Open RAN에서의 E2 인터페이스 보호를 위한 정적 ARP 테이블 관리 xApp 설계

김지혜[1], 박재형[2], 이종혁[3]
[1]세종대학교 정보보호학과 학부생
[2]세종대학교 정보보호학과 & 지능형드론 융합전공 석사과정
[3]세종대학교 정보보호학과 & 지능형드론 융합전공 교수
jihye@pel.sejong.ac.kr, jaehyoung@pel.sejong.ac.kr, jonghyouk@sejong.ac.kr

Design of a Static ARP Table Management xApp for an E2 Interface Security in Open RAN

Jihye Kim[1], Jaehyoung Park[2], Jong-Hyouk Lee[3]
[1]Dept. of Computer and Information Security, Sejong University
[2, 3]Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University

요 약

Open RAN(Radio Access Network)을 선도적으로 연구하고 있는 O-RAN Alliance에서는 Open RAN의 E2 인터페이스에서 발생 가능한 보안 위협 중 하나로 MitM(Man-in-the-Middle) 공격을 명시하였다. 그러나 이에 대응하기 위한 보안 요구사항으로는 3계층 보안 프로토콜인 IPsec 사용을 명시하고 있으며, 2계층 공격인 ARP(Address Resolution Protocol) 스푸핑에 대한 요구사항은 명시하고 있지 않다. 따라서 본 논문에서는 MitM 공격 중 하나인 ARP 스푸핑으로부터 E2 인터페이스를 보호하기 위해, Near-RT RIC의 ARP 테이블에서 E2 인터페이스로 연결되는 장비에 대한 MAC 주소를 정적으로 설정할 수 있는 xApp을 제안한다.

1. 서론

최근 차세대 이동통신 기술을 위해 연구되고 있는 Open RAN(Radio Access Network)은 RAN의 개방화 및 지능화를 위해 등장한 개념으로, 서로 다른 벤더 간의 상호운용을 가능하게 한다. Open RAN에서는 데이터를 비실시간(1초 이상)과 근실시간(0.1초~1초)으로 처리하는 2개의 RIC(RAN Intelligent Controller)을 활용하여 RAN의 자동화 및 최적화를 지원한다[1]. Near-RT(Real-Time) RIC가 E2 인터페이스를 통해 안전하게 RAN을 최적화하기 위해서는 E2 인터페이스에서 발생 가능한 보안 위협에 대응할 수 있어야 한다[2]. 따라서 본 논문에서는 E2 인터페이스에 대한 보안 위협 중 하나인 MitM(Man-in-the-Middle) 공격으로부터 E2 인터페이스를 보호하기 위한 기술을 xApp으로 설계하여 제안한다.

2. E2 인터페이스 보안 위협

O-RAN Alliance는 Open RAN을 선도적으로 연구하고 있는 사실표준화 기구이다. O-RAN Alliance에서는 기존 RAN에 새로운 컴포넌트 및 인터페이스가 추가된 Open RAN에서의 보안 위협과 보안 요구사항을 정의하여 표준 문서로써 제공하고 있다. RAN의 지능화를 위해 활용되는 E2 인터페이스 보호 방안을 연구하기 위해, O-RAN Alliance가 제공하는 표준 문서에서 E2 인터페이스에 대한 보안 위협을 분석하였으며, 이는 <표 1>과 같다[3].

<표 1> E2 인터페이스 보안 위협

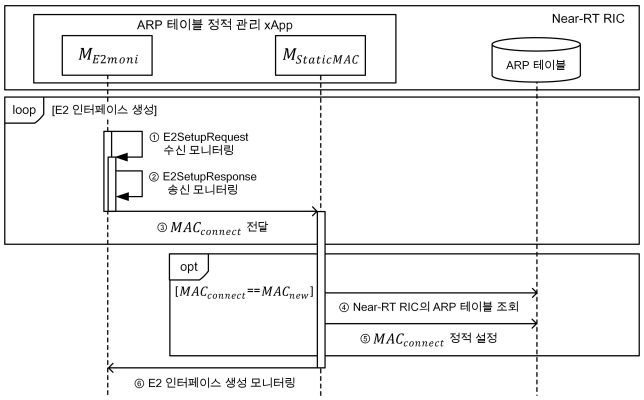
No.	위협 제목	위협 설명
1	Near-RT RIC와 RAN 노드 간의 약한 상호 인증	악의적인 Near-RT RIC와 E2 노드는 E2 인터페이스를 통해 통신 가능
2	악의적인 행위자의 메시지 모니터링 및 수정	악의적인 행위자는 E2 인터페이스의 MitM을 통해 메시지에 접근하여 메시지 조회, 수정, 삽입 가능

3. ARP 테이블 정적 관리 xApp

O-RAN Alliance의 보안 위협 표준 문서를 통해 E2 인터페이스에서는 MitM 공격이 발생 가능함을 확인할 수 있다. 본 논문에서는 E2 인터페이스 2계층에서 발생 가능한 MitM 공격을 보호하기 위한 xApp을 설계한다. ARP(Address Resolution Protocol) 스푸핑이란 공격자가 정상 장비들의

MAC(Media Access Control) 주소를 공격자의 주소로 변조하여 위장하는 공격이므로, 이에 대응하기 위해서는 정상 장비들의 MAC 주소를 정적으로 설정해야 한다. 따라서, Near-RT RIC의 정적 ARP 테이블 관리 xApp에서는 E2 인터페이스로 연결되는 E2 노드의 MAC 주소를 정적으로 설정한다.

정적 ARP 테이블 관리 xApp에서 활용되는 모듈은 E2 인터페이스 모니터링 모듈인 M_{E2moni}와 MAC 주소 정적 설정 모듈인 $M_{StaticMAC}$이며, 각 모듈은 Near-RT RIC에 내장된 xApp에서 동작한다. 정적 ARP 테이블 관리 xApp은 M_{E2moni}로 E2 인터페이스가 생성되는 과정을 모니터링하고, $M_{StaticMAC}$로 E2 인터페이스에 새로 연결되는 E2 노드의 MAC 주소를 정적으로 설정한다. 정적 ARP 테이블 관리 xApp의 동작과정은 (그림 1)과 같다.



(그림 1) ARP 테이블 정적 관리 xApp 동작과정

먼저 E2 인터페이스 생성 모니터링 단계에서는 M_{E2moni}이 Near-RT RIC 내에서 수신되는 패킷을 주기적으로 모니터링한다. 해당 단계에서는 새로운 E2 노드로부터 ***E2SetupRequest*** 패킷을 수신하는지 모니터링하고, Near-RT RIC가 해당 E2 노드에게 ***E2SetupResponse*** 패킷을 송신하는지 모니터링한다. Near-RT RIC가 두 과정을 순차적으로 수행한 경우, M_{E2moni}은 E2 인터페이스가 생성된 것으로 간주한다. ***E2SetupRequest***는 E2 노드가 Near-RT RIC에게 E2 인터페이스 연결을 요청하는 패킷이고, E2SetupResponse는 Near-RT RIC가 해당 E2 노드와의 E2 인터페이스 연결을 승인하는 응답 패킷이다. 따라서 두 패킷을 송수신하는 경우, Near-RT RIC와 E2 노드 간의 E2 인터페이스가 수립된 것을 의미한다. 이때 M_{E2moni}은 E2 인터페이스 연결 수립이 완료된 E2 노드의 MAC 주소인 $MAC_{connect}$를 $M_{StaticMAC}$에 전달한다.

다음으로 정적 ARP 테이블 설정 단계로, M_{E2moni}는 $M_{StaticMAC}$에게 $MAC_{connect}$를 전달함과 동시에 E2 인터페이스가 생성되었음을 알린다. 이를 수신한 $M_{StaticMAC}$은 Near-RT RIC의 ARP 테이블을 조회하여 새로 추가된 MAC 주소가 있는지 확인하고, 이를 MAC_{new}로 설정한다. 이때 MAC_{new}와 $MAC_{connect}$가 동일한 경우, 해당 MAC 주소를 정적 설정한다. 이후에 다시 M_{E2moni}이 E2 인터페이스 생성 모니터링을 반복적으로 수행함으로써 Near-RT RIC의 ARP 테이블 내 MAC 주소를 정적으로 관리한다. 따라서, 새로운 E2 노드의 MAC 주소는 변조될 수 없으므로 공격자의 ARP 스푸핑을 방지할 수 있다.

4. 결론

O-RAN Alliance 표준 문서를 통해 Near-RT RIC가 E2 인터페이스를 활용하여 RAN 노드를 제어하는 도중, MitM 공격이 발생할 수 있음을 확인하였다. 따라서 본 논문에서는 2계층 MitM 공격인 ARP 스푸핑으로부터 E2 인터페이스를 보호하기 위한 Open RAN 전용 xApp을 설계하였다. ARP 스푸핑은 MAC 주소가 변조되는 공격이므로, Near-RT RIC의 ARP 테이블에서 E2 인터페이스로 연결된 E2 노드에 대한 MAC 주소를 정적으로 설정함으로써 공격자가 ARP 스푸핑을 시도하더라도 공격에 성공하기 어렵게 한다. 제안하는 정적 ARP 테이블 관리 xApp은 ARP 스푸핑을 사전에 방지함으로써 E2 인터페이스를 보호할 수 있다. 이를 기반으로 향후 연구에서는 E2 인터페이스에 대한 ARP 스푸핑을 탐지 및 대응할 수 있는 사후 기능을 가진 xApp을 설계하여 E2 인터페이스를 보호할 수 있는 연구를 수행하고자 한다.

Acknowledgement

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00796, 상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구)

참고문헌

[1] L. Bonati, et. al., “Intelligence and Learning in O-RAN for Data-Driven NextG Cellular Networks”, *IEEE Communications Magazine*, vol. 59, no. 10, 2021.
[2] M. Liyanage, et al., “Open RAN security: Challenges and opportunities”, *Journal of Network and Computer Applications*, vol. 214, no. 103621, 2023.
[3] O-RAN ALLIANCE, “O-RAN Security Threat Modeling and Risk Assessment 2.0”, 2024.