심층 학습을 이용한 에지 컴퓨팅 보안 향상 및 최적화 방안에 관한 연구 동향

오신혁, 고윤영, 정재욱, 정종문*
연세대학교 전기전자공학과, 연세대학교 전기전자공학과, 연세대학교 전기전자공학과,
*연세대학교 전기전자공학과

ohsh99@yonsei.ac.kr, rhdbsdud@yonsei.ac.kr, qazaq9669@yonsei.ac.kr,
*jmc@yonsei.ac.kr

Research Trends on Security Enhancement and Optimization Strategies for Edge Computing Using Deep Learning

Shinyeok Oh, Yunyeong Goh, Jaewook Jung, Jong-Moon Chung*
Yonsei Univ. Electrical and Electronic Engineering, Yonsei Univ. Electrical and Electronic Engineering, Yonsei Univ. Electrical and Electronic Engineering, *Yonsei Univ. Electrical and Electronic Engineering

요 약

5G 가 상용화되면서 생겨난 증강 현실, 산업용 사물 인터넷과 같이 높은 컴퓨팅 능력을 요구하는 서비스들로 인해 에지 컴퓨팅에 대한 요구가 증가하고 있다. 에지 컴퓨팅은 익명의 다수의 단말이 이용하므로 보안성 향상이 중요하고 보안 취약점이 제대로 알려지지 않았다. 본 논문은 에지 컴퓨팅의 보안을 강화하기 위해 심층 학습을 이용한 최신 연구 동향을 제시하고 향후 연구 방향성을 모색한다.

Ⅰ. 서 론

5G 가 상용화되면서 증강 현실, 산업 사물인터넷, 자율주행 차량과 같은 새로운 서비스들이 생기고 있다. 이러한 서비스들은 빠른 데이터 처리 속도와 낮은 지연시간을 요구하여 높은 컴퓨팅 능력을 요구한다. 단말의 부족한 컴퓨팅 능력으로 인해 컴퓨팅 능력을 보완해주는 에지 컴퓨팅에 대한 요구가 떠오르고 있다. 하지만 에지 컴퓨팅에는 서버, 단말, 무선 통신 과정 등 각 단계에 많은 보안 취약점이 존재한다. 에지 컴퓨팅 환경에서 보안을 확보하는 것은 에지 컴퓨팅을 상용화하기 위해서는 필수적이므로 이에 대해 많은 연구들이 진행중이다. 본 연구에서는 에지 컴퓨팅에 보안 향상을 위한 기법 중 심층 학습을 이용한 기법들을 소개하고 비교함으로써 보안 향상을 위한 향후 연구 방향성을 제시하고자 하였다.

Ⅱ. 본론

에지 컴퓨팅에서의 공격은 크게 단말이 공격자인 경우, 무선 통신 과정에서의 공격, 서버가 공격자인 경우인 경우로 나눌 수 있다.[1] 본 논문에서는 단말이 공격자인 경우와 서버가 공격자인 경우에 대해 분석하고자 한다. 그림 1 은 각 에지 컴퓨팅 환경에서 공격자인 단말이 존재하는 경우와 서버 중 공격자가 존재하는 경우를 나타낸다.

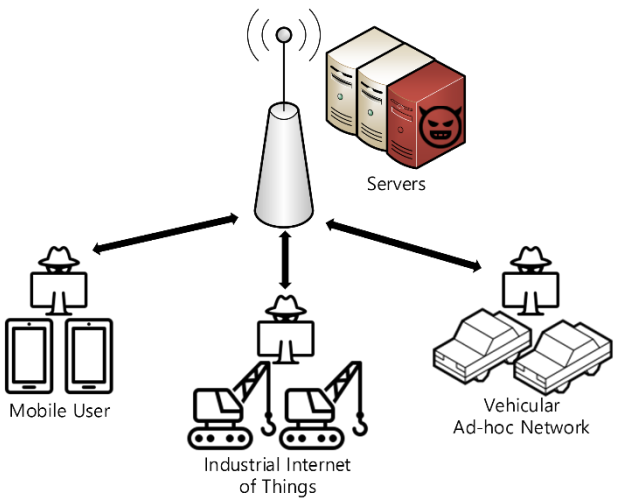

그림 1. 에지 컴퓨팅 단말과 서버가 공격자인 경우

최근 그래프에서 심층 학습을 이용하여 이상 노드 감지 혹은 이상 에지 감지 기법에 대한 연구가 진행중이다.[2] 전통적인 이상 노드 감지 기법은 데이터 셋에서 일반적이지 않은 패턴을 보이는 데이터를

분류하는 방식이므로 이상 노드 혹은 이상 에지를 분류할 수 없지만 그래프 이상 감지 기법을 이용하면 이상 노드, 이상 에지 뿐 아니라 이상 노드 그룹도 알아낼 수 있다는 장점이 있다. 그래프 이상 감지 방식 중 심층 학습을 이용한 기법이 이용하지 않은 기법에 비해 좋은 성능을 내므로 심층 학습을 이용한 방식이 연구되는 중이다.

에지 컴퓨팅 환경은 모든 단말, 서버와 기지국을 노드로 생각하고 기지국을 통해 연결된 하나의 그래프로 생각할 수 있다. 따라서 그래프 이상 감지 기법은 에지 컴퓨팅 환경에서 사용될 수 있다. 특히 심층 학습을 이용한 이상 노드 감지 기법은 에지 컴퓨팅 환경에서 단말 공격자를 감지하는데 활용될 수 있으며, 실제로 심층 학습을 이용해 이상 단말을 검출하는 연구들이 진행 중이다. 표 1 에 시뮬레이션 환경 별 단말의 공격 및 이상 행동 감지 기법을 정리했다.

표 1. 단말 공격 및 이상 행동 감지 기법

구분	시뮬레이션 환경	알고리즘
[3]	차량 애드혹 네트워크	GNN, CNN, LSTM
[4]	산업 사물인터넷	Transformer, Federated Learning
[5]	에지 컴퓨팅	GAN

[3]에서는 소프트웨어 정의 네트워크 기반 차량 애드혹 네트워크 환경에서 차량이 디도스 공격하는 것을 심층 학습을 이용해 감지하고 심층 강화학습을 이용해 공격을 회피하여 전체 시스템의 지연시간과 에너지 소모를 최소화하도록 하였다. Graph Neural Network (GNN)을 이용해 차량 사이 연결 및 상태에 대한 특징을 추출했으며 Convolutional Neural Network (CNN)을 이용해 차량 위치에 대한 정보를 추출했다. GNN 과 CNN 을 통해 추출된 특징을 결합해 Long Short Term Memory (LSTM) 네트워크에 입력하여 시계열 분석을 통한 공격을 감지를 진행했다. LSTM 네트워크는 결과 값은 심층 강화학습에 행동으로 이용되어 심층 강화학습 알고리즘을 돌리는데 이용되었다. 시뮬레이션 결과 GNN, CNN, LSTM 으로 공격을 방어하는 행동을 골라 심층 강화학습을 진행할수록 공격을 회피해 전체 시스템의 지연시간과 에너지 소모가 최소화되도록 학습됐다.

[4]에서는 산업 사물인터넷 환경에서 에지 장치의 이상 행동을 심층 학습 방법 중 Transformer 와 Federated Learning 기법을 이용해 감지했다. Transformer 네트워크의 인코더는 에지 장치들에 저장하고 디코더는 에지 서버에 저장하다. 에지 장치들은 자신의 현재 상태를 인코더에 입력하여 인코딩한다. 그리고 인코딩 값에 가우시안 노이즈를 추가하여 개인 정보가 역추적되는 것을 방지하여 에지 서버에 전송한다. 에지 서버는 인코딩 된 값을 디코딩하여 이상 행동 여부를 판단한다. 이와 같이 인코더와 디코더를 분리하고 노이즈를 추가하는 연합학습 방식을 통해 에지 장치 정보를 보호면서 이상 행동 감지를 했다.

[5]에서는 Generative Adversarial Networks (GAN)을 이용하여 일반적인 에지 컴퓨팅 상황에서의 공격을 감지하는 방법을 제안했다. 생성자가 만든 공격을 공격 식별자와 이상 행동 식별자 총 2 개의 식별자가 공격을 식별하고 이를 반복하며 학습하여 식별자의 감지 성능을 향상시켰다. 또한 학습 과정에서 보안 전문가가 중앙 모니터링 시스템을 통해 얻은 정보와 식별자를 통해 식별된 이상 보고서를 분석해 생성자의 공격 생성 방식을 갱신하는 방법을 통해 공격 감지 성능을 더 향상시켰다.

최근 연구 동향은 에지 단말이 공격자인 경우에 심층 학습 알고리즘을 이용해 공격을 감지하는 방향으로 이루어지고 있다. 하지만 에지 서버도 공격자가 될 수 있으며 가상 플랫폼으로 분리된 서버에 대한 보안 취약점은 아직 잘 분석되지 않았다. 따라서 심층 학습을 이용해 서버가 공격을 하는 경우 감지 및 방어하는 방안에 대한 연구가 필요해 보인다.

Ⅲ. 결론

본 논문에서는 에지 컴퓨팅 환경에서 단말의 이상 행동과 공격을 그래프 이론과 접목해 심층 학습을 이용하여 감지 및 방어하는 방안에 대해 분석하였다. 에지 단말이 공격하는 경우를 감지하기 위해 최신 심층 학습 알고리즘인 GNN, LSTM, Transformer, GAN 이 이용된 연구에 대해 분석하였다. 하지만 에지 노드 뿐만 아니라 에지 서버도 공격자가 될 수 있으므로 심층 학습을 이용해 서버의 공격을 방어하는 것을 같이 고려한 연구가 필요할 것으로 보인다.

참 고 문 헌

[1] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1078-1124, Secondquarter 2021.

[2] X. Ma *et al.*, "A Comprehensive Survey on Graph Anomaly Detection With Deep Learning," *IEEE Trans. Knowledge and Data Engineering*, vol. 35, no. 12, pp. 12012-12038, Dec. 2023.

[3] Y. Deng *et al.*, "Resource Provisioning for Mitigating Edge DDoS Attacks in MEC-Enabled SDVN," *IEEE Internet of Things J.*, vol. 9, no. 23, pp. 24264-24280, Dec. 2022.

[4] S. Ma *et al.*, "Privacy-Preserving Anomaly Detection in Cloud Manufacturing Via Federated Transformer," *IEEE Trans. Industrial Informatics*, vol. 18, no. 12, pp. 8977-8987, Dec. 2022.

[5] H. Sedjelmaci, S. -M. Senouci, N. Ansari, and A. Boualouache, "A Trusted Hybrid Learning Approach to Secure Edge Computing," *IEEE Consumer Electronics Mag.*, vol. 11, no. 3, pp. 30-37, May 2022.