오픈랜 보안과 AI 동향

나재훈 ITU-T SG17 WP4 의장, 한국전자통신연구원 전문위원

1. 머리말

오픈랜(Open RAN)에서 오픈(개방)이란 'RAN(무선 접속 네트워크, Radio Access Network) 구성에서 장비 제공업자에 종속되지 않고, 서비스 요구에 따라 장비를 자유롭게 선택할 수 있다'는 뜻이다. 그간 장비 선택권이 벤더들에게 종속돼 있었는데, 오픈랜 개념의 출현으로 장비 선택이 자유롭고 다양해졌다. 2018년 설립된 O-RAN 얼라이언스가 개발하는 오픈랜 표준은 프로그래밍, 지능적, 분리, 가상화, 상호운용성 등의 특징을 지원한다.

특히 독점적인 RRH(원격 라디오 헤드, Remote Radio Head)와 BBU(베이스밴드 유닛, Base Band Unit)는 RU(라디오 유닛, Radio Unit), DU(분산 유닛, Distributed Unit), CU(중앙 집중식 유닛, Central Unit)로 모듈화되며, 이 중 상당수는 가상화 또는 컨테이너화 할 수 있다. 이러한 구성요소 간의 인터페이스는 상호운용성을 제공한다.

1.1 오픈랜 구조

레거시 네트워크가 오픈랜으로 진화하는 과정을 살펴보면, 가상화되지 않은 레거시 사이트에는 RRH와 BBU가 물리적 위치에 함께 배치돼 있다. RRH는 수신·발신 무선신호를 처리하고 BBU는 업링크·다운링크 데이터 트래픽의 디지털 신호를 처리한다. BBU는 백홀 전송 네트워크를 통해 코어에 연결돼 있다.

일부 서비스 제공업체는 중앙집중식 RAN 또는 C-RAN(Centralized RAN)이라는 새로운 네트워크 토폴로지를 개발했다. 여기서 BBU는 데이터 센터와 같은 중앙 위치에 그룹화되며, 중앙집중식 BBU는 프론트홀 전송 네트워크를 통해 RRH에 연결된다. 중앙집중식 BBU는 전력 및 냉각 측면에서 운영 비용을 절감하고 무선 네트워크 관리를 간소화했지만, 클라우드가 포함되지 않은 물리적 BBU 구조다.

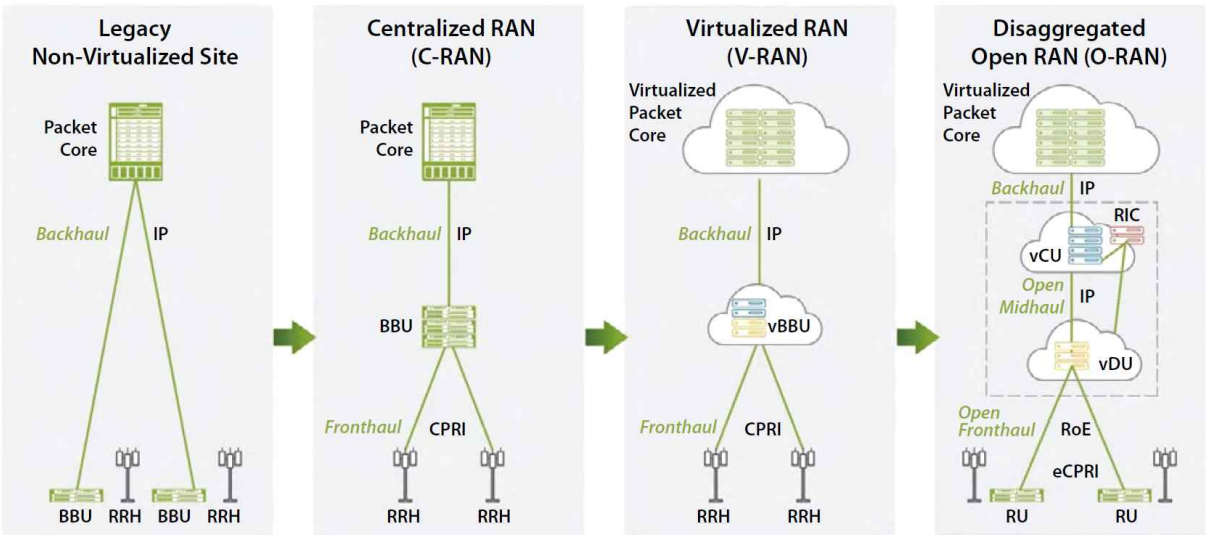
다음으로는 vRAN(Virtualized RAN) 또는 V-RAN이라고도 하는 가상화된 RAN이 제시됐는데, 이는 BBU 기능을 클라우드로 이동해 제어의 민첩성과 확장성을 높인 구조다. 오픈랜 이전에는 BBU와 RRH 간 인터페이스가 독점적이었기 때문에 한 공급업체만이 BBU와 RRH를 모두 제공했다.

오픈랜은 이 아키텍처를 분리하고 개방형 인터페이스를 도입해 RRH와 BBU 대신 RU, DU, CU로 기능을 세분화하고, 이들 사이에 개방형 인터페이스를 도입했다. RU, DU, CU 기능은 가상화하거나 컨테이너화할 수 있으며, 새로운 요소인 RIC(RAN Intelligent Controller)는 네트워크에 지능을 도입한다. 서비스 제공업체는 RIC를 사용해 혁신적인 응용을 발굴하는 동시에 AI·머신러닝 기술

을 통해 대규모로 RAN 기능을 제공하는 제3의 rApp/xApp을 온보딩할 수 있다.
O-RAN 얼라이언스는 개방형 RAN에 대한 구성요소로 서비스 관리 및 오케스트레이션(Service Management and Orchestration), RIC, O-Cloud, 오픈랜 중앙장치(O-CU), 오픈랜 분산장치(O-DU), 오픈랜 무선장치(O-RU) 구조를 제안했다[1].

1.2 오픈랜의 장점

오픈랜은 서비스 제공업체가 공급업체 종속을 탈피함과 동시에 공급업체 다양성을 장려한다. 서비스 제공업체는 단일 공급업체가 장비와 소프트웨어를 제공하는 종속된 관계를 원하지 않는다. 오픈랜 접근방식은 'RIC의 도움을 받아 완전히 프로그래밍 가능한 지능형 멀티벤더 RAN을 구축' 할 수 있는 솔루션 제공에 초점을 둔다.
RIC는 RAN 기능을 제어하고 최적화하는 소프트웨어 정의 구성요소로서 오픈랜 구조의 핵심이며, 무선 액세스 네트워크에 멀티 벤더 상호 운용성, 지능, 민첩성, 프로그래밍 기능을 제공하는 오픈랜 부품화(Disaggregation)의 중요한 부분이다. 이를 통해 대규모로 RAN 운영을 자동화하고 최적화하며, 제3의 응용 온보딩을 지원한다. RIC는 동시에 모바일 사업자의 총소유비용(Total cost of ownership)을 낮추고 고객의 체감 품질(QoE)을 향상하는 혁신적인 서비스 구조도 제공한다.
오픈랜은 여러 가지 잠재적 이점을 제공하는 반면, 상호운용성 보장, 복잡성 관리, 네트워크 성능 및 보안 유지와 같은 과제를 안고 있다. 하지만 네트워크 사업자, 공급업체, 표준화 기관을 비롯한 많은 업계 관계자들은 이러한 과제를 해결하고 기존 셀룰러 네트워크 구조를 대체할 수 있는 대안으로 오픈랜을 채택하기 위해 노력하고 있다.



출처: Juniper networks https://www.juniper.net/us/en/research-topics/what-is-open-ran.html

[그림 1] RAN 구조 진화

2. 오픈랜 보안

모바일 통신 네트워크는 점점 더 세분화되고 있고, 통신 사업자들은 클라우드 인프라와 운영 기법을 사용해 소프트웨어가 실행되는 하드웨어에서 소프트웨어를 분리하고 있다. 이전에는 프로토콜과 인터페이스 독점이던 것을, O-RAN 얼라이언스는 RAN를 통해 구조적으로 모듈화하고 있다. 이를 통해 모듈화가 더 세분화돼 제어 시스템이 분리가능해지고, 실행 효율성과 공급업체 다양성도 향상됐다.

오픈랜을 통해 전체 시스템에서 프로그래밍 영역이 증가하면서 투명성과 내부 검토 기회가 늘어났다. 반면 사이버 보안 관점에서 보면, 잠재적 공격 위험도 늘어난다. 그러나 보안에 대한 의구심이 혁신과 변화를 저해해서는 안 된다고 생각한다. 위험은 항상 존재하며 관리가 필요한 것이지, 배제는 적절한 대응이 아니라고 판단된다. 안전성 제고를 위해 통신 사업자는 공급업체 및 동종 업계와 협력하여 보안 전략을 수립해야 한다.

IMT-2020(5G)/2030(6G) 구조는 액세스, 백홀, 코어 네트워크에서 보안 위협이 발생하고 있다[2]. 사이버웨어 및 중요 인프라 위협, 네트워크 기능 가상화(NFV) 및 소프트웨어 정의 네트워킹(SDN) 관련 위협, 클라우드 컴퓨팅 관련 위협은 IMT-2020(5G)에서 가장 일반적인 보안 문제다[3]. 중요한 API가 의도하지 않은 소프트웨어에 노출되거나, 오픈플로우가 시작되거나, 네트워크 제어가 중앙 집중화돼 디도스공격에 노출되는 등 SDN이 보안 위협을 야기하는 경우는 많다[4]. 무엇보다도 IMT-2030(6G) 비전의 가장 중요한 원동력은 첨단 네트워킹, AI·머신러닝 기술과 함께 통신 네트워크에 연결된 지능화가 추가된다는 점이다. 그러나 AI·머신러닝과 IMT-2030(6G)의 결합은 많은 경우, 보안·프라이버시를 보호하거나 혹은 침해하는 양날의 검이 될 수도 있다[5].

네트워킹 및 통신 기술의 발전과 동반해, 보안은 네트워크의 복원력(Resilience)과 안정성을 보장하기 위해 항상 고려해야 할 중요한 기능이다. 따라서 구상 중인 IMT-2030(6G) 네트워크의 보안 관련 연구 방향을 파악하는 것은 향후 연구 활동에 유용하다. IMT-2030(6G) 표준 기능의 요구사항이 아직 정의되지 않았기 때문에, 보안에 대한 인사이트를 제공하는 문헌은 아직 제한적이다. 또한, IMT-2020(5G)연구를 체계적으로 구축하고 IMT-2030(6G) 보안을 확보하기 위한 새로운 연구와 통합이 필요하다. 이미 많은 IMT-2030(6G) 비전 논문이 발표됐지만, 앞으로도 관련 보안을 체계적으로 분석하는 연구가 필요하다[6, 7, 8, 9].

IMT-2030(6G) 네트워크 비전은 아키텍처, 응용, 기술, 정책, 표준화 측면에서 많은 참신한 아이디어와 성능 개선으로 구성돼 있다. 클라우드화되고 소프트웨어화된 IMT-2020(5G) 네트워크 위에 지능이 추가된 일반적인 IMT-2030(6G) 비전, 그리고 네트워크 자동화를 위해 보안은 AI·머신러닝과 긴밀하게 융합해야 한다. 현재 공격자들 역시 더욱 지능화되어 새로운 형태의 보안 위협을 만들어 내고 있다.

딥러닝이 도입된 이후, 무선통신 연구 커뮤니티에서 AI 응용에 대한 관심이 다시 높아지고 있다. AI 기반 솔루션과 관련해 아직 해결해야 할 보안 문제에도 불구하고, AI 자동화 보안 솔루션은 미래 무선 네트워크의 필수 핵심 요소가 될 것으로 예측된다. AI 적용은 매우 중요하게 여겨지며, 전체 보안 프레임워크에 AI 알고리즘을 활용하는 것이 제안되고 있다(Security by AI).

관련 논문[10]에선 신뢰할 수 없는 네트워크에 보안을 제공하기 위해 AI 알고리즘을 사용하는 지능형 제로 트러스트(Zero Trust) 구조 개념 설계를 제안했다. 이 프레임워크는 통합 용이성을

보장하기 위해 오픈랜 구조를 활용하는 서비스 기반 설계를 채택했다. 오픈랜에서의 세 가지 주요 구성요소로, 지능형 에이전트 또는 포털(IGP), 지능형 네트워크 보안 상태 분석(INSSA), 지능형 정책 엔진(IPE)을 구분하고 있다.

3. 오픈랜 AI

IMT-2020(5G)/IMT-2030(6G) 시대에는 네트워크에서 지원되는 다양한 사용 사례와 응용, 네트워크 파라미터 및 구성의 다양한 조합으로 인해 RAN 구축과 운영이 복잡해지고 있다. 또한 분할 아키텍처와 가상화의 도입으로 RAN의 복잡성도 더욱 증가할 것이다. 이러한 상황에서 기존 수동 작업으로 RAN 구축·운영을 관리하고, 최적화를 달성하기는 점점 더 어려워지고 있다. 이를 해결하기 위해 빅데이터 분석과 AI·머신러닝을 활용한 RAN의 지능 도입은 필연적이며, 이는 자동화된 관리와 제어를 가능하게 해준다.

통신사 입장에서 지능 도입의 이점 중 하나는 RAN 운영의 디지털 혁신을 통해 운영 활동과 비용을 절감할 수 있다는 것이다. 또 다른 중요한 이점은 무선 리소스 관리 및 제어 자동화를 통해 RAN 성능을 개선, 고객 만족도 향상과 신규 비즈니스 창출에 기여할 수 있다는 점이다.

위에서 언급한 RAN의 지능화를 실현코자 O-RAN 얼라이언스는 혁신적인 멀티 벤더, 상호운용성 및 자율성을 갖춘 RAN과 관련해 생태계 개발을 위한 모바일 산업 활동을 주도하고 있다. RIC는 AI·머신러닝 모델을 사용해 지능형 무선 리소스 관리 및 최적화를 제공하는 핵심 기술이다. RIC에는 제어 주파수가 1초 이상인 비실시간(non-RT) RIC와 1초 미만인 근실시간(near-RT) RIC라는 두 가지 기능이 있다.

RIC는 플랫폼과 소프트웨어 응용을 분리해 구현되며, 이 응용은 O-RAN 얼라이언스에서 개발 중인 개방형 인터페이스를 통해 연결된다. 개방형 인터페이스 덕분에 제어 정책 또는 RAN 노드에 대한 소프트웨어 응용 개발은 RAN 공급업체에 국한되지 않고 통신사 및 타사 공급업체에 개방된다.

오픈랜은 새로운 구조를 제안했으며, 이를 효율적으로 관리하기 위해 새로운 기능이 필요하다. 모바일 네트워크 사업자는 IMT-2030(6G)으로 진화하는 이동통신 네트워크가 '운영 비용(OPEX)을 절감할 수 있고, 지능적이며, 스스로 구성되면서도(Selforganizing) 비용 효율적(Cost-effective)이어야 함'을 목표로 한다. AI의 한 분야인 머신러닝은 이러한 여러 과제에 대한 실용적 솔루션을 제공함으로써, 무선 네트워크 기술의 미래를 희망적으로 보이게 하고 있다. AI·머신러닝은 오픈랜의 RIC에서 다음과 같은 중요한 역할을 담당할 것으로 예상된다.

- 최적화와 효율성: AI·머신러닝 알고리즘은 실시간으로 자원 할당, 전력 사용, 전체 네트워크 효율을 최적화할 수 있다. 네트워크에서 수집된 방대한 양의 데이터를 분석해 성능을 향상시키고 운영 비용을 줄이는 지능적인 결정을 내릴 수 있다.
- 동적 적응: 오픈랜 환경은 네트워크 조건이 급속하게 변하는 동적인 특성을 가지고 있다. AI·머신러닝은 이러한 변화에 빠르게 적응해 네트워크 매개변수를 조정하고, 최적의 성능과 사용자 경험을 보장할 수 있다.

- 예측적 유지보수: AI·머신러닝 기반 분석을 통해 RAN 구성요소의 잠재적 고장이나 성능 저하를 예측할 수 있다. 이를 통해 장애가 발생하기 전, 사전에 유지보수를 수행해 장애시간을 줄이고 서비스 중단을 최소화할 수 있다.
- 자가치유 네트워크: AI·머신러닝은 RAN 내에서 자가치유 기능을 활성화할 수 있다. 네트워크 요소가 인간 개입 없이 문제를 자동으로 감지하고 완화할 수 있다. 이는 네트워크 신뢰성과 내구성을 향상시킨다.
- 향상된 보안: AI·머신러닝은 네트워크 트래픽 패턴을 분석해 실시간으로 이상 현상이나 잠재적인 보안 위협을 감지할 수 있다. 네트워크를 지속적으로 모니터링하고, 이를 AI·머신러닝으로 분석해 보안 위협을 더 효과적으로 식별하고 대응할 수 있다.
- 네트워크 슬라이싱: AI·머신러닝은 다양한 사용 사례나 고객 세그먼트를 제공하기 위해 가상화된 네트워크 인스턴스를 생성하는, 효율적인 네트워크 슬라이싱을 용이하게 할 수 있다. AI·머신러닝 알고리즘은 각 네트워크 슬라이스에 대한 특정 요구사항에 따라 자원을 동적으로 할당하고 성능을 최적화할 수 있다.

종합적으로, 오픈랜의 RIC에 AI·머신러닝을 통합함으로써 네트워크 지능, 민첩성 및 자동화가 구축돼최종 성능, 확장성, 비용 효율성이 향상된다.

3.1 이동통신 네트워크의 AI 관련 요구사항(ITU-R WP 5D)

IMT-2030(6G) 권고개발은 ITU-R WP 5D(Working Party 5D–IMT Systems)에서 'Vision' 문서라는 명칭으로 2021년 3월 착수됐다. 이후 2023년 6월 제네바에서 열린 44차 회의에서 'IMT-2030(6G) Framework'라고 수정된 제목으로 상위 위원회인 ITU-R SG5(Terrestrial services)에 표준 제정이 요청됐다. 이를 바탕으로 2023년 11월 ITU-R에서 최종 M.2160(Framework and overall objectives of the future development of IMT for 2030 and beyond) 권고가 제정됐다.

해당 문서는 향후 IMT-2030(6G) 관련 시리즈 권고 작업을 위한 기초문서가 된다. 이 프레임워크 문서를 기반으로 최소 기술 성능 요구사항(Minimum Technical Performance Requirement) 및 평가방법(Evaluation) 문서들이 작성·계획되고 있으며, 기술 성능 요구사항을 기반으로 3GPP에서 세부기술규격 개발이 이뤄진다. 그 이후엔 평가를 위한 후보 기술을 서비스 제공자 또는 벤더들이 제안하고, 제안된 기술들에 대한 평가를 거쳐 최종 무선접속 기술 권고를 제정하는 일련의 일정이 향후 7년 동안 진행될 것이다.

[그림 2]는 IMT-2030(6G)의 15개 기능을 도식화한 것이다. 녹색은 이전에 있던 기능이고, 파란색은 신규 기능으로 구분된다. 신규 기능으로는 Coverage, Sensing-related capabilities, Applicable AI-related capabilities, Sustainability, Interoperability, Positioning 등과 같은 기능이 소개되고 있다.

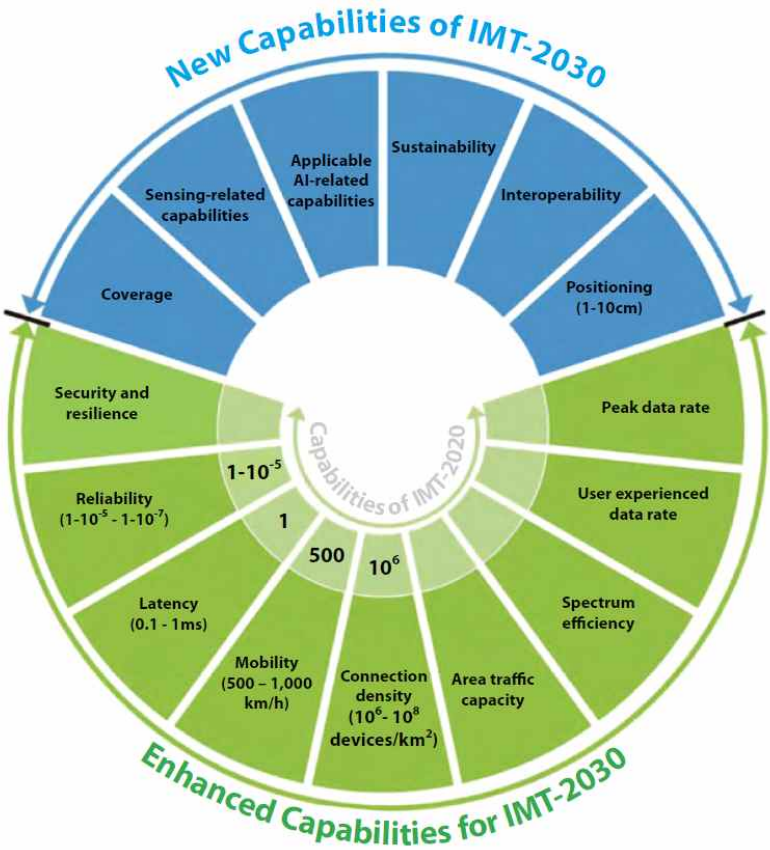
권고 M.2160 제정 이후 ITU-R WP 5D 내의 SWG(Sub Working Group) Radio Aspects에서 TPR(Techical Performance Requirement)이라는 최소 성능 요구사항 문서가 개발되고 있다. 각국에서 기고가 한창 진행 중에 있으며, AI 관련해 중국 화웨이(Huawei)와 스웨덴 에릭슨(Ericsson), 한국전자통신연구원에서 주요 기고가 있었다. 지난 6월 WP 5D에서 4.13절의 AI 관련 기능

(Capabilities) 회의 결과는 다음과 같다.

> AI 관련 기능은 AI 애플리케이션을 지원하기 위해 IMT-2030 전반에 걸쳐 특정 기능을 제공할 수 있는 기능을 의미한다. 이러한 기능에는 분산 데이터 처리, 분산 학습, AI 컴퓨팅, AI 모델 실행, AI 모델 추론 등이 포함된다. AI 기능은 통신을 위한 AI 서비스 및 AI·머신러닝도 포함한다.

한편 4.13A 정성적 지표(Qualitative metrics) 절에선 'IMT-2030 시스템은 AI 애플리케이션을 위한 분산형 AI 인프라·아키텍처를 지원하는, 최소 N개의 기능과 관련된 메커니즘 및 시그널링을 제공해야 한다'는 내용을 기술했다. 4.13B 정량적 지표(Quantitative metrics) 절은 AI 서비스 정확도, AI 서비스 지연, AI 서비스 밀도 지표에 집중하고 있다.

AI 서비스 정확도는 '주어진 AI 추론·학습 작업을 높은 정확도로 처리하는 능력'을 의미한다. AI 서비스 지연 시간은 '목표 서비스 정확도로, 주어진 AI 추론·학습 작업 시작부터 종료까지 걸리는 시간'을 의미하며, 지연발생으로 서비스 품질이 저해되는 영역을 측정한다. AI 서비스 밀도는 '주어진 AI 추론·학습 작업에 대해서, 단위 커버리지 영역의 네트워크에서 지원할 수 있는 AI 서비스 품질(QoS) 요구사항(예: AI 서비스 정확도 및 AI 서비스 지연 시간 요구사항)을 만족하는 총 AI 서비스 수'를 의미한다.



[그림 2] IMT-2030의 새로운 기능

3.2 안전한 자원관리를 위한 AI·머신러닝 (ITU-T SG17)

ITU-T SG17(Security)은 보안 관련 국제표준을 개발하는 연구그룹이다. 본 그룹에서도 IMT-2020(5G) 보안 표준 개발이 진행돼 왔으며, 4년 주기 연구 기간이 2024년에 종료되는 것과 맞물려, 구조조정이 진행되고 있다. 이러한 변화와 함께 신규 표준 주제로 IMT-2030(6G) 보안 및 AI 보안에 관심이 집중되고 있으며, 연구과제 Q7/17에 AI 보안 항목을 ToR에 포함하는 것, 그리고 IMT-2020 보안의 후속으로 IMT-2030 보안을 Q2/17에서 개발할 것을 합의하는 문서가 마련됐다. 오는 10월 뉴델리에서 열릴 차기 SG17회의 WTSA-24에서 최종 승인이 될 예정이다. 이러한 추세에 따라, 지난 3월 총회에선 신규 아이템 X.pg-cla(Procedural guideline for continual learning to actively respond to network attacks)[11]이 채택됐다. 이는 오픈랜에 안전한 지능형 자원관리 기능 개발을 위한 표준으로써, 많은 관심이 집중되고 있다.

이 표준 아이템에 대한 배경은 다음과 같다. 디지털 시대 네트워크는 통신과 데이터 전송의 기반이며, 네트워크가 계속 성장하고 복잡해짐에 따라 효과적인 네트워크 관리와 능동적 방어 기술의 필요성이 점점 증가하고 있다. 네트워크 관리는 네트워크 성능을 모니터링, 유지, 최적화하는 과정을 말하며, 능동 방어 기술은 악성 응용, 컴퓨터 바이러스(코드) 등 사이버 위협을 능동적으로 탐지, 예방, 대응하는 것을 말한다.

클라우드, AI 등 새로운 기술의 등장으로 네트워크 환경은 더욱 복잡해지고 있으며, 차세대 무선 기술은 더 빠른 속도, 더 낮은 지연시간, 더 높은 안정성을 약속한다. 동시에 AI는 네트워크 관리와 보안을 혁신함으로써, 사이버 위협을 좀 더 효과적으로 탐지하고 대응할 수 있는 잠재력을 가지고 있다.

이러한 기술 발전으로 인해, 네트워크의 안정성(Stability), 가용성(Availability), 보안(Security)을 보장하기 위해선 강력한 네트워크 관리와 능동적 방어 기술을 갖추는 것이 필수적이다. 컴퓨팅이 활성화된 네트워크에선 새로운 변종 공격이 더 빠르게 생성될 수 있으며, 생성형 AI에 의해 공격 패턴이 더 빠르게 개발될 수 있다. AI와 같은 신기술이 빠르게 발전함에 따라, 이러한 신기술을 수용할 수 있는 차세대 네트워크의 핵심 기능인 능동형 방어 기술을 지속적으로 학습하는 것이 중요하다.

시시각각으로 변하는 무선 네트워크 환경에서 네트워크 공격이 이뤄지는 사례를 살핌으로써, 지속적학습 기술의 필요성을 엿볼 수 있다. 네트워크 서비스는 점차 지능화되고, 기능도 확장되고 있다. 다양한 서비스가 네트워크와 기능을 결합하면서 점차 우수한 서비스로 확장되고 있는 것이다. 하지만 네트워크 기능 확장과 함께 다양한 응용을 구동해야 하는 특성으로 인해 위험에 노출될 수 있다.

기존 방어방식 대부분은 서비스 차단에 중점을 두지만, 네트워크 기능 확장을 통해 추가된 기능은 공개와 공유를 기반으로 한다. 특정 서비스를 차단하는 방식으로는 관리가 불가능 하다는 의미다. 따라서 다양한 시나리오에 따른 공격을 지속적으로 학습하고 탐지하는 기술이 필요하다.

4. 결론

이동통신 트렌드의 중심이 IMT-2020(5G)에서 IMT-2030(6G)로 이동하고 있다. IMT-2030(6G)은 여러 가지 측면에서 IMT-2020(5G)와 차별성을 보인다. 일반적 측면에서 보면, IMT-2030(6G)은

성능 수치가 상향됐고, 서비스와 응용을 수용한다. 단순 전송 서비스를 제공하던 네트워크가 그것을 인프라에 배치하고, 그 위에 서비스를 제공하는 것으로 진화하고 있다는 것이다. 그 주요 특징이 AI를 기반으로 하는 네트워크의 지능화와 자율화라 볼 수 있다. 즉, 네트워크가 정형화된 전통적 모습에서 탈피해 가변적이고, 능동적이며, 자율적인 속성을 추구하고 있다. 이러한 변화의 속도에 동반돼야 하는 것이 개방화다. 독점으로 제공되는 서비스와 장비는 변화의 속도를, 경쟁의 우위를 유지할 수 없다. 이러한 시점에서 오픈랜 개발의 개방화 및 표준화는 매우 중요한 시사점을 보여주고 있다.

AI 발전은 다방면에 영향을 주고 있으며, 이동통신 인프라 및 서비스도 마찬가지다. 이러한 추세에서, AI를 그 이용 측면에만 집중하다 보니 보안상 어려움이 생겨나고 있다. 예를 들어, AI가 해킹을 당한 경우, 잘못된 초기데이터로 모델링이 틀리게 구축된 경우, 잘못된 입력에 의한 잘못된 결과를 이용하는 공격(Garbage In Garbage Out), AI를 이용한 해킹 등이 있다.

이러한 공격의 시작점이 오픈소스 혹은 AI의 초기학습이 될 수도 있다. 더불어, 우리는 사용자 요구사항이 지속적으로 변하는 환경에 대비하는 한편, 가변적·자율적 네트워크 관리를 위해서, 지속적인 학습을 통한 사용자 서비스 및 네트워크 관리 제공을 설계해야 한다. 관련 연구가 시작된 것은 매우 고무적인 진전이라고 사료된다.

[참고문헌]

[1] What is Open RAN?, https://www.juniper.net/us/en/research-topics/what-is-open-ran.html

[2] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, A Comprehensive Guide to 5G Security. Hoboken, NJ, USA: Wiley, 2018.

[3] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and challenges of software-defined mobile networks in network security," IEEE Security Privacy, vol. 14, no. 4, pp. 34–44, Jul./Aug. 2016.

[4] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp.196–248, 1st Quart., 2020.

[5] B. Schneier, "Artificial intelligence and the attack/defense balance," IEEE Security Privacy, vol. 16, no. 2, p. 96, Mar./Apr. 2018.

[6] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Netw., vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[7] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" Nat. Electron., vol. 3, no. 1, pp. 20–29, 2020.

[8] S. Chen, Y.-C. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, "Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed," IEEE Wireless Commun., vol. 27, no. 2, pp. 218–228, Apr.

2020.
[9] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, "A survey on green 6G network: Architecture and technologies," IEEE Access, vol. 7, pp. 175758–175768, 2019.
[10] Ramezanpour, K., Jagannath, J., "Intelligent zero trust architecture for 5G/6G tactical networks: Principles, challenges, and the role of machine learning", arXiv preprint arXiv:2105.01478, 2021.
[11] ITU-T SG17 X.pg-cla, Procedural guideline for continual learning to actively respond to network attacks, https://www.itu.int/md/T22-SG17-240220-TD-PLEN-2005

※ 출처: TTA 저널 제214호