BOSS: 차원 축소와 클래스간 거리를 활용한 체계적인 네트워크 침입 탐지용 특징 선택 프레임워크*

김선호*, 백동명*, 이현우**

*KENTECH (학부생), **KENTECH (교수)

A Systematic Framework to Select Intrusion Detection Features based on the Dimension Reduction and the Inter-class Distance

Seon-Ho Kim*, Dong-Myeong Back*, Hyunwoo Lee**

*KENTECH (Undergraduate student) *KENTECH (Faculty)

요 약

AI 기반 네트워크 침입 탐지 시스템(NIDS)에서 특징 선택은 탐지 성능 및 연산 시간에 주목할만한 영향을 미친다. 본 연구에서는 NIDS 데이터셋 내 클래스 간의 구조적 분리도를 최대화하여 최적의 특징 조합을 추출하는 BOSS(Boundary-Optimized Structural feature Selection) 프레임워크를 제안한다. BOSS는 경계 평균(Boundary Mean) 지표를 도입해 공격과 정상 샘플 간의 분리도를 정량화하며, 고차원 거리 집중 현상 완화 및 탐색 연산량 절감을 위해 UMAP 차원 축소를 활용한다. CIC-IDS-2018 및 UNSW-NB15 데이터셋을 통한 평가 결과, BOSS는 기존 기법 대비 경계 평균값을 최대 163% 증가시켜 기하학적 분리도를 극대화하였다. 또한, 트리 계열 분류기에서 경쟁력 있는 성능을 유지하면서도 선형 회귀와 LSTM 등에서 최대 2.79%의 성능 우위를 달성하였다. 이는 단순한 성능 지표를 넘어, 데이터의 기하학적 분포를 고려한 특징 선택 방식이 NIDS 환경에서 효용성과 발전 가능성을 지니고 있음을 시사한다.

I. 서론

AI 기반의 IDS 연구에서 탐지 성능 향상과 연산 비용 절감은 중요한 요구사항이다[1]. 이를 달성하기 위한 대표적인 방법의 하나는 데이터셋으로부터 최적의 특징 조합을 선택하는 것이다. 효과적인 특징은 공격과 정상 간의 경계를 명확하게 형성함으로써 탐지 성능을 높이며, 동시에, 최소 개수의 특징을 사용할 경우, 모델의 학습 및 추론에 필요한 연산 비용을 줄일 수 있다. 이러한 관점에서, 특징 선택은 단순히 개별 특징의 중요도를 평가하는 것을 넘어, 데이터 분포를 반영하여 클래스 간 경계가 어떻게 형성되는지 고려할 필요가 있다.

그러나 기존 연구[2, 3]들은 F1 점수만을 기준으로 개별 특징의 기여도를 평가함으로써, 특징 공간 내 공격과 정상 샘플 간의 분포를 반영하지 못한다. 이에 따라 특징 간 상호작용을 반영하지 못할 뿐만 아니라, 데이터 분포로 형성되는 클래스 간 경계의 기하학적 특성을 충분히 반영하지 못하는 한계가 있다.

본 논문에서는 데이터셋의 클래스 간의 구조적 분리도를 최대화하여 최적의 특징 조합을 선택하는 BOSS 프레임워크를 제안한다. 먼저, BOSS는 고차원에서 발생하는 거리 집중 현상을 완화하고 데이터의 구조를 보존하기 위해 Extratrees와 ANOVA, 그리고 UMAP[4]을 활용하여 차원 축소를 수행한다. 이후 축소된 공간에서 다양한 특징 조합에 대해 정상 샘플 별로 공격 샘플과의 경계 평균을 계산한다. 최종적으로, 경계 평균값을 최대로 하는 특징 조합을 추출한다.

우리는 BOSS의 성능을 평가하기 위해, 이를

* 이 연구는 2025년도 산업통상자원부 및 한국산업기술기획평가원(KEIT) 연구비 지원에 의한 연구임(과제번호 RS-2025-02653102)

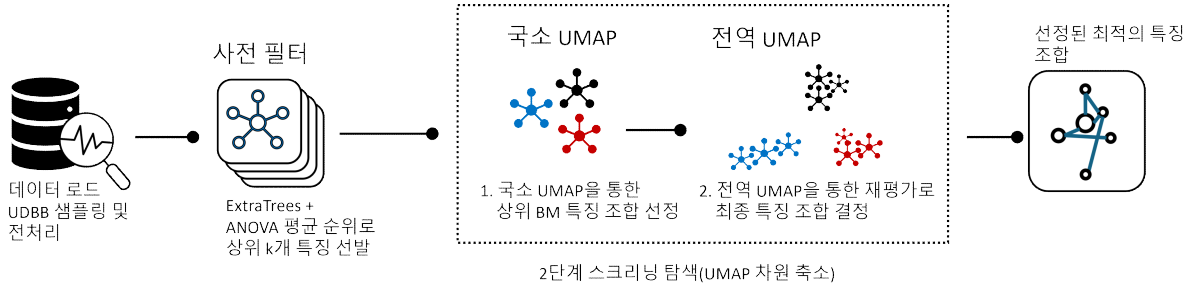

그림 1 BOSS 파이프라인

CSE-CIC-IDS-2018 및 UNSW-NB15에서 그 유효성을 검증하였다.

II. BOSS 설계

본 장에서는 BOSS 프레임워크 구조(그림 1)에 관해 설명한다. BOSS는 NIDS 데이터셋을 입력으로 받아, 사전 필터, 국소 UMAP 기반 경계 평균 계산, 전역 UMAP 기반 경계 평균 계산의 3단계를 거쳐 최적의 특징 조합을 추출한다.

사전 필터. 이 단계에서 BOSS는 모든 특징의 중요도를 Extra Trees와 ANOVA를 활용하여 각각 계산한 후 이들의 평균값을 기준으로 하여 상위 m개의 특징을 선정한다. 이를 통해 통계적으로 무의미한 특징을 제거함으로써, 이후 단계에서 활용할 UMAP 탐색 비용을 획기적으로 절감한다.

국소/전역 UMAP 축소 차원에서의 경계 평균 계산. 사전 필터 단계를 거쳐 선발된 특징들을 대상으로 BOSS는 UMAP으로 m 차원을 다시 n 차원으로 축소하고 특징 조합별로 다음의 경계 평균을 계산한다.

$$BM = \frac{1}{|A|}\sum_{i\in A}\min_{j\in B} d(i,j)$$

위에서 A는 공격 샘플들의 집합이고 B는 정상 샘플들의 집합이며, d(i, j)는 두 샘플 간의 유클리드 거리이다. 이는 곧 모든 공격 샘플에 대해 최근접 정상 샘플과의 거리의 평균값을 의미한다. 이 값이 클수록 공격과 정상 샘플 사이의 거리가 멀리 분포하며, 경계가 명확하다.

우리는 연산량이 많은 UMAP을 보다 효율적으로 활용하기 위해, 국소 UMAP 축소 차원과 전역 UMAP 축소 차원에서의 계산 등 두 단계로 나누었다. 여기서 국소와 전역의 차이는 UMAP을 활용하여 구조를 유지하며 차원 축소를 할 때, 고려하는 구조의 범위이다. 국소 UMAP은 전역 UMAP에 비해 데이터 분포 구조의 유지 범위가 더 좁다. 이로써, 국소 UMAP 축소 차원에서의 경계 평균 계산 단계를 통해 후보 특징 조합들을 보다 신속하게 추출하고, 전역 UMAP 축소 차원에서의 경계 평균 계산 단계를 통해 최적의 특징 조합을 선택한다.

이 단계에서 모든 가능한 특징 조합에 대해 경계 평균값을 계산하는 것은 연산 비용이 높으므로, 그리디 알고리즘을 활용하여 최적의 특징 조합을 만들어낸다. 우선 개별 특징들에 대한 경계 평균을 계산하고, 경계 평균값이 높은 특징들을 결합하여 특징 조합을 생성하며 경계 평균을 계산한다.

III. 실험 및 결과

3.1 실험 설정

BOSS(제안), ANOVA, Extratrees, Random의 특징 수를 통일하여 차원 혼입을 제거하였다. UMAP 차원 축소 및 특징 선택 과정은 테스트셋과 완전히 분리하여 데이터 누수를 방지하였다. 대조군으로는 특징 선택과 관련하여 데이터 분포를 고려하지 않은 Umar [2], 그리고 IGRF-RFE [3]를 선택하였다. Umar 는 의사결정트리를 활용하여 정확도에 기여하는 특징들을 모아 특징 조합을 만들고, CIC-IDS-2018에서 검증되었다. IGRF-RFE는 랜덤포레스트의 중요 특징을 기준으로 필터링하고, F1 점수를 기준으로 이에 기여하는 특징들을 모아 특징 조합을 만들며, 이는 UNSW-NB15에서 검증되었다.

3.2 UMAP 축소 공간에서의 특징 분석

그림 2는 CIC-IDS-2018에 대한 BOSS와 Umar의 특징 조합에 대한 UMAP 공간(2차원)을 비교

한 것이다. BOSS에서는 공격 샘플이 정상 샘플과 명확히 분리된 클러스터를 형성하는 반면, Umar에서는 공격과 정상 샘플이 중심부에서 동심원 형태로 혼재하여 경계가 존재하지 않는다.

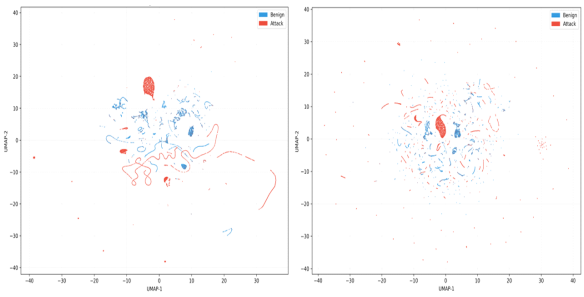

그림 2 BOSS(좌) 및 Umar(우) 특징 조합의 UMAP 시각화(CSE-CIC-IDS-2018)

그림 3의 기하 지표는 이를 수치로 뒷받침한다. CIC-IDS-2018에서 BOSS는 경계 평균 값이 8.92인 반면 Umar는 7.12인 것을 확인할 수 있다. UNSW-NB15에서는 그 격차가 더욱 두드러져 IGRF-RFE의 경계 평균값이 2.05인데 비해, BOSS는 경계 평균값 5.37을 기록하였다 (+163% 증가).

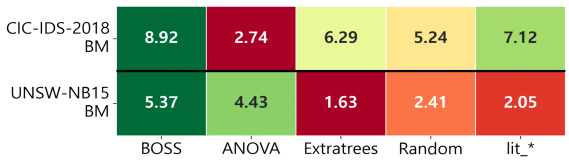

그림 3 시스템별 특징 분석

3.3 분류 성능 분석

표 1 데이터셋 별 기법 간 성능 비교

Table 1: ML 분류 성능 비교 (Binary F1, %)

데이터셋	방법	피처 수	XGBoost	RF	CNN	LSTM	LogReg
CICIDS2018	BOSS	16	93.68	93.12	90.51	92.17	**74.29**
	Umar [2]	12	**93.75**	**93.43**	**91.58**	**93.37**	72.51
UNSW-NB15	BOSS	17	58.96	58.96	45.62	**57.90**	**42.85**
	IGRF-RFE [3]	20	**59.24**	**59.06**	**49.86**	55.44	40.06

표 1은 데이터셋 별 기법 간 성능 비교 결과를 보여준다. CIC-IDS-2018에서 트리 계열 모델은 Umar 대비 0.07–0.31% 차이로 유사한 수준을 유지하였으며, Logistic Regression에서는 1.78% 높은 성능을 보였다.

UNSW-NB15에서는 BOSS를 활용한 LSTM 모델이 IGRF-RFE 대비 2.46% 높은 F1 점수를 보였으며, 로지스틱 회귀 모델은 IGRF-RFE 대비 2.79% 상회하였다. BOSS는 분류 성능을 직접 최적화하지 않음에도 선형 구조에 민감한 분류기에서 일관된 우위를 보이며, 경계 평균 최대화를 통한 특징 선택 기법이 작동한다는 것을 시사한다.

IV. 결론 및 제언

본 연구에서는 개별 특징의 성능 지표에만 의존하던 기존 방식의 한계를 극복하고자, 차원 축소와 클래스 간 경계 평균(Boundary Mean)을 결합해 데이터의 구조적 분리도를 극대화하는 특징 선택 시스템 'BOSS'를 제안하였다.

CSE-CIC-IDS-2018 및 UNSW-NB15 데이터셋을 통한 실험 결과, BOSS는 특징 공간 내 공격과 정상 샘플 간의 기하학적 경계를 뚜렷하게 개선하였으며, 기존 방법 대비 경계 평균값을 최대 163% 향상하였다. 또한, 특징 선택 과정에서 분류 성능을 직접 최적화하지 않았음에도 선형 구조에 민감한 분류기(로지스틱 회귀, LSTM)에서 최대 2.79%의 성능 향상을 기록하였다. 이는 데이터 분포 기반의 특징 선택이 NIDS 환경에서 실효성을 가짐을 시사한다.

향후 연구로, 다중 데이터셋 일반화 검증, UMAP 하이퍼파라미터 민감도 분석, 그리고 실시간 NIDS 환경에서의 적용 가능성을 분석할 계획이다.

[참고문헌]

[1] M. A. Ferrag et al., "Deep Learning for Cyber Security Intrusion Detection," J. Inf. Secur. Appl., 2020.

[2] M. A. Umar et al., "Effects of Feature Selection and Normalization on Network Intrusion Detection," TechRxiv, 2020.

[3] C. Yin et al., "IGRF-RFE: A Hybrid Feature Selection for MLP-Based NIDS on UNSW-NB15," J. Big Data, vol. 10, no. 15, 2023.

[4] L. McInnes et al., "UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction," arXiv:1802.03426, 2018.