5G 특화망 보안을 위한 지능형 모델 자기지도 학습관리 프레임워크에 관한 연구

한미경, 박노삼, 신용윤, 이훈기, 이종훈

한국전자통신연구원

A Study on a Self-Supervised Learning Management Framework for Intelligent Models in 5G Private Network Security

Mikyong Han, Noh-Sam Park, Yongyoon Shin, Hoon-Ki Lee, Jong-Hoon Lee

Electronics & Telecommunication Research Institute

요 약

보안성, 초저지연, 고신뢰성이 제공되는 5G 특화망은 다양한 유형으로 구축 가능하며, 기존에 구축된 기업망과의 통합 환경을 고려할 때 복잡한 인프라 환경뿐만 아니라 지능화, 고도화되는 보안위협에 대응하기 위한 인공지능 기반 네트워크 보안 솔루션이 요구된다. 본 연구는 5G 특화망 및 기업망과의 통합 환경에서 발생하는 보안 취약점을 능동적이고 효율적으로 개발하기 위한 지능형 자기지도학습 모델관리 프레임워크의 구조와 기능을 제시하고, 개발 결과물을 제시한다. 제안된 지능형 자기지도학습 모델관리 프레임워크를 통해 5G 특화망 보안을 강화하고 복잡한 기업망과의 통합 환경에서 네트워크 위협으로부터 신뢰성 있는 서비스 환경을 보장할 수 있는 지능형 보안탐지 모델개발을 지원하고자 한다.

Ⅰ. 서 론

최근 다양한 산업 현장에서 보안성, 초저지연·고신뢰 통신에 대한 요구 증가로, 이를 충족할 수 있는 전용 네트워크 인프라인 5G 특화망이 주목받고 있다. 5G 특화망은 별도의 전용 주파수 대역을 활용하며, 스마트 제조, 에너지 관리, 자율주행, 스마트시티, 공항, 항만, 의료기관, 교육 등 다양한 서비스 환경에서 안정적 통신을 지원한다.

5G 특화망은 망 구축 주체와 코어망의 물리적 배치에 따라 자가구축형, 사업장 독립형, 제어평면 공유형, 전체공유형으로 나뉜다. 그러나, 실제 도입 단계에서는 보안성이 가장 높은 독립형보다는 기존 기업 ICT 인프라와의 통합이 용이하면서 관리 효율이 높은 공유형 또는 관리형 구조가 주로 선호되고 있다[1,4].

5G 특화망은 다수의 이기종 단말과 네트워크 구성요소가 연동되는 복잡한 구조를 갖으며, 물리계층부터 가상화 인프라 계층에 이르기까지 아래 <표1>과 같이 다층적 보안위협이 존재한다. 이에 더해, 5G 특화망과 기업망 통합관리 측면에서는 통합 인프라에 대한 접근성을 고려한 신뢰성 있는 보안기술에 대한 고려도 필요하다.

이러한 요구에 따라 해외에서는 이미 5G 특화망에 대한 보안연구가 활발히 진행되고 있으나[2-3], 국내의 경우 보급 초기 단계로 기업망과의 통합 환경에 대한 보안기술 연구는 미진한 실정이다. 특히, 5G 특화망의 여러 가지 구축유형과 운용환경의 다양성을 만족시키면서 더욱 정교하고 지능화되고 있는 보안위협에 빠르게 대처하기 위해서는 인공지능 기반의 지능형 네트워크 위협탐지 분석을 위한 보안 솔루션 기술개발이 절실하다.

그러나, 네트워크 데이터의 특성상 방대한 네트워크 데이터에 대한 정밀 라벨링 부담 문제, 다양한 위협 데이터 확보, 정상과 비정상 데이터 간 품질의 일관성 확보가 어려운 실정이며, 라벨 분포와 트래픽 특성 또한 도메인이나 응용 서비스 환경에 따라 지속적으로 변화되는 환경에서 꾸준한 재학습 요구로 인공지능 모델의 운영, 배포, 유지가 부담이 되고 있다.

위협 구분	주요보안 위협요소	위협 예시
연결기기 (Endpoint)	인증 및 접근통제 취약, 암호화·키 관리 미흡, 멀웨어·IoT 봇넷 감염, 사용자 추적 및 도청	단말 인증 위·변조, 악성코드 감염, 무선통신 성능저하 유도 공격
RAN 구간	무선 구간 도청, 중간자 공격, 허위 기지국(Rogue BS), 개방형 인터페이스 취약점	amming, ARP Spoofing, Eavesdropping, Exploit Open Interfaces
코어망 및 네트워크	NF 설정 오류, 인증정보 유출, DoS/DDoS 공격, 상이한 보안 수준의 네트워크 간 연동 취약	Signaling Storm, 인증 토큰 탈취, 코어 자원 마비 공격
가상화 인프라	SDN/NFV 보안취약점, 슬라이싱 격리 실패, 오픈소스 취약 코드, 가상화 이미지 변조	슬라이스 간 정보유출, VNF 이미지 해킹, Cloud Function 변조

〈표 1 〉 5G 특화망 및 기업망 통합환경의 주요 보안 위협 요소

이러한 문제를 해결하고자 5G 특화망의 구축유형 및 서비스 유형을 고려하면서 기존 기업망과 신뢰 통합을 보장하고 안전한 5G 특화망 서비스 이용환경을 제공하기 위한 지능형 5G 특화망 네트워크 보안 서비스 플랫폼 개발을 추진중에 있으며, 본 논문에서는 플랫폼 내 지능형 자기지도학습 모델 생성 관리를 위한 프레임워크 기술개발에 대해 기술하고자 한다.

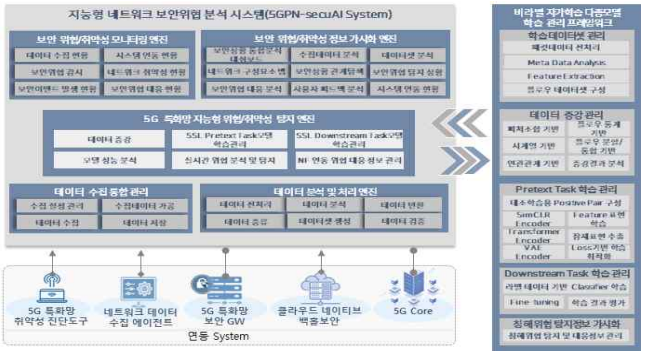
본 논문의 구성은 2장에서 5G 특화망과 기업망 통합환경을 위한 보안 서비스 플랫폼 내 자기지도학습 모델 생성 프레임워크 기능 및 개발 결과물을 소개하고, 3장에서 결론 및 향후 연구개발 추진계획을 서술한다.

Ⅱ. 본 론

2.1 5G 특화망 네트워크 보안 서비스 플랫폼 기능

5G특화망의 다양한 서비스 이용환경을 고려한 네트워크 보안 서비스 개발을 위해서는 무선환경이나 비인가 단말에 대한 취약성을 진단하기 위한 기능, 네트워크 보안위협 진단을 위한 데이터 수집 에이전트 기능, 특화망과

기업망 통합환경에서 신뢰성 있는 접근관리를 제공하기 위한 보안 GW 시스템 기능, 네트워크 취약성 및 보안위협 분석을 위한 분석 시스템 등의 기능이 요구된다. <그림1>은 이러한 요구사항을 지원하기 위해 개발 중인 지능형 5G 특화망 네트워크 보안 서비스 플랫폼의 연동구조 및 지능형 네트워크 보안위협 분석 시스템 기능구조를 도식화한 것이다.



〈그림 1〉 지능형 5G특화망 네트워크 보안 서비스 플랫폼 기능 구조

5G 특화망 네트워크 보안 서비스 플랫폼 내 지능형 네트워크 보안위협 분석 시스템은 전술한 여러 가지 시스템과의 연동을 통해 네트워크 보안위협 분석에 필요한 정보를 수집하는 데이터 수집통합 관리 기능과 수집된 데이터를 분석하기 위한 데이터 처리 기능, 네트워크 데이터를 기반으로 위협 분석 및 탐지를 위한 엔진기능, 위협 및 취약성 정보를 모니터링하는 엔진 기능과 실시간 대응을 위해 정보를 가시화하는 기능으로 구성된다.

특히, 지능형 보안위협 분석 시스템 내 네트워크 보안 위협탐지 엔진은 네트워크 APT 공격과 같은 알려지지 않은 치명적인 공격에 대응하기 위해 수집되는 네트워크 데이터를 기반으로 인공지능 기법을 이용하여 분석하고 침해위협을 정밀하게 탐지하는 기능을 제공한다.

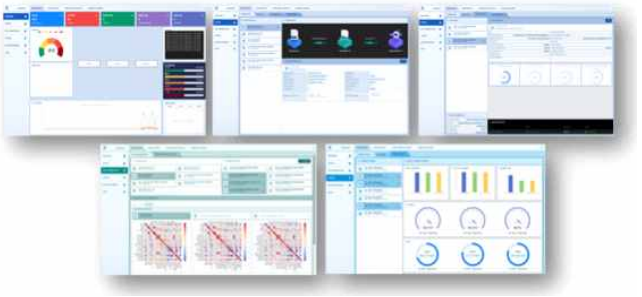
2.2 지능형 자기지도학습 모델 관리 프레임워크 구조 및 주요 기능

5G 특화망의 네트워크 보안을 위해서는 다양한 구축유형 및 서비스 환경에 능동적으로 적용가능 하면서 특히, 방대한 네트워크 데이터로부터 학습을 위한 데이터 라벨링 문제뿐만 아니라 정상/비정상 데이터 분포 및 품질 문제를 해결하면서 지능화 정교화되는 네트워크 위협을 탐지하기 위한 인공지능기반 위협탐지 분석 모델이 요구된다.

수행중인 사업에서는 이를 해결하기 위한 비라벨 네트워크 데이터를 이용한 자기지도학습 기반의 지능형 위협분석 모델을 개발중에 있으며, 본 절에서는 이러한 모델 개발을 지원하기 위한 비라벨 자기지도학습 다종모델 학습관리 프레임워크 기능을 소개하고 개발 결과를 기술한다. <그림1>에 제시된 바와 같이, 비라벨 자기지도학습 다종모델 학습관리 프레임워크의 주요 기능은 다음과 같다.

- **학습데이터셋 관리 기능 :** 수집된 패킷데이터에 대한 전처리를 통해 패킷단위 메타정보 추출, 네트워크 플로우 피쳐추출을 통한 네트워크 플로우 학습 데이터셋 구성
- **데이터 증강 관리 기능 :** 네트워크 플로우 피쳐 데이터셋을 이용하여 비라벨 자기지도학습에 필요한 데이터 증강 및 증강데이터 분석정보 가시화를 통한 고품질 데이터셋 생성 관리
- **자기지도학습을 위한 모델 학습 관리 기능 :** 네트워크 플로우 데이터와 증강된 데이터를 기반으로 다종의 인코더 지원을 통한 자기지도학습의 Pretext Task 단계 학습 지원 및 소량의 라벨 데이터를 이용한 분류기 Fine-tuning 등 Downsteam Task 학습관리, 생성된 모델 성능 분석 지원을 통한 고품질 모델 생성 관리
- **침해위협 탐지정보 가시화 기능 :** 생성된 모델을 이용한 실시간 침해위협 탐지 및 탐지정보 가시화를 통해 5G 특화망 서비스 이용 환경에 최적화된 모델 지원 관리

<그림2>는 전술한 지능형 자기지도학습 모델관리 프레임워크의 개발 결과물 예시로, 지능형 자기지도학습 모델관리 프레임워크를 통해 학습 데이터를 구성하고, 데이터 증강과 자기지도학습을 통한 모델을 생성하여, 실환경에서 수집된 네트워크 데이터 적용을 통해 침해위협 탐지 기능을 시험하였다.



〈그림 2 〉 지능형 자기지도학습 모델관리 프레임워크 개발 예시

Ⅲ. 결 론

본 논문에서는 5G 특화망 및 기업망과의 통합환경을 위한 지능형 5G 특화망 보안관리 서비스 플랫폼을 위한 지능형 자기지도학습 모델관리 프레임워크 기능과 개발결과를 제시하였다.

제안한 지능형 자기지도학습 모델관리 프레임워크는 다양한 5G 특화망 구축 유형 및 서비스 유형에 적용가능하며 네트워크 데이터의 라벨링 문제를 해결하면서 고신뢰 위협분석을 위한 모델 생성관리를 지원한다. 향후, 기술개발 보완 및 실 서비스 환경에 적용가능 하도록 실증을 통한 기능을 검증하고 보완하고자 한다.

ACKNOWLEDGMENT

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT)(No. RS-2024-00397469, Development of Private 5G Security Technology for Integrated Private 5G and Enterprise Network Security).

참 고 문 헌

[1] 박노삼." 인공지능기반 네트워크 침입탐지 및 사이버보안 기술동향", 전자통신동향분석지, 제40권, pp. 40-51, 2025.

[2] J. Morimoto, "Private 5G Network Security Expectations Part 1", trendmicro.com.https://www.trendmicro.com/en_us/research/22/g/private-5g-network-security-part-1.html.

[3] A. Weinberg, "Top 10 Cyber Threats to Private 5G/LTE Networks",firstpoint-mg.com.https://www.firstpoint-mg.com/blog/top-10-cyber-threats-to-private-5g-ltenetworks/

[4] 한미경." 5G특화망 및 기업망 통합보안을 위한 지능형 네트워크 보안 플랫폼 구조에 관한 연구", 한국통신학회 추계학술대회, pp. 0767-0768, 2024.