네트워크 트래픽의 특징 그룹을 이용한 오토인코더 기반 이상탐지에 관한 연구

최다영°, 이주홍°*, 박형곤°*
이화여자대학교 전자전기공학전공°, 이화여자대학교 스마트팩토리융합전공*
{dddaynz, joohong.rheey}@ewhain.net, hyunggon.park@ewha.ac.kr

Autoencoder-Based Anomaly Detection Using Network Traffic Feature Grouping

Dayoung Choi°, Joohong Rheey°* and Hyunggon Park°*
Department of Electronic and Electrical Engineering, Ewha Womans University°,
Graduate Program in Smart Factory, Ewha Womans University*

요 약

본 논문에서는 고차원의 네트워크 트래픽에서 발생하는 이상 징후 탐지를 최대화하고자 특징 그룹을 이용한 오토인코더 기반 이상탐지 시스템을 제안한다. 제안하는 방법은 네트워크 트래픽 데이터를 흐름 및 패킷 수준의 특성에 따라 분류하여 특징 그룹을 구성하고, 오토인코더를 이용해 이상 트래픽을 탐지한다. 실제 다크넷 트래픽 데이터를 활용한 실험을 통해, 제안 방법이 원본 데이터를 그대로 사용하는 방법보다 탐지 성능이 우수함을 확인하였다. 또한 정상 트래픽과 이상 트래픽 분류에 있어 유용한 정보를 포함하는 특정한 특징 그룹이 존재함을 확인하였다. 제안 방법을 통해 네트워크 데이터와 같이 명확히 분류 가능한 특징으로 구성된 고차원 데이터에 대해 효과적인 이상탐지가 가능할 것으로 기대된다.

Ⅰ. 서 론

6G 네트워크 시스템을 통한 초연결 시대의 도래로 네트워크 공격이 더욱 지능적으로 발전하고, 보안 및 개인 정보의 취약점이 증가함에 따라 네트워크 보안의 중요성이 강조되고 있는 전망이다[1]. 네트워크 트래픽 이상탐지(anomaly detection)는 서비스 거부(Denial of Service, DoS) 공격, 중간자 공격(Man-in-the-Middle attack, MitM)과 같은 이상 징후에 실시간으로 대응하여 네트워크를 안전하게 운영하는 데에 필수적이다. 방대한 양의 네트워크 트래픽 중 이상 트래픽을 자동으로 탐지하기 위해 머신러닝 및 딥러닝을 활용한 연구가 활발히 진행되고 있으며, 대표적으로 오토인코더를 활용한 이상탐지 시스템이 있다[2-3]. 오토인코더 기반 이상탐지 시스템은 정상 데이터로만 학습된 오토인코더에 대해 이상 데이터가 주어질 경우 이상 데이터가 효과적으로 재구성되지 못한다는 점을 활용하여, 입력 데이터와 재구성 데이터 간 편차를 기준으로 이상 여부를 결정한다[3].

6G 네트워크에서 많이 수집될 것이라 예상되는 네트워크 데이터는 많은 수의 특징으로 구성된 고차원 데이터이다. 고차원 데이터는 특징 간 상관관계가 높거나 중복성(redundancy)이 높은 특징(feature)이 포함되어 있을 가능성이 높아, 데이터 분류가 어렵다. 따라서 네트워크 이상탐지 시스템에서 고차원의 원본 데이터(raw data)를 그대로 이상탐지에 활용하면 분류기가 제대로 동작하지 않는 경우가 있다. 이러한 경우, 특징 선택(feature selection)을 통해 데이터를 정제하여 탐지 성능을 향상시킬 수 있다[4].

네트워크 트래픽 데이터는 특성(attribute)이 명확하고 트래픽을 수집한 계층(layer)과 수준(level)에 따라 특징을 분류할 수 있는 고차원 데이터이기 때문에, 본 논문에서는 데이터의 특징 그룹(feature group)을 만들어 오토인코더를 학습시키는 방법을 제안한다. 제안 방법을 통해 각 특징 그룹이 이상 트래픽 탐지에 유용한지 확인하고, 유용한 특징 그룹을 선별하여 이상 트래픽 탐지 성능을 향상시키고자 한다. 구체적으로 네트워크 트래픽 특징을 흐름 및 패킷 수준의 특성(flow/packet-level attributes)에 따라 특징 그룹으로 분류하고, 특징 그룹을 이용한 이상탐지 오토인코더의 다크넷 트래픽 탐지 성능을 확인한다.

Ⅱ. 특징 그룹을 이용한 오토인코더 기반 이상탐지 시스템

본 논문에서는 원본 데이터의 특징을 모두 활용하지 않고, 특징 그룹에 따라 선별된 특징만을 활용하여 데이터의 이상 여부를 판단하는 오토인코더 기반 이상탐지 시스템을 제안한다. 그림 1과 같이 특징 집합 $F=\{f_1,f_2\cdots,f_K\}$에 속하는 K개의 데이터 특징을 m개의 특징 그룹 $G_i\,(i=1,2,...,m)$으로 분류한다. 입력 데이터 구성에 활용할 특징 그룹을 결정하기 위해, G_i를 식 (1)에 따라 조합하여 선별된 특징 그룹 $\mathcal{G}$를 만든다.

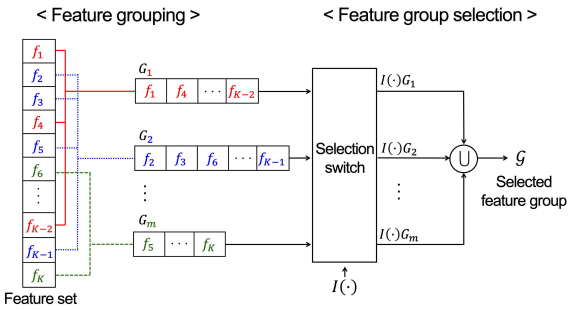


그림 1. 입력 데이터 구성을 위한 특징 그룹 구성 알고리즘

$$\mathcal{G}=\bigcup_{i=1}^{m} I(\cdot)\,G_i \tag{1}$$

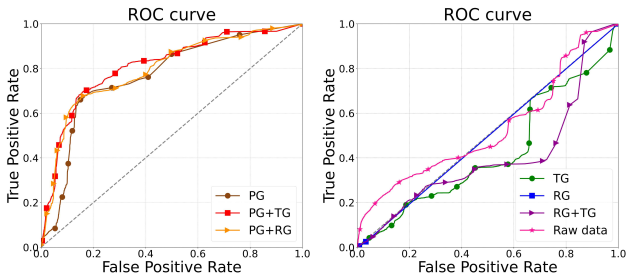
i번째 특징 그룹 G_i의 포함 여부를 결정하는 지시 함수(indicator function) $\boldsymbol{I}(\cdot)$는 다음과 같다.

$$\boldsymbol{I}_{\mathcal{G}}(G_i)=\begin{cases}0, & G_i\subset\mathcal{G}\\ 1, & G_i\subset\mathcal{G}\end{cases} \tag{2}$$

$\mathcal{G}$에 속하는 특징들로만 구성된 k차원 입력 데이터 벡터를 $\boldsymbol{x}=[x_1,x_2\cdots,x_k]$라고 할 때, 오토인코더의 입력으로 데이터 벡터의 집합 $\boldsymbol{X}$을 사용한다. 이때 오토인코더가 재구성한 출력 데이터 벡터 집합을 $\hat{\boldsymbol{X}}$이라고 하면, $\hat{\boldsymbol{x}}=[\hat{x_1},\hat{x_2},\cdots,\hat{x_k}]$는 출력 데이터이다.

본 논문에서는 정상 트래픽과 이상 트래픽을 구분하는 지표인 이상치 점수(anomaly score)를 계산하기 위해 평균 제곱 오차(MSE)를 사용한다.

$$e(\boldsymbol{x})=\frac{1}{k}\sum_{j=1}^{k}\left|x_j-\hat{x}_j\right|^2 \tag{3}$$



(a) (b)

그림 2. 특징 그룹별 다크넷 트래픽 탐지 성능에 따른 ROC curve

식 (3)에 따라 이상탐지 오토인코더가 재구성한 출력 데이터 $\hat{\boldsymbol{x}}$와 입력 데이터 $\boldsymbol{x}$의 차이에 따라 이상치 점수가 결정된다. 그러므로 정상 트래픽 특징의 주성분과는 다른 속성을 지닌 이상 트래픽은 정상 트래픽에 비해 큰 이상치 점수를 갖는다. 이에 정상 트래픽의 이상치 점수와 이상 트래픽의 이상치 점수 사이의 값 중 두 종류의 트래픽을 분리 가능하도록 하는 임계값(threshold)을 설정하여, 정상 트래픽과 이상 트래픽을 분류한다. 임계값을 δ, 데이터 $\boldsymbol{x}$의 이상치 점수를 $e(\boldsymbol{x})$라고 하면, 데이터 $\boldsymbol{x}$의 이상 트래픽 여부 t는 다음과 같이 표현된다.

$$t = \begin{cases} 0, & e(\boldsymbol{x}) \leq \delta \\ 1, & e(\boldsymbol{x}) > \delta \end{cases} \quad (4)$$

$t=0$은 $\boldsymbol{x}$가 정상 트래픽임을, $t=1$은 이상 트래픽임을 의미한다.

Ⅲ. 특징 그룹을 이용한 오토인코더 기반 다크넷 트래픽 탐지 실험

본 논문에서 사용한 데이터셋은 CIC-Darknet2020 Internet Traffic으로, 정상 트래픽과 Tor 및 VPN 네트워크를 통해 발생한 다크넷 트래픽으로 구성되어 있다[5]. 본 논문에서는 제한된 접속 권한으로 폐쇄된 네트워크 공간을 형성하여 각종 범죄 활동 및 사이버 공격에 악용되는 다크넷 트래픽을 이상 트래픽으로 간주한다.

데이터셋 내에 중복되는 특징, 단일값으로 구성된 특징 그리고 결측값이 존재하는 데이터는 배제한 후 사용한다. 또한 네트워크 흐름(flow) 고유의 속성을 반영하기 위해 IP 주소, port number와 같은 소켓 정보와 protocol을 제외한 측정값 기반 특징 63개를 활용한다. 흐름 및 패킷 수준의 특성을 기준으로 측정값 기반 특징을 크게 세 가지 그룹으로 나눈다. 구체적으로 시간과 관련된 특징으로 구성된 그룹(Time-related Group, TG), 패킷 정보와 관련된 특징으로 구성된 그룹(Packet-related Group, PG), 데이터 전송 비율과 관련된 특징으로 구성된 그룹(Rate-related Group, RG)으로 구분한다. TG는 IAT(Inter Arrival Time)의 통계값과 같이 연속적인 두 패킷 사이 측정된 시간 정보와 관련된 19개의 특징, PG는 packet length, flag counts 등 패킷 크기 및 길이를 비롯하여 플래그 정보와 관련된 34개의 특징, RG는 시간당 패킷 수와 같이 데이터가 전송되는 비율과 관련된 10개의 특징으로 구성된다.

특징 그룹을 이용한 오토인코더 기반 이상탐지 시스템을 활용하여 다크넷 트래픽 탐지 성능을 최대화하기 위해 세 가지 그룹의 특징을 단독으로 사용하여 입력 데이터를 구성하는 경우(TG/PG/RG), 두 가지 그룹을 조합하여 입력 데이터를 구성하는 경우(PG+TG/PG+RG/RG+TG), 세 가지 그룹을 모두 포함하는 원본 데이터를 입력 데이터로 사용하는 경우에 대한 실험을 각각 진행한다. 그림 2는 수신자 조작 특성 곡선(Receiver Operator Characteristic curve, ROC curve)으로, (a)는 원본 데이터를 제외하고 데이터 구성에 있어 PG를 사용한 경우(PG/PG+TG/PG+RG)이며, (b)는 원본 데이터 혹은 TG와 RG로만 구성한 데이터를 이용하여 탐지한 경우(TG/RG/RG+TG)이다. 그림 2에서 (b)의 곡선에 비해 (a)의 곡선이 좌상단에 가까운 것을 확인할 수 있다. 이는 특징 선택 시 PG를 포함하는 것이 이상탐지에 유리하다는 것을 의미한다. 즉, PG에 속하는 특징

*N/A: Not Available

		Accuracy	Precision	Recall	F1-score
Feature group	TG	0.43	0.42	0.36	0.39
	PG	**0.78**	**0.81**	**0.73**	**0.77**
	RG	N/A	N/A	N/A	N/A
	PG+TG	**0.79**	**0.83**	**0.73**	**0.78**
	PG+RG	**0.79**	**0.82**	**0.74**	**0.78**
	RG+TG	N/A	N/A	N/A	N/A
	Raw data	0.50	0.50	0.41	0.45

표 1. 특징 그룹별 오토인코더 기반 다크넷 트래픽 탐지 성능

이 정상 트래픽과 다크넷 트래픽을 구분 가능하도록 하는 속성을 지니고 있음을 알 수 있다. 각 특징 그룹을 활용하여 구성한 데이터를 이용한 오토인코더 기반 다크넷 트래픽 탐지 성능 지표는 표 1에서 확인할 수 있다. 별도의 특징 선택 과정 없이 원본 데이터를 사용하거나, TG로만 구성된 데이터를 사용할 경우 낮은 탐지 성능을 보인다. 또한, RG를 단독으로 사용하거나 RG와 TG를 조합하여 입력 데이터를 구성하는 경우에는 정상 트래픽과 다크넷 트래픽을 구분하지 못하는 것을 알 수 있다.

Ⅳ. 결 론

논문에서는 이상 네트워크 트래픽 탐지 성능을 최대화하기 위하여 특징 그룹을 이용한 오토인코더 기반 이상탐지 시스템을 제안하였다. 패킷 수준의 특성을 기준으로 네트워크 트래픽의 특징 그룹을 구분하고, 각 특징 그룹에 따라 이상탐지 오토인코더의 이상 트래픽 탐지 성능을 확인하는 실험을 진행하였다. 실험을 통해 원본 데이터에 포함된 특징 전체를 사용했을 때보다 우수한 탐지 성능을 보이는 것을 확인하였다. 데이터의 전체 특징 중 이상 트래픽 탐지를 최대화하는 특정한 특징 그룹이 존재하며, 탐지에 유용한 특징 그룹을 선별하여 사용하는 것이 이상 탐지의 성능에 중요한 영향을 미친다는 것을 알 수 있다. 제안한 방식은 네트워크 데이터 분류 성능을 효과적으로 향상시킬 수 있으며, 네트워크 데이터와 같이 특성이 명확하여 특징 그룹을 구분할 수 있는 고차원 데이터에 대해서도 확장 가능할 것으로 기대된다.

ACKNOWLEDGMENT

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No. 2021-0-00739, 분산/협력AI 기반 5G+ 네트워크 데이터 분석 기능 및 제어 기술 개발)과 2020년도 한국연구재단의 지원(No. NRF-2020R1A2B5B01002528)을 받아 수행된 연구임.

참 고 문 헌

[1] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, “The Roadmap to 6G Security and Privacy,” *IEEE Open Journal of the Communications Society,* Vol. 2, pp. 1094-1122, 2021.

[2] G. Pang, C. Shen, L. Cao, and A. V. D. Hengle, “Deep Learning for Anomaly Detection: A review,” *ACM Computing Surveys*, Vol. 54, No. 2, pp. 1-38, 2022.

[3] D. Park, Y. Hoshi and C. C. Kemp, “A Multimodal Anomaly Detector for Robot-Assisted Feeding Using an LSTM-Based Variational Autoencoder,” *IEEE Robotics and Automation Letters,* Vol. 3, No. 3, pp. 1544-1551, 2018.

[4] F. Iglesias and T. Zseby, “Analysis of Network Traffic Features for Anomaly Detection,” *Machine Learning,* Vol. 101, pp. 59-84, 2015.

[5] P. Friedrich, “CIC-Darknet2020 Internet Traffic,” Sep. 24, 2020. https://www.kaggle.com/peterfriedrich1/cicdarknet2020-internet-traffic (Accessed Aug. 26, 2022)