IEEE 802.11 관리 프레임 분석을 통한 사전연결 단계 무선 네트워크 위협 탐지 연구: 규칙 기반 및 머신러닝 접근법 비교

이시연§, 이채혁§, 방인규■†, 김태훈■§

§국립한밭대학교 컴퓨터공학과, †국립한밭대학교 지능미디어공학과

{20242032, 20242073}@edu.hanbat.ac.kr, {ikbang, thkim}@hanbat.ac.kr

Pre-Association Threat Detection in Wi-Fi via IEEE 802.11 Management-Frame Analysis: A Comparative Study of Rule-Based and Machine-Learning Methods

Siyeon Lee§, Chaehyeok Lee§, Inkyu Bang■†, Taehoon Kim■§

§Department of Computer Engineering, Hanbat National University

†Department of Intelligence Media Engineering, Hanbat National University

요 약

무선 트래픽이 생활 전반으로 확산되면서 사전연결(Pre-association) 단계에서 발생하는 MITM(중간자 공격)은 네트워크의 심각한 보안 위협으로 부상하고 있다. 본 논문은 개별 프레임 단위 분석의 한계를 보완하기 위해 시간 윈도우 기반의 행위 분석을 도입하고, 이를 규칙 기반 접근법과 세 가지 머신러닝 모델(Random Forest, XGBoost, LSTM)에 각각 적용한 탐지 시스템을 제안한다. 공개 데이터셋 기반 실험에서 동일 조건으로 공정 비교 및 평가한 결과, 제안 방식이 기존 방식의 한계를 극복하고 높은 탐지 정확도를 달성함을 확인하였다.

Ⅰ. 서론

Wi-Fi 보편화와 함께 무선망 위협이 고도화되면서, 사전연결 단계에서 교환되는 802.11 관리 프레임만으로도 악성 AP 스푸핑과 강제 분리가 발생해 MITM 환경이 조성될 수 있다. 이는 암호화를 우회시키고 심각한 데이터 유출로 이어질 수 있는 치명적인 위협이다. 한편 실제 환경과 다양한 공격 시나리오를 반영한 AWID 공개 데이터셋이 제안되면서 재현 가능한 연구 기반이 마련되었지만 [1], 개별 프레임의 정적 특징만으로는 공격의 시간적 맥락을 충분히 설명하기 어렵다. 더불어 PMF(IEEE 802.11w)가 도입되었으나, pre-association 단계에서 교환되는 일부 관리 프레임은 여전히 비보호 상태로 남아 있다 [2].

본 연구는 이러한 한계를 보완하기 위해 시간 윈도우 기반 행위 분석을 도입한다. 일정 시간 창에서 관측되는 통계 패턴을 행위 기반 피처로 정식화하여 정상 활동과 악의적 행위를 구분하고, 이를 규칙 기반 모델과 머신러닝 모델(Random Forest, XGBoost, LSTM)에 각각 적용해 동일 조건에서 성능을 비교 분석한다. 본 논문을 통해 제안하는 접근법이 개별 프레임 단위 분석이 갖는 높은 오탐율 문제를 해결하고, 기존 탐지 기법의 한계를 어떻게 극복하는지 실험을 통해 입증하고자 한다.

Ⅱ. 용어 및 위협모델

802.11 관리 프레임은 무선 네트워크에서 AP와 클라이언트 간의 탐색, 인증, 연결 유지 및 해제 등의 제어 기능을 수행하는 프레임군이다[3]. 본 연구는 운용 관점의 비교 일관성을 위해 FPR@TPR=x를 사용한다. 이는 탐지율(FPR)을 x로 고정했을 때의 오탐율(FPR)을 의미하며, 본문에서는 x=0.9를 기본 운용점으로 설정한다. 위협 모델은 합법 AP의 전파 범위 내에서 공격자가 가짜 AP(Evil Twin)를 가동하거나, Deauthentication 프레임을 대량 송출해 특정 사용자의 연결을 강제로 해제하는 시나리오를 가정한다.

Ⅲ. 시스템 구현

1. 시스템 환경

본 시스템은 로컬 개발 환경에서 파이썬 기반 단일 파이프라인으로 구축되었다. 데이터 전처리, 피처 엔지니어링, 모델 학습 및 평가가 동일 장비에서 수행되며, 실험 재현을 위해 하드웨어 및 소프트웨어 사양을 표 1에 요약하였다.

표 1 실험 환경 구성

구분	사양
CPU	Intel Core Ultra 7 155H
GPU	Intel Arc Graphics
RAM	32GB
OS	Windows 11 Home
Software	Python 3.10, scikit-learn 1.3, XGBoost 2.0, TensorFlow 2.12
Dataset	AWID3 (Combined & Filtered)

2. 시스템 구조

본 시스템의 대규모 802.11 트래픽으로부터 MITM 전조를 조기 탐지하기 위한 AI 모델링 파이프라인으로 설계되었다. 전체 시스템은 데이터 재구성, 피처 엔지니어링, 모델 학습 및 평가의 세 단계로 구성되며, 각 단계는 탐지 성능과 해석 가능성을 동시에 극

■ Corresponding Authors: Inkyu Bang (ikbang@hanbat.ac.kr), Taehoon Kim (thkim@hanbat.ac.kr)

대화하도록 설계하였다.

먼저, 원본 AWID3 데이터셋에서 연구 목표와 무관한 공격 라벨을 제거하고 Normal과 Impersonation, Deauth만 추출하여 MITM 특화 이진 분류 데이터셋으로 재구성하였다. 다음으로, 802.11 관리 프레임 지문에서 추출한 핵심 피처 6종을 사용하고, 이를 10초 단위의 시간 윈도우를 적용해 행위 기반 피처를 생성한다. 이를 통해 단일 프레임의 모호성을 줄이고 공격의 빈도, 지속성, 다변량 조합을 반영하였다. 마지막으로, 생성된 피처셋으로 규칙 기반 모델과 머신러닝 모델(Random Forest, XGBoost, LSTM)을 동일 분할에서 학습 및 평가하여 성능을 비교하였다. 특히 동일 AP의 학습 및 평가 동시 포함을 금지하여 데이터 누수를 차단했고, Precision, Recall, F1과 함께 FPR@TPR=0.9를 운용 지표로 병행 보고하여 실제 운영 적합성을 검증하였다. 그림 1은 데이터셋으로부터 최종 탐지 모델을 생성하기까지의 전체 시스템 구조를 보여준다.

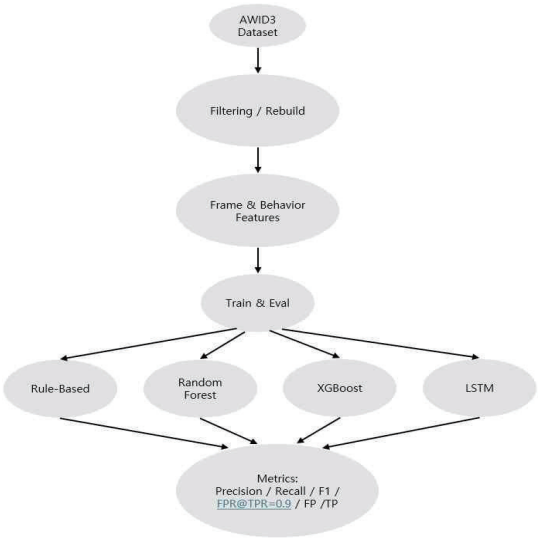

그림 1. 시스템 구조

Ⅳ. 테스트 및 결과

본 시스템의 성능을 검증하기 위해, 최종 생성된 행위 기반 피처 데이터셋을 학습용(80%)과 테스트용(20%)으로 분할하였다. 베이스라인으로 규칙 기반 모델을 설정하고, Random Forest, XGBoost, LSTM 모델의 성능을 비교 평가하였다. 평가는 정밀도, 재현율, F1-Score를 주요 지표로 사용하고, 운용 적합성 확인을 위해 FPR@TPR=0.9를 추가로 점검하였다.

표 2 윈도우링 적용 전 결과에서 규칙 기반 모델은 막대한 오탐을 발생시켰고, 머신러닝 모델들도 일부 오탐/미탐이 존재하였다. 이는 개별 프레임 단위 분석의 구조적 한계를 가지고 있음을 보여주며, 본 연구에서 제안하는 시간 윈도우 기법의 필요성을 뒷받침한다. 반면 표 3 윈도우링 적용 후 결과에서 규칙 기반 모델은 명시적 임계 규칙으로 구성되었으며, 윈도우링 적용 후 정밀도가 1.0을 기록하며 오탐이 사라지는 비약적인 성능 향상을 보였다. 다만 실제 공격 123건 중 24건을 놓쳐 재현율 0.8049로 간헐적, 저강도 공격에 대한 한계를 보였다. 머신러닝 모델은 규칙을 뛰어넘는 복합 패턴을 학습하였다. Random Forest와 XGBoost 모델은 테스트셋에서 오탐이나 미탐도 없이 완벽하게 탐지해내며 F1-Score 1.0000을 기록하여 행위 피처, 트리 앙상블의 결합이 규칙의 한계를 실질적으로 극복함을 입증하였다. 특히 두 모델 모두 FPR@TPR=0.9를 기록하여 90% 탐지율 운용점에서도 거짓경보가 발생하지 않음을 의미한다. LSTM 모델 또한 높은 성능을 보였으나, 트리 앙상블 대비 소수의 오탐과 미탐이 발생하였다.

표 2 프레임 단위(윈도우링 이전) 성능 비교

모델	정밀도	재현율	F1-Score	오탐	미탐
규칙 기반	0.0246	0.2109	0.0441	360,807	34,040
Random Forest	0.9997	0.9999	0.9998	11	6
XGBoost	0.9994	1.0000	0.9997	27	1
LSTM	0.9965	0.9992	0.9979	150	33

표 3 윈도우 기반 행위 피처 적용 후 성능 (제안 기법 성능)

모델	정밀도	재현율	F1-Score	FPR@TPR=0.9	오탐	미탐
규칙 기반	1.0000	0.8049	0.8919	-	0	24
Random Forest	1.000	1.0000	1.0000	0.0	0	0
XGBoost	1.0000	1.0000	1.0000	0.0	0	0
LSTM	0.8586	0.6911	0.7658	0.3702	14	38

※ 모든 모델에 윈도우 기반의 행위 피처가 적용된 결과임.

Ⅴ. 결론

본 논문에서는 IEEE 802.11 관리 프레임에 대한 시간 윈도우 기반 행위 피처와 머신러닝 모델을 결합하여 사전연결 단계의 MITM 전조 및 행위를 효과적으로 탐지하는 방법을 제안하였다.

실험 결과, 제안 방식은 프레임 단위 정적 분석의 한계를 극복했으며, 특히 Random Forest와 XGBoost 모델은 F1-Score 1.0000을 달성했고, FPR@TPR=0.0을 달성하며 사실상 완벽한 탐지 성능을 보였다. 이는 제안한 행위 기반 피처가 공격과 정상을 구분하는 결정적인 단서로 작용하며, 트리 기반 앙상블과의 결합이 본 문제 설정에서 특히 효과적임을 시사한다.

향후 연구로는 다양한 네트워크 환경에서 추가 실험으로 일반화 성능을 점검하고, 본 탐지 모델을 무선 침입 방지 체계(WIPS)와 연동하여 자동화된 능동 방어 체계로 확장함으로써 제안 모델의 실효성을 높일 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 국립한밭대학교 공학교육혁신센터의 「창의융합형공학인재양 성지원사업」의 지원 및 2025년도 교육부 및 대전광역시의 재원으로 대전RISE센터의 지원을 받아 수행되었음 (2025-RISE-06-002)

참 고 문 헌

[1] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,” in Proc. IEEE Conf. on Communications and Network Security (CNS), 2015, pp. 347 - 355.

[2] IEEE, “IEEE Std 802.11w-2009 – Protected Management Frames,” 2009.

[3] Y. Daldoul, “A robust certificate management system to prevent evil twin attacks in IEEE 802.11 networks,” arXiv preprint arXiv:2302.00338, Feb. 2023. doi:10.48550/arXiv.2302.00338.