LSTM 기반 네트워크 트래픽 실시간 이상 탐지에 관한 연구

류다은, 김기천*
건국대학교, *건국대학교
daeun0501@konkuk.ac.kr, *kckim@konkuk.ac.kr

A Study on the Real-Time Anomaly Detection in Network Traffic Using LSTM

Ryu Da Eun, Kim Kee Cheon*
Konkuk Univ., *Konkuk Univ.

요 약

본 연구는 네트워크 트래픽에서 발생하는 이상 행위를 실시간으로 탐지하기 위한 방안으로, LSTM(Long Short-Term Memory)을 활용하여 접근법을 실험적으로 검토하였다. 실험에서는 NSL-KDD 데이터셋 기반으로 이진 라벨링, 범주형 특성 인코딩, 정규화 및 시계열 입력 구조로 변환하였다. 구축된 LSTM 모델은 이진 분류를 통해 정상과 비정상 트래픽을 구분하였으며, 실험 결과, 본 모델은 정확도 91%, 평균 F1-score 0.91의 우수한 성능을 보였다. 또한, 실제 트래픽 수집 없이 구조적 테스트 환경에서 모의 실시간 탐지 실험을 통해 연속된 입력에 대한 안정적인 예측 능력을 확인하였다.

Ⅰ. 서 론

IT 환경의 급속한 변화에 따라 네트워크 트래픽의 양뿐만 아니라 그 구조와 패턴도 점차 복잡해지고 있다. 특히 최근 발생하는 사이버 공격은 정교하고 예측이 어려운 형태로 변화하고 있어, 고정된 보안 규칙에 의존하는 기존 시스템만으로는 이를 실시간으로 탐지하는 데 한계가 있다 [1]. 이러한 배경에서, 시간에 따라 변화하는 트래픽의 시계열 특성을 효과적으로 분석할 수 있는 모델로 LSTM(Long Short-Term Memory)이 주목받고 있다 [2]. LSTM은 순환 신경망(RNN)의 일종으로, 과거의 정보를 장기적으로 기억하고 이를 기반으로 현재 상태를 판단하는 데 유리한 구조를 지니고 있으며, 네트워크 이상 탐지 분야에서도 성능이 입증되고 있다 [3][4]. 본 연구에서는 공개 데이터셋인 NSL-KDD를 활용하여 LSTM 기반의 이상 탐지 모델을 구축하고, 그 실효성과 실시간 적용 가능성을 실험적으로 검증하였다.

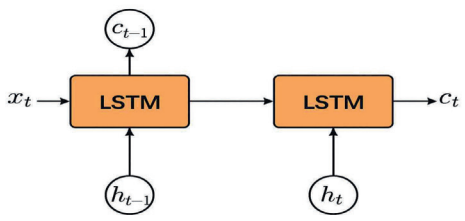
Ⅱ. 본론

1. 데이터셋 구성 및 전처리

본 연구에서는 네트워크 트래픽의 이상 행위를 탐지하기 위해 공개 데이터셋인 NSL-KDD를 활용하였다. NSL-KDD는 정상 트래픽과 다양한 유형의 공격 데이터를 포함하고 있으며, KDD Cup 1999 데이터셋의 중복 문제를 개선 할 수 있는 구조이다. 본 연구에서는 해당 데이터셋을 기반으로, 'normal' 클래스는 정상(0), 그 외 모든 공격 클래스는 이상(1)으로 이진 라벨링하여 이진 분류 문제를 재구성하였다. 학습 및 테스트 데이터는 NSL-KDD에서 제공하는 기본 학습용(kdd_train.csv)과 테스트용(kdd_test.csv) 분할을 그대로 활용하였으며, 정상과 이상 트래픽이 균형있게 포함되도록 구성하여 모델이 특정 클래스에 편향되지 않도록 구성하였다. 본 연구에서의 데이터 전처리는 protocol_type, service, flag와 같은 범주형 특성에 대해 Label Encoding을 적용하여 문자열 값을 정수형으로 변환한다. 수치형 특성은 값의 분포를 일정하게 맞추기 위해 MinMax 정규화를 사용하였고, 결과적으로 0과 1 범위 내에서 비교 가능하도록 조정되었다. 정제된 데이터는 LSTM 모델이 요구하는 시계열 입력 형태에 맞추어 3차원 텐서 (samples, timesteps, features)로 변환하였다. 본 연구에서는 각 입력 레코드의 특성 값들을 시계열의 시간 단위처럼 구성하여, 이에 따라 timsteps는 입력 개수와 동일하게 features = 1로 설정되었다. 최종적으로 전처리 된 입력 데이터는 LSTM 기반 이상 탐지 모델의 학습 및 평가에 사용되었으며, 실험 전반에 걸쳐 동일한 전처리 방식이 유지되도록 하였다.

2. 모델 설계 및 학습 전략

본 연구에서는 네트워크 트래픽의 시간적 특성을 효과적으로 반영하기 위해, LSTM(Long Short-Term Memory) 모델을 사용하였다. LSTM은 과거 데이터를 오래 기억할 수 있다는 특성으로, 시간 축에서 변하는 네트워크 트래픽의 흐름을 잡아내는 데 상대적으로 유리한 구조로 판단된다. 모델 구조는 두 개의 LSTM 계층을 중심으로 구성된다.



[그림 1] : 두 개의 LSTM 구조도

첫 번째 LSTM 계층은 입력 시계열의 패턴을 충분히 학습할 수 있도록 32개의 유닛으로 구성하였으며, Batch Normalization과 Dropout(0.5)을 적용해 과적합을 방지하였다. 두 번째 LSTM 계층은 상위 계층의 정보를 압축하여 최종 분류에 적합한 표현을 생성하도록 16개의 유닛으로 설정하

였다. 동일한 방식으로 정규화와 드롭아웃이 적용된다. 최종 출력층은 Sigmoid 활성 함수를 갖는 단일 노드(Dense Layer)로 구성되어 이진 분류를 수행하였다. 손실 함수로는 Binary Crossentropy를 사용하였으며, 최적화 알고리즘으로는 Adam 옵티마이저(learning rate=0.0005)를 적용하였다. 학습은 epoch 10회, batch size 32로 설정하였으며 검증 성능이 더 이상 개선되지 않을 경우, 학습을 조기 종료하는 EarlyStopping 기법을 사용하여 모델의 과적합을 방지하였다.

3. 실험 결과 및 성능 분석

본 연구에서 제안한 LSTM 기반 이상 탐지 모델의 성능을 검증하기 위해 NSL-KDD 테스트 데이터셋을 기반으로 모델 평가를 수행하였다. 테스트 데이터는 정상 및 이상 트래픽이 비교적 균형 있게 포함되어 있으며, 전처리 및 입력 형식은 학습 시 사용한 조건과 동일하게 적용하였다.
평가 과정에서 모델은 약 91%의 정확도를 기록했으며, F1-score 또한 0.91로 나타났다. 또한 모델 전반의 성능을 확인하기 위해 Macro Avg와 Weighted Avg 기준 F1-score는 모두 0.91로 나타났다. 이는 정밀도와 재현율 사이의 균형이 일정 수준 이상 확보되었음을 나타낸다.

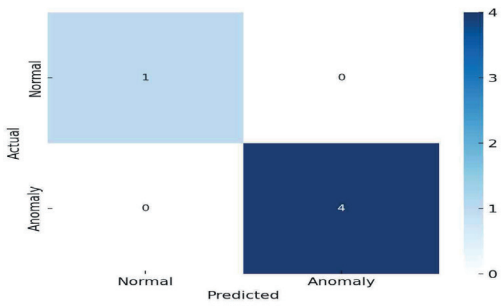
Class	Precision	Recall	F1-Score
Normal (0)	0.85	0.99	0.92
Anomalous (1)	0.99	0.83	0.9
Accuracy	-	-	0.91
Macro Avg	0.92	0.91	0.91
Weighted Avg	0.92	0.91	0.91

[그림 2] : LSTM 모델 성능 평가표

[그림 2]에서 보면 특히 정상 클래스에서는 높은 재현율(Recall)을 기록하였으며, 이상 클래스에서는 높은 정밀도(Precision)를 달성하여, 모델이 오탐률(false positive rate)과 누락률(false negative rate)을 효과적으로 낮추고 있음을 확인할 수 있다.

4. 실시간 탐지 가능성 검토

본 연구에서는 제안한 모델의 실시간 적용 가능성을 사전 검토하기 위해, 테스트 환경에서 모의 실시간 이상 탐지 실험을 수행하였다. 실험은 실제 네트워크 패킷을 수집하여 처리하는 방식이 아닌, 학습된 모델에 임의로 생성한 입력 데이터를 연속적으로 주입하는 방식으로 구현되었다. 각 입력은 모델의 시계열 입력 구조에 맞춰 생성되었으며, 실시간 환경에서의 연속적인 탐지 흐름을 시뮬레이션하기 위한 목적을 가진다. 총 5회의 테스트 입력에 대해 모델은 4건을 이상으로, 1건을 정상으로 판단하였으며, 이는 학습되지 않은 입력에 대해서도 모델이 안정적인 분류를 수행할 수 있음을 간접적으로 보여준다.



[그림 3] : 모의 실시간 이상 탐지 실험 결과

다만, 본 실험은 구조적인 테스트로 진행되어 통계적으로 충분한 데이터 수에 기반으로 진행한 정량적 검증은 아니므로 실시간 시스템 적용을 위한 가능성 검토 단계로 해석되어야 한다.

Ⅲ. 결론

본 연구에서 제안된 모델은 테스트 데이터셋을 대상으로 오프라인 실험을 통해 정확도 91%, 평균 F1-score 0.91의 성능을 기록하였다. 정상 및 이상 트래픽 모두 높은 정밀도와 재현율로 나타냈으며, 특히 이상 트래픽 탐지에 있어 높은 정밀도를 유지함으로써 오탐률(false positive rate)을 효과적으로 낮췄다. 또한, 모델의 실시간 적용 가능성을 평가하기 위해, 실제 패킷 수집 없이 모델 입력 형식에 맞춘 임의의 데이터를 기반으로 연속적인 분류를 수행하는 모의 실시간 탐지 테스트를 진행하였다. 이 실험만으로 일반화를 단정 지을 순 없지만, 적어도 스트림 구조에서의 기본 동작 가능성을 확인할 수 있었다. 다만, 본 연구에서는 실제 네트워크 트래픽을 실시간으로 수집하여 처리한 것은 아니므로, 향후에는 실제 데이터를 기반으로 진행한 실시간 이상 탐지 시스템 구현 및 검증을 추가로 연구할 계획이며, 또한 최신 네트워크 환경을 반영할 수 있는 다양한 트래픽 유형의 데이터셋을 활용하여 모델의 일반화 성능을 강화할 계획이다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임

(RS-2024-00410875, 2024년 산업혁신인재성장지원사업)

참 고 문 헌

[1] B. J. Radford, L. M. Apolonio, A. J. Trias, and J. A. Simpson, "Network traffic anomaly detection using recurrent neural networks," arXiv preprint

[2] Z. Niu, K. Yu, and X. Wu, "LSTM-based VAE-GAN for time-series anomaly detection," *Sensors*, vol. 20, no. 13, p. 3738, Jul. 2020,

[3] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, "An optimized LSTM-based deep learning model for anomaly detection in network traffic," *Sci. Rep.*, vol. 15, no. 1, p. 1554, Apr. 2025,

[4] Y. Li, Y. Xu, Y. Cao, J. Hou, C. Wang, W. Guo, X. Li, Y. Xin, Z. Liu, and L. Cui, "One-class LSTM network for anomalous network traffic detection," *Appl. Sci.*, vol. 12, no. 10, p. 5051, May 2022,