오픈랜 시스템에서의 네트워크 이상 탐지 연구 동향

이예린, 위성률, 송승엽, 박희재, 박래혁
서울과학기술대학교
{21101146, holylaw, sysong, prkhj98, lhpark}@seoultech.ac.kr

Research Trends on Network Anomaly Detection in Open RAN System

Yerin Lee, Seongryool Wee, Seungyeop Song, Heejae Park, Laihyuk Park
Seoul National Univ. of Science and Technology

요 약

O-RAN (Open Radio Access Network) 은 개방형 인터페이스와 분산 아키텍처를 기반으로 네트워크의 유연성과 지능형 자동화를 구현하는 차세대 무선 접속망 구조이다. 하지만 RIC (RAN Intelligent Controller) 을 중심으로 다양한 xApp과 개방형 인터페이스가 연동되는 O-RAN은 시스템 복잡도가 높고 공격 표면이 넓어, 비정상적인 트래픽 및 악의적인 제어 시그널링과 같은 네트워크 이상 발생 가능성이 크다. 이에 따라 O-RAN에 특화된 지능형 이상 탐지 기술의 중요성이 점차 부각되고 있다. 본 논문에서는 O-RAN 아키텍처 특성을 반영한 네트워크 이상 탐지 기술의 최신 연구 동향을 정리하였다.

Ⅰ. 서론

O-RAN (Open Radio Access Network) 은 개방형 인터페이스와 RAN 기능 분리를 기반으로 지능형 RAN 운영을 지원하는 네트워크 아키텍처이다. 이러한 개방성과 유연성은 동시에 시스템 복잡도를 증가시키고 새로운 보안 및 운영상의 위험을 초래한다 [1]. 특히 O-RAN 시스템에서는 개방형 인터페이스, RAN Intelligent Controller (RIC) 중심의 제어 구조와 xApp의 도입으로 인해 기존 RAN 대비 새로운 보안 위협이 발생할 가능성이 제기되고 있다 [2].

또한, O-RAN은 Near-RT RIC이 RAN 구성 요소들을 중앙에서 제어하는 구조적 특성으로 인해 제어 오류나 비정상 동작이 네트워크 전반으로 빠르게 전파될 수 있다. 이로 인해, 전체 네트워크의 서비스 품질 (QoS: Quality of Service) 저하가 발생할 수 있다 [3]. 이와 같이 O-RAN 환경에서는 문제 발생 시 그 영향이 빠르게 확산될 수 있으므로, RIC 및 개방형 인터페이스의 특성을 고려한 네트워크 이상 탐지 기술의 중요성이 부각되고 있다. 본 논문에서는 O-RAN 시스템에서의 네트워크 이상 탐지에 관한 최신 연구들을 정리하였다.

Ⅱ. O-RAN 네트워크 이상 탐지 연구 동향

연구 [3]에서는 Near-RT RIC이 제어 신호를 집중적으로 처리하는 구조를 고려하여, 악의적인 제어 시그널링이 발생할 경우 서비스 거부 및 네트워크 불안정성이 초래될 수 있음을 공격 시나리오로 설명하였다. 이를 해결하기 위해 저자들은 프로토콜 적합성 검증과 상태 전이 분석을 기반으로 비정상적인 제어 신호 및 트래픽 패턴을 탐지하는 방식을 적용하였다. 실험 결과, 제안된 기법은 정상 동작과 공격 시나리오를 구분하고, 악의적인 제어 메시지에 의해 발생하는 비정상적인 신호 패턴을 효과적으로 탐지하였다. 이를 통해 O-RAN 시스템에서 네트워크 이상 탐지가 안정적인 운영과 보안을 위한 요소임을 확인하였다.

연구 [4]에서는 5G O-RAN 환경에서 수집된 KPI (Key Performance Indicator) 데이터셋을 사용하여, 기존 머신러닝 기반 네트워크 이상 탐지 기법들의 성능을 평가하였다. 저자들은 O-RAN 구조에서 발생하는 다양한 네트워크 상태 정보를 KPI 형태로 수집하고, 다층 퍼셉트론 (MLP: Multilayer Perceptron), 결정 트리 (Decision Tree), 서포트 벡터 머신 (SVM: Support Vector Machine) 모델을 적용하여 정상 상태와 이상 상태를 탐지하였다. 또한 O-RAN 환경에서 이상 상황에 대한 레이블링의 어려움을 고려하여, t-SNE (t-Distributed Stochastic Neighbor Embedding) 을 활용한 시각화 기반 라벨링 보조 기법을 적용하였다. 실험 결과, 모든 모델에서 90% 이상의 이상 탐지 정확도를 달성하였으며, 이를 통해 KPI 기반 지도학습 방식이 O-RAN 환경에서도 효과적인 이상 탐지 수단으로 활용 가능함을 확인하였다.

연구 [5]에서는 네트워크 이상 탐지 기법을 검증하기 위해 srsRAN 기반 오픈소스 O-RAN 테스트베드를 구축하고, AI 기반 이상 탐지 프레임워크를 평가하였다. 저자들은 5G O-RAN 시스템에서 다수의 사용자 장비 (UE: User Equipment) 와 다양한 무선 환경을 반영한 테스트 시나리오를 구성하고, 이를 통해 대규모 네트워크 트래픽 데이터를 수집하였다. 수집된 데이터는 총 31개의 네트워크 특성을 포함한다. 이후 주성분 분석 (PCA: Principal Component Analysis) 을 통해 차원을 축소한 후 DNN (Deep Neural Network) 을 적용하여 정상 트래픽과 비정상 트래픽을 탐지하였다. 저자들은 시뮬레이션을 통해 DNN 기반 트래픽 이상 탐지 기법이 높은 분류 정확도와 낮은 지연 시간을 달성함을 보였다. 특히 비정상 트래픽의 한 사례로 설정된 사용자 식별자 변조 공격에 대해서도 효과적인 탐지 성능을 보였다.

연구 [6]은 xApp을 통해 RF (Radio Frequency) 이상을 탐지하기 위한 딥 오토인코더 기반 모델을 제안하였다. 해당 연구에서는 UE에서 수집된 RF 관련 지표를 입력 데이터로 사용하여 정상 동작 상태의 특성을 학습한 후, 재구성 오차를 기반으로 이상 여부를 판단한다. 이러한 접근 방식은

사전 레이블링이 어려운 RF 이상 상황을 효과적으로 탐지할 수 있다는 장점을 가진다. 또한 제안된 모델은 xApp 형태로 Near-RT RIC 상에서 실행 가능하도록 설계되어, O-RAN의 실시간 제어 구조를 고려한 딥러닝 기반 RF 이상 탐지 기법의 적용 가능성을 제시했다. 특히 정상 상태의 패턴을 재구성하는 오토인코더 구조를 활용함으로써, 복잡한 다중 클래스 분류 과정 없이 이상 여부를 판단할 수 있어 연산 복잡도를 낮출 수 있다. 실험 결과, 제안한 딥 오토인코더 모델은 기존의 경량 이상 탐지 기법 대비 더 높은 탐지 정확도를 보였다.

연구 [7]에서는 Near-RT RIC을 대상으로 한 보안 위협을 분석하고, A1 인터페이스의 취약성을 중심으로 이상 탐지 및 보안 검증의 필요성을 논의하였다. 저자들은 Near-RT RIC을 대상으로 A1 인터페이스에 대한 정적 분석과 동적 보안 테스트를 수행하여, 접근 제어 미흡, 암호화 미적용, 정책 검증 부재와 같은 취약점을 확인하였다. 특히 악의적인 정책 주입을 통해 서비스 거부 (DoS: Denial of Service) 및 제어 지연을 유발할 수 있음을 검증하였으며, 일부 구현에서는 A1 요청에 대해 수 초 이상의 응답 지연이 발생함을 보였다. 저자들은 실험을 통해 부적절한 정책 주입이 Near-RT RIC 기반 중앙 제어 구조에서 O-RAN 시스템의 안정성과 가용성에 직접적인 위협으로 작용할 수 있음을 확인하였다.

Ⅲ. 결론

본 논문에서는 O-RAN 아키텍처의 특성을 고려한 네트워크 이상 탐지 연구에 대한 최신 연구 동향을 정리하였다. 향후 연구에서는 트래픽의 시계열 특성을 반영한 딥러닝 기반 이상 탐지 기법과 Near-RT RIC의 실시간 제약을 고려한 경량 이상 탐지 모델을 O-RAN 제어 구조에 적용한 연구를 조사할 예정이다.

ACKNOWLEDGMENT

본 연구는 정부 (과학기술정보통신부)의 재원으로 한국연구재단의 지원 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (RS-2025-16070295, IITP-2026-RS-2022-00156353)

참 고 문 헌

[1] Polese, Michele, et al. "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges." IEEE Communications Surveys & Tutorials 25.2 (2023): 1376-1411.

[2] Motalleb, Mojdeh Karbalaee, et al. "Towards secure intelligent O-RAN architecture: vulnerabilities, threats and promising technical solutions using LLMs." Digital Communications and Networks (2025).

[3] Hung, CHENG-Feng, CHI-Heng Tseng, and Shin-Ming Cheng. "Anomaly Detection for Mitigating xApp and E2 Interface Threats in O-RAN Near-RT RIC." IEEE Open Journal of the Communications Society (2025).

[4] Alves, Pedro VA, et al. "Machine learning applied to anomaly detection on 5g o-ran architecture." Procedia Computer Science 222 (2023): 81-93.

[5] Parada, Raúl, et al. "An open testbed for O-RAN experimentation with AI-enabled control and monitoring." Internet of Things (2025): 101729.

[6] Başaran, Osman Tugay, et al. "Deep autoencoder design for RF anomaly detection in 5G O-RAN Near-RT RIC via xApps." 2023 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2023.

[7] Thimmaraju, Kashyap, et al. "Security testing the o-ran near-real time ric & a1 interface." Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2024.