전장형 CPS 이상행동 탐지 기술 조사

하영빈*, 최상훈[1], 박기웅†

세종대학교 SysCore Lab. (대학원생, 연구교수[1])

**세종대학교 정보보호학과 (교수†)

Detection Techniques for Anomalous Behavior in Battlefield-Type CPS: A Technical Investigation

Young-Bin Ha*, Sang-Hoon Choi[1], Ki-Woong Park†

* SysCore Lab., Sejong University

**Dept. of Computer and Information Security, Sejong University

(Graduate Student*, Research Professor[1], Professor†)

요 약

정보 수집과 더욱 정밀한 작전 수행을 위해 국방 분야에서는 센서, 제어기, 통신 장치 등을 통합하여 동작하는 사이버물리시스템(Cyber-Physical Systems, CPS)의 활용이 증가하고 있다. 그러나 이러한 시스템은 내·외부적인 다양한 위협에 취약하며, 정상적인 동작을 가장한 이상행동(Anomalous behavior)이 발생할 가능성도 존재한다. 갈수록 진화하는 기술에 따라 공격의 정교함도 높아지고 있으며, 이에 대응하기 위해서는 보다 지능화된 이상행동 탐지 기법이 요구된다. 이에 본 논문은 국방 분야에서 활용되는 CPS에 대한 위협 요소 및 이상행동 유형을 정리하고, 이를 탐지하기 위한 기술들을 조사한다. 나아가, 다양한 위협 유형에 대응하기 위한 이상행동 탐지 기법에 대한 향후 연구 과제를 제시하고자 한다.

I. 서론

최근 복잡해지는 전장 환경과 고도화된 위협에 대응하기 위해, 국방 분야에서는 정보 기반 지능성과 네트워크 기술을 결합한 군사 시스템 운용이 현대 전장에서 확대되고 있다. 이러한 시스템의 예로는 FANET, Swarm CPS, Cognitive CPS와 같은 전장 상황 인식 기반 네트워크 구축 시스템, 무인 시스템, C5ISR, 위성 시스템(ISL, Federated Satellite System) 등이 있으며, 이들은 모두 사이버물리시스템(CPS)에 속한다. 일반적인 CPS는 산업 제어, 자율 주행과 같은 민간 분야에 널리 활용되며, 주로 효율성과 자동화를 중심으로 설계된다. 그러나 실시간성과 보안성, 생존성 등의 요구가 훨씬 더 강한 전장에서 운용되는 CPS는 산업용 CPS와 유사한 형태를 가지더라도, 시스템의 운용 목적이나 물리적 환경, 위협 양상과 같은 측면에서 큰 차이를 보이며 특히, 전장에서 동작하는 CPS는 작은 오차나 위협에도 심각한 재산적, 안보적 피해가 발생할 수 있다. 지난 2024년 드론의 공격으로 인해 덴마크 호위함의 미사일 시스템에서 오작동이 발생하여 큰 피해가 있었던 사례와 최근 알래스카에서 훈련 중이던 전투기가 선회하며 추락하는 등의 사례로 보았을 때 가시적으로 확인할 수 있는 이상행동뿐만 아니라 은닉된 형태의 이상행동이 발생하여 심각한 피해를 초래할 수 있다. 이처럼 CPS에 발생하는 이상행동을 신속하게 탐지하고 효과적으로 대응할 수 있는 기술은 필수적이며, 이에 본 논문

†교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원 (IITP)의 정보보호핵심원천기술개발(Project No. RS-2024-00438551,30%), 한국연구재단(NRF) 중견후속연구사업(Project No. RS-2023-00208460, 40%), 국방ICT융합연구(Project No. 2022-11220701, 30%)의 지원을 받아 수행된 연구임.

은 전장 환경에서 운용되는 CPS에서 발생할 수 있는 위협 요소와 이상행동의 유형을 정리하고, 이를 탐지하기 위한 다양한 대응 기법들을 조사·분석한다.

II. 국방 CPS 위협 요소

산업용 CPS에 대한 공격은 주로 금전적인 목적을 가지고 수행되지만, 전장에서 운용되는 CPS는 작전의 성공 여부와 국가 안보에 직결되는 시스템인 만큼, 이에 대한 공격은 그 위협의 목적뿐만 아니라 범위 및 결과의 심각성이 본질적으로 다르다. 재밍 및 HPM 공격 같은 전자전 위협이나 악성 코드를 이용한 위성 및 통신망 무력화, 국가 중요 시설을 겨냥한 APT 공격 등은 전장 환경에서 운용되는 CPS가 직면하는 주요 위협 요소에 해당한다. 이러한 요소들을 정리하고자 본 장에서는 CPS에서 나타날 수 있는 주요 위협 요소들을 유형별로 정리한다.

Abshari and Sridhar [1]은 공격 벡터를 디지털 기반 위협, 물리적 위협, 내부자 위협의 세 가지 범주로 구분하였으며, Duo et al. [2]는 기밀성, 무결성, 가용성 관점에서 분류하였다.

[표 1] 주요 위협 요소 분류표

위협요소	기밀성	무결성	가용성
디지털 기반 위협	- 네트워크 스니핑 - 인증 우회 - 세션 하이제킹	- 패킷 인젝션 - 제로 데이 공격 - 악성 코드 삽입 - 재전송 공격	- DoS/DDoS 공격 - 자원 고갈 - 시스템 마비 유도
물리적 위협	- 물리 접근 후 정보 유출 - 사회 공학	- 센서 조작 - 악성 구성품 삽입	- 재밍 - 인프라 파괴 - 시설 및 시스템 공격
내부자 위협	- 권한 초과 접근 - scavenging	- 설정 변경 및 백도어 - 미션 데이터 변조 - 조작된 부품 설치	- 시스템 종료 - 오작동 유발 - 서비스 중단 유도
공급망 위협	- 악성 펌웨어 주입 - 위조 인증서 생성	- SW/HW 변조 - 악성 업데이트 삽입 - 서드파티 조작	- 구성 요소 마비 유도 - 필수 시스템 기능 상실 유도

앞서 언급한 분류를 바탕으로 주요 위협 요소의 기준을 재정립하였으며, 해당 기준에 따른 위협 요소를 정리한 결과는 [표 1]과 같다.

III.이상행동 유형 분류 및 탐지 기법

실시간으로 변하는 복잡한 전장 환경 속에서 운용되는 CPS에는 [표 1]에 제시한 단일 위협 요인뿐만 아니라 여러 위협 요소가 복합적으로 적용되거나 이외의 요소들로 인해 이상행동이 발생할 수 있다. 수많은 위협의 종류와 발생 방식이 존재하는 환경인 만큼, 이로부터 파생되는 이상행동 또한 다양하게 양상으로 나타나는데, 이에 CPS를 구성하는 필수 요소인 SW와 HW를 기준으로 각 구성 요소별 공격 대상과 해당 대상에서 일어날 수 있는 이상행동의 유형을 분류하고 이를 탐지 하기 위한 관련 연구를 조사하였다.

우선 SW 영역에서는 응용 소프트웨어, 운영체제 및 펌웨어, 미들웨어, 보안 소프트웨어로 세분화하고, 각 영역에서 발생할 수 있는 이상행동으로 동작 오류, 펌웨어 오작동, 시퀀스 번호 오류 등과 같은 형태로 분류하였다. 이러한 이상행동을 탐지하기 위한 연구로는 악성 코드 탐지[6], 루트킷 탐지[7], 네트워크 패킷 분석[3], 인증 우회 탐지[14] 등이 있었다. HW 영역에서는 센서, 액추에이터, 통신 모듈 그리고 메모리와 MCU를 공격 표면으로 세분화한 다음, 이 영역에서 발생할 수 있는 이상행동으로는 비정상 값, 동작 이상, 펌웨어 무결성 손상 등으로 분류하였으며, 이를 탐지하기 위한 기술로는 센서 데이터 이상 탐지[17], 시스템 상태 이상 탐지[8, 9], IoT 시스템에 대한 이상 탐지[18] 등이 연구된 바가 있었다. 각 연구의 평가를 보았을 때 정확도는 0.9에서 0.99, 정밀도는 0.87부터 0.98, 재현율은 0.93에서 1, F1-score는 0.83부터 0.97의 수치를 나타내었고 동일한 대상에 대한 실험은 아니지만, 각 탐지 기법별로 성능의 차이가 있었으며 이러한 연구를 통해 실제 개발된 기술로는 CADS, HACMS 등이 있었다. 앞서 언급한 분류 결과를 토대로 작성한 [표 2]는 공격 대상과 해당 대상에서 발생할 수 있는 이상행동 그리고 이를 탐지하기 위한 기술 간의 연쇄 구조를 나타내었다. 조사한 연구들은 SW와 HW 간의 경계 또는 SW 안에서도 대상이 되는 요소 간에 대한 복합적 탐지 연구는 주로 다루고 있지 않는 것으로 나타났다.

[표 2] 주요 이상행동 유형 분류표

공격 대상		이상행동 유형	관련 연구	정확도
SW	응용 소프트웨어	- 제어 오류 - 동작 오류	- LLVM IR 대상 악성 코드 탐지를 위한 이미지 기반 모델[6] - GAN 기반 런타임 이상 탐지[15]	0.9
	운영체제 및 펌웨어	- 커널 패닉 - 펌웨어 오작동	- ARM PMU 이벤트를 활용한 TrustZone 루트킷 탐지[7] - 오토인코더를 사용한 하드웨어 및 펌웨어 이상 탐지[12]	0.99
	미들웨어 및 통신 계층	- 시퀀스 번호 오류 - 전송 지연 - 비인가 메시지 수신	- LSTM AE를 이용한 네트워크 패킷 분석[3] - 네트워크 트래픽 탐지를 위한 DAGMM[5] - 시그니처 정보 기반 ARP 스푸핑 탐지[13]	0.9~0.98
	보안 소프트웨어	- 인증 우회 - 접근 권한 상승	- SVDD을 이용한 디바이스 유효성 검사[4] - 자기 유도 방식 무선 충전을 통한 인증 우회 탐지[14]	N/A
HW	센서	- 비정상 값 - 무응답 및 간헐적 실패	- CNN을 활용한 항공 시스템 이상 탐지 모델[8] - GCN 기반 센서 데이터 이상 탐지[17]	0.93
	액추에이터	- 연결 이상 - 동작 이상	- LSTM 기반 비행 상태 오류 탐지[9] - LSTM VAE를 활용한 장치 이상 탐지[16]	0.98
	통신 모듈	- 신호 감쇠 - 패킷 누락	- MIL-STD-1553 버스에 대한 이상 탐지[11] - 셀룰러 IoT 시스템에 대한 이상 탐지[18]	0.99
	메모리/MCU	- 부팅 오류 - 펌웨어 무결성 손상	- TinyML 이산 시계열 이상 감지[10]	0.99

IV.결론

본 논문에서는 국방 분야에서 운용되는 CPS에 대한 주요 위협 요소와 이상행동 유형을 분류하고 이를 탐지하기 위한 다양한 기법들을 조사하였다. 조사했던 연구들은 단일 구성 요소에 대한 이상 행위의 탐지를 주로 진행하였는데, 이러한 탐지는 국지적인 위협만 판단할 수 있을뿐더러 다양한 위협이 있는 전장 환경에 효율적이지 못하다. 또 이를 해결하기 위해 탐지 로직이 더해진다고 하더라도 오버헤드가 증가한다는 단점이 생긴다. 따라서 효과적인 이상 행위 탐지를 위해, 경량화와 동시에 다중 구성 요소 간의 관계를 분석하고 이를 기반으로 이상 패턴을 식별할 수 있는 멀티모달 데이터 기반 탐지 기법에 관한 연구를 제안한다.

[참고문헌]

[1] D.Abshari and M.Sridhar, A Survey of Anomaly Detection in Cyber-Physical Systems, arXiv preprint arXiv:2502.13256, Feb, 2025.

[2] W.Duo, M.C.Zhou and A.Abusorrah, A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges, IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 5, pp. 784 - 800, May, 2022.

[3] H.S.Park, D.K.Shin and D.I.Shin, Research on Network Packet Analysis and Unknown Intrusion Detection Method based on LSTM-Autoencoder, Journal of Internet Computing & Services, Feb, 2025.

[4] H.W.LEE, D.W.Hong and K.H.Nam, A Method of Device Validation Using SVDD-Based Anormaly Detection Technology in SDP Environment, Journal of The Korea Institute of Information Security & Cryptology, vol. 31, no. 6, Dec, 2021.

[5] W.Hao, Z.Zhang, X.Wang, Q.Yang, B.Liu, W.Wang, T.Yang and P.Ye, Unsupervised Real-Time Communication Traffic Anomaly Detection for Multi-Dimensional Industrial Networks, IEEE TRANSACTIONS ON INDUSTRIAL CYBER-PHYSICAL SYSTEMS, vol. 3, 2025.

[6] K.B.Park, Y.S.Yoon, B.Duulga and K.B.Yim, Image-Based Machine Learning Model for Malware Detection on LLVM IR, Journal of The Korea

Institute of Information Security & Cryptology, vol. 34, no. 1, Feb, 2024.

[7] J.M.Choi and Y.J.Shin, Detection of TrustZone Rootkits Using ARM PMU Events, Journal of The Korea Institute of Information Security & Cryptology, vol. 33, no. 6, Dec, 2023.

[8] H.J.Im, T.R.Kim, J.G.Song and B.S.Kim, Anomaly Detections Model of Aviation System by CNN, Journal of Aerospace System Engineering, vol. 17, no. 4, pp. 67-74, 2023.

[9] K.Guo, N.Wang, D.T.Liu and X.Peng, Uncertainty-Aware LSTM Based Dynamic Flight Fault Detection for UAV Actuator, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, vol. 72, 2023.

[10] E.S.Pereira, L.S.Marcondes and M.Silva, On-Device Tiny Machine Learning for Anomaly Detection Based on the Extreme Values Theory, IEEE Micro, vol. 43, no. 6, pp. 58 - 65, Nov,/Dec, 2023, doi: 10.1109/MM.2023.3316918.

[11] E.Levy, N.Maman, A.Shabtai and Y.Elovici, AnoMili: Spoofing Prevention and Explainable Anomaly Detection for the 1553 Military Avionic Bus, arXiv preprint arXiv:2202.06870, Feb, 2022.

[12] J.P.G.de.Oliveira, C.J.A.Bastos-Filho and S.C.Oliveira, Non-invasive embedded system hardware/firmware anomaly detection based on the electric current signature, Advanced Engineering Informatics, vol. 51, pp. 101519, Apr, 2022.

[13] J.H.Choi, S.W.Lee and Y.G.Seo, Spoofing Attack Detection and Blocking Model Based on ARP Attack Signature Information, Journal of Digital Contents Society, vol. 23, no. 8, pp. 1485-1495, ISSN: 1598-2009 (Print) 2287-738X (Online), Aug, 2022.

[14] S.K.Ahn and K.W.Park, Analysis of Wireless Charging Technology And Security Solution Trend, Journal of the Korea Next Generation Computing Society, Aug, 2022.

[15] S.Kong, J.Ai, M.Lu and Y.Gong, GRAND: GAN-based software runtime anomaly detection method using trace information, vol. 169, pp. 365 - 377, 2024, doi: 10.1016/j.neunet, 2023.

[16] J.H.Seo, J.S.Park, J.W.Yoo and H.J.Park, Anomaly Detection System in Mechanical Facility Equipment: Using Long Short-Term Memory Variational Autoencoder, Journal of the Korean Society for Quality Management, vol. 49, no. 4, pp. 581 - 594, Dec, 2021, doi: 10.7469/JKSQM.2021.49.4.581.

[17] K.W.Lee, GCN-based multivariate time series anomaly detection method with sensor-specific time-lagged cross correlation, M.S. thesis, Dept. of Computer Engineering, Sogang Univ., Seoul, South Korea, Feb, 2023, [Online], Available: http://www.dcollection.net/handler/sogang/000000069875.

[18] B.Santos, I.Q.Khan, B.Dzogovic, B.Feng, V.T.Do, N.Jacot and T.V.Do, Anomaly Detection in Cellular IoT with Machine Learning, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 364, pp. 51 - 64, 2021.