6G 환경을 고려한 트러스트 모델 및 지능형 침입 탐지 기술 동향

Study on Trusted Models and Intelligent Intrusion Detection Systems for 6G Mobile Networks

박철희 (C.H. Park, chpark0528@etri.re.kr) 인공지능데이터보안연구실 연구원
박경민 (K.M. Park, kmpark@etri.re.kr) 인공지능데이터보안연구실 선임연구원
송지현 (J.H. Song, dmon95@etri.re.kr) 인공지능데이터보안연구실 학생연구원
김종현 (J.H. Kim, jhk@etri.re.kr) 인공지능데이터보안연구실 책임연구원
김수형 (S.H. Kim, lifewsky@etri.re.kr) 인공지능데이터보안연구실 책임연구원/실장

ABSTRACT

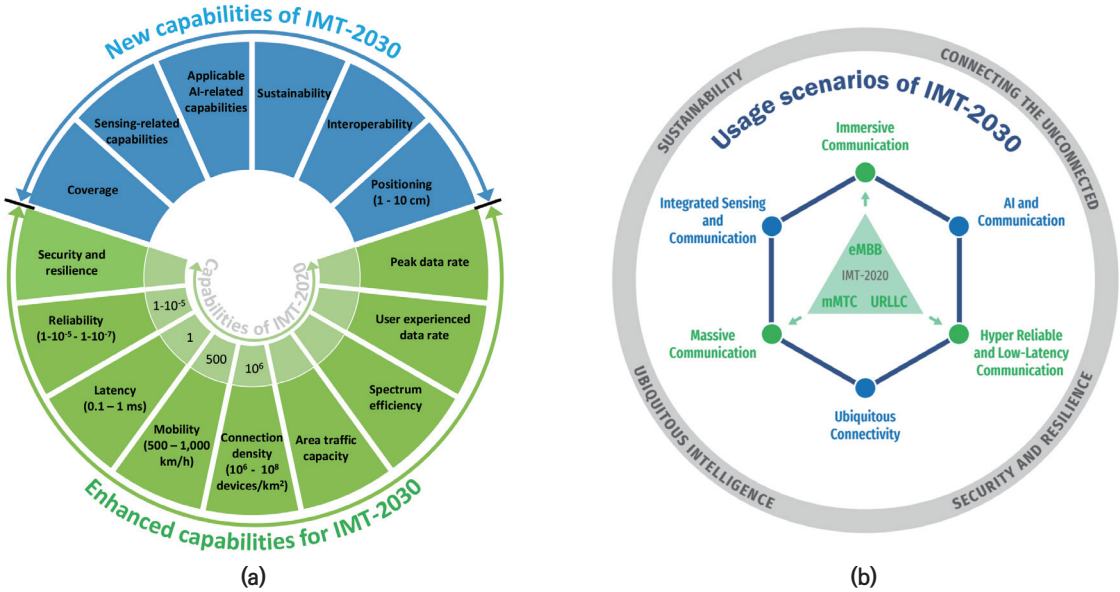
The advent of 6G mobile communication technologies promises to surpass the capabilities of existing 5G by offering ultra high-speed data transmission, ultra low latency, and extensive connectivity, enabling a new wave of digital transformation across various fields. However, the openness and decentralized nature of 6G systems, which enhance their flexibility and scalability, can expand the attack surface and increase security threats from cyber-attacks. In this article, we analyze the current research trends related to security in the 6G mobile communication landscape.

KEYWORDS 6G security, 6G trustworthy, intelligent security, network security

Ⅰ. 서론

이동통신 기술의 발전에 따라 사회 전반에 걸쳐 새로운 비즈니스 모델이 등장하고 있으며, 다양한 응용 서비스를 기반으로 디지털 전환이 가속화되고 있다. 현재 이동통신 기술은 5G를 넘어 6G에 대한 연구가 활발히 진행되고 있으며, 차세대 이동통신 시스템에서는 구조적 및 환경적 변화가 예상됨에 따라 새로운 융합 서비스와 산업 혁신이 기대되고 있다. 특히, 국제전기통신연합(ITU: International Telecommunication Union)은 2023년 6G 비전 권고안을 발표하여 증강현실, 초저지연 통신, 광범위한 연결성, 지능형 네트워크 등 차세대 이동통신 기술에 대한 다양한 핵심 성능 지표와 목표 서비스를 제시하였다[1](그림 1 참고). 이를 통해 6G는 더욱 진보된 산업 자동화, 원격 의료, 스마트 시티 등 다양한 응

* DOI: https://doi.org/10.22648/ETRI.2024.J.390508
* 이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임[No. RS-2024-00444170, 6G 개방형 네트워크 환경에서 트러스트 모델 기반 지능형 침해대응 기술 연구 및 국제협력].



출처 Reprinted with Permission from ITU-R Working Party 5D, IMT-2030 6G Vision, 2023. 6. [1].

그림 1 IMT-2030 6G 비전 권고안의 핵심 성능지표 및 목표 서비스: (a) Capabilities of IMT-2030, (b) Usage Scenarios

용 분야에서 혁신을 이끌 핵심 기술이 될 것으로 기대된다. 한편, 6G 이동통신 기술은 개방형 플랫폼을 기반으로 지능화 및 분산화될 것으로 예상됨에 따라 공격 접점이 확대될 우려가 제기되고 있으며, 보안 기술의 중요성이 강조되고 있다. 특히, IMT-2030의 6G 비전 권고안에서는 보안, 프라이버시, 복원력을 핵심 성능 지표로 다루고 있으며, 6G 이동통신의 환경변화를 고려한 강화된 보안 기술과 인공지능 기반의 지능형 보안 기술에 대한 중요성을 강조하고 있다.

6G 이동통신 환경에서는 테라헤르츠(THz) 대역의 초고주파수를 활용하여 기존 5G 이동통신보다 더욱 빠른 속도와 초저지연 등을 바탕으로 새로운 서비스를 제공할 수 있을 것으로 기대된다. 이러한 요구를 충족하기 위해 차세대 이동통신 환경은 AI 기반의 지능형 네트워킹을 통해 에너지 효율성을 최대화하고, 소형 셀과 분산형 네트워크 인프라를 통해 에너지 소비를 최적화하는 것을 목표로 네트워크 구조와 환경이 변화될 것으로 예상된다. 특히, 네트워크 인프라의 개방화와 6G 환경을 고려한 분산 AI 기술은 차세대 이동통신의 핵심 기술이 될 것으로 예상된다. 그러나, 이러한 구조적/환경적 변화에 따라 악의적인 공격자의 공격 표면이 확대될 우려가 제기되고 있으며, 새로운 기술 및 인프라의 도입으로 인한 보안 취약점에 대한 우려가 제기되고 있다. 이러한 문제를 해결하기 위해 기존의 이동통신 보안 기술을 고려할 수 있으나, 네트워크 구조 및 환경의 변화를 충분히 반영하지 못한다는 문제가 있으며, 기존 보안 기술을 그대로 적용하기에는 한계가 있다.

본고에서는 6G 환경을 고려한 차세대 이동통신 환경에서의 보안 기술 연구 동향을 분석하고, 향후 6G 이동통신 보안 기술 개발 방향을 제시한다. 특히, 6G 환경에서의 트러스트 모델을 고려하여 DLT 기반의 트러스트 보장 기술과 DPKI 기반의 차세대 인증 기술 동향에 대해 분석하고, 개방형 무선 인프라 환경을 고려하여 Open RAN 보안 기술 동향을 분석한다. 또한, 6G 환경에서 분산 AI 기술 연구 동

향을 분석하고 분산 AI 기반의 지능형 네트워크 보안 기술에 대해 분석한다.

II. 6G 이동통신과 보안

6G 이동통신 기술은 5G와 비교하여 더욱 빠른 데이터 속도와 넓은 대역폭을 제공하고, 초저지연 및 확장된 연결성을 가능하게 할 것으로 예상된다. 또한, 인공지능 기술을 활용한 지능형 네트워크 기술은 세분화 및 분산화된 네트워크의 효율성과 성능을 극대화할 것으로 기대된다. 최근, 이러한 6G 네트워크의 환경을 고려한 연구가 활발히 수행되고 있으며, 이동통신 환경변화에 따른 보안 및 프라이버시에 대한 중요성이 강조되고 있다. 특히, 6G 환경에서는 글로벌 커버리지와 광범위한 AI를 통해 '연결된 지능'이 실현될 것으로 기대되고 있으며, '네트워크 지능화'와 '서브-네트워크의 네트워크(Network of Sub-Networks)'의 실현이 전망되고 있다[2]. 이러한 환경변화에 따라 데이터 보안과 프라이버시에 대한 중요성이 강조되고 있으며, 양자암호 기술, 블록체인 기술, 강건한 AI 학습 기술, 그리고 물리 계층 보안(Physical Layer Security) 등은 6G 보안의 주요 기술로 분류되고 있다[3].

최근, 핀란드 오울루 대학의 Mika Ylianttila 연구진은 6G 보안 관련 백서를 통해 이동통신 환경 변화에 따른 신뢰 네트워킹의 중요성을 강조하였으며, 6G 이동통신 환경 변화에 적합한 네트워크 보안 아키텍처와 AI 기반의 지능형 네트워크 보안 기술의 중요성을 강조하였다[4,5]. 또한, 테라헤르츠 통신 및 가시광 통신과 같은 새로운 기술의 도입과 더불어, 물리 계층 취약성은 6G의 새로운 보안 위협으로 분류되고 있으며, AI 기반의 지능형 네트워크 기술의 도입과 더불어 프라이버시 보존형 AI 학습 기술 및 AI 시스템의 투명성과 신뢰성을 보장하기 위한 XAI에 대한 중요성이 강조되고 있다[6,7].

6G 이동통신 환경은 테라헤르츠 통신, 광범위한 AI, 개방형 무선통신 등 새로운 기술의 도입을 예고하고 있으며, 이에 따라 신뢰성 보장과 보안 및 프라이버시에 대한 중요성이 강조되고 있다. 본고에서는 이러한 이동통신의 환경 변화를 고려하여 포괄적인 6G 이동통신 신뢰 모델, 개방형 무선통신 환경에서의 보안 기술, 그리고 광범위한 AI 기술을 고려한 분산 AI 기반의 네트워크 보안 기술에 대한 연구 동향을 분석한다.

III. 6G 트러스트 모델 연구 동향

6G 이동통신 환경은 5G와 비교하여 더욱 개방적이고 분산화된 기능들이 적용될 것이다. 이와 같은 6G의 변화는 기존에는 고려되지 않았던 새로운 사이버 보안 위협에 대한 공격 표면을 드러나게 할 것이다. 따라서 6G 이동통신 환경이 도입되기 전에 6G의 환경과 생태계를 합리적으로 예측하고 그에 적합한 신뢰성 보장 기술에 대한 연구가 선행되어야 한다.

본 장에서는 6G 이동통신 환경에 대한 신뢰성 확보 및 6G 기반의 안전한 이동통신 서비스 제공을 목표로 하는 6G 트러스트 모델 연구의 국내외 동향을 소개한다.

1. 6G Flagship

유럽연합은 2018년부터 6G 생태계 조성을 목표로 핀란드 오울루 대학을 중심으로 6G Flagship 프로젝트를 진행 중이다. 6G Flagship에서는 6G와 관련된 통신 및 네트워크, 인공지능, 비즈니스 모델 등의 핵심 분야에 대한 비전을 제시해왔으며, 최근에는 안전한 6G 인프라 및 서비스 제공을 위한 6G 트

러스트 모델에 대한 비전을 담은 백서를 발간하였다[4]. 이 백서에서는 다가올 6G 시대에는 사용자 또는 수많은 이기종 장치들이 현재보다 더욱 정보통신 기술 및 네트워크에 대한 의존이 커질 것이기 때문에 초신뢰성이 보장되는 6G 환경에 관한 연구 필요성이 제기되었다. 더불어, 신뢰성 있는 6G를 위해 필요한 4가지 도전과제로서, (1) 6G 환경에 특화된 트러스트 네트워킹, (2) 양자암호 기반의 네트워크 보안 아키텍처, (3) 6G 무선 접속망의 특성을 고려한 물리 계층 보안 기술, (4) 초연결 서비스에 필요한 프라이버시 보호 기술을 강조하고 있다.

2. 화웨이

세계적인 이동통신 장비 제조 업체인 화웨이는 2022년 12월에 발간된 “6G Native Trustworthiness” 백서를 통해 6G에서의 신뢰성 있는 인프라 제공을 위해 블록체인 기술을 활용한 다자간 트러스트 모델의 구축을 제안하였다[8]. 6G에서는 5G와 비교하면 네트워크 기능이 더욱 분산화되고 서비스는 사용자 중심으로 진화할 것이기 때문에 이러한 변화의 흐름에 대비하여 통신, 네트워크, 서비스, 개인화 등을 아우르는 포괄적인 6G 신뢰 모델의 필요성이 제시되고 있다.

화웨이는 중앙집중형 네트워크 아키텍처에 어울리는 5G 보안 아키텍처와는 달리 분산 네트워크를 제공하고 기존의 보안 아키텍처와도 호환되는 6G 네트워크를 구축하려면 새로운 보안 아키텍처 설계 개념이 필요함을 강조하면서 Bridge, Consensus, Endorsement 개념으로 구분되는 다자간 신뢰 모델을 제시하였다.

제시된 모델의 Bridge 모드에서는 인증 기관이 A, B 두 객체를 각각 인증하고 두 객체는 상호 신뢰 관계를 형성한다. Endorsement 모드는 제3자가 두 객체의 신뢰성을 평가하도록 하고 있으며, 각 객체에 대한 평가 결과를 서로 다른 객체에 전달하여 신뢰를 검증한다. Consensus 모드는 블록체인의 합의 알고리즘과 유사하게 네트워크에 참여하고 있는 모든 객체의 신뢰 정보가 네트워크 전체에 분산된 구조이다. Consensus 모드에서의 객체는 네트워크 객체, 서비스 제공자, 인프라 공급자, 사용자 등 6G 생태계를 구성하는 모든 구성요소다. Consensus 모드에서의 신뢰 검증에 대한 책임은 모든 참여자 간에 공유되어 있으므로 신뢰성 보장에 대한 높은 효율성과 확장성을 제공한다.

화웨이는 이 세 모드가 모두 6G 보안 아키텍처 설계에 고려되어야 함을 주장하며 이를 가능케 하는 요소기술로서 신원 관리 및 권한 부여, Third-Party 보안 평가, 블록체인 기술 등의 중요성을 제시하였다.

3. NGMN

NGMN은 차세대 네트워크 인프라 및 서비스에 대한 산업 지침을 제공하는 것을 목표로 구성된 통신 산업 구성원들 간의 공개 포럼이다. NGMN은 자체 프로젝트 결과물들이 3GPP, IEEE 등에서 채택되기도 하며 이동통신 산업계 전반에 걸쳐 높은 영향력을 갖고 있다. NGMN은 2023년 4월에 발간된 “6G Trustworthiness Considerations” 백서를 통해 6G 네트워크에서는 범용적인 신뢰성을 확보하는 것이 중요함을 주장하며 6G 트러스트와 관련된 요구사항 및 기술적 고려 사항들을 제시하였다[9]. 제시된 요구사항은 Security, Privacy, Reliability, Resilience 등의 관점을 다루고 있다.

Security 관점에서의 요구사항은 6G 보안에서 기대되는 경량화, 탬퍼링 방지, 양자 내성 등의 특성을 반영하여 진화된 암호/인증 기술의 필요성을 강조하고 있다. Privacy 관점에서, 6G에서는 개인화된 AI

네이티브 서비스가 대중화되고 보편화될 것임에 따라 6G 인프라 전반에 걸친 Privacy 보존이 필요함이 강조된다. Reliability 관점에서는 6G 시스템의 라이프 사이클 전체에 걸쳐 보안 기능은 지속적으로 제공되어야 하고 보안 위협탐지와 취약점 패치 등이 자동화되어야 한다는 요구사항이 제시되고 있다. Resilience 관점에서는 6G 시스템이 다양한 위협에 노출되어 공격을 받을지라도 서비스 제공의 영속성에 대한 신뢰 보장을 위해 자동화된 피해 복원이 되어야 한다는 개념을 기반으로 AI 기반의 자동화된 공격 피해 억제와 시스템 복원기술의 필요성이 제시된다.

이와 같은 요구사항들은 현재 시점에서 6G 환경과 생태계의 변화를 빠르게 예측하고 현재의 각 보안 기술들을 그에 맞게 진화시킴으로써 6G 트러스트 모델 개념 정립과 요소기술 개발 등에 활용될 수 있을 것으로 기대된다.

4. 국내 R&D 사업

6G 보안과 관련된 기존 국내 R&D 사업으로는 ETRI 주관의 6G 보안 내재화 아이템을 발굴하고 검증하는 연구사업이 수행되고 있다. 이 사업은 포괄적인 6G 보안이나 트러스트 모델의 개념을 다루기보다는 6G 표준화가 본격적으로 시작되기 전에 6G에 보안 기능을 선제적으로 내재화하는 것을 목표로 6G 환경을 예측한 각종 보안위협 검증 및 보안 요소기술들을 발굴하고 각 시나리오와 기술 단위로 검증을 하는 것을 목표로 한다. 본 사업에 이은 6G 보안 관련 연구사업은 본격적으로 6G 트러스트 모델을 대상으로 하며 2024년 7월부터 2년 6개월에 걸쳐 수행될 예정이다. 연구 목표는 6G 환경의 개방형 아키텍처, 이동통신 기능의 분산화, 네트워크의 지능화 등을 고려하여 6G 트러스트 모델을 구축하고 그것에 기반한 지능형 침해대응 기술을 개발하는 것이다.

이 사업에서는 트러스트 모델 적용 1단계로 통신, 네트워크 계층을 타겟으로 기지국 간, 이기종 장치 간의 신뢰성 확보를 위해 DPKI 기반의 신뢰성 보장 기술을 연구한다. 2단계로는, 화웨이의 다자간 신뢰 모델과 같이, 개방화/분산화된 이동통신 환경에서의 각종 서비스 및 데이터를 다루는 계층을 타겟으로 분산 원장 기술을 활용한 트러스트 모델 및 유즈케이스를 연구한다.

NGMN에서 제시한 6G 트러스트 모델 요구사항 중 “Resilience”는 각종 6G 비전에서 비중 있게 다루고 있는 개념으로서 그 중요도가 매우 높음에 따라, 이 사업에서는 제로트러스트 기반의 레질리언스 강화 기술을 연구하고 있다.

이 사업을 통해 개발될 트러스트 모델은 궁극적으로는 통신, 네트워크, 서비스, 데이터를 아우르는 6G 환경 전반에 걸친 포괄적 트러스트를 제공하는 플랫폼을 지향하고 있으며, 분산 AI 기술과 같은 차세대 지능형 보안 기술과 융합을 통해 안전하고 신뢰성 있는 6G 서비스 제공에 기여할 것으로 기대된다.

Ⅳ. 개방형 무선통신 보안 기술 동향

개방형 무선통신 구조인 오픈랜은 개방형 아키텍처 및 AI가 내재된 구조를 지향하기 때문에 6G에서 매우 주목받고 있는 기술이다. 오픈랜은 3GPP나 O-RAN Alliance 등에서는 표준화를 진행하고 있으며 기본적인 시스템 구축에 대한 가이드를 제공하고는 있으나, 불특정 다수의 제조사나 SW 컴포넌트 개발 업체들의 참여로 인한 예기치 않은 인터페이스 간 호환성 문제, 공급망 위협에 대한 노출, 체계적인 보안성 패치 등의 관리 부족 등의 이슈와 같은 보안적 측면에 대한 고려는 부족한 실정이다. 본 장

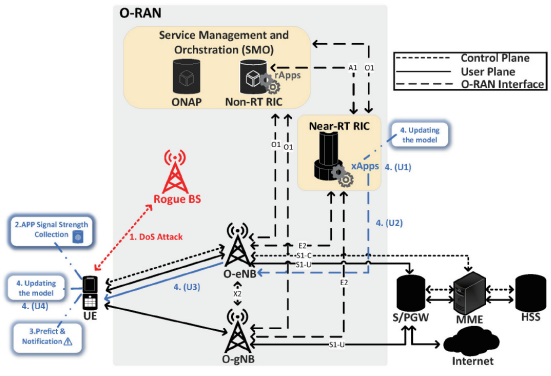
에서는 신뢰성 있는 오픈랜 서비스 제공을 위한 보안 기술 연구 동향을 소개한다.

1. xApp 기반 DoS 공격 탐지

오픈랜은 지능형 RAN 제어 컴포넌트인 RIC를 기반으로 xApp이라는 RAN 제어 어플리케이션을 활용하는 것을 특징으로 하고 있다. xApp의 목적은 오픈랜 전체적인 관리나 실시간 성능 최적화 등의 지능화 서비스를 제공하는 것인데, 최근에는 xApp을 오픈랜 침해위협 탐지에 활용하는 연구들이 발표되고 있다.

브라질의 Espirito Santo Federal 대학의 연구팀은 2023년 IEEE ICC 컨퍼런스에서 xApp을 이용한 오픈랜 내부에서의 DoS 공격 탐지에 대한 연구를 발표하였다[10].

이 연구팀은 그림 2와 같은 오픈랜의 무선 접속망에서 DoS 공격 데이터를 수집하고 이를 기반으로 머신러닝을 이용한 공격 탐지 모델을 개발하였다. 공격 탐지 응용은 xApp으로 개발되었으며 Near-RT RIC의 저지연성을 기반으로 하여 빠르게 공격을 탐지할 수 있다. 이 연구는 RAN에서 수집한 DoS 공격 데이터가 오픈랜에 특화된 공격이라고 할 수 없다는 한계점이 있으나 Near-RT RIC의 특성을 이용한 고속의 탐지 성능을 보이는 xApp 연구에 대한 선도적 시도에 의미가 있다.



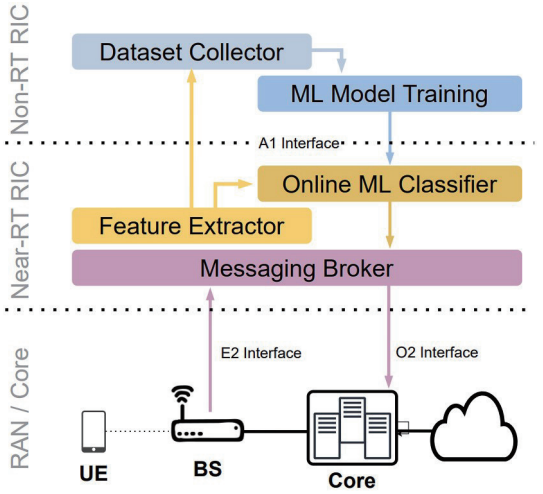
출처 Reprinted with permission from J. H. Huang et al., "Developing xApps for rogue base station detection in SDR-enabled O-RAN," IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops(INFOCOM WKSHPS), 2023.

그림 2 xApp 서포트를 통한 허위기지국 탐지 사례

2. xApp 기반 허위기지국 탐지

대만의 타이완 대학 연구팀은 2023년 IEEE INFOCOM 컨퍼런스에서 오픈랜 환경에서 허위기지국을 탐지하기 위한 xApp에 대한 연구를 발표하였다[11].

허위기지국은 4G/5G에서도 지속적으로 이동통신 환경에서의 주된 보안 위협으로 거론되어 오고 있으며 오픈랜에서는 개방형 구조의 특성상 허위기지국에 의한 위협이 더욱 실체화될 것으로 전망된다. 이 연구팀은 RAN 및 오픈랜 환경을 제공하는 오픈소스인 srsRAN[12]을 기반으로 그림 3과 같은



출처 Reprinted with permission from B. M. Xavier et al., "Machine learning-based early attack detection using open RAN intelligent controller," ICC 2023-IEEE International Conference on Communications, 2023.

그림 3 xApp 기반 오픈랜 침해위협 구축 사례

테스트베드를 구축한 뒤, srsRAN에서 제공하는 기지국 설정 파일을 일부 조작하는 방식으로 허위기지국을 구축하였다. 정상적인 UE와 같은 채널을 갖게 된 허위기지국으로 인해 UE는 정상기지국이 아닌 허위기지국에 연결되는 등의 피해를 입을 수 있으며, 이 연구에서는 물리 계층에서의 신호를 분석하여 허위기지국을 탐지하는 머신러닝 모델을 제안하였다. 탐지 응용은 xApp으로 개발되었으며 99% 이상의 탐지 정확도를 보였다.

3. 오픈랜 Layer-3 공격 탐지

미국의 오하이오 주립 대학 연구팀은 2024년 NDSS 컨퍼런스에서 오픈랜 Layer-3 프로토콜에 가해지는 외부 공격을 탐지하기 위한 프레임워크인 5G-Spector를 발표하였다[13].

연구팀은 지난 수 년 동안 광범위한 5G 프로토콜 레벨의 취약점을 검증하고 보고해왔으며 이 취약점들 대부분은 저렴한 SDR 장치를 이용하여 쉽게 재현할 수 있다. 이와 같은 공격들은 기지국과 사용자 단말 사이의 메시지 조작, 플러딩, 스푸핑 등의 악성 행위를 통해 프라이버시 유출, 서비스 거부, 사용자 단말 위치 추적 등의 심각한 사이버 침해사고를 유발할 수 있다. 5G-Spector에서 제안하는 CU/DU와 RIC 사이의 에이전트는 F1 인터페이스를 통해 전달되는 이동통신망 Layer-3 제어 메시지인 RRC 상태, 메시지 암호 알고리즘과 더불어 TMSI, C-RNTI 등의 사용자 단말 식별자를 추출하여 E2 인터페이스를 통해 RIC로 전달한다. 연구팀은 RIC에 전달된 데이터를 분석하여 UE의 식별자 추적 및 상태정보 변화를 관리함으로써 다양한 SDR 기반의 외부 공격을 탐지하기 위한 xApp을 구현하였으며 실시간 보안 위협 탐지 기능을 검증하였다. 5G-Spector의 공격 탐지는 탁월한 성능을 보이고 있으나 실시간 공격 대응은 불가능하며 내부 컴포넌트의 버그로 인한 보안 취약점 탐지 및 대응에도 한계가 있어서 좀 더 적극적인 보안 기술에 대한 요구가 계속되고 있다.

Ⅴ. 분산 AI 기반 네트워크 보안 기술 동향

6G 이동통신 환경은 개방화 분산화될 것으로 예상되며, 광범위한 AI를 기반으로 지능형 네트워킹이 실현될 것으로 기대된다. 이러한 환경 변화에 따라 공격 접점이 확대될 우려가 제기되고 있으며, 분산 AI 기반의 지능형 네트워크 보안 기술에 대한 중요성이 강조되고 있다. 본 장에서는 이동통신 환경에 적용될 수 있는 분산 AI 기술을 분석하고 분산 AI 기반의 지능형 네트워크 침입 탐지 연구 동향을 분석한다.

1. 분산 AI 기술

분산 AI 기술은 중앙 서버에 데이터를 전송하지 않고, 각 로컬 노드에서 독립적으로 데이터를 처리하고 학습하는 방식을 말한다. 이러한 특성으로 인해 분산 AI 학습 방식은 데이터 프라이버시를 보존할 수 있고 보안 측면에서 큰 이점을 제공할 수 있다. 6G 이동통신 환경에서 적용될 수 있는 주요 분산 AI 학습 기술로는 Federated Learning[14], Split Learning[15], SplitFed Learning[16], 그리고 Gossip Learning[17] 등이 있다.

Federated Learning(연합학습)은 데이터가 생성된 위치에서 개별적으로 로컬 모델을 학습하고, 중앙 서버는 개별 장치에서 학습된 로컬 모델(또는 Gradients)을 집계(Aggregation)하여 글로벌 모델을 최적화하는 주요 분산학습 프레임워크이다. 이는 로컬 데이터의 지역적 보존을 가능하게 하며, 민감한

정보가 중앙 서버로 전송되지 않아 데이터 프라이버시를 보호할 수 있다.

Split Learning(분할학습)은 AI 모델을 분할하여 로컬 노드와 중앙 서버에서 각각 학습하는 분산학습 방식으로, 데이터 프라이버시를 유지하면서 효율적인 학습을 가능하게 한다. Split Learning 학습 방식에서 로컬 노드는 AI 모델의 초기 층(Front-End Model)을 학습하고, 중앙 서버는 상대적으로 많은 연산을 필요로 하는 나머지 층(Back-End Model)을 학습한다. 학습 과정에서 로컬 노드는 중앙 서버에 데이터를 전송하지 않고 모델의 초기 층 출력값을 전송함으로써 로컬 데이터의 프라이버시를 보존한다.

SplitFed Learning(분할-연합학습)은 Federated Learning과 Split Learning의 강점을 결합한 방식으로, 모델의 일부는 로컬 노드에서 학습되고 나머지는 중앙 서버에서 학습되며, Split Learning과 달리 학습된 로컬 모델은 연합학습 방식으로 집계된다. 이러한 특성을 기반으로 SplitFed Learning은 데이터 프라이버시를 보존하면서 효율적인 분산학습을 가능하게 한다.

Gossip Learning(GL)은 중앙 서버 없이 네트워크 상의 노드들이 서로 데이터를 교환하며 학습하는 분산학습 방식이다. 각 노드는 인접 노드와 정보를 교환하고 학습을 진행하며, 이를 통해 네트워크 전체의 모델 성능을 최적화한다. Gossip Learning은 중앙 서버가 존재하지 않는 완전히 분산된 환경에서 로컬 데이터의 프라이버시를 보존하면서 효과적인 AI 모델 학습을 가능하게 한다.

2. 분산 AI 기반 네트워크 침입 탐지 기술

분산 AI를 활용한 지능형 네트워크 침입 탐지 기술의 초기 연구는 주로 다층 퍼셉트론과 신경망 모델을 분산학습 방식과 결합하는 방향으로 수행되었다. Rahman 등과 Huong 등은 사물인터넷(IoT) 환경을 고려하여 기존의 중앙집중식 학습 방식을 벗어나 연합학습을 적용한 분산 AI 기반의 침입 탐지 시스템에 관한 연구를 수행하였다[18,19]. 해당 연구를 통해, 연합학습 기반 네트워크 침입 탐지 모델은 전통적인 머신러닝 방식과 비교하여 높은 탐지율을 달성할 수 있음을 입증하였으며, 데이터 프라이버시를 유지하면서 중앙집중식 탐지 모델과 유사한 정확도를 달성할 수 있음을 보였다. Qin 등은 엣지 네트워크 환경에 초점을 두고 이진 신경망과 연합학습을 결합한 침입 탐지 시스템을 제안하였으며, 연합학습 과정에서 가중치 업데이트를 이진화하여 통신 오버헤드를 크게 줄일 수 있음을 입증하였다[20].

순환 신경망 모델(RNN)과 연합학습을 결합한 접근 방식으로, Nguyen 등은 IoT 네트워크 환경에서 취약한 IoT 기기를 탐지하기 위해 Gated Recurrent Unit(GRU)과 연합학습을 결합한 이상 탐지 시스템을 제안하였다[21]. 각 IoT 기기의 통신 패턴을 분석하여 정상적인 행동 프로파일을 생성하고 해당 프로파일을 기반으로 통신 이상을 탐지하는 메커니즘을 제안하였으며, 높은 탐지율과 0%의 오탐률로 공격을 감지할 수 있음을 입증하였다. Li 등은 산업용 사물인터넷(IIoT) 환경에서 DDoS 공격을 완화하기 위한 연합학습 기반의 침해위협 탐지 시스템을 제안하였다[22]. 자원 제약적인 IIoT 장치와 동적 위협 환경을 고려하여 Gated Recurrent Unit과 연합학습을 결합한 침입 탐지 시스템을 제안하였으며, 중앙집중식 탐지 모델과 유사한 정확도를 달성할 수 있음을 입증하였다. Khoa 등은 IIoT 환경에서 사이버 공격 탐지를 위한 연합학습 기반의 침입 탐지 시스템을 제안하였다[23]. 해당 연구에서는 IoT 게이트웨이에 스마트 필터를 배치하여 각 네트워크의 데이터를 수집하고 학습하는 접근법을 도입하였으며,

Deep Belief Network 모델과 연합학습을 결합한 공격 탐지 시스템을 제안하였다. Li 등은 산업용 사이버-물리 시스템(CPS)에서 발생할 수 있는 위협을 탐지하기 위한 연합학습 기반의 침입 탐지 시스템을 제안하였다[24]. 특히, CNN 모델과 GRU를 결합한 침입 탐지 모델을 도입하였으며, 여러 CPS 소유자의 데이터 프라이버시를 보존하면서 포괄적인 침입 탐지 모델을 학습할 수 있도록 연합학습을 결합하였다. 또한, Paillier 암호 시스템 도입하여 학습 과정에서 학습된 모델의 보안과 프라이버시를 동시에 보장할 수 있는 솔루션을 제안하였으며, 실 환경 데이터에 대한 실험을 통해 높은 탐지율로 공격을 감지할 수 있음을 입증하였다.

이동통신 환경을 고려한 지능형 침입 탐지 기술로써 Jayasinghe 등은 5G 및 Beyond-5G 이동통신 환경을 고려한 연합학습 기반의 네트워크 침입 탐지 시스템을 제안하였다[25]. 특히, 다중 단계로 구성된 Zero-touch Network and Service Management 아키텍처 기반의 침입 탐지 시스템을 제안하였으며, 각 단계에서 공격 탐지 모델은 연합학습 방식을 통해 학습되도록 설계하였다. 6G 이동통신 환경을 고려하여, Park 등은 분산학습을 적용한 지능형 네트워크 침입 탐지 시스템을 제안하였다[26]. 특히, 자원 제약적인 로컬 노드를 고려하여 분할학습을 적용한 침입 탐지 모델을 제안하였으며, 5G 테스트 네트워크에서 수집된 데이터상에서의 실험을 통해 높은 공격 탐지율을 달성할 수 있음을 입증하였다. Open RAN 환경을 고려한 침입 탐지 기술로써 Attanayaka 등은 연합학습 기반의 네트워크 침입 탐지 모델을 제안하였다[27]. 특히, Open RAN의 개방적이고 분산된 특성을 고려하여 Peer-to-Peer 연합학습 방식을 도입하였으며, 로컬 노드의 분산 시나리오를 고려하여 다양한 침입 탐지 시스템을 설계하였다.

Ⅵ. 6G 이동통신 표준화 현황

본 장에서는 6G 이동통신 표준화 현황을 분석한다. 특히, ITU-R WP5D 표준화 동향과 3GPP의 표준화 동향을 분석하고, 이동통신 보안의 관점에서 ITU-T의 SG17 표준화 현황을 분석한다.

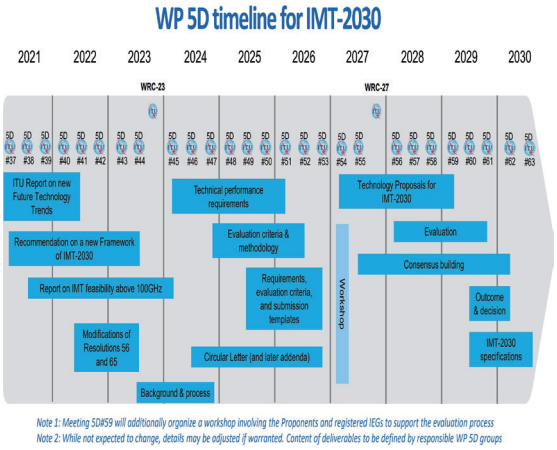
1. ITU-R WP5D

ITU-R WP5D에서는 기술, 주파수 및 서비스 등 IMT 분야의 국제표준화를 담당하고 있다. 2020년 2월에 개최된 34차 회의를 통해 2030년 및 그 이후에 대한 미래 기술보고서(Future Technology Trends) 개발을 시작하였으며, 2021년 3월에 개최된 37차 회의를 통해 6G Vision 권고안을 개발하기로 결정함으로써 본격적인 6G 표준화 논의를 착수하였다.

6G Vision 문서는 2023년 1월 회의에서 6G Framework라는 이름으로 개칭되었으며, 지난 2023년 6월 WP5D 44차 회의에서 6G Framework 권고안(M.2160) 개발이 완료되고, 같은 해 11월 WRC-23에서 공식 승인됨에 따라 6G 이동통신 표준화의 첫 번째 단계를 성공적으로 마쳤다[1].

2022년 6월 WP5D 41차 회의에서 수립된 IMT-2030(6G) 표준화 작업 계획(그림 4)에 따라, 2024년 1월 WP5D 45차 회의부터 6G 후보 기술 평가에 필요한 기술 성능 요구사항(TPR: Technical Performance Requirements) 보고서 개발 논의를 착수하였다.

TPR 후보 항목으로는 IMT-2020(M.2410)[28]에 포함되었던 기존 항목 13개와 신규 항목 7개(Coverage, Positioning, Sensing-Related Capabilities, AI-Related Capabilities, Sustainability(Energy efficiency), Security and Resilience, Interoperability)를 포함하여 총 20개 항목이 있으며, 기존 항목에 대한 정의는 M.2410을 기반으로 하고 각 항목별 시험환경/목표값 등



출처 Reprinted with permission from ITU-R Working Party 5D, IMT-2030 6G Vision, 2023. 6. [1].

그림 4 IMT-2030(6G) 표준개발 로드맵

은 TBD로 처리하였고, 신규 항목에 대한 정의는 M.2160을 기반으로 초기 논의가 진행 중이다.

본격적으로 6G 기술 및 주파수 표준화가 시작됨에 따라 기술 성능 요구사항 및 평가 방법 보고서 개발을 위한 우리나라의 전략 수립 및 글로벌 리더십을 유지할 수 있도록 선제적인 준비가 필요하다. 또한, WP5D 연구반 중심으로 국내 관련 회의체(TTA PG1101, 6G 포럼 등)와 협력을 통해 TPR 항목 및 평가 방법의 세부 사항을 제안할 수 있도록 준비가 필요하다.

2. 3GPP

최근 3GPP Release 19 작업에서는 네트워크 구조 관점에서 5G-Advanced 네트워크의 전체적인 AI/ML 지원을 위한 표준화 연구를 시작하였다. 현재 RAN 구간과의 인터페이스 및 연동을 포함한 단말, 기지국, 네트워크, 응용 서버 간의 협업을 통한 종단간 네트워크 최적화 이슈뿐만 아니라 온라인 학습, 강화 학습, 전이 학습 등을 포함하여 기존 AI/ML 기술을 5G 시스템에 활용하기 위한 표준화 항목 등이 폭넓게 표준화 후보 항목으로 논의되고 있다[29]. 6G 기술을 고려한 네트워크 아키텍처 관점의 가장 큰 변화는 네트워크 전 구간에 분산화된 AI/ML 기술이 적용되고 AI/ML 기능이 6G 구조 설계부터 반영되는 등의 AI/ML 기능이 내재화된 네트워크 구조일 것이다.

3GPP 구성 파트너인 TTA(한국), ETSI(유럽), ATIS(미국), ARIB/TTC(일본), CCSA(중국), TSDSI(인도)는 2023년 12월 3GPP 기술총회에서 3GPP의 6G 주요 표준화 일정을 확정했으며, 2025년 3월에 열릴 3GPP 6G 기술 워크숍을 우리나라에서 개최할 예정이다.

3GPP는 Release 20에서 6G 연구에 착수해 2024년부터 6G 유스케이스 논의를 시작으로, 2025년 3월 6G 기술 워크숍을 거쳐 2025년 6월 Release 20 연구 범위를 확정 예정이다. 이후 3GPP의 첫 번째 6G 기술 표준이 될 Release 21을 국제전기통신연합(ITU) IMT-2030 후보 기술로 제출하는 3GPP 6G 표준화 주요 계획을 확정지었다[30]. 실제 세부 기술 표준을 개발하는 3GPP가 6G 표준화 일정을 발표함으로써 6G 표준 경쟁이 공식적으로 시작된 것이다.

3. ITU-T SG17

ITU-T SG17 연구그룹은 보안 관련 국제표준 개발을 담당하고 있다. 현재 ITU-T SG17에서는 3GPP에서 정의하고 있는 5G 코어 네트워크 구조를 기반으로 통신사업자 및 서비스 제공자들이 5G 네트워크 구축 및 운영 시 요구되는 IMT-2020 보안 기능 및 보안 지침에 대한 국제표준을 개발하고 있다[31]. 차기 회기가 시작되는 2025년부터는 IMT-2030(6G) 보안 및 인공지능 보안 분야의 신규 표준 아이템 개발이 시작될 것으로 예상된다.

Ⅷ. 결론

6G 이동통신 기술은 초고속 데이터 전송, 초저지연, 광범위한 연결성 등 기존 5G를 넘어서는 성능을 제공하고 사회 전반에 걸쳐 새로운 디지털 전환을 촉진할 것으로 전망된다. 6G 이동통신 환경에서 개방형 플랫폼과 분산 네트워크의 확산은 유연하고 확장성 있는 이동통신 서비스를 가능하게 하지만, 동시에 보안 위협을 증가시킬 우려가 있다. 이러한 환경 변화에 따른 보안 위협에 대응하기 위해 네트워크의 신뢰성을 보장하는 진보된 보안 기술 개발이 필요하다.

본고에서는 6G 트러스트 네트워킹, 개방형 무선통신 보안 기술, 그리고 분산 AI 기반 네트워크 보안 기술에 대한 연구 동향을 분석하였으며, 보안의 관점에서 6G 이동통신 표준화 현황을 분석하였다. 특히, 인공지능은 6G 이동통신 환경에서 필수적인 기술이 될 것으로 전망되며, 동시에 보안 위협에 대응할 수 있는 지능형 보안 기술에 핵심적인 역할을 할 것으로 기대된다.

6G 이동통신 기술 개발이 진행됨에 따라 보안의 중요성은 더욱 강조되고 있다. 차세대 이동통신 보안을 위해 업계와 학계는 협력하여 지속적인 연구와 기술 개발을 추진해야 하며, 안전하고 신뢰할 수 있는 네트워크 환경을 구축하는 것은 중요한 과제가 될 것이다.

약어 정리

3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
ARIB	Association of Radio Industries and Businesses
ATIS	Alliance for Telecommunications Industry Solutions
CCSA	China Communications Standards Association
CNN	Convolutional Neural Network
CPS	Cyber Phisical Systems
C-RNTI	Cell Radio Network Temporary Identifier
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DoS	Denial of Service
DPKI	Distributed Public Key Infrastructure
ETSI	European Telecommunications Standards Institute
IIoT	Industrial Internet of Things
IMT	International Mobile Telecommunication
IoT	Internet of Things
ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Sector
NGMN	Next Generation Mobile Networks
RAN	Radio Access Network
RIC	RAN Intelligence Controller
RNN	Recurrent Neural Network
RRC	Radio Resource Control
SDR	Software Defined Radio
SG	Study Group
TMSI	Temporary Mobile Subscriber Identities
TSDSI	Telecommunications Standards Development Society, India
TTA	Telecommunications Technology Association
WP	Working Party
WRC	World Radio Congress
XAI	Explainable AI

참고문헌

[1] Recommendation ITU-R M.2160, Framework and overall objectives of the future development of IMT for 2030 and beyond, Nov. 2023.

[2] K.B. Letaief et al., "The roadmap to 6G: AI empowered wireless networks," IEEE Commun. Mag., vol. 57, no. 8, 2019, pp. 84-90.

[3] S. Dang et al., "What should 6G be?," Nature Electron., vol. 3, no. 1, 2020, pp. 20-29.

[4] M. Ylianttila et al., "6G white paper: Research challenges for trust, security and privacy," arXiv preprint, 2020. arXiv: 2004.11665.

[5] P. Porambage et al., "The roadmap to 6G security and privacy," IEEE Open J. Commun. Soc., vol. 2, 2021, pp. 1094-1122.

[6] V.L. Nguyen et al., "Security and privacy for 6G: A survey on prospective technologies and challenges," IEEE Commun. Surv. Tut., vol. 23, no. 4, 2021, pp. 2384-2428.

[7] B. Veith et al., "The road to trustworthy 6G: A survey on trust anchor technologies," IEEE Open J. Commun. Soc., 4, 2023, pp. 581-595.

[8] HuaweiTech, "6G native trustworthiness," 2022. 12.

[9] NGMN, "6G trustworthiness considerations," 2023.

[10] J.H. Huang et al., "Developing xApps for rogue base station detection in SDR-enabled O-RAN," in IEEE Conf. Comput. Commun. Workshops, (Hoboken, NJ, USA), 2023.

[11] B.M. Xavier et al., "Machine learning-based early attack detection using open RAN intelligent controller," in IEEE Int. Conf. Commun., (Rome, Italy), 2023.

[12] srsRAN Project, https://www.srsran.com/5g

[13] H. Wen et al., "5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service," in Proc. 31st Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS '24), San Diego, CA, USA, 2024.

[14] B. McMahan et al., "Communication-efficient learning of deep networks from decentralized data," in Artificial Intelligence and Statistics, PMLR, 2017, pp. 1273-1282.

[15] O. Gupta and R. Raskar, "Distributed learning of deep neural network over multiple agents," J. Netw. Comput. Applicat., vol. 116, 2018, pp. 1-8.

[16] C. Thapa et al., "SplitFed: When federated learning meets split learning," in Proc. AAAI Conf. Artif. Intell. vol. 36, no. 8, 2022, pp. 8485-8493.

[17] R. Ormándi et al., "Gossip learning with linear models on fully distributed data," Concurr. Comput.: Pract. Exp., vol. 25, no. 4, 2013, pp. 556- 571.

[18] S.A. Rahman et al., "Internet of things intrusion detection: Centralized, on-device, or federated learning?," IEEE Netw., vol. 34, no. 6, 2020, pp. 310-317.

[19] T.T. Huong et al., "Lockedge: Low-complexity cyberattack detection in IoT edge computing," IEEE Access, 9, 2021, pp. 29696-29710.

[20] Q. Qin et al., "Line-speed and scalable intrusion detection at the network edge via federated learning," in IFIP Netw. Conf., (Paris, France) 2020, pp. 352-360.

[21] T.D. Nguyen et al., "DÏoT: A federated self-learning anomaly detection system for IoT," in IEEE 39th Int. Conf. Distrib. Comput. Syst. (Dallas, TX, USA), 2019, pp. 756-767.

[22] J. Li et al., "FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT," IEEE Trans. Ind. Inform., vol. 18, no. 6, 2021, pp. 4059-4068.

[23] T.V. Khoa et al., "Collaborative learning model for cyberattack detection systems in iot industry 4.0," in IEEE Wirel. Commun. Netw. Conf. (Seoul, Rep. of Korea), 2020, pp. 1-6.

[24] B. Li et al., "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," IEEE Trans. Industr. Inform., vol. 17, no. 8, 2020, pp. 5615-5624.

[25] S. Jayasinghe et al., "Federated learning based anomaly detection as an enabler for securing network and service management automation in beyond 5g networks," In Joint Eur. Conf. Netw. Commun. 6G Summit (Grenoble, France), 2022, pp. 345-350.

[26] C. Park et al., "Distributed learning-based intrusion detection in 5g and beyond networks," in Joint Eur. Conf. Netw. Commun. 6G Summit (Gothenburg, Sweden), 2023, pp. 490-495.

[27] D. Attanayaka et al., "Peer-to-peer federated learning based anomaly detection for open radio access networks," in IEEE Int. Conf. Commun. (Rome, Italy), 2023, pp. 5464-5470.

[28] Report ITU-R M.2410(11/2017), "Minimum requirements related to technical performance for IMT-2020 radio interfaces," 2017.

[29] 3GPP TR 38.843, "Study on Artificial Intelligence(AI)/ Machine Learning(ML) for NR air interface(Release 18)," 2023.

[30] https://www.etnews.com/20240712000173

[31] ITU-T SG17 Homepage, htps:/ww.itu.int/en/ITU-T/studygroups/2017-20/17/Pages/default.aspx