네트워크 데이터 표현 방식에 따른 네트워크 이상 상황 탐지 및 공격 특성 분류 성능 비교 분석

김민광 [1] 이경호 [2], 백명선 [2]

1 세종대학교 전자정보통신공학과, 2 세종대학교 지능정보융합학과

alsrhkd326@naver.com, gyeongho@sejong.ac.kr, msbaek@sejong.ac.kr

Comparative Analysis of Network Intrusion detection and Attack Characteristic Classification Performance According to Network Data Representation

Min-Kwang Kim[1], Gyeong-Ho Lee[2], Myung-Sun Baek[2]
1 Department of Information and Communication Engineering
2 Department of Artificial Intelligence and Information Technology

요 약

본 논문은 네트워크 침입 탐지 시스템(NIDS) 환경에서 데이터 표현 방식인 원시 패킷 바이트(Raw Packet)와 통계적 플로우(Flow) 특징이 학습 모델의 탐지 성능에 미치는 영향을 분석해 보고자 한다. 동일한 딥러닝 모델 구조를 기반으로 CIC-IDS2017 데이터셋을 활용하여 비교 실험을 수행하였다. 실험 결과, 구조적 패턴 분석이 중요한 네트워크 공격은 패킷 기반 모델이, 트래픽의 거시적 통계 양상이 중요한 네트워크 공격은 플로우 기반 모델이 우수한 성능을 보임을 확인하였다. 이러한 결과는 단일 데이터 형식에 의존하는 기존 네트워크 침입 탐지 시스템의 한계를 보여주며, 향후 각 방식의 장점을 결합한 하이브리드 탐지 체계가 유효할 것으로 보인다.

Ⅰ. 서 론

최근 사이버 보안 위협이 지능화됨에 따라 기존의 규칙 기반 이상 탐지 방식은 한계에 직면했다. 따라서 이러한 한계를 극복하기 위해 딥러닝 기반의 이상 탐지 모델 도입이 활발히 연구되고 있다. 효과적인 이상 탐지 시스템을 구축하기 위해서는 정교한 모델 설계뿐만 아니라, 모델에 입력되는 데이터가 지닌 정보적 특성을 명확히 이해하는 과정이 필수적이다. 특히 네트워크 트래픽을 어떠한 단위로 정의하여 모델에 학습시킬 것인가는 이상 탐지 시스템의 최종적인 탐지 성능을 결정짓는 핵심적인 요소로 작용한다.

그간의 연구들은 주로 CIC-IDS2017 등에서 제공하는 통계적 요약치인 플로우 기반 데이터를 주요 학습 데이터로 활용해 왔다[1]. 플로우 기반 데이터는 대규모 트래픽을 효율적으로 요약할 수 있는 이점이 있으나, 특징 추출 과정에서 주관적 판단이 개입되거나 미세한 패턴 정보가 유실될 가능성이 존재한다. 따라서 원시 정보를 모두 포함하고 있는 패킷 바이너리 데이터를 직접 활용하는 방식이 더 향상된 이상탐지 성능을 제공할 수 있다는 연구가 발표되고 있다[2].

따라서 본 연구에서는 각 데이터 표현 방식이 지닌 고유한 특성을 바탕으로, 동일한 분석 환경 내에서 두 형식 간의 탐지 변별력을 비교해보고자 한다. 이에 본 연구는 플로우 데이터와 원시 패킷 기반 데이터를 동일 환경에서 학습하고 검출 성능을 분석하였다. 이를 통해 원시 패킷 바이트가 지닌 독자적인 탐지 가능성을 검토하고, 네트워크 공격의 성격에 따라 성능 우위를 보이는 데이터 표현 방식을 탐색하고자 한다.

Ⅱ. 활용 데이터셋 및 실험 모델

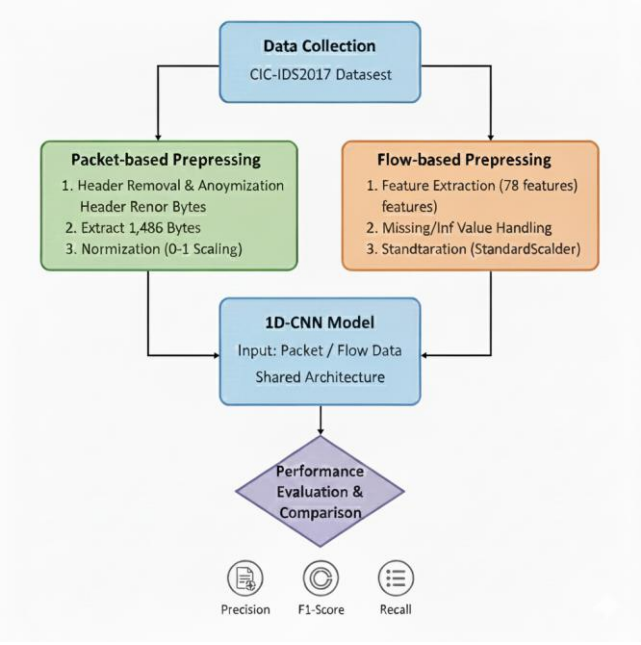

그림 1. 패킷 및 플로우 기반 분석을 위한 프레임워크

본 연구는 데이터 표현 방식별 이상 탐지 성능을 공정하게 비교하기 위하여 그림 1 과 같은 실험 구조를 채택한다. 먼저 동일한 네트워크 환경에서 수집된 원시 pcap 파일과 특징 추출된 csv 파일을 확보한 후, 각 데이터 특성에 맞는 전처리를 수행한다. 두 방식 모두 IP 주소와 같은 식별 정보가 포함될 경우 모델이 특정 단말에 편향될 위험이 있으므로, 데이터의 표현 형식과 관계없이 이를 제거하는 적절한 전처리가 요구된다. 따라서 패킷 데이터의 경우 모델이 특정 식별자에 편향되지 않도록 이더넷 및 IP 헤더를 제거하여 비식별화 처리를 완료한 후 고정 길이의 바이트 시퀀스를 추출한다. 패킷 바이너리 데이터를 직접 활용하는 방식은 원시 정보를 보존하여 세밀한 학습이 가능하게 할 수 있을 것으로 예상된다.

플로우 데이터는 추출된 통계 피처들에 표준화를 적용하여 수치적 편차를 조정한다. 가공된 각 데이터는 동일한 1D-CNN 딥러닝 모델을 거쳐 학습되며, 최종적으로 Precision, Recall, F1-score 의 평가 지표를 통해 데이터 표현 방식 간의 탐지 효율을 대조 분석한다[3].

Ⅲ. 실험 결과 및 비교 분석

표 1. 패킷 기반 분석 결과

Attack	Precision	Recall	F1-score
Benign	1	0.99	1
DoS slowloris	0.97	0.54	0.70
DoS slowhttptest	0.96	0.21	0.34
DoS hulk	0.95	1	0.97
DoS goldeneye	0.99	0.29	0.45
Heartbleed	0.99	1	0.99
FTP-Patator	0.88	1	0.94
SSH-Patator	0.99	0.91	0.95
Web Bruteforce	0.85	0.97	0.90
Web XSS	0.91	0.52	0.66
Web SQL	1	0.12	0.21
Infiltration	1	1	1
Botnet	0.91	0.97	0.94
Portscan	1	1	1
DDoS	1	1	1

표 2. 플로우 기반 분석 결과

Attack	Precision	Recall	F1-score
Benign	0.98	1	0.99
DoS slowloris	0.97	0.36	0.52
DoS slowhttptest	0.97	0.25	0.40
DoS hulk	0.99	0.96	0.98
DoS goldeneye	0.98	0.99	0.98
Heartbleed	0.89	0.96	0.92
FTP-Patator	0.99	1	1
SSH-Patator	1	0.51	0.67
Web Bruteforce	0.99	0.99	0.99
Web XSS	0.98	0.99	0.99
WeB SQL	0	0	0
Infiltration	1	0.29	0.44
Botnet	0.94	0.1	0.19
Portscan	0	0	0
DDoS	0	0	0

표 1 은 패킷 기반 네트워크 이상 탐지 및 분류 성능을 나타낸다. 또한 표 2 는 플로우 기반 네트워크 이상 탐지 및 원인 분류 성능을 보여준다. 표 1 과 같이 특정 프로토콜의 구조적 결함이나 바이트 배열의 패턴을 이용하는 네트워크 공격 유형에서는 패킷 기반 모델이 우수한 성능을 보였다. 표 1 에서 보듯, 특히 Portscan 이나 DDoS 와 같은 네트워크 공격에 F1-score 1.00 에 가까운 수치를 기록하였는데, 이는 모델이 주소 정보를 배제하고도 패킷 내의 구조적 정보를 정확히 학습했음을 시사한다.

반면, 트래픽 발생 빈도와 전송 속도 등 거시적인 통계적 흐름이 중요한 네트워크 공격 유형에서는 플로우 기반 모델이 우수한 성능을 보였다. 표 2 의 결과와 같이 Dos goldeneye, Web Bruteforce, Web XSS 등의 네트워크 공격에서 패킷 기반 분석 결과보다 더 좋은 수치를 기록하였다. 이는 해당 네트워크 공격을 탐지함에 있어 개별 패킷의 바이트 패턴보다 전체적인 트래픽 통계 정보가 더 유효한 변별력을 제공함을 의미한다.

결과적으로, 이상 탐지 시스템 설계 시 모든 공격에 단일한 분석 표현방식을 적용하기보다는 공격의 특성에 부합하는 데이터 표현 방식을 선택하는 것이 시스템의 신뢰성 향상의 핵심을 확인하였다.

Ⅳ. 결 론

본 논문은 원시 패킷과 통계적 플로우라는 두 가지 데이터 표현 방식이 네트워크 침입 탐지 시스템 성능에 미치는 영향을 실증적으로 비교 분석하였다. 이를 통해 패킷 기반 분석은 세밀한 패턴 탐지에, 플로우 기반 분석은 거시적 트래픽 양상 파악에 효율적임을 확인하였다.

결론적으로, 특정 데이터 형식에 치우친 기존 이상 탐지 체계의 보완 필요성을 확인하였고, 공격 메커니즘의 특성에 최적화된 분석 단위를 선정하는 것이 이상 탐지 정밀도 향상의 핵심임을 입증하였다. 본 연구의 결과는 향후 두 방식의 장점을 결합한 하이브리드 이상 탐지 체계 설계가 필요함을 시사한다.

ACKNOWLEDGMENT

이 논문은 2025 년도 정부(국방부)의 재원을 받아 정보통신기획평가원의 국방 ICT 혁신기술사업으로 수행된 연구성과입니다[No. RS-2025-02363049, 다중 다계층 네트워크의 동적 신뢰 연결 및 지능적 관제기술 개발].

참 고 문 헌

[1] Sharafaldin, Iman, et al. "Towards a reliable intrusion detection benchmark dataset." *Software Networking* 2018.1 (2018): 177-200.

[2] Lotfollahi, Mohammad, et al. "Deep packet: A novel approach for encrypted traffic classification using deep learning." *Soft Computing* 24.3 (2020): 1999-2012.

[3] Wang, Wei, et al. "Malware traffic classification using convolutional neural network for representation learning." *2017 International conference on information networking (ICOIN)*. IEEE, 2017.