패킷의 필드 특징을 활용한 E-GraphSAGE 기반 네트워크 공격 트래픽 분류 성능 향상

남승우, 유경민, 장윤성, 김주성, 김지민, 김명섭*

고려대학교

{nam131119, rudals2710, brave1094, jsung0514, illiard1209, *tmskim}@korea.ac.kr

Improving Network Traffic Classification with E-GraphSAGE Using Packet-Level Field Features

Seung-Woo Nam, Gyeong-Min Yu, Yoon-Seong Jang, Ju-Sung Kim, Ji-Min Kim, Myung-Sup Kim*

Korea Univ.

요 약

네트워크 공격이 점차 정교해지고 다양해짐에 따라, 효과적인 침입 탐지 시스템(IDS)에 대한 수요가 지속적으로 증가하고 있다. 그래프 신경망(GNN) 기반의 E-GraphSAGE[1] 모델은 네트워크 트래픽을 그래프 구조로 표현하여 세션 단위 분류를 수행한다. 그러나 E-GraphSAGE는 세션 단위의 통계적 특징만을 엣지 피처로 활용하기 때문에, 패킷에서 나타나는 미세한 공격 패턴을 충분히 반영하지 못하는 한계가 존재한다. 또한 다른 연구들 역시 세션 특징 또는 원시 바이트(raw byte) 구조를 사용하는 점에 있어, 네트워크 트래픽의 구조를 활용하지 못하는 문제가 있다. 따라서 본 논문에서는 패킷 내 필드 특징을 활용하여 E-GraphSAGE의 공격 트래픽 분류 성능을 향상시키는 방법을 제안한다. 세션을 구성하는 패킷으로부터 IP, Port 필드를 제외한 IP, Transport Layer의 필드를 기반으로 총 17개의 필드에 대한 평균, 표준편차, 최대값, 최소값의 네 가지 값으로 집계하여 엣지의 특징 리스트를 생성하였다. 이를 E-GraphSAGE의 입력으로 활용하여 CIC-IDS-2017, USTC-TFC-2016 데이터셋으로 실험한 결과, 기존 E-GraphSAGE에서 사용한 세션 통계 특징 입력보다 높은 성능을 보여주었다.

Ⅰ. 서론

최근 네트워크 환경의 고도화와 함께 공격 기법 또한 점차 지능화·다양화되고 있으며, 이에 따라 보다 정밀하고 효과적인 침입 탐지 시스템(IDS)에 대한 요구가 지속적으로 증가하고 있다. 이러한 흐름 속에서 기존의 시그니처 기반 탐지 방식의 한계를 극복하기 위해 다양한 머신러닝 및 딥러닝 기반의 연구들이 활발히 수행되어 왔다. 특히 네트워크 트래픽을 노드와 엣지로 구성된 그래프 형태로 표현할 수 있다는 점에서 그래프 신경망(GNN)을 활용한 접근 방식이 주목받고 있으며, 세션 간 관계를 반영한 학습을 통해 기존 방법 대비 향상된 성능을 보이는 연구들이 제안되고 있다.

그러나 기존 연구들에서는 입력 데이터 구성 측면에서 한계가 존재한다. 원시 바이트 데이터를 직접 입력으로 사용하는 연구[2]는 패킷의 모든 정보를 손실 없이 반영할 수 있다는 장점이 있으나, 데이터의 구조적 의미를 명시적으로 반영하기 어렵고 해석 가능성이 낮다는 문제가 있다. 반면, 세션 단위의 통계적 특징을 활용하는 연구[3]는 계산 효율성과 모델의 안정성을 확보할 수 있으나, 패킷 내부에서 나타나는 세밀한 필드 수준의 행위 정보가 손실된다는 한계를 가진다. 이와 같이 기존 접근 방식들은 네트워크 트래픽이 가지는 계층적 구조와 필드 단위의 세부 정보를 충분히 반영하지 못하고 있으며, 이는 정교한 공격 패턴 탐지에 있어 성능 저하로 이어질 수 있다.

따라서 본 연구에서는 패킷 내 필드 특징을 기반으로 한 새로운 입력 구성 방식을 제안한다. 구체적으로, 세션을 구성하는 각 패킷으로부터 다양한 프로토콜 계층의 필드 정보를 추출하고 이를 통계적으로 집계하여 그래프의 엣지 특징으로 활용함으로써, 트래픽의 구조적 정보를 반영하고자 한다.

이 논문은 과기정통부-정보통신기획평가원의 정보통신방송표준개발지원(R&D,정보화)사업(No. RS-2025-02219319, 양자컴퓨터 공격에도 안전한 양자암호 기반 제로트러스트 보안 네트워크/서비스 및 제어/관리 기술 표준개발)과 정부(중소벤처기업부)의 재원으로 중소기업기술정보진흥원(TIPA)의 창업성장기술개발사업(TIPS)사업(RS-2025-25466990, 5G/6G 네트워크 Cross-domain Observability Engineering Orchestrator 기술 및 표준 개발)의 지원을 받아 수행된 연구임.

Ⅱ. 본론

기존 E-GraphSAGE에서는 세션의 통계, DNS, HTTP 특징을 추출하여 엣지의 피처로 사용하였다. E-GraphSAGE에서 사용한 특징은 크게 5가지로 나눌 수 있는데, 세션의 통계 특징(바이트 수, 패킷 수, 세션 유지 시간 등), DNS 특징(query, authoritative answer, recursion desired 등), SSL 특징(version, cipher, issuer 등), HTTP 특징(method, uri, version 등), weird 특징(name, addl, notice 등)으로 나누어 볼 수 있다. DNS, SSL, HTTP 특징의 경우 패킷 내 필드에서 추출한 특징이긴 하나, 공격을 분류하기 위한 일부 특징만을 사용한 것이며, 네트워크 트래픽 구조를 반영한 특징이라 보기 어렵다.

따라서 본 논문에서는 패킷 내 필드 특징을 기반으로 특징 리스트를 만들고, 이를 엣지의 피처로 사용하고자 한다. 먼저 패킷은 Ethernet, IP, Transport, Application Layer로 나눌 수 있으며, 네 가지의 레이어 중 IP, Transport Layer만을 사용하고자 한다. Ethernet Layer는 사용할 특징이 MAC Address와 타입 정보만을 가지고 있으며, MAC Address는 데이터셋에 편향될 수 있는 특징이므로 사용하지 않는다. 그리고 GNN에서 모든 엣지가 동일한 피처 구조를 가지기 위해 IP, Transport Layer의 필드를 사용하며 프로토콜에 따라 구조가 달라지는 Application Layer는 사용하지 않았다.

IP Layer에서는 Version, IHL(IP Header Length), ToS(Type of Service), Total Length, Identification, Flags, Fragment Offset, TTL(Time To Live), Protocol, Header Checksum 필드를 사용하였다. Source & Destination IP Address 필드는 MAC Address와 마찬가지로 데이터셋에 편향될 수 있는 특징이므로, 노드와 엣지를 구성하는 데이터로 사용하고 엣지의 피처로 사용하지 않았다. Transport Layer에서는 Seq Number, Ack Number, Header Length, Flags, Window Size, Checksum, Urgent Pointer 필드를 사용하였다. Source & Destination

데이터셋	설명	세션 통계 특징	필드	피처 개수	Accuracy	Precision	Recall	Weight F1	Macro F1
CIC-IDS-2017	[1] 특징	-	-	44	0.79	0.77	0.79	0.77	0.32
	필드 특징만 사용	X	O	68	0.98	0.96	0.98	0.97	0.58
	세션 통계 특징만 사용	O	X	8	0.86	0.86	0.86	0.83	0.33
	모두 사용	O	O	76	0.98	0.96	0.98	0.97	0.53
USTC-TFC-2016	[1] 특징	-	-	44	0.46	0.67	0.46	0.38	0.46
	필드 특징만 사용	X	O	68	0.96	0.96	0.96	0.96	0.95
	세션 통계 특징만 사용	O	X	8	0.52	0.49	0.52	0.43	0.38
	모두 사용	O	O	76	0.96	0.96	0.96	0.96	0.96

표 1 E-GraphSAGE 입력 설계에 따른 실험 결과

Port는 IP와 마찬가지로 데이터셋에 편향될 수 있는 특징이므로, 노드와 엣지를 구성하는 데이터로 사용하고 엣지의 피처로 사용하지 않았다. 정리하면, IP Layer의 필드 9개, Transport Layer 필드 8개를 사용하여 총 17개의 필드에 대해서, 세션 내 패킷의 필드를 집계하여 각 필드의 평균, 표준편차, 최대값, 최소값을 계산하여 엣지의 피처로 사용하였다. 따라서 패킷 내 필드 특징은 총 17 * 4 = 68개가 사용되었다.
세션 통계 특징은 공격 클래스를 고려하여 송수신 패킷 및 바이트 비율, 패킷 개수, 방향 변경 빈도, 패킷 간 간격 평균·표준편차·최대값·최소값으로 총 8개의 세션 통계 특징을 사용하였다.

사용한 모델은 E-GraphSAGE 모델로, 기본적인 GNN은 노드에 피처를 구성하고 엣지는 연결 여부만을 나타내는 그래프에서 인접 노드의 피처를 집계하여 노드를 업데이트하는 방식과 달리, 엣지에 피처를 구성하고 인접 엣지를 집계하여 노드를 업데이트하는 방식을 사용한다. 그림 1은 E-GraphSAGE 구조를 표현한 그림이다.

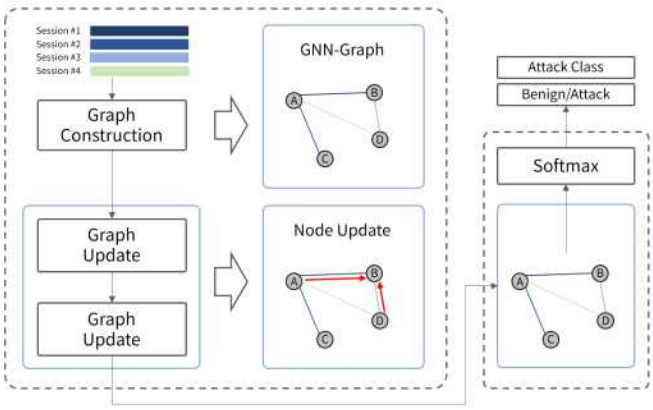

그림 1 E-GraphSAGE 모델 구조

실험은 CIC-IDS-2017, USTC-TFC-2016 두 데이터셋과 E-GraphSAGE 모델을 사용하였다. 모델의 세부 정보는 다음과 같다.

- Layer 수 : 2
- F'(임베딩 차원) : 128
- Batch 크기 : 512
- Activation : ReLU
- Dropout : 0.2
- Loss : Cross-Entropy
- Optimizer : Adam(LR = 0.001)

실험은 CIC-IDS-2017, USTC-TFC-2016 데이터셋에 대해, E-GraphSAGE를 제안한 연구에서 사용한 피처 44개 리스트, 필드 특징과 추출한 세션 통계 특징의 비교를 수행하였다. 추가로 필드 특징만을 사용한 것과 추출한 세션 통계 특징을 사용한 것을 추가로 실험하여 필드 특징이 성능에 얼마나 영향을 끼치는지 비교를 수행하였다. 실험 결과는 표 1과 같다.

두 데이터셋 모두 필드 특징이 포함된 피처 리스트를 사용한 실험이 가장 높은 성능을 보여주었다. CIC-IDS-2017에서는 기존 특징을 사용한 방법보다 필드 특징을 사용한 방법이 모든 평가 지표에서 최대 21%까지 향상한 것을 확인할 수 있다. USTC-TFC-2016에서는 정확도가 50% 향상되었으며, Weight F1은 58% 향상된 것을 확인할 수 있다.

기존 통계 특징과 추출한 통계 특징만을 사용한 방법이 모두 필드 특징을 포함한 방법보다 성능이 비교적 낮은 것을 확인할 수 있으며, 이는 세션 통계 특징만으로 공격을 판별하기에는 비교적 한계가 존재한다는 것을 알 수 있다. 패킷 내 세부적인 필드 정보를 모델이 학습함으로써, 공격 클래스 분류 성능이 향상된다는 점을 시사한다.

Ⅲ. 결론

본 논문에서는 E-GrpaphSAGE 기반 네트워크 공격 트래픽 분류 모델의 입력 구성의 한계를 해결하기 위해, 패킷 내 필드 특징을 활용한 새로운 엣지 피처 구성 방식을 제안하였다. 이를 위해 IP, Transport Layer의 필드 정보를 추출하고, 추가적인 세션 통계 특징 추출을 통해 피처 리스트를 생성하였다. 이를 CIC-IDS-2017, USTC-TFC-2016 데이터셋에 평가한 결과, 성능이 세션 통계 특징을 사용한 방법보다 성능이 향상된 것을 확인할 수 있었다.

향후 연구에서는 패킷 내 필드 특징이 공격 탐지 성능 향상에 어떠한 영향을 미치는지에 대한 세부적인 분석을 수행하고자 한다. 또한 다차원적 그래프 표현 및 그래프 구성 방법에 대한 연구도 수행할 예정이다.

참 고 문 헌

[1] LO, Wai Weng, et al. E-graphsage: A graph neural network based intrusion detection system for iot. In: NOMS 2022-2022 IEEE/iFIP network operations and management symposium. IEEE, 2022. p. 1-9.

[2] ZHANG, Haozhen, et al. Tfe-gnn: A temporal fusion encoder using graph neural networks for fine-grained encrypted traffic classification. In: Proceedings of the ACM web conference 2023. 2023. p. 2066-2075.

[3] ARINDAM, Abhirup; BAGHEL, Anurag Singh. Advancing Network Security Through Deep Learning: A Hybrid Graph-Based and Temporal Approach to Anomaly and Threat Detection.