트래픽 이상 탐지를 위한 CNN-LSTM 기반 임베디드 시스템 구조 제안

류기연, 김종한*
LIG 넥스원

kiyoun.ryu@lignex1.com, *jonghan.kim@lignex1.com

CNN-LSTM Based Embedded System for Real-Time Traffic Anomaly Detection and QoS Maintenance

Ryu Ki Youn, Kim Jong Han*
LIG Nex1.

요 약

본 연구에서는 Jetson 임베디드 시스템 기반의 CNN-LSTM, 1D CNN 및 MLP 모델을 활용하여 이상 트래픽 감지 시스템을 구현하고, 보안적 응용 가능성을 평가한다. 제안하는 구조는 실시간 처리와 저전력 동작이 가능하며, 침입 탐지 시스템(NIDS), 제로데이 공격 탐지, 암호화 트래픽 분석, 엣지 기반 보안 등에 활용될 수 있다. 실험 결과, 경량화된 모델 구조가 엣지 디바이스에서도 GPU 가속을 통하여 높은 감지 정확도를 유지하며 안정적인 실시간 성능을 보였다. 본 연구의 1D CNN, MLP 모델의 경우 추후 FPGA 기반의 하드웨어 가속기 적용을 통해 확장 가능성 또한 가지고 있다.

Ⅰ. 서 론

최근 고속화된 네트워크 환경에서 발생하는 다양한 보안 위협은 정형화된 시그니처 기반의 탐지 방식으로는 대응하기 어려운 경우가 많다. 특히, 제로데이 공격, 암호화된 트래픽 내 이상 행위 등은 사전 정의된 규칙만으로는 실시간 탐지가 불가능한 경우가 많아, 머신러닝 기반의 이상 트래픽 감지 기술에 대한 연구가 활발히 진행되고 있다.

이상 트래픽 감지는 비정상적인 트래픽 흐름을 실시간으로 식별함으로써, 침입 탐지 시스템(NIDS), 암호화된 데이터 흐름 분석, 고속 네트워크 내의 QoS(Quality of Service) 보장 등 다양한 보안 요소와 직접적으로 연결된다. 특히 QoS는 단순한 서비스 속도 이상의 문제로, 실시간성이 요구되는 자율주행, 전술 네트워크, 산업 제어 시스템에서는 이상 트래픽이 서비스 지연 또는 중단을 유발할 수 있어, 이를 사전에 탐지하고 대응할 수 있는 경량화된 시스템이 필수적이다.

본 연구에서는 NVIDIA의 저전력 고성능 임베디드 플랫폼인 Jetson AGX Xavier에서 동작 가능한 CNN-LSTM[1], 1D-CNN[2] 및 MLP[3] 기반 트래픽 이상 탐지 모델을 포함한 시스템을 제안하고, 이를 실시간 네트워크 환경에 적용 가능한지 시험하였다. Jetson은 ARM 기반의 CPU와 CUDA를 지원하는 GPU를 통합한 플랫폼으로, 엣지 컴퓨팅 환경에서의 신경망 추론 처리에 최적화되어 있으며, 전력 소비를 최소화하면서도 높은 연산 성능을 제공한다.

제안하는 시스템은 트래픽의 시계열 특성을 학습하여 이상 패턴을 실시간으로 검출할 수 있으며, CPU 또는 GPU 기반 서버 환경 없이 독립적으로 동작이 가능하여 엣지 기반 보안 시스템으로서의 활용 가능성이 높다. 또한, 구조 중 CNN 단독 구조 또는 MLP 모델은 향후 FPGA 기반의 하드웨어 구조로 확장이 용이하며, QoS 보장을 위한 실시간 트래픽 감시·제어 시스템으로 적용할 수 있다.

이러한 점에서 본 연구는 이상 트래픽 감지를 통한 보안 강화와 함께, 고신뢰 실시간 네트워크 서비스를 위한 QoS 유지 기술로의 확장이 가능한 임베디드 시스템 구조를 제안한다는 점에서 학술적 및 산업적 기여를 동시에 제공한다.

Ⅱ. 본론

2.1. 데이터셋

본 연구에서는 University of Queensland에서 제공하는 NF-BoT-IoT 데이터셋을 활용하였다. 이 데이터셋은 UNSW-BoT-IoT의 NetFlow 기반 버전으로, 실제 IoT 환경에서 발생 가능한 다양한 공격 유형(DoS, DDoS, Reconnaissance, Theft 등)과 정상 트래픽(Benign)을 포함한다.

전체 데이터는 학습:검증:테스트를 60:20:20 비율로 분할하여 실험을 수행하였다. 한 가지 고려점은 전체 데이터셋 중 비정상(Attack) 클래스가 약 97% 이상을 차지하며, Benign 데이터는 상대적으로 매우 적다는 점이다. 이러한 클래스 불균형은 학습 모델의 일반화 성능에 영향을 줄 수 있으며, 이 때문에 정상 상태를 이상으로 오분류하는 현상(false positive)이 관찰되었다.

2.2. CNN-LSTM, CNN, MLP 기반 이상 탐지 모델

본 논문에서는 시계열 데이터에서 이상 징후를 탐지하기 위해 CNN-LSTM 하이브리드 모델[1], 1D-CNN 모델[2], MLP 모델[3] 총 3가지 모델을 구현하였다.

본 논문에서 제안하는 시스템 아키텍처는 Figure 1과 같다. 모델은 Jetson AGX Xavier 환경에서 PyTorch +

CUDA 기반으로 구동되었으며, 학습 또한 엣지 디바이스에서 직접 수행 가능하도록 설계되었다. 서버 기반 학습이 가능함에도 불구하고, Jetson 내 GPU를 활용하여 20 Epoch 기준 수 분 이내 학습이 완료되는 수준의 속도를 확보하였다.

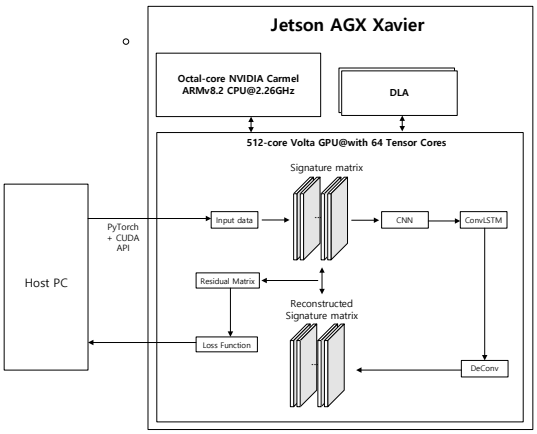

Figure 1. 전체 시스템 아키텍쳐.

2.3. 이상 탐지 성능 결과 및 한계

C-LSTM, CNN, MLP 각각의 모델을 노트북용 CPU, Jetson의 CPU 및 GPU로 성능을 평가한 결과는 Table 1과 같다. MLP 모델의 경우가 가장 높은 정확도를 보였고, CNN 기반 모델에서는 C-LSTM 모델에서 LSTM 계층을 제거한 1D CNN 단독 구조를 적용한 결과, 샘플 길이가 짧은 시계열 데이터의 특성으로 인하여 CNN 기반의 특징 추출만으로도 93%의 이상 탐지 성능을 확보할 수 있음을 확인하였다. 임베디드 GPU에서의 추론 속도가 임베디드 CPU에 비해 향상되었음을 확인하였고, 노트북용 CPU보다는 느린 이유는 파라미터와 층 수가 적은 네트워크 구조가 QoS 탐지에 보통 사용되는데 이는 병렬 처리할 요소가 적기 때문으로 분석된다.

		Ryzen 5700u	8-Core ARMv8.2	512-Core Volta
C-LSTM[1]	Parameter	748,962		
	Accuracy	93 %		
	학습 (1 Epoch, 512 batch)	01m 50s	-	02m 09s
	추론 (1 batch)	1.37ms	8.86ms	1.85ms
CNN[2]	Parameter	73,122		
	Accuracy	93 %		
	학습 (1 Epoch, 512 batch)	26s	-	35s
	추론 (1 batch)	0.28ms	2.80ms	1.09ms
MLP[3]	Parameter	9,794		
	Accuracy	95 %		
	학습 (1 Epoch, 512 batch)	05s	-	12s
	추론 (1 batch)	0.05ms	0.22ms	0.25ms

Table 1. 하드웨어 환경 별 모델 성능

2.4. 경량 구조의 확장 가능성

실험을 통해 CNN 단독 구조 또는 MLP 모델 등의 경량화 모델로 이상 트래픽을 효과적으로 탐지할 수 있음을 확인하였다. 이 결과는 추후 FPGA 기반의 파이프라인 구조로 하드웨어 가속기를 설계한다면 더 높은 성능의 가속 효과를 얻을 수 있을 것으로 보이며, Jetson과 같은 GPU 엣지 디바이스뿐만 아니라 정형화된 고속 보안 시스템 아키텍처로의 이식 가능성을 제시한다.

Ⅲ. 결론

본 연구에서는 이상 트래픽 감지를 통한 보안 강화 및 실시간 네트워크 서비스를 위한 QoS 유지 기술로의 확장이 가능한 이상 탐지 모델을 임베디드 플랫폼인 Jetson 에서 CNN-LSTM 하이브리드 모델과 LSTM 계층을 제거한 1D CNN 단독 모델로 구현하여 CNN 단독 구조가 이상 트래픽을 효과적으로 탐지할 수 있음을 확인하였다. 추후 Cross-Validation 와 같은 기법을 통해 과적합을 방지하고 모델의 일반화 성능 및 분류 정확도를 향상시키고자 한다.

본 논문에서 제안하는 이상 트래픽 감지를 위한 임베디드 시스템 구조가 추후 Jetson 과 같은 GPU 엣지 디바이스뿐만 아니라 FPGA 기반의 하드웨어 가속기에서 파이프라인을 추가하는 확장이 가능하며, 이를 적용함으로써 실시간 고속 네트워크 환경에서의 보안 강화에 기여할 수 있음을 시사한다.

ACKNOWLEDGMENT

본 연구는 LIG 넥스원 미사일시스템핵심기술연구소의 지원을 받아 이루어졌음에 감사드립니다.

참 고 문 헌

[1] M. Ghuge, N. Ranjan, R. A. Mahajan, P. A. Upadhye, S. T. Shirkande, and D. Bhamare, "Deep Learning Driven QoS Anomaly Detection for Network Performance Optimization," *Journal of Electrical Systems*, vol. 19, no. 2, pp. 97- 104, 2023.

[2] M. Azizjon, A. Jumabek and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 2020, pp. 218-224,

[3] Saksham Mittal, Amit Kumar Mishra, Mohammad Wazid, D. P. Singh, Ashok Kumar Das, Sachin Shetty, "Multiclass Classification Approaches for Intrusion Detection in IoT-Driven Aerial Computing Environment", GLOBECOM 2023 - 2023 IEEE Global Communications Conference, pp.2160-2165, 2023.

[4] S. Ness, V. Eswarakrishnan, H. Sridharan, V. Shinde, N. Venkata Prasad Janapareddy and V. Dhanawat, "Anomaly Detection in Network Traffic Using Advanced Machine Learning Techniques," in IEEE Access, vol. 13, pp. 16133-16149, 2025,

[5] C. Zhang, D. Song, Y. Chen, et al., “A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data,” Proc. AAAI Conf. Artif. Intell., vol. 33, pp. 1409- 1416, 2019.