EisP-GraphSAGE: 패킷 단위 엣지 표현 기반 GNN을 통한 네트워크공격트래픽분류

남승우, 유경민, 장윤성, 김주성, 김지민, 김명섭*

고려대학교

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

EisP-GraphSAGE:NetworkAttackTrafficClassificationviaaPacket-LevelEdge Representation-BasedGNN

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

Myung-Sup Kim*

Korea Univ.

요 약

최근 클라우드, IoT, 5G/6G 환경의 확산으로 네트워크 구조가 복잡해짐에 따라 공격 유형 또한 정교하고 다양해지고 있다. 머신러닝 및 딥러닝 기반 네트워크 침입 탐지 기법은 주로 세션 또는 플로우 단위의 데이터를 활용하여 분류를 수행하고 있다. 그중 GNN은 다중 세션을 그래프로 모델링하고 이를 입력으로 사용하여 다중 세션 간의 관계 정보를 학습하는 모델로, 특히 E-GraphSAGE[1]는 엣지 정보를 활용하여 노드 표현을 학습하는 효과적인 방법으로 제안되었다. 그러나 E-GraphSAGE는 세션 단위로 가공된 특징이나 원시 바이트 기반 입력에 의존하며, 이는 패킷 수준의 세밀한 정보 반영에는 한계가 존재한다. 본 논문에서는 이러한 한계를 극복하기 위해 패킷 단위를 엣지로 표현하는 EisP-GraphSAGE를 제안한다. 제안하는 방법은 각 패킷을 개별 엣지로 정의하여 다중 엣지 그래프를 구성하고, 이를 통해 세션 내부의 시간적 흐름과 상호작용을 자연스럽게 반영한다. 또한 각 엣지에는 IP 및 Transport 계층의 필드 기반 특징을 포함시켜 패킷 수준의 정밀한 표현을 가능하게 한다. 이를 통해 기존 세션 기반 접근 방식에서 발생하는 정보 손실을 완화하고, 네트워크 트래픽의 구조적 및 동적 특성을 효과적으로 학습할 수 있다. 실험 결과, CIC-IDS-2017 데이터셋에서 제안하는 방법은 기존 세션 기반 특징을 사용하는 방식 대비 향상된 공격 트래픽 분류 성능을 보였다.

Ⅰ. 서 론

최근 네트워크 환경은 클라우드, IoT, 5G/6G와 같은 다양한 기술의 확산으로 인해 점점 더 복잡해지고 있으며, 이에 따라 네트워크 공격의 유형 또한 정교하고 다양하게 진화하고 있다. 이러한 환경에서 효과적인 네트워크 침입 탐지 및 공격 트래픽 분류는 보안 분야에서 매우 중요한 과제로 자리 잡고 있다. 기존의 머신러닝, 딥러닝 기반 접근 방식은 단일 세션 또는 세션 내 패킷 단위의 데이터를 입력으로 사용하며[2][3], 각 세션에서 추출된 통계적 특징(패킷 수, 바이트 수, 평균 패킷 길이 등)을 사용하거나 원시 바이트 값, 네트워크 패킷의 레이어 내 필드 등 여러 입력 방식을 기반으로 정상/비정상 또는 공격 유형을 분류한다.

그 중, 세션을 그래프 형태로 모델링하고 이를 Graph Neural Network(GNN)를 통해 학습하는 접근 방식에 대해 많은 연구가 진행되고 있다. GNN은 노드 간 연결 관계를 기반으로 정보를 전달하고 인접 노드 정보를 집계하여 노드를 업데이트하는 방식으로, 개별 세션뿐만 아니라 다중 세션도 그래프로 구성하여 세션 간 관계 및 구조적 정보를 효과적으로 학습할 수 있다. 이를 통해 기존 단일 세션만으로 포착하지 못했던 공격 패턴을 보다 정밀하게 분석할 수 있으며[4], 네트워크 전체의 상호작용을 고려한 탐지가 가능해진다.

GNN 연구 중 E-GraphSAGE[1]는 엣지 정보를 활용하여 노드 표현을 학습하는 모델로, 네트워크 트래픽을 그래프로 구성하여 분석하는 데 효과적인 방법이라 할 수 있다. 그러나 E-GraphSAGE를 포함한 기존 GNN 기반 접근 방식 역시 여전히 세션 단위로 가공된 특징을 사용하거나 원시 바이트 값을 사용하여 그래프를 구성하며, 이는 패킷 수준에서 발생하는 세밀한 변화나 프로토콜 계층 간 상호작용을 충분히 반영하지 못한다.

이러한 한계를 극복하기 위해, 본 논문에서는 패킷 하나를 엣지로 설정하여 그래프를 구성하는 EisP-GraphSAGE를 제안한다. 제안하는 방법은 네트워크 트래픽을 그래프로 표현할 때, 기존의 세션 단위 엣지 대신 각 패킷을 개별 엣지로 정의하는 방식을 채택한다. 이를 통해 하나의 노드 쌍 사이에 다수의 엣지가 존재하는 다중 엣지 그래프로 구성하며, 세션 내부의 시간적 흐름과 상호작용을 자연스럽게 반영하도록 한다.

각 엣지에는 단순한 연결 관계를 넘어, IP Layer와 Transport Layer 계층의 필드 값을 기반으로 한 특징을 포함하도록 설계하였다. 이를 통해 패킷 수준에서의 정밀한 표현이 가능하며, 기존 세션 기반 특징이 가지는 정보 손실 문제를 완화하고 네트워크 트래픽의 구조적 및 동적 특성을 보다 효과적으로 반영할 수 있도록 한다.

본 논문은 2장에서는 관련 연구, 3장에서는 제안하는 모델의 그래프 구성과 방법론에 대해 설명하며, 4장에서는 실험 설계 및 결과에 대해 설명하며, 5장은 결론 및 추후 방향을 정리하였다.

Ⅱ. 관련 연구

최근 네트워크 트래픽 분석에서 단일 세션 기반 접근 방식의 한계를 극복하기 위해, 트래픽을 그래프 형태로 모델링하고 이를 GNN을 통해 학습하는 연구가 활발히 진행되고 있다. 이러한 GNN 기반 접근 방식은 그래프 구성 방법에 따라 단일 세션을 하나의 그래프로 표현하는 방식과 다중

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) 및 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.

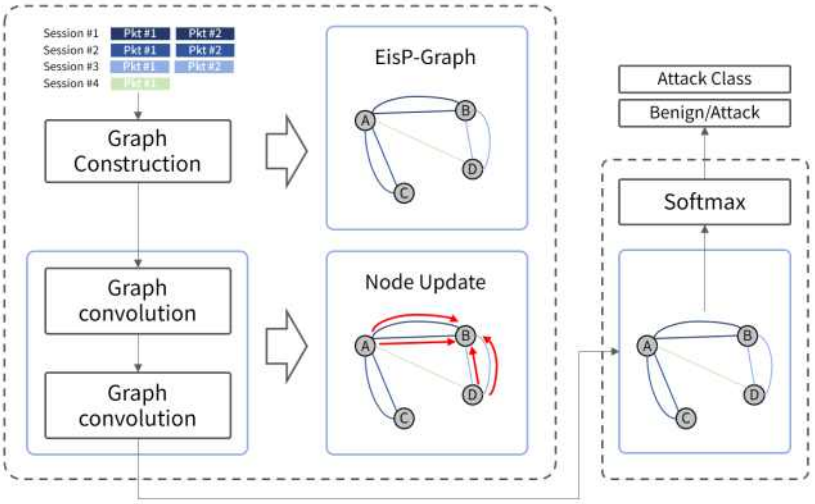


그림 1 EisP-GraphSAGE 구조

세션을 통합하여 하나의 그래프로 표현하는 방식으로 구분할 수 있다.

단일 세션 처리 방식 중 [5][6]는 패킷을 노드로 설정하고, 패킷 간의 관계를 기반으로 엣지를 구성하는 방식으로, 세션 내부의 패킷 간 상호작용을 반영하여 모델을 학습한다. 엣지는 패킷 순서 정보나 ACK 정보를 기반으로 연결되므로, 노드 업데이트 과정에서 해당 패킷과 인접한 이전 및 이후 패킷의 정보를 집계하여 표현을 갱신한다.

다중 세션 처리 방식 중 [1]은 IP, Port 정보를 기반으로 노드를 생성하고, 각 세션 정보를 엣지로 구성하는 방식으로, 엣지를 단순한 연결 정보가 아닌 세션의 주요 특징을 포함하는 속성으로 활용하였다. 기존 GNN은 인접 노드의 정보를 집계하여 노드를 업데이트하였으나, 해당 연구에서는 인접 노드 대신 세션 정보를 포함하는 인접 엣지를 집계하여 노드를 업데이트하는 방식을 사용하였다. [7]은 노드를 세션으로 설정하고, 세션 간 시간 정보 및 패턴 유사성을 기반으로 엣지를 구성한다. 이는 노드 업데이트 과정에서 시간적·행태적 특성이 유사한 세션들을 선택적으로 집계하여 표현을 학습하는 방식으로 해석할 수 있다.

그러나 다중 세션을 처리하는 GNN 기반 접근 방식들은 그래프 구조를 활용하여 세션 간 관계를 효과적으로 반영한다는 장점에도 불구하고, 여전히 트래픽을 구성하는 최소 단위인 패킷 내 구조적인 정보를 충분히 반영하지 못하는 한계를 가진다. 다중 세션을 그래프로 구성할 때 세션의 가공된 특징을 사용하거나 원시 바이트를 사용하며, 이는 패킷 내 필드 정보를 온전히 담아내지 못한다. 따라서 패킷 내 구조 정보를 그래프 구조 내에서 직접적으로 활용할 수 있는 새로운 표현 방식이 필요하다.

Ⅲ. 본론

GraphSAGE[8]는 각 노드가 인접 노드의 정보를 집계하여 자신의 표현을 업데이트하는 GNN 모델이다. 이 모델은 대규모 그래프에서도 효율적인 학습이 가능하다는 장점으로 다양한 도메인에서 활용되고 있다. 그러나 GraphSAGE는 엣지의 속성을 직접적으로 활용하지 못한다는 한계를 가진다. 이를 확장한 E-GraphSAGE는 엣지 특징을 활용하여 노드 표현을 학습하는 구조를 가진다. E-GraphSAGE에서는 노드 v의 표현을 업데이트할 때, 인접 노드 u뿐만 아니라 해당 노드 간의 엣지 e_{uv}의 특징을 함께 고려한다. 일반적으로 각 노드는 인접 엣지의 특징을 집계한 후, 자신의 기존 표현과 결합하여 새로운 표현을 생성한다.

이러한 구조는 단순한 연결 관계를 넘어, 노드 간 상호작용의 속성을 반영할 수 있다는 점에서 네트워크 트래픽 분석에 적합하다. 그러나 E-GraphSAGE 방식에서는 엣지 특징으로 주로 세션 단위로 가공된 통계적 특징이 사용되며, 이는 패킷 수준의 세밀한 정보를 충분히 반영하지 못하는 한계를 가진다.

본 논문에서는 이러한 한계를 극복하기 위해 EisP-GraphSAGE를 제안한다. 제안하는 그래프는 네트워크 트래픽 세션을 구성하는 패킷을 엣지로 표현하는 것을 핵심으로 한다. 그림 1은 EisP-GraphSAGE의 다중 세션 처리 과정을 표현한 그림이다.

그래프 G=(V,E) 에서 노드 V는 통신 주체를 나타내며, IP 주소와 Port 정보를 기반으로 정의된다. 엣지 E는 노드 간의 통신 과정에서 발생하는 개별 패킷을 의미한다. 따라서 하나의 노드 쌍 사이에는 다수의 엣지가 존재할 수 있으며, 이는 자연스럽게 다중 엣지 그래프를 형성한다.

EisP-Graph에서 각 엣지는 단순한 연결 정보가 아닌, 패킷의 세부 정보를 포함하는 특징 벡터를 가진다. 특징의 크기는 F이다. 본 연구에서는 네트워크 세션 내 패킷의 구조적 정보를 반영하기 위해, IP 계층과 Transport 계층의 필드 값을 활용하였다. IP 계층에서는 헤더 길이, 버전, 프로토콜 타입과 같은 필드를 포함하며, Transport 계층에서는 플래그, 헤더 길이, 윈도우 크기 등의 특징을 사용한다. 이를 통해 기존 세션 기반 특징에서 발생하는 정보 손실 문제를 완화하고, 네트워크 트래픽 세션 내 패킷의 구조적 특성을 정밀하게 표현한다. 각 계층 별 사용한 특징은 표 1과 같다.

EisP-GraphSAGE는 E-GraphSAGE를 기반으로 하되, 패킷 단위 엣지 특징을 활용하도록 확장된 모델이다. 따라서 각 노드 v의 표현은 다음과 같이 업데이트된다. 먼저 각 노드는 엣지와 동일한 차원 F를 가진다.

먼저, 노드 v와 연결된 모든 인접 엣지 e_{uv}의 특징을 집계하여 엣지 기반 표현을 생성한다. 엣지 기반 표현은 인접 엣지에 대한 평균이다. 이후, 이 집계된 엣지 표현과 기존 노드 표현을 결합하여 차원 F'을 가지는 새로운 노드 표현을 계산한다. 이 과정은 식 1과 같이 표현할 수 있다.

$$h_v^{(k+1)} = \sigma \circ \left(W \bullet CONCAT\left(h_v^{(k)}, AGG(e_{uv} \mid u \in N(v))\right)\right) \quad (1)$$

여기서 $h_v^{(k+1)}$는 k번째 레이어의 노드 표현, e_{uv}는 엣지 특징, AGG는 평균 집계 함수, σ는 활성화 함수이다. 이와 같은 구조를 통해, 제안

계층	특징 이름
IP	version
	ihl
	tos
	total_length
	identification
	flags
	fragment_offset
	ttl
	protocol
	checksum
Transport	seq
	ack
	header_length
	flags
	window_size
	checksum
	urgent_pointer

표 1. 엣지에 사용되는 특징 리스트

모델은 인접 엣지의 정보를 집계하고, 이를 기반으로 노드 특징을 갱신한다. 갱신한 노드 특징은 각 엣지와 결합하여 엣지도 갱신한다. 이러한 과정을 레이어 수만큼 반복하여 노드와 엣지를 갱신한다. 레이어 수가 많아질수록 각 노드는 더 많은 엣지 정보를 간접적으로 활용하여 업데이트된다. GNN 레이어를 거친 후의 그래프는 세션 단위 분류를 위해 엣지 단위로 분류를 수행한다. 엣지에 연결된 두 노드의 특징을 결합하고, 이를 사용하여 해당 세션에 대한 최종적인 분류를 수행한다.

Ⅳ. 실험

제안한 모델에 대한 네트워크 공격 트래픽 분류 성능을 평가하기 위해 CIC-IDS-2017 데이터셋[9]을 사용하였다. 해당 데이터셋은 정상 트래픽과 함께 다양한 공격 유형을 포함하고 있으며, 실제 네트워크 환경을 반영한 대표적인 침입 탐지 데이터셋으로 널리 사용된다. 본 연구에서는 기존 E-GraphSAGE와의 공정한 비교를 위해 동일한 데이터셋을 기반으로 실험을 수행하였다.

본 연구에서 제안하는 EisP-GraphSAGE의 성능을 검증하기 위해, 기존 E-GraphSAGE와의 비교 실험을 수행하였다. E-GraphSAGE의 경우, 원 논문에서 사용된 설정을 최대한 반영하기 위해 47개의 세션 기반 특징을 추출하여 사용하였다. 해당 특징들은 패킷 수, 바이트 수, 흐름 지속 시간과 같은 세션의 통계 특징과 DNS, HTTP, TLS 관련 특징으로 구성되며, 각 세션을 하나의 엣지로 표현하는 그래프를 구성하는 데 활용된다. 반면 EisP-GraphSAGE는 동일한 데이터셋으로부터 추출된 패킷 데이터를 기반으로 그래프를 구성하였다. 각 패킷은 엣지로 정의되며, 앞서 정의한 특징 리스트를 기반으로 특징 벡터를 사용하였다. EisP-GraphSAGE 실험의 세부 정보는 표 2와 같다.

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

표 2. 모델 세부 정보

모델의 성능 평가는 네트워크 공격 분류 문제의 특성을 고려하여 Accuracy, Precision, Recall, F1-Score를 사용하였다. 두 모델 간 성능 비교 결과는 표 3에 정리하였다. 실험 결과, EisP-GraphSAGE는 모든 평가 지표에서 E-GraphSAGE 대비 향상된 성능을 보였다. 정확도는 E-GraphSAGE 대비 약 16% 증가했으며, 특히 F1-score 기준으로 약 0.2 정도의 성능 향상을 확인할 수 있으며, 이는 제안하는 방법이 E-GraphSAGE 보다 안정적인 분류 성능을 제공함을 의미한다.

Model	Accuracy	Precision	Recall	F1
E-GraphSAGE	78.95%	0.74	0.78	0.75
Proposed	**95.23%**	**0.95**	**0.95**	**0.94**

표 3. E-GraphSAGE, 제안한 모델과의 공격 클래스 분류 성능 평가

표 4는 E-GraphSAGE와 EisP-GraphSAGE의 클래스별 성능 비교 결과를 나타낸다. 전반적으로 EisP-GraphSAGE는 다양한 공격 유형에서 기존 E-GraphSAGE 대비 뚜렷한 성능 향상을 보이며, 특히 기존 모델이 탐지하지 못했던 클래스들에 대해 유의미한 성능 개선이 확인되었다.

먼저, benign 클래스의 경우 두 모델 모두 높은 성능을 보였으나, 제안 모델은 Recall이 1.00으로 향상되며 F1-score가 0.98까지 증가하였다. 이는 정상 트래픽을 보다 안정적으로 식별할 수 있음을 의미한다.

botnet-ares의 경우, 기존 모델은 Precision 0.04, F1-score 0.08로 매우 낮은 성능을 보였으나, 제안 모델에서는 Precision 0.43, Recall 1.00, F1-score 0.60으로 크게 향상되었다. 이는 패킷 단위 표현이 해당 공격의 특징을 보다 효과적으로 반영했음을 보여준다. 기존 모델에서 전혀 탐지하지 못했던 ddos-loic-http와 dos-goldeneye의 경우, 제안 모델에서는 각각 F1-score 0.58, 0.22로 탐지할 수 있게 되었다. 특히 ddos-loic-http는 Precision이 0.99로 매우 높게 나타났으며, 이는 특정 공격 패턴을 매우 정확하게 구분할 수 있음을 의미한다. 또한, ftp-patator의 경우 F1-score가 0.27에서 0.87로 크게 향상되었으며, ssh-patator 역시 F1-score가 0.27에서 0.92로 증가하였다. 특히 ssh-patator는 Recall이 1.00으로 증가하여 공격 트래픽을 거의 놓치지 않고 탐지하는 성능을 보였다. infiltration 클래스의 경우 기존 모델에서는 탐지하지 못했으나, 제안 모델에서는 Recall 0.97, F1-score 0.45로 유의미한 탐지 성능을 보였다. 이는 패킷 단위의 세밀한 특징이 기존 세션 특징 기반 접근 방식으로는 포착하기 어려운 공격을 식별하는 데 기여했음을 의미한다.

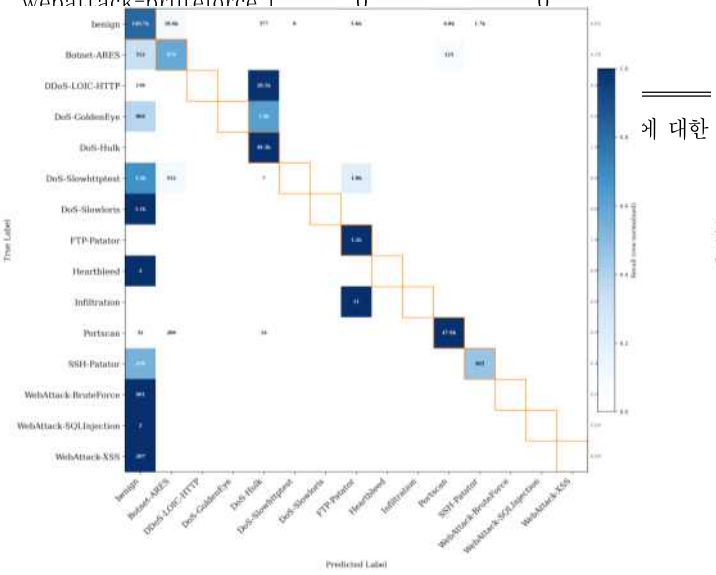
반면, dos-hulk와 portscan과 같은 일부 클래스에서는 기존 모델 대비 성능이 감소하는 경향이 나타났다. dos-hulk의 경우 F1-score가 0.76에서 0.61로 감소하였으며, portscan 역시 0.93에서 0.84로 감소하였다. 이는 제안 모델이 더욱 다양한 패턴을 학습하는 과정에서 일부 클래스에 대한 trade-off가 발생했음을 시사한다. 또한, webattack-bruteforce의 경우 기존 모델에서는 탐지하지 못했으나 제안 모델에서는 F1-score 0.48을 기록하며 일부 탐지가 가능해졌다. 반면, webattack-sqlinjection, webattack-xss, dos-slowloris, heartbleed, dos-slowhttptest와 같은 클래스는 여전히 두 모델 모두에서 탐지되지 않았다. 이는 해당 클래스들의 데이터 수 부족 또는 패턴의 희소성으로 인해 학습이 어려운 문제로 해석할 수 있다.

그림 2, 3는 각각 E-GraphSAGE 혼동 행렬과 EisP-GraphSAGE 혼동

행렬 그림이다. 그림 2를 보면, 일부 클래스에서 대각선 값이 뚜렷하게 나타나기는 하나, 전반적으로 여러 공격 클래스가 특정 클래스로 집중적으로 오분류되는 경향이 확인된다. 특히 DoS-GoldenEye, DoS-Slow 계열, Heartbleed, Infiltration과 같은 클래스는 대각선 값이 매우 낮거나 거의

션 단위 특징 의존 문제를 해결하기 위해, 패킷 단위 엣지 표현을 활용한 EisP-GraphSAGE를 제안하였다. 제안한 방법은 네트워크 트래픽을 그래프로 표현할 때, 각 패킷을 엣지로 정의하고 IP 및 Transport 계층의 필드 정보를 엣지 특징으로 활용함으로써, 기존 세션 기반 접근 방식에서 발생

Model	E-GraphSAGE			EisP-GraphSAGE		
	Precision	Recall	F1	Precision	Recall	F1
benign	**0.96**	0.82	0.88	0.95	**1**	**0.98**
botnet-ares	0.04	0.58	0.08	**0.43**	**1.00**	**0.60**
ddos-loic-http	0	0	0	**0.99**	**0.41**	**0.58**
dos-goldeneye	0	0	0	**0.86**	**0.13**	**0.22**
dos-hulk	0.62	**1.00**	**0.76**	**0.96**	0.45	0.61
dos-slowhttptest	0	0	0	0	0	0
dos-slowloris	0	0	0	0	0	0
ftp-patator	0.15	1	0.27	**0.76**	**1.0**	**0.87**
heartbleed	0	0	0	0	0	0
infiltration	0	0	0	**0.30**	**0.97**	**0.45**
portscan	**0.87**	**0.99**	**0.93**	0.83	0.84	0.84
ssh-patator	0.19	0.46	0.27	**0.86**	**1.00**	**0.92**
webattack-bruteforce	0	0	0	**0.86**	**0.33**	**0.48**



에 대한

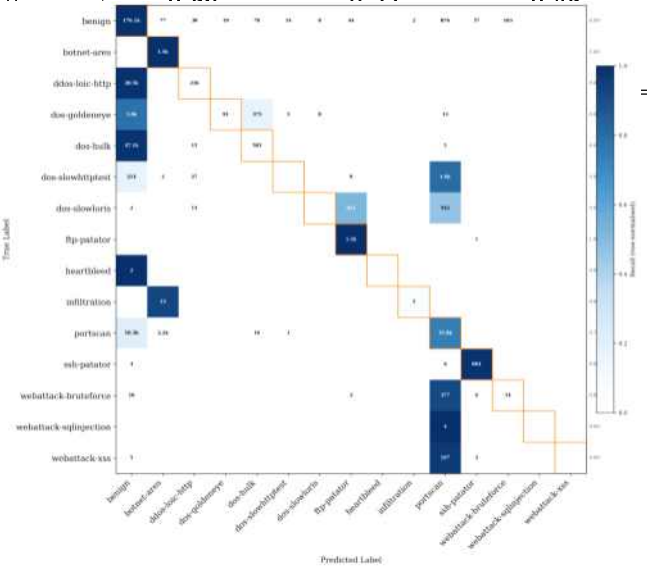


그림 2 E-GraphSAGE의 CIC-IDS-2017에 대한 혼동 행렬

그림 3 EisP-GraphSAGE의 CIC-IDS-2017에 대한 혼동 행렬

형성되지 않으며, 대부분 다른 클래스에 흡수되는 형태를 보인다. 반면, 그림 3에서는 대각선 방향의 값이 그림 2보다 일부 클래스에 대해 더 형성되며, 클래스별 분류 성능이 개선된 것을 확인할 수 있다. 특히 기존 모델에서 거의 탐지되지 않았던 일부 클래스에서 분류가 이루어지며, 클래스 간 구분 능력이 향상된 모습을 보인다. 또한 Botnet, FTP-Patator, SSH-Patator와 같은 클래스에서 오분류가 감소하고 특정 클래스에 대한 편향된 예측이 완화된 것을 확인할 수 있다. 이는 패킷 단위 엣지 표현이 트래픽의 구조적 차이를 보다 잘 반영하여, 유사한 공격 유형 간의 경계를 명확하게 만든 결과로 해석할 수 있다.

다만, 표 4와 마찬가지로 일부 클래스는 여전히 낮은 분류 성능을 보이며, benign 또는 특정 클래스로 집중되는 경향이 존재한다. 이 역시 데이터 불균형에 기인한 문제로 판단된다.

V. 결론

본 논문에서는 기존 GNN 기반 네트워크 트래픽 분석 방법의 한계인 세

하는 정보 손실 문제를 완화하였다.

또한, 다중 세션을 하나의 그래프로 구성하는 과정에서 패킷 단위의 세밀한 상호작용과 구조적 정보를 직접적으로 반영할 수 있도록 하였으며, 이를 통해 네트워크 공격 트래픽의 동적 패턴을 보다 효과적으로 학습할 수 있도록 하였다. CIC-IDS-2017 데이터셋을 활용한 실험 결과, 제안하는 EisP-GraphSAGE는 기존 E-GraphSAGE 대비 Accuracy, Precision, Recall, F1-score 모든 지표에서 성능 향상을 보였으며, 특히 기존 모델이 탐지하지 못했던 일부 공격 유형에 대해서도 유의미한 탐지 성능을 확인할 수 있었다. 이는 패킷 단위 엣지 표현이 네트워크 트래픽의 구조적 특성을 효과적으로 반영하며, 공격 탐지 성능 향상에 기여함을 보여준다.

그러나 일부 공격 클래스에서는 여전히 낮은 성능이 나타났으며, 이는 데이터의 불균형 문제와 특정 공격 유형의 복잡한 패턴에 기인한 것으로 판단된다. 이에 따라 향후 연구에서는 클래스 불균형 문제를 완화하기 위해 오버샘플링, 언더샘플링, 가중치 기반 학습 등 다양한 기법을 적용하여 모델의 성능을 개선할 예정이다. 또한, 탐지 성능이 낮은 공격 유형에 대

해 보다 심층적인 공격 기법 분석을 수행하고, 이를 기반으로 모델 구조 및 특징 설계를 개선함으로써 전반적인 분류 성능을 향상시키고자 한다.

ACKNOWLEDGMENT

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] LIN, Xinjie, et al. Et-bert: A contextualized datagram representation with pre-training transformers for encrypted traffic classification. In: *Proceedings of the ACM Web Conference 2022*. 2022. p. 633-642.

[3] ZHAO, Ruijie, et al. Yet another traffic classifier: A masked autoencoder based traffic transformer with multi-level flow representation. In: *Proceedings of the AAAI Conference on Artificial Intelligence*. 2023. p. 5420-5427.

[4] FARRUKH, Yasir Ali, et al. Xg-nid: Dual-modality network intrusion detection using a heterogeneous graph neural network and large language model. *Expert Systems with Applications*, 2025, 287: 128089.

[5] HUOH, Ting-Li, et al. Flow-based encrypted network traffic classification with graph neural networks. *IEEE Transactions on Network and Service Management*, 2022, 20.2: 1224-1237.

[6] PANG, Bo, et al. High-performance network traffic classification based on graph neural network. In: *2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. IEEE, 2023. p. 800-804.

[7] MAKINDE, Omowunmi Folashayo. Graph Neural Networks for Anomaly Detection in Encrypted Network Traffic Flows. *IJSAT-International Journal on Science and Technology*, 2025, 16.4.

[8] HAMILTON, Will; YING, Zhitao; LESKOVEC, Jure. Inductive representation learning on large graphs. *Advances in neural information processing systems*, 2017, 30.

[9] SHARAFALDIN, Iman, et al. Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 2018, 1.2018: 108-116.