 한다.

제 2절 5G 특화망 연동 구간 및 네트워크 보안 고려사항

본 절에서는 5G 특화망 네트워크와 5G 특화망에 연동되는 기업의 내부망 또는 인터넷망과 내부 연동 구간에 대한 보안 고려사항을 설명한다. 5G 특화망 네트워크는 5G 코어망을 구성하는 제어 평면상의 통신장비와 사용자 평면상의 통신장비, MEC 플랫폼 등의 5G 네트워크 장비들로 구성된 특화망 네트워크를 말하며, 내부 연동망은 5G 특화망 네트워크와 연결되는 기업 내부망(인터넷망 포함)을 의미한다.

5G 특화망 네트워크 및 내부 연동구간 보안 고려사항으로는 5G 특화망 보호, 기업 내부 네트워크와 연동구간 보호, 네트워크 슬라이싱 보호로 구분한다.

1. 5G 특화망 네트워크 보호

- IP 및 5G 네트워크 보안장비 구축 : 비정상 트래픽 분석 및 탐지, 차단 기능을 지원하는 네트워크 보안장비, GTP 방화벽 등 5G 전용 네트워크 보안 솔루션이 구축되어야 한다.
- 네트워크 접근통제 및 상호인증 : 비인가 통신을 제어하기 위한 5G 네트워크 접근제어, 제3자에 의한 통신 데이터 노출 또는 위변조를 방어를 위한 통신장비 간 인증(단방향 인증, 상호인증) 적용하여야 한다.
- 전송 데이터 보호 : 5G 네트워크를 통해 전송되는 민감한 정보는 기밀성 및 무결성이 보장되도록 안전한 암호 알고리즘을 적용하여 암호화 또는 안전한 암호통신 프로토콜을 이용하여 전송하여야 한다.

2. 기업 내부 네트워크 연동 구간 보호

- 기업 내부망과 분리 : 네트워크 세분화 및 분리를 통하여 네트워크 무결성을 보장하고 중요도가 높은 시스템의 네트워크를 중요도가 낮은 시스템의 네트워크와 물리적 또는 논리적으로 분리하여야 한다.
- 내부 네트워크 연동 구간의 데이터 전송 보안 : 분리된 네트워크 영역 간 파일 이동 시 안전한 방법(망간자료전송 등)을 활용하여야 한다.

- 기업 내부망의 내부 시스템 보호 : 중요시스템은 이중화하여 운영, Legacy 내부 시스템과 5G 네트워크 구축된 시스템과는 정의된 통신 트래픽만 허용하여야 한다.
- 공개 서버 관리 : 기업 내부망의 업무 네트워크와 5G 네트워크 간에 직접적인 통신 연결을 하지 않고 중간에 DMZ 영역을 구축하여 공개 서버를 구축하고 관리하는 것을 고려해야 한다.
- 시스템에 대한 외부 연결을 제한 : 외부 시스템 연결이 필요할 경우 연결 기본 값은 거부로 설정해야 하며, 보안 채널 옵션 비활성화, 구간 암호화 방식 VPN 등 기술적·관리적 보안조치 필요하다.

3. 네트워크 슬라이싱 보호

- 네트워크 슬라이스 간 격리 : 네트워크 슬라이스는 기지국, 코어네트워크, MEC 간 5G 코어 네트워크 인프라를 공유하므로 네트워크 슬라이스 간 물리적 논리적 격리가 필요하다.
- 네트워크 기능(Network Function)간 접근통제 : 서로 다른 보안 수준을 가진 NF를 다른 보안 도메인에 배치할 수 있다. 5세대(5G) 통신망에는 MEC 애플리케이션이 대거 탑재돼 있다. UPF와 같은 NF는 코어에서 네트워크 가장자리로 재배치해야 하며 기지국이나 DU/CU와 동일한 위치에 배치할 수 있다. 재배치된 NF와 다른 핵심 NF가 서로 다른 보안 영역에 존재한다는 의미다. 슬라이스 공유 NF가 슬라이스 특정 NF에 액세스하는 경우, 무단 액세스를 방지하기 위해 보안 보호 메커니즘(예: 화이트리스트)을 설정할 필요가 있다.

제 3 절 5G 특화망 네트워크 통신 장비 보안 고려사항

본 절에서는 5G 특화망 구성하는 5G 통신 장비들에 대한 보안 고려사항을 설명한다.

5G 통신장비의 보안 고려사항으로는 물리적 접근통제, 5G 통신장비 보안, 가상화 인프라 보안, 5G 공급망 보안으로 구분한다.

1. 물리적 접근통제

- 물리적 영역 분리 : 5G 통신장비(사설망 구축 UPF, MEC, 기지국 등)가 구축된 주요 시설이 설치된 구역을 통제구역으로 설정하여야 한다.
- 물리적 접근 모니터링 : 물리적 접근시도를 탐지 및 차단하기 위한 기능, 물리적 접근 감시 및 접근 기록을 유지·검토하여야 한다.

2. 5G 통신장비 보안

- 악성코드 및 해킹 대응 : 불필요한 서비스(포트 차단), 비인가 SW 설치 및 사용 제한, 주기적인 보안 취약점 점검하여야 한다.
- 보안솔루션 구축 및 운영 : 5G 통신장비 보호를 위한 보안 솔루션 구축, 시스템 및 어플리케이션 로그 및 보안 이벤트 기록을 수행해여야 한다.
- 5G 통신장비의 관리자·사용자 인증 및 특수 권한관리 : 5G 통신장비 접근 시 사용자 인증 관리, 관리자 계정의 경우 복합인증 사용, 일정 시간 미사용시 자동 접속 해제 기능 등을 적용하여야 한다.
- 5G 통신 장비 데이터 보호 : 통신 장비 저장된 데이터 암호화, 통신 장비의 시스템 정보의 위변조 방지를 위한 무결성 검증을 수행하여야 한다.
- 불필요한 네트워크 서비스 제거 : 5G 통신 장비의 열린 서비스 포트가 필수적으로 필요한지 확인하여 사용하지 않는 불필요한 네트워크 서비스는 비활성화 조치를 수행하여야 한다.

3. SDN/NFV 가상화 인프라 보안

- 가상화 인프라 보안 : 가상자원(가상 PC, 가상 스토리지, 가상 SW) 생성, 변경, 회수 등에 관한 관리방안을 수립하여 운영하여야 한다.
- 가상머신 인터페이스 및 API 보안 : 가상 환경(가상 PC, 가상서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안취약점을 주기적으로 분석하여야 한다.
- 악성코드 탐지 및 통제 : 악성코드로부터 가상 환경(가상 PC, 가상서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술 적용하고 악성코드 감염 시 사용 중지 및 격리 조치를 수행하여야 한다.
- SDN 컨트롤러 보안 : SDN 컨트롤러가 악성코드에 감염되지 않도록 SDN 컨트롤러(제어평면)과 데이터 장비 사이에 가상화 인프라 보안장비를 배치하여 방어해야 한다.

4. 5G 공급망 보안

- 외주 및 오픈소스 SW 보안 관리 : 외주 개발, 오픈소스 SW 업데이트 보안 관리 체계 수립하여야 하며, 외주 및 오픈 SW 업데이트 및 보안 패치 파일의 안전성을 확인하고 무결성 검증 이후 설치하여야 한다. 또한, SW 개발·유지보수 환경 및 SW 개발 보안 가이드(Secure Coding)를 적용하였는지 확인하여야 한다.
- 공급망 SW 업데이트 위험관리 및 보안성 검토 : 안전한 경로(White List 방식 안전한 경로 상 IP, URL)를 통한 보안 패치와 보안 패치 후 안전성과 보안성 테스트를 수행하여야 한다. 특히 제3자 보안 평가기관 및 인증 기관과 협력하여 제품과 서비스를 독립적으로 테스트 및 평가하여 5G 통신장비 소스 코드 검토, 보안 설계 감사, 절차 문서 검토, 블랙박스 테스트, 침투 테스트 등을 실시하여야 한다.

제 4 절 5G 특화망 MEC 및 어플리케이션 보안 고려사항

본 절에서는 5G 특화망에 구축되는 MEC 플랫폼 보안과 MEC 탑재되는 어플리케이션의 보안 고려사항을 설명한다.

MEC 보안 고려사항으로는 MEC 플랫폼 자체의 보안, MEC 플랫폼과 연결되는 연동 구간보안, MEC 탑재 어플리케이션 보안으로 구분한다.

1. MEC 플랫폼 보안

- 가상화된 보안 솔루션 구축 : MEC 플랫폼 보안은 클라우드 인프라와 NFV 기술을 기반으로 가상 머신 보안, 컨테이너 보안 등 가상화된 보안 솔루션을 활용하여 구축하여야 한다.
- MEC 소프트웨어 보안 : MEC 소프트웨어 보안을 위해 VNF 소프트웨어 패키지에 대한 서명(발행자)과 검증(수신자) 지원, 벤더가 출시한 소프트웨어 패키지에 대해서는 서명 검증이 필요하다.
- MEC 서비스 장애관리 : MEC 리소스 풀을 설정하여 상호 원격 재해 복구를 제공하여 사고가 발생하면 MEC 서비스를 다른 MEC로 신속하게 전환하여 서비스 연속성을 보장이 필요하다.
- 보안 인증 획득 플랫폼 활용 : 민간 클라우드 플랫폼 및 서비스를 이용하여 MEC 구축 시 보안 인증 획득한 서비스 도입하여야 한다.

2. MEC 연동 구간 보안

- MEC 연결 API 보안 : MEC는 인터넷 인터페이스, 엔터프라이즈 네트워크 인터페이스, 무선 장치 인터페이스, 기능 노출 인터페이스, 타사 애플리케이션 인터페이스를 포함하므로 각각 보안 솔루션 도입하여 운영하여야 한다.
- MEC 연동 구간 보안 관제 : 네트워크 침입 탐지, 비정상적인 트래픽 분석, 악성코드 탐지 등 네트워크 에지에서 MEC 분포를 감안하여, 복수의 감시 지점을 배치하고,

통합 보안 모니터링해야 한다.

3. MEC 어플리케이션 보안

- 어플리케이션 인증 및 통신 암호화 : MEC 탑재 어플리케이션의 통신 채널을 보호하기 위해서는 엄격한 인증, 분리 또는 암호화하여야 한다.
  ※ 에지 도메인이 코어 도메인, 특히 제어 신호·충전 서비스와 통신할 때는 TLS/IPSec, 5G 프로토콜, 802.11 프로토콜을 활용하여 인증·전송 암호화를 구현해야 함
- 어플리케이션 간 접근통제 : MEC는 신뢰할 수 없는 응용 프로그래의 트래픽과 악의적인 행위를 분석하기 위해 어플리케이션 및 API 접근통제 정책 적용해야 한다.
- 감사 및 모니터링 : 보안위협이 MEC의 다른 기능 도메인에 영향을 미치지 않도록 MEC 탑제 3자 어플리케이션 등록, 바이러스 검사, 액세스 제어 등 어플리케이션 모니터링 및 감사로그 기록하여야 한다.

4. MEC 데이터 보호

- 데이터 자산 식별 : MEC 구축 및 서비스 운영 중에는 사용자 식별 및 액세스 위치를 포함하되 이에 국한되지 않는 관련 사용자 데이터 자산을 파악 등 데이터 자산 식별이 필요하다.
- 데이터 위변조 및 유출 방지 : MEC 플랫폼에 저장되는 기업용 데이터는 IPSec, TLS 등 전송되어 데이터 유출과 변조 방지 기술적 조치가 필요하다.
- 개인정보 및 민감 데이터 비식별 조치 : 개인정보 데이터 프라이버시가 관련되면 개인 데이터를 마스킹 등 비식별 조치를 하여야 한다.
- 저장 데이터 보호 : 서비스 유형과 데이터 등급에 따라 보안 요건이 높은 데이터(개인정보, 민감정보)는 국제표준 암호 알고리즘을 통해 데이터를 보호하여야 한다.

참 고 문 헌

국내 문헌

과학기술정통부・KCA (2021), 『5G 특화망 가이드라인』

박지성 (2022), 『5G 특화망 1주년, 새로운 초연결 인프라 생태계 가능성을 보다』, 한국전자파학회지, 제33권 제4호.

Netmanias (2019), 『Private 5G Networks 구축 방안』

박지현, 김인희 (2021), 『5G 특화망 해외 구축사례 및 정책적 시사점』, KISDI Perspectives.

박희재, 박래혁 (2021), 『5G 특화망 동향 및 사례』, 한국통신학회지, 제38권 제12호.

육영수 (2021), 『5G 특화망 해외 구축 및 운용 사례』, TTA 저널 194호.

김영수, 박종근, 이종훈, 장종수, 문대성, 김익균 (2020), “5G 환경에서의 MEC 보안 위협 및 대응 기술”, 정보과학회지

최환국, 최보민, 박성민, 심원태 (2019), “5G 네트워크 기술 진화에 따른 보안 이슈와 사이버대응 기술의 고려사항”, 정보통신기획평가원 주간기술동향

김환국, 최보민, 고은혜, 박성민 (2019), “5G 네트워크 기술 진화에 따른 새로운 5G 보안 도전과제와 해외 보안 아키텍처 연구 동향”, 정보보호학회지

최상훈, 전우진, 박기웅 (2017) “메모리 트랩기법을 활용한컨테이너 취약점 침입 탐지 프레임워크.“ 한국차세대컴퓨팅학회 논문지

박동주, 박병성 (2019), “5G 네트워크 기술 현황 및 진화 방안,” 정보통신기획평가원 주간기술동향 1905호, 2019. 07.

과학기술정보통신부 (2019), “5G 세계 최초 상용화… ‘정보통신 최강국’ 입증,” 대한민국 정책브리핑, 2019. 04. Available: https://www.korea.kr/news/policyNewsView. do?newsId=148859737 [Online; accessed on Sep. 6, 2021]

김문홍, 박종한, 나민수, 조성호 (2015), “5G 이동통신기술 발전방향,” 한국통신학회 정보와 통신 열린강좌, 제1권 제1호, pp. 46-56, 2015. 09.

김환국, 최보민, 박성민, 심원태 (2019), “5G 네트워크 기술 진화에 따른 보안 이슈와 사이버대응 기술의 고려사항,” 정보통신기획평가원 주간기술동향 1917호, 2019. 10.

과학기술정통신부, 한국방송통신전파진흥원 (2021), 5G 특화망 가이드라인

관계부처 합동 (2019), 5G 기반 스마트공장 고도화 전략(안)

넷매니아즈 (2019), Private 5G: 이통사와 비이통사의 Private 5G 망 구축 전략 및 현황, https://www.netmaniax.com/

박종근 외 (2019), 3GPP 5G 보안 구조의 특징 및 주요 개선사항, 정보보호학회지, 제29권 5호, pp. 21-30

삼성전자 (2020), Cloud Native 5G Core, Technical Report

박종근 외 (2020), 5G 엣지 보안 기술 동향, 정보보호학회지, 제30권 6호, pp.5-14

과학기술정보통신부, 한국방송통신전파진흥원 (2021), 5G 특화망 가이드라인

윤영우 외 (2021), 5G 특화망을 위한 무선접속 기술, TTA 저널, 제194호, pp.40~51

나성욱 (2021), 한국에서의 특화망 활용방안, TTA 저널, 제194호, pp.62-69

황성기·황승흠 (2003),『인터넷은 자유공간인가?: 사이버 공간의 규제와 표현의 자유』, 커뮤니케이션북스.

LG경제연구원 (2005),『대한민국 2010 트렌드』, 한국경제신문사.

해외 문헌

NTT (2022). “Private 5G: rising adoption collides with CIOs’ security concerns.” White paper.

5G-ACIA (2019). “5G Non-Public Networks for Industrial Scenarios.” White Paper.

Fortinet (2021), “Securing 5G Private Mobile Network.” White paper.

Fortinet (2022), “Security Considerations in Industrial 5G Environments.” White paper.

Cisco public (2022), “Cisco’s Private 5G solution Security Overview.”

GSMA (2020), “5G IoT Private & Dedicated Networks for Industry 4.0.”

Lufthansa Technik (2020), “Lufthansa gets spectrum licence, deploys Nokia private 5G for remote engine checks.”

Samsung (2021), “Virtualized RAN-vol.2.” White paper.

Industrial ethernet book (2021), “5G on test bench for Industry: What’s possible in the future?”

Bosch Press (2020), “Bosch puts first 5G campus network into operation.”

Nokia (2019), “Sendai city improves tsunami preparedness with connected drones.”

Smart sound plymouth (2022), “Vodafone, Plymouth city council and Plymouth marine laboratory announce use cases for world’s first 5G marine focused testbed.”

Im-mining (2018), “Sandvik and Nokia team up to offer miners LTE and 5G networks.”

RFC3748: https://www.rfc-editor.org/rfc/rfc3748

3GPP TS 33.102, “3rd Generation Patnership Project; Technical Specification Group Services and System Aspects; 3G Security, Security architecture”, June 2003

Draft-arkko-pppext-eap-aka-12.txt “Extensible Authentication Protocol for UMTS Authentication and Key Agreement(EAP-AKA),” Apr. 2004

T. Wan, “False Base Station or IMSI Catcher: What You Need to Know”, CableLabs, Oct 2019.

3GPP, “NR; Radio Resource Control (RRC); Protocol specification”, 3GPP TS 38.331, Sep 2020.

S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, “LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE”, Network and Distributed System Security (NDSS) Symposium 2018, Feb 2018.

Richard Chirgwin, “Fake mobile base stations spreading malware in China”, The Register, Mar 2017.

A. Shaik, R. Borgaonkar, S. Park, J. Seifert, “New vulnerabilities in 4G and 5G cellular access net- work protocols: exposing device capabilities”, Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp.

221-231, May 2019.

3GPP, "Study on 5G Security Enhancement against False Base Stations", 3GPP TR 33.809, Oct 2020.

3GPP, "Security architecture and procedures for 5G system", 3GPP TS 33.501, Sep 2020.

3GPP, "Study on evolution of Cellular Internet of Things (CIoT) security for the 5G System", 3GPP TR 33.861, Sep 2020.

3GPP, "Study on the Self-Organizing Networks (SON) for 5G networks", 3GPP TR 28.861, Dec 2020.

A. Shaik, R. Borgaonkar, S. Park, and J. Seifert. "On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks". In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '18). pp. 75-86, 2018.

R. David, K. Katharina, H. Thorsten, and P. Christina. "IMP4GT: IMPersonation Attacks in 4G NeTworks". https://imp4gt-attacks.net/me- dia/imp4gt_camera_ready.pdf (2020)

R. David, K. Katharina, H. Thorsten, and P. Christina, "Breaking LTE on Layer Two". 1121-1136. Available online at https://alter-attack .net/media/breaking_lte_on_layer_two.pdf (2019)

Olimid, Ruxandra F., and Gianfranco Nencioni. (2020). "5G network slicing: A security overview." *J IEEE Access 8*, (2020), pp.99999-100009.

Sattar, Danish, and Ashraf Matrawy. (2019). "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices." 2019 IEEE Conference on Communications and Network Security (CNS). pp.82-90.

Madi, Taous, et al. (2021). "NFV security survey in 5G networks: A three-dimensional threat taxonomy." Computer Networks 197.

Bonfim, Michel, et al. (2020). "A real-time attack defense framework for 5G network slicing." Software: Practice and Experience 50.7. pp.1228-1257.

Barakabitze, Alcardo Alex, et al. (2020). “5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges.“ Computer Networks 167 (2020)

ETSI. (2022). “MEC Security; Status of standards support and future evolutions.” ETSI White Paper No. 46

C. Benzaid and T. Taleb (2020), “AI-Driven zero touch network and service management in 5G and beyond: Challenges and research directions,” IEEE Network, vol. 34, no. 2, pp. 186–194, 2020.

P. P. Ray and N. Kumar (2021), “SDN/NFV architectures for edge-cloud oriented IoT: A systematic review,” Computer Communications, vol. 169, pp. 129–153, 2021.

R. Rosa and C. Rothenberg (2020), “Experiences in IETF-bMWG: Towards a methodology for VNF benchmarking automation,” in Anais do VII Workshop Pré-IETF (WPIETF 2020), Porto Alegre, RS, Brazil, pp. 43–56.

I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck (2018), “Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 3, p. 2429–2453, 2018.

A. Esmaeily, K. Kralevska, and D. Gligoroski (2020), “A Cloud-based SDN/NFV Testbed for End-to-End Network Slicing in 4G/5G,” in 6th IEEE Conference on Network Softwarization, 2020.

3GPP (2021), “Advanced plans for 5G,” 3GPP News, July 2021. Available: https://www.3gpp.org/news-events/2210-advanced_5g [Online; accessed on Sep. 6, 2021]

ITU (2015), “IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond,” Recommendation ITU-R M.2083-0, Sep. 2015.

3GPP (2021), “NG-RAN; Architecture description,” 3GPP TS 38.401 V16.4.0, Jan. 2021.

Open RAN 101-RU (2020), “DU, CU: Why, what, how, when?“ RCR Wireless News, 2020. Available: https://www.rcrwireless.com/20200708/open_ran/openran-101-ru-du-cu-reader-forum [Online; accessed on Sep. 6, 2021]

F. Campioni, S. Choudhury, and F. Al-Turjman (2019), "Scheduling RFID networks in the IoT and smart health era," Journal of Ambient Intelligence and Humanized Computing, Vol. 10, pp. 4043-4057, Jan. 2019.

3GPP (2013), "Study on Small Cell enhancements for E-UTRA and E-UTRAN; Higher layer aspects," 3GPP TR 36.842 v12.0.0, Dec. 2013.

3GPP (2021), "Security architecture and procedures for 5G system," 3GPP TS 33.501 v17.2.1, June 2021.

J. Arkko, V. Lehtovirta, and P. Eronen (2009), "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')," IETF RFC 5448. May 2009.

3GPP (2018), "Security Architecture and Procedures for 5G System," Technical Specification Group Services and System Aspects (SA3): TS 33.501 version 15.2.0, pp.36-48, September 2018.

Jari Arkko and Henry Haverinen (2006), "Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)," IETF RFC 4187, January 2006.

Dan Simon, Bernard Aboba, and Ryan Hurst (2008), "The EAP-TLS authentication protocol," IETF RFC 5216, March 2008.

H. Ștefănescu, M.Iordache, B.Rusti, C.Brezeanu, J. Ghenţa, M.Chabiera, L.Rajewski, G.Panek (2020), "5G Programmable Infrastructure Orchestration using ONAP", IARIA AICT The Sixteenth Advanced International Conference on Telecommunications, Lisbon, Portugal, 2020.

L.Yala, M.Iordache, A. Bousselmi and S. Imadali (2019), "Testbed Federation for 5G Experimentation: Review and Guidelines, "IEEE Conference on Standards for Communications and Networking (CSCN), GRANADA, Spain, pp.106, 2019.

L.Yala, M.Iordache, A.Bousselmi and S.Imadali (2019), "5G Mobile Network Orchestration and Management Using Open-Source, "IEEE 2nd 5G Forum (5GWF), Dresden, Germany, pp. 421-426, 2019

3GPP TS 23.222 (2021), “Common API Framework for 3GPP Northbound APIs” , Release 17, V17.4.0, April 2021.

D. Santos, R. Silva, D. Corujo, R. L. Aguiar and B. Parreira (2021), “Follow the User: A Framework for Dynamically Placing Content Using 5G-Enablers,“ in IEEE Access, vol. 9, pp. 14688-14709, 2021.

V.A. Cunha, E. Silva, M.B. Carvalho, D. Corujo, J.P. Barraca, D. Gomes, L.Z. Granville, and R.L. Aguiar (2019), “Network slicing security: Challenges and directions,” Internet Technology Letters, 2(5):e125, Sep. 2019.

Xiaoting Huang, Vlasios Tsiatsis, Anand Palanigounder, Li Su, and Bo Yang (2021), “5G Authentication and Key Management for Applications,” IEEE Communications Standards Magazine, vol. 5, no. 2, June 2021.

3GPP (2021), “Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS),” 3GPP TS 33.535 v17.2.1, June 2021.

3GPP (2021), “Generic Bootstrapping Architecture (GBA) (Release 17),” 3GPP TS 33.220, Version 17.1.0, 3GPP, June 2021.

3GPP (2019), Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST) (Release 16), document 3GPP TS 33.163, Version 16.2.0, 3GPP, Sep. 2019.

3GPP (2020), “Study on security aspects of the 5G Service Based Architecture (SBA),” 3GPP TR 33.855, Version 16.1.0, 3GPP, Sep. 2020.

Christine Jost (2020), “Security for 5G Service-Based Architecture: What you need to know,” Ericsson Blog, Aug. 2020. Available: https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture [Online; accessed on Oct. 25, 2021]

T. Dierks and E. Rescorla (2008), “The Transport Layer Security (TLS) Protocol Version 1.2,” IETF RFC 5246, Aug. 2008.

E. Rescorla (2018), “The Transport Layer Security (TLS) Protocol Version 1.3,” IETF RFC 8446, Aug. 2018.

D. Hardt (2012), “The OAuth 2.0 Authorization Framework,” IETF RFC 6749, Oct. 2012.

Cybersecurity&Infrastructure Security Agency (CISA) (2022) “ 5G Security Evaluation Process Investigation ”

European Union Agency for Cybersecurity (2021) “ SECURITY IN 5G SPECIFICATIONS ”

3GPP, 3GPP TS 23.501 (2022): “System architecture for the 5G System (5GS)”

IETF, RFC6819 (2013): “OAuth 2.0 Threat Model and Security Considerations

A. Freie (2011), The Secure Sockets Layer (SSL) Protocol Version 3.0, URL : https://tools.ietf.org/html/rfc6101

E. Rescorla. (2008) The Transport Layer Security(TLS) Protocol Version 1.2 RFC 5246(Proposed Standard), URL : https://tools.ietf.org/html/rfc5246

E. Rescorla. (2018) The Transport Layer Security(TLS) Protocol Version 1.3 RFC 8446(Proposed Standard), URL : https://www.rfc-editor.org/rfc/rfc8446

Benjamin Dowling, Marc Fischlin, Felix Gunther, and Douglas Stebila (2020), “A Cryptographic Analysis of the TLS 1.3 Handshake Protocol”, In ACM CCS 15

F. Giust et.al. (2017), “Multi-Access Edge Computing: An Overview of ETSI MEC ISG”, IEEE 5G Tech Focus, 1(4)

NIST (2020), “Zero Trust Architecture”, NIST SP 800-207, 2020

5G-ACIA (2021). “Security Aspects of 5G for Industrial Networks”

CISA (2021), “Zero Trust Maturity Model”, 2021.

DeLong, Bradford J. (2002). “Introduction to the Symposium on Business Cycle.” Journal of Economic Perspectives 13(2), pp.19 ~ 22.

DeLong, Bradford J. (2002). “Do We Have a ‘New’ Macro- economy?.” Innovation Policy & the Economy.

[부록 1] 5G 특화망 무선 액세스 및 기지국 보안 고려사항 연구

제1절 무선 RAN 구간 보안 위협

1. 무선 RAN 보안 위협

무선 RAN 구간은 다양한 형태(매크로셀, 마이크로셀, 펨토셀 등)의 기지국 장비들로 구성된다. 무선 RAN 기지국 장비는 무선통신 인터페이스(Air Interface)를 통해 사용자 단말기(UE)와 연결되고 유선(Wired) 전송 네트워크를 통해 5G 코어장비와 연결해주는 중계 장비 역할을 한다.

5G 무선 RAN 기술은 다양한 이종 무선접속과 대량 IoT 기기의 접속이 허용되면서 무선 RAN 구간의 보호가 중요하다. 이동통신 서비스 연결을 위해서는 사용자 장치와 무선RAN 구간의 기지국(eNB, gNB) 장비와 코어망의 통신장비(MME) 간 제어 신호(이동, 인증, 과금 등)를 교환한다. 무선 RAN 기지국에 연결되는 수백만의 사용자 장치로 인한 비정상 제어 트래픽이 송수신할 경우 장애에 대한 복원력 이슈와 접근이 용이한 스몰셀 기지국 보안이 중요하다.

무선 RAN 보안위협은 대표적으로 악성코드에 감염된 대량의 IoT 봇넷에 의해 무선 자원에 과도한 접속을 요청하는 무선 RAN DDoS 공격과 무선 신호 채널에 대한 재밍(Jamming) 공격이 있다. 무선 RAN DDoS와 전파 방해 재밍 공격에 의해 기지국들이 비정상 데이터를 송수신함으로써 RAN 구간의 무선 인터페이스 자원을 고갈시켜 정상적인 데이터 수신을 방해하는 가용성 이슈 발생이 가능하다. 허위 기지국(Rogue Base Station) 이슈는, 공격자가 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 수행될 수 있다.

〈표 부록1-1〉 무선 RAN 보안위협 유형

보안위협	주요내용

보안위협	주요내용
주파수자원 남용	· 같은 동적 할당/재할당 때문에 이러한 자원의 불법적인 사용은 합법적으로 허가를 받은 단위의 특성을 모방하고 무선 주파수 간섭을 야기하여 특정 유휴 주파수 대역을 점유할 수 있음 · 주파수의 불법 점유는 네트워크 노드가 무면허 장치에 의해 요청된 주파수 자원을 거부하도록 유도할 수 있으며 이는 유휴 자원의 명백한 부족으로 인해 코어 네트워크 밖으로 누군가가 빠져나가는 것을 차단
ARP(주소 결정 프로토콜 포이즈닝 공격	· 공격자가 스푸핑된 ARP 메시지를 네트워크로 보내는 기술인 ARP 캐시 스푸핑이라 함 · 공격자의 MAC 주소를 기본 게이트웨이와 같은 다른 호스트의 IP 주소와 연결하여 해당 IP 주소를 대신 공격자에게 전송하도록 하는 공격임
가짜 액세스 네트워크 노드	· 위협은 모바일 사용자 장비(UE)와 네트워크 사이의 통신을 변조하여 다른 악의적인 행동을 개시함 · 가짜 엑세스 노드를 합법적인 노드로 위장하여 기지국(gNB)과 연결설정을 통해, 중간자공격(man-in-the-middle) 이나 네트워크 트래픽 조작과 같은 다른 유형의 2차 공격을 용이하게 함
Flooding 공격	· 다량의 요청 신호를 무선 RAN 인터페이스에 보내는 공격으로, 무선 RAN 기지국의 자원을 소진여 무선 주파수를 감소시키거나 완전히 정지시킬 수 있는 과도한 데이터 전송 공격임
가입자식별정보 포획 (IMSI Catcher) 공격	· 이 위협은 피해자와 인접한 악의적인 행위자가 피해자의 soft-identity(예: 전화번호, 트위터 핸들)를 호출과 연관시키기 위해 악용할 수 있는 휴대 전화 호출 프로토콜과 관련이 있음 · 악의적인 행위자는 '$mathsf{ToRPEDO}$'라는 이름의 공격을 통해 피해자의 거친 위치 정보를 확인하고, 조작된 페이징 메시지를 주입하고, 서비스 거부 공격(denial-of-service, dos)을 할 수 있음
무선 주파수 재밍	· 악의적인 활동/자산 남용으로 분류되는 이 위협은 네트워크 무선 주파수(NRF)의 의도적인 중단/간섭으로 인해 코어 네트워크(및 관련 서비스)가 영향을 받는 사용자에게 접근할 수 없게 함 · 무선 주파수 재밍은 무선 기반 네트워크를 사용할 때 전송 계층을 사용할 수 없는 GPS 간섭을 말함
MAC 스푸핑	· MAC 스푸핑은 네트워크 기기에 있는 네트워크 인터페이스의 MAC(Media Access Control) 주소를 변경하는 공격임 · NIC(네트워크 인터페이스 컨트롤러)에서 하드 코딩된 MAC 주소는 변경할 수 없으나 많은 드라이버는 MAC 주소 변경을 허용하는 취약성으로 인해, MAC 주소를 공격자의 MAC 주소로 마스킹하는 과정을 MAC 스푸핑이라고 함
액세스	· 액세스 네트워크 요소(예: 기지국)와 연결과정에서 환경설정

보안위협	주요내용
네트워크 환경설정 데이터 조작	데이터를 위조하여 2차 공격(예: DoS)을 개시할 수 있음
무선 채널 간섭	· 무선 액세스 네트워크 서비스를 일시적 또는 무한정 방해하여 공격자가 의도한 사용자가 네트워크 리소스를 사용할 수 없게 하려는 위협임 · 무선 액세스 네트워크에 손상된 5G 기기가 도입되면 보다 상당한 DoS 위협이 발생할 수 있음.
무선 트래픽 조작	· 악의적인 공격자가 자신의 기지국(BTS)을 실제 네트워크의 기지국으로 위장하여 중간자 공격을 통해 트래픽 조작을 수행 · 이 위협은 이전 세대의 이동통신기술과의 역호환성 때문에 여전히 유효함
세션 하이재킹	· 세션 하이재킹은 악의적인 활동 또는 자산 남용으로 분류되며, 다른 유형의 공격을 수행하기 위해 특정 트래픽의 전체 세션을 제어하기 위해 악의적인 행위자에 의한 합법적인 인증 communication 세션 ID의 도용을 통해 수행됨
시그널링 사기	· 우려되는 영역 중 하나는 사기에 악용될 수 있는 네트워크 간의 international 신호 상호 연결이다(예: false charging). 가짜 기존 신호를 전송하고 다른 모든 사용자가 특정 대역(스펙트럼 구멍)을 비우도록 강제해 전용을 획득하는 그리드 이동 노드(greedy mobile nodes)의 위협도 한 예임
시그널링 DoS	· 시그널링 DoS(Stroming)은 사용자 기기가 악성코드 감염되거나 악성앱에 의해 발생될 수 있으며, 이는 이동통신 장비들(셀, 백본 signaling 서버, 클라우드 서버)의 대역폭에 과부하를 주며, 모바일 장치의 배터리 전력을 고갈될 수 있음 · 시그널링 DoS 공격은 사용자 기기의 과도한 연결 요청, 소규모 기지국, 높은 사용자 이동성으로 인해 대응이 더욱 어려움

제2절 5G에서의 허위 기지국 대응 주요 이슈

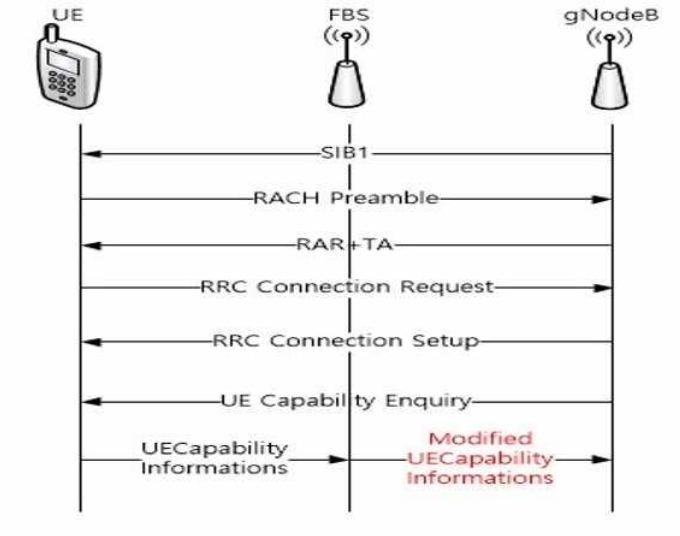
1. 보호되지 않은 유니캐스트 메시지 보안

이 주요 이슈는 보호되지 않은 상태로 전송할 수 있는 Uplink 및 Downlink 유니캐스트 메시지를 공격자가 악용하여 발생할 수 있는 메시지를 다룬다. 보호되지 않은 채로 전송되는 Uplink 메시지의 예시로는 RRC_UECapabilityInformation이 있고, Downlink 메시지로는 RRC_UECapabilityEnquiry 및 RRC/NAS(Non-Access Stratum) 계층의 Reject 메시지가 있다.

(1) RRC UECapabilityEnquiry와 RRC UECapabilityInformation

현재 3GPP Release 18 표준에서는 RRC_UE_Capability_Enquiry 및 RRC_UE_Capability_Informations 메시지가 AS 보안 활성화 전에 보호되지 않고 전송되도록 설계되었다. 그 이유는 네트워크가 더 나은 서비스와 연결성을 위해 초기 최적화를 수행하기 위함이다. 따라서 gNB가 UE의 AS 보안설정을 위한 Capability를 요청하기 위해 UE_Capability_Enquiry 메시지를 보내고 UE는 AS 보안 설정 전에 UE_Capability_Informtaions 메시지를 gNB에게 전송한다. 다음 그림과 같이 허위 기지국은 중간자 공격을 통해 무선상에서 UE_Capability_Information을 캡처하고 이 메시지의 값을 더 낮은 무선 기능 수준으로 수정하고 이를 실제 gNB로 전달하여 UE가 제한된 무선 능력 수준으로만 작동하도록 할 수 있다.

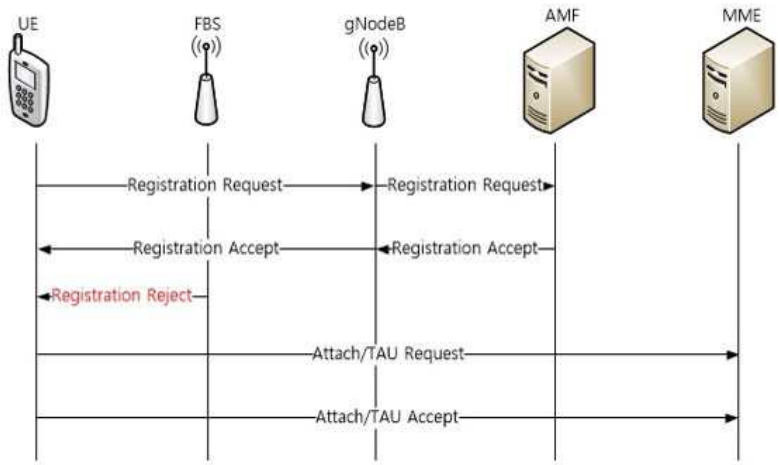
[그림 부록1-1] 허위 기지국을 활용한 UE의 Capability 정보 변조



(2) RRC/NAS 계층의 Reject 메시지

등록 절차 중 등록 거부를 나타내는 Reject 메시지를 위조하여 CIoT UE에 전송한 후 UE가 5GC에서 EPC(Evolved Packet Core) 네트워크로 강제 리다이렉션 되도록 할 수 있다. 이로 인해 SUPI 보호, 초기 NAS 보호 등과 같은 5G 보안 강화 기능을 사용할 수 없어 UE의 프라이버시가 노출될 수 있다. 또한 UE가 RRC_INACTIVE 상태인 경우와 gNB, UE가 AS 보안 컨텍스트를 계속 유지하는 동안에도 RRC_REJECT 메시지는 보호되지 않고 전송된다. Reject 메시지의 유형과 내용에 따라 UE는 서비스 거부 공격을 받을 수 있다.

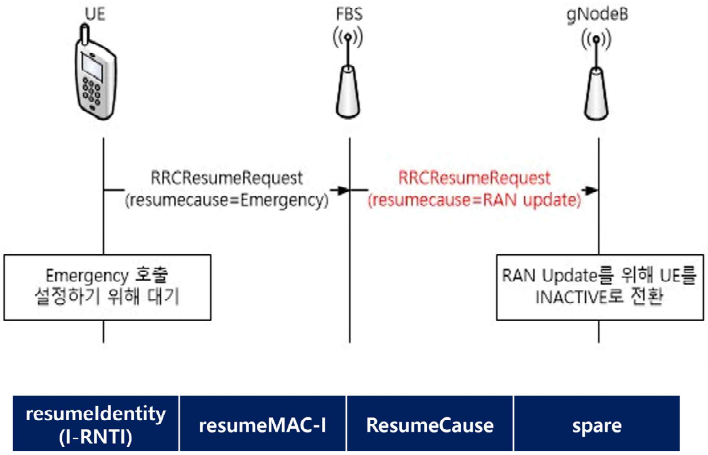
[그림 부록1-2] Reject 메시지를 악용한 다운그레이드 공격



(3) RRC_Resume_Request 메시지의 resumeCause 필드

RRCResumeRequest 메시지의 재개 사유를 나타내는 resumeCause 필드는 resumeMAC-I 토큰으로 무결성 보호가 되지 않기 때문에 다른 값으로 수정하여 허위 기지국에 의한 중간자 공격이 가능해진다. 위 그림과 같이 공격자가 resumeCause 필드 값을 “emergency”에서 “ran update”로 수정하면 네트워크 변조를 탐지할 수 없고 UE가 Emergency 호출을 설정하기 위해 대기하는 동안 네트워크는 RAN Update를 위해 UE를 INACTIVE 상태로 전환하게 된다.

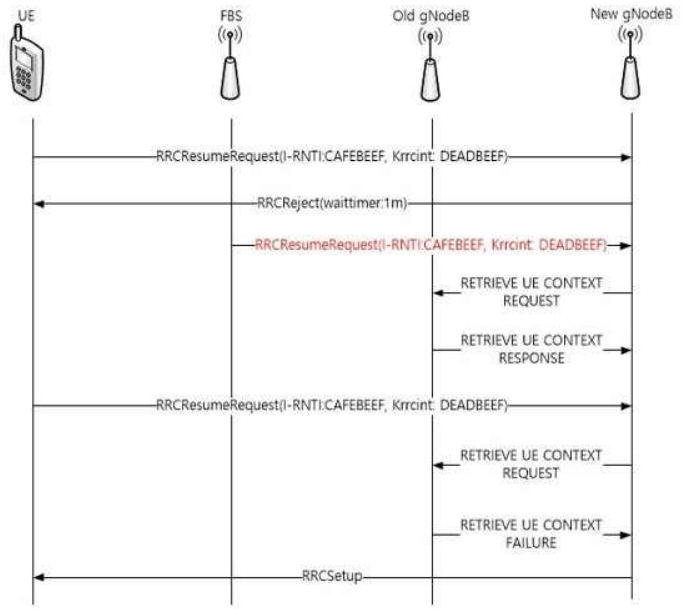
[그림 부록1-3] resumeCause 필드 수정을 통한 중간자 공격



(4) RRC_Resume_Request 메시지 재전송 공격

UE가 RRC 재개 절차를 시작하는 경우, UE는 이전 메시지와 동일한 I-RNTI와 KRRCint를 기반으로 계산한 resumeMAC-I를 포함하여 RRCResumeRequest 메시지를 전송한다. 새로 연결한 gNB가 부하가 많은 상태인 경우, wait timer와 함께 RRC Reject 메시지를 전송하고 UE는 메시지를 수신하면 wait timer의 값만큼 대기 후에 재시도한다. 이때, UE는 이전에 보낸 메시지와 동일한 I-RNTI와 KRRCint를 사용해야 하므로 처음 보낸 메시지와 두 번째 메시지가 같다. 만약, 허위 기지국이 첫 메시지를 획득할 수 있다면 wait timer가 만료되기 전에 새 gNodeB로 그 메시지를 보낼 수 있고 이전 gNodeB는 resumeMAC-I를 검증하여 유효한 것으로 판단하여 새로운 gNB에게 UE 문맥을 전송한다. UE가 다시 Resume 절차를 시도하면 새 gNodeB가 UE 문맥을 할당하지 못하므로 실패하게 되어 초기 RRC 설정 절차를 다시 진행하게 된다.

[그림 부록1-4] RRC Resume Request 메시지 재전송 공격 절차



2. System Information의 보안

허위 기지국은 주기적으로 동기화 신호와 SI(System Information)을 브로드캐스트 한다. SI를 브로드캐스팅 하는 것은 TS 38.331에 정의된 RRC 프로토콜의 기능 중 하나이다. 이러한 브로드캐스트 메시지는 셀에 머무르고 있는 모든 UE에게 전송된다. UE는 RRC_IDLE 모드 또는 RRC_INACTIVE 모드일 때 셀의 SI를 모니터링하고 연결하기에 적합한 셀을 선택한다. UE는 일반적으로 셀로부터 SI를 수신하고 서비스를 받기 위해 RRC_CONNECTED로 전이하기 위한 초기 액세스 절차를 수행한다. SI에는 셀 (재)선택 매개변수, 인접 셀 정보, 주파수 우선순위, 블랙리스트 셀, 공용 채널 구성 정보, NAS 공용 정보, Public Warning System(PWS) 메시지와 같은 정보가 포함된다. 일반적으로 시스템 정보는 RRC_IDLE, RRC_INACTIVE, RRC_CONNECTED에 있는 UE에 적용가능하다.

RRC_IDLE 모드의 UE는 PLMN(Public Land Mobile Network) 선택과 페이징을 모니터링, 셀 선택 및 재선택, 그리고 액세스 시도 전에 접근제어를 적용한다. 향후 릴리즈에서는

단말 근접 서비스, MBMS(Multimedia Broadcast/Multicast Service) 등과 같은 다른 서비스도 IDLE 모드에서 UE에 의해 지원될 가능성이 있다.

이 주요 이슈는 악성 SI 메시지를 브로드캐스트하거나 이전에 수집한 SI 메시지를 수정 없이 그대로 재전송하는 무선 공격자에 대해서 새로운 보호 메커니즘을 도입할 수 있는지 여부와 방법을 연구해야 한다는 것이다. SI 메시지는 모든 UE를 위한 브로드캐스트 메시지이므로 무결성 및 재전송 보호가 엄격하게 필요한지는 명확하지 않다. 그런데도 일반적으로 무결성 및 재전송 보호 SI는 무선 공격자가 나중에 UE를 유인하기 위해 불량 SI 또는 이전에 캡처한 SI를 사용하거나 잘못된 인접 셀과 함께 SI 메시지를 사용하고 자체 제작 또는 오래된 PWS 메시지를 전송하는 것을 성공하는 것을 최소한 어렵게 만들어 보안 가치를 추가할 수 있다.

3GPP의 보안 담당 워킹그룹인 SA3는 TR 33.969에서 PWS(Public Warning System) 보안을 연구하였다. 이 문서에서 PWS의 경고 알림 메시지를 허위 기지국으로부터 보호하는데 사용되는 보안 메커니즘이 허위 기지국 공격 대응 연구에 도움이 될 수 있다. 브로드캐스트 메시지에 보안을 적용하는 것에 키 관리, 시간 동기화, 시그널링 복잡도 등의 주요 문제점이 있다.

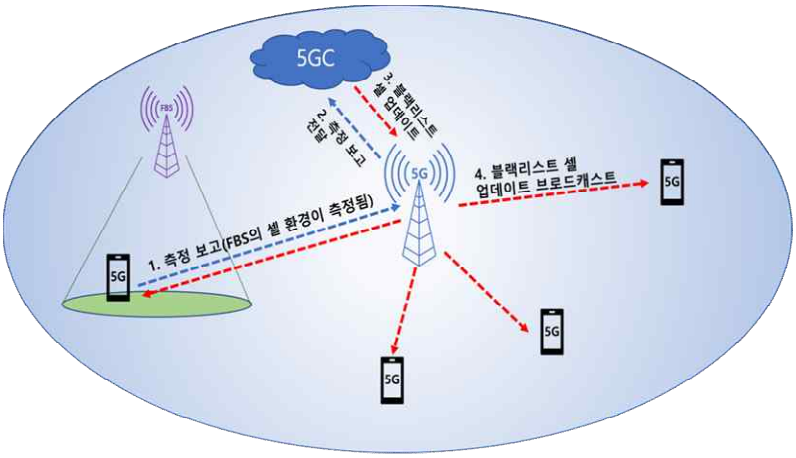
그럼에도 불구하고 일반적으로 SI 메시지를 보호하기 위해 5G 시스템을 지원할 수 있는 경우에만 신중하게 보호 메커니즘을 적용해야 한다. 이 주요 이슈는 무선 인터페이스와 관련이 있고 이 문서에서는 네트워크 내의 SI 무결성 보호는 포함하지 않는다. SI의 보호 부재는 UE에 대한 서비스 거부 공격, 비인가 서비스를 야기할 수 있다. 따라서 5G 시스템은 임의의 RRC 상태에 있는 UE가 셀로부터 수신한 SI의 신뢰성을 결정할 수 있도록 보장하는 수단을 제공해야 한다.

3. 네트워크 기반의 허위 기지국 탐지

3GPP Measurement 절차는 주로 핸드오버 및 SON(Self-Organizing Networks) 기능을 지원하도록 설계되었다. 하지만 이 절차는 허위 기지국을 탐지하는데 유용하다는 점에서 보안 목적도 제공한다. 허위 기지국 탐지를 위한 이러한 프레임워크는 현재 3GPP TS 33.501 부록 E에 설명되어 있다. UE가 네트워크로 보낸 Measurement Report(MR)에는

이미 주변 무선 상태에 대한 다양한 정보가 포함되어 있다. 그리고 이러한 MR은 허위 기지국 탐지에 더 효과적이 되도록 더욱 강화될 수 있다. 또한, Logged Measurement Report와 같은 다양한 유형의 MR을 사용할 수 있다. 현재 이 주요 이슈는 탐지 프레임워크의 잠재적인 개선 사항과 허위 기지국 탐지를 더욱 강화하기 위한 MR의 강화를 연구하는 것이다.

[그림 부록1-5] 측정 보고를 활용한 허위 기지국 탐지 절차 예시



허위 기지국을 탐지하기 위해 특정 기지국이 허위이고 정상 사업자 네트워크에 속하지 않는다는 것을 확인하기 위한 정보 추가 처리 중요하다. 특정 기지국이 허위라는 결정에 도달하면, 정상 네트워크는 그러한 허위 기지국을 격리하려는 조처를 할 수 있다. 정상 네트워크는 허위 기지국에 연결하는 것을 피하기 위한 정보로 UE를 보호할 수 있다. UE가 사업자에 속한 정상 기지국의 정보를 사용하는 경우 사업자 네트워크에 속한 정상 기지국의 이러한 안내 정보는 RRC_CONNECTED 모드와 RRC_IDLE 모드 모두에서 허위 기지국을 피하기 위해 신뢰할 수 있다.

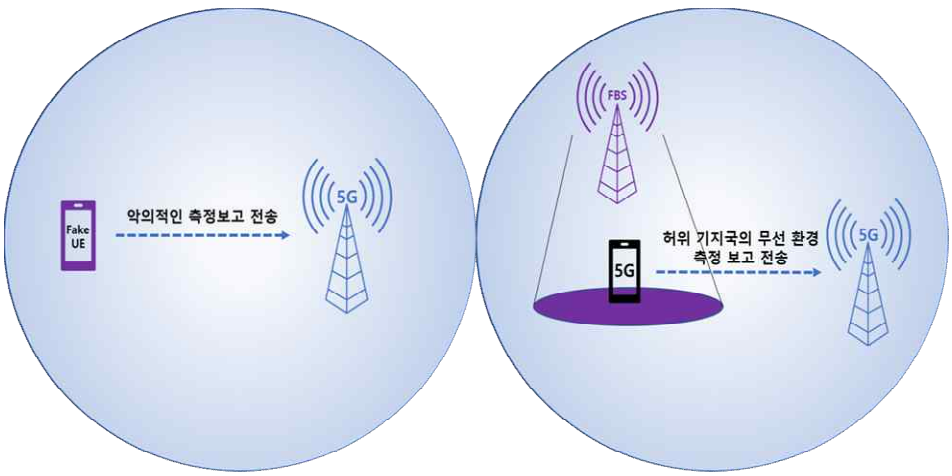
탐지되지 않은 허위 기지국은 네트워크에 대한 서비스 거부 공격, UE에 대한 서비스 거부 공격, 기만, 가입자 개인 정보 유출 등의 공격을 수행할 수 있으므로 네트워크에서 대응 조치를 취해야 한다. 따라서 5G 시스템은 허위 기지국을 탐지할 수 있어야 하고

UE가 허위 기지국에 연결하지 못하는 방법을 적용해야 한다.

4. SON 오염 시도에 대한 보호

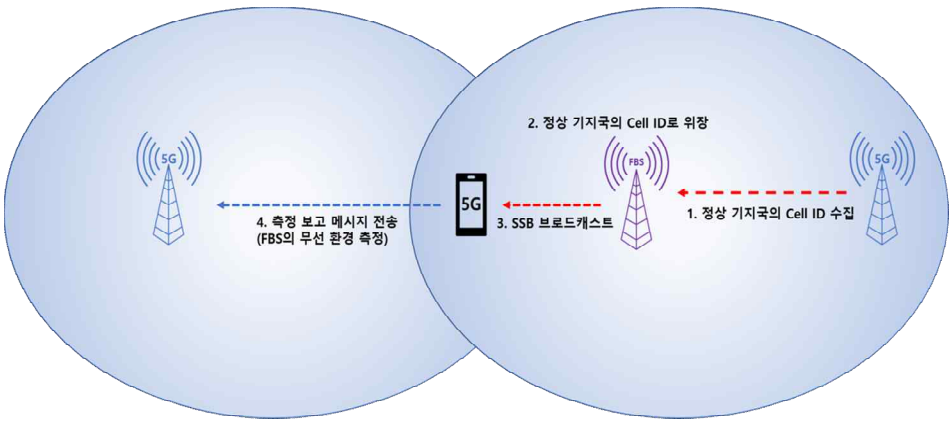
SON(Self-Organizing Network) 기능은 모바일 무선 접속 네트워크의 계획, 구성, 관리 최적화, 문제 수정을 더 간단하고 더 빠르게 만들기 위해 설계된 자동화 기술이다. SON 처리 과정의 높은 수준에서 SON 기능은 UE로부터 수신한 측정 보고를 바탕으로 동작한다. UE에서 모뎀, 베이스밴드와 같은 측정 보고를 처리하는 부품은 악성코드와 유저 어플리케이션으로부터 보호되고 있기 때문에 UE가 전송한 측정 보고는 일반적으로 신뢰할 수 있고 공격자로부터 손상되지 않았다고 고려된다. 하지만 UE는 보호되지 않은 채로 전송되는 동기화 신호와 MIB(Master Information Block)을 전달하는 SSB(Sychronization Signal Block)을 기반으로 인접한 셀의 신호 강도 측정을 수행한다. UE는 SSB 신호를 검증할 수 없으므로 허위 기지국에 의해 생성된 SSB를 기반으로 측정을 수행할 수 있다. 이때, 허위 기지국 C가 정상 기지국 B로 위장하고 무선 환경을 구축한 다음 UE가 이 환경을 측정하여 서빙 기지국 A로 측정 보고를 전송하게 되면 A는 C의 무선 환경을 B에서 측정된 것으로 믿는다.

[그림 부록1-6] 허위 또는 잘못된 측정 보고 전송으로 SON 오염 시도



위 그림과 같이, 공격자는 자체 구축한 SDR(Software Defined Radio)를 사용하는 UE를 활용하여 악의적으로 생성한 측정 보고를 전송하거나 허위 기지국을 통해 정상 UE 주변에 잘못된 무선 환경을 구축하여 공격자가 원하는 측정 보고를 전송하도록 하여 측정 보고를 오염시킬 수 있다.

[그림 부록1-7] 정상 기지국으로 위장한 허위 기지국의 무선 환경 측정 보고



허위 기지국은 인접한 정상 gNB들의 Cell ID를 수집할 수 있고 그들 중의 하나로 위장할 수 있다. UE는 gNB들로부터 오는 SI를 검증할 수 없기 때문에 UE는 gNB가 허위인지 아닌지 구분할 수 없다. 그 결과로 UE는 허위 기지국으로부터 수신된 정보를 기반으로 측정 보고를 수행하여 현재 연결된 서빙 gNB로 전송하게 된다.

앞선 사례들이 성공적으로 공격이 수행되더라도 매우 국지적이고 소규모의 영향을 끼친다. 공격자가 이러한 기술들을 사용하여 대규모로 공격하는 것은 상당히 비용이 많이 들고, 비실용적이다. 더 중요한 것은 네트워크가 UE의 측정 보고를 맹목적으로 신뢰하는 경우에만 이러한 SON 오염 시도가 성공한다는 것이다. 일반적으로 적절하게 구현된 SON은 측정 보고가 위조된 정보일 가능성을 고려하고 우수한 복원 기능이 있기 때문에 이러한 오염 시도의 영향은 전혀 없거나 거의 영향을 미치지 않을 수 있다.

하지만, 부실한 SON 구현은 네트워크에서 잠재적인 Signaling Flood 상태 및 셀 정지와 같은 원치 않은 결과를 초래할 수 있다. 따라서 표준화된 해결책을 명세할 수 있는

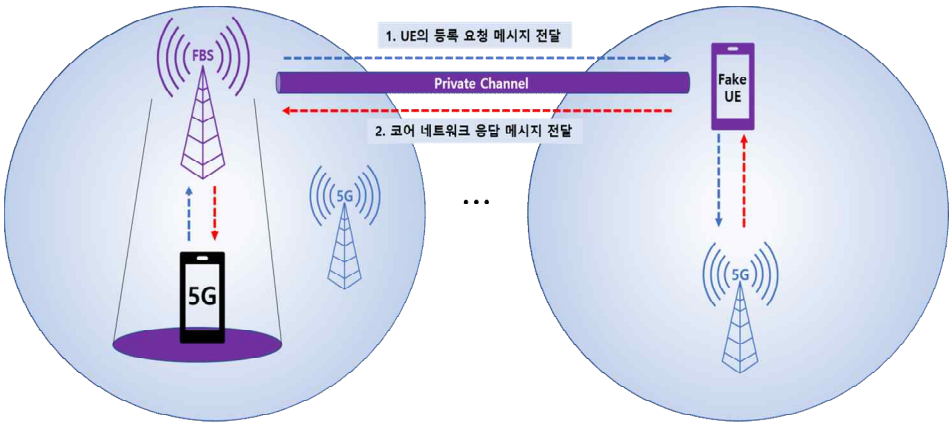
SON의 보안 및 개인정보 사용 사례를 조사하거나 구현을 개선하는 데 도움이 되는 보안 및 개인정보보호 지침을 제공하는 것이 필요하다. 5G 시스템은 네트워크(NG-RAN 또는 5GC)가 허위 기지국으로 인한 다양한 구성 또는 의도하지 않은 업데이트로부터 보호되도록 잠재적인 SON 오염 시도(측정 보고의 위조된 정보)에 대한 보호 메커니즘을 지원해야 한다.

5. 인증 릴레이 공격에 대한 대응

허위 기지국이 정상 기지국보다 더 강한 무선 신호를 보내게 되면 UE는 허위기지국으로 연결될 수 있다. 그렇게 된다면 허위 기지국은 또 다른 악의적인 UE와 사설 채널을 통해 협력하여 공격을 인증 릴레이 공격을 수행할 수 있게 된다.

허위 기지국과 악의적인 UE는 멀리 떨어져 있고, LAN(Local Area Network) 또는 WAN(Wide Area Network)으로 연결되어 두 개의 PLMN(Public Land Mobile Network)을 통해 악성 네트워크를 형성할 수 있다. 허위 기지국은 피해자 UE의 등록 요청 메시지를 악성 UE로 전달하고, 악성 UE는 이를 멀리 떨어진 정상 기지국을 통해 코어 네트워크로 전달한다. 다시 역순으로 허위 기지국과 악성 UE는 코어 네트워크가 보낸 응답 메시지를 피해자 UE에게 전달하여 인증을 완료한다. 이러한 방식으로 네트워크가 인식하는 사용자의 위치와 사용자의 실제 위치가 일치하지 않아 거짓 알리바이를 만들거나 허위 증거로 범죄 수사를 방해할 수 있다. 또한, 공격자가 정상 UE가 로밍 네트워크에 액세스한 것처럼 조작하여 많은 과금을 유도할 수 있다. 다음 그림과 표는 각각 인증 릴레이 공격 흐름과 인증 릴레이 공격을 통해 발생할 수 있는 공격 위협을 나타낸다.

[그림 부록1-8] 인증 릴레이 공격 절차



〈표 부록1-2〉 인증 릴레이 공격을 통해 발생할 수 있는 공격 위협

공격 위협	주요내용
기만	공격자는 피해 UE가 코어 네트워크에 연결되어 있다고 속임
위치 기록 오염	악성 UE는 서로 다른 TA에서 이 공격을 지속적으로 수행하여 피해 UE의 위치 기록을 오염시킬 수 있음
완전 또는 선택적 서비스 거부 공격	악성 UE와 허위 기지국은 피해 UE의 전화/SMS/데이터 전송을 모두 또는 선택적으로 거부할 수 있음
SON에 대한 공격	물리적으로 떨어진 기지국을 중계함으로써 공격자는 UE가 허위 기지국의 신호 강도 및 무선 환경의 신호 강도 측정치를 정상 기지국에 보고하도록 하여 네트워크 SON 구성에 혼란을 줄 수 있음

따라서 허위 기지국으로 인한 인증 릴레이 공격을 완화할 수 있는 수단이 필요하다.

6. 전파 교란에 대한 방어

전파 교란(재밍)은 불법 무선 장치를 사용하여 합법적인 발신자와 수신자 사이의

무선 통신을 방해하는 것이다. 5G 시스템에는 전파 교란 공격을 어렵게 만드는 빔 포밍과 같은 기술적 기능들이 존재한다. 더욱이 전파 교란의 특성상 공격자가 완전히 탐지되지 않는 것은 어렵다. 또한 공격자가 공격을 정지하면 시스템이 자체적으로 복구하므로 지속적인 공격 효과를 보기에는 많은 어려움이 있다.

그럼에도 불구하고 3GPP가 무선 전파 교란에 대한 내성을 어떻게 더욱 향상시킬 수 있을지 연구하는 것이 필요하다. 예를 들어, 탐지 솔루션으로 인해 공격자의 위치와 같은 정보가 노출되는 경우, 탐지될 확률이 높을 때 공격자가 공격하는 것을 포기할 수 있다.

7. 허위 기지국 중간자 공격에 대한 보호

전형적인 허위 기지국 공격은 UE에 대한 서비스 거부를 야기하지만 결과적으로 UE 또는 사용자는 서비스 이용 불가를 기반으로 이러한 공격을 유추하고 그에 따라 조치를 취할 수 있다. 그러나 보다 정교한 공격자는 허위 기지국을 사용하여 은밀하게 다양한 유형의 공격을 시도할 수 있다. MitM(Man in the Middle) 허위 gNB는 UE와 네트워크 간에 메시지를 전달한다. 예를 들어, 보안된 메시지는 그대로 전송하지만 사전 인증 트래픽, MAC/RLC 계층 메시지 헤더, 버퍼 상태 보고와 같은 낮은 계층의 제어 메시지 등과 같은 보호되지 않은 메시지는 삭제, 변경 및 삽입할 수 있다.

일부 상황에서 MitM 공격은 주로 메시지를 재전송함으로써 수행된다. 즉, MitM 허위 기지국은 정상 기지국과 UE 사이에 있고 허위 기지국은 기지국의 메시지를 UE로, UE의 메시지를 기지국으로 전달한다. 중간에서 MitM 허위 기지국은 오랫동안 아무 작업도 하지 않아 탐지하기가 매우 어렵다. 특정한 경우에 허위 기지국은 메시지를 삽입, 변경, 삭제할 수 있다. MitM 공격에 대응하기 위한 기본적인 요구사항 중 일부는 재전송 보호와 관련이 있다.

MitM 허위 gNB로서 동작하는 허위 기지국은 공격자의 목표에 따라 다르게 행동한다. 특히, 허위 기지국이 무선 환경 구성과 관련하여 위장한 gNB를 얼마나 모방하는지는 알려지지 않았다. 개념 증명으로 실제 네트워크에서 수행된 알려진 공격은 위장한 gNB를 모방하는 기능을 포함하지 않고 실험이 진행되었다. 그러나 공격자가 UE 및 네트워크가

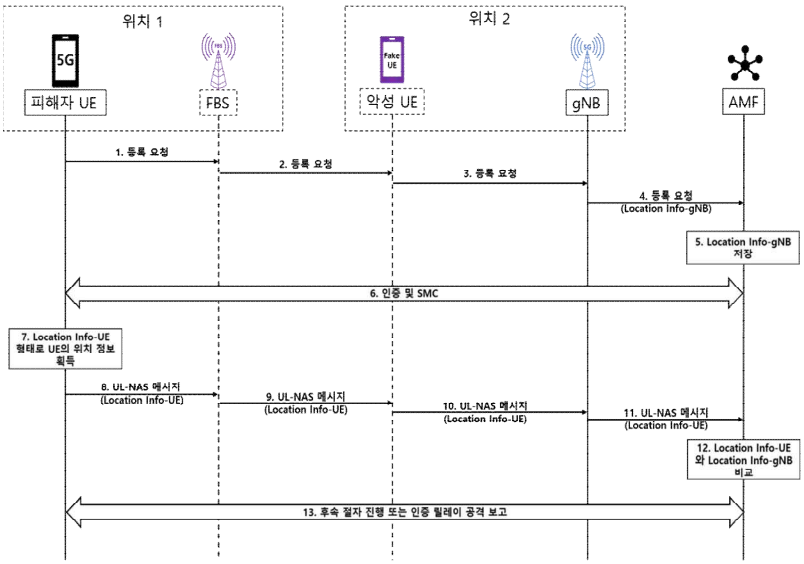
허위 기지국을 탐지하기 위한 조치를 할 수 있다는 점을 고려한다면 실제 공격에서는 gNB를 모방하여 동작할 수 있다. MitM 위협을 해결하지 않으면 허위 기지국 탐지 및 이에 대한 대응책의 효율성이 감소한다. 모든 트래픽을 변조하지 않고 단순히 전달만 하는 중계기는 이 중요 이슈의 목적상 MitM 허위 기지국으로 간주하지 않는다. 전파 범위 확장기와 같은 이러한 장치에 대한 합법적인 사용이 존재할 수 있다.

제3절 5G에서의 허위 기지국 공격 대응 방안

1. 인증 릴레이 공격에 대한 대응

이 대응 방안은 같은 PLMN(Public Land Mobile Network)을 사용하는 피해 UE와 악성 UE가 있고, 피해 UE가 허위 기지국 FBS(False Base Station)에 연결되어 있으며 이 경우 FBS는 악성 UE와 사설 채널을 통해 통신한다고 가정한다. 이 대응 방안에서 GNSS(Global Navigation Satellite System) 정보는 UE의 GNSS 칩에 의해 생성되는 Location Info-UE로 사용된다. 개인 정보 보호 문제의 경우, 사용자는 UE가 자신의 GNSS 정보를 코어 네트워크에 전송할 수 있는지 여부를 나타내기 위해 eLCS 절차에 따라 개인정보 설정을 수동으로 구성할 수 있다. 사용자의 위치 정보 검증에 실패하면 거부 메시지가 UE로 전송된다. 이때 전송된 원인 값을 UE의 지역 위치로 지정한다.

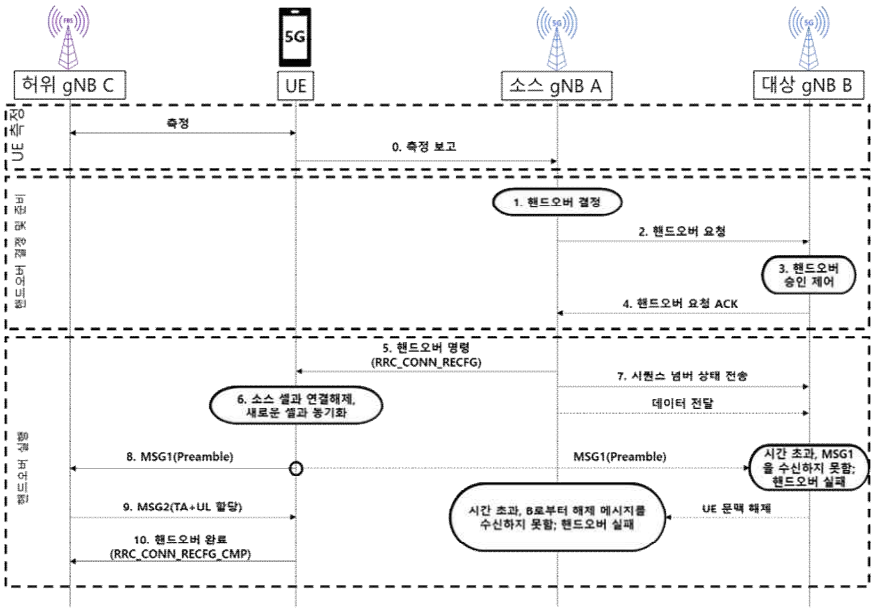
[그림 부록1-9] 위치 정보 기반 인증 릴레이 공격 대응 절차



2. 핸드오버 중 UE의 허위 기지국 연결 회피

일반적으로 5G RAN(Radio Access Network)에서 핸드오버 결정은 UE의 측정 보고를 바탕으로 한다. UE는 브로드캐스트 된 동기화 신호를 운반하는 SSB와 보안 없이 전송되는 MIB 신호를 기반으로 인접한 셀의 신호 강도 측정을 수행한다. 정상 기지국 B의 SI를 위조하는 허위 기지국 C가 있다고 가정하고 서빙 기지국 A는 C에서의 측정값을 포함한 UE의 측정 보고를 수신하면 기지국 A는 UE 측정 보고에 포함된 정보를 통해 UE가 기지국 B에 속한다고 판단하고 UE를 B로 핸드오버 하기로 할 수 있다. 결과적으로는 UE는 허위 기지국 C에 연결을 시도하게 된다.

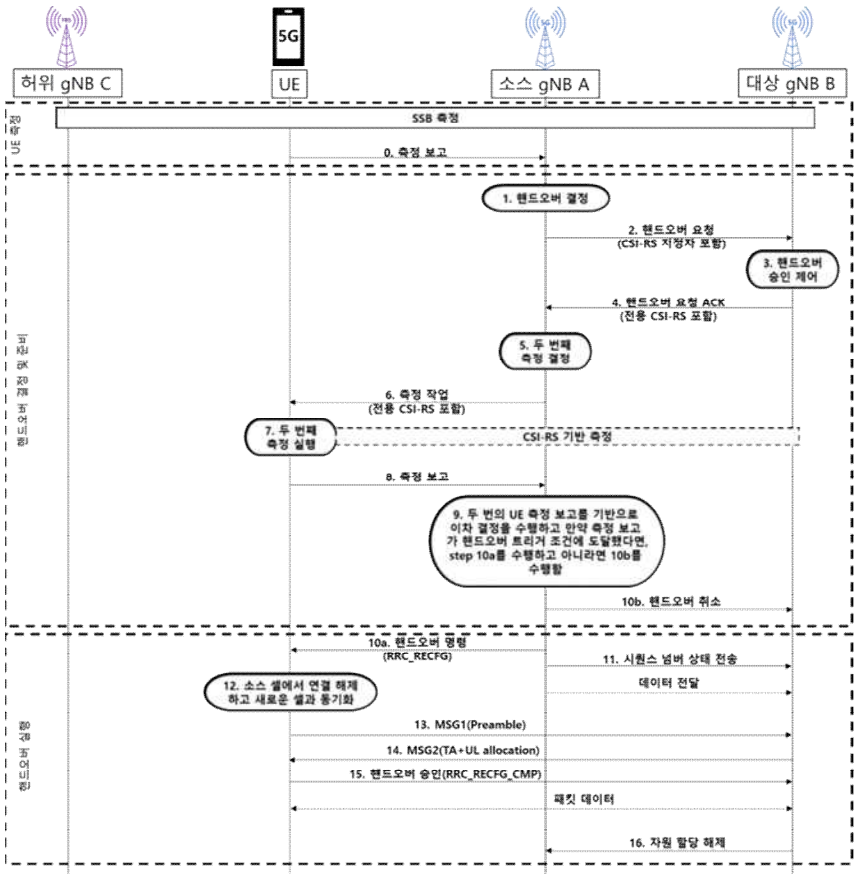
[그림 부록1-10] 허위 기지국에 의한 핸드오버 실패 절차 예시



실제 대상 gNB B는 UE로부터 핸드오버 완료 메시지를 수신하지 못하여 핸드오버가 실패한 것으로 간주한다. 소스 gNB A는 대상 gNB B로부터 UE 문맥 해제 메시지를 수신하지 못하여 핸드오버 실패로 판단한다. UE의 경우, 허위 기지국에는 UE 보안 컨텍스트가 없기 때문에 UE는 후에 RLF(Radio Link Failure) 상태로 전환하지만 허위

기지국에 연결되어 있기에 공격자는 공격을 수행할 수 있다. 이를 완화하기 위한 대응 방안은 대상 gNB가 UE에 할당한 특정 CSI-RS(Channel State Information Reference Signal을 기반으로 하는 2차 측정을 도입하였다.

[그림 부록1-11] 2차 측정을 활용한 허위 기지국 연결 회피 절차



CSI-RS는 UE가 측정을 수행하기 위해 사용되며, 대상 RAN에서 할당하는 UE 지정 매개 변수이며 각 UE마다 다르다. 이 대응 방안에서 CSI-RS는 암호화되고 무결성 보호된 RRC 측정 작업 메시지로 UE에게 제공되므로 허위 기지국은 CSI-RS를 위조할 수 없다. 따라서, UE는 대상 RAN의 실제 신호를 측정할 것이고, 허위 기지국의 위조된 셀로

인한 잘못된 핸드오버를 시작하지 않게 된다. 핸드오버 전에 새로운 신호 오버헤드가 필요하지만 On Demand로 구성할 수 있다.

3. 호출 통계 및 측정 보고를 활용한 근처의 허위 기지국의 네트워크 기반 탐지

이 대응 방안은 Connected 상태의 UE를 대상으로 한다. Connected UE가 정상 gNB에서 허위 기지국으로 핸드오버를 시도하면 실패하게 되고, UE는 새로운 대상 셀을 선택한다. UE는 그 후에 새로운 대상 셀과 연결되기 때문에 핸드오버에 한 번 실패했더라도 이 절차로부터 수집된 정보는 보통 무시된다. UE가 Connected 상태에 있으면 핸드오버 준비단계에서 허위 기지국 환경을 측정하고 선택할 수도 있다. 서빙 기지국이 UE 측정 보고를 수신했을 때, 핸드오버 임계점을 넘겨서 보고된 대상 셀 ID에 핸드오버를 위한 X2/Xn 링크 설정을 시도한다. UE로부터 보고된 대상 셀 ID가 허위 기지국이면 X2/Xn 링크 설정에 실패한다. 여기서 서빙 기지국은 UE에 의해 보고된 셀 ID가 구성 데이터베이스에 없거나, X2/Xn 링크 설정에 실패하면 대상 셀은 PLMN 네트워크에 속하지 않은 것을 의미한다. 서빙 기지국은 보고된 셀 ID가 자신의 PLMN 네트워크에 속하지 않는다고 결정할 수 있다.

[그림 부록1-12] 측정 보고를 활용한 허위 기지국의 네트워크 기반 탐지 절차

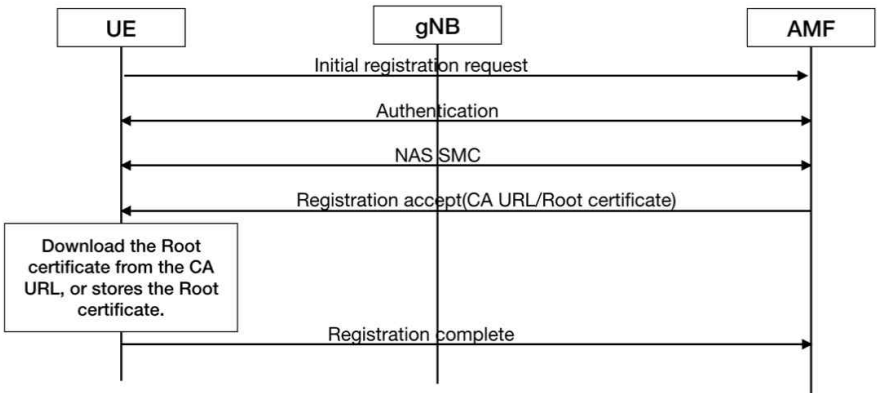
또는 허위 기지국이 실제 셀의 셀 ID를 복사하여 최대한 정상 기지국과 비슷하게 동작할 수도 있다. 이 경우, UE는 두 개의 송신기를 탐지하고 측정하기 때문에 같은 셀 ID이지만 다른 값을 가진 두 개의 측정 보고를 전송한다. 서빙 기지국은 두 개의 UE 측정 보고로부터 중복된 셀 ID를 통해 위장한 허위 기지국이 있다는 것을 알 수 있다. 하지만 측정 보고에서 서빙 기지국이 어떤 셀 ID가 PLMN의 진짜 기지국에 속하는지 아닌지 판단하는 것은 어렵다.

4. 허위 기지국에 대응하기 위한 인증서 기반의 대응 방안

이 대응 방안은 네트워크가 PKI(Public Key Infrastructure)를 기반으로 하고 gNB는 자체 개인키로 브로드캐스트 메시지에 서명하고 메시지, 전자서명, gNB의 인증서를 UE에 전송하고 UE는 프로비저닝 인증서 발급자의 CA(Certificate Authority) 공개키와 같은 신뢰 Root를 활용하여 메시지의 진위를 검증할 수 있다. MNO(Mobile Network Operator)에는 신뢰 체인의 Root로 하나 이상의 CA가 있어야 한다. UE는 USIM(Universal Subscriber

Identity Module) 또는 기타 구현 종속 방식으로 정할 수 있는 둘 이상의 CA Root 인증서 저장을 지원할 수 있어야 한다.

[그림 부록1-13] AS(Access Stratum) 기반 키 프로비저닝 절차

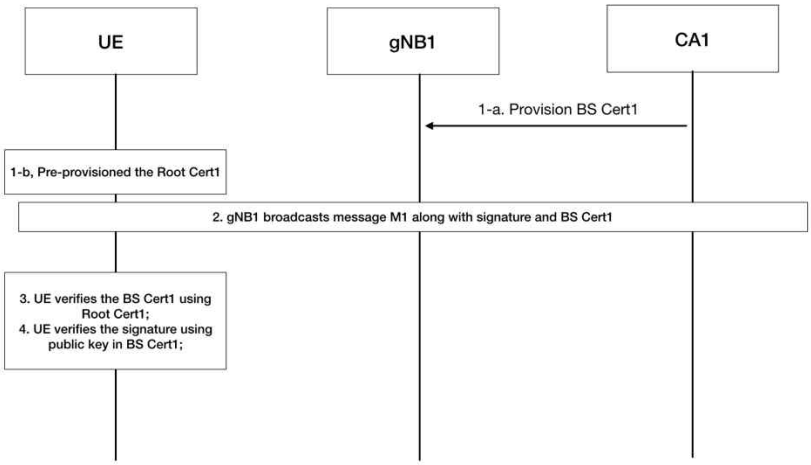


UE에 Root 인증서를 프로비저닝 하는 기법이 2가지 존재한다. 첫 번째는 USIM 또는 ME(Mobile Equipment)를 제조할 때 Root 인증서를 포함하는 방법과 두 번째로 UE가 네트워크에 등록하고 인증을 수행한 후 신뢰할 수 있는 서빙 네트워크에서 Root 인증서를 신청하고 UE는 서빙 네트워크에서 직접 인증서를 얻거나 다운로드하기 위한 URL(Uniform Resource Locator)을 획득한다.

Root 인증서는 일반적으로 수명 주기가 길기 때문에 사용자가 UE를 변경하기 전에 업데이트가 발생하지 않을 수 있다. CA가 손상된 경우 Root 인증서를 변경해야 하며 공급 업체는 소프트웨어 업데이트와 같이 사설 채널을 사용하여 업데이트한다. MNO가 CA 프로비저닝 및 해지를 제어하는 방법의 추가 연구가 필요하다. 각 gNB는 자체 개인키와 인증서로 프로비저닝 되어야 한다. gNB는 자신의 개인키를 사용하여 브로드캐스트 메시지에 서명해야 하며 gNB 인증서는 서명과 함께 또는 별도의 메시지를 UE에 전송되어야 한다.

이 대응 방안을 지원하는 UE는 ECDSA(Elliptic Curve Digital Signature)를 지원해야 한다.

[그림 부록1-14] 인증서 기반 브로드캐스트 메시지 서명 절차



MNO는 CA1을 구축하고 Root 인증서는 Root Cert1, CA1은 해당 개인키와 관련된 gNB의 공개키를 포함하는 BS Cert1을 gNB1에 프로비저닝 한다. UE는 ME 또는 USIM에서 CA1의 공개키로 프로비저닝 된다. gNB1이 메시지를 브로드캐스트 할 때 메시지 M1, 전자 서명 및 BS Cert1을 UE에 보내야 한다. 전자서명은 메시지와 gNB의 개인키에서 생성되며 BS Cert1에는 확인하는 데 필요한 공개키가 포함되어 있다. UE는 메시지를 수신하면 해당 CA 공개키를 사용하여 BS Cert1의 유효성을 검증해야하고 검증에 실패하면 메시지를 삭제한다. 그 다음 UE는 BS Cert의 gNB 공개키를 사용하여 서명을 검증한다. 서명 검증에 성공하면 UE는 이 메시지를 승인하고 실패하면 메시지를 삭제한다.

[부록 2] 5G 특화망 적용 기술 유형 및 기술별 보안 고려사항 연구

제1절 5G 보안 위협 및 보안구조

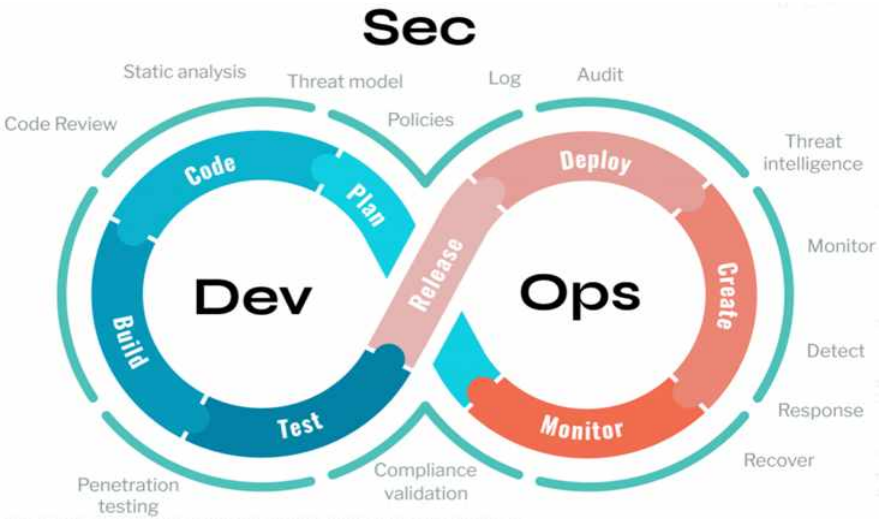
1. 5G 공통보안위협

3장에서는 5G 특화망의 주요 보안위협에 대해 살펴보았다. 이번 장에서는 보안위협에 대한 피해 최소한을 위한 보안 고려사항에 대해 살펴보겠다.

(1) 5G 특화망 연결 단말 · 운영 장비 제품 개발 및 운영 보안 고려사항

5G 특화망에는 주요 구성 요소인 사용자 단말 (UE), 5G 특화망 운영 장비인 5G 코어 네트워크, MEC 등이 소프트웨어을 기반으로 하고 있다. 따라서 소프트웨어 개발 과정에서의 안정성 확보가 무엇보다 중요하다. 따라서, 소스코드 검토 프로세스, 코딩 모범 사례 적용, 정적 및 동적 코드 분석, 외부 코드 안정성 검토 프로세스, 개별 제품 취약점 스캔 등 제품을 개발하는 단계별 보안 평가 및 테스트 등 체계적이고 검증 가능한 개발 프로세스를 갖추는 것이 필요하다. [그림 부록2-1]와 같이 제품 개발 후 운영 상에서 발생하는 문제점 등을 다시 제품 개발에 개선 사항으로 받아들이는 선순환 구조와 각 단계 별로 고려되어야 하는 보안 고려사항을 반영한 DevSecOps 방안을 도입하여 개발하는 것이 좋을 것이다.

[그림 부록2-1] 5G 특화망 제품 개발을 위한 DevSecOps 개념도



제품 개발과 판매가 끝이 아니라, 제품 개발 버전 관리, 보안취약점에 대한 공지 및 지속적인 보안 업데이트를 통해 5G 특화망 단말 및 운영 장비의 보안을 강화해 나가야 할 것이다.

소프트웨어 제품 · 운영 장비를 공급하는 업체의 보안과 체계적인 개발 프로세스도 중요하지만, 제품을 도입하는 사용자도 제품 검증이 동시에 필요하다. 제품 공급 업체의 공급과정에서 발생할 수 있는 악성코드 주입, 취약한 개발 시스템을 통한 공격 등에 대응이 필요하다. 따라서, 제품 사용자는 공급업체에 대한 위험평가, 하드웨어 육안 검사, 자체 제품 보안 점검 및 소프트웨어 취약점 테스트 등 공급망 사고로 인한 위험 수준 평가 및 정량화, 사고 발생 시 대응 지침 수립이 필요하다.

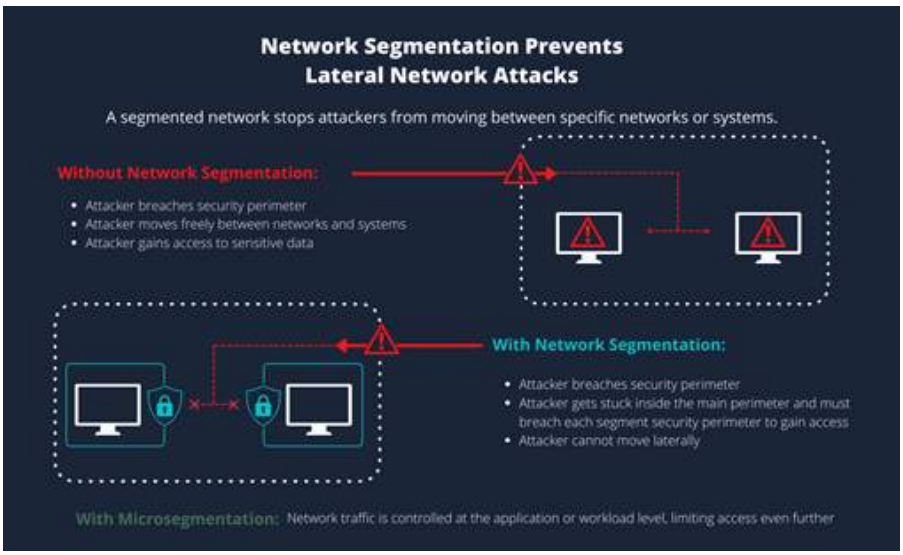
(2) 5G 특화망 네트워크 및 연동구간 보안 고려사항

5G 특화망 네트워크는 [그림 부록2-2]와 같이 네트워크 세그멘테이션 (Network Segmentation)[1] 적용하고 네트워크 보안시스템이 생성하는 보안이벤트에 대응할 수

1) 공격자가 접근할 수 있는 데이터를 제한하기 위해 전체 네트워크에서 일부 부문만 접속할 수 있도록 네트워크 상에서 서브 네트워크를 만들어 설정하는 방법

있도록 구성하고 지속적인 모니터링이 가능하도록 설계되어야 한다.

[그림 부록2-2] Network Segmentation 개념도

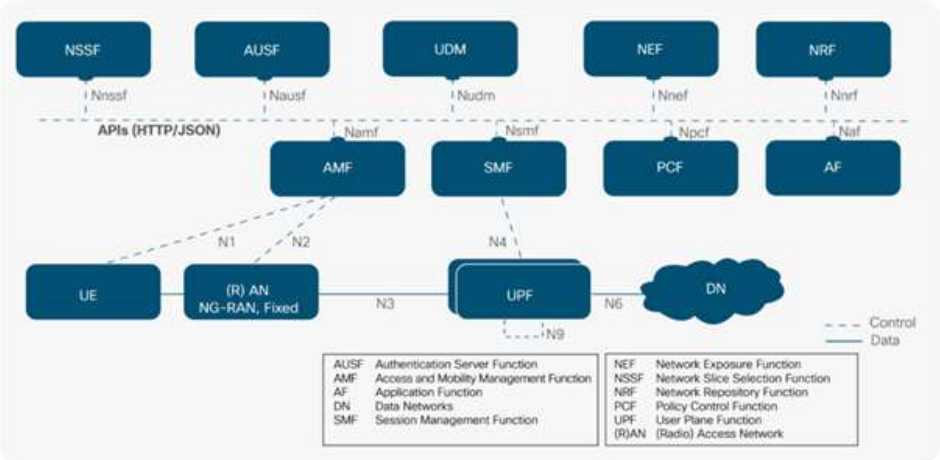


그리고 각 엔티티 (사용자 및 장치)의 식별되고 각 시스템에 접근할 수 있는 ID/암호, 인증서, 멀티펙터 인증수단 등을 활용한 자격증명과 자격에 합당한 역할, 속성, 권한 수명 등 권한 할당이 고려되어야 할 것이다.

각 네트워크 인터페이스 별 특성을 고려하여 네트워크 침입탐지, 방화벽 및 암호화 등의 보호조치를 해야한다. 중요 NF 보호를 위한 IDS 및 Anti-DDoS 장비를 설치하고 모니터링을 해야한다. [그림 부록2-3]에서 보는 바와 같이 외부 인터넷과 연결되는 User Plane Function (UPF)의 N6 인터페이스를 통해 각종 보안위협 시도가 발생할 수 있다. 따라서 이에 대한 네트워크 보안 제어가 적용되어 있어야 하고, 5G 특화망에 다양한 접속 단말의 해킹사고로 발생할 수 있는 DDoS 공격에 대비하여 N3 인터페이스에 DDoS 방어 장비 설치를 고려해야 한다. 그리고, 사용자 데이터에 제어 데이터를 실어서 N4 인터페이스를 통해 SMF등 주요 NF에 접근을 시도하는 등의 해킹시도를

차단하기 위해 트래픽 관리를 위한 네트워크 설정에 신경을 써야할 것이다.

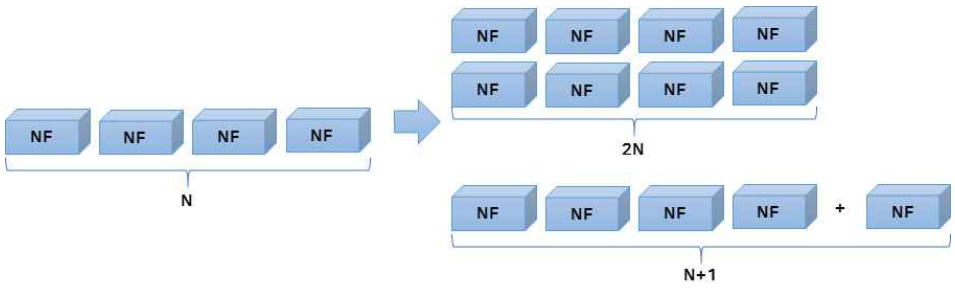
[그림 부록2-3] 5G SA 시스템 아키텍처



(3) 5G 특화망 코어 네트워크 보안 고려사항

5G 특화망 코어 네트워크의 주요 NF는 사이버 공격 및 재해로 인한 서비스 중단을 최소화하고 연속성을 보장할 수 있도록 조치를 해야 한다. SDN/NFV를 도입하여 NF 부하, 사이버 위협에 빠른 대응이 가능하도록 할 수 있으며, NF 중요도에 따라 원격 이중화 등 중복 운영 (Redundancy) 등을 고려해야 한다. [그림 부록2-4]와 같이 중요도가 높은 NF의 경우 2N, 다른 NF 경우 N+1 운영을 고려해 볼 수 있다.

[그림 부록2-4] 5G 특화망 NF 중요도에 따른 이중화



5G 특화망 코어 네트워크는 NF간 SBA 기반 TLS 통신이 가능하기 때문에 이를 위한 Public-Key Infrastructure (PKI) 및 인증서의 안정한 보관 및 관리가 중요하다. 따라서, 인증서의 발급부터 배포 등 키 관리에 대한 안정성 확보가 필요하다. 그리고 SDN과 NFV을 기반으로 NF가 빠르게 배치되고 변화할 수 있기 때문에 수동으로 인증서를 발급하는 것은 불가능해질 것이다. 따라서 인증서 발급 및 배포를 자동화할 방안이 고려되어야 할 것이다.

(4) 5G 특화망 MEC 및 네트워크 슬라이싱 보안 고려사항

5G 특화망의 MEC는 클라우드 이용하여 서비스를 제공할 것이다. 따라서, 자체 클라우드 구축 또는 외부 클라우드 인프라 활용에 따라 접근 제어 등의 보안이 필요할 것이고 클라우드 간 안전한 통신을 위한 보호 수단이 고려되어야 한다. 그리고 MEC에 설치되는 Application 및 API의 안정성에 대한 고려가 필요할 것이다. 특히 바이러스, Structured Query Language (SQL) Injection 같은 악성코드 삽입, 디렉토리 접근 공격 (Directory traversal), 비인가 시스템 및 데이터 접근 허용 등과 같은 취약점 예방을 위한 관리 방안이 필요하다.

5G 특화망에 활용될 네트워크슬라이싱은 한 슬라이스의 데이터 트래픽이 다른 슬라이스로 이동을 차단할 수 있는 “트래픽 분리”, 다른 슬라이스에 할당된 대역폭 사용을 금지하는 “대역폭 분리”, 모든 가상 슬라이스가 동일한 물리적 리소스를 사용하지만 패킷은 독립적인 프로세스에서 처리되도록 하는 “프로세싱 관리”, 특정

슬라이스에 사용되는 데이터는 다른 슬라이스에서 접근할 수 없도록 별도 저장하는 “스토리지 분리” 4가지를 고려하여 설정해야 한다.

⑸ 5G 특화망 운영 및 모니터링 보안 고려사항

5G 특화망의 안정성을 위해 운영·관리 및 모니터링을 위한 인력과 조직이 필요하다. 이들 인력과 조직을 통해 5G 특화망 운영을 위해 저장된 민감 데이터를 암호화 하고 데이터의 무결성 보호, 부인방지를 위한 해싱 및 전자서명, 백업 및 복구에 대한 지침, 데이터 중요도 평가 및 평가에 따른 접근 제한을 해야할 것이다.

그리고, 주요 5G 특화망 운영 장비에 접근하는 단말 및 사람에 대한 인증 및 권한 부여, 접근 관리에 대한 설정이 필요하고 운영 장비에 접근하는 관리 단말에 대한 보안 관리 및 접속 시 암호화 통신 등을 고려하여 운영해야 할 것이다.

AI 및 ML이 5G 특화망에서 본격적으로 도입되어 사용될 경우, 학습데이터 조작, 악의적 샘플 삽입 등 AI 운영에 영향을 줄 수 있는 공격에 대한 대응을 고려하여 안전한 알고리즘에 대한 선택 및 운영이 이루어져야 할 것이다.

5G 특화망이 다양한 분야에 도입됨에 따라 보안을 잘 운영하는 기업이 있는 반면, 보안이 잘 고려되지 않는 사업장도 생겨날 것이다. 서비스 가용성을 위해 보안을 제한적으로 운영하고 이동통신 보안 요소들이 발전 및 적용 사례에 관심없이 기존에 운영 방식을 관행적으로 따르거나 5G 특화망 고려사항에 대한 지식이 없어서 어떻게 적용하고 관리해야 하는지 모르는 등 운영자에 대한 교육 및 보안 의식 제고 또한 필요한 것이다.

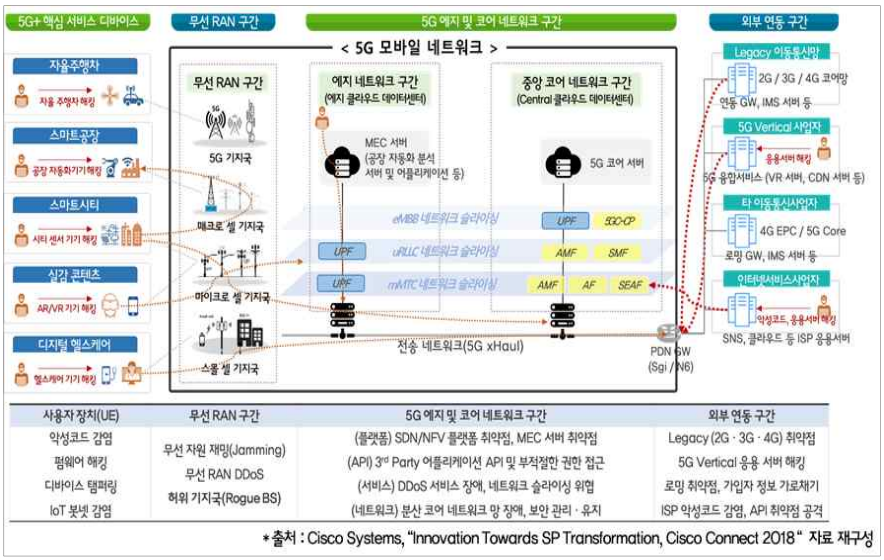
2. 5G 네트워크 구간별 보안위협

다음은 5G 기술에 특화된 각 구간별 보안위협을 설명한다. 일반적으로 이동통신 망에 연결되어 데이터가 전송되는 경로는 사용자 단말(UE)에서 시작하여 무선 액세스 네트워크(RAN), 이동성 관리, 인증, 과금 등 이동통신기능을 제공하는 코어 네트워크를 거쳐 IP망(인터넷, 로밍 등)의 응용 서버들과 연결된다.

5G 특화된 보안 이슈를 요약하면, 5G 네트워크에 기존 Legacy 이동통신망(2G・3G・4G)과 인터넷 서비스망(SNS, 클라우드 서버 등)과 연결될 뿐만 아니라 자동차, 의료, 공장 등 수직 산업 군의 네트워크와 IoT 기기들이 연결되기 때문에 5G 네트워크를 중심으로 복잡한 이기종 망들의 네트워크 연결 구조를 만들게 될 것이다.

이러한 망의 복잡성은 서로 다른 보안 요구사항과 적용하는 보안 기술의 수준이 상이한 네트워크와 기기의 상호 연결로 인해 취약한 연결 고리가 발생할 수 있다. 5G 보안성을 저하(downgrade)시킬 수 있다는 점이 가장 큰 보안 위협이 될 수 있다. 다음은 5G 기술 관련된 보안 이슈들을 IoT 기기 보안위협, 무선 RAN 보안위협, 5G 네트워크 보안위협, 가상화 인프라 보안위협, MEC 보안위협 5가지로 분류하여 설명한다.

[그림 부록2-5] 5G 네트워크 구간별 보안위협 구조



(1) IoT 기기 보안위협

IoT 기기는 스마트폰과는 달리 기기 유형(공장 기기, 스마트시티 센서, CCTV 등)과 어플리케이션, 공급망 생태계가 다양하고 복잡하기 때문에 공통된 보안 표준과 아키텍처 설계가 쉽지 않다. 따라서, 해커들은 취약한 IoT 기기에 접근하여 악성코드에 감염시켜

대량의 IoT 봇넷을 구성하여 C&C 서버를 통한 원격으로 제어하여 IoT 기기를 공격 수단으로 활용이 가능하다. 5G 특화망에 연결되는 IoT 기기의 보안위협유형은 다음 표와 같다.

<표 부록2-1> IoT 기기 보안위협 유형

보안위협	주요내용
USIM(UICC) 카드 공격	· 5G에서 새로운 UICC 카드형식(eUICC, 소프트 sim)은 데이터 유출, 부정 행위 또는 DoS 목적으로 악용될 수 있음 · 다양한 유형의 새로운 UICC 구성요소(eUICC, iUICC, 소프트 SIM 등)는 사용자 프로파일과 사용자 life cycle의 제공을 위한 새로운 관리 프로토콜을 요구되며, 이러한 프로토콜은 사용자를 향한 DoS를 생성하거나 사용자 의인화를 포함한 사기 시나리오에 이용될 수 있음
소프트웨어・펌웨어 변조 및 악용	· IoT 제품의 소프트웨어 및 펌웨어를 불법적으로 위・변조하거나, 취약점을 악용하여 악성코드 삽입 또는 민감한 데이터에 불법적으로 접근 시도
전송 메시지 유출 및 변조	· IoT 제품 간 유・무선 네트워크를 통해 전송되는 민감한 데이터를 불법적으로 유출 또는 변조
저장 데이터 유출 및 변조	· IoT 제품 내부에 저장된 운영 관련 중요 데이터 또는 민감한 데이터를 불법적으로 유출 또는 변조
위장(Spoofing)	· 정당한 사용자 또는 IoT 제품으로 위장하여 IoT 서비스에 불법적으로 접근 시도
물리적 인터페이스접근	· IoT 제품의 물리적 인터페이스 접근을 통해 펌웨어 불법적으로 교체 또는 탈취하거나 악성코드를 무단으로 삽입
취약한 네트워크 서비스	· 제거되지 않은 IoT 제품의 불필요한 네트워크 서비스를 통해 IoT 제품 또는 민감한 데이터로 접근 시도
보안구성 옵션 미흡	· IoT 제품에서 강력한 비밀번호 적용, 암호화 적용, 사용자 권한별 접근권한설정 등 보안구성이 미흡하여 IoT 디바이스로 불법 접근 허용
서비스거부 공격(DOS)	· 대량의 네트워크 트래픽을 유발시켜 IoT 자원 및 대역폭을 고갈시키거나 무선신호 방해, 혼선 등을 통해 정상적인 IoT 서비스를 방해
무작위 공격	· 사용자 인증 정보에 대한 무작위 공격을 수행하여 IoT 제품 또는 네트워크에 불법적으로 접근 시도

(2) 무선 RAN 보안위협

무선 RAN 구간은 다양한 형태(매크로셀, 마이크로셀, 펨토셀 등)의 기지국 장비들로 구성된다. 무선 RAN 기지국 장비는 무선통신 인터페이스(Air Interface)를 통해 사용자 단말기(UE)와 연결되고 유선(Wired) 전송 네트워크를 통해 5G 코어장비와 연결해주는 중계 장비 역할을 한다.

5G 무선 RAN 기술은 다양한 이종 무선접속과 대량 IoT 기기의 접속이 허용되면서 무선 RAN 구간의 보호가 중요하다. 이동통신 서비스 연결을 위해서는 사용자 장치와 무선RAN 구간의 기지국(eNB, gNB) 장비와 코어망의 통신장비(MME) 간 제어 신호(이동, 인증, 과금 등)를 교환한다. 무선 RAN 기지국에 연결되는 수백만의 사용자 장치로 인한 비정상 제어 트래픽이 송수신할 경우 장애에 대한 복원력 이슈와 접근이 용이한 스몰셀 기지국 보안이 중요하다.

무선 RAN 보안위협은 대표적으로 악성코드에 감염된 대량의 IoT 봇넷에 의해 무선 자원에 과도한 접속을 요청하는 무선 RAN DDoS 공격과 무선 신호 채널에 대한 재밍(Jamming) 공격이 있다. 무선 RAN DDoS와 전파 방해 재밍 공격에 의해 기지국들이 비정상 데이터를 송수신함으로써 RAN 구간의 무선 인터페이스 자원을 고갈시켜 정상적인 데이터 수신을 방해하는 가용성 이슈 발생이 가능하다. 허위 기지국(Rogue Base Station) 이슈는, 공격자가 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 수행될 수 있다.

<표 부록2-2> 무선 RAN 보안위협 유형

보안위협	주요내용
주파수자원 남용	· 같은 동적 할당/재할당 때문에 이러한 자원의 불법적인 사용은 합법적으로 허가를 받은 단위의 특성을 모방하고 무선 주파수 간섭을 야기하여 특정 유휴 주파수 대역을 점유할 수 있음 · 주파수의 불법 점유는 네트워크 노드가 무면허 장치에 의해 요청된 주파수 자원을 거부하도록 유도할 수 있으며 이는 유휴 자원의 명백한 부족으로 인해 코어 네트워크 밖으로 누군가가 빠져나가는 것을 차단
ARP(주소 결정 프로토콜	· 공격자가 스푸핑된 ARP 메시지를 네트워크로 보내는 기술인 ARP 캐시 스푸핑이라 함

보안위협	주요내용
포이즈닝 공격	· 공격자의 MAC 주소를 기본 게이트웨이와 같은 다른 호스트의 IP 주소와 연결하여 해당 IP 주소를 대신 공격자에게 전송하도록 하는 공격임
가짜 액세스 네트워크 노드	· 위협은 모바일 사용자 장비(UE)와 네트워크 사이의 통신을 변조하여 다른 악의적인 행동을 개시함 · 가짜 엑세스 노드를 합법적인 노드로 위장하여 기지국(gnB)과 연결설정을 통해, 중간자공격(man-in-the-middle) 이나 네트워크 트래픽 조작과 같은 다른 유형의 2차 공격을 용이하게 함
Flooding 공격	· 다량의 요청 신호를 무선 RAN 인터페이스에 보내는 공격으로, 무선 RAN 기지국의 자원을 소진여 무선 주파수를 감소시키거나 완전히 정지시킬 수 있는 과도한 데이터 전송 공격임
가입자식별정보 포획 (IMSI Catcher) 공격	· 이 위협은 피해자와 인접한 악의적인 행위자가 피해자의 soft-identity(예: 전화번호, 트위터 핸들)를 호출과 연관시키기 위해 악용할 수 있는 휴대 전화 호출 프로토콜과 관련이 있음 · 악의적인 행위자는 '$mathsf{ToRPEDO}$'라는 이름의 공격을 통해 피해자의 거친 위치 정보를 확인하고, 조작된 페이징 메시지를 주입하고, 서비스 거부 공격(denial-of-service, dos)을 할 수 있음
무선 주파수 재밍	· 악의적인 활동/자산 남용으로 분류되는 이 위협은 네트워크 무선 주파수(NRF)의 의도적인 중단/간섭으로 인해 코어 네트워크(및 관련 서비스)가 영향을 받는 사용자에게 접근할 수 없게 함 · 무선 주파수 재밍은 무선 기반 네트워크를 사용할 때 전송 계층을 사용할 수 없는 GPS 간섭을 말함
MAC 스푸핑	· MAC 스푸핑은 네트워크 기기에 있는 네트워크 인터페이스의 MAC(Media Access Control) 주소를 변경하는 공격임 · NIC(네트워크 인터페이스 컨트롤러)에서 하드 코딩된 MAC 주소는 변경할 수 없으나 많은 드라이버는 MAC 주소 변경을 허용하는 취약성으로 인해, MAC 주소를 공격자의 MAC 주소로 마스킹하는 과정을 MAC 스푸핑이라고 함
액세스 네트워크 환경설정 데이터 조작	· 액세스 네트워크 요소(예: 기지국)와 연결과정에서 환경설정 데이터를 위조하여 2차 공격(예: DoS)을 개시할 수 있음
무선 채널 간섭	· 무선 액세스 네트워크 서비스를 일시적 또는 무한정 방해하여 공격자가 의도한 사용자가 네트워크 리소스를 사용할 수 없게 하려는 위협임 · 무선 액세스 네트워크에 손상된 5G 기기가 도입되면 보다 상당한 DoS 위협이 발생할 수 있음.

보안위협	주요내용
무선 트래픽 조작	· 악의적인 공격자가 자신의 기지국(BTS)을 실제 네트워크의 기지국으로 위장하여 중간자 공격을 통해 트래픽 조작을 수행 · 이 위협은 이전 세대의 이동통신기술과의 역호환성 때문에 여전히 유효함
세션 하이재킹	· 세션 하이재킹은 악의적인 활동 또는 자산 남용으로 분류되며, 다른 유형의 공격을 수행하기 위해 특정 트래픽의 전체 세션을 제어하기 위해 악의적인 행위자에 의한 합법적인 인증 communication 세션 ID의 도용을 통해 수행됨
시그널링 사기	· 우려되는 영역 중 하나는 사기에 악용될 수 있는 네트워크 간의 international 신호 상호 연결이다(예: false charging). 가짜 기존 신호를 전송하고 다른 모든 사용자가 특정 대역(스펙트럼 구멍)을 비우도록 강제해 전용을 획득하는 그리드 이동 노드(greedy mobile nodes)의 위협도 한 예임
시그널링 DoS	· 시그널링 DoS(Stroming)은 사용자 기기가 악성코드 감염되거나 악성앱에 의해 발생될 수 있으며, 이는 이동통신 장비들(셀, 백본 signaling 서버, 클라우드 서버)의 대역폭에 과부하를 주며, 모바일 장치의 배터리 전력을 고갈될 수 있음 · 시그널링 DoS 공격은 사용자 기기의 과도한 연결 요청, 소규모 기지국, 높은 사용자 이동성으로 인해 대응이 더욱 어려움

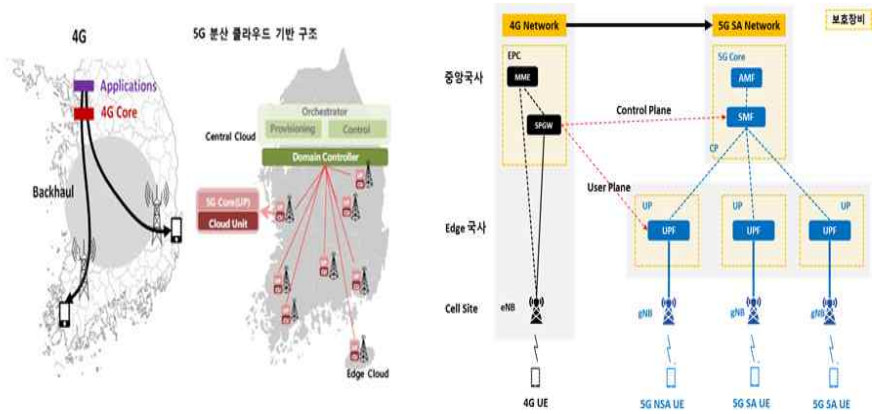
(3) 5G 네트워크 보안위협

5G 네트워크는 분산화된 코어 네트워크 구조를 채택한다. 4G까지 신호 및 데이터 전달경로가 코어 네트워크(4G EPC)까지는 중앙국사로 트래픽이 모이는 중앙집중형 네트워크 구조로 구성되어 있으며, 5G는 통신기능을 지역적으로 재배치하기 위해 코어네트워크와 에지 네트워크로 분리하여 분산화하였다.

5G 네트워크의 주요 특징은 첫째, 제어 트래픽(Control Plane)과 사용자 데이터(User Plane) 트래픽의 경로가 물리적으로 분리되었다. 둘째, 중앙국사에서는 제어 트래픽을 주로 처리하고 사용자 데이터는 지역 국사에 구축된 클라우드 에지 통신센터에서 처리하도록 하였다. 따라서 분산 코어 네트워크 구조는 보호대상이 광범위하게 지역적으로 분산화되어 보안 가시성 이슈 발생할 수 있으며, 보호 수준이 다른 Legacy 네트워크(2G, 3G, 4G) 장비들이 상호 연결되어 사이버공격 발생 시 종합적이고 분산적 대응이 요구된다.

5G 네트워크 보안 위협은 원격 엑세스 남용, 인증 트래픽 급증, API 취약점, 5G 네트워크 설계 취약점, 네트워크 구성설정 오류 등 네트워크 장비 보안 위협이 존재한다.

[그림 부록2-6] 5G 네트워크 구조



* 그림 출처: (좌) 통신사업자 관점의 5G 네트워크 기술, KT 융합기술원, (우) Netmania 홈페이지 (이장우) 그림 재수정

<표 부록2-3> 5G 네트워크 보안위협 유형

보안위협	주요내용
원격 액세스 남용	· 이 위협은 중요한 네트워크 구성 요소에 원격으로 액세스하고 가상 머신을 제어하여 다른 유형의 공격을 수행하는 악의적인 행위자로 구성됨 · 원격 액세스 기능에 대한 불법적인 액세스를 확보함으로써, 악의적인 행위자는 네트워크의 중요한 영역에서 운영 체제와 애플리케이션에 연결할 수 있음 · 네트워크상의 기계에 접속하면, 악성 행위자는 구성 데이터를 변조하거나 악성코드를 배포하는 등의 2차 공격 수행이 가능
인증 트래픽 급증	· 이 위협은 짧은 시간에 악의적인 행위자가 보낸 엄청난 수의 인증 요청과 관련이 있으며, 악의적인 행위자는 연결을 목표로 하는 IoT 기기의 인증 트래픽 급증을 개시함 · 결과적으로, 네트워크는 처리할 수 있는 더 많은 신호 전달과 인증 요청이 발생
사용자 인증/인증	· 이 위협은 코어 네트워크 장비를 관리하는 내부자 또는 적대적이거나 신뢰할 수 없는 직원에 의해 사용자 인증 정보 및

보안위협	주요내용
데이터 남용	보안 통제 데이터(예, keys) 오남용과 관련이 있음
제3자 호스팅된 네트워크 기능(NFs) 남용	· 이 위협은 5G 네트워크를 구성할 때 제3자 클라우드 서비스 제공자의 시스템에 호스팅되는 핵심 네트워크 기능으로 인한 가용성 문제와 민감한 데이터의 공개와 관련이 있다. · 신뢰할 수 없는 클라우드 서비스 제공자는 사용자/제어 트래픽에 접근, 중단 및 수정할 수 있는 우려가 있음
API 취약점	· 애플리케이션 프로그래밍 인터페이스(API)를 이용하여 다양한 유형의 공격이 가능함 · 내부 네트워크 기능, 로밍 인터페이스 등을 서로 다른 네트워크 계층에 노출시키는 다른 유형의 API를 대상으로 할 수 있음 · 부정확한 액세스 제어 규칙으로 잘못 설계되거나 구성된 API는 핵심 네트워크 기능과 민감한 매개변수를 노출시킬 수 있음
5G 네트워크 아키텍처 설계 취약점	· 5G 네트워크 망 설계 시에 의도하지 않은 손상(부적절한 설계, 계획 또는 부적절한 적응)에 의한 위협으로서 최적의 아키텍처, 적절한 보안 및 운영 절차에 도달하기 위한 복잡성 수준과 어려움은 설계와 구현의 저하를 초래함. · 디자인 결함은 악의적인 행위자들이 악용할 수 있으며, 적절하게 구현되거나 보호되지 않는 특정 기능을 알고 있기 때문에 악의적인 행위자는 침입을 악용하여 코어 네트워크에 악성코드 침투 등에 이용될 수 있음
시스템/네트워크상의 잘못된 구성 및 환경설정 취약점	· 구성 설정 결함은 제품 설치 및 유지보수와 같은 솔루션 구현 life-cycle의 서로 다른 단계에서 발생할 수 있음 · 예를 들어 제대로 구성되지 않은 API, 네트워크 기능, 액세스 제어 규칙, 네트워크 조각, 관리 권한, 가상화 환경, 트래픽 격리, 엣지 노드, 조정 소프트웨어, 방화벽 등이 있음
네트워크, 시스템 및 장치의 잘못된 사용 또는 관리	· 의도하지 않은 손상(장치와 시스템의 잘못된 관리과 제대로 유지되고 관리되지 않는 네트워크에서 발생하는 오류는 네트워크의 기밀성, 무결성 및 가용성을 손상시킬 수 있음 · 잘 관리되지 않는 시스템과 관련된 조치의 예로는 네트워크를 공격에 노출시킬 수 있는 운영 프로세스와 절차 부족 포함
로밍 상호 연결과 관련된 사기 시나리오	· 로밍은 방문한 네트워크가 사용자의 홈 네트워크에게 인증 벡터를 요청해야 하며, 이를 통해 사용자를 간접적으로 인증하여 서비스로서 이동통신사업자(MNO) 리소스(위치정보 등)에 대한 액세스를 제공하여 이를 악용할 경우 정보유출 문제가 발생
네트워크	· 중요 구성 데이터의 관리와 보호에 불충분한 정책은 네트워크의

보안위협	주요내용
환경설정 데이터 조작	기밀성과 무결성에 영향을 미치면서 예측 불가능한 시스템 행동과 중요 플랫폼에 대한 무단 액세스를 초래할 수 있음 · 이 위협은 구성 데이터를 위조하여 다른 공격(예: DoS)을 실행함으로써 코어 네트워크 요소(예: SDN 컨트롤러, 네트워크 기능, 관리 및 조정 기능)를 타협하는 것이 포함 · 네트워크 구성 및 제어부(control plane)의 환경설정 데이터 조작은 라우팅 테이블, 환경설정 위변조, DNS 조작들이 있음
코어 네트워크 구성요소의 악의적인 플루딩 공격	· 플러딩 공격은 데이터 전송 중에 발생할 수 있으며, 네트워크 구성품 자원을 소진하고 구성품이 제공하는 서비스의 감소 또는 완전 종료와 같은 네트워크 가용성 훼손을 초래할 수 있음 · 특정 SDN 구성요소에서 가짜 발신자의 작은 요청이 대규모의 응답을 이끌어 내는 증폭(reselection)/홍수(Flood) DDos 공격이 발생
악의적인 트래픽 전환	· 트래픽 흐름을 우회시키는 트래픽 전환은 데이터 평면(data plane)의 네트워크 요소와 관련된 위협이며, 가상화된 네트워크에서 이용할 수 있는 특정한 종류의 트래픽 전환은 네트워크 슬라이스 침입이 있을 수 있음 · 이러한 위협은 모든 활성 노드에서 슬라이스 사이의 필수 절연이 손상되거나 엣지 장비의 슬라이스에 대한 강제 액세스가 우회되거나 잘못 구성될 때 발생 가능함
네트워크 리소스 오케스트레이션 조작	· 이 위협은 Orchestrator의 설정(E2E 서비스 인벤토리, 서비스 프로그래밍 기능)을 변경하여 네트워크 기능 간의 분리를 저해하여 네트워크 기능 동작을 수정하는 것을 말함
공유 자원의 불법접근 및 사용 사용	· 5G 연결 장치의 무단 액세스 및/또는 수정 중요 데이터. End-to-end 키는 중앙집중식 키 서버에서 도난당하거나 유출 가능 · 결과적으로, End-to-end 보안 통신은 서로 다른 공격에 취약하고 적들은 end-points에 접근가능하며, 근본 원인은 통신사업자(MNO)의 직원 네트워크에서 인증, 인가, 회계(AAA) 자격 증명이 유출된 데 있다.
악의적인 네트워크 기능(NFs) 등록	· 이동통신사업자(MNO) 또는 벤더/서비스 제공자에 의해 네트워크에 소개된 트로이 목마를 내장한 허가받지 않은 네트워크 기능(NF) 또는 기능은 다른 악성 API를 노출하기 위해 SBA(서비스 기반 아키텍처)에 남용하여 설치되고 NRF를 통해 코어 네트워크에 등록될 수 있음 · 비허가 네트워크 기능을 설치하거나 활성화함으로써 악의적인 행위자는 네트워크의 민감한 자산에 접근하여 DoS, 악성 소프트웨어 배포, 민감한 정보 도용 등의 다른 유형의 공격을 수행할 수 있음

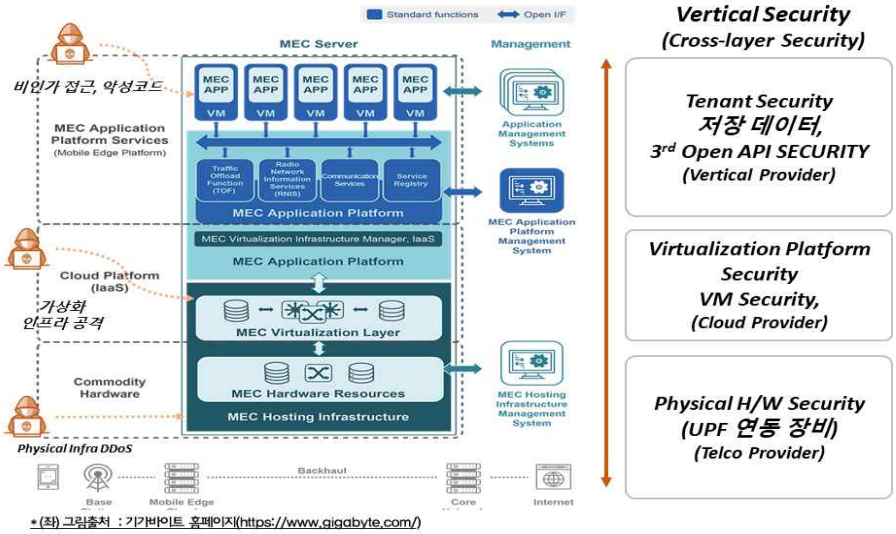
보안위협	주요내용
트래픽 스니핑	· 악성 행위자는 스니핑과 함께 네트워크 요소나 링크의 데이터를 도청하고 정보를 훔칠 수 있음 · 예를 들어 SDN에서 악의적인 행위자는 암호화되지 않은 통신을 이용하여 중앙 통제기로의 트래픽을 가로채 캡처된 데이터는 네트워크에서 허용되는 흐름이나 트래픽에 대한 중요한 정보가 포함될 수 있음

(4) 가상화 인프라 보안 위협

5G 소프트웨어 기반 인프라는 5G 통신서버와 네트워크 장비, 네트워크 슬라이싱 서비스를 SDN 및 NFV 가상화 기술을 통해 구현된다. 네트워크 슬라이싱기술은 하나의 물리적 네트워크를 다수의 가상 네트워크로 분리하여 uRLLC, mMTC, eMBB 응용 서비스별 독립적인 네트워크 슬라이싱 서비스를 제공한다. 가상화 서버는 물리적 전용장비 대신 범용 x86 서버 상에 네트워크 통신기능을 가상화 소프트웨어 (가상머신) 형태로 구현된다. 마지막으로 가상화 인프라 기술은 5G 장비 및 서비스 구현 핵심으로 물리적 네트워크 및 HW 서버 자원(CPU, 메모리 등)을 공유하여 자원의 효율성, 유연성과 가용성 측면에서 장점을 가진다.

그러나, 물리적으로 공유된 HW 자원에 대한 부하공격, 네트워크 슬라이싱과 공유 자원의 비인가 엑세스, 공유자원을 통한 악성 코드 전파, 가상화 관리 SW 구성설정 오류에 상대적으로 취약할 수 있다.

[그림 부록2-7] 가상화 인프라 보안위협 구조



*(좌) 그림출처 : 기가바이트 홈페이지(https://www.gigabyte.com/)

가상화 인프라 보안 위협은 2가지 우려사항이 존재한다. 첫째 SDN/FNV 보안 이슈이다. SDN 기술은 네트워크 제어 기능(SDN 컨트롤러)과 트래픽 전달(SDN 스위치) 기능을 분리하여 HW적으로 처리되던 네트워크 전달 기능을 SW로 제어하고 통제하기 위한 기술이다. SDN 컨트롤러와 스위치 간 제어 프로토콜 취약점을 악용한 트래픽 우회 공격, 스위치와 컨트롤러 간 비인가 접근, DoS 공격으로 인해 SDN 시스템들의 자원을 고갈시켜 서비스 마비 공격이 가능하다. 범용 서버 상에 구현되는 NFV 기술은 하이퍼바이저 보안, 악성 가상머신(VM) 마이그레이션 이슈, 가상화된 NF 상에 동작하는 응용 프로그램의 변경 또는 인증과 네트워킹 기능에 대한 권한 부여가 적절히 통제되지 않으면 보안 이슈가 발생할 우려가 높으며, 응용 프로그램의 인증 및 권한 부여에 대한 보호 메커니즘이 없다면 3rd Party의 악성 응용 프로그램이 SDN 컨트롤러로부터 네트워크 정보 유출 가능성 존재할 수 있다.

둘째, 네트워크 슬라이싱 보안 이슈이다. 네트워크 슬라이싱은 5G에서 신기술로 물리적으로 동일한 네트워크를 사용하면서 5G 서비스별 트래픽을 논리적으로 분리해주는 가상 네트워크 전송 기술로서, 네트워크 슬라이싱이 적절히 분리되지 않으면 공격자가

하나의 슬라이스에서 다른 슬라이스로 공격을 수행할 가능성이 존재한다. 예를 들어, 특정 서비스의 네트워크 슬라이스에 악의적으로 트래픽 용량을 초과시켜 다른 슬라이스에 영향을 주거나 특정 어플리케이션을 동시 활성화로 슬라이싱 자원고갈 공격 야기할 수 있다. 또한 네트워크 슬라이스에 적절한 암호화가 적용되어 있지 않다면 공격자는 다른 슬라이스에 속한 데이터를 도청하거나 변조 위협에 대한 우려가 존재한다.

<표 부록2-4> 가상화 인프라 보안위협 유형

보안위협	주요내용
데이터센터 연결 프로토콜 남용	· 가상화된 시스템은 데이터 센터(MEC) 내에 배치되므로 데이터 센터의 보안 위협을 고려해야 함 · 이 위협은 DCI(Data Center Interconnect) 프로토콜의 특정 취약성(예: 인증 및 암호화 부족)의 이용과 관련이 있음 · 공격자는 DCI 링크를 통과하거나 DCI 연결의 DoS 공격을 발생시키는 방식으로 스푸핑된 트래픽을 생성할 수 있음
클라우드 컴퓨팅 리소스 남용	· 소프트웨어와 하드웨어 구성요소를 모두 포함한 영향력 있는 컴퓨팅 인프라의 남용은 클라우드 컴퓨팅 서비스 프로바이더의 간단한 등록 프로세스를 통해 쉽게 달성할 수 있음 · 예를 들어, 클라우드 컴퓨팅의 힘을 남용하여 brute force(무차별 대입) 공격과 DoS 공격이 있음
네트워크 가상화 우회	· 잘못된 네트워크 슬라이싱 구현 및 구성이나 부적절한 분리와 관련된 문제는 데이터 기밀성/개인 정보 보호(다른 슬라이스 엔터티(entities of other slices)에 의해 차단된 데이터/트래픽)의 손실을 초래할 수 있음 · 서로 다른 테넌트에 의해 사용되는 네트워크는 합법적인 트래픽만 네트워크 슬라이스에 들어오거나 나가는 것을 보장할 필요가 있음 · 코어 네트워크 하이퍼바이저(hypervisor) 취약성과 흐름 규칙 구성을 이용하여 슬라이스 분리를 침해하고 다른 tenants에 속하는 데이터를 노출 시킬 수 있음
가상화된 호스트 남용	· 이 위협은 가상화된 호스트에서 실행되는 애플리케이션과 관련되며, 가상화된 환경의 공유 리소스 남용과 관련이 있으며, 물리적 자원이 tenants 간에 공유되는 가상 환경에서는 민감한 정보를 공개 우려가 있음 · 예를 들어 가상화된 환경에서 가로채기(interceptions)가 인접 가상머신의 데이터 흐름을 교차-검사할 수 있고 DoS 공격을

보안위협	주요내용
	설정하는 데 도움이 될 수 있는 토폴로지 추론을 허용하기 때문에 가상 환경에서 가로채기 공격은 위험할 수 있음

(5) MEC(다중 엑세스 에지컴퓨팅) 보안위협

다중 액세스 에지 컴퓨팅(Multi access Edge Computing) 기술은 기존 이동통신 코어 내부망을 지나 인터넷 서비스의 응용서버와 연결되는 방식에서 사용자 기기와 가까운 모바일 네트워크 내부에서 응용서버를 구축하여 서비스를 제공하는 개념이다. 5G 네트워크와 에지 컴퓨팅 개념이 결합되어 5G 에지네트워크에 컴퓨팅 서버를 전진 배치시켜 원격의료, 공장자동화, IoT 어플리케이션 및 서비스를 지연 없이 실시간 제공에 장점이다.

이러한 장점에도 불구하고 에지 컴퓨팅 서버가 5G 에지 네트워크 내부(UPF 장비와 연결)로 전진 배치되기 때문에 새로운 연결 경로가 생기는 보안 이슈 우려된다. 특히, MEC는 클라우드 및 가상화 기술을 통해 구현되어 3rd Party 응용 프로그램을 탑재하는 개방형 시스템에서 운영될 것으로 예상되어, 모바일 네트워크의 내부망에 구축되는 MEC 시스템들이 해커들의 주요 공격 대상이 될 수 있다. MEC가 가상화 플랫폼으로 구축되어 일부 VNF(Virtual Network Functions)와 동일한 플랫폼에서 MEC 응용 프로그램이 실행 될 경우, 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 정보 접근하거나,

공격자는 악의적인 응용 프로그램을 삽입하여 분산된 5G 네트워크 내부 장비인 UPF 등 에지 네트워크 기능에 공격을 시도할 수 있는 새로운 공격 경로를 제공할 위험이 우려된다.

3. 5G 보안표준

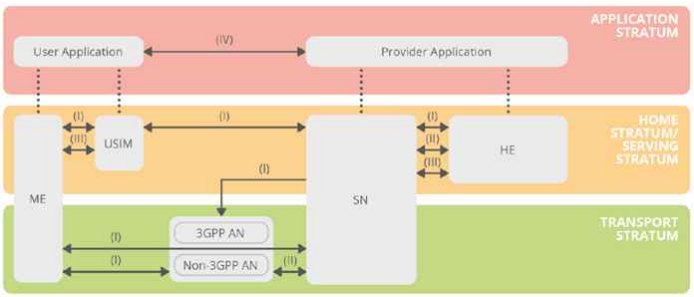
5G 특화망은 5G 단독모드(Standalone, SA)의 보안표준을 기반으로 보안을 고려해야 한다. 5G 보안표준에 관련이 있는 국제 표준 기구는 [그림 부록2-8]과 같이 가장 직접적인 연관이 있는 3rd Generation Partnership Project (3GPP)를 비롯하여 Institute of Electrical

and Electronics Engineers (IEEE), International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), Internet Engineering Task Force (IETF), Engineering Science and Technology Intellects (ESTI)가 있다. 3GPP에서도 Service/System Aspects (SA) Technical Specification Working Group 3에서 Security를 담당하고 있으며, 3GPP Technical Specification (TS) 33.501 "Security architecture and procedures for 5G System" 에 5G 관련 보안이 정의되어 있다.

[그림 부록2-8] 5G 보안표준 관련 국제 표준 기구

TS 33.501에서는 각 스펙트럼 별로 중점적으로 고려한 보안 고려사항을 [그림 부록2-9]와 같이 정의하였다. 각 구간별로 Mobile Equipment (ME)에서 Serving Network (SN) 및 Home Environment (HE) 간 통신하는 과정에서 고려되어야 할 보안 사항 및 User Application과 Provider Application 간 보안 고려사항들이 개념이 정의되어 있다.

[그림 부록2-9] TS 33.501에 정의된 5G 보안 아키텍처 모델



- **Network access security (I)** – security features that enable a user terminal to authenticate and access the network by providing protection on the radio interfaces.
- **Network domain security (II)** - security features that enable network nodes to exchange signalling and user data securely.
- **User domain security (III)** - security features that enable the secure user access to mobile devices.
- **Application domain security (IV)** - security features that enable user and provider domain applications to exchange messages securely. 33.501 specifications do not cover application domain security.
- **Service Based Architecture (SBA) domain security (V)** - a new set of security features that enable network functions of the SBA to communicate securely within serving and other network domains.
- **Visibility and configurability of security (VI)** - security features that enable the user to be informed regarding which security features are in operation or not.

4. 5G SA 보안 강화 사항

5G SA은 이전 세대 이동통신인 4G(LTE)에 비해 프로토콜 면에서 보안적으로 많은 향상이 있었다. 5G 특화망에서는 이러한 보안 강화 사항을 이해하고 적용하는 것이 중요하다. 따라서, 5G SA 보안 강화 사항에 대해 알아보겠다.

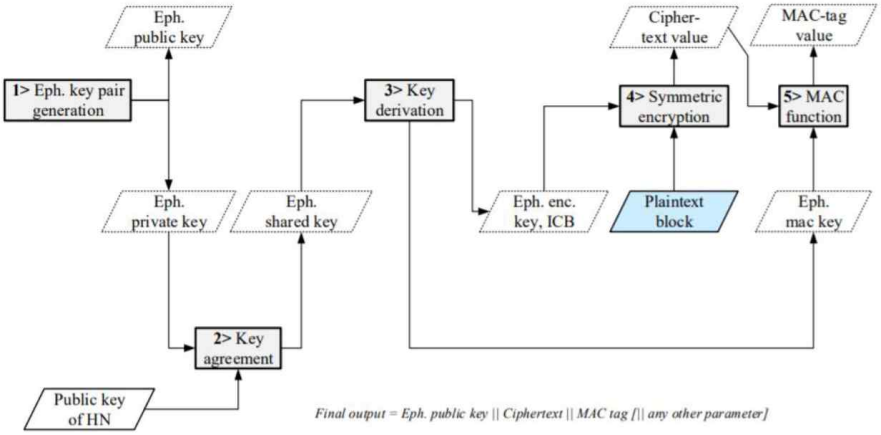
강화된 보안사항 중 인증 부분에서 사용자 단말(User Equipment, UE)이 Serving Network에 접속을 시도할 때, 암호화된 가입 식별자인 Subscription Concealed Identifier (SUCI)를 사용한다. 이는 크게 2가지 면에서 보안이 강화된다.

첫째, 4G(LTE)에서 사용하던 가입 식별자인 International Mobile Subscriber Identity (IMSI)는 평문인데 비해 SUCI는 암호화 되었기 때문에 노출이 되더라도 악용을 최소화할 수 있다. 게다가 이동통신 무선구간의 암호채널이 만들어지기 전까지는 평문으로 통신할 수 밖에 없기 때문에 가입 식별자는 노출될 수 밖에 없다. 따라서, 가입 식별자가 노출되더라고 악용을 최소화할 수 있는 방안 필요했는데, 5G SA에서는 SUCI를 통해 보안을 강화할 것이다.

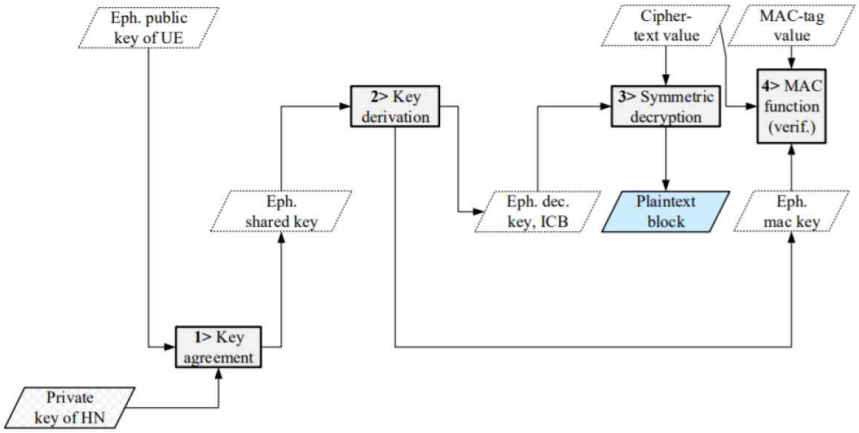
둘째, SUCI 암호화 방식은 Elliptic Curve Integrated Encryption Scheme (ECIES)를

사용되고, [그림 부록2-10]과 같이 사용자 단말에서의 암호화, [그림 부록2-11]과 같이 복호화를 통해 사용자 단말과 이동통신사 (Home Network)간 상호 인증도 가능하다.

[그림 부록2-10] UE에서 ECIES 기반 암호화

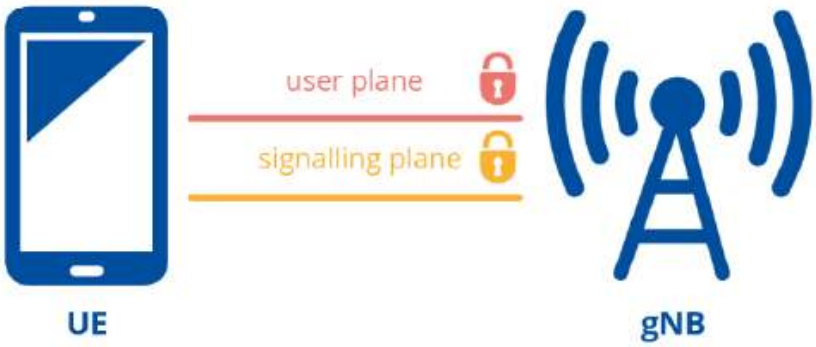


[그림 부록2-11] Home Network에서 ECIES 기반 복호화



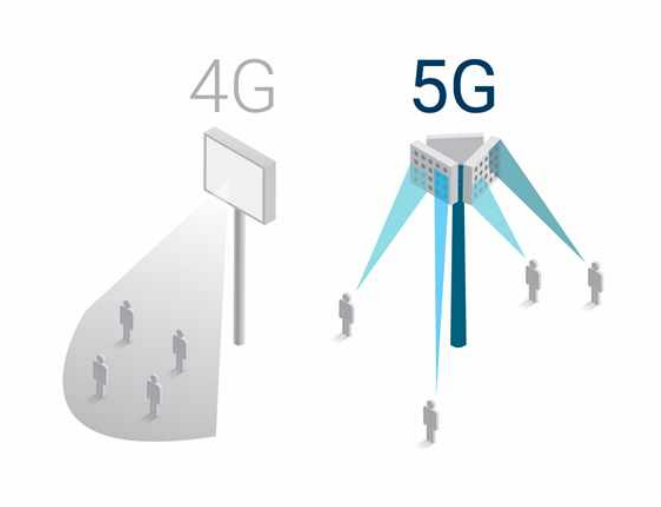
5G SA에서는 4G에 비해 암호화가 강화되었다. 이동통신 데이터는 인증, 암호화 방식 제어 등을 관리하는 제어 데이터 (Control Plane, CP)과 통화, 인터넷 사용 등 사용자 데이터 (User Plane, UP)로 나눌 수 있다. 4G에서는 CP의 경우 Protocol Data Unit (PDU) 암호화 및 데이터 무결성 확인을 위한 Message Authentication Code – Integrity (MAC-I) 암호화가 둘 다 되었던 반면, UP는 PDU 암호화만 지원되었다. 하지만 5G SA에서는 CP와 UP 모두 PDU, MAC-I 암호화가 지원된다.

[그림 부록2-12] UE와 5G 기지국 (gNB) 간 사용자 및 제어 데이터 암호화 통신



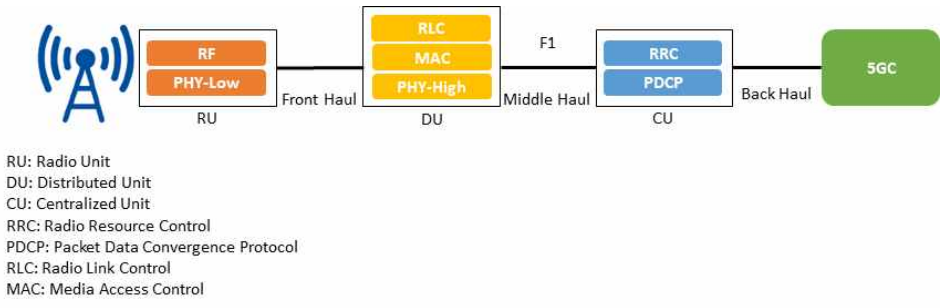
5G New Radio (NR) 기지국은 [그림 부록2-13]과 같이 대량의 안테나와 빔포밍 기술을 활용할 수 있다. 4G 기지국의 경우 서비스 셀 단위에 다수의 사람이 기지국 신호를 공유하는 데 비해, 5G는 대량의 안테나와 빔포밍 기술을 활용하여 개별적인 신호에 의한 서비스 이용이 가능하게 되어 간섭 및 무선 구간 도청을 완화할 수 있는 효과를 가질 수 있다.

[그림 부록2-13] 4G 기지국과 5G 기지국 비교



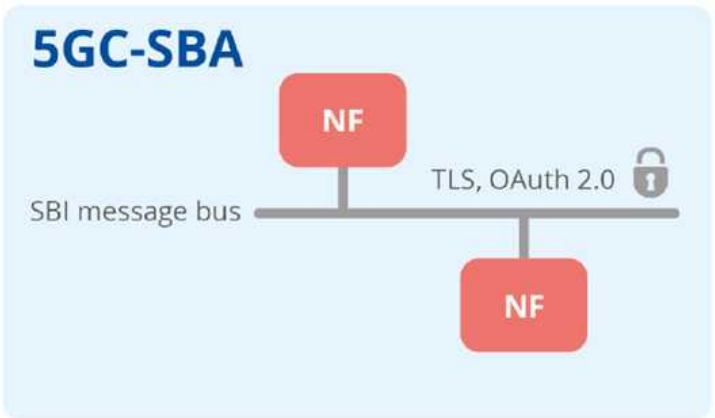
5G NR 기지국은 [그림 부록2-14]과 같이 Radio Unit (RU), Distributed Unit (DU), Centralized Unit (CU)으로 분리되면서, 데이터 전송과 관련된 DU는 안테나 근처에 위치하고 제어 기능와 관련된 CU는 신뢰할 수 있고 물리적으로 안전한 공간에 위치하도록 함으로서 안정성을 강화하였다.

[그림 부록2-14] 5G 기지국과 코어망 간 기능적 분리



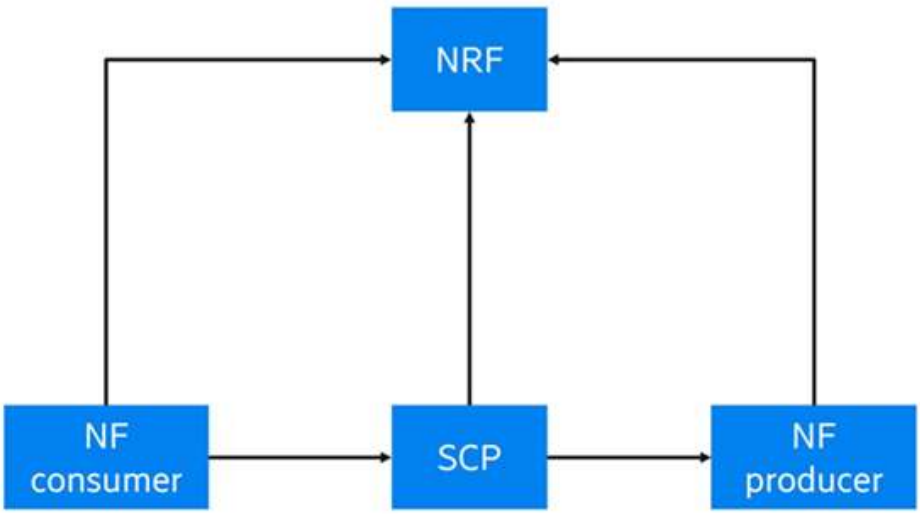
5G SA 코어 네트워크의 기능들이, 장비를 기반으로 한 4G 코어 네트워크 기능들이 기능 수행에서 소프트웨어적인 Network Function (NF) 기반으로 수행될 수 있도록 진화하였다. 이에 따라 [그림 부록2-15]와 같이 각 NF 간 Transport Layer Security (TLS) 기반 인증 및 암호화를 지원하는 Service-based architecture (SBA)로 전환되었다. TLS 기반으로 NF 간 상호 인증과 NF 간 통신에서 암호화 등 기밀성이 보장되게 되었다. NF간 보안성은 TLS 뿐만 아니라 Internet Protocol Security (IPS)와 OAuth 2.0과 같이 속성 기반 보안 (Attribute-based security)도 사용이 가능하도록 지원하고 있다.

[그림 부록2-15] 5G 코어 네트워크의 SBA 기반 NF간 통신 보안 개념도



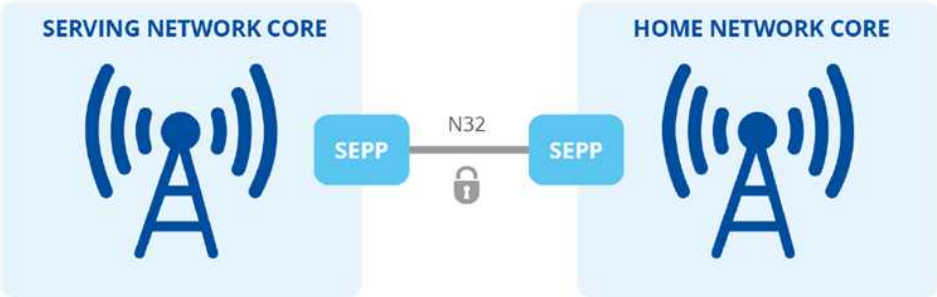
그리고 3GPP Rel. 16에서는 [그림 부록2-16]과 같이 서비스 기반 검색 및 등록을 지원하는 Network Repository Function (NRF)과 Service Communication Proxy (SCP)를 통해 NF consumer (서비스 요청자)가 필요한 NF producer (서비스 제공자)에 직접 접근하지 않도록 함에 따라 특정 NF의 해킹으로 인해 다른 NF로 직접 공격을 시도하는 상황을 예방할 수 있다.

[그림 부록2-16] Rel.16에 정의된 NF간 간접 통신 기반 SBA 모델



5G SA는 [그림 부록2-17]과 같이 로밍 구간에서도 TLS 기반의 JSON Web Encryption (JWE), JSON Web Signature (JWS)와 같은 보안이 강화 뿐만 아니라 Home Network가 Serving Network로부터 서비스 요청을 수신 시 Serving Network에 장비가 존재하는지 검증도 가능하다.

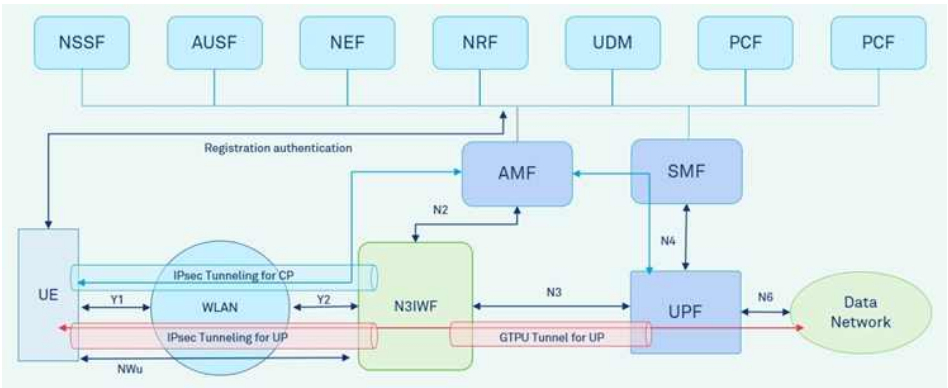
[그림 부록2-17] Security Edge Protection Proxy (SEPP) 간 보안이 강화된 통신 가능



네트워크 슬라이싱을 통해 사용자 및 단말 특성에 맞는 보안 적용 및 데이터 격리가 가능하고 Software-Defined Networking (SDN) / Network Function Virtualization (NFV) 기반으로 5G 특화망의 코어 NF 구성이 가능하기 때문에 사이버 공격이나 운영 부하에 따라 NF를 확대해서 만들거나 망을 효율적으로 변화할 수 있어 빠른 대응이 가능하다.

그리고, 3GPP 또는 non-3GPP 표준 네트워크에 상관없이 5G SA 인증 절차를 사용할 수 있기 때문에 단말 및 Home Network 간 상호 인증과 같은 강력한 보안 사항을 사용할 수 있다.

[그림 부록2-18] 5G Core Network에서 non 3GPP 표준 (WLAN) 통신을 위한 아키텍처



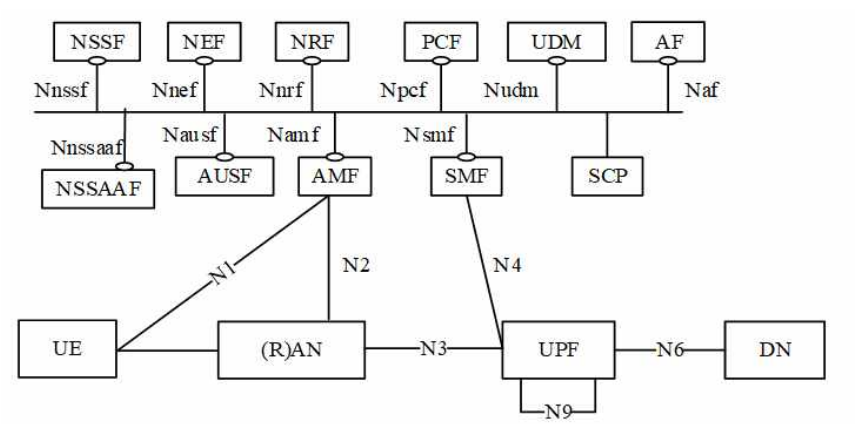
5. 5G 서비스 기반 아키텍처 보안의 구현

(1) 개요

5G 서비스 기반 아키텍처는 웹 기술 및 웹 프로토콜을 기반으로 구축되어 가상화 및 컨테이너 기술과 클라우드 기반 처리 플랫폼을 사용하여 유연하고 확장 가능한 구현을 가능하게 한다. 그러나 광범위한 5G 시스템 구조와 가상화된 구현 및 클라우드 프로세싱이 5G SBA에 다양하고 많은 보안을 요구하도록 만든다[9]. 이러한 보안 요구 사항의 변화를 인식하여 5G SBA에 대한 보안은 새로운 사용 사례와 가상화된 구현에 적절한 보안을 제공하도록 설계되었다.

1) 직접 통신을 위한 SBA 보안

[그림 부록2-19] 3GPP TS 23.501에 명시된 비 로밍 5G 시스템 아키텍처



SBA 보안은 일반적인 5G 보안과 마찬가지로 3GPP TS 33.501에 명시되어 있다. SBA의 중요한 특징은 NF들이 모두 서로 통신할 수 있다는 것이다. NF 서비스 소비자와 NF 서비스 생산자 간의 요청/응답 또는 가입/알림으로 상호 작용한다. 이를 위해서는 NF 간의 통신을 구현할 수 있는 방법과 각 NF의 서비스 API를 보호하는 방법과 이러한 API의 사용을 적절하게 승인하는 방법에 대한 신중한 명세가 필요하다.

또한 기본 프로토콜 스택은 HTTP 및 JSON과 같은 웹 프로토콜을 기반으로 하기 때문에 상호 작용을 보호하는데 사용되는 보안 프로토콜의 선택에도 영향을 미친다.

일반적으로 서로 다른 엔티티 간의 통신을 보호하려면 다음 보안 메커니즘이 구현되어야 한다.

- 메시지 스푸핑을 대응하기 위한 통신 엔드 포인트 사이의 인증
- 메시지 변조, 부인, 정보 노출을 막기 위한 통신 전송 보호(기밀성, 무결성, 재전송 보호)
- 권한 상승을 막기 위한 요청의 인가

SBA 보안 사양의 첫 번째 버전인 릴리즈 15는 NF 간의 직접 통신, 즉 프록시 없이 보안을 자세히 설명한다. 다음의 두 가지 중요한 구성 요소를 기반으로 한다.

- TLS 1.2 및 1.3 기반의 NF 간 상호 인증 및 전송 보안
- OAuth 2.0을 기반으로 NF 서비스 생산자가 제공하는 서비스에 대한 NF 서비스 소비자의 액세스를 위한 토큰 기반 인증

TLS 1.2 및 1.3은 인터넷 및 기타 네트워크에서 통신 보안을 위해 사용되는 최첨단 프로토콜이다. 이전 세대의 모바일 네트워크와 SBA 외부의 5G 네트워크는 IPSec에 의존한다. 보안 관점에서 IPSec이 문제가 있는 것은 아니지만 TLS를 사용하면 전체 네트워크 도메인을 보호하는데 사용되는 보안 게이트웨이 대신 NF에서 직접 보안을 쉽게 종료할 수 있다. 이러한 접근 방식은 다중-차용을 사용하는 가상화된 구현에 적합하다.

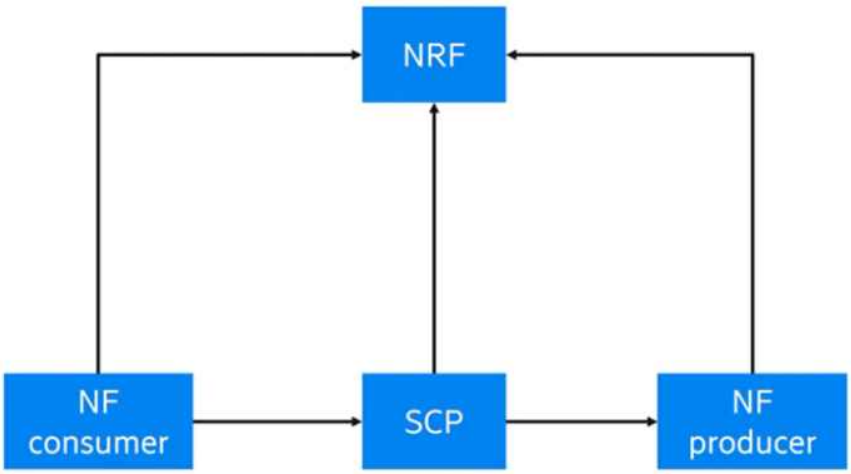
OAuth 2.0을 사용한 토큰 기반 인증은 동적 가상화 구현에서 인증을 수행하는 방식이다. 클라이언트(SBA의 NF 서비스 소비자)에게 인증한 후 액세스 토큰을 발급하는 중앙 인증 서버를 기반으로 한다. 클라이언트는 서비스를 호출할 때 NF 서비스 생산자에게 액세스 토큰을 제공한다. NF 서비스 생산자는 소비자에게 접근 권한을 부여하기 위해 액세스 토큰의 유효성을 검증한다.

SBA에서 NRF는 인가 서버의 역할을 한다. 인가 규칙은 NRF에 등록하는 동안 NF 서비스 생산자가 자체적으로 제공할 수 있다. 토큰 기반 권한은 인증과 결합되어야

유효하다: NRF 및 NF 서비스 소비자는 NRF가 액세스 토큰을 발급하기 전에 상호 인증(TLS 사용)한다. 또한 토큰이 가로채지거나 오용되는 것을 방지하기 위해 전송 보호(TLS가 지원)가 필수적이다.

2) 간접 통신을 위한 SBA 보안

[그림 부록2-20] 서비스 통신 프록시를 통한 간접 통신을 사용하는 릴리즈 16의 SBA 모델



SBA 보안의 두 번째 버전(릴리즈 16)은 간접 통신에 대한 보안을 명세한다. NF 소비자가 NF 생산자와 직접 상호 작용하는 대신 간접 통신은 NF 소비자와 생산자 간의 경로에 SCP(Service Communication Proxy)을 도입한다. 보안 관점에서 중요한 측면은 소비자와 생산자가 NF 서비스 소비자를 대신하여 서비스 요청을 보내고 NF 서비스 생산자의 응답을 소비자에게 전달하기 위해 SCP에 의존해야 한다는 것이다. 이는 기본 신뢰 모델에 영향을 미친다.

SCP는 단순히 소비자의 서비스 요청을 전달만 하지 않는다. SCP의 표준화된 기능과 독점적 기능 모두에 대해 SCP가 활성화되고 서비스 요청 메시지를 수정할 수 있어야 한다. 따라서 각 Hop에 대한 상호 인증 및 전송 보안은 TLS 기반으로 하지

만 직접 통신에서 TLS로 충족하는 소비자와 생산자 간의 종단 간 전송 보안은 간접 통신에서는 불가능하다.

하지만 직접 통신을 위해 이미 명세 된 토큰 기반 인증은 SCP가 이를 대신할 권한이 있음을 생산자에게 증명할 수 있는 수단을 제공한다. SCP는 단순히 NF 서비스 소비자에게 발급된 유효한 액세스 토큰을 생산자에게 전달한다. 일부 배포 모델의 SCP는 NF 서비스 소비자를 대신하여 액세스 토큰을 요청할 수 있다. 이는 NRF가 소비자를 대신하여 액세스 토큰을 요청하도록 승인된 SCP만 할 수 있도록 보장하는 경우에만 가능하다. 이를 위해 소비자는 SCP가 NRF에서 사용하는 자체 서명된 인증서를 SCP에 전송하여 소비자가 승인했음을 증명한다. 이 메커니즘은 토큰 기반 인증을 수행한다. 앞서 언급했듯이 NF 서비스 소비자와 생산자 간의 통신을 위해 SCP는 액세스 토큰 사용하여 대신할 권한이 있음을 증명할 수 있다.

3) SBA 보안 구현

SBA에서 TLS와 OAuth 2.0을 모두 사용하려면 네트워크에서 PKI(Public-Key Infrastructure)를 구축해야 한다. PKI에서 CA(Certificate Authority)는 적절한 신원 관리 기능 및 정책에 따라 각 통신의 엔드 포인트에 인증서를 발급한다. 인증서와 관련된 공개/개인키 쌍은 SBA에 명시 된대로 TLS 및 OAuth 2.0을 사용하는데 필요한 토큰의 상호 인증 및 서명/검증에 사용되는 비대칭 암호화에 사용될 수 있다.

SBA 구현은 주로 빠른 속도로 지속적인 배포 및 업데이트를 지원하는 마이크로서비스 아키텍처를 사용하여 수행된다. NF 간의 연결을 위한 TLS 사용과 함께하려면 NF가 안전하게 보관해야하는 인증서를 발급하고 관리하는 고도로 자동화된 프로세스가 필요하다.

동적 5G 시스템에서 인증서를 안전하게 발급하는 방법을 고려하는 것 외에도 클라우드 환경에서 TLS 엔드 포인트에 대한 비밀 저장소를 보호하는 방법에 대한 문제도 존재한다. 이러한 문제들은 NF가 실제로 하나씩 동작하는 서비스가 아니라 내부 NF 통신을 보호해야하는 상호 작용 마이크로 서비스 모음이라는 상황으로 인해 발생한다. 이 내부 NF 통신은 3GPP 문서에 명시되어 있진 않지만 TLS 일반적으로 통신을 보호하고 API 사용 권한을 부여하며 NF의 토폴로지를 마이크로서비스

집합으로 유지하는데 사용된다. 이 인트라 NF에 대한 인증서가 제공되는 방식은 3GPP 사양에 포함되지는 않지만 NF 내 통신을 위한 인증서 공급 솔루션이 차용자가 요구하는 경우 차용 PKI와 통합할 수 있는 방식으로 구현되어야하므로 밀접하게 관련되어 있다.

SBA는 강력한 규제 요구사항이 있는 모바일 네트워크 사용을 위한 것이므로 차용자의 인증서 제어 문제는 더욱 심화된다. 현재 3GPP 사양에는 인증서를 프로비저닝하는 방법과 적절한 PKI를 지정하지 않은 설정 방법에 대한 몇 가지 세부 정보들이 있다. 대체로 SBA를 구현할 때 인증서 관리 및 관련된 키의 저장이 보안을 위한 중요한 작업을 차지한다.

4) 결론

SBA 및 마이크로서비스 기술의 도입으로 효율적인 모바일 네트워크를 구현할 수 있다. 그러나 5G 보안 사양에서 3GPP가 고려한 새로운 특정 보안 요구사항도 야기한다. SBA 보안은 가상화된 구현에 적합한 TLS 및 기타 웹 기반 보안 프로토콜 사용에 의존한다.

SBA 보안 사양은 직접 및 간접 통신과 상호 인증, 전송 보안 및 인가의 측명을 다룬다. 3GPP SA3 사양은 SBA 보안의 필수 부분을 다루지만 구현 시 고려해야할 측면도 존재한다. 인증서의 수, 슬라이싱 사용 및 다양한 NF는 자동화된 인증서 관리가 SBA 보안 구현의 중요한 부분임을 의미한다. 모든 요구사항을 지원할 수 있는 효율적인 PKI는 NF의 구현 및 관리에 중요하다. 또 다른 측면은 잘 설계된 PKI를 통해 여러 업체의 구현을 보다 쉽게 지원할 수 있다는 것이다.

일반적으로 5G 보안과 관련하여 SBA 보안은 신중하게 정의된 표준, 구현, 배포 및 운영 관리의 조합으로 구성된다. SBA 보안 사양은 새로운 사용 사례, 가상화된 구현에 적합한 보안이 되도록 설계되었다. 사양은 보안의 한 구성 요소일 뿐이므로 구현 측면도 필수적으로 고려되어야 한다.

제 2 절 MEC 및 네트워크 슬라이싱 기술 및 보안 동향 분석

1. MEC 및 네트워크 슬라이싱 보안 기술 동향 연구

다음 그림 [그림 부록2-21]은 MEC 및 네트워크 슬라이싱 관련 표준 및 연구 분석으로 ETSI IGS NFV에서는 MEC의 인프라 가상화 및 관리와 관련된 보안 표준을 설명하였고 3GPP에서는 5G 네트워크 슬라이싱 정의와 보안 아키텍쳐 및 요구사항을 TR33.811, TR33.813. 그리고 TS533.501에서 설명하였다.

[그림 부록2-21] MEC, 네트워크슬라이싱 및 표준과 연구

	MEC	네트워크 슬라이싱
표준	ETSI ISG NFV : MEC의 인프라 가상화 및 관리와 관련된 보안 표준	3GPP : 5G 네트워크 슬라이싱 정의와 보안 아키텍처 및 요구사항 (TR33.811, TR33.813 및 TS33.501)
	TCG : 물리적 플랫폼 보안 표준	GSMA : 자동화된 네트워크 관리 및 제어 네트워크를 도입하여 액세스 네트워크의 보안 수준을 높이기 위한 보안 권장 사항
	IETF : MEC 서비스 액세스 보안 표준	NGMN : 5G의 보안 요구사항 및 네트워크 기능 조사와 네트워크 슬라이싱으로 발생할 수 있는 결함 식별 및 권장 사항
연구 및 프로젝트	MEC AI : MEC 및 AI 통합을 통해 5G 네트워크에서 짧은 대기 시간 및 보안 보장 연구	적응형 보안 메커니즘(Adaptive Security Mechanisms) : 다양한 슬라이스 보안 요구 사항에 따라 노드 선택 및 경로를 선택할 수 있는 SDN 기반 적응 방식의 오케스트레이터 연구
	ANASTACIA (Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures) : NFV/SDN 기반 네트워킹 인프라를 사용하는 통합 MEC 및 IoT 개념을 사용하는 CPS용 설계 솔루션을 통해 전체적인 신뢰 및 보안 연구	FloodDefender : SDN에 대한 Dos 공격을 감지하고 대응하는 솔루션으로 흐름 관리 및 table-miss packet 기능을 가진 다양한 모듈이 공격으로 인한 트래픽을 식별 불필요한 스위치 흐름을 제거하여 리소스를 보호
	SUPERFLUID(A Super-Fluid, Cloud-Native, Converged Edge System) : 서비스 기능을 전체 네트워크로 확장하여 모바일 에지 사용 사례를 지원하는 융합형 클라우드 기반 5G 및 네트워크 처리 기능의 액세스를 제어하는 보안 프레임워크를 개발	동적 스펙트럼 슬라이싱 : 네트워크 트래픽 변동을 고려한 정책 기반 동적 스펙트럼 슬라이싱 방식을 제시하여 단일 물리적 네트워크 리소스를 안전하게 관리

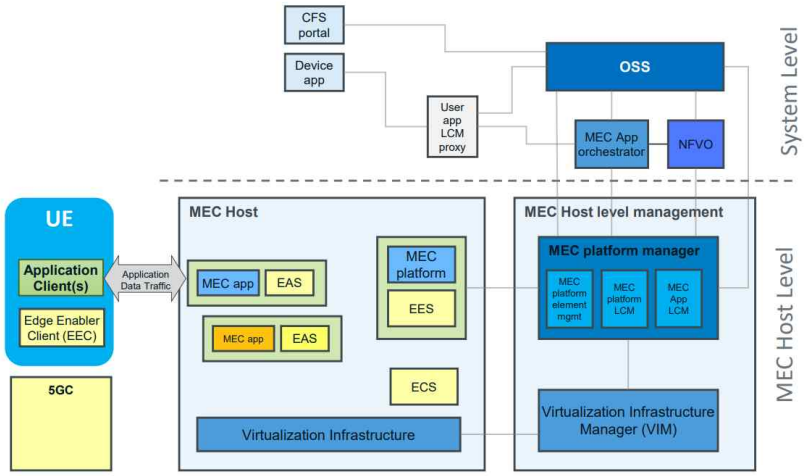
※ 자료: ETSI MEC Security, MEC-enabled 5G Use Cases, Network Slicing: Recent Advances, Taxonomy, Requirements, and Open Research Challenges, SoftSLICE: Policy-Based Dynamic Spectrum Slicing in 5G Cellular Networks

2. MEC 보안 고려사항 연구

본 장에서는 [그림 부록2-22]과 같이 ETSI에서 정의한 MEC 표준 구조를 중심으로 MEC 시스템을 구성하는 핵심 요소를 크게 다음과 같이 선정하고 각 관점으로 보안 위

협과 고려사항을 분석하였다.

[그림 부록2-22] ETSI MEC 참조 구조



자료: ETSI

- 가상화 인프라: MEC 시스템은 클라우드 및 가상화 기술을 바탕으로 제3자 애플리케이션을 실행한다. MEC 호스트는 가상화 인프라에서 MEC 애플리케이션을 실행하고 서비스를 제공하는 필요한 기능들로 구성되며 MEC 애플리케이션의 가상화를 위해 가상머신이나 컨테이너 기술을 사용하여 MEC 애플리케이션 사이에 격리된 공간을 제공한다.
- MEC 애플리케이션 : MEC 호스트가 제공하는 가상화 인프라 상에서 실행되며, MEC 서비스를 소비하고 제공하기 위해 MEC 플랫폼과 통신한다.
- MEC 오케스트레이터(orchestrator): MEC 오케스트레이터는 MEC 시스템 레벨 관리의 핵심 기능으로, 배포된 MEC 호스트, 사용 가능한 자원, 사용 가능한 MEC 서비스나 토폴로지 등을 기반으로 MEC 시스템의 전체 뷰를 유지한다.

(1) MEC 가상화 인프라 관점에서의 보안 위협 및 보안 고려사항 분석

MEC 애플리케이션이 MEC 호스트에서 구동되기 위해 가상화 기술을 필요로 하며,

컨테이너 및 가상머신(VM)이 주로 사용된다. VM은 운영체제가 독립되어 완전히 격리된 환경을 제공하지만 컨테이너의 경우 단일의 운영체제 커널을 공유하며 사용되는 불완전한 격리 환경으로 상대적으로 보안성이 취약하다. <표 부록2-5>은 가상머신과 컨테이너 구조의 특징을 비교한 표이다.

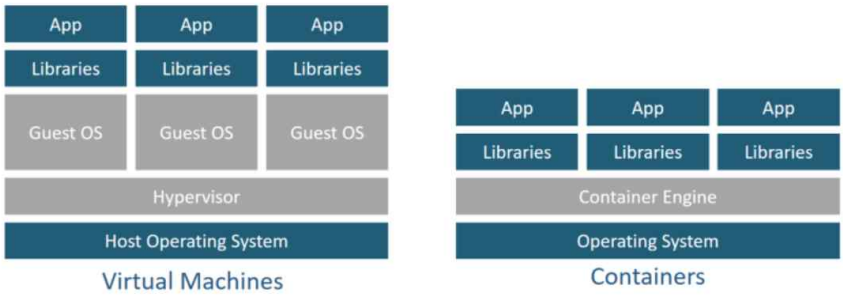
<표 부록2-5> 가상화 기술 특징 비교

	가상머신	컨테이너
가상화	하드웨어 레벨 가상화	OS 레벨 가상화
운영체제	독립적인 이종 다중 운영체제	단일 운영체제 커널 공유
격리	완전한 격리 제공	프로세스 레벨의 격리
효율성	낮음	높음
확장성	제한적	무제한
보안	높은 보안성	낮은 보안성

가상머신은 [그림 부록2-23]과 같이 하이퍼바이저를 통해 호스트 머신과 다른 가상머신으로부터 격리된 환경을 제공한다. 컨테이너는 호스트 운영체제 위에 컨테이너 엔진을 설치하여 애플리케이션 작동이 필요한 바이너리, 라이브러리 등을 하나로 모아 각자가 별도의 서버인 것처럼 사용한다. 5G에서는 클라우드 네이티브 환경[2]을 지향하고 있는 관계로 MEC 애플리케이션 실행을 위해 가상머신에 비하여 상대적으로 보안이 취약한 컨테이너의 비중이 높아지고 있다. 컨테이너와 VM 간에는 많은 기술적 차이가 있지만 운영상의 차이도 상당하며 이러한 운영상의 차이는 컨테이너 보안의 여러 측면에 영향을 미친다. 컨테이너와 VM 간의 운영상의 차이는 다음 내용과 같다.

2) 클라우드 네이티브(Cloud Native) : 클라우드 컴퓨팅 모델의 장점을 최대한 활용할 수 있는 애플리케이션을 개발하고 구축하며 실행하는 방법론으로서, 응용을 가능한 한 작은 단위로 나누고 (Micro-service 구조), 세분화된 응용 단위는 컨테이너로 실행하며, 시장 및 서비스 요구에 따라 즉각적으로 서비스를 실행하고 빈번하게 지속적으로 업그레이드(DevOps)하기 위한 전략

[그림 부록2-23] 가상머신 및 컨테이너 구조 비교



그림출처: Redhat

- 컨테이너 및 마이크로서비스를 통해 애플리케이션을 구축하면 해당 애플리케이션을 VM 중심의 단일 모델에서 실행했을 때보다 훨씬 더 많은 개별 구성 요소가 있다. 예를 들어, VM에서 실행되는 단순한 2계층 웹 애플리케이션에는 프런트엔드에 웹 서버 VM 클러스터만 있고 백엔드에 데이터베이스 VM 클러스터만 있을 수 있다. 마이크로서비스에서는 앱의 기능이 분해되어 다수의 프론트 엔드 컨테이너를 가질 수 있으며, 각각은 앱의 웹 부분의 서로 다른 부분을 실행하고 백엔드의 여러 데이터베이스와 캐시 인스턴스를 실행할 수 있다. 이러한 마이크로서비스를 통해 반복 및 확장이 용이한 반면에 더 많은 개체를 이해하고 관리하고 보호해야 한다.
- 컨테이너를 주요 이점 중 하나는 컨테이너가 제공하는 민첩성으로, 신속한 애플리케이션 반복을 통해 비즈니스 요구에 보다 쉽고 빠르게 대응할 수 있도록 하는 것이다. 기존의 보안 도구와 프로세스는 훨씬 덜 동적인 환경을 가정하는 경우가 많기 때문에 컨테이너형 환경의 변화 속도에 맞게 구성해야 한다.
- 퍼블릭 클라우드 테스트 환경, 프라이빗 클라우드 프로덕션 환경 등 다양한 환경에서 컨테이너와 이미지를 이동할 수 있다. 환경이 더 정적이고 예측 가능했던 VM과 달리 운영 과정에서 여러 위치에서 컨테이너를 이동할 수 있다. 따라서 이들을 보호하는 데 사용되는 보안 도구와 프로세스는 특정 클라우드 제공자, 호스트 OS, 네트워크 토폴로지 또는 자주 변경될 수 있는 런타임 환경의 다른

측면에 대해 가정해서는 안된다.

- VM 및 베어메탈(Bare-metal) 서버는 일반적으로 관리자가 정적 IP 주소를 할당하며, 이러한 주소는 시간이 지남에 따라 상대적으로 일관성이 유지된다. 반대로 컨테이너는 일반적으로 사용되는 모든 조정 도구를 통해 IP 주소를 할당받는다. 지정된 컨테이너에 할당된 IP 주소는 일반적으로 미리 알려져 있지 않으며, 일반적으로 이러한 주소를 할당하는 데 관여하는 관리자가 없다. 컨테이너는 VM보다 생성 및 파괴 빈도가 훨씬 높기 때문에 시간이 지남에 따라 사람의 개입 없이 IP 주소도 자주 변경된다. 이로 인해, IP 주소를 기반으로 트래픽을 필터링하는 방화벽 규칙 집합과 같이 정적 IP 주소에 의존하는 보안 기술을 사용하여 컨테이너를 보호하는 것이 어렵거나 불가능하게 된다.

1) 호스트 운영체제 보안 위협과 고려사항

ⅰ) 부적절한 사용자 접근 권한

컨테이너별 OS는 일반적으로 컨테이너 배치 및 확장을 제공하는 오케스트레이터(Orchestrator)와 함께 사용된다. 이러한 배포에서 OS는 일반적으로 다중 사용자 시나리오를 지원하도록 최적화되지 않는다. 수동적인 구성 및 관리 방식을 사용하는 경우 자신이 호스팅하는 컨테이너형 앱에 필요 이상으로 액세스할 수 있다.

대응 기술은 다음과 같다. 대부분의 컨테이너 배포는 오케스트레이터에 의존하여 호스트 간에 작업을 분산시키지만 관리자는 OS에 대한 모든 검증을 수행하고 비정상적인 상태를 모니터링해야 한다. 또한, 작업을 위해 권한이 상승된 경우와 작업 내용을 모두 기록해야 한다. 이러한 과정을 통해 호스트에 직접 접근하고 권한 있는 명령을 실행하는 것과 같은 비정상적인 액세스 패턴을 식별할 수 있다. 또한 관리자가 작업을 수행하는 데 필요한 특정 리소스에 대해 오케스트레이터가 필요한 특정 액세스만 제공하도록 해야 한다. 예를 들어 프로젝트 foo에서 작업하는 개발자는 프로젝트 foo와 관련된 리소스만 관리할 수 있어야 하며 액세스 할 수 없어야 한다. 오케스트레이터가 기본적으로 이 기능을 제공하지 않는 경우 이를 위해 타사 솔루션을 사용해야 한다.

ii) 호스트 구성요소의 취약점

컨테이너용 OS는 범용 OS보다 공격 표면이 훨씬 작다. 예를 들어 범용 OS가 데이터베이스 및 웹 서버 앱을 직접 실행할 수 있도록 지원하는 라이브러리 및 패키지 관리자는 포함되지 않는다. 그러나 컨테이너용 OS에서도 원격 연결을 인증하는 데 사용되는 암호화 라이브러리와 일반적인 프로세스 호출 및 관리에 사용되는 커널 프리미티브와 같은 호스트 OS가 제공하는 기본 시스템 구성 요소가 있다. 다른 소프트웨어와 마찬가지로 이러한 구성 요소에는 취약성이 있을 수 있으며, 이러한 취약성은 운영체제의 낮은 레벨에 존재하기 때문에 호스트에서 실행되는 모든 컨테이너 및 애플리케이션에 영향을 줄 수 있다.

대응 기술로 기본 OS 관리 및 기능을 위해 제공되는 구성 요소의 버전을 검증하기 위해 관리 및 도구를 사용해야 합니다. 컨테이너용 OS는 범용 OS보다 훨씬 더 적은 구성 요소 집합을 가지고 있지만 여전히 취약점이 있고 여전히 문제가 해결되어야 한다. 호스트는 OS 공급업체 또는 기타 신뢰할 수 있는 조직에서 제공하는 도구를 사용하여 OS 내에서 사용되는 모든 소프트웨어 구성 요소를 정기적으로 확인하고 업데이트를 적용해야 한다. 이 접근방식에서 마찬가지로 중요한 것은 앱과 호스트 OS 간에 명확하게 분리하여 앱을 구축, 테스트 및 운영하는 것이다. 컨테이너형 앱은 호스트별 구성이나 데이터 스토리지에 의존해서는 안된다. 이러한 종속성으로 인해 호스트 OS를 활용하기가 더 어려워지는 경우가 많기 때문이다. 또한 운영 측면에서 여러 노드에 걸쳐 수평적 확장을 통해 복원력을 달성할 수 있도록 앱을 구축하고 운영해야 한다. 이는 배포 환경의 모든 호스트에 대한 간단한 업데이트를 가능하게 하여 보안 취약성을 시기적절하게 해결하는 데 가장 일반적인 장벽 중 하나를 제거하기 때문에 호스트 OS 업데이트 적용에 중요하다.

2) 컨테이너 런타임 보안 위협과 고려사항

i) 안전하지 않은 컨테이너 런타임 설정(Configuration)

컨테이너 런타임은 복잡한 소프트웨어이며 일반적으로 구성이 가능한 많은 옵션을 관리자에게 노출시킨다. 종종 잘못 구성하면 시스템의 상대적 보안이

저하될 수 있다. 예를 들어 Linux 컨테이너 호스트에서는 허용된 시스템 콜(system call) 목록이 컨테이너의 안전한 작동에 필요한 시스템 콜으로만 기본적으로 제한되는 경우가 많다. 이 목록이 넓어지면 런타임과 호스트가 손상된 컨테이너로 인한 위험 증가에 노출될 수 있다.

안전하지 않은 런타임 구성의 또 다른 예는 컨테이너가 호스트에 중요한 디렉토리를 마운트하도록 허용하는 것이다. 컨테이너는 호스트 파일 시스템을 거의 변경하지 않아야 하며 호스트 OS의 기본 기능을 제어하는 /boot 또는 /etc와 같은 위치를 변경하지 않아야 한다. 컨테이너가 이러한 경로를 변경할 수 있는 경우 손상된 컨테이너를 사용하여 권한을 높이고 호스트 자체와 다른 호스트를 공격할 수 있다.

대응기술로 컨테이너 런타임 구성의 표준 준수를 자동화해야 한다. Center for Internet Security Docker Benchmark와 같은 문서화된 기술 구현 지침에서는 옵션 및 권장 설정에 대한 세부 정보를 제공하지만, 이 지침의 운영은 자동화에 따라 달라진다. 다양한 도구를 사용하여, 한 시점에서 규정 준수를 '검색'하고 평가할 수 있지만, 이러한 접근방식은 확장하기 어렵다. 대신 시스템 전반에 걸쳐 구성 설정을 지속적으로 평가하고 적극적으로 시행하는 도구나 프로세스를 사용해야 한다.

또한 SELinux[3] 및 AppArmor[4]와 같은 필수 접근제어 기술은 컨테이너에 대한 향상된 제어 및 격리를 제공할 수 있다. 예를 들어, 이러한 기술은 추가 세분화를 제공하고 컨테이너가 특정 파일 경로, 프로세스 및 네트워크 소켓에만 액세스할 수 있어야 한다는 보장을 제공하여 손상된 컨테이너가 호스트나 다른 컨테이너에 영향을 미치는 기능을 더욱 제한할 수 있다.

---

3) SELinux(Security Enhanced Linux): 소스코드가 공개되어 있기 때문에 보안이 취약한 리눅스 시스템 액세스 권한을 제어하기 위해 미국 국가안보국(NAS)에서 개발한 보안 아키텍쳐

4) AppArmor: 시스템 관리자가 프로그램 프로필 별로 프로그램의 역량을 제한할 수 있게 해주는 리눅스 커널 보안 모듈

ii) 커널 공유

컨테이너는 강력한 소프트웨어 수준의 리소스 분리를 제공하지만 커널 공유를 사용하면 하이퍼바이저에서 환경보다 객체 간 공격 표면이 커진다. 즉, 컨테이너 런타임에 의해 제공되는 격리 수준은 하이퍼바이저가 제공하는 격리 수준만큼 높지 않다.

대응 기술은 다음과 같다. 대부분의 컨테이너 런타임 환경은 컨테이너를 서로 분리하거나 호스트 OS로부터 분리하는 효과적인 작업을 수행하지만, 경우에 따라서는 동일한 런타임에 서로 다른 수준의 앱을 함께 실행하는 것은 불필요한 위험이 될 수 있다. 용도와 민감도에 따라 컨테이너를 세분화하면 심층 방어가 추가로 필요하다. 컨테이너를 상대적인 민감도로 그룹화하고 주어진 호스트 커널이 단일 민감도 수준의 컨테이너만 실행하도록 하는 것이다. 이러한 세분화는 여러 물리적 서버를 사용하여 제공될 수 있지만 최근 하이퍼바이저에서는 이러한 위험을 효과적으로 완화할 수 있을 만큼 강력한 격리 기능을 제공한다.

iii) 컨테이너 손상

기존 호스트 기반 침입 탐지 프로세스 및 도구는 아키텍처 및 운영 방식이 다르기 때문에 컨테이너 내의 공격을 탐지하고 방지할 수 없는 경우가 많다. 따라서, 컨테이너를 자동으로 인식하고 컨테이너에서 일반적으로 볼 수 있는 규모와 변화율로 작동하도록 설계된 추가 도구를 구현해야 한다. 이러한 도구는 컨테이너형 앱을 자동으로 프로파일링하고 보호 프로파일을 구축하여 관리자와의 상호작용을 최소화할 수 있어야 한다. 또한, 이러한 프로파일은 런타임에 다음과 같은 이벤트를 포함하여 이상 징후를 탐지할 수 있어야 한다.

- 올바르지 않거나 예기치 않은 프로세스 실행
- 올바르지 않거나 예기치 않은 시스템 콜 호출
- 보호된 구성 파일 및 이진 파일의 변경
- 예기치 않은 위치 및 파일 형식에 쓰기
- 예기치 않은 네트워크 리스너를 만듭니다
- 예기치 않은 네트워크 목적지로 전송된 트래픽

- 악성 프로그램 스토리지 또는 실행

3) 컨테이너 이미지 보안 위협과 고려사항

ⅰ) 이미지 취약점

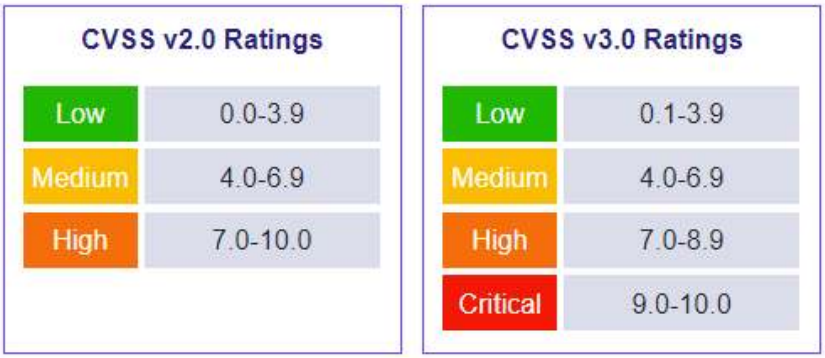
이미지는 특정 응용 프로그램을 실행하는 데 사용되는 모든 컴포넌트를 포함하는 정적 아카이브 파일이기 때문에 이 이미지 내의 컴포넌트가 오래되어 중요한 보안 업데이트가 누락되는 경우가 많다. 예를 들어 이미지를 완전히 최신 컴포넌트로 생성한 경우 해당 이미지는 생성된 후 며칠 또는 몇 주 동안 계속 취약점이 없을 수 있다. 그러나 추후 어느 시점에서 해당 이미지에 포함된 컴포넌트에는 취약성이 발견될 가능성이 높기 때문에 전체 이미지가 더 이상 최신 상태가 되지 않는다. 배포된 소프트웨어가 실행되는 시스템에서 '현장'으로 업데이트되는 기존의 운영 패턴과는 달리 컨테이너를 사용하여 이러한 업데이트는 이미지 자체의 업스트림에서 수행되어야 하며, 그런 다음 다시 배포된다. 따라서 컨테이너 환경에서 일반적인 위험은 실행 중인 이미지의 버전에 필요한 모든 업데이트가 포함되어 있지 않기 때문에 취약점이 있는 이미지를 배포하는 것이다.

대응 기술로 컨테이너용 취약점 관리 도구와 프로세스가 필요하다. 기존의 취약성 관리 도구는 컨테이너형 모델과 근본적으로 일치하지 않는 호스트 내구성, 앱 업데이트 메커니즘 및 업데이트 빈도에 대해 많은 가정이 필요하다. 이러한 도구는 종종 컨테이너 내의 취약성을 탐지하지 못한다. 파이프라인 기반 빌드 접근방식과 컨테이너 및 이미지의 불변성을 설계에 반영하여 보다 실행 가능하고 안정적인 결과를 제공하는 도구를 사용해야 한다. 효과적인 도구 및 프로세스의 주요 측면은 다음과 같다.

- 빌드 프로세스의 시작부터 사용 중인 레지스트리에 이르기까지 이미지 및 컨테이너의 전체 라이프사이클과 통합된다.
- 이미지의 베이스 레이어뿐만 아니라 사용 중인 애플리케이션 프레임워크 및 사용자 지정 소프트웨어 등 이미지의 모든 레이어에서 취약성을 파악할 수 있다.
- 정책 기반 시행으로 구축 및 배포 프로세스의 각 단계에서 '품질 게이트'를

만들어 정책을 충족한 이미지만 사용할 수 있도록 해야 한다. 예를 들어 조직은 [그림 부록2-24]의 CVSS(Common Vulnerability Scoring System) 등급이 선택된 임계값보다 높은 취약점이 포함된 이미지의 사용을 방지하기 위해 빌드 프로세스에서 규칙을 구성할 수 있어야 한다.

[그림 부록2-24] NVD CVSS 등급



자료: NVD

ii) 이미지 구성

소프트웨어 결함 외에도 이미지에도 구성 결함이 있을 수 있다. 예를 들어 루트로 실행되도록 이미지를 구성하거나 과도한 권한으로 실행하도록 설정된 실행 파일을 포함할 수 있다. 기존 서버 또는 VM과 마찬가지로, 구성이 잘못되면 공격에 노출될 수 있으며, 구성이 잘못된 이미지에 포함된 모든 구성요소도 위험을 증가시킬 수 있다.

대응기술로 소프트웨어 취약점 외에도 보안 위험을 높이고 정책을 위반하는 방식으로 이미지를 구성할 수 있다. 예를 들어 이미지는 권한이 없는 사용자로 실행되도록 구성되어야 하며 원격 액세스를 허용하지 않아야 한다. 이러한 보안 구성 모범 사례를 검증하고 준수하기 위해 도구와 프로세스를 채택해야 한다. 이러한 도구 및 프로세스에는 다음이 내용이 포함되어야 한다.

- 공급업체 권장 사항 및 맞춤형/제3의 공급자의 모범 사례를 모두 포함한

이미지 구성 설정 검증

- 이미지 컴플라이언스 상태에 대한 중앙 집중식 보고 및 모니터링으로 조직 차원의 취약점과 위험을 파악
- 비준수 이미지의 실행을 방지하여 규정 준수 요구사항의 시행

(2) MEC 애플리케이션 관점에서의 보안 위협 및 보안 고려사항 분석

MEC 애플리케이션은 MEC 호스트의 가상화 인프라 내에서 구동되는 프로그램으로 이동통신사업자의 내부망에 위치하여 일반 사용자의 접근 및 사용이 제한되는 NFV 시스템과는 달리, 제3자 MEC 애플리케이션이 통신사업자 망내에서 실행될 수 있으므로 악성코드 등에 노출될 경우 치명적인 보안 위협을 가져올 수 있다. 따라서, MEC의 컨테이너 가상화 플랫폼 내에서 구동되는 MEC 애플리케이션으로 인한 보안위협과 고려사항을 분석한다.

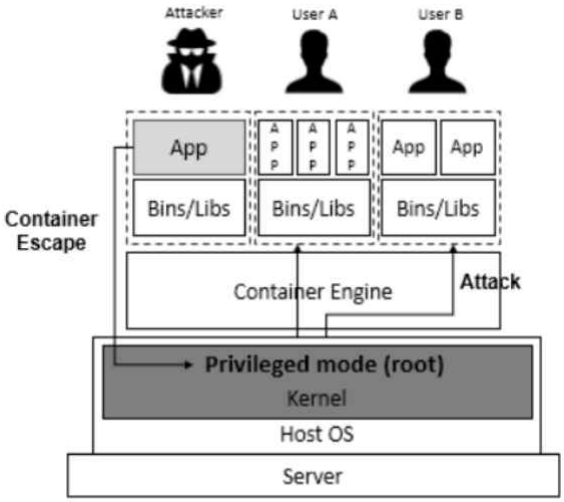
1) 런타임 소프트웨어 내의 보안 위협 및 보안 고려사항 분석

ⅰ) 소프트웨어 취약점

악성 소프트웨어가 취약점을 활용하여 다른 컨테이너 및 호스트 OS 자체를 포함한 컨테이너 외부의 리소스를 공격할 수 있는 '컨테이너 탈출' 공격 [그림 부록2-25] 시나리오가 이러한 위협에 해당된다. 공격자는 취약점을 이용하여 런타임 소프트웨어 자체를 손상시킨 다음 공격자가 컨테이너에 액세스하고 컨테이너 간 통신을 모니터링할 수 있도록 해당 소프트웨어를 변경할 수 있다.

대응 기술로 컨테이너 런타임은 취약점에 대해 주의 깊게 모니터링해야 하며 문제가 감지되면 신속하게 대처해야 한다. 취약한 런타임은 호스트 자체뿐만 아니라 모든 컨테이너를 잠재적으로 심각한 위험에 노출시킨다. 따라서, 도구를 사용하여 배포된 런타임에서 CVE(Common Vulnerabilities and Exposure) 취약점을 찾고, 취약한 인스턴스를 업데이트해야 한다.

[그림 부록2-25] 컨테이너 탈출 공격



자료: 최상훈, 박기웅, 메모리 트랩기법을 활용한 컨테이너 취약점 침입 탐지 프레임워크

ii) 멀웨어(Malware)

도구를 사용하여 유휴 상태 및 컨테이너에서 실행되는 동안의 이미지의 멀웨어를 모니터링해야 한다. 이러한 프로세스에는 다음이 포함되어야 한다.

- 레지스트리와 호스트 모두에서 이미지 내에서 악성 프로그램 식별
- 악성코드 시그니처 탐지
- 런타임 시 컨테이너에 침입한 악성 프로그램 탐지(예: 컨테이너가 전복되고 공격자가 해당 컨테이너에 루트킷을 다운로드하는 경우)

iii) 컨테이너 런타임 공격 시나리오

컨테이너 런타임에 문제가 발생할 경우 공격자는 이 액세스 권한을 사용하여 호스트의 모든 컨테이너를 공격하고 호스트 자체를 공격할 수 있다.

이 위협 시나리오에 대한 관련 완화 조치에는 다음이 포함된다.

- 필수 액세스 제어 기능의 사용은 프로세스 및 파일 시스템 활동이 정의된 영역 내에서 분할되도록 하는 추가적인 경계를 제공할 수 있다.

- 워크로드를 세분화하면 손상 범위가 호스트를 공유하는 공통 분류 수준의 애플리케이션으로 제한된다.
- 런타임의 보안 상태를 보고하고 취약한 사용자에게 이미지를 배포하지 못하도록 하는 보안 도구를 사용하면 워크로드 실행을 방지할 수 있다.

(3) MEC 오케스트레이터 및 네트워크 관점 보안 위협

1) 컨테이너의 언바운드 네트워크 액세스

기본적으로 대부분의 컨테이너 런타임에서는 개별 컨테이너가 네트워크를 통해 컨테이너간 및 호스트에 액세스할 수 있다. 컨테이너가 손상되어 악의적으로 작동하는 경우 이러한 네트워크 트래픽을 허용하면 가상화 환경의 다른 리소스가 위험에 노출될 수 있다. 예를 들어 손상된 컨테이너는 공격자가 악용할 수 있는 다른 취약점을 찾기 위해 연결된 네트워크를 스캔하는 데 사용될 수 있다. 송신 네트워크 액세스는 컨테이너 간 연결의 많은 부분이 가상화되기 때문에 컨테이너 환경에서 관리하기가 더 복잡하다. 따라서 한 컨테이너에서 다른 컨테이너로의 트래픽은 최종 소스, 목적지 또는 페이로드를 분석하지 않고 단순히 캡슐화된 패킷으로 나타날 수 있다. 컨테이너를 인식하지 못하는 도구 및 운영 프로세스는 이 트래픽을 검사하거나 위협을 나타내는지 여부를 확인할 수 없다.

대응 기술로 컨테이너가 보내는 송신 네트워크 트래픽을 제어해야 한다. 최소한 이러한 통제는 네트워크 경계에 배치되어야 하며, 컨테이너가 기존의 아키텍처에 사용되는 패턴과 유사하게 보안 데이터를 호스팅하는 환경에서 인터넷까지와 같이 서로 다른 감도 수준의 네트워크를 통해 트래픽을 전송할 수 없도록 해야 한다. 그러나 컨테이너 간 트래픽의 가상화된 네트워킹 모델은 추가적인 과제를 제기한다. 여러 호스트에 배포된 컨테이너는 일반적으로 암호화된 가상 네트워크를 통해 통신하기 때문에 기존의 네트워크 장치는 종종 이 트래픽을 인식하지 못한다. 또한 일반적으로 컨테이너에는 오케스트레이터가 배포할 때 동적 IP 주소가 자동으로 할당되며, 이러한 주소는 앱의 확장 및 로드 밸런싱에 따라 지속적으로 변경된다. 따라서 기존 네트워크 수준 장치와 더 많은 애플리케이션 인식 네트워크 필터링을 함께 사용하는 것이 이상적이다. 앱 인식 도구는 컨테이너 간 트래픽을 볼 수 있을

뿐만 아니라 컨테이너에서 실행되는 앱의 특정 특성을 기반으로 이 트래픽을 필터링하는 데 사용되는 규칙을 동적으로 생성할 수 있어야 한다. 이러한 동적 규칙 관리는 컨테이너형 앱의 규모와 변경 속도뿐만 아니라 사용 후 삭제되는 네트워킹 토폴로지로 인해 매우 중요하다. 특히, 앱 인식 툴은 다음과 같은 기능을 제공해야 한다.

- 언바운드 포트 및 프로세스 포트 바인딩을 모두 포함하여 적절한 컨테이너 네트워킹을 자동으로 결정한다.

- 컨테이너와 다른 네트워크 엔티티 간의 트래픽 흐름, 즉 'on the wire' 트래픽과 캡슐화된 트래픽을 모두 탐지하고, 예기치 않은 트래픽 흐름, 포트 검색 또는 잠재적으로 위험한 대상에 대한 아웃바운드 액세스와 같은 네트워크 이상 징후를 탐지한다.

2) 언바운드 관리자 액세스

많은 오케스트레이션 도구는 사용자와 상호 작용하는 모든 사용자가 관리자이며 이러한 관리자는 환경 전반에 걸친 통제권을 가져야 한다고 가정했다. 그러나 많은 경우 오케스트레이터 한 명이 각기 다른 팀에 의해 관리되고 민감도 수준이 다른 여러 가지 앱을 실행할 수 있다. 사용자 및 그룹에 제공된 액세스 범위가 특정 요구 사항에 맞지 않으면 악의적이거나 부주의한 사용자가 오케스트레이터가 관리하는 다른 컨테이너의 작업에 영향을 미치거나 전복될 수 있다.

대응 기술은 다음과 같다. 오케스트레이터는 광범위한 제어 범위 때문에 사용자에게 특정 호스트, 컨테이너 및 이미지에서 특정 작업을 수행할 수 있는 권한만 부여되는 최소 권한 액세스 모델을 사용해야 한다. 예를 들어, 특정 팀의 구성원은 사용된 이미지와 해당 이미지를 실행하는 데 사용된 호스트에 대한 액세스 권한만 부여되어야 하며 자신이 만든 컨테이너만 조작할 수 있어야 한다.

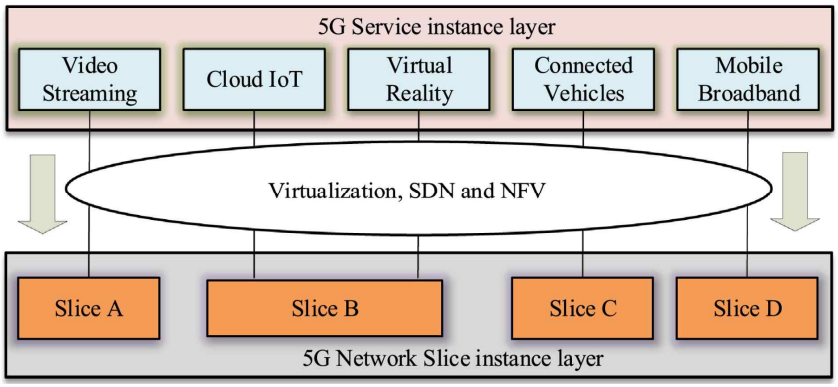
3. 네트워크 슬라이싱 보안 고려사항 연구

5G 네트워크 슬라이싱은 NGMN에 의해 만들어지고 처음 도입되었다. [그림 부록2-26]

은 다음 세 계층으로 구성된 슬라이스 기능을 나타낸다.

- 5GSIL(5G Service Instance Layer): 지원해야 하는 다양한 서비스를 나타낸다. 서비스 인스턴스는 각 서비스를 나타내며 일반적으로 서비스는 네트워크 사업자 또는 제3자가 제공할 수 있다.
- 5GNSI(5G Network Slice Instance): 5GSI에서 요구하는 네트워크 특성을 제공한다. 5GNSI는 네트워크 사업자가 제공하는 여러 5GSI에서 공유될 수도 있다. 5GNSI는 다른 NSI가 공유할 수 있는 하나 이상의 하위 네트워크 인스턴스로 구성되지 않을 수 있다.
- 5GRL(5G Resource Layer): 물리적 리소스(무선 액세스를 포함한 컴퓨트, 스토리지 또는 전송을 위한 자산) 및 논리적 리소스(NF(Network Function) 전용 또는 공유되는 여러 물리적 리소스의 그룹화 또는 물리적 리소스의 분할)로 구성).

[그림 부록2-26] NGMN 네트워크 슬라이싱 개념



자료: Barakabitze, Alcardo Alex, et al. (2020). "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges." Computer Networks 167 (2020)

네트워크 슬라이싱은 5GRL의 기능에 해당되는 SDN(Software Defined Network) 및 NFV(Network Function Virtualization)와 함께 가상화 네트워킹 패러다임 범주에 속한다. 이를 통해 공유 네트워크 인프라 위에 종단 간 논리 네트워크를 유연하고 효율적으로 생성할 수 있다. 이런 방식으로 하나의 네트워크를 논리적으로 여러 개의 네트워크로

분리해, 각 용도에 맞추어 활용할 수 있다. 본 장에서는 네트워크 슬라이싱의 보안 고려사항을 분석하기 위해 네트워크 슬라이싱의 핵심 기술과 관련된 보안 위협을 분석하고 슬라이스의 보안 위협을 분석한다.

(1) 네트워크 슬라이싱 핵심 기술의 보안 위협 및 고려사항 분석

네트워크 슬라이싱 서비스는 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 서버상에 네트워크 통신 기능을 가상화 형태로 구현한다. NFV가 다양한 산업 표준 하드웨어에서 네트워크 기능의 소프트웨어 인스턴스를 통합하여 레거시 네트워크의 변환을 제공하는 반면, SDN은 자동화된 트래픽 경로 선택 및 관리를 허용하는 프로그래밍 가능한 네트워크를 가능하게 하는 역할을 한다. <표 부록2-6>는 SDN과 NFV의 관계 및 비교를 나타낸 것이다.

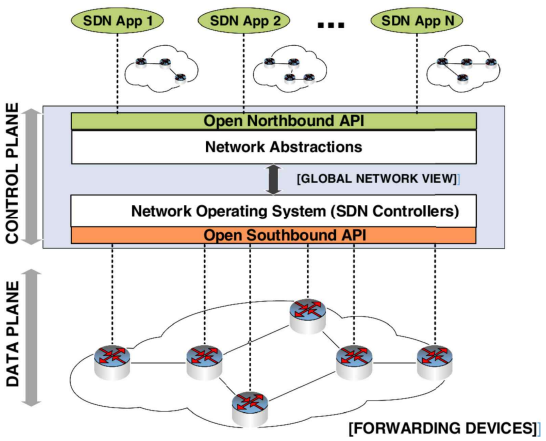
<표 부록2-6> SDN과 NFV 관계 및 비교

	NFV	SDN
네트워크 제어	NF 제어 및 동적 프로비저닝	중앙 집중식 네트워크 제어 제공
설계	서비스 또는 NF 추상화	네트워킹 추상화
주요 이점	네트워크에 필요한 유연성 제공	개방형 제어 인터페이스로 프로그래밍 가능한 네트워크 제공
비용 효율성	하드웨어를 소프트웨어로 교체	운영 효율성 및 에너지 소비 감소
표준 프로토콜	다중 제어 프로토콜 지원	OpenFlow는 디펙터 표준 프로토콜
표준화	ETSI	ONF

1) SDN 보안 위협 및 대응기술

SDN은 보다 세분화되고 네트워크 전반에 걸친 방식으로 애플리케이션/서비스를 오케스트레이션 및 제어할 수 있는 지능과 유연한 프로그래밍 가능한 5G 네트워크를 제공하는 접근방식이다. Open Network Foundation(ONF)은 SDN을 "네트워크 컨트롤 플레인(Control Plane)이 포워딩 플레인(Fowarding Plane)과 물리적으로 분리되어 있고 컨트롤 플레인이 여러 장치를 제어하는 것"으로 정의한다. 이러한 분리로 인해 전체 네트워크에 대한 글로벌 뷰를 통해 유연성과 중앙 집중식 제어가 가능해진다. 또한 유동적인 네트워크 조건, 비즈니스, 시장 및 최종 사용자 요구사항에 신속하게 대응할 수 있는 기능을 제공한다. SDN은 서비스 프로비저닝과 네트워크 관리 간의 격차를 해소하는 네트워크 기능 간에 지능적인 관리 결정을 시행할 수 있는 가상화된 컨트롤 플레인을 생성한다. SDN을 사용하면 OpFlex, ForRCES 및 OpenFlow와 같은 표준화된 SBI(Southbound Interface)를 사용하여 네트워크 제어를 직접 프로그래밍할 수 있다. 이러한 표준은 데이터 플레인(Data Plane)의 전달 장치와 컨트롤 플레인 요소 간의 통신을 정의한다.

[그림 부록2-27] SDN 참조 아키텍쳐



자료: Bonfim, Michel, et al. (2020). "A real-time attack defense framework for 5G network slicing." Software: Practice and Experience 50.7.

SDN 패러다임의 주요 특징은 제어 플레인과 데이터 플레인의 분리이다. 개방형 API의 가용성과 함께 제어 플레인의 중앙 집중화를 통해 네트워크 프로그래밍으로 새로운 네트워크 애플리케이션을 만들고 배포하는 프로세스를 더 쉽게 만드는 이점이 있다. SDN은 네트워크 정책 시행의 단순화와 유연성을 제공하여 네트워크 구성 및 관리를 용이하게 한다. SDN 컨트롤러라는 소프트웨어로 대표되는 컨트롤 플레인은 네트워크 트래픽을 처리 방식을 결정하는 역할을 담당한다. SDN 컨트롤러는 네트워크 장비와 분리된 기성품 플랫폼에서 실행할 수 있다. 네트워크 장치로 표시되는 데이터 플레인은 일련의 규칙에 따라 트래픽을 전달하는 역할을 수행한다. 이러한 규칙은 SDN 컨트롤러에 의해 생성 및 관리된다. SDN 컨트롤러는 네트워크 토폴로지에 대한 글로벌 뷰를 갖고 있으며 OpenFlow와 같은 사우스바운드(Southbound) 프로토콜을 통해 데이터 플레인 요소를 직접 제어한다.

[그림 부록2-27] 은 SDN 아키텍처의 주어진 세 계층과 이들 간의 상호 작용을 담당하는 API를 보여준다. SDN 노스바운스(Northbound) API는 애플리케이션 계층과 컨트롤 플레인 계층 간의 통신 지원을 제공한다. 여기에는 트래픽 엔지니어링(Traffic Engineering, TE), 라우팅, 방화벽, QoS 등과 같은 SDN 애플리케이션에 대한 지원도 포함된다. 사우스바운드 API는 SDN 컨트롤러와 스위치 간의 통신을 담당한다. SDN 아키텍쳐로 인한 전주기적(탐지-예방-대응) 보안 프로세스에서 활용될 수 있는 구조적 이점은 다음과 같다.

- 탐지: 네트워크의 보안 서비스(예: 이상 탐지 및 침입 탐지)는 기본 트래픽 흐름이 중앙 집중식 컨트롤러로 전송될 수 있도록 경고를 트리거하고 분석하여 관리자에게 피드백을 제공할 수 있다.
- 예방: 관리자는 컨트롤러의 노스바운드 API를 사용하여 네트워크 전반에 걸쳐 보안 정책을 생성하거나 업데이트하여 공격자 또는 악성 코드를 차단할 수 있다.
- 대응: SDN의 프로그래밍 가능성 및 유연성과 전체 네트워크 뷰를 기반으로 보안 위협에 대한 빠른 제어 및 방어를 제공할 수 있다. 트래픽 격리, 포트 차단, 패킷 삭제, 속도 제한(예: 컨트롤 플레인에 대한 DoS 공격) 및 더 짧은 대응 조치를 효율적으로 배포할 수 있다.

i) SDN 아키텍쳐 보안 위협

SDN 아키텍처의 컨트롤 및 데이터 플레인의 분리는 잠재적으로 네트워크 모니터링 및 보안 정책 시행을 단순화할 수 있지만 이러한 새로운 아키텍처 자체는 기존 네트워크 배포에 없는 새로운 보안 위협과 공격 표면을 도입한다. 다음은 SDN 아키텍쳐에서 발생할 수 있는 보안 문제를 설명한다.

- 무단 액세스: 공격자는 취약하거나 존재하지 않는 액세스 제어 메커니즘을 이용하여 SDN 요소에 액세스 권한을 부여하고 로깅 세션을 노출하는 관리 터미널 및 REST API에 대해 무차별 대입 공격을 수행한다. 네트워크 구성 요소의 취약점을 악용한 악성 디바이스를 설치하거나 네트워크에 원격 연결을 바인딩한다.
- 데이터 유출: 공격자는 민감한 네트워크 정보를 빼기 위해 여러 공격 표면을 사용할 수 있다. 예를 들어 공격자는 타겟 네트워크에 패킷을 브로드캐스트하여 네트워크 동작을 추측할 수 있다. 취약한 네트워크 응용 프로그램을 성공적으로 손상시킨 공격자는 네트워크 정책 데이터베이스 및 기타 내부 네트워크 데이터 스토리지에 액세스할 수 있다. 패킷 스니핑 및 도청을 위해 안전하지 않은 채널을 점유할 수 있다. 마지막으로 디바이스 사칭 공격을 통해 공격자는 원래 손상된 네트워크 요소로 원하는 정보를 획득할 수 있다.
- 데이터 변조: 공격자는 흐름 규칙을 충돌시키는 악성 애플리케이션을 통해 취약한 프로토콜과 API, 검증 및 인증 메커니즘의 부재를 활용할 수 있다. 게다가 내부 스토리지에 대한 무단 액세스는 공격자가 네트워크 정책을 도입하거나 기존 정책을 수정할 가능성을 제공한다. 반면에 네트워크 토폴로지의 변경은 장치 가장 및 위조 패킷 주입 공격과 함께 잘못된 프로토콜 구성을 활용하여 유도될 수 있다.
- 네트워크 정보의 파괴: 스위치의 흐름 규칙 플러싱, 다른 애플리케이션이나 서비스 체인을 위한 제어 패킷을 버리는 악성 애플리케이션, 그리고 관리 스테이션 또는 내부 네트워크 데이터베이스에 대한 승인 되지 않은

액세스로 인한 네트워크 정책 제거가 포함된다.

- 서비스 거부(DoS): 서비스 중단의 세 가지 주요 원인인 플러딩 공격, 연결 끊김 또는 타겟 장치의 종료를 자주 일으키는 잘못된 형식의 패킷 주입 공격 그리고 컨트롤러 네트워크 뷰를 속이는 토폴로지 중독 공격이다.
- 구성 문제: 프로토콜, 인터페이스, API 및 시스템의 잘못된 구성은 새로운 취약성과 보안 위반을 의미한다. 또한, 충돌하는 네트워크 정책 및 흐름 규칙으로 보안 위협이 발생한다.

ii) SDN 아키텍처에 대한 공격

모든 계층과 인터페이스는 계층 내에 있는 네트워크 구성 요소를 손상시키거나 다른 계층의 요소를 손상시킬 수 있는 특정 공격에 민감하다. 다음은 SDN 아키텍처의 모든 계층을 나열하고 각 계층에서 식별된 가장 일반적인 공격을 설명한다.

① 애플리케이션 계층

- 서비스 무력화: 성공적으로 설치된 악성 애플리케이션은 제어 패킷 핸들러를 조작하는 데 사용될 수 있으며, 제어 패킷이 의도한 애플리케이션에 도달하지 못하도록 제어 패킷을 폐기함으로써 서비스 중단을 실행할 수 있다. 제어 패킷 포워딩을 방해하기 위해 서비스 체인을 방해한다. 제어 패킷을 분석하여 민감한 네트워크 정보를 스니핑하고 그에 따라 특정 비정상적인 작업을 실행한다.
- 취약한 노스바운드 API에 대한 공격: 노스바운드 API의 잘못된 구성 및 취약성을 활용하여 시스템 명령을 실행하여 피해자 애플리케이션을 종료하거나 컨트롤러와 대상 애플리케이션 간에 교환되는 정보를 노출할 수 있다.

② 컨트롤 계층

- 동적 흐름 규칙 터널링: 공격자는 중첩 및 충돌하는 흐름 규칙을 지시할

수 있는 악성 응용 프로그램을 실행하는 경우 방화벽과 같은(차단, 삭제) 흐름 규칙을 우회할 수 있다.

- 네트워크 운영체제 손상: 손상된 애플리케이션 및 불량 데이터 플레인 장치는 컨트롤러 취약성과 잘못된 구성을 악용하여 컨트롤러를 강제 종료하는 시스템 명령 실행과 같은 다양한 목표를 달성할 수 있다. 1) 내부 네트워크 데이터 스토리지의 모든 인스턴스에 있는 민감한 정보의 누출, 2) 합법적인 장치를 위한 정보 리디렉션 네트워크 정책 데이터베이스 하이재킹, 3) 컨트롤러에 대한 무단 액세스 채널을 유지하기 위한 루트킷 또는 원격 액세스 연결 설치
- 패킷 인 플러딩(Packet-in flooding): 단일 또는 분산된 형태의 손상된 호스트 또는/및 스위치를 통해 공격자는 네트워크 인프라 수신자가 컨트롤러에 대한 패킷 인 메시지로 변환하는 대규모 네트워크 패킷을 브로드캐스트한다. 컨트롤러는 사우스바운드 인터페이스를 통해 들어오는 방대한 양의 패킷에 응답하여 모든 연산 리소스를 낭비할 수 있다.
- 컨트롤러의 스위치 테이블 플러딩(switch table flooding): 컨트롤러의 OpenFlow 제어 패킷 수신에서 들어오는 패킷의 발신자의 신원 확인 및 인증을 위한 메커니즘이 없기 때문에 다양한 공격 표면이 발생할 수 있다. 스위치 테이블 플러딩은 위조된 “응답“ 메시지의 지속적인 수신에 대한 응답이 제어되지 않은 결과이다. 이 상황에서 공격자는 타겟 컨트롤러의 스위치 테이블에 가짜 스위치에 대한 정보가 있는 항목을 저장할 수 있다. 이 공격을 계속 실행하면 해당 스위치 테이블의 지속적인 플딩으로 인해 컨트롤러 성능이 저하된다.

③ 제어 채널

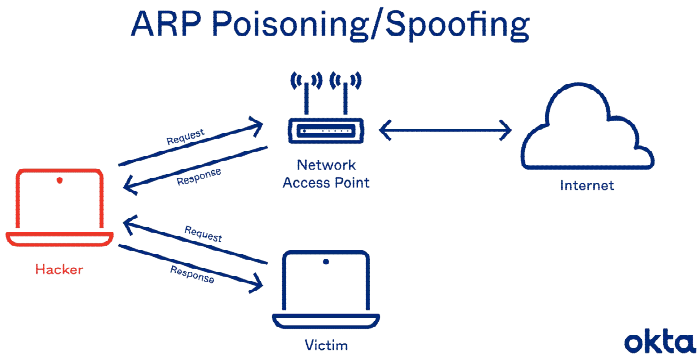
- 도청: 공격자는 암호화되지 않은 제어 채널을 활용하여 패킷 스니핑 공격을 수행할 수 있으며, 공격자는 제어 채널에서 교환되는 네트워크의 모든 제어, 토폴로지 및 관리 정보를 들을 수 있다.
- 중간자: ARP 포이즈닝 공격과 함께 암호화되지 않은 제어 채널을 활용하여 제어 채널 중간에 침입자 호스트를 삽입하여 컨트롤러와 타겟 데이터

플레인 장치 간의 통신에 침투할 수 있다.

④ 인프라 계층

- ARP 포이즈닝 공격을 이용한 서비스 거부: 공격자는 컨트롤러를 가장하여 대상 스위치 격리를 수행할 수 있다. ARP 포이즈닝 공격을 사용하여 공격자는 컨트롤러의 ID를 가로채고 대상 스위치가 정상 컨트롤러에 대한 연결을 끊고 대신 가짜 컨트롤러에 연결하도록 한다. 그 결과 네트워크에 대한 스위치 연결이 끊어진다.
- 흐름 규칙 수정/플러시: 공격자는 기존 흐름 규칙을 덮어쓰거나 플러시하여 스위치의 흐름 테이블에 설치된 정보를 조작할 수 있다. 공격자는 손상된 애플리케이션이나 손상된 네트워크 컨트롤러에서 이 공격을 시작할 수 있다.
- 부채널 공격: 정찰 공격이라고도 하는 공격은 일반적으로 특정 네트워크 상황에 대한 특정 대상 장치의 결과 반응을 활용하여 공격자가 나중에 다른 종류의 공격을 시작하는 데 사용할 수 있는 특정 암시적 정보를 유추한다. 예를 들어, 공격자는 특정 패킷이 특정 스위치로 전송되었을 때 실험한 RTT(Round-Trip Time)를 기록할 수 있으며, 이러한 정보는 나중에 해당 스위치에 대한 플로우 테이블 플러딩 공격을 시작하는 데 활용될 수 있다.

[그림 부록2-28] ARP 포이즈닝/스푸핑 공격



그림출처: okta

iii) SDN 보안 대응 방안

SDN 아키텍처를 대상으로 하는 공격 벡터 및 위협 표면에 대한 대응 솔루션과 관련 연구를 살펴본다.

- 위협 탐지

안정적인 트래픽 검사 및 공격 탐지를 위한 보안 응용 프로그램의 개발은 인프라 장치에서 흐름 기능을 요청한 다음 수집된 정보에서 네트워크 상태, 트래픽 패턴 및 기타 특성을 유추하는 SDN 컨트롤 플레인의 기능을 활용하여 달성할 수 있다. 특수 보안 응용 프로그램의 소프트웨어 루틴은 컨트롤 플레인에서 요청한 네트워크 정보를 추출 및 분석하여 비정상적인 동작을 감지하도록 설계되었다. 소프트웨어 프로그래밍 가능성과 네트워크 유연성은 SDN 네트워크에서 고정 미들박스 기기를 교체하는 데 도움이 된다. 소프트웨어 기반 솔루션과 머신러닝 접근방식을 관리하여 효과적인 보안 체계를 제공할 수 있다.

- 공격 대응 및 완화

기존 네트워크에서 일반적으로 관찰되는 대부분의 보안 위협은 SDN 시나리오에서 재현될 수 있으므로 네트워크 프로그래밍 및 중앙 집중식 흐름 관리와 같은 SDN 아키텍처의 구성적 특성을 적용하는 위협 완화 전략을

구축해야 한다. 컨트롤러는 네트워크 상태에 관한 모든 정보를 사용할 수 있으므로 제어 응용 프로그램의 형태로 다양한 솔루션이 고안될 수 있으며, 비정상적인 동작에 대한 응답으로 응용 프로그램은 상황을 완화해야 하는 관련 흐름 항목을 발행하도록 컨트롤러에 지시할 수 있다. 예를 들어, 강력한 SDN 공격 완화 애플리케이션은 보안 정책 세트에 설명된 특정 고유 기능에 따라 비정상적인 네트워크 동작의 특정 특성을 구별할 수 있는 탐지 엔진과 직접 적용하는 리액터 모듈로 구성될 수 있다.

- ID 및 액세스 관리

SDN에서 매우 민감한 정보는 제어 채널을 통해 전달되기 때문에 많은 공격이 네트워크를 손상시키기에 충분한 정보를 얻기 위해 해당 인터페이스를 도청하는 데 중점을 둔다. 통신 채널에 강력한 암호화 메커니즘을 적용하면 공격자가 암호화된 데이터를 계속 유출할 수 있지만 일반 텍스트로 된 실제 데이터를 얻지 못할 수 있으므로 보안이 향상된다. 그러나 영리한 공격자는 손상된 네트워크 요소를 사용하여 네트워크에 침투할 수 있는 전문 지식을 보유하고 있을 수 있다. 이 경우 데이터 보호에는 외부 네트워크 에이전트가 데이터 교환에 참여할 수 없도록 하는 추가 보안 조치가 필요하다. 외부인이 네트워크에 침입하는 것을 방지하려면 네트워크 권한의 인증 및 권한 부여를 위한 신뢰 메커니즘이 수행되어야 한다. 이러한 방식으로 데이터가 암호화 체계를 사용하여 보호될 뿐만 아니라 네트워크에 대한 무단 액세스도 방지된다.

- 네트워크 상태 모니터링 및 분석

네트워크 활동 모니터링은 광범위한 보안 구현 도입의 첫 번째 단계로 생각할 수 있다. 보안 프레임워크가 현재 네트워크 상태에 대한 지속적인 글로벌 뷰를 유지할 수 있는 경우 모니터링 단계에서 식별된 기능을 사용하여 특정 조치를 미리 수행한 경우 예기치 않은 상황에 대한 대응이 빨라질 수 있다. 다른 공격에서 자주 발견되는 한 가지 일반적인 특성은 공격이 시작될 때 발생하는 네트워크 상태와 활동의 급격한 변화이다. 모니터링 솔루션은 이러한 갑작스러운 상태 위반을 식별한 다음, 탐지 엔진에 적절한 입력을 제공하거나 공격을 완화하기 위한 적절한 대응이 포함된 보안 애플리케이션을 직접

트리거 할 수 있다.

- 보안성 평가

방대한 양의 네트워크 보안 위험과 문제는 다음과 같은 상황에서 발생할 수 있다. 잘못된 구성, 잘못된 구현, 예상치 못한 입력 또는 런타임 상황에 대한 준비되지 않았거나 결정되지 않은 반응, 잘못된 프로토콜 사양 및 디자인 등. 네트워크의 기능과 보안을 모두 보장하기 위해 테스트와 평가를 요구하는 프로덕션 네트워크를 출시하기 전에 실행해야 한다. 그러나, 많은 보안 테스트는 그렇게 엄격하지 않고 일부 공통 기능만 확인하여 숨겨진 보안 문제는 그대로 남아있다. 공격자는 이러한 확인되지 않은 문제를 남용하여 공격에 활용할 수 있다. 안전한 보안 네트워크 배치는 최소한 네트워크가 취약하지 않고 공격 벡터에 대해 적절하게 보호됨을 보장해야 한다. SDN에서 이러한 종류의 솔루션은 온디맨드 또는 주기적으로 포괄적인 취약성 평가를 수행할 수 있는 보안 애플리케이션을 통해 수행 될 수 있다.

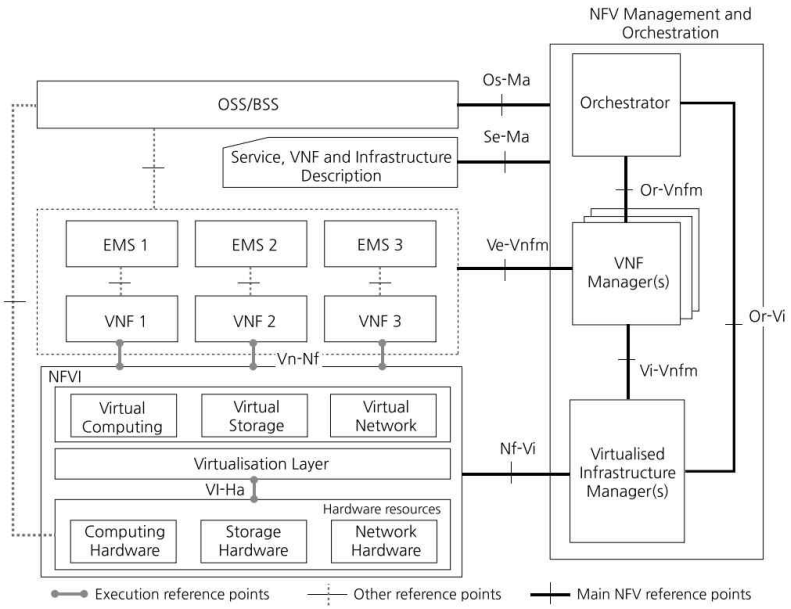
2) NFV 보안 위협 및 대응기술

NFV는 상용 하드웨어 장치 위에 네트워크 기능(예: 방화벽, TCP 옵티마이저, NAT64, VPN, DPI)을 가상화한 것이다. NFV는 상용 하드웨어에서 VNF 의 인스턴스화를 구상한다. 이러한 방식으로 기존 공급업체 제품에 존재하는 소프트웨어 및 하드웨어를 사용하는 통합 접근방식을 깨뜨린다. NFV를 사용하면 NF(Network Function)를 쉽게 배포하고 동적으로 할당할 수 있다. 또한 동적 확장을 통해 네트워크 리소스를 VNF(Virtual Network Function)에 효율적으로 할당하여 SFC(Service Function Chaining) 소프트웨어 기반 NFV 솔루션을 사용하면 일부 NF가 서비스 공급자(SP)로 이동되어 범용 서버와 같은 공유 인프라에서 실행된다. SP의 경우 NFV는 변화하는 고객 요구사항을 해결하기 위해 서비스를 확장/축소하고, 저비용의 민첩한 네트워크 인프라를 통해 자본 지출(CAPEX) 및 운영 지출(OPEX)을 줄이고, 배포를 줄일 수 있는 필요한 유연성을 제공한다. 5G 네트워크의 맥락에서 NFV는 리소스 프로비저닝 최적화를 보장한다. 높은 QoS로 최종 사용자에게 제공하고 최소 대기시간 및 실패율을 포함한 VNF 작업의 성능을 보장한다.

[그림 부록2-29]은 ETSI에서 정의한 NFV 아키텍쳐를 나타낸 것이다. NFV 아키텍

처는 기능에 따라 크게 다음과 같이 구분할 수 있다.

[그림 부록2-29] ETSI NFV 참조 구조



자료: ETSI

ⅰ) NFV Infrastructure(NFVI)

NFVI는 VNF가 배포, 관리 및 실행되는 환경을 구축하는 네트워크, 스토리지 및 컴퓨팅 리소스를 포함한 물리적 및 가상 리소스를 통합한다. 물리적 리소스는 가상화 계층(예: 하이퍼바이저)을 통해 스토리지 및 VNF에 대한 연결을 통한 처리를 제공한다. 가상화 계층 위에서 실행되는 가상 리소스는 물리적 리소스의 논리적 파티셔닝이 서로 다른 VNF에 할당되도록 하는 동시에 격리를 보장한다. 가상 리소스는 하이퍼바이저에서 관리하는 VM 이거나 컨테이너를 포함한다. NFVI는 여러 위치에 있을 수 있으므로 하나 또는 여러 운영자에 속하는 여러 NFVI-PoP를 가질 수 있다.

ⅱ) VNF and Services

VNF는 잘 정의된 기능과 외부 인터페이스 가 있는 네트워크 기능의 소프트웨어 구현이다. VNF는 동일하거나 다른 VM 또는 컨테이너에서 실행되는 여러 컴포넌트로 구성될 수 있다. 하나 이상의 VNF는 EMS(Element Management System)에 의해 관리되며 동일하거나 다른 NFVI-PoP에 배치될 수 있다.

iii) NFV Management and Orchestration(MANO)

NFV MANO는 NFVI 리소스, VNF 및 NS(Network Service) 수명 주기의 자동화된 관리를 가능하게 하는 것을 목표로 한다. NFV MANO는 다음과 같이 여러 기능 블록으로 구성된다.

iv) VIM(Virtualised Infrastructure Manager)

VIM은 일반적으로 한 운영자의 인프라 도메인 내에서 NFVI 리소스의 할당, 업그레이드, 릴리스 및 관리를 조정한다. 가상 연결, 가상 네트워크 및 포트를 생성하고 유지함으로써 VNF-FG(Virtual Network Function Forwarding Graph)의 관리를 지원한다.

v) VNF Manager(VNFM)

VNFM은 VNF의 수명 주기 관리를 담당한다. 여기에는 VNF의 인스턴스화, 확장, 업데이트 및 종료가 포함된다. 이러한 결정은 가상화된 리소스 성능 측정 및 VIM에서 수집된 오류 정보를 기반으로 수행된다. VNFM은 EMS와 상호 작용하여 구성 및 성능과 같은 일부 관리 작업을 수행한다. 하나 이상의 VNFM을 사용하여 관리 도메인에서 VNF 인스턴스를 관리할 수 있다.

vi) NFV Orchestrator(NFVO)

NFVO는 여러 VIM에서 NFVI 리소스 오케스트레이션을 담당한다. 또한 토폴로지 업데이트, 확장, 종료 및 성능 측정 수집을 포함한 NS의 수명 주기 관리를 처리한다.

① NFV 계층에 따른 위협 분석

이전에 기능에 따라 NFV 아키텍처를 구성하는 요소를 구분하였고 각 계층에서 발생할 수 있는 보안 위협을 살펴본다.

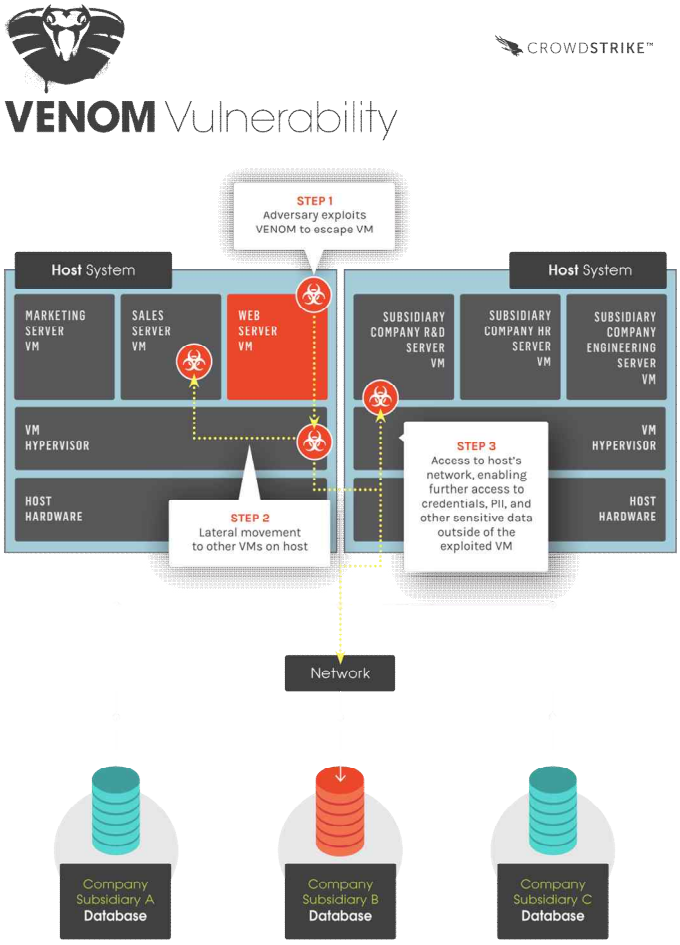
❶ NFVI 위협 분석

NFVI 보안 위협은 주로 가상화 및 통신 링크 위협 벡터와 관련이 있다.

- 권한 상승: 하이퍼바이저의 취약점을 이용한 공격이 있을 수 있다. 이러한 공격의 예로는 하이퍼재킹(hyperjacking) 또는 VM 탈출 [그림 부록2-30]가 있으며, 권한 상승 공격은 악성 VM이 하이퍼바이저의 취약성을 악용하여 루트 권한을 얻은 다음 호스트를 제어하고 이후 다른 모든 VM을 제어한다. 네트워크 종속성을 이용하는 다른 공격(예: VM 간의 통신 링크)이 추가되어 사설 가상 네트워크의 격리를 위반할 수 있다. 컨테이너 취약점은 다른 진입점을 가진다. 예를 들어, 권한 모드에서 실행되는 애플리케이션을 활성화하도록 구성된 컨테이너는 호스트 OS 및 동일한 호스트에서 실행되는 다른 컨테이너에 액세스 할 수 있는 기회를 제공한다. 컨테이너 탈출 공격을 통해 컨테이너 런타임을 탈출하고 호스트 OS를 대상으로 할 수 있다.
- 변조: 손상된 하이퍼바이저는 롤백 공격을 시작하는 데 사용할 수 있다. 또한 피해자 VM의 할당된 메모리를 조작하여 동작을 변경하거나 최악의 경우 DoS로 이어져 피해자 VM을 중지할 수 있다. 스펙터 공격(Spectre attack)은 애플리케이션이 메모리의 임의 위치를 액세스/변경하도록 속이는 변조 공격이다.
- 정보 유출: VM 호핑 공격(Hopping attack)에서 악성 VM은 사이드 및/또는 은밀한 채널을 사용하여 암호화 키와 같은 비밀 정보를 복구하거나 피해자 VM과 관련하여 불법 통신 채널을 설정한다. VM 호핑 공격의 예로는 최종 레벨 캐시 공격, 레이어 2 캐시 공격, CPU의 캐싱 시스템을 악용하여 비밀 키를 유출하는 타이밍 공격 등이 있다.
- DoS: 가상화된 환경에서 수행할 수 있는 DoS 공격의 한 종류는 호스트 기반 DoS 공격이다. 대상 호스트 내에 잘 조정된 악성 VM을 배치하여 공유 CPU, 메모리 및 대역폭 리소스 사용량을 소모하여 동일한 호스트를 공유하는 VM의 리소스 부족 상황을 초래한다. 대역폭 포화 공격(Bandwidth saturation attack)은 대역폭 초과를 이용하는 또 다른 DoS

공격이다. 이 공격으로 인해 에지 또는 집합 라우터/스위치가 병목 상태가 될 수 있다.

[그림 부록2-30] 하이퍼바이저 취약점을 통한 VM 탈출 사례



자료: Cloudstrike

❷ VNF and Services 위협 분석

VNF 수준에서는 가상화 및 소프트웨어화, 통신 링크 및 인터페이스, 상호 운용성 및 서비스 운영이라는 세 가지 범주의 위협 벡터가 악용될 수

있다. NFV가 서비스 운영, 제어 및 관리 기능을 모두 개발하고 배포하기 위해 VNF를 사용한다는 사실을 감안할 때 VNF 소프트웨어는 알려진 취약점과 제로 데이 취약점이 많기 때문에 큰 위협 벡터가 되고 있다. 다음은 VNF 소프트웨어 취약점 및 해당 공격의 몇 가지 예를 보여준다.

- 권한 상승: Cisco VNF 요소 관리자의 CVE-2017-6710 취약성은 원격으로 인증된 공격자가 호스트 시스템에서 루트 사용자로 명령을 실행할 수 있게 하여 구성 설정으로 인해 루트 사용자의 컨텍스트에서 임의 명령을 실행할 수 있게 한다.
- 변조: CVE-2016-1417은 알려진 침입 탐지 시스템인 Snort 에서 발견된 취약점으로, 원격 공격자가 원격 파일 공유를 사용한 DLL 하이재킹과 같은 임의 코드 실행 및 스푸핑 공격과 같은 변조 공격을 수행하여 정보 공개를 발생시킬 수 있다.
- 정보 유출: 다양한 네트워크 어플라이언스에서 많은 정보 유출 취약성이 발견되었다. 예를 들어, Fortinet 운영체제 버전 6.0.1, 5.6.5 이하에서 발견된 취약점 CVE-2018-13365은 공격자가 FortiGate 방화벽의 호스트 이름과 사설 IP를 발견할 수 있도록 한다.
- DoS: 여러 취약점을 악용하여 서비스 계층을 사용할 수 없게 만들 수 있다. 예를 들어, CVE-2019-15225은 원격 공격자가 매우 긴 URI로 요청을 보낼 때 과도한 메모리 소비를 유발할 수 있다. Apache HTTP 서버 취약점 CVE-2019-10097을 악용 하면 스택 버퍼 오버플로가 발생한다. 또한, 취약점 CVE-2017-1000411을 악용하여 컨트롤러 오버플로 공격을 수행할 수 있으며, 이는 DoS를 유발하는 SDN 컨트롤러의 리소스를 대량으로 고갈시킬 수 있다.

❸ MANO 위협 분석

MANO는 NFV 생태계의 핵심으로 간주되며 이 수준에서 가능한 모든 위협을 명확하게 정의하는 것은 보안을 위한 대응기술 및 접근 방식을 제안하기 위한 기본 단계이다.

고유 시스템의 탄력성을 활용하고 단일 장애 지점을 피하기 위해 NFV

MANO 기능 블록 자체를 가상화할 수 있다. 이러한 설계는 MANO 서비스를 유지하는 데 필요한 안정성을 제공하지만 MANO 블록을 가상화 위협 벡터에 노출시킨다. 다음은 NFV MANO 계층의 잠재적 위협을 설명한다.

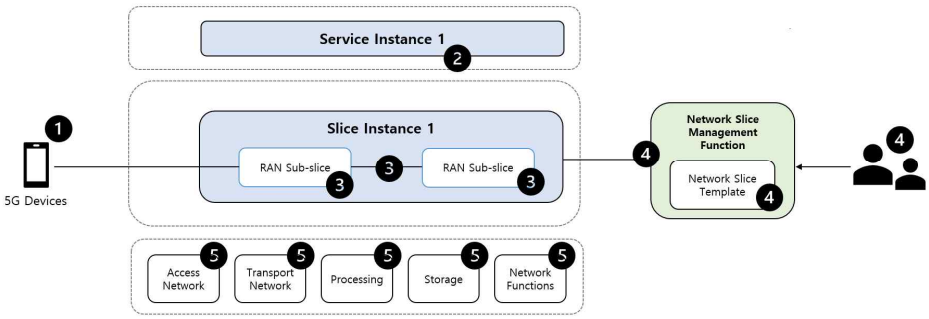
- 변조: 내부 공격자가 NFVO 기능 블록에 액세스할 수 있다고 가정하면, 공격자는 NFVO 데이터베이스 내에서 경쟁 네트워크 운영자의 정책을 변경하거나 자신의 VNF에 대한 리소스 할당량을 늘리면서 다른 테넌트의 VNF에 대한 리소스 할당량을 줄일 수 있다. 공격자는 또한 악성 네트워크 서비스 템플릿과 검증되지 않은 VNF 소프트웨어 이미지를 주입할 수 있으며, 이는 런타임 단계에서 추가로 악용될 수 있다. 공격자는 또한 네트워크 서비스 및 VNF의 수명 주기 관리를 조작할 수 있다. 또한 MANO 기능 블록 내의 통신 링크는 중간자 공격을 통해 변조될 수 있다. 공격자는 NFVO와 VIM(Or-Vi) 사이, NFVO와 VNFM(Or-Vnfm) 사이, 또는 VIM과 VNFM(Vi-Vnfm) 사이의 참조 포인트 내에서 통신을 도청하여 교환된 데이터를 변조할 수 있다.
- DoS: NFVO 블록은 제어 하에 있는 여러 VNFM/VIM과 관련하여 논리적으로 중앙 집중화된 제어 지점이므로 관리 수준의 볼륨 공격에 취약하다. 예를 들어, 경보 폭풍(alarm storm)에서 손상된 VIM(각각 VNFM)은 리소스 가용성 성능 메트릭(각각 리소스 요청)에 대한 높은 속도로 업데이트를 계속 보낼 수 있어 NFVO에서 병목 현상을 일으켜 수신된 요청에 즉시 응답하지 못할 수 있다.
- MANO 블록은 다른 공급업체에서 제공할 수 있으므로 공급업체의 구현이 ETSI 사양에서 벗어날 수 있으므로 상호 운용성 문제가 발생할 수 있다. 이것은 네트워크 수준의 보안 정책을 시행하고 상호 작용하는 MANO 구성 요소 사이의 안전한 협업을 보장하는 데 문제를 제기할 수 있다. 이는 전체 시스템의 심각한 장애를 유발하는 서비스 수명 주기 관리 및 오케스트레이션의 중단으로 나타날 수 있다.

(2) 네트워크 슬라이스 관련 보안위협 및 고려사항 분석

네트워크 슬라이싱 기술에서는 슬라이스가 논리적으로 격리되어 서로 다른 특성을 갖는 서비스에 특화된 전용 네트워크를 제공한다. 그러나, 이러한 슬라이스 간 격리가 제대로 수행되지 않으면 여러 가지 보안 위협을 발생시킬 수 있다. 본 절에서는 네트워크 슬라이스 내의 보안 위협과 네트워크 슬라이스 간 보안 위협을 분석하기 잠재적인 위협 지점을 식별하고 대응기술을 분석한다.

1) 네트워크 슬라이스 내 위협 지점 및 대응 기술

[그림 부록2-31] 슬라이스 내 위협 지점



자료: Olimid, Ruxandra F., and Gianfranco Nencioni. (2020). "5G network slicing: A security overview." *J IEEE Access 8*, (2020), pp.99999-100009.

ⅰ) 5G 고객 단말

사용자가 사용하는 고객 장치는 액세스 가능한 공격 지점이다. 즉각적인 위협에는 슬라이스 또는 서비스에 대한 무단 액세스가 포함된다. 프라이버시 및 기밀성 문제 외에도 무단 액세스는 리소스 소비에 영향을 미치므로 DoS 공격 가능성이 존재한다. 또한 슬라이스에 부착한다는 단순한 사실 자체가 고객 개인 정보 보호 문제를 야기할 수 있다. 예를 들어 슬라이스 식별은 동일한 슬라이스를 사용하고 따라서 대부분 동일한 서비스를 사용하는 가입자로 구성된 관심 그룹을

구분함으로써 고객 장치의 영구 식별자와의 상관 관계에서 취약성이 될 수 있다. 5G 고객 장치와 관련된 위험은 비 3GPP 네트워크를 통해 네트워크 슬라이스에 액세스할 때 증가한다.

대응기술에는 5G 고객 장치에 대한 강력한 인증 및 액세스 제어가 포함된다. 장치가 네트워크에 액세스할 수 있도록 하는 기본 인증 외에 슬라이스 수준의 보조 인증 (또는 슬라이스 특정 인증)이 권장된다. 기본 인증은 로밍 및 다른 기술 상호 연결을 허용하도록 표준화되어야 한다. 비용을 줄이고 통합을 용이하게 하기 위해 2차 인증도 표준화되어야 한다. 2차 인증은 슬라이스를 관리하는 엔터티의 책임이다. 슬라이스 테넌트의 경우 테넌트는 자신이 관리하는 슬라이스에 대한 액세스 제어에 직접 관여하므로 리소스 할당이 보다 효율적이다. 네트워크 슬라이스에 동시에 액세스할 수 있는 고객 장치 수, 동시 활성 세션 수 및 네트워크의 여러 수준에서 수행되는 장치당 데이터 속도의 제한은 DoS와 관련된 위험을 완화할 수 있다.

ii) 슬라이스 서비스 인터페이스

가능한 공격 지점은 슬라이스와 슬라이스를 사용하는 서비스 간의 인터페이스이다. 공격자가 서비스를 공격하여 슬라이스를 손상시킬 수 있다. 이로 인해 동일한 슬라이스에서 실행 중인 다른 서비스가 손상될 수 있다. 또한 서비스 간 직접 통신의 경우 이 역시 공격 포인트가 될 수 있다.

대응기술에는 적절한 보안 수준의 구현과 올바른 서비스 구성(예: 권한 및 리소스 제한)이 포함된다. 서비스 간에 그리고 슬라이스와 소비 서비스 간에 올바른 수준의 격리를 구현해야 한다.

iii) 하위 슬라이스

슬라이스가 여러 하위 슬라이스의 체인으로 정의되면 하위 슬라이스 자체와 하위 슬라이스 간의 상호 연결이 모두 공격 지점을 나타낸다. 하위 슬라이스 체인의 전체 보안 수준은 가장 약한 하위 슬라이스에 의해 정해진다.

대응기술에는 특히 액세스 네트워크가 3GPP가 아닌 경우 상호 연결 시 위험을 줄이기 위한 하위 슬라이스 보안 및 구현 메커니즘이 포함된다. 서로 다른 기술의 상호 연결에서 보안 문제를 조사하는 것은 여전히 향후 작업의 대상이며 RAN 하위 슬라이스와 관련하여 더 많은 연구가 필요하다.

iv) 슬라이스 관리자

슬라이스 관리자는 네트워크 슬라이스 템플릿, API, 액세스 권한, 상호 인증, 신뢰 등과 관련하여 보안 위협을 가져온다. 테넌트가 슬라이스 관리를 담당할 때 위험이 증가한다.

대응기술에는 호스트 플랫폼과 네트워크 관리자 사이에 상호 인증이 설정되어야 한다. 더 많은 슬라이스 관리자가 존재하는 경우 서로를 상호 인증해야 한다. 테넌트가 슬라이스 관리를 담당하는 경우 당사자 간의 약속에 따라 해당 기능이 제한되어야 한다. 보다 정확하게는 테넌트는 합의된 것 이외의 모든 요청, 데이터, 리소스 및 기능에 대한 액세스를 방지해야 한다. 3GPP는 또한 다중 테넌트 환경에서 네트워크 슬라이스 성능 및 장애 모니터링을 권장한다.

v) 리소스 및 네트워크 기능

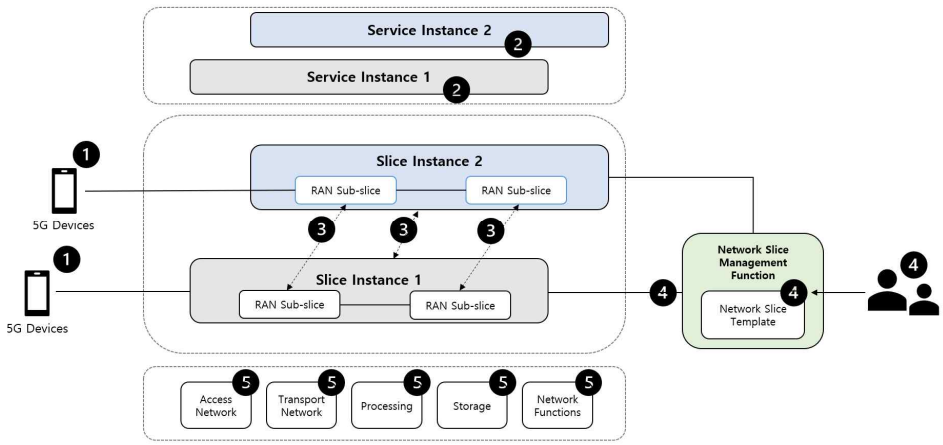
자원 및 네트워크 기능은 이를 소비하는 슬라이스를 손상시키기 위해 공격을 받을 수 있다. 물리적 공격, 소프트웨어 공격 및 보다 일반적인 사이버 공격을 포함하여 매우 다양한 공격이 발생할 수 있다.

대응기술에는 상호 인증, 보안 부팅, 자격 증명 액세스, 물리적 보안 및 무결성 확인이 포함된다. 이러한 기술은 신뢰 수준을 높이지만 네트워크 슬라이싱에만 국한되지 않는다. 서로 다른 수준의 보안 또는 민감도를 위해 공동 호스팅을 피해야 한다. 특히 민감한 서비스를 제공하는 슬라이스와 실험적 또는 테스트

코드를 사용하는 슬라이스 간의 공동 호스팅은 피해야 한다.

2) 네트워크 슬라이스 간 위협 지점 및 대응 기술

[그림 부록2-32] 네트워크 슬라이스 간 위협 지점



자료: Olimid, Ruxandra F., and Gianfranco Nencioni. (2020). "5G network slicing: A security overview." *J IEEE Access 8*, (2020), pp.99999-100009.

ⅰ) 5G 고객 디바이스

5G 고객 디바이스는 가장 취약한 공격 지점 중 하나이다. 한 슬라이스에 대한 액세스 권한이 부여된 고객 장치가 다른 권한 없는 슬라이스에 대한 액세스 권한을 얻으려고 할 때 보안 위협이 나타난다. 또 다른 위협은 적대적인 장치가 액세스 권한이 있는 슬라이스의 공유 리소스를 과도하게 소비하여 슬라이스의 성능을 손상시키거나 DoS 공격에 성공할 수도 있다는 것이다. 성능 공격은 리소스 부족으로 인해 슬라이스가 필요한 수준에서 보안 프로토콜을 수행하는 것을 방지하여 다른 유형의 공격을 용이하게 할 수 있다. 일반적으로 장치는 단일 슬라이스에 연결할 수 있는 권한이 있어야 한다. 그러나 장치에 서비스에 대한 다양한 액세스가 필요한 경우 여러 슬라이스에 동시에 연결하는 것이 허용될 수 있다. 그렇다면 장치가 더 안전한 슬라이스에서 덜 안전한 슬라이스로 민감한 데이터를 유출할

위험이 있는 것처럼 보인다.

대응 기술에는 액세스 제어, 기밀성, 무결성, 신뢰성 및 리소스 소비 측면에서 슬라이스 간의 적절한 격리가 포함된다. 여기서 특별한 경우는 고객 장치가 두 개(또는 그 이상)의 네트워크 슬라이스에 동시에 액세스하도록 제한되는 경우 네트워크 슬라이스에 대한 상호 배타적 액세스이다. 그렇지 않은 경우 각 슬라이스와 고객 장치 간에 별도의 상호 인증을 권장한다. 리소스는 보안 메커니즘 실행을 위한 가용성을 보장하고 DoS를 방지하도록 구성되어야 한다.

ii) 서비스-서비스 통신

가능한 공격 지점은 서로 다른 슬라이스를 사용하는 서비스 간의 인터페이스이다. 공격자가 일부 서비스를 공격하여 다른 슬라이스 위에서 실행되는 다른 서비스를 손상시킬 수 있다. 일반적으로 서로 다른 슬라이스에서 실행되는 서비스가 독립적이고 통신이 필요하지 않기 때문에 이를 보안 위험이 낮은 것으로 간주한다.

대응기술에는 적절한 격리 구현이 포함된다. 트래픽 및 행위 분석, 이상 탐지는 슬라이드와 다른 구성요소 사이 또는 내부에서 허용되지 않는 통신을 조사하는 일반적인 기술이다. 인공 지능을 사용하는 트래픽 캡처 및 방어 메커니즘에 기반한 특정 기술을 사용하여 기본 필터를 우회하는 지능형 공격으로부터 보호할 수 있다. 트래픽 격리는 슬라이스 침입을 방지하는 흐름 규칙을 정의하여 네트워크 요소에 의해 시행될 수도 있다.

iii) Intra-Slices 및 Intra-Sub-Slices 통신

공격자는 덜 안전한 슬라이스(특히 RAN 하위 슬라이스)를 공격하여 더 안전한 슬라이스를 공격하려고 할 수 있다. 슬라이스 간의 통신이 허용되는 경우 가능한 위협에는 무단 액세스, 공유 매개변수 누출, 슬라이스 간에 전송되는 민감한 데이터가 포함된다.

대응기술에는 슬라이스 간의 적절한 격리가 포함된다. 한 슬라이스가 손상되면 다른 슬라이스에 영향을 미치지 않아야 한다. 유출을 방지하려면 암호화 매개변수(예: 암호화 키)를 슬라이스 간에 공유해서는 안 된다. 기본 인증의 키가 슬라이스

내에서 사용되는 경우 키 생성 기능을 사용하여 각 슬라이스에 대해 새롭고 독립적인 키를 생성해야 한다. 슬라이스 간 격리 활성화 기술의 예에는 태그(예: MPLS 사용), VPN-(예: SSL/TLS 사용) 또는 VLAN 기반 격리가 포함된다.

ⅳ) 관리 시스템

관리 시스템은 공격 지점으로 테넌트는 다른 테넌트의 슬라이스에 액세스하거나 다른 테넌트에 속하는 슬라이스 간에 공유되는 매개변수를 변경하려고 시도할 수 있다.

대응기술에는 슬라이스 관리자의 개별 슬라이스 간의 적절한 격리와 다른 테넌트에 속하는 슬라이스 간에 공유되는 매개변수에 대한 변경 제한이 포함된다. 강력한 인증 및 액세스 제어 절차가 수행되어야 한다.

ⅴ) 자원 인프라

리소스 계층은 DoS뿐만 아니라 소프트웨어 공격과 같은 다른 측면에서도 공격 지점이다. 예를 들어 공격자는 한 조각의 코드에 액세스하고 변조하여 동일한 코드를 사용하는 모든 코드 조각의 실행을 변경시킬 수 있다.

대응기술에는 코드 보호 기술 및 코드 격리가 포함되며, 이는 네트워크 슬라이싱에만 국한되지 않는다.

3) 네트워크 슬라이스 보안 고려사항

ⅰ) 네트워크 슬라이스 내 보안 고려사항

- 슬라이스는 종단 간 논리 네트워크이므로 종단 간 보안을 고려해야 한다.
- 모든 통신(예: 슬라이스와 리소스 계층, 슬라이스와 슬라이스 관리자, 슬라이스의 하위 슬라이스, 네트워크의 고객 장치 및 액세스 포인트)은 대상 보안 수준을 보장하기 위해 적절한 메커니즘을 사용해야 한다. 최소한의 요구 사항에는 데이터의 기밀성, 무결성, 신뢰성 및 피어 간의 상호 인증이 포함되어야 한다.
- 5G 고객 장치는 1차 인증과 선호하는 2차 인증을 통해 강력하게 인증되어야 한다.

- 슬라이스에서 사용하는 모든 리소스와 네트워크 기능은 보호되어야 한다.
- 민감한 식별자는 보호되어야 하며 식별자 간의 상관관계가 유출되어서는 안 된다.
- 합법적인 차단은 슬라이스 및 서비스 계층 모두에서 액세스할 수 있어야 한다.
- 테넌트 액세스, 권한 및 구성 기능은 당사자 간의 계약을 준수해야 한다.
- 모든 3GPP 일반 보안 요구 사항도 슬라이스 수준에서 충족되어야 합니다.

ii) 네트워크 슬라이스 간 보안 고려사항
- 모든 슬라이스에 대해 최소한의 권한을 부여해야 한다.
- 슬라이스 간의 격리는 덜 안전한 슬라이스를 통한 공격을 방지할 수 있을 만큼 충분히 되어야 한다.
- 슬라이스 간의 통신은 최소한으로 줄여야 하고 엄격한 규칙에 따라 정의되며 보안 채널을 통해 구현되어야 한다.
- 암호화 키(및 기타 민감한 매개변수)는 슬라이스 간에 공유되어서는 안된다.
- 리소스 할당은 각 슬라이스에 대해 최소 수준의 가용성을 보장해야 합니다. 특히 보안 메커니즘은 리소스 소비에 관계없이 실행할 수 있어야 한다.
- 보안 수준에 상당한 차이가 있는 슬라이스는 리소스 또는 네트워크 기능을 공유해서는 안된다. 특히 런타임 단계의 슬라이스와 함께 테스트 모드의 슬라이스를 실행하면 안된다.
- 고유한 인증, 권한 부여 및 액세스 제어 메커니즘은 각 슬라이스에 대해 독립적이어야 한다.
- 5G 고객 장치가 여러 슬라이스에 동시에 연결되도록 허용되는 경우 고객 장치에서도 (데이터의) 격리가 가능해야 한다.
- 테넌트는 다른 테넌트의 슬라이스 및 서비스에 영향을 미치는 구성 변경을 수행하지 못하도록 해야 한다.

제 3 절 NetApp 보안 고려사항 연구

1. 서론

5G 기술은 다양한 수직 부문의 사용 사례에서 비롯된 요구사항을 충족하기 위해 높은 수준의 프로그래밍 활용, 제어 및 유연성을 제공할 뿐만 아니라 더 높은 용량과 더 낮은 지연 시간을 제공하는 것을 목표로 한다. 또한, 엄청난 수의 사용자에게 여러 이기종 서비스를 지원하기 위하여 효율적이고 동적인 관리가 중요하다. 이를 위해 NFV(Network Function Virtualization) 패러다임의 진화는 이전에 볼 수 없었던 네트워크 내 유연성을 가능하게 하고 있다. 그러나 운영 중인 5G 인프라 내에서 타사에서 개발한 네트워크 기능을 통합하기 위해서는 엄격한 테스트와 평가 프로세스를 통해 보안성을 준수해야 한다.

5G는 리소스의 동적 할당, 분산 클라우드 인프라의 유연한 기능 배치, 전송 수준에서 물리적 네트워크 전반에 걸쳐 소프트웨어 피어 엔터티와 터미널 사이의 종단 간 제어 및 데이터 평면 연결을 포함해야 한다. 이러한 5G의 요구는 개발, 테스트 및 인증 사이의 주기를 단축할 수 있는 5G NetApp (5G Network Application)을 통해 지원할 수 있을 것으로 기대하고 있다. 5G 환경에서 NetApp 배포를 위한 핵심 기술로 NFV, SDN (Software-Defined Network), 클라우드 컴퓨팅 및 MEC (Multi-Access Edge Computing)가 언급되고 있다. 리소스 관리 및 오케스트레이션은 사용가능한 물리적 및 가상 네트워킹, 스토리지 및 컴퓨팅 리소스 간의 조정을 제공하는 MANO(Management and Network Orchestration) 프레임워크에서도 매우 중요하다.

본 절에서는 5G의 보안구조와 키 계층, 인증 프레임워크에 대하여 살펴보고, 5G 네트워크에서 이기종 서비스를 효과적으로 제공하기 위한 NetApp에 대하여 알아본다.

2. NetApp

오늘날 5G 네트워크를 통한 연결성의 엄청난 성장, 많은 양의 트래픽 데이터 및 광범위한 비즈니스 모델로 기능 및 서비스 품질(QoS) 제공 측면에서 유연한 인프라로 전환할 필요가 있다. 이와 관련하여 5G 네트워크는 성능 요구사항이 서로 다른 광범위한 이기종의

어플리케이션을 지원할 수 있어야 하며 동시에 이전 세대의 모바일 네트워크와 비교하여 향상되고 최적화된 방식으로 제공해야 한다. 따라서 다양한 형태로 개방성을 제공하기 위해 업계와 표준화 기구의 노력이 필요하다. 실제로 3GPP (3rd Generation Partnership Project)의 5G 사양은 5G Core 네트워크에서 채택한 SBA (Service based Architecture)를 통해 이러한 개방성을 구체화하고 있다. SBA를 통한 방식은 리소스 할당, 서비스 오케스트레이션, 수명 주기 관리 및 서비스 슬라이싱을 보다 효율적인 방식으로 제공할 수 있으며 네트워크 내에서 유연성, 가용성 및 안정성이 향상되어 새로운 비즈니스 기회를 활용할 수 있다.

5G 물리적 인프라는 눈에 띄는 수준의 성숙도에 도달하고 있다. 엄청난 수의 사용자를 위해 과다한 이기종 서비스를 지원할 수 있는 잠재력을 감안할 때 효율적이고 동적인 관리가 중요하다. 이를 위해 NFV (Network Function Virtualization) 패러다임의 진화는 이전에 볼 수 없었던 네트워크 내 유연성을 가능하게 하고 있다. 그러나 운영 중인 5G 인프라 내에서 타사에서 개발한 네트워크 기능의 통합은 보안상의 이유로 엄격한 테스트 및 평가 프로세스를 따라야 한다.

현재 유럽에서 진행되는 주요 H2020 연구 과제 중 5GASP (https://5g-ppp.eu/5gasp/)에서 이를 지원하기 위한 개방형 및 도메인 간 5G NFV 기반 테스트베드 인프라를 구축하고 있다. 이외에도 5G 테스트베드 인프라를 구축하고 있는 그룹에는 5GVINNI (https://www.5g-vinni.eu/), 5GinFIRE (https://5ginfire.eu/), SLICENET (https://slicenet.eu/) 등이 있다. 또한 5GASP 인프라는 5GASP 용어에 따라 새로운 네트워크 기능 또는 네트워크 애플리케이션(NetApps)의 테스트를 목표로 Vertical 산업의 완전히 소프트웨어화된 아키텍처를 인스턴스화하기 위한 토대를 마련할 것으로 기대하고 있으며, 이를 통해 NetApp이 인증되면 NetApp Marketplace를 통해 사용자들에게 제공될 수 있다.

모바일 네트워크는 지난 몇 년 동안 4G 네트워크에서 5G 네트워크로 진화하여 광섬유 네트워크에 상당한 속도와 개선된 지연시간을 제공하여 다양한 사용 사례 요구사항을 제공한다. 5G 네트워크는 eMBB (Enhanced Mobile Broadband), mMTC (Massive Machine Type Communications) 및 URLLC (Ultra Reliable Low Latency Communications)라는 세 가지 서비스를 지원할 뿐만 아니라 전용 네트워크 슬라이스를 통해 통신 서비스를 제공할 수 있는 버티컬을 통해 요구사항이 다양한 어플리케이션 서비스에 적합한

네트워크를 지원할 수 있다. 소비자에게 제공되는 새로운 5G 기능은 가상화된 소프트웨어 기반 네트워크 기능 (SDN), 클라우드 네이티브 애플리케이션 및 오케스트레이션 도구, 다양한 가상 네트워크 기능 (VNF)의 자동 배포 및 인스턴스화, 수명 주기 관리 (LCM) 도구를 통해 기술적으로 유지된다. 네트워크 슬라이싱, 5G RAN 및 코어 참조 아키텍처 또는 가상화된 환경 배포 및 오케스트레이션과 같은 이러한 초기 개념은 다양한 5G-PPP 프로젝트 및 문서에서 제시되었다.

위에서 설명한 바와 같이 API를 통해 구체화된 5G 네트워크의 개방성을 고려하여 NetApp (Network Application)의 개념을 정의한다. EVOLVED-5G의 맥락에서 NetApp은 표준화되고 신뢰할 수 있는 환경에서 API (예: 5G 코어의 Northbound API 및/또는 MEC API)를 사용하여 모바일 네트워크의 제어 평면과 상호 작용하는 소프트웨어 부분으로 정의된다. 즉, 5G 네트워크의 경우 NetApp은 CAPIF (Common API Framework)를 준수해야 한다. 또한, NetApp은 버티컬 산업을 위한 서비스를 구성해야 하며, 버티컬 애플리케이션의 통합 부분으로 API를 제공하여 버티컬 애플리케이션 서비스를 제공해야 한다. 이러한 맥락에서 버티컬 산업은 3GPP API 및 기타 통신 자산을 사용하여 새로운 서비스를 구성하는 NetApp을 개발할 수 있다.

예를 들어, VoD (Video on Demand) 콘텐츠를 배치하기 위해 NEF API (데이터 경로 구성에 영향을 미치는 TrafficInfluence API 및 위치 정보 검색을 위한 MonitoringEvent API)를 활용하는 프레임워크를 제안했다. 제안된 프레임워크는 전체 비디오의 세그먼트를 MEC 캐시에 배포하지만 사용자가 MEC의 커버리지 영역을 횡단하는 동안 대기 시간을 최소화하고 코어 네트워크의 트래픽 부하를 최적화한다. 제안된 프레임워크를 통해 NetApp의 배포 및 활용을 최적화할 수 있을 것으로 기대할 수 있다. NetApp은 5G Core에서 정보를 수신할 뿐만 아니라 이러한 데이터를 활용하여 보다 효과적인 작업을 수행할 수 있다. 또한, 기계 학습 알고리즘을 프레임워크에 적용하여 세그먼트를 배치할 위치를 예측할 수도 있다.

서비스가 버티컬에 제공되는 방식을 고려할 때 NetApp은 다음과 같이 분류할 수 있다.

- 독립형 NetApp : 독립형 NetApp은 직접 또는 수직 애플리케이션에 대한 통합을 통해 하나 이상의 버티컬 산업에 서비스를 제공한다. 버티컬 애플리케이션에 통합된

NetApp은 5G 네트워크에 통해 네트워크 관리 및 모니터링 기능을 추가하여 애플리케이션의 기능을 개선할 수 있다.

- 비독립형 NetApp : 비즈니스 API를 통해 서비스를 제공하기 위해 Northbound API의 래퍼로 작동하는 NetApp이며, 비즈니스 API가 앱에서 활용될 때 기능하게 되는 비독립형 소프트웨어이다. 비독립형 NetApp을 사용하면 소프트웨어의 필수 부분을 변경하지 않고도 버티컬 애플리케이션을 개발할 수 있다.

NetApp 에코시스템은 5G 네트워크와 상호 작용할 수 있는 버티컬 애플리케이션의 환경을 의미한다. 대규모 버티컬 시스템의 구현 및 배포를 단순화하기 위해 미들웨어 계층을 분리하고, 미들웨어 계층의 요청에 응답하는 방식으로 구동한다. 이는 3GPP SA6에서 진행되고 있는 VAE (Vertical Application Enabler)의 개발과 맞물려 진행되고 있으며, NetApp을 MNO (Mobile Network Operator)와의 상호 작용 및 신뢰 수준에 따라 분류하여 활용할 수 있다.

- 타사 NetApp : 신뢰할 수 있는 타사 도메인에 있는 NetApp으로서 타사 NetApp은 Northbound API를 사용하여 버티컬에 대해 네트워크에서 정의한 신뢰 메커니즘 및 보안 정책을 지원한다.
- 운영자 NetApp : 주로 NPN (NonPublic Network) 배포를 고려하여 운영자 도메인에 상주하고 잠재적으로 Northbound API를 통해 제공되는 기능 외에 5G 네트워크 기능에 추가로 액세스할 수 있는 NetApp 및 타사 NetApp에서 사용할 수 있다. 이 경우 NetApp은 5GC NF와 직접 상호 작용할 수 있다.

3. 인더스트리 4.0 시대에서의 NetApp

인더스트리 4.0은 스마트 팩토리 (Smart Factory)의 등장과 함께 제4의 제조업 변화 시대를 의미한다. 공급망에서 생산 및 서비스에 이르는 모든 제조 프로세스는 사물 인터넷 (IoT) 및 사이버-물리 시스템 (CPS)을 기반으로 하는 지능형 자율 시스템의 도입을 통해 변화하고 있다. 따라서 대량의 통신 및 연결 요구를 지원할 수 있을 뿐만 아니라 스마트팩토리 내부의 다양한 이기종 프로세스를 지원할 수 있는 유연성을 가질 수 있는

산업 네트워크 인프라가 요구된다. 이러한 인프라 주요 후보로는 5G NPN (5G Non-Public-Network)이 있으며, 5G NPN은 인더스트리 4.0의 주요 요구사항인 높은 데이터 전송률과 안정성, 대기 시간이 짧은 통신을 제공할 수 있다. 미래의 5G 네트워크 기반 스마트팩토리를 고려하면 5G 네트워크의 개방성을 통해 NetApp 에코시스템을 활용할 수 있을 것으로 예상된다. 특히, NetApp 개발의 주요 그룹인 EVOLVED-5G은 스마트 제조 부문에 NetApp을 적용하는 것을 목표로 개발을 진행하고 있다. EVOLVED-5G가 제안한 목표는 산업 서비스 제공업체에서 근무하는 작업자의 전문 지식 부족한 경우 발생할 수 있는 문제를 해결할 수 있다. EVOLVED-5G는 5G 코어와 기존 산업용 버티컬 애플리케이션 사이에 미들웨어 계층을 제공함으로써 5G 기능을 최대한 활용하는 5G 지원 산업용 애플리케이션의 개발을 목표하고 있다.

산업 부문에 NetApp을 제공할 수 있는 가능성에 대응하기 위해 EVOLVED-5G에서는 다음과 같은 산업 서비스의 4개 그룹을 대상으로 한다.

- Interaction of Employees and Machines (IEM).
- Efficiency in FoF Operations (FoF).
- Security Guarantees and Risk Analysis (SEC).
- Production Line Infrastructure (PLI).

혁신적인 5G 환경은 새로운 최첨단 네트워크 애플리케이션에 대응해야 하며, 5G 버티컬의 서비스 요구사항과의 상호 운용성을 보장하는 테스트베드인 Advanced 5G Testbed를 통해 구현 및 검증할 필요가 있다. 통신 사업자는 시설에 DevOps 원칙을 적용하고 기존 테스트베드 및 인프라를 구축하고 미래를 위한 네트워크 지원을 제공하기 위해 인공 지능 알고리즘의 지원, 종단 간 네트워크 자동화 기능을 도입해야 한다. 5G 네트워크에 대한 테스트. 통신 사업자의 활동은 5G가 컴퓨팅 및 스토리지 리소스의 동적 할당, 5G NFV 기반 참조 아키텍처를 기반으로 하는 새롭고 혁신적인 NetApp, 앱의 개발 및 테스트를 지원할 수 있다. 5G 서비스는 NetApp의 종단 간 요구사항을 충족하기 위해 물리적 및 가상화된 네트워크 요소 전반에 걸쳐 엔터티 간의 종단 간 제어 및 데이터 평면 연결에 필요한 전송 수준을 고려하여 필요한 곳이면 어디든지 제공되어야 한다.

제 4 절 AKMA
(Authentication and Key Management for Application)

1. 개요

네트워크 기술의 발전과 이에 따른 새로운 어플리케이션 서비스의 등장으로 사용자들은 언제 어디서나 원하는 서비스를 누리게 되었다. 특히, 5G에서는 높은 처리량과 낮은 지연시간을 통해 사용자가 활용할 수 있는 서비스의 양과 질이 급격히 늘어나고 있다. 또한, 물리적 네트워크 인프라가 네트워크 가상화 기술을 통해 논리적 네트워크로 전환되면서 5G 네트워크 슬라이싱 기술 기반의 서비스 맞춤형 네트워크를 제공할 수 있게 되었다. 요구사항을 만족하는 네트워크를 각각의 서비스에 제공하게 되면서 서비스에 접근하는 사용자가 인가된 사용자임을 확인해야 한다. 즉, 이동 통신망에서 어플리케이션 제공자로부터 서비스를 제공받기 위해서는 어플리케이션 계층에서의 사용자 단말에 대한 인증 절차가 필요하다. 일반적으로 사용자 단말과 어플리케이션 사이의 인증은 단순히 ID/패스워드 조합에서부터 인증서까지의 다양한 자격증명 기반의 인증 방식이 사용되고 있다. 사용자 단말과 어플리케이션 사이의 통신을 보호하기 위하여 통신 당사자만이 알고 있는 세션 키 등을 활용한 자격증명을 활용하는 것은 합당하다. 그러나 셀룰러 및 WiFi, 블루투스에 이르기까지 다양한 무선 통신 기술에서 사용자 단말과의 어플리케이션 계층 인증 및 초기인증을 진행할 때, 사전 공유 키 혹은 인증서를 활용하는 방식에 의존하고 있다. 이러한 대규모의 사전 공유 키 및 인증서를 관리하는 것은 서비스 제공자에게 큰 부담이 될 수 있다.

3GPP에서는 5G 시스템에 접속하면서 필수적으로 생성하는 3GPP 자격증명을 기반으로 어플리케이션 인증 및 키 관리를 지원하고자 AKMA (Authentication and Key Management for Application)의 표준화에 박차를 가하고 있다. AKMA는 이전 세대의 이동통신 시스템에서 유사한 서비스를 수행한 GBA (Generic Bootstrapping Architecture)와 BEST (Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices)를 확장시킨 것이다. GBA는 이전 세대에서 SBI

(Service-Based Interface)를 지원하지 않았지만 5G가 등장하면서 SBI를 지원할 수 있는 방향으로 개선되고 있다. 그러나 키를 파생하는 절차에서 CK (Cipher Key)와 IK (Integrity Key)에서 직접적으로 어플리케이션 키를 파생하고, 5G 초기 인증 절차 이후에 추가적인 AKA (Authentication and Key Agreement) 프로토콜을 실행한다는 점에서 비효율적이다. BEST는 SBI를 고려하지 못함과 동시에 5G 네트워크에서 동작할 수 없다. 또한, GBA와 유사하게 어플리케이션 키가 CK와 IK로부터 직접 파생되고, 초기 인증 절차 이후 추가적인 인증 절차가 요구된다. 이에 반해, AKMA는 SBI를 지원하고, 5G 초기 인증 절차의 결과를 재사용하기 때문에 효율적이다.

AKMA 구조는 기존 5G 네트워크 기능 이외에 추가적으로 AAnF (AKMA Anchor Function)와 AF (Application Function)라는 두 가지 새로운 네트워크 기능을 포함한다. AAnF는 HPLMN (Home Public Land Mobile Network)에서 AKMA를 위한 앵커 기능을 수행하며, 5G 초기 인증이 완료되고 AUSF로부터 KAKMA를 부여받아 이를 저장한다. AUSF로부터 부여받은 KAKMA는 차후 키를 파생하는 데 활용된다. AF는 사용자에게 서비스를 제공하는 기능으로서 사용자 단말로부터 접근 요청이 들어오면 AAnF에게 KAF를 부여받아 사용자 단말과의 세션을 구성을 완료한다. 이와 같이 [31]에서는 AKMA의 절차 및 구성 요소에 대하여 언급하고 있다.

2. 서비스 기반 구조 (Service based Architecture)

SBA (Service Based Architecture)는 다양한 소스 및 공급 업체의 구성 요소를 사용하여 공통 어플리케이션을 배포할 수 있는 모듈식 프레임워크를 제공한다. 3GPP는 SBA를 정의하면서 5G 네트워크의 제어 영역과 공통 데이터 저장소는 서로 접근할 수 있도록 권한이 있는 NF를 통해 제공되도록 하였다. 서비스 소비자 혹은 서비스 생산자의 역할을 가정하고 NF는 독립적이며 재사용이 가능하다. 각 NF 서비스는 HTTP/2를 사용하여 REST 인터페이스를 사용하는 SBI (Service Based Interface)를 통해 노출된다. TCP HOL (head-of-line) 차단과 관련된 문제를 완화하기 위해 향후 QUIC (Quick UDP Internet Connections) 프로토콜을 사용할 수 있다. 5G SBA는 다음과 같은 다양한 요소로 구성된다.

• NRF (NF Repository Function)

5G SBA는 마이크로서비스 방법론을 사용하여 구축된 NF를 통해 궁극적으로 서비스 검색, 로드 밸런싱, 암호화, 인증 및 권한 부여가 포함된 완전한 서비스 메시로 발전하고자 함. 그러나, 현재의 SBA는 NRF를 활용하는 중앙 집중식 검색 프레임워크를 사용함. NRF는 사용 가능한 NF 인스턴스 및 지원되는 서비스에 대한 기록을 유지함. 다른 NF 인스턴스가 구독을 허용하고 지정된 유형의 NF 인스턴스에서 등록 알림을 받을 수 있음. NRF는 NF 인스턴스의 검색 요청과 특정 서비스를 지원하는 세부 정보를 수신하여 서비스 검색을 지원함.

• NSSF (Network Slice Selection Function)

네트워크 슬라이싱은 5G 인프라의 근본적인 새로운 기능으로 다양한 네트워크 서비스 및 어플리케이션을 배포할 때 높은 수준의 배포 유연성과 효율적인 자원 활용을 제공함. 논리적 종단 간 네트워크 슬라이스에는 미리 결정된 기능, 트래픽 특성 및 서비스 수준 계약이 있으며 UPF (User Plane Function), SMF (Session Management Function), PCF (Policy Control Function)을 포함하는 MVNO (Mobile Virtual Network Operator) 혹은 가입자 그룹의 요구사항을 처리하기 위한 가상화된 자원이 포함됨. UE를 지원하는 AMF (Access and Mobility Management Function) 인스턴스는 UE가 속한 모든 네트워크 슬라이스에 일반적임. 네트워크 슬라이스의 식별은 S-NSSAI (Single Network Slice Selection Assistance Information)를 통해 이루어지며, 네트워크 슬라이스 인스턴스의 선택은 UE 등록 요청을 수신하는 첫 번째 AMF에 의해 실행됨. 해당 요청은 UDM (Unified Data Management)에서 허용된 슬라이스를 검색하여 NSSF에게 적절한 네트워크 슬라이스 인스턴스를 요청함.

• UDM (Unified Data Management)

UDM은 AMF, SMF 및 NEF와 같은 다른 SBA 기능에 서비스를 제공함. UDM은 일반적으로 로컬 메모리에 정보를 보유하는 상태 저장 메시지 저장소로 인식되지만, 상태를 저장하지 않을 수도 있으며, UDR (Unified Data Repository)에 정보를 저장할 수 있음. UDM은 HSS (Home Subscriber Server)와 유사하며 AMF 및 SMF에서

구독자의 데이터 및 컨텍스트를 검색하고 인증 자격을 증명하는 데 사용됨.

• PCF (Policy Control Function)

PCF는 네트워크의 동작을 관리하기 위하여 5G 인프라 내에서 통합 정책 프레임워크를 지원함. PCF는 UDM에서 정책을 결정하는데 필요한 구독 정보에 접근하여 제어 평면 기능에 적절한 정책 규칙을 제공함. PCF는 EPC 구조의 PCRF (Policy and Charging Rule Function)와 유사함.

• SCP (Service Communication Proxy)

3GPP 5G Rel-16에서 등장하는 SCP는 5G 시스템을 위한 시스템 구조인 TS 23.501에서 정의됨. SCP는 5G SBA를 동작하는 데 필요하지 않지만, MEC (Multi-access Edge Computing) 환경에서 작동하는 데 필요함. SCP는 NRF에 의해 성공적으로 검색되면 네트워크 기능 클러스터에 대한 단일 진입점을 제공함. 이를 통해 SCP는 데이터 센터에서 위임된 검색 지점으로서 궁극적으로 네트워크 운영자의 인프라를 구성하는 수많은 분산 서비스 메시에서 NRF를 오프로드할 수 있음. SCP는 NRF와 함께 계층적 5G 서비스 메시를 형성함.

SBA는 웹 기술 및 웹 프로토콜을 기반으로 구축되어 가상화 및 컨테이너 기술과 클라우드 기반 처리 플랫폼을 사용하여 유연하고 확장 가능한 구현을 가능하게 한다. 그러나 광범위한 5G 시스템 구조와 가상화된 구현 및 클라우드 프로세싱이 5G SBA에 다양하고 많은 보안을 요구하도록 만든다. 이러한 보안 요구사항의 변화를 인식하여 SBA에 대한 보안은 새로운 사용 사례와 가상화된 구현에 적절한 보안을 제공하도록 설계되었다.

• 직접 통신을 위한 SBA 보안

SBA 보안은 일반적인 5G 보안과 마찬가지로 3GPP TS 33.501에 명시되어 있다. SBA의 중요한 특징은 NF들이 모두 서로 통신할 수 있다는 것이다. NF 서비스 소비자와 NF 서비스 생산자 간의 요청/응답 또는 가입/알림으로 상호 작용한다.

이를 위해서는 NF 간의 통신을 구현할 방법과 각 NF의 서비스 API를 보호하는 방법과 이러한 API의 사용을 적절하게 승인하는 방법에 대한 신중한 명세가 필요하다. 또한, 기본 프로토콜 스택은 HTTP 및 JSON과 같은 웹 프로토콜을 기반으로 하므로 상호 작용을 보호하는데 사용되는 보안 프로토콜의 선택에도 영향을 미친다. 일반적으로 서로 다른 엔티티 간의 통신을 보호하려면 다음 보안 메커니즘이 구현되어야 한다.

- 메시지 스푸핑에 대응하기 위한 통신 엔드 포인트 사이의 인증
- 메시지 변조, 부인, 정보 노출을 막기 위한 통신 전송 보호(기밀성, 무결성, 재전송 보호)
- 권한 상승을 막기 위한 요청의 인가

SBA 보안 사양의 첫 번째 버전인 Rel-15는 NF 간의 직접 통신, 즉 프록시 없이 보안을 자세히 설명한다. 다음의 두 가지 중요한 구성요소를 기반으로 한다.

- TLS 1.2 및 1.3 기반의 NF 간 상호인증 및 전송 보안
- OAuth 2.0 을 기반으로 NF 서비스 생산자가 제공하는 서비스에 대한 NF 서비스 소비자의 액세스를 위한 토큰 기반 인증

TLS 1.2 및 1.3은 인터넷 및 기타 네트워크에서 통신 보안을 위해 사용되는 최첨단 프로토콜이다. 이전 세대의 모바일 네트워크와 SBA 외부의 5G 네트워크는 IPSec에 의존한다. 보안 관점에서 IPSec이 문제가 있는 것은 아니지만 TLS를 사용하면 전체 네트워크 도메인을 보호하는데 사용되는 보안 게이트웨이 대신 NF에서 직접 보안을 쉽게 종료할 수 있다. 이러한 접근 방식은 다중-차용을 사용하는 가상화된 구현에 적합하다. OAuth 2.0을 사용한 토큰 기반 인증은 동적 가상화 구현에서 인증을 수행하는 방식이다. 클라이언트 (SBA의 NF 서비스 소비자)에게 인증한 후 액세스 토큰을 발급하는 중앙 인증 서버를 기반으로 한다. 클라이언트는 서비스를 호출할 때 NF 서비스 생산자에게 액세스 토큰을 제공한다. NF 서비스 생산자는 소비자에게 접근 권한을 부여하기 위해 액세스 토큰의 유효성을 검증한다. SBA에서 NRF는 인가 서버의 역할을 한다. 인가 규칙은 NRF에 등록하는 동안 NF 서비스 생산자가 자체적으로 제공할 수 있다.

토큰 기반 권한은 인증과 결합하여야 유효하다: NRF 및 NF 서비스 소비자는 NRF가 액세스 토큰을 발급하기 전에 상호 인증한다. 또한, 토큰이 가로채지거나 오용되는 것을 방지하기 위해 전송 보호가 필수적이다.

- 간접 통신을 위한 SBA 보안

  SBA 보안의 두 번째 버전 (Rel-16)은 간접 통신에 대한 보안을 명세한다. NF 소비자가 NF 생산자와 직접 상호 작용하는 대신 간접 통신은 NF 소비자와 생산자 간의 경로에 SCP (Service Communication Proxy)을 도입한다. 보안 관점에서 중요한 측면은 소비자와 생산자가 NF 서비스 소비자를 대신하여 서비스 요청을 보내고 NF 서비스 생산자의 응답을 소비자에게 전달하기 위해 SCP에 의존해야 한다는 것이다. 이는 기본 신뢰 모델에 영향을 미친다. SCP는 단순히 소비자의 서비스 요청을 전달만 하지 않는다. SCP의 표준화된 기능과 독점적 기능 모두에 대해 SCP가 활성화되고 서비스 요청 메시지를 수정할 수 있어야 한다. 따라서 각 Hop에 대한 상호인증 및 전송 보안은 TLS 기반으로 하지만 직접 통신에서 TLS로 충족하는 소비자와 생산자 간의 종단 간 전송 보안은 간접 통신에서는 불가능하다. 하지만 직접 통신을 위해 이미 명세 된 토큰 기반 인증은 SCP가 이를 대신할 권한이 있음을 생산자에게 증명할 수 있는 수단을 제공한다. SCP는 단순히 NF 서비스 소비자에게 발급된 유효한 액세스 토큰을 생산자에게 전달한다. 일부 배포 모델의 SCP는 NF 서비스 소비자를 대신하여 액세스 토큰을 요청할 수 있다. 이는 NRF가 소비자를 대신하여 액세스 토큰을 요청하도록 승인된 SCP만 할 수 있도록 보장하는 경우에만 가능하다. 이를 위해 소비자는 SCP가 NRF에서 사용하는 자체 서명된 인증서를 SCP에 전송하여 소비자가 승인했음을 증명한다. 이 메커니즘은 토큰 기반 인증을 수행한다. 앞서 언급했듯이 NF 서비스 소비자와 생산자 간의 통신을 위해 SCP는 액세스 토큰 사용하여 대신할 권한이 있음을 증명할 수 있다.

- SBA 보안의 구현

  SBA에서 TLS와 OAuth 2.0을 모두 사용하려면 네트워크에서 PKI(Public-Key

Infrastructure)를 구축해야 한다. PKI에서 CA(Certificate Authority)는 적절한 신원 관리 기능 및 정책에 따라 각 통신의 엔드 포인트에 인증서를 발급한다. 인증서와 관련된 공개/개인 키 쌍은 SBA에 명시된 대로 TLS 및 OAuth 2.0을 사용하는데 필요한 토큰의 상호인증 및 서명/검증에 사용되는 비대칭 암호화에 사용될 수 있다. SBA 구현은 주로 빠른 속도로 지속적인 배포 및 업데이트를 지원하는 마이크로서비스 아키텍처를 사용하여 수행된다. NF 간의 연결을 위한 TLS 사용과 함께하려면 NF가 안전하게 보관해야 하는 인증서를 발급하고 관리하는 고도로 자동화된 프로세스가 필요하다. 동적 5G 시스템에서 인증서를 안전하게 발급하는 방법을 고려하는 것 외에도 클라우드 환경에서 TLS 엔드 포인트에 대한 비밀 저장소를 보호하는 방법에 대한 문제도 존재한다. 이러한 문제들은 NF가 실제로 하나씩 동작하는 서비스가 아니라 내부 NF 통신을 보호해야 하는 상호 작용 마이크로서비스 모음이라는 상황으로 인해 발생한다. 이 내부 NF 통신은 3GPP 문서에 명시되어 있진 않지만, TLS 일반적으로 통신을 보호하고 API 사용 권한을 부여하며 NF의 토폴로지를 마이크로서비스 집합으로 유지하는 데 사용된다. 이 내부 NF에 대한 인증서가 제공되는 방식은 3GPP 사양에 포함되지는 않지만, NF 내 통신을 위한 인증서 공급 솔루션이 차용자가 요구하는 경우 차용 PKI와 통합할 수 있는 방식으로 구현되어야 하므로 밀접하게 관련되어 있다. SBA는 강력한 규제 요구사항이 있는 모바일 네트워크 사용을 위한 것이므로 차용자의 인증서 제어 문제는 더욱 심화된다. 현재 3GPP 사양에는 인증서를 프로비저닝하는 방법과 적절한 PKI를 지정하지 않은 설정 방법에 대한 몇 가지 세부 정보들이 있다. 대체로 SBA를 구현할 때 인증서 관리 및 관련된 키의 저장이 보안을 위한 중요한 작업을 차지한다.

SBA 및 마이크로서비스 기술의 도입으로 효율적인 모바일 네트워크를 구현할 수 있다. 그러나 5G 보안 사양에서 3GPP가 고려한 새로운 특정 보안 요구사항도 야기한다. SBA 보안은 가상화된 구현에 적합한 TLS 및 기타 웹 기반 보안 프로토콜 사용에 의존한다. SBA 보안 사양은 직접 및 간접 통신과 상호인증, 전송 보안 및 인가의 측면을 다룬다. 3GPP SA3 사양은 SBA 보안의 필수 부분을 다루지만, 구현 시 고려해야

할 측면도 존재한다. 인증서의 수, 슬라이싱 사용 및 다양한 NF는 자동화된 인증서 관리가 SBA 보안 구현의 중요한 부분임을 의미한다. 모든 요구사항을 지원할 수 있는 효율적인 PKI는 NF의 구현 및 관리에 중요하다. 또 다른 측면은 잘 설계된 PKI를 통해 여러 업체의 구현을 더욱 쉽게 지원할 수 있다는 것이다. 일반적으로 5G 보안과 관련하여 SBA 보안은 신중하게 정의된 표준, 구현, 배포 및 운영 관리의 조합으로 구성된다. SBA 보안 사양은 새로운 사용 사례, 가상화된 구현에 적합한 보안이 되도록 설계되었다. 사양은 보안의 한 구성요소일 뿐이므로 구현 측면도 필수적으로 고려되어야 한다.

3. 어플리케이션을 위한 인증 및 키 관리 (Authentication and Key Management for Application; AKMA)

네트워크를 활용한 어플리케이션 서비스는 사용자의 삶의 질을 향상시키고 서비스 제공자의 인프라 투자 의욕을 고취시켰다. 안전한 어플리케이션 서비스 사용 환경을 구축하기 위하여 어플리케이션에 접근하는 사용자에 대한 인증이 필수적이다. 어플리케이션 인증 기술인 GBA와 BEST은 네트워크 접근과 어플리케이션 접근에서 인증을 중복으로 실행하고, 5G 네트워크 구조에 적합하지 않다는 문제점이 있다. 이를 위해 3GPP에서 네트워크 초기 접속에서 생성한 3GPP 자격 증명을 기반으로 어플리케이션을 위한 인증 및 키 관리에 대한 표준화를 진행하고 있다. 본 논문에서는 TS 33.535를 중심으로 어플리케이션을 위한 인증 및 키 관리의 동향을 살펴본다.

3GPP는 현재 서드 파티 어플리케이션은 물론 3GPP 서비스에 대하여 5G 시스템에서 지원하는 3GPP 자격증명을 통해 인증 및 키 관리를 지원하기 위하여 AKMA (Authentication and Key Management for Application)를 제안하였다. AKMA는 이전 세대의 이동통신 시스템에서 활용하였던 GBA와 BEST를 확장한 서비스로써 어플리케이션 서버에 접근을 사용자의 셀룰러 가입 정보를 기반으로 하는 인증 및 키 관리 서비스이다. AKMA에 관하여 서술하기 이전에 이전 네트워크에서 동일한 서비스를 제공한 GBA와 BEST에 대하여 분석한다.

GBA는 GBA Bootstrapping과 GBA Bootstrapping Usage로 구성된다. GBA

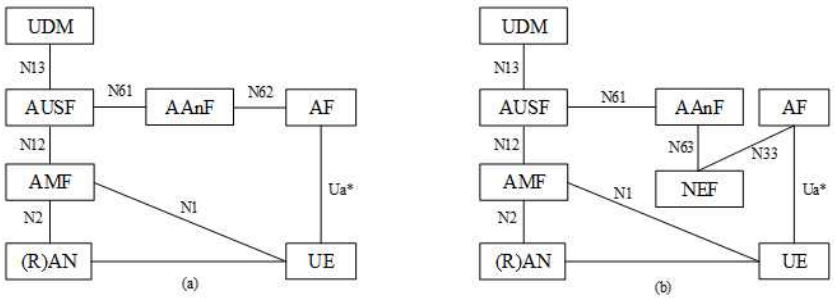
Bootstrapping에서는 UE와 홈 서버의 인증을 위하여 중개자 역할을 수행하는 부트스트랩 서버 기능 (BSF; Bootstrapping Server Function)을 통해 인증 프로토콜을 실행한다. 이를 통해 UE와 BSF는 부트스트랩 키를 공유하게 된다. GBA Bootstrapping을 통해 부트스트랩 키가 공유되면, GBA Bootstrapping Usage가 실행된다. 이 절차에서 UE는 부트스트랩 키를 사용하여 어플리케이션 기능 (NAF; Network Application Function)과의 통신을 보호할 수 있다. UE가 NAF에 임시식별자를 제공하고, NAF는 BSF에게 UE의 임시식별자를 전송하여 세션키 계산을 위임한다. 이를 통해 UE와 NAF는 세션키를 공유하여 통신 채널을 보호할 수 있다. GBA는 SBI (Service-Based Interface)를 지원하지 않았지만 5G가 등장하면서 SBI를 지원할 수 있는 방향으로 개선되고 있다. SBI는 가상화된 네트워크 기능 간 API 기반 통신을 의미하며, 서비스를 호출하기 위하여 SBI를 통한 API 호출을 활용할 수 있다. 그러나 키를 파생하는 절차에서 CK와 IK에서 직접적으로 어플리케이션 키를 파생하고, 초기 인증 이후에 추가적인 AKA (Authentication and Key Agreement) 프로토콜을 실행한다는 점에서 비효율적이다.

BEST는 GBA와 유사하지만, 배터리가 제한된 대기 시간이 긴 저연산 장치에 최적화되어 있다. BEST는 키 교환 서비스와 사용자 평면 보호 서비스를 제공한다. BEST에서 교환되는 모든 메시지는 홈 보안 엔드 포인트 (HSE; Home Security Endpoint)를 통해 라우팅된다. BEST의 사용자 평면 보호 서비스는 UE-to-HSE 모드와 UE-EAS 모드로 구분된다. UE-to-HSE 모드는 UE에서 HSE로 전송되는 사용자 평면 트래픽을 보호하는데 사용되며 UE-EAS 모드는 UE와 EAS (Enterprise Application Server) 사이에 설정된 키를 통해 트래픽을 보호한다. BEST는 SBI를 고려하지 못함과 동시에 5G 네트워크에서 동작할 수 없다. 또한, GBA와 유사하게 어플리케이션 키가 CK와 IK로부터 직접 파생되고, 초기인증 이후 추가적인 인증 절차가 요구된다.

5G 네트워크에서는 인가된 사용자만이 허가된 어플리케이션에 접근할 수 있어야 한다. 이는 어플리케이션 계층에서 사용자 단말에 대한 인증이 필요로 하며, 사용자 단말과 어플리케이션 사이의 토큰, 인증서 혹은 사용자 ID/암호와 같은 자격증명을 기반으로 이루어진다. 3GPP에서는 사용자 단말과 Application 사이의 인증 및 키 교환을 위하여 TS 33.535를 통해 AKMA를 제안하였다. AKMA는 셀룰러, WiFi, 블루투스와 같은 접근 매체와 관계없이 어플리케이션 계층에서 인증 및 키 교환을 지원한다. AKMA에서

어플리케이션 공급자는 AF (Application Function)로 정의되며 사용자에 대한 인증은 HPLMN (Home Public Land Mobile Network)로 위임한다. 여기서 HPLMN은 해당 사용자의 가입 정보가 있는 3GPP 네트워크를 의미한다. 결과적으로 어플리케이션 공급자는 유지 관리해야 할 민감한 사용자 가입 데이터가 감소하고 사용자는 관리해야 할 암호 정보가 줄어든다. AKMA 구조는 기존 5G 네트워크 기능 이외에 추가적으로 AAnF (AKMA Anchor Function)와 AF (Application Function)라는 두 가지 새로운 네트워크 기능을 포함한다. AAnF는 HPLMN (Home Public Land Mobile Network)에서 AKMA를 위한 앵커 기능을 수행하며, 초기인증 절차가 완료되고 AUSF로부터 KAKMA를 부여받아 이를 저장한다. AUSF로부터 부여받은 KAKMA는 차후 키를 파생하는 데 활용된다. AF는 사용자에게 서비스를 제공하는 기능으로써 사용자 단말로부터 접근 요청이 들어오면 AAnF에게 KAF를 부여받아 사용자 단말과의 세션을 구성을 완료한다. TS 33.535에서는 어플리케이션의 위치에 따라 AKMA의 구조를 두 가지로 구분하였으며, 이는 [그림 부록2-33]과 같다.

[그림 부록2-33] AKMA 구조



[그림 부록2-33]의 (a)는 네트워크 내부에서 어플리케이션에 접근하는 시나리오를 나타내며, (b)는 네트워크 외부에서 어플리케이션에 접근하기 위한 시나리오이다. 또한, <표 부록2-7>과 같이 AKMA를 위한 네트워크 요소 및 기능이 정의되었다. 또한, 위의 AKMA 구조 및 요소는 원활한 어플리케이션 관리를 위하여 <표 3-8>와 같은 보안 요구사항 및 원칙을 준수해야 한다.

AKMA에서 사용되는 각 키는 5G 초기인증에서 교환되는 KAUSF를 기준으로

파생된다. AAnF에서 사용되는 키인 KAKMA는 ME와 AUSF가 KAUSF에서 파생하고, AUSF가 AAnF에게 전달한다. 또한, AF에서 사용되는 키인 KAF는 ME와 AAnF가 KAKMA에서 파생하고, AAnF가 AF의 요청에 따라 KAF를 AF에게 전달한다. AKMA 키 계층의 최상단에서 사용되는 KAKMA와 키 식별자 A-KID는 다음 초기인증이 성공할 때까지 암시적으로 유효하며, 초기인증이 수행되면 KAKMA 및 A-KID는 교체된다. KAF는 네트워크 운영 정책에 따른 명시적 수명을 사용하며, AAnF가 KAF를 AF에 같이 전송한다. 새로운 KAKMA가 설정되는 경우에는 기존의 KAF의 수명이 만료될 때까지 사용할 수 있으며, KAF의 수명이 만료되는 경우에는 현재의 KAKMA를 기반으로 새로운 KAF를 파생하여 사용한다. TS 33.535에서 제안된 AKMA의 키 계층은 [그림 부록2-34]과 같다.

<표 부록2-7> AKMA를 위한 네트워크 요소

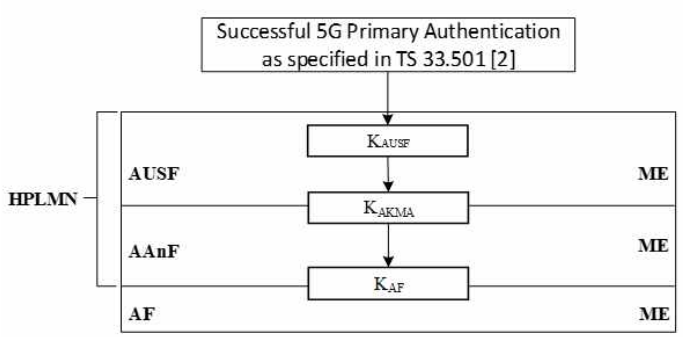
네트워크 요소	기능
AKMA Anchor Function (AAnF)	HPLMN의 앵커 기능 초기인증을 완료하고 AUSF로부터 수신된 KAKMA를 저장 UE와 AF 간 사용할 키 자료를 생성하고 UE AKMA Context를 유지
Application Function (AF)	A-KID (AKMA Key Identifier)를 통해 AAnF로부터 KAF (AKMA Application Key)를 요청 KAF가 제공되기 전에 네트워크에 인증 및 권한 부여 필요 네트워크 내부에 위치한 AF는 AAnF Selection을 수행
Network Exposure Function (NEF)	외부 AF의 활성화 및 승인 외부 AF의 요청을 AAnF에 전달 AAnF Selection 수행
Authentication Server Function (AUSF)	UE의 SUPI 및 AKMA 키 자료 (A-KID, KAKMA)를 AAnF에게 제공
Unified Data Management (UDM)	가입자의 AKMA 가입 데이터를 저장

<표 부록2-8> AKMA 보안 요구사항 및 원칙

요구사항	원칙
일반 요구사항	AKMA는 5G Access에 사용된 동일한 UE 가입 및 자격증명을 재사용해야 함 AKMA는 AKMA 서비스에 대한 암시적 인증을 위하여 3GPP TS 33.501에서 정한 5G 초기인증 절차 및 방법을 재사용해야 함 AAnF와 AUSF 사이의 SBA 인터페이스는 기밀성, 무결성 및 재생으로 보호되어야 함 AAnF와 AF/NEF 사이의 SBA 인터페이스는 기밀성, 무결성 및 재생으로 보호되어야 함 KAF는 최대 수명으로 제공
Ua* 기준점에 대한 요구사항	Ua* 기준점은 어플리케이션에 따라 다름 Ua* 프로토콜은 AKMA 키 식별자 (A-KID)를 전달할 수 있어야 함 UE와 AKMA AF는 KAKMA (AKMA Anchor Key)에서 파생된 KAF (AKMA Application Key)를 사용하여 참조 포인트 Ua*를 확보할 수 있어야 함
AKMA 키 식별자(A-KID)에 대한 요구사항	A-KID는 전 세계적으로 고유함 A-KID는 참조 포인트 Ua*에서 사용되는 프로토콜에서 키 식별자로 사용할 수 있음 AKMA AF는 A-KID로부터 UE를 서비스하는 AAnF를 식별할 수 있어야 함
UE에 대한 요구사항	UE의 어플리케이션은 KAKMA에 접근할 수 없음 UE의 어플리케이션은 어플리케이션에 허가된 특정 AF-ID와 관련된 KAF만 가져와야 함 UE의 어플리케이션은 다른 어플리케이션에 속한 KAF에 접근할 수 없음

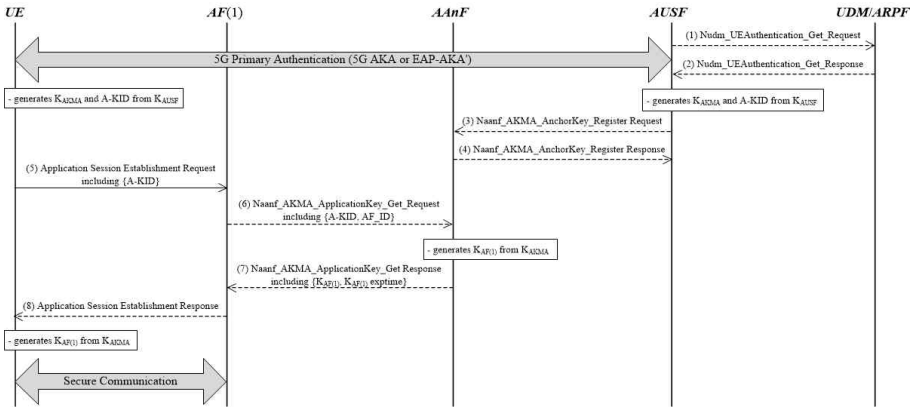
AKMA Reference Point	초기인증 절차를 실행하기 위해 5GC에서 다음 참조점을 재사용함 N1: UE와 AMF 사이의 기준점 N2: (R)AN과 AMF 사이의 기준점 N12: AMF와 AUSF 사이의 기준점 N13: UDM과 AUSF 사이의 기준점 N33: NEF와 외부 AF 사이의 기준점 AKMA 구조는 다음 참조점을 정의함 N61: AAnF와 AUSF 사이의 기준점 N62: AAnF와 내부 AF 사이의 기준점 N63: AAnF와 NEF 사이의 기준점

[그림 부록2-34] AKMA 키 계층



본 논문에서는 3GPP에서 표준화가 진행 중인 AKMA와 이전 세대 네트워크에서 활용된 GBA, BEST에 대하여 분석하였다. GBA와 BEST는 이전 세대의 네트워크에서 사용자와 어플리케이션 사이의 보안 채널을 구성하는 데 활용되었으나 네트워크 접근을 위한 인증 및 키 관리 절차 이외에 추가적인 인증 절차와 인증을 위한 서버 기능이 요구된다. 3GPP는 AKMA를 통해 이러한 GBA와 BEST의 단점을 개선하여 네트워크 초기인증 정보를 활용하여 인증 및 키 관리를 실행한다. [그림 부록2-35]는 TS 33.535에서 정의한 AKMA 절차를 나타낸 것이다.

[그림 부록2-35] AKMA 절차



ⅰ) AUSF는 5G 초기인증 절차 중 Nudm_UEAuthentication_Get Request 메시지를 통해 UE의 가입자 자격증명과 인증정보를 UDM/ARPF에게 요청한다.

ⅱ) UE가 정당한 어플리케이션 사용자라면 UDM/ARPF는 KAKMA 생성 여부를 결정하고, 이에 필요한 정보를 포함하여 Nudm_UEAuthentication_Get Response 메시지를 AUSF에게 전송한다. AUSF는 UDM/ARPF로부터 전달받은 라우팅 식별자를 통해 KAUSF에서 KAKMA와 A-KID를 파생한다. UE 또한 AF와 통신하기 이전에 KAUSF로부터 KAKMA와 A-KID를 파생한다.

ⅲ) AUSF는 AAnF Selection 절차를 통해 UE에게 서비스를 제공할 AAnF를 선정하고, UE의 SUPI와 KAKMA를 Naanf_AKMA_KeyRegistration Request 메시지에 포함하여 전달한다.

ⅳ) AAnF는 UE의 SUPI와 KAKMA를 저장하고, Naanf_AKMA_KeyRegistration Response 메시지를 AUSF에게 전송한다. AUSF는 AAnF와의 통신 이후 AKMA 키 자료를 저장할 필요가 없으며, 재인증이 필요한 경우에는 새로운 AKMA 키 자료를 생성하여 AAnF에게 전송한다.

ⅴ) UE는 AF(1)과의 통신을 개시하기 전에 KAUSF에서 KAKMA와 A-KID를 파생하고, A-KID를 Application Session Establishment Request 메시지에 포함하여 AF(1)에게 전송한다.

ⅵ) AF(1)은 A-KID에 매칭되는 Context를 검색하고, 존재하지 않으면 AAnF Selection을

통해 AAnF를 선택한다. 선택한 AAnF에게 KAF(1)를 요청하기 위하여 UE로부터 전달받은 A-KID와 자신의 ID를 Naanf_AKMA_ApplicationKey_Get_Request 메시지에 포함하여 AAnF에게 전송한다.

vii) AAnF는 AF(1)이 서비스를 제공할 수 있는지 확인하고, 수신한 A-KID를 통해 KAKMA를 식별한다. KAKMA로부터 KAF(1)을 파생하고, KAF(1)의 유효시간을 Naanf_AKMA_ApplicationKey_Get Response 메시지에 포함하여 AF(1)에게 전송한다.

viii) AF(1)은 수신한 KAF(1)을 저장하고, Application Session Establishment Response 메시지를 통해 세션 구성이 완료되었음을 UE에게 알린다.

4. AKMA 개선 연구

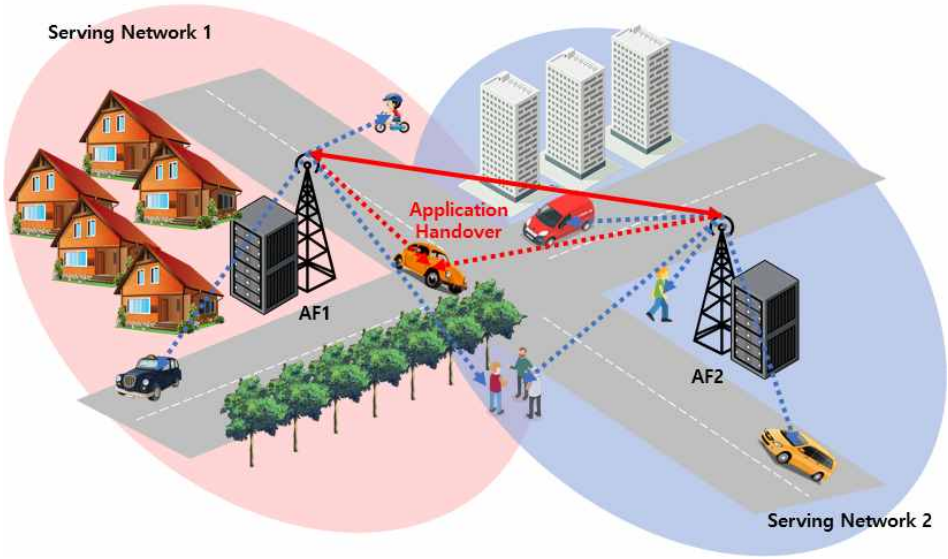
5GB 네트워크에서는 사용자 단말이 지속해서 움직이고 네트워크의 셀이 상대적으로 작다는 것을 고려하면 사용자 단말과 AF 사이의 연결 또한 핸드오버가 일어날 수 있다. 그러나 현재 제안된 AKMA에서는 외부 네트워크에서의 AF 접근 절차를 제외하면 마땅한 핸드오버 절차를 명시하지 않고 있다. 사용자에게 끊김 없는 어플리케이션 서비스를 제공하기 위해서는 안전하고 효율적인 핸드오버 절차가 필수적이다.

5G 초기인증 절차 및 AAnF (AKMA Anchor Function)에게 키를 분배하는 등록 단계와 UE가 AF (Application Function)에 접근하고 보안 채널을 구성하는 초기 접근 단계, UE의 이동 혹은 네트워크 상황에 따라 서빙 네트워크가 변경되는 경우에서 UE에게 서비스를 제공하는 AF가 전환되는 어플리케이션 핸드오버 단계로 구성된다. 제안하는 프로토콜은 3GPP TS 33.535를 기반으로 설계되었으며, 5G 시스템에서 3GPP 자격증명 기반의 어플리케이션 인증 및 키 관리는 물론 핸드오버를 지원하는 것을 목표로 한다. 제안하는 프로토콜의 대상 환경인 어플리케이션 서비스 핸드오버 시나리오는 [그림 부록2-36]과 같다.

[그림 부록2-36]에서는 Serving Network 1에서 차량 내비게이션과 같은 어플리케이션 서비스를 제공받는 사용자가 AF1과 통신하고 있다. 이때, 사용자가 Serving Network 2로 이동하게 되면서 핸드오버 상황이 발생한다. 여기서 어플리케이션 서비스 핸드오버

를 제공하면 최소한의 지연으로 사용자에게 끊김 없는 서비스를 제공할 수 있다. 제안 프로토콜에서 사용되는 기호는 <표 부록2-9>와 같다.

[그림 부록2-36] AKMA 절차



제안하고자 하는 어플리케이션 서비스 핸드오버 보안 프로토콜은 사용자에게 끊김 없는 서비스를 제공하고 사용자의 통신 및 데이터를 보호해야 한다. 그러나 앞서 제안한 프로토콜들과 동일하게 개방된 환경에서의 무선 통신을 활용한다. 이로 인해 UE와 AF 사이의 통신 채널을 완전히 신뢰할 수 없으며 언제든지 공격자가 네트워크 통신 및 데이터의 탈취 혹은 악성 데이터 주입과 같은 공격을 시도할 수 있다. 따라서 제안하는 어플리케이션 서비스 핸드오버 보안 프로토콜은 위와 같은 공격자의 존재를 상정하고 설계될 필요가 있으며, 이를 위해 Dolev-Yao 위협 모델을 참고하였다.

<표 부록2-9> 기호 정리

기호	의미
UE	사용자 단말
AF	어플리케이션 기능
AAnF	AKMA 앵커 기능
AUSF	인증 서버 기능
IDX	X의 식별자
AIDX-Y	X와 Y 사이에서 사용되는 익명 식별자
KX	X의 키
KAKMA	UE와 AAnF 사이의 키
KAF	UE와 AF 사이의 키
X, Y	ECDH 개인 키
Seq	순서 번호
nX	x번째 임시 값
SK	세션 키
HM	메시지 인증 코드

Dolev-Yao 위협 모델은 사용자의 통신 및 데이터가 공개된 채널을 사용하기 때문에 발생하는 위협을 다룬다. Dolev-Yao 위협 모델을 고려하면 통신 참여자는 인증 및 키 교환 절차를 통해 보안 채널을 설정하고 메시지를 보호해야 한다. 이를 위해 제안하는 프로토콜은 아래 보안 요구사항을 충족해야 한다. 제안하는 프로토콜에 대한 가정은 아래와 같다.

ⅰ) AF(1)과 AF(2), AAnF, AUSF, UDM/ARPF는 적절한 공유 키를 통해 각 개체 간 보안 채널을 구성하고 있다.

ⅱ) AF는 각 서빙 네트워크의 기지국에 위치하고 있으며, AAnF는 네트워크 코어에 위치하고 있다.

ⅲ) AF는 UE의 이동에 따라 적절히 핸드오버 대상을 결정하여 UE의 Context를 전달할 수 있다.

ⅳ) AF는 UE와 ECDH 키 교환을 위한 적절한 ECDH 도메인 파라미터를 공유하고 있다.

대상 네트워크 환경의 보안 요구사항은 다음과 같다.

ⅰ) 상호인증 : 제안하는 보안 프로토콜의 통신 참여자는 서로를 인증해야 한다.

ⅱ) 기밀성 : 승인되지 않은 참가자는 승인된 참가자 사이에서 전송된 메시지를 읽을 수 없다.

ⅲ) 무결성 : 승인되지 않은 참가자는 승인된 참가자 사이에서 전송된 메시지를 변경할 수 없다.

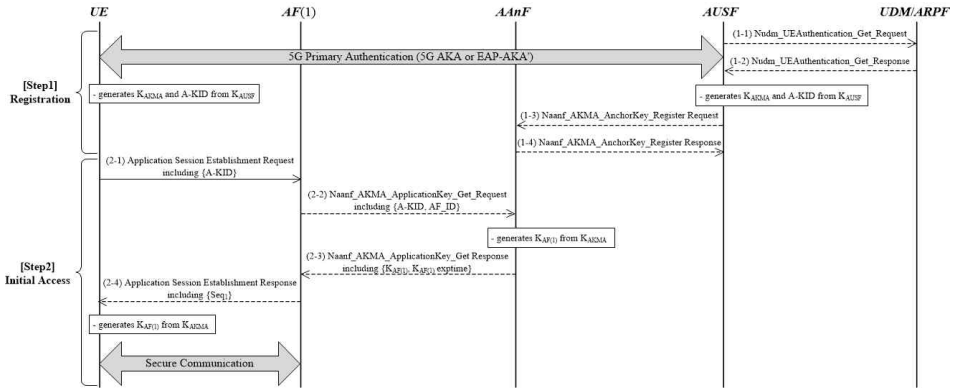
ⅳ) 안전한 키 교환 : 제안하는 보안 프로토콜이 수행되면 프로토콜의 참가자들 사이의 인증키와 암호키가 안전하게 협상이 이뤄져야 한다.

ⅴ) 완전 순방향 비밀성 : 제안하는 프로토콜의 현재 세션 키는 어떠한 방법으로도 과거 키에서 파생되어서는 안 된다.

ⅵ) 익명성: 제안하는 프로토콜은 익명 식별자를 사용하여 서비스 사용자의 식별자가 공개되지 않아야 한다.

제안하는 프로토콜은 등록 단계, 초기 접근 단계, 어플리케이션 핸드오버 단계의 3단계로 구성된다. 등록 단계에서는 5G 초기인증 절차를 통해 UE와 AUSF 사이의 비밀키 KAUSF를 생성하고, UDM/ARPF로부터 UE의 어플리케이션 사용에 대한 허가를 받는다. 또한, UE의 어플리케이션 사용이 승인되면 UE와 AUSF는 비밀키 KAUSF로부터 KAKMA와 A-KID를 파생하고, AAnF는 AUSF로부터 KAKMA를 분배를 받는다. 초기 접근 단계에서는 UE가 Ua* 기준점을 통해 AF에 접근하고, 보안 채널을 구성하기 위한 KAF를 파생하는 일련의 절차를 의미한다. 제안하는 프로토콜의 등록 및 초기 접근 단계의 절차는 [그림 부록2-37]과 같다.

[그림 부록2-37] 등록 및 초기 접근 단계



i-1) AUSF는 5G 초기인증 절차 중 Nudm_UEAuthentication_Get Request 메시지를 통해 UE의 가입자 자격증명과 인증정보를 UDM/ARPF에게 요청한다.

i-2) UE가 정당한 어플리케이션 사용자라면 UDM/ARPF는 KAKMA 생성 여부를 결정하고, 이에 필요한 정보를 포함하여 Nudm_UEAuthentication_Get Response 메시지를 AUSF에게 전송한다. AUSF는 UDM/ARPF로부터 전달받은 라우팅 식별자를 통해 KAUSF에서 KAKMA와 A-KID를 파생한다. UE 또한 AF와 통신하기 이전에 KAUSF로부터 KAKMA와 A-KID를 파생한다. UE와 AUSF가 파생하는 A-KID는 KAKMA를 인식하기 위한 식별자이며 IETF RFC 7542 [97]에서 지정한 형식에 따라 'username@realm'으로 구성된다. username 부분은 라우팅 식별자와 A-TID로 realm 부분은 Home Network Identifier로 이루어진다. username 부분의 A-TID는 KAUSF에서 파생된다.

i-3) AUSF는 AAnF Selection 절차를 통해 UE에게 서비스를 제공할 AAnF를 선정하고, UE의 SUPI와 KAKMA를 Naanf_AKMA_KeyRegistration Request 메시지에 포함하여 전달한다.

i-4) AAnF는 UE의 SUPI와 KAKMA를 저장하고, Naanf_AKMA_KeyRegistration Response 메시지를 AUSF에게 전송한다. AUSF는 AAnF와의 통신 이후 AKMA 키 자료를 저장할 필요가 없으며, 재인증이 필요한 경우에는 새로운 AKMA 키 자료를 생성하여 AAnF에게 전송한다.

ii-1) UE는 AF(1)과의 통신을 개시하기 전에 KAUSF에서 KAKMA와 A-KID를 파생하고, A-KID를 Application Session Establishment Request 메시지에 포함하여 AF(1)에게 전송한다.

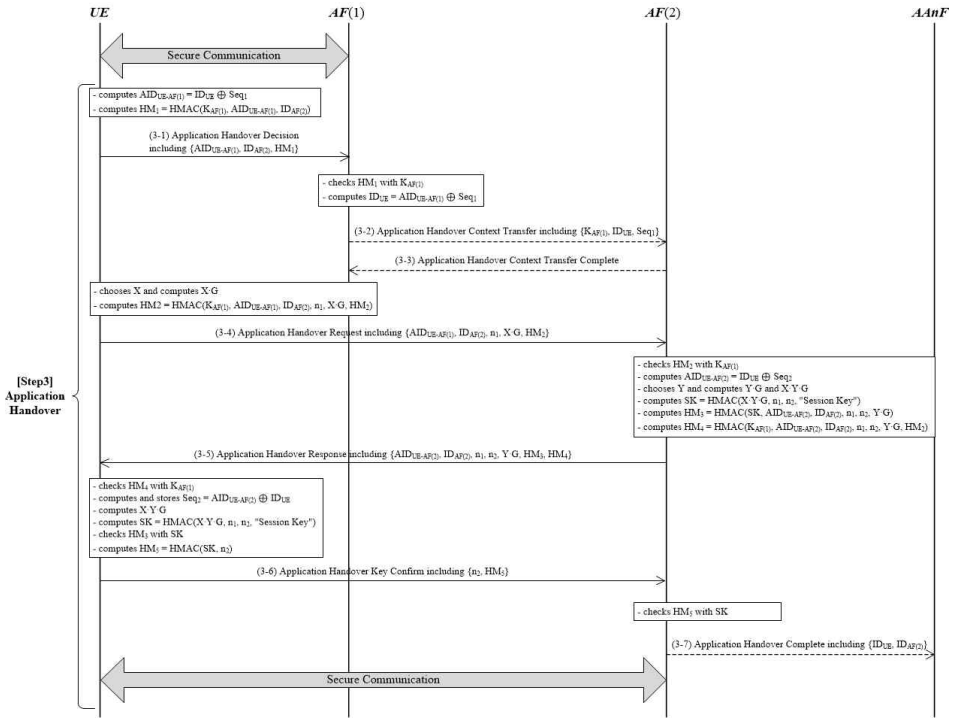
ii-2) AF(1)은 A-KID에 매칭되는 Context를 검색하고, 존재하지 않으면 AAnF Selection을 통해 AAnF를 선택한다. 선택한 AAnF에게 KAF(1)를 요청하기 위하여 UE로부터 전달받은 A-KID와 자신의 ID (AF_ID)를 Naanf_AKMA_ApplicationKey_Get_Request 메시지에 포함하여 AAnF에게 전송한다.

ii-3) AAnF는 AF(1)이 서비스를 제공할 수 있는지 확인하고, 수신한 A-KID를 통해 KAKMA를 식별한다. KAKMA로부터 KAF(1)을 파생하고, KAF(1)의 유효시간을 Naanf_AKMA_ApplicationKey_Get Response 메시지에 포함하여 AF(1)에게 전송한다.

ii-4) AF(1)은 수신한 KAF(1)을 저장하고, Application Session Establishment Response 메시지를 통해 세션 구성이 완료되었음을 UE에게 알린다. 이때, 핸드오버 단계에서 익명 식별자를 생성할 수 있도록 순서 번호 Seq1을 메시지에 포함하여 전송한다. UE는 KAKMA에서 KAF(1)을 파생하고, 순서 번호 Seq1을 저장한다.

제안하는 프로토콜의 핸드오버 단계는 네트워크 상황에 따라 Push 기법과 Pull 기법의 두 가지로 구분된다. Push 기법과 Pull 기법은 핸드오버가 일어나기 전까지의 절차는 동일하며, 핸드오버 단계에서 UE의 Context가 전달되는 순서에 따라 구분된다. 우선, Push 기법은 UE가 이동하기 전에 핸드오버를 결정하고, 핸드오버에 필요한 Context를 AF(2)에게 전송하도록 AF(1)에게 요청한다. 이후, AF(2)는 AF(1)로부터 받은 Context를 기반으로 UE와 인증 및 키 교환을 진행한다. 제안하는 프로토콜의 핸드오버 단계 (Push 기법)는 [그림 부록2-38]와 같다.

[그림 부록2-38] 핸드오버 단계 (Push 기법)



iii-1) UE는 핸드오버 상황을 감지하고, 익명 식별자 AIDUE-AF(1)와 핸드오버 대상 AF의 식별자 IDAF(2)를 Application Handover Decision 메시지에 포함하여 AF(1)에게 전송한다. 이때, Application Handover Decision 메시지는 UE와 AF(1) 사이의 비밀키 KAF(1)을 통해 생성한 메시지 인증 코드 HM1에 의해 무결성이 보호된다.

iii-2) AF(1)은 수신한 Application Handover Decision 메시지의 HM1을 검증한다. HM1이 유효하면, AIDUE-AF(1)와 Seq1를 통해 UE의 ID (IDUE)를 복원한다. 이후, KAF(1)과 IDUE, Seq1을 Application Handover Context Transfer 메시지에 포함하여 AF(2)에게 안전한 채널을 통해 전송한다.

iii-3) AF(2)는 수신한 KAF(1)과 IDUE, Seq1을 저장하고 이에 대한 응답으로 Application Handover Context Transfer Complete 메시지를 AF(1)에게 전송한다.

iii-4) UE가 이동하여 AF(2)와 연결되면, UE는 임시값 n1과 ECDH 개인 키 X, 공개키

X·G를 생성한다. 이후, AIDUE-AF(1)와 IDAF(2), n1, X·G를 Application Handover Request 메시지에 포함하여 AF(2)에게 전송한다. 이때, Application Handover Request 메시지는 KAF(1)을 통해 생성한 HM2에 의해 무결성이 보호된다.

iii-5) AF(2)는 Application Handover Request 메시지를 수신하고, 먼저 HM2와 AIDUE-AF(1)를 검증한다. HM2와 AIDUE-AF(1)가 모두 유효하면, Seq2와 임시값 n2를 생성하고, 새로운 세션에서 사용할 익명 식별자 AIDUE-AF(2)를 계산한다. 이후, ECDH 개인 키 Y와 공개키 Y·G를 생성하고, UE의 ECDH 공개키 X·G와 자신의 개인 키 Y를 통해 세션 키 X·Y·G를 유도한다. 유도한 ECDH 세션 키 X·Y·G와 n1, n2를 통해 UE와 AF(2)의 세션 키 SK를 파생한다. AF(2)는 키 파생을 마치고 새로운 익명 식별자 AIDUE-AF(2)와 자신의 식별자 IDAF(2), 임시값 n1, n2, ECDH 공개키 Y·G를 Application Handover Response 메시지에 포함하여 UE에게 전송한다. Application Handover Response 메시지는 세션 키 SK와 KAF(1)를 통해 보호되는 HM3와 HM4으로 무결성을 보장할 수 있다.

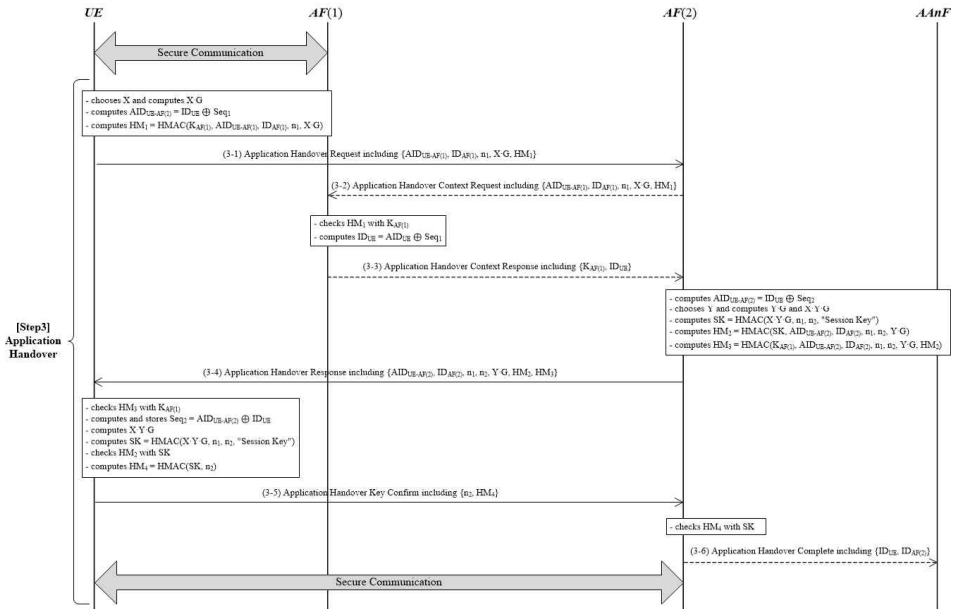
iii-6) UE는 Application Handover Response 메시지에 포함된 HM4를 검증하고, 새로운 익명 식별자 AIDUE-AF(2)와 자신의 식별자 IDUE를 통해 다음 순서 번호 Seq2를 구한다. 이후, AF(2)의 ECDH 공개키 Y·G와 자신의 ECDH 개인 키 X를 통해 ECDH 세션 키 X·Y·G를 유도한다. 유도된 ECDH 세션 키와 임시값 n1, n2에서 UE와 AF(2)의 세션 키 SK를 파생할 수 있다. SK를 통해 나머지 메시지 인증 코드인 HM3을 검증하여 메시지의 무결성을 확인할 수 있다. 메시지에 대한 검증이 완료되면 UE는 AF(2)를 인증할 수 있다. UE는 AF(2)에 대한 인증을 완료하고, 세션 키 확인 절차를 위하여 임시값 n2와 SK로 보호되는 HM5를 Application Handover Key Confirm 메시지에 포함하여 AF(2)에게 전송한다.

iii-7) AF(2)는 Application Key Confirm 메시지에 포함된 HM5를 검증하여 UE에 대한 인증과 세션 키가 정상적으로 교환되었는지 확인한다. 또한, Application Handover Complete 메시지를 통해 UE와의 핸드오버가 정상적으로 종료되었음을 AAnF에게 보고한다.

Push 기법과는 반대로 Pull 기법은 UE가 AF(2)로 이동하면, AF(2)에게 AF(1)로부터

Context를 요청하도록 유도한다. AF(2)는 AF(1)로부터 전달된 Context에 기반을 둔 UE와의 인증 및 키 교환을 진행한다. [그림 부록2-39]는 Pull 기법을 활용한 핸드오버 절차를 나타낸 것이다.

[그림 부록2-39] 핸드오버 단계 (Pull 기법)



iv-1) UE는 AF(2)가 포함된 네트워크로 이동하면, ECDH 개인 키 X와 공개키 X・G, 임시값 n1, 익명 식별자 AIDUE-AF(1)를 생성한다. 그리고 AIDUE-AF(1)와 이전에 접속한 AF(1)의 식별자 IDAF(1), 임시값 n1, ECDH 공개키 X・G, 비밀키 KAF(1)을 통해 생성한 메시지 인증 코드 HM1을 Application Handover Request 메시지에 포함하여 AF(2)에게 전송한다.

iv-2) AF(2)는 UE로부터 수신한 Application Handover Context Request 메시지를 AF(1)에게 전달한다.

iv-3) AF(1)은 Application Handover Context Request 메시지에서 HM1을 검증하고, AIDUE-AF(1)에서 IDUE를 추출한다. 이를 통해 이전에 접속했던 UE임을 확인하면,

UE와의 비밀키 KAF(1)과 UE의 식별자 IDUE를 AF(2)에게 안전한 채널을 통해 전송한다.

ⅳ-4) KAF(1)과 IDUE를 획득한 AF(2)는 ECDH 개인 키 Y와 공개키 Y・G, 임시값 n2를 생성하고, 3-1에서 수신한 UE의 ECDH 공개키 X・G를 통해 ECDH 세션 키 X・Y・G를 계산한다. ECDH 세션 키 X・Y・G와 임시값 n1, n2로 UE와 AF(2) 사이의 세션 키 SK를 파생한다. 또한, IDUE와 다음 순서 번호 Seq2를 조합해 새로운 익명 식별자 AIDUE-AF(2)를 계산한다. 모든 계산이 완료되면, AF(2)는 AIDUE-AF(2)와 IDAF(2), n1, n2, Y・G가 포함된 Application Handover Response 메시지를 작성하고, 해당 메시지를 보호하기 위하여 각각 SK와 KAF(1)으로 생성한 메시지 인증 코드 HM2와 HM3를 메시지에 추가하여 UE에게 전송한다.

ⅳ-5) UE는 우선 KAF(1)을 통해 HM3를 검증하고, 수신한 AIDUE-AF(2)와 보유한 IDUE로 새로운 순서 번호 Seq2를 도출하여 저장한다. AF(2)의 ECDH 공개키 Y・G를 통해 ECDH 세션키 X・Y・G를 파생하고, X・Y・G와 n1, n2로 AF(2)와의 세션키 SK를 유도하여 HM2를 검증한다. 모든 메시지 인증 코드가 유효하면 UE는 AF(2)를 인증할 수 있으며, 세션 키 SK를 신뢰할 수 있다. UE는 키 확인 절차를 위하여 n2와 SK로 생성한 HM4를 Application Handover Key Confirm 메시지에 포함하여 AF(2)에게 전송한다.

ⅳ-6) AF(2)는 SK를 통해 HM4를 검증함으로써 UE를 인증하고, SK를 신뢰할 수 있다. 또한, AF(2)는 UE와의 핸드오버 절차가 완료되었음을 AAnF에게 보고하기 위하여 IDUE와 IDAF(2)를 포함하는 Application Handover Complete 메시지를 전송한다.

5. AKMA 개선 프로토콜의 정형화 검증

제안하는 보안 프로토콜의 보안성을 입증하기 위하여 정형화 검증을 수행한다. 제안하는 핸드오버 보안 프로토콜은 등록 단계, 초기 접근 단계, 핸드오버 단계로 구성되어 있으나 등록 단계와 초기 접근 단계는 5G 초기인증 및 식별자 교환, 키 계층에 따른 키 파생만 이루어지기 때문에 정형화 검증의 대상인 암호화 알고리즘을 통해 보호되는 메시지가 존재하지 않는다. 따라서 본 고에서는 핸드오버 단계의 Push 기법과 Pull 기법에 대하여 검증한다.

본 고에서는 프로토콜 검증을 위하여 Scyther를 사용하였다. Scyther는 자동화된 정형화 검증 도구로서 Cas J. F. Cremers에 의해 제안되었다. Scyther의 검증은 ⅰ) 모델링, ⅱ) 검증, ⅲ) 결과의 3단계로 구성된다. 우선, 모델링에서 검증 대상인 보안 프로토콜은 Scyther의 고유한 스크립트 언어인 SPDL (Security Protocol Description Language)로 각 절차를 모델링된다. 기본적으로 SPDL은 보안 프로토콜의 각 참여자에 대한 역할을 정의하고, 프로토콜에서 교환되는 모든 메시지를 명세해야 한다.

SPDL로 작성된 프로토콜 모델은 크게 전역 변수 선언, 프로토콜 정의, 개별 역할 정의 순서로 이루어진다. 전역 변수 선언은 프로토콜에서 공통적으로 사용되는 Agent, 사용자 정의 함수, 매크로 등이 선언되고, 프로토콜 정의에서는 개별 역할을 포함하는 프로토콜 동작이 정의된다. 프로토콜 정의는 단일 프로토콜뿐만 아니라 필요에 따라 병렬 프로토콜을 정의할 수 있다. 마지막으로 개별 역할 정의는 프로토콜 통신 참여자의 행위를 정의하는 것으로 지역변수를 선언하고, send와 recv로 구성된 통신 메시지, 보안 프로토콜의 검증을 위한 claim event를 포함한다.

제안하는 프로토콜의 어플리케이션 핸드오버 단계는 Push 기법과 Pull 기법으로 구분되기 때문에 각각 SPDL 기반의 모델링을 진행하였다. 제안하는 프로토콜의 검증 결과는 각각 [그림 부록2-40]의 (a), (b)과 같으며, 결과에 따르면 제안하는 프로토콜의 핸드오버 단계의 Push 기법과 Pull 기법은 알려진 공격에 대하여 안전함을 확인할 수 있다.

[그림 부록2-40] Scyther 검증 결과

(a) (b)

저 자 소 개

유 일 선

· 단국대 전산통계학과 졸업
· 단국대 전산학과 석사
· 단국대 전산학과 박사
· 규슈대 정보보호학과 박사
· 현 국민대학교 정교수

○ ○ ○

· ○○대 ○○학과 졸업
· ○○대 ○○학과 석사
· 현 정보통신기획평가원 선임연구원

○ ○ ○

· ○○대 ○○학과 졸업
· ○○대 ○○학과 석사
· ○○대 ○○학과 박사
· 현 정보통신기획평가원 책임연구원

방송통신정책연구 RS-2022-00156261

0000 000 0000에 따른 0000 연구

2020년 00월 일 인쇄
2020년 00월 일 발행

발행인 과학기술정보통신부 장관
발행처 과학기술정보통신부
세종 가름로 194 세종파이낸스센터
Homepage: www.msit.go.kr