고신뢰 분산 운영기술 시스템 보안 메커니즘

문정현[1], 이일구[2]
[1] 성신여자대학교 미래융합기술공학과 석사
[2] 성신여자대학교 융합보안공학과, 미래융합기술공학과 교수

moon_aver@naver.com, iglee@sungshin.ac.kr

Highly reliable distributed OT system security mechanism

Jung-Hyun Moon[1], Il-Gu Lee[1,2]
[1]Dept. of Future Convergence Technology Engineering, Sungshin Women's University
[2]Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

중앙 집중형 OT 시스템은 여러 센서와 장비에서 수집된 데이터가 중앙 서버로 전송되며 처리된다. 이러한 중앙 집중 방식은 모니터링, 의사결정, 제어 등의 데이터 관리를 효율적으로 처리할 수 있지만 구조적으로 데이터 처리가 중앙 시스템에 집중되는 문제가 있다. 그리고 대규모의 산업 데이터가 서버로 전송되기 때문에, 데이터 전송과 활용 과정의 데이터 프라이버시 문제가 존재한다. 그리고 중앙 집중 방식 시스템의 단일 장애 취약점에 의한 데이터 유출이나 시스템 장애로 이어질 수 있다. 이러한 문제를 해결하기 위해 본 연구에서는 고신뢰 분산 OT 보안 메커니즘을 제안한다. 실험 결과에 따르면 제안한 메커니즘은 전체적인 시스템의 구조를 강화하면서 99%의 위험상황 분류 정확도를 보였다.

1. 서론

운영기술(OT, Operational technology) 시스템은 가용성이 중요해서 새로운 기술을 도입하는 대신에 전통적인 방식을 고수하는 레거시 산업(Legacy industry)이다. 이러한 이유로 OT 시스템은 기존의 기술, 방법론, 운영 모델에 의존하고 오래된 장비를 사용하는 경우가 많아서, 고도화된 공격 기법에 대응하기 어렵다. 이로 인해 OT 시스템은 보안이 취약하며, 사이버 해킹의 주요 대상이 되어 사이버 공격 횟수 및 규모가 점점 증가하고 있다. 이러한 피해를 방지하기 위해 임계치 기반의 중앙 집중형 알람 시스템이 활용되고 있으나 비효율적인 성능과 보안 취약성이 큰 문제가 되고 있다[1]. 따라서 OT 산업의 특성을 고려하여 산업 시스템의 보안성과 효율성을 동시에 향상시킬 수 있는 새로운 접근 방식이 필요하다.

본 연구의 주요 기여점은 다음과 같다.

- 인네트워크 컴퓨팅(In-Network Computing)을 활용한 고신뢰 분산 OT 보안 메커니즘을 제안한다.
- 중앙 서버에 대한 의존도를 낮추고 데이터 처리 효율성과 신뢰성을 높이는 데 기여한다.

2. 관련연구와 문제점 분석

OT 가 정보기술(IT, Information Technology)과 격리되어 운영되던 과거와 다르게 최근에는 OT 시스템이 온라인을 통해 IT 시스템과 연결되었지만 특수 목적의 프로토콜에 의존하고 있어서 다른 분야 대비 발전 속도가 느리다. 특히, 기술 발전을 고려하지 않고 운영되는 레거시 산업 시스템은 첨단 보안 솔루션에 대한 지원뿐만 아니라, 기본적인 보안 조치마저 미흡하다[2]. 이로 인해 사회기반시설과 공장 등의 주요 인프라에 대한 보안 사고가 발생하면 치명적인 결과를 초래할 수 있으므로 OT 시스템 보안 강화가 필요하다. 본 장에서는 OT 시스템의 특징을 확인하고, 보안 강화를 위한 고려 사항을 분석한다. 종래 연구들에서는 표 1 과 같이 OT 문제 상황 해결을 위해 임계치 또는 중앙 처리 기법으로 정확도를 높이고 있으나, 중앙에서 데이터를 처리하기 때문에 단일 지점 장애 취약점과 데이터 전송 시 보안 취약점이 존재한다. OT 환경은 안정성이 중요하지만 사이버 공격으로 인한 피해가 큰 만큼, 단순히 다른 분야에서 활용되는 기술을 그대로 도입하는 것이 아닌 산업의 특성을 고려한 효율적이고 안전한 보안 솔루션이 요구된다.

<표 1> 종래 OT 알람 시스템 기술 동향

관련연구	주요 기여점	한계점
[3]	파이프라인 누출 감지를 위한 동적 임곗값 식별 방법 제안	중앙 데이터 처리 방식의 규모가 커질 경우 성능 저하
[4]	산사태 예측을 위해 강우 임곗값과 기울기 센서를 결합한 경보 시스템 제안	확장성 측면에서의 성능 저하
[5]	퍼지를 통해 샘플을 분류하는 퍼지 기반 준지도 학습 접근 방식 제안	데이터 품질에 따른 정확도 하락
[6]	산업 시스템에서 공격 탐지 정확도를 높이기 위한 기계학습 기법 소개 및 평가	한정된 환경에서 성능 검증이 요구되며, 다양한 데이터셋 검토 필요

1) 종래 OT 시스템

OT 알람 시스템은 실시간 모니터링과 제어를 목적으로, 다양한 산업 공정에서 발생할 수 있는 잠재적 위험을 감지하고 경고하는 데 중요한 역할을 한다. 현재 대부분의 OT 알람 시스템은 수많은 센서 및 장치에서 측정된 값이 설정된 임계치를 벗어날 때 위험을 경고하는 임계치 기반의 알람 방식으로 운영된다. 산업 현장에서 온도, 압력, 소리 등의 데이터를 검출하기 위한 임계치, 알람 유형, 반응 프로토콜 등을 설정할 수 있다. 또한, 산업 환경의 안전과 효율을 유지하도록 도와주지만, 센서 오류나 복잡한 환경으로 인하여 잘못된 알람이 발생할 수 있는 문제가 있다[7]. 이러한 문제는 오탐률과 미탐률을 증가시키는 요인이 되고, 위험 대응을 방해하여 작업자의 피로도를 증가시킨다. 이상 탐지 정확도를 높이기 위해 복합적인 데이터를 활용하는 중앙 집중형 모델을 활용하고 있으나, 중요 데이터의 중앙 집중화로 인한 보안과 프라이버시 문제가 발생할 수 있다.

2) 레거시 산업 시스템

레거시 산업 시스템은 오랜 기간 동안 검증되어 안정성을 제공하지만, 현대의 기술 발전 속도 대비 기술의 혁신이 느리다. OT 장비는 특수 목적으로 장기간 사용하기 위해 다양한 프로토콜과 OS 를 활용해 제작되어 복잡하고 새로운 장치와 호환이 어렵다[8]. 이로 인해 시스템 간의 통합이 어려우며, 오래된 OS 를 사용하는 등 기본적인 보안 조치가 부족하다. 또한, 초기 OT 시스템은 온라인과 격리된 환경에서 작동하도록 설계되어, 암호화, 인증과 같은 보안 기능이 중요하지 않았다[9]. 그러나, OT 와 IT 가 연결되어 구조적으로 통합 운영됨에 따라, 공격 표면이 넓어져 사이버 위협이 산업 제어 시스템에 영향을 미치고 있다. 이로 인해, 산업 자동화를 위해 개발된 Modbus, PROFIBUS(Process Field Bus), DNP3(Distributed Network Protocol version 3)와 같은 폐쇄적인 프로토콜 환경에서는 안정적인 통신을 제공했지만, 명령어 패킷의 무결성을 확인하지 않는 취약점과 버전 차이로 인한 호환성 문제를 해결해야 한다[10].

3) OT 실증의 특수성과 곤란성

OT 시스템의 기능이 중단될 경우 심각한 손실이나 산업 재해로 이어질 수 있기 때문에 가용성 및 무결성이 중요하다[11]. 그러나, 보안 강화를 위한 연구의 필요성이 커지고 있음에도 불구하고, 실증이 어렵다. 실제 환경에서의 실험은 시스템 다운이나 생산 중단과 같은 예상치 못한 문제가 발생할 수 있고, 이에 따른 피해가 막대하기 때문이다. 이를 방지하기 위해 대부분의 OT 보안 연구는 실제 환경이 아닌, False data injection, Reconnaissance, DoS, Spoofing 등의 공격이 포함된 공개 데이터 세트를 통해 제한적으로 진행되어 왔다[12]. OT 시스템은 구성 요소와 프로토콜이 다양하기 때문에 실제 환경에서 발생할 수 있는 취약점과 공격 유형을 포괄적으로 다루기 어렵고, 현실적인 보안 솔루션을 개발하고 검증하는 데 한계가 있다. 따라서, 넓은 공격 표면을 커버하기 위해서는 다양한 방식을 결합한 Defence in depth 를 활용하거나, OT 의 특성을 고려한 새로운 보안 기법이 개발되어야 한다.

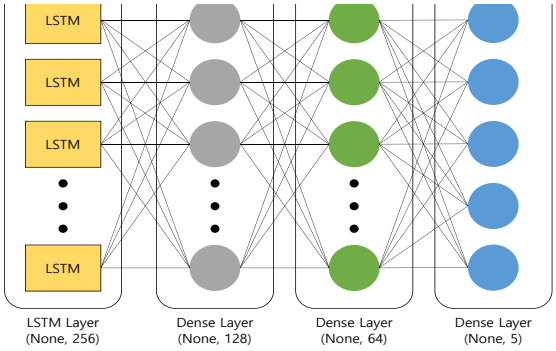
3. 고신뢰 분산 OT 보안 메커니즘

본 장에서는 OT 보안 시스템의 효율성과 신뢰성을 강화하는 고신뢰 분산 OT 보안 메커니즘을 제안한다. 인네트워크 컴퓨팅은 스위치, 라우터 등의 네트워크 장비가 논리, 산술 작업을 수행함으로써, 네트워크 전체에 작업이 분산되는 컴퓨팅 기술이다. 인네트워크 컴퓨팅을 활용하면 정보의 중앙 집중 이슈를 해결하고, 전통적인 중앙 집중식 시스템 대비 부하를 낮출 수 있다[13]. 이 기술을 이상 탐지에 적용할 경우, 실시간으로 네트워크 트래픽의 비정상 패턴을 탐지하여 초기 공격 차단 등의 신속한 대응을 할 수 있고, 모니터링, 데이터 집계, 혼잡 제어에 활용할 수 있다[14]. 제안하는 고신뢰 분산 OT 보안 메커니즘은 네트워크 및 OT 장비들이 서로 연결되어 네트워크를 형성한다. 네트워크 내 센서는 데이터를 수집하고, 네트워크 장치는 데이터를 처리한 뒤 본래 역할인 중앙 서버로 전달한다. 이때, 외부 메모리에 액세스하지 않고 데이터를 처리하기 때문에 대기 시간이 적으며, 실시간으로 데이터를 처리할 수 있다[15]. 또한, 네트워크 장비가 데이터를 처리한 후 결과를 저장하지 않고 결과값을 전달하므로 정보를 보호할 수 있다.

4. 성능평가

1) 실험 환경

본 연구에서는 OT 시스템에 인네트워크 컴퓨팅을 적용했을 때 성능을 평가하기 위해 Python 3.7.12 환경에서 31Gi RAM 과 Ubuntu 운영 체제가 탑재된 CPU 4xAMD EPYC 7B12 를 활용하여 모델을 학습하였다. 그림 1 은 실험에서 활용한 학습 모델의 구조로, LSTM 레이어와 3 개의 dense 레이어로 구성된다.



(그림 1) 네트워크 레이어 구조도

OT 환경에서의 위험 상황은 다양하지만, 제조, 에너지 관리, 수처리 시설 등과 같이 광범위한 환경을 포함하므로, OT 산업에서의 위험 상황을 일반화하였다. 경보, 화재, 사회 기반 시설의 문제, 자연재해로 인한 위험과 정상 상황으로 구분하여 OT 시스템에서 발생할 수 있는 danger, fire, gas, non, tsunami 5 가지 상황의 wav 확장자 소리 데이터를 각각 600 개씩, 총 3,000 개로 구성된 데이터셋을 활용했다[16].

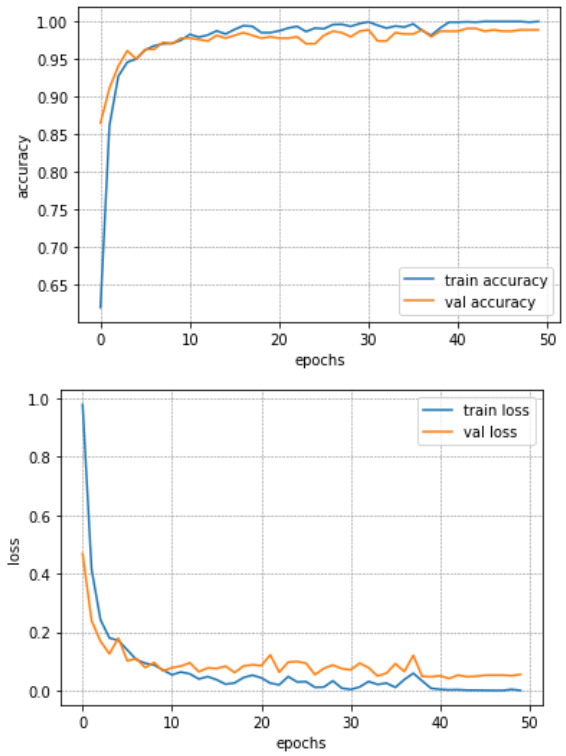
2) 실험 결과 및 분석

본 장에서는 제안 메커니즘의 성능을 평가하기 위해 오픈소스를 활용하여 위험 상황 분류 결과를 분석하였다[17]. 표 1 은 위험 상황에 대한 분류 성능을 평가한 결과이다. non 클래스의 recall 은 상대적으로 낮아서 정상 상황에 대해서는 오탐을 할 가능성이 있지만, 위험 상황인 gas 와 tsunami 클래스에 대해서는 100%의 precision 과 recall, f1-score 를 보였다.

<표 1> 위험 상황별 분류 성능 평가

Category	Precision	Recall	F1-score
danger	99%	98%	99%
fire	99%	98%	99%
gas	100%	100%	100%
non	96%	98%	97%
tsunami	100%	100%	100%

그림 2 는 모델의 훈련 및 검증 데이터에 대한 accuracy 와 loss 를 측정한 결과를 보여준다. 제안한 모델이 10 epoch 이후에 안정적으로 높은 성능을 유지하여 일반화되었다. 이 실험 결과를 통해 고신뢰 분산 OT 보안 메커니즘의 보안성과 성능을 확인하였다.



(그림 2) 학습 결과에 따른 accuracy, loss

5. 결론

OT 와 IT 시스템이 통합되면서 사이버 위협 및 취약성이 증가하여 OT 보안 강화의 중요성이 부각되고 있다. 그러나, OT 산업의 레거시 프로토콜과 제한된 테스트 환경은 기존 보안 강화 방안의 적용을 어렵게 만들고 있다. 중앙 집중형 알람 시스템으로 위험 탐지 정확도를 제공하고 있지만, 데이터가 중앙 서버로 전송되어 스니핑, 스푸핑 공격에 의한 데이터 유출 위협에 노출된다. 본 연구에서는 데이터 보안 및 구조 강화와 효율성을 개선하기 위해 고신뢰 분산 OT 보안 메커니즘을 제안하였다. 제안 메커니즘은 인네트워크 컴퓨팅 기술을 기반으로 네트워크 장치에서 데이터를 처리하여 결과만을 중앙 서버에 전달해 보안 문제를 효율적으로 해결하고 높은 분류 성능을 유지했다. 향후 연구에서는 사이버 위협에 대한 분석을 수행하고, 오류에 강한 OT 보안 메커니즘을 연구할 계획이다.

Acknowledgement

본 논문은 2024 년도 산업통상자원부 및 한국산업기술진흥원의 산업혁신인재성장지원사업 (RS-2024-00415520)과 과학기술정보통신부 및 정보통신기획평가원의 ICT 혁신인재 4.0 사업의 연구결과로 수행되었음 (No. IITP-2022-RS-2022-00156310)

참고문헌

[1] Qin L, Peña-García A, Leon AS, Yu J-C, Comparative Study of Energy Savings for Various Control Strategies in the Tunnel Lighting System, Applied Sciences, vol. 11, no. 14, 2021.

[2] R. Khan, K. McLaughlin, B. Kang, D. Laverty and S. Sezer, A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems, 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, pp. 1-5, 2020.

[3] Y. Xu et al., Pipeline Leak Detection Using Raman Distributed Fiber Sensor With Dynamic Threshold Identification Method, in IEEE Sensors Journal, vol. 20, no. 14, pp. 7870-7877, 15 July15, 2020.

[4] Abraham, M.T, Satyam, N, Bulzinetti, M.A, Pradhan, B, Pham, B.T, Segoni, S, Using Field-Based Monitoring to Enhance the Performance of Rainfall Thresholds for Landslide Warning. Water, vol. 12, 2020.

[5] Ashfaq, Rana Aamir Raza, et al, Fuzziness based semi-supervised learning approach for intrusion detection system. Information sciences, vol. 378, pp/ 484-497, 2017.

[6] Wang, Wu, et al, Cyber-attacks detection in industrial systems using artificial intelligence-driven methods, International Journal of Critical Infrastructure Protection, vol. 38, 2022.

[8] Serror, Martin, et al, Challenges and opportunities in securing the industrial internet of things, IEEE Transactions on Industrial Informatics, vol. 17, no. 5 pp. 2985-2996. 2020.

[9] Køien, G.M, Zero-Trust Principles for Legacy Components, Wireless Pers Commun, vol. 121, pp. 1169–1186, 2021.

[10] O.Givehchi, K. Landsdorf, P. Simoens and A. W. Colombo, Interoperability for Industrial Cyber-Physical Systems: An Approach for Legacy Systems, in IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 3370-3378, 2017.

[11] Dhirani LL, Armstrong E, Newe T, Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap, Sensors, vol. 21, no. 11, 2021.

[12] Koay, A.M.Y., Ko, R.K.L. Hettema, H. et al., Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges, J Intell Inf Syst, vol. 60, pp. 377–405, 2023.

[13] S. Kianpisheh and T. Taleb, A Survey on In-Network Computing: Programmable Data Plane and Technology Specific Applications, in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 701-761, 2023.

[14] H. Wu, Y. Shen, X. Xiao, G. T. Nguyen, A. Hecker and F. H. P. Fitzek, Accelerating Industrial IoT Acoustic Data Separation With In-Network Computing, in IEEE Internet of Things Journal, vol. 10, no. 5, pp. 3901-3916, 1 March, 2023.

[15] M. Blöcher, L. Wang, P. Eugster and M. Schmidt, Holistic Resource Scheduling for Data Center In-Network Computing, in IEEE/ACM Transactions on Networking, vol. 30, no. 6, pp. 2448-2463, 2022.

[16] Kaggle, Alarm dataset, https://www.kaggle.com/datasets/devisdesnug/alarm-dataset, 2022

[17] Kaggle, https://www.kaggle.com/code/devisdesnug/rnn-mfcc/notebook, 2022