O-RAN Near-RT RIC 환경에서 악의적 xApp 제어의 선제적 차단을 위한 LSTM 기반 Active - Standby 보안 기법

박종현[1], 이재민[2], 김동성*

금오공과대학교, 전자공학부[1,2,*]

{dooq1123[1], ljmpaul[2], dskim*}@kumoh.ac.kr

Design of an LSTM-Based Active - Standby Security Scheme for Preemptive Blocking of Malicious xApp Control in O-RAN Near-RT RIC

Jong-Hyeon Park[1], Jae-Min Lee[2], and Dong-Seong Kim*

Kumoh National Institute of Technology School of Electronic Eng.[1,2,*]

요 약

본 논문은 O-RAN에서 Near-RT RIC(Near Real-Time RAN Intelligent Controller) 상에서 동작하는 xApp의 구조적 보안 취약성 문제를 다룬다. xApp은 무선 자원 제어에 직접 관여하는 3rd-party 애플리케이션으로, 보안 침해 시 RAN 성능에 즉각적인 영향을 미치지만 기존 연구들은 주로 공격 발생 이후의 사후 대응에 초점을 두어 공격자의 제어권 장기 점유를 효과적으로 제한하지 못한다. 이에 본 논문에서는 Near-RT RIC에서 수집되는 KPI(Key Performance Indicator) 시계열 데이터를 기반으로 정상 제어 패턴을 학습하는 LSTM(Long Short-Term Memory) 기반 이상 탐지 모델을 적용하고, Active - Standby 이중화 구조를 통해 xApp 인스턴스를 신속히 전환하는 선제적 보안 아키텍처를 제안한다. 시뮬레이션 결과, 제안 기법은 공격 구간에서 KPI 이상을 조기에 탐지하고 짧은 시간 내 전환을 수행함으로써 Near-RT RIC 환경에서 요구되는 제어 연속성과 실시간성을 효과적으로 만족함을 확인하였다.

Ⅰ. 서 론

개방형 무선 접속망(O-RAN)은 기존 RAN의 폐쇄적 구조를 탈피하여 개방성과 유연성을 강화한 아키텍처를 지향한다[1]. Near-RT RIC(Near Real-Time RAN Intelligent Controller)를 중심으로 3rd-party 애플리케이션인 xApp을 활용한 지능형 무선 자원 제어가 가능해졌으나, 외부 개발자가 구현한 xApp이 제어에 직접 관여함으로써 새로운 보안 취약점이 발생한다[2]. 특히 Near-RT RIC는 실시간 제어를 담당하므로, xApp 침해는 RAN 제어 안정성에 즉각적인 영향을 미칠 수 있다. 기존 O-RAN 보안 연구들은 주로 공격 발생 이후의 성능 복구나 xApp 내부 AI 모델의 강건성 향상에 초점을 두어, 공격자의 제어권 장기 점유를 구조적으로 차단하는 데에는 한계를 가진다[3]. 이에 본 논문에서는 Near-RT RIC 환경에서 관측되는 KPI 시계열을 기반으로 정상 제어 패턴을 학습한 LSTM(Long Short-Term Memory) 기반 이상 탐지 모델을 통해 xApp의 비정상적인 제어 행위를 성능 저하 이전 단계에서 선제적으로 포착하고, Active - Standby 이중화 구조를 통해 xApp 인스턴스를 즉시 전환함으로써 서비스 중단 없이 대응하는 보안 메커니즘을 제안한다.

Ⅱ. 관련 연구 및 문제점 분석

기존 O-RAN 보안 연구들은 주로 xApp 내부 AI 모델의 강건성 향상이나, 침해 발생 이후 제어 성능을 복구하는 사후 대응 중심의 접근을 취해 왔다[4]. 이러한 방식은 공격 이후의 영향 완화에는 효과적이나, 공격자의 제어권 장기 점유를 구조적으로 차단하는 데에는 한계를 가진다. xApp은 Near-RT RIC를 통해 무선 자원 제어에 직접 관여하는 3rd-party 애플리케이션으로, 단일 인스턴스로 운용될 경우 침해 시 공격자가 제어권을 독점할 가능성이 존재한다. 이는 단순한 AI 모델 성능 개선만으로는 해결하기 어려운 구조적 취약점으로, Near-RT RIC 환경에서는 제어 이상을 조기에 탐지하고 오염된 xApp을 즉시 배제할 수 있는 운용 구조 차원의 보안 대응 메커니즘이 요구된다.

Ⅲ. 제안하는 Active - Standby 기반 xApp 보안 기법

그림 1은 본 논문에서 제안하는 Near-RT RIC 내 Active - Standby 기반 xApp 보안 아키텍처를 나타낸다. 제안 구조는 Near-RT RIC 내부에 독립적인 보안·감시 모듈을 추가하고, 동일 기능의 xApp 인스턴스를 Active와 Standby 상태로 이중화하여 운용하는 것을 특징으로 한다. Near-RT RIC는 E2 인터페이스를 통해 O-DU(Distributed Unit)/O-CU(Central Unit)로부터 KPI(Key Performance Indicator) 및 상태 정보를 수집하며, Active 상태의 xApp은 이를 기반으로 무선 자원 제어를 수행한다.

구조에서 보안·감시 모듈은 xApp 내부의 알고리즘 구조나 학습 파라미터를 직접 분석하지 않고, Near-RT RIC에서 관측되는 입력 KPI와 출력 제어 결과의 시계열 패턴을 외부에서 관찰한다. 이를 통해 정상 운용 구간

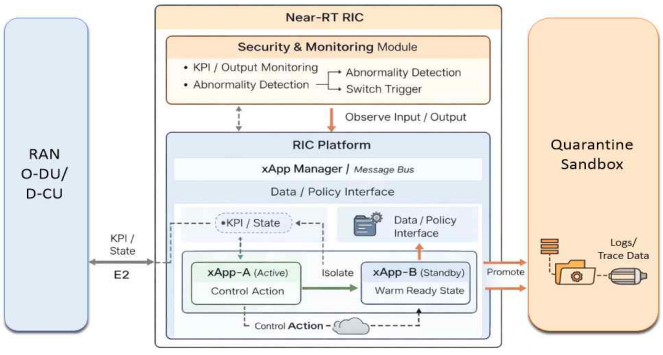

그림 1 Near-RT RIC 내 Active - Standby xApp 기반 보안 아키텍처

에서 형성된 제어 행위의 시간적 패턴을 학습하고, 실제 제어 결과가 해당 패턴에서 이탈하는지를 지속적으로 분석함으로써 침해가 완전히 발생하기 이전 단계에서 나타나는 비정상 제어 징후를 탐지한다.

본 논문에서는 이러한 이상 징후를 식별하기 위해 정상 운용 구간의 KPI 시계열 데이터를 학습한 LSTM 기반 이상 탐지 기법을 적용한다. LSTM 모델은 과거 일정 구간의 KPI 시퀀스를 입력으로 받아 다음 시점의 KPI 값을 예측하며, 실제 관측된 KPI 값과 예측값 간의 차이를 이상 점수로 정의한다. 해당 예측 오차 기반 이상 점수는 KPI의 평균적인 변화 이전에 나타나는 시간적 패턴 붕괴를 반영하므로, 점진적이거나 은닉된 제어 조작 공격을 선제적으로 포착할 수 있다. 수식 1의 $S(t)$는 LSTM 모델의 예측 결과와 실제 KPI 관측값 간의 오차로부터 산출된 이상 점수이며, 수식 2의 $\hat{K}(t)$는 LSTM 모델에 의해 예측된 KPI 벡터이다.

$$t) = \quad K(t) - K(t) \parallel \qquad (1)$$

$$\hat{K}(t) = LSTM(K(t-n), \ldots, K(t-1)) \qquad (2)$$

$K(t)$는 실제 관측된 KPI 값이다. 임계값 Θ는 정상 운용 구간에서 관측된 이상 점수 분포를 기반으로 경험적으로 설정되며, 단발성 노이즈나 일시적인 트래픽 변동에 의한 오탐지를 방지하기 위해 이상 점수가 연속적인 T 구간에서 이상이 지속될 경우에 제어 이상 상태로 판단한다. 이를 통해 공격이나 오염으로 인해 지속적으로 발생하는 제어 행위 변형만을 효과적으로 식별할 수 있도록 설계하였다. 이상 징후가 감지될 경우, 보안·감시 모듈은 Near-RT RIC 플랫폼 내 xApp Manager를 통해 현재 Active 상태의 xApp-A를 즉시 제어 경로에서 분리한다. 동시에 Standby 상태로 대기 중이던 xApp-B를 Active 상태로 승격하여 무선 자원 제어를 이어받도록 한다. Standby xApp은 사전에 warm-ready 상태로 유지되므로, 이 전환 과정은 RIC 내부에서 신속하게 수행되며 서비스 중단 없이 제어 연속성을 유지할 수 있다. 격리된 xApp-A는 Quarantine Sandbox로 이동되어 로그 및 트레이스 데이터가 수집되며, 이는 사후 분석이나 복구를 위한 자료로 활용될 수 있다. 본 논문에서는 공격자의 제어권 지속 시간을 최소화하는 구조적 대응 메커니즘에 초점을 둔다. 이를 통해 기존의 사후 대응 중심 보안 접근과 달리, O-RAN Near-RT RIC 환경에서 요구되는 실시간성을 유지하면서 선제적으로 보안 위협을 완화할 수 있는 구조를 제공한다.

IV. 시뮬레이션

본 논문에서는 실제 O-RAN Near-RT RIC 환경의 제어 특성을 모사하여 생성한 시뮬레이션 기반 KPI 시계열 데이터셋을 사용하고, 정상 운용 구간의 KPI 시계열로 학습된 LSTM 기반 이상 탐지 모델에 제어 조작 공격을 주입하여 제안 기법의 동작을 검증하였다. 그림 2는 시간에 따른 LSTM 기반 이상 점수와 임계값을 함께 나타내며, 공격 구간에서 KPI 값의 단순 크기 변화만으로는 이상 여부를 식별하기 어려운 상황에서, 제어 패턴 불일치로 인해 이상 점수가 임계값을 초과하고 xApp 전환이 발생하는 과정을 보여준다. 이상 탐지 시 Active xApp은 격리되고 Standby xApp이 제어를 이어받으며, 이후 이상 점수는 정상 수준으로 복귀한다. 표 1은 제안한 이상 탐지 모델의 정량적 성능을 요약한 것으로, 정상 운용 구간에서 오탐 없이 안정적으로 동작하면서도 공격 발생 이후 제한된 지연 내에 탐지가 가능함을 확인하였다. 이를 통해 제안 기법이 Near-RT RIC 환경에서 KPI 성능 저하가 명확히 관측되기 이전 단계에서도 제어 연속성을 유지하는 선제적 보안 대응이 가능함을 보였다.

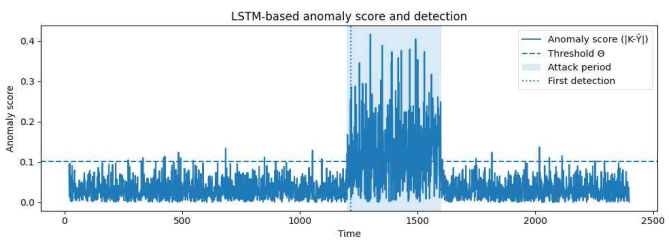

그림 2 LSTM 기반 이상 점수 및 임계값 기반 탐지 결과

표 1 LSTM 기반 탐지 기법의 성능

Metric	Value
Threshold Θ (percentile)	99%
Consecutive window T	5
Precision	1.000
Recall	0.060
False Positive Rate (FPR)	0.000
Detection Delay (steps)	17

V. 결론

본 논문은 Near-RT RIC 환경에서 xApp의 제어 행위를 LSTM 기반 이상 탐지 기법으로 감시하고, 이상 징후 발생 시 xApp을 격리하여 대기 인스턴스로 전환함으로써 서비스 연속성을 유지할 수 있는 보안 구조를 제시하였다. 제안 기법은 정상 KPI 데이터로 학습된 LSTM 기반 이상 탐지를 통해 Near-RT RIC 환경에서 실시간 제어를 저해하지 않는 선제적 보안 대응이 가능함을 확인하였다. 이를 통해 제안 기법이 Near-RT RIC 환경에서 실시간 제어를 저해하지 않는 선제적 보안 대응 구조로 활용 가능함을 보였다. 향후 연구에서는 공개된 실제 침입 데이터를 활용한 실험과 다양한 공격 시나리오를 고려한 분석을 통해 제안 기법의 실효성과 확장성을 보완·검증할 예정이다.

ACKNOWLEDGMENT

본 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 지역지능화혁신인재양성사업(IITP-2025-RS-2020-II201612, 33%)과 2025년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(2018R1A6A1A03024003, 33%)과 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터사업의 연구결과로 수행되었음 (IITP-2025-RS-2024-00438430, 34%)

참 고 문 헌

[1] W. J. Ryu, Y. J. Kwon, H. J. Shin, J. M. Lee, and D. S. Kim, "A Study on RIC Applying Deep Reinforcement Learning to Resolve Conflicts Between Interference and QoS xApps in ORAN Networks," in Proc. KICS Winter Conf., pp. 414-415, 2024.

[2] C.-F. Hung, C.-Y. Chen, T.-C. Chiu and S.-M. Cheng, "Security Threats to xApps Access Control and E2 Interface in O-RAN," IEEE Open Journal of the Communications Society, vol. 5, pp. 1 - 16, 2024.

[3] A. Lacava, S. Maxenti, L. Bonati, S. D'Oro and T. Melodia "O-RAN xApps: Survey and Research Challenges," Computer Networks, vol. 238, pp. 1-46, 2025.

[4] M. Karbalaee Motalleb, C. Benzaid, T. Taleb, M. Katz, V. Shah-Mansouri and J. Kim, "Towards secure intelligent O-RAN architecture: vulnerabilities, threats and promising technical solutions using LLMs," Digital Communications and Networks, pp. 1-12, 2025.