시계열 그래프 신경망 기반 컨테이너 네트워크 이상행위 탐지 시스템

권순홍, 손우영*, 이종혁

세종대학교 정보보호학과 & 지능형드론 융합전공,

*세종대학교 프로토콜공학연구실

soonhong@pel.sejong.ac.kr, *wooyoung@pel.sejong.ac.kr, jonghyouk@sejong.ac.kr

An Anomaly Detection System for Container Networks based Temporal Graph Neural Networks

Soonhong Kwon, Wooyoung Son*, Jong-Hyouk Lee

Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University,

*Protocol Engineering Lab., Sejong University

요 약

최근 대부분의 기업 및 기관에서는 기존 모놀로식 아키텍처에서 마이크로서비스 아키텍처로 전환을 진행하고 있다. 마이크로서비스 아키텍처로의 전환은 클라우드 네이티브로의 전환으로 이끄는 주요 원동력이 되었으며, 이로 인해 Docker와 같은 플랫폼을 기반으로 한 컨테이너 기술의 활용도가 높아지고 있는 상황이다. 이에 따라 컨테이너 환경에 대한 보안이 중요시되는 환경에서 대부분의 연구는 호스트 혹은 호스트와 컨테이너 간의 트래픽에 집중하여 이상행위에 대한 탐지를 수행할 뿐 컨테이너 간 통신에서의 이상행위 탐지에 대해서는 중요하게 고려하고 있지 않은 실정이다. 이에 본 논문에서는 시계열 그래프 신경망을 이용한 컨테이너 네트워크 이상행위 탐지 시스템을 제안하였으며, 정적 그래프 신경망 모델인 GCN보다 동적 그래프 신경망 모델인 TGAT 모델을 적용하였을 시, 정확도 측면에서 약 10.72%의 높은 성능을 달성함을 보임으로써 TGAT 모델을 통해 상시적 보안을 달성할 수 있음을 보인다.

Ⅰ. 서 론

최근 대부분의 기업 및 기관에서는 기존 모놀리식 아키텍처를 기반으로 한 서비스를 제공하던 추세에서 마이크로서비스 아키텍처로의 전환을 진행하고 있다 [1]. 마이크로서비스 아키텍처로의 전환은 클라우드 네이티브로의 전환으로 이끄는 주요 원동력이 되었으며, 이로 인해 Docker와 같은 플랫폼을 기반으로 한 컨테이너 기술의 활용도가 점차 높아지고 있다.

(문제정의및한계점) 하지만, 컨테이너 기술은 격리에 기반한 독립성을 제공하는 반면, 호스트 시스템을 공유하고 있음에 따라 개발에서부터 운영까지 전주기 관리가 요구된다는 한계점이 존재한다. 이에 많은 연구에서는 도커 컨테이너를 빌드하기 위해 요구되는 도커 이미지에 대해 정적/동적 방식에 기반하여 취약점을 사전에 식별하도록 함으로써 이에 대응하고자 하나, 이를 완벽히 보안하지 못한다. 보다 세부적으로 도커 이미지를 기반으로 내재되어 있는 취약점을 식별하고 이를 보안하는 것 자체가 구동중인 도커 컨테이너의 모든 공격 표면을 보안하지 못함을 의미한다. 이에 많은 선행 연구에서는 도커 컨테이너가 운영중인 상황에서 시스템 혹은 네트워크에서 비이상행위를 탐지하고자 많은 노력을 기울이고 있다. 하지만, 대부분의 연구는 호스트 시스템 혹은 호스트 시스템과 컨테이너 간 발생하는 트래픽 데이터를 기반으로 시그니처를 구성하여 비이상적인 행위에 대해 탐지하거나, 이에 더 나아가서는 딥러닝 모델을 활용하여 지능화되고 고도화된 네트워크 보안위협에 대한 탐지를 수행하고 있다. 이는 컨테이너 간 통신에서 발생 가능한 보안위협에 대한 탐지는 어려움을 의미하며, 특히 대부분의 네트워크 보안위협을 탐지하기 위한 딥러닝 모듈 적용 방안은 GCN(Graph Convolutional Networks)과 같은 정적 그래프에 기반을 두고 있어 유기적으로 변화하는 컨테이너 환경에 적합하지 않다는 한계가 존재한다.

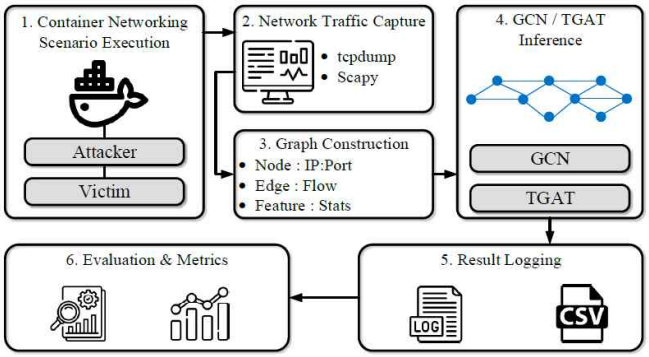
(기여) 이에 본 논문에서는 클라우드 네이티브로 전환되고 있는 환경의 마이크로서비스 아키텍처를 보안하기 위해 독립성이 보장되고 유기적으로 변화하는 컨테이너 환경에 적합한 TGAT(Temporal Graph Attention Network) 모델 [2]을 적용한 네트워크 이상행위 탐지 시스템을 제안한다.

1. **네트워크에대한실시간이상행위탐지시스템제안:**
   도커 컨테이너 환경에서 발생하는 트래픽에 대해 GNN에 활용 가능한 그래프 형태로 변환하여 구성함으로써 유기적으로 변화하는 환경에 용이하게 적용할 수 있는 형태로 구성함
2. **시계열그래프신경망적용:**
   실험 환경에서 컨테이너 간 통신에 대해 시계열 그래프로 구성함으로써 정적 그래프 신경망 모델에서는 식별하지 못하는 시간적 상관관계를 식별할 수 있도록 함
3. **확장가능한프레임워크구성:**
   제안하는 시스템은 데이터 세트 구성에서부터 학습 및 추론까지 하나의 파이프라인으로 구성함으로써 실 환경에서 쉽게 확장하여 사용될 수 있도록 함
4. **실험평가:**
   대표적인 정적 그래프 신경망 모델인 GCN과 동적 그래프 신경망 모델인 TGAT 모델을 교차검증 방식인 K-Fold 방식에 기반하여 비교/분석함으로써 탐지 성능(99.76%)의 우수성을 보임

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 시계열 그래프 신경망 기반 컨테이너 네트워크 이상행위 탐지 시스템에 대해 설명하며, 3장에서는 제안하는 시스템에 대한 성능 분석을 수행한다. 4장에서는 본 논문의 결론을 맺는다.

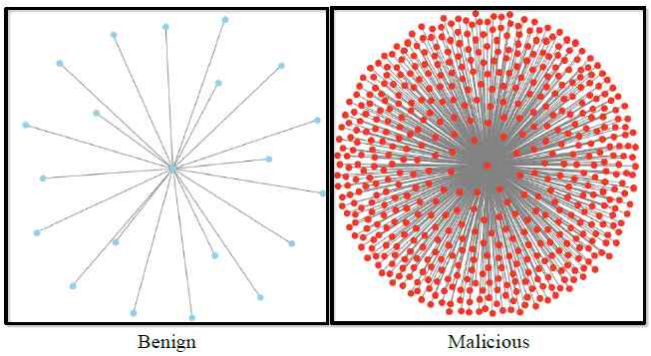
Ⅱ. 제안하는 시스템

정부기관 및 행정기관의 주요 시스템이 클라우드 네이티브 기반의 마이크로서비스 아키텍처로 급속하게 전환되고 있는 상황에서 시스템의 가용성을 보장하기 위해 컨테이너에 대한 보안은 필수적으로 이루어져야 한다.



(그림 1) 제안하는 시스템

이에 컨테이너 간 통신 트래픽의 시계열 정보를 기반으로 TGAT를 적용한 컨테이너 이상행위 탐지 시스템을 구성하였으며, 이는 (그림 1)과 같다. (그림 1)을 통해 확인할 수 있듯이 실험 환경에서는 Attacker(Ubuntu 도커 컨테이너) 및 Victim(Nginx 서버 도커 컨테이너)을 구성하였다. 이후, 사전에 정의한 시나리오를 실행하였으며, 컨테이너 간 HTTP 요청 수행, Redis Key-value 요청, DB 쿼리, API 호출, Ping 메시지 전달을 통해 정상 네트워크 트래픽을 생성하도록 하였으며, port scanning, ssh brute-force, reverse shell, DDoS, ARP Spoofing을 통해 악성 네트워크 트래픽을 생성하도록 하였다. 생성된 네트워크 트래픽은 tcpdump 및 scapy를 통해 캡쳐되도록 하였으며, 캡쳐된 트래픽에 대해 Node에 대해서는 IP:Port로 Edge는 네트워크 트래픽 흐름으로 하여 (그림 2)와 같이 그래프 형태로 구성되도록 하였다.



(그림 2) Benign 및 Malicious 트래픽 그래프 구성 예시

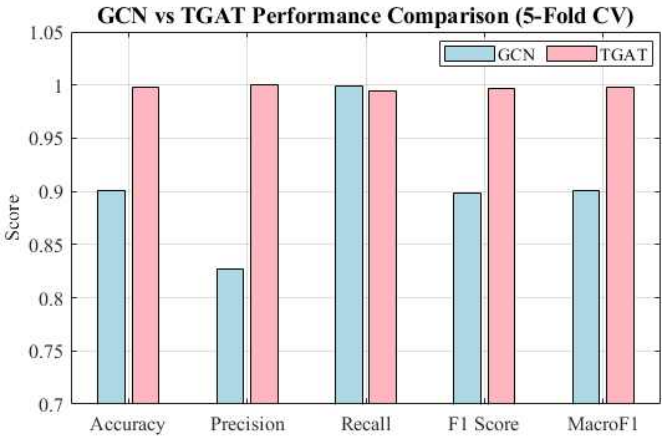
(그림 2)와 같은 그래프 파일을 기반으로 하여 GCN 및 TGAT 그래프 신경망 모델을 활용함으로써 학습 및 추론을 진행하였으며, 이를 통해 네트워크 이상행위 탐지가 이루어지도록 하였다. 이에 대한 결과는 CSV 및 로그 파일로 저장되도록 하고, 다양한 지표를 통해 모델 평가가 이루어지도록 하였다.

Ⅲ. 실험 결과 분석

제안된 시스템은 정적 그래프 신경망 모델인 GCN의 한계를 보안하는 데 주 목적을 두고 있다. 앞서 언급한 바와 같이 대부분의 선행 연구에서는 컨테이너 간 통신에서의 비이상행위 탐지에 집중하고 있지 않으며, 호스트 및 호스트와 컨테이너 간 통신 데이터셋을 활용하고 있다는 한계점이 존재한다. 이에 2장에서 설명한 바와 같이 컨테이너 간 통신을 기반으로 하여 총 5,000개의 데이터셋을 수집하였으며, 이를 (그림 2)와 같은 그래프 형식으로 모두 변환하였다. 또한, 모든 학습은 Distributed Data Parallel 환경에서 수행되도록 하였으며, K-Fold 값을 5로 두어 교차 검증이 이루어진 값에서 최고의 성능을 보인 값을 도출하도록 하였다. 이를 기반으로 정적 그래프 기반 GNN 모델인 GCN과 동적 그래프 기반 TGAT 모델의 성능을 비교하였으며, 이는 [표 1] 및 (그림 3)을 통해 확인할 수 있다.

〔표 1〕 네트워크 이상행위 탐지에서의 GCN/TGAT 성능 비교

Model	Accuracy	Precision	Recall	F1 Score	Macro F1
GCN	0.9010	0.8271	0.9994	0.8988	0.9010
TGAT	0.9976	1	0.9941	0.9971	0.9975



(그림 3) GCN/TGAT 모델 성능 비교

[표 1]을 통해 확인할 수 있듯이 TGAT 모델의 경우, Precision이 100%로 도출되는 것을 확인할 수 있으며, 이를 모든 Fold의 결과 값을 통해 확인하였을 때, 모두 100%로 나왔음을 확인하였다. 이는 특정 상황에서 비롯된 상황이 아님을 보이며, 이로 인해 상대적으로 Racall 성능이 떨어짐을 확인할 수 있다. 또한, [표 1] 및 (그림 3)을 통해 확인할 수 있듯이 정확도 측면에서 TGAT가 GCN에 비해 약 10.72%의 성능 우위에 있음을 확인할 수 있다. 이에 따라 시계열 정보를 활용할 수 있는 상황에서는 TGAT 모델이 GCN 모델보다 적합함을 확인할 수 있으며, 이는 컨테이너 네트워크 환경에서 상시적 보안을 제공하기 위한 모델로 고려할 수 있음을 의미한다.

Ⅳ. 결론

본 논문에서는 클라우드 네이티브 전환에 따른 마이크로서비스 아키텍처의 보안을 위한 TGAT 기반 컨테이너 네트워크 이상행위 탐지 시스템을 제안하였다. 대부분의 선행 연구에서는 호스트 혹은 호스트와 컨테이너 간 트래픽에 집중하여 이상행위를 탐지하고 있어 제안된 시스템에서는 컨테이너 간 통신 트래픽을 캡쳐하여 GNN에서 학습 가능한 그래프 형태로 변환하여 GCN 및 TGAT 모델을 통해 학습 및 추론을 진행하였다. 이에 따라 총 5,000개의 데이터셋에 대해 실험을 진행한 결과, TGAT 모델이 GCN 모델에 비해 정확도 측면에서 약 10.72% 높은 성능을 달성할 수 있음을 보였으며, 이를 통해 기존 정적 그래프 신경망 모델의 한계를 보안하고, 유기적으로 변환하는 컨테이너 환경의 네트워크 보안을 위해 시계열 정보를 고려한 모델이 컨테이너 환경의 상시적 보안을 달성할 수 있을 것으로 기대할 수 있음을 보인다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임 (No. RS-2024-00444170, 6G 개방형 네트워크 환경에서 트러스트 모델 기반 지능형 침해대응 기술 연구 및 국제협력).

참 고 문 헌

[1] BLINOWSKI, Grzegorz; OJDOWSKA, Anna; PRZYBYŁEK, Adam. Monolithic vs. microservice architecture: A performance and scalability evaluation. *IEEE access*, 10: 20357-20374, 2022.

[2] FATHY, Ahmed; LI, Kan. TemporalGAT: Attention-based dynamic graph representation learning. In: Advances in Knowledge Discovery and Data Mining: 24th Pacific-Asia Conference, *PAKDD 2020*, Singapore, May 11-14, 2020, Proceedings, Part I 24. *Springer* International Publishing. p. 413-423. 2020.