Revue d'Intelligence Artificielle
Vol. 38, No. 1, February, 2024, pp. 277-284

Journal homepage: http://iieta.org/journals/ria

Securing Cyber Physical System Using Machine Learning: A Survey on Attack Resistant Algorithms

Pramod S. Aswale[1,3*], Dipak P. Patil[2], Omkar S. Vaidya[1]

[1] Sandip Institute of Technology and Research Center, Nashik 422213, Maharashtra, India
[2] Department of E&TC, Sandip Institute of Engineering and Management, Nashik 422213, Maharashtra, India
[3] Department of Computer Science and Engineering (Cyber Security and Data Science), G.H. Raisoni College of Engineering and Management, Pune 411011, Maharashtra, India

Corresponding Author Email: psaswale@gmail.com

https://doi.org/10.18280/ria.380129

Received: 10 October 2023
Revised: 29 November 2023
Accepted: 29 December 2023
Available online: 29 February 2024

Keywords:
cyber-physical systems, cyber-security threats, attacks and issues, cyber-physical vulnerabilities and challenges, security, privacy and forensics solutions, security and performance analysis

ABSTRACT

In order to protect Cyber-Physical Systems (CPS) against constantly changing cyberattacks, machine learning (ML) algorithms must be integrated. The goal of this survey is to investigate attack-resistant machine learning methods that improve CPS security. The limits of standard techniques are emphasized while discussing notable issues in CPS security. The survey thoroughly explores a range of machine learning methods, such as K-Nearest Neighbor (KNN), Support Vector Machines (SVM), and Deep Neural Networks (DNN), that are utilized in CPS for behavior analysis, anomaly identification, and intrusion detection. We discuss the importance of having solid training data and the difficulties in ML model adaptation to the dynamic nature of CPS situations. We examine the trade-offs between responsiveness and precision as well as the effects of false positives and false negatives on attack detection. This papers aims to provide a quick overview of the strengths, limitations, and future prospects of these algorithms, enabling stakeholders to formulate effective strategies for CPS security.

1. INTRODUCTION

Cyber-Physical Systems (CPS) are interconnected networks that smoothly merge the cyber and physical realms. These systems use cutting-edge technologies to monitor, evaluate, and regulate physical processes, allowing for more efficient interactions between the digital and physical worlds as depicted in Figure 1. In this paper we present a deep literature survey on machine learning algorithms to secure CPS. CPSs are distinguished by the incorporation of physical systems into the tangible world and control software within the virtual domain. The connection between these two domains is facilitated by networks responsible for seamless information exchange [1, 2]. Recent advances in communication technology have enabled real-time, low-latency interactions, allowing remote control of numerous physical systems and providing CPS users with a variety of intelligent services [3-5]. The incorporation of both wired and wireless networks within CPSs permits the monitoring of extensive industrial equipment states, thereby enabling the efficient organization and adaptable management of complex industrial systems [5-8]. As a result, CPS develops as a critical technology in a variety of industrial areas, including intelligent transportation systems [9-11], medical applications [12, 13], and smart grids [14, 15]. The communication-based train control (CBTC) system [6, 9], which uses communication technologies to connect trains and ground stops, is a famous example of CPS. In comparison to conventional railway control systems, this exchange involves transmitting train statuses and control signals through a real-time wireless network, which results in shorter dispatch intervals and increased safety [16].

The complexity and interconnectivity of Cyber-Physical Systems (CPS) are on the rise, leading to an expansion of potential attack vectors within these systems [17-19]. Among the vulnerable areas, the networks linking physical components and control software are particularly susceptible, making them attractive targets for external attackers seeking to disrupt CPS operations [20, 21]. Figure 2 shows the categorization of CPS attacks and Figure 3 represents attacks and threats on CPS.

When an attacker gains access to these networks, they can manipulate physical states to deceive attack detection systems [14, 15]. This access also enables them to assume control over physical system operations within the network, potentially causing shutdowns and interfering with the execution of critical control software in the cyberspace. These cyber-physical attacks carry substantial risks, including damage to industrial equipment, economic losses, and even human casualties. Because of their common integration into key infrastructure and daily life, Cyber-Physical Systems (CPS) security is critical. CPS seamlessly connects the physical and digital worlds, affecting industries such as energy, healthcare, transportation, and manufacturing. It is critical to ensure the security of these systems in order to protect against malicious cyber attacks that can disrupt critical services, risk data integrity, and pose substantial threats to public safety.

Notable incidents, such as the 2015 BlackEnergy malware incident that triggered a significant power plant malfunction in Ukraine, leading to a widespread power outage [20], and the 2014 cyber attack on a German steel mill, resulting in a loss of control over plant equipment and substantial damage to blast furnaces [20], underscore the growing urgency of cyber-physical security research. Such research is crucial to safeguarding the reliability of Cyber-Physical Systems (CPS) in the face of evolving adversarial threats [17, 21].

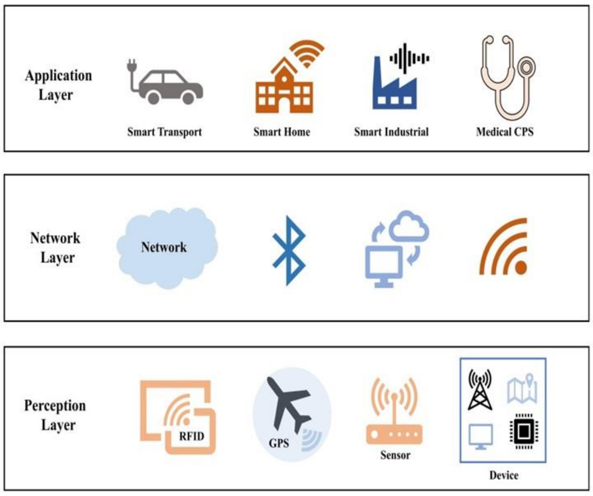

Figure 1. CPS layer structure

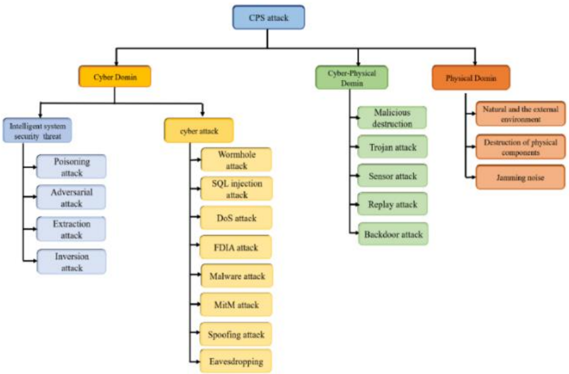

Figure 2. CPS attack categorization

In the study [22], various machine learning algorithms, including K-Nearest Neighbour (KNN), Support Vector Machines (SVM), and Deep Neural Networks (DNN), are explored for their application in enhancing artificial intelligence (AI) and safeguarding Cyber-Physical Systems (CPS) against Denial-of-Service (DoS) attacks. The work by Chen et al. [23] delves into code mutation techniques, aiming to understand and adapt to diverse CPS variants. The research conducted by Settanni et al. [24] suggests the potential for automated Machine Learning (ML) approaches within CPS, enabling the implementation of self-adaptive mechanisms to effectively handle anomalies.

The investigations outlined in the studies [25-28] have extensively addressed various aspects of Cyber-Physical Systems (CPS), with a specific emphasis on harnessing machine learning techniques to bolster the system's capacity for cyberattack intelligence and mitigation.

Given the intricate nature of contemporary Cyber-Physical Systems (CPS), the imperative to ensure both security and safety within these systems remains paramount. The potential threats manifest in the cyber, physical, or hybrid dimensions of CPS, necessitating a multifaceted method for the identification and mitigation of vulnerabilities in terms of security and safety. In the current study, our objective was to provide a comprehensive understanding of vulnerabilities, attack typologies, and mitigation strategies, considering the intricate attributes of CPS including scalability, distribution, component diversity, and the nuanced differentiation between security and safety challenges. A particular emphasis was placed on Intrusion Detection Systems that leverage Machine Learning algorithms for the purpose of detecting and mitigating threats. Extensive literature review was conducted to explore the range of algorithms employed, the specific threats they were applied to, the datasets used, and the targeted objects of investigation. Furthermore, recognizing that the majority of CPS function as open-loop systems, engaging in continuous collaboration with other systems, we also address the associated problems, challenges, and issues that emerge within this context.

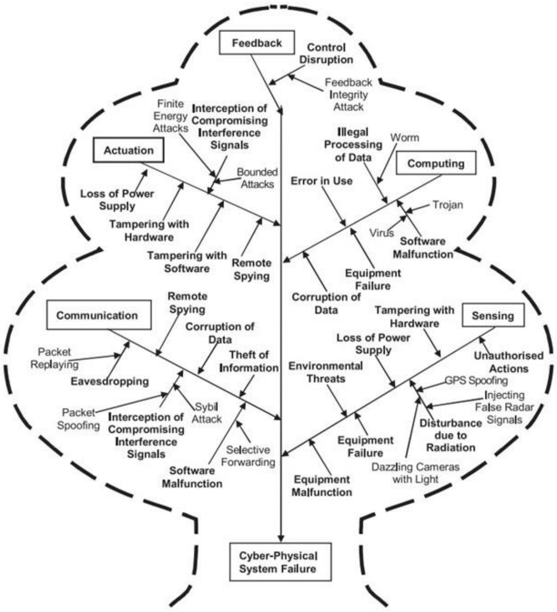

Figure 3. A tree diagram representing attacks and threats on cyber-physical systems (CPS) [29]

Section II of the study examines state-of-the-art systems and provides a complete literature survey. We also give a comparative analysis of the system in terms of several metrics. Section III discusses research gaps, and Section IV concludes the work by discussing future directions.

2. LITERATURE SURVEY

In spite of their advantageous attributes, Cyber-Physical Systems (CPSs) exhibit heightened susceptibility to cyber intrusions owing to their reliance on digital resources, particularly within the realm of networking protocols. Consequently, CPSs face an elevated spectrum of potential attack vectors targeting their physical and cyber domains, as well as the interconnections bridging these domains. Consequently, assaults directed at these systems are classified as cyber-physical (cp) attacks [30].

The comprehensive exploration of the repercussions stemming from attacks on CPSs is exhaustively addressed in references [30-34]. Within this segment, a thorough examination of current methodologies pertinent to our specific case study is presented.

2.1 Machine learning applications in CPS security

Lv et al. [35] explored the application of Artificial Intelligence (AI) to enhance the security of Cyber-Physical Systems (CPS). They chose a "CPS-based indoor environment measurement and control system for intelligent buildings" as their case study. Their objective involved creating a multi-agent system composed of various components including detection, control, execution, and communication. Back-Propagation Neural Network (BPNN) was employed for tasks related to classification and regression.

The system's performance was evaluated using several key performance metrics, including Mean Absolute Error (MAE), Normalized Root Mean Square Error (NRMSE), and Peak Signal-to-Noise Ratio (PSNR). The results illustrated superior performance with minimal false positives.

Tantawy et al. [36] used a model-based approach to develop an integrated strategy for increasing CPS security. For their security analysis, they used a Continuous Stirred Tank Reactor (CSTR) in an industrial environment and integrated it with the cyber domain. Their CPS test bed included both corporate and control networks, as well as data sharing, for machine learning-based cyberattack monitoring. The proposed system encompassed the plant, control logic, monitoring system, corporate analysis, and safety logic. To enhance cyberattack detection, a hybrid automaton was designed, and an efficient tree-based approach was employed for optimal data management and attack detection.

Salahdine and Kaabouch [37] investigated cybersecurity challenges, vulnerabilities, and countermeasures in Cognitive Radio Networks (CRN) physical layer. Their primary emphasis was directed towards addressing physical layer attacks that encompassed dynamic spectrum access, belief manipulation, eavesdropping, and malicious traffic injection. They explored an array of detection techniques, including compressive sensing, learning-based methods, Intrusion Detection System (IDS) models, feature-based methods, data-assisted approaches, localization-based strategies, belief propagation, and spectrum sensing techniques.The focus was on PU (Primary User) emulation attacks, which were classified as cryptography-based, fingerprint-based, game theory-based, and hybrid approaches.

Sargolzaei et al. [38] investigated the utility of machine learning for fault detection in the context of vehicular CPS. Their focus was on False Data Injection (FDI) assaults, which might cause accidents in vehicle networks. A approach for detecting FDI attacks and taking corrective actions to ensure accurate signal creation was proposed. This assists the driver or controller in keeping a safe distance from vehicles ahead. For fault identification, the proposed method used a neural network-based methodology.

Goh et al. [39] employed deep learning and LSTM-RNN to create systems designed for the identification of abnormal behavior through an unsupervised learning method. Their research specifically targeted two categories of time synchronization attacks that exploit GPS to disrupt Cyber-Physical Systems (CPS): Time Synchronization (TS) attacks and Stealth Time Synchronization (STS) attacks.

A suggestion for a Machine Learning (ML)-dependent approach to detect threats in Cyber-Physical Systems (CPS) security was made in Yan et al. [40]. The effectiveness of this strategy was due to a thorough feature creation process that used statistical methods, physical domain knowledge, and Deep Learning (DL) techniques. These elements were created to more correctly portray the physical system's complicated non-linear and spatio-temporal interactions. Furthermore, combining these generated features with the new deployment of an Extreme Learning Machine (ELM) for the detection model resulted in excellent accuracy and early detection of hostile attacks within CPS.

In the study [41], a behavior-based Machine Learning (ML) technique was developed to detect intrusions within Cyber-Physical Systems (CPS), with a specific focus on intrusion detection within the SWaT (Secure Water Treatment) testbed.

Macas and Chunming [42] emphasized the critical importance of automated attack detection and intelligent response within complex CPS environments. Given the heterogeneous nature of networked CPS and the time series data generated by diverse sensors, conventional statistical process control methods like Cumulative Sum (CUSUM) and Exponentially Weighted Moving Average (EWMA) were deemed insufficient. Supervised ML approaches faced challenges due to a scarcity of labeled data, while unsupervised techniques, including clustering and temporal prediction, struggled to capture temporal dependencies among disparate time series data—especially considering the noise inherent in multivariate time series data originating from operational CPS activities.

As a solution, an approach based on statistical correlation analysis between multivariate time series data and unsupervised Deep Learning (DL) algorithms was proposed for the detection of adversarial actions in complex multi-process CPS. This approach utilized Convolutional Neural Network autoencoders (CNN-AE) and Convolutional Long Short-Term Memory Encoder-Decoder (ConvLSTM-ED) models. The effectiveness of this method was demonstrated through simulations on the SWaT testbed, including comparisons with state-of-the-art baseline techniques.

2.2 Deep learning for threat identification

In contrast, Wang et al. [43] delved into the utilization of machine learning techniques for preempting such attacks. They introduced a detection model based on Artificial Neural Networks (ANN) that exhibited strong performance in detecting various attack types.

They have devised a Machine Learning classifier designed to identify temporal synchronization threats within Cyber-Physical Systems (CPS). Employing the "first aware" methodology, this classifier demonstrated its capability to detect various types of time synchronization attempts, including both direct and stealthy ones.

On a related note, Shin et al. [44] introduced a Deep Learning (DL)-based approach for detecting adversarial attacks on sensors integrated into autonomous vehicles. Their study delved into the performance of sensors like inertial measurement units and wheel encoders when exposed to uncertain and non-linear scenarios. Furthermore, Ghafouri et al. [45] used supervised regression to detect aberrant sensor data in CPS. An approach was introduced to determine an approximate optimal threshold for the defender. This was achieved by modeling the interaction between defenders and attackers within Cyber-Physical Systems (CPS) as a Stackelberg game. In this game, defenders adapt their detection thresholds in response to adversarial attacks. The analysis demonstrated that it is possible to enhance robustness without compromising accuracy in CPS security.

2.3 Advance techniques in CPS security

Kholidy [46] introduced a security framework designed for autonomous mitigation of cyberattacks targeting Cyber-Physical Systems (CPS). This framework amalgamates conventional Intrusion Detection Systems (IDS) like SNORT with machine learning-based methods to enhance overall security. It takes into account established security methodologies and risk assessment models to materialize the new concept of the Autonomous Response Controller (ARC) framework. The proposed model integrates a probabilistic risk assessment technique to evaluate potential risks and make well-considered decisions.

Given the crucial nature of CPS, dependability and security are critical. Dependability includes availability, dependability, safety, integrity, and maintainability, whereas security includes the CIA triad of confidentiality, integrity, and availability. Because CPS is widespread, varied, and complicated, operating conditions may vary. As a result, the term "resilience" is used to define a system's ability to continue providing services even in the face of adverse conditions or failures. Resilience also refers to a system's ability to remain reliable in the face of changing circumstances [47]. Barbeau et al. [48] proposed a vision for next-generation CPS, emphasizing the need of resilience. Recognizing the potential for increased hostile activities to disrupt systems, the authors proposed utilizing fuzzy decisions and ML methods to assure operational efficiency in such scenarios. Nonetheless, in order to design robust systems, potential security-threatening flaws must be properly analyzed, and strategies for detecting and mitigating such threats must be thoroughly investigated.

In the study [49], a novel probabilistically timed dynamic model is introduced to assess physical security attack scenarios on critical infrastructures (CIs). The model simulates attacks on vulnerabilities within the targeted CIs. Specifically, it models the time it would take for an attacker to successfully breach physical barriers, intrusion detection systems, and backup safety measures. This time is represented as a random variable, and its probability distribution is customizable by the user. The model operates under the assumption of a highly skilled attacker, evaluates the likelihood of mission success even in the presence of erroneous information, and documents the cumulative time taken by the attacker to compromise the targeted assets, comparing it to a predefined mission time.

According to Martins et al. [50], an effective technique for reaching this goal is to detect potential hazards systematically during the design process of constructing such systems, which is commonly performed using threat modeling. A tool for doing systematic threat modeling analysis for CPS is presented in this context. A practical wireless train temperature monitoring system serves as a real-world case study to corroborate the suggested approach. Subsequently, the identified vulnerabilities within the system are addressed in alignment with the guidelines outlined in the National Institute of Standards and Technology (NIST) SP 800-82.

Mavani and Asawa [51] proposed a model to assess the feasibility of executing an IPv6 spoofing attack within the 6LoWPAN network. This investigation has revealed two novel attack avenues, both of which establish a false association between an incorrect IPv6 address and a node's MAC address. These pathways leverage spoofed RPL and 6LoWPAN-ND packets to execute the IPv6 spoofing attack within an unsecured wireless environment. The likelihood of the attack's success is evaluated by considering environmental factors affecting signal reception in the radio propagation environment.

Mitchell and Chen [52] constructed an analytical model for cyber physical systems based on stochastic Petri nets to depict the interaction between adversary behavior and protection. They investigate many sorts of failures that can occur in a cyber physical system, including attrition, pervasion, and exfiltration failure. They show the parameterization process using a modernized electrical grid as an example. Our findings lead to optimal design conditions, such as the intrusion detection interval and redundancy level, that increase the modernized electrical grid's mean time to failure.

Genge et al. [53] propose communication and control logic implementation factors that impact the outcome of NICS attacks that could be used as successful strategies to increase industrial installation resilience in this study. The primary purpose of this project is to begin an investigation of cyber-physical impacts in specific settings. This is the first study of its sort to look into cyber-physical systems, and it reveals how the cyber domain affects the physical sphere.

Innovative countermeasures were devised to support the constancy of Kalman filtering against fake data injection assaults, as detailed in the study [54]. These countermeasures have been tested and implemented across IEEE 14-bus, 30-bus, and 118-bus systems. The (UKF) technique proved to be the most effective solution, particularly in minimizing the influence of random benign noise and guarding against attacks. It is worth mentioning that the suggested temporal-based recognition method identifies compromised meters with high accuracy and speed, which is consistent with the authors' findings.

The growing integration of Internet of Things (IoT) and the imminent rise of Internet of Autonomous Vehicles have spurred continuous developments in Vehicular ad hoc networks (VANETs). In this evolving landscape, the potential for malicious actors to compromise vehicles and co-opt them into a network of zombie vehicles, awaiting commands from a central control server, has garnered substantial attention. Addressing this concern, Sakiz and Sen [55] presents a comprehensive examination of intrusion and misbehavior detection approaches. The discourse extends to proactive \& reactive solutions that can be deployed as countermeasures to thwart such attacks.

2.4 Machine learning models and detection techniques

The evolution of an attack occurs only when the network operator is mislead, leading in data compromise. In order to address this scenario, powerful countermeasures against arbitrary undetectable assaults are presented, which take advantage of the intrinsic security of Phasor Measurement Units (PMUs) with known integrity [56].

In the study [57], a comprehensive examination of replay attacks aiming Cyber-Physical Systems (CPS) was undertaken, accompanied by a rigorous analysis of their impact on control system functionality. The research explores the intricate interplay between performance degradation, detection rates, and the strength of authentication signals. Furthermore, the paper introduces a methodology for optimizing noisy authentication signals, striking a delicate balance between achieving desired detection efficiency and tolerating permissible losses in control system performance. An intriguing proposal within the study suggests the sporadic introduction of authentication signals into the system at random intervals, thereby mitigating their impact on system performance over time.

Yoo and Shon [58] engage in a comprehensive discourse centered on the vulnerabilities inherent in Cyber-Physical Systems (CPS), laying out stringent security requirements to safeguard these systems. The authors also delve into the intricacies of CPS architecture and present a suite of countermeasures designed to fortify the ecosystem. Notably, the research implements a security architecture proposed for the IEC 61850-to-DNP3 conversion environment model, as recommended by IEC 61850 80-2/IEEE 1815.1, and subsequently verifies its efficacy.

Yampolskiy et al. [59] presents a novel descriptive language optimized for characterizing probable CPS assaults and their related repercussions in the quest of improving CPS cybersecurity. This language's capacity to specify and delineate elements that thoroughly incorporate attacks and defenses is a distinguishing feature. Despite the fact that these characteristics are not explicitly addressed in the security assessment process, the authors believe that the suggested attack description language can be an asset to analyze CPS's overall security posture.

Abosuliman [60] apply a Machine Learning (ML) approach for detecting network anomalies and building data-driven models to detect DDoS assaults on Industry 4.0 CPSs. Existing approach flaws, such as artificial data and tiny datasets, are addressed by collecting network traffic data from a real-world semiconductor manufacturing company. Lydia et al. [61] provide an in-depth examination of the numerous security scenarios in CPS, the assaults, the various methodologies for simulating different attacks, and the necessity for CPS testbeds. The enormous research challenges addressed in terms of ethical considerations, as well as the use of cutting-edge approaches such as big data and machine learning in CPS protection, have been suggested.

Table 1. Comparative analysis of state of art systems

Ref	Technique	Advantages	Limitations	Datasets
[35]	[1] (BPNN) in a (MAS)	high level of CPS security effectiveness and sturdiness	Needs further research to improve the system.	Data from construction industry.
[36]	Hybrid automaton based approach.	Security, effectiveness cost-	There is a desire for further integration of a model-based approach into Machine Learning (ML).	Data of CSTR testbed
[37]	Survey on countermeasures for physical layer attacks on CRNs	Insights on many types of attacks.	There is no empirical method.	-
[38]	Neural network based fault detection system	Improved reliability, safety and robustness of CPS	The scope of the research is confined to the domain of fault detection.	Vehicular CPS dataset
[39]	(LSTM-RNN)	Low false positives.	The selection of features must be improved.	SWAT Dataset
[46]	ARC framework.	Capable of mitigating attacks such as Aurora.	Consideration is Given to limited data.	Industrial cyber-attack dataset
[62]	Anomaly detection, KNN & random forest	The selection of features must be improved.	There is a growing need for a novel se curity framework in this context.	Data of cyber manufacturing system
[63]	EPIC	EPIC testbed enables security research.	Limited to domain specific attacks.	Electric Power CPS dataset

3. DISCUSSIONS

After conducting a thorough literature review, we examined cutting-edge technologies aimed at protecting Cyber-Physical technologies (CPS) against cyber attacks. The results of our review as per Table 1 highlighted significant research gaps that require further investigation. Notably, centralized frameworks are a prominent emphasis in the existing literature on attack detection techniques. However, given the increasing popularity of distributed control systems due to their lower computing complexity and efficient use of network resources, there is a clear research void in researching attack detection approaches specialized to distributed systems. Targeting many sensors or communication lines at once is a real hazard in real-world circumstances, especially in installations with a large number of sensors. In spite of this fact, a large number of currently in use attack detection systems follow the single-attack premise, which limits their usefulness. Given the significance of multiattack detection techniques in engineering, it is clear that there are obstacles facing this field's present development. The widespread emphasis on single-type attack detection techniques might not work against a variety of threats. Replay attacks, for example, may be too much for a well-engineered system meant to detect Denial of Service (DoS) attacks. As a result, it becomes necessary to solve this constraint, which calls for the creation of algorithms that can efficiently mitigate a variety of cyber risks.

The research gaps that have been revealed emphasize how urgently an intelligent and robust algorithm utilizing machine learning must be developed in order to improve CPS's information security. The development of an algorithm aimed at improving the precision of cyber attack identification would constitute a noteworthy advancement in strengthening Cyber-Physical Systems' defenses against a constantly changing array of cyber threats.

4. CONCLUSIONS

In summary, by undertaking a detailed evaluation of vulnerabilities, attack typologies, and mitigation measures, our research profoundly alters the landscape of Cyber-Physical Systems (CPS) security. This contribution goes beyond theoretical frameworks, providing practical insights into the complex interplay between the cyber and physical elements inside CPSs. Our work adds significant practical significance to the field of CPS security by empirically exploring weaknesses and analyzing various attack scenarios, uncovering critical details.

A significant part of our contribution is the emphasis on Intrusion Detection Systems (IDS) that use Machine Learning methods. Our findings highlight the efficiency of IDS in both detecting and mitigating threats as we navigate the complexities of open-loop CPSs and their ongoing collaboration with other systems. This emphasis strengthens the defense mechanisms built into CPSs. Furthermore, the comparative analysis offered in Section II serves as a baseline for future developments, while the study of research gaps in Section III provides options for enhancing CPS security techniques. Overall, our research represents a watershed moment in the understanding of CPS security, providing useful insights for researchers, practitioners, and policymakers. Its influence resonates in driving the development of robust security measures, bolstering the resilience of Cyber-Physical Systems against ever-evolving adversarial threats.

REFERENCES

[1] Park, K.J., Zheng, R., Liu, X. (2012). Cyber-physical systems: Milestones and research challenges. Computer Communications, 36(1): 1-7. https://doi.org/10.1016/j.comcom.2012.09.006

[2] Kim, D., Won, Y., Kim, S., Eun, Y., Park, K.J., Johansson, K.H. (2019). Sampling rate optimization for IEEE 802.11 wireless control systems. In Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems, pp. 87-96. https://doi.org/10.1145/3302509.3311045

[3] Rajkumar, R., Lee, I., Sha, L., Stankovic, J. (2010). Cyber-physical systems: the next computing revolution. In Proceedings of the 47th design automation conference, pp. 731-736. https://doi.org/10.1145/1837274.1837461

[4] Kim, K.D., Kumar, P.R. (2012). Cyber–physical systems: A perspective at the centennial. In Proceedings of the IEEE, 100(Special Centennial Issue), pp. 1287-1308. https://doi.org/10.1109/JPROC.2012.2189792

[5] Ahlén, A., Akerberg, J., Eriksson, M., Isaksson, A.J., Iwaki, T., Johansson, K.H., and Sandberg, H. (2019). Toward wireless control in industrial process automation: A case study at a paper mill. IEEE Control Systems Magazine, 39(5): 36-57. https://doi.org/10.1109/MCS.2019.2925226

[6] Wang, X., Liu, L., Tang, T., Sun, W. (2018). Enhancing communication-based train control systems through train-to-train communications. IEEE Transactions on Intelligent Transportation Systems, 20(4): 1544-1561. https://doi.org/10.1109/TITS.2018.2856635

[7] Mozaffari, M., Saad, W., Bennis, M., Nam, Y.H., Debbah, M. (2019). A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. IEEE Communications Surveys & Tutorials, 21(3): 2334-2360. https://doi.org/10.1109/COMST.2019.2902862

[8] Lakew, D.S., Sa'ad, U., Dao, N.N., Na, W., Cho, S. (2020). Routing in flying ad hoc networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(2): 1071-1120. https://doi.org/10.1109/COMST.2020.2982452

[9] Farooq, J., Soler, J. (2017). Radio communication for communications-based train control (CBTC): A tutorial and survey. IEEE Communications Surveys & Tutorials, 19(3): 1377-1402. https://doi.org/10.1109/COMST.2017.2661384

[10] Cho, B.M., Jang, M.S., Park, K.J. (2020). Channel-aware congestion control in vehicular cyber-physical systems. IEEE Access, 8: 73193-73203. https://doi.org/10.1109/ACCESS.2020.2987416

[11] Paranjothi, A., Khan, M.S., Zeadally, S. (2020). A survey on congestion detection and control in connected vehicles. Ad Hoc Networks, 108: 102277. https://doi.org/10.1016/j.adhoc.2020.102277

[12] Meng, W., Li, W., Wang, Y., Au, M.H. (2020). Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. Future Generation Computer Systems, 108: 1258-1266. https://doi.org/10.1016/j.future.2018.06.007

[13] Cho, B.M., Park, K.J., Park, E.C. (2016). Fairness-aware radio resource management for medical interoperability between WBAN and WLAN. Annals of Telecommunications, 71(9-10): 441-451. https://doi.org/10.1007/s12243-016-0499-6

[14] Manandhar, K., Cao, X., Hu, F., Liu, Y. (2014). Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Transactions on Control of Network Systems, 1(4): 370-379. https://doi.org/10.1109/TCNS.2014.2357531

[15] Rawat, D.B., Bajracharya, C. (2015). Detection of false data injection attacks in smart grid communication systems. IEEE Signal Processing Letters, 22(10): 1652-1656. https://doi.org/10.1109/LSP.2015.2421935

[16] Kim, S., Won, Y., Park, I. H., Eun, Y., Park, K.J. (2019). Cyber-physical vulnerability analysis of communication-based train control. IEEE Internet of Things Journal, 6(4): 6353-6362. https://doi.org/10.1109/JIOT.2019.2919066

[17] Koutsoukos, X. (2020). Systems science of secure and resilient cyberphysical systems. Computer, 53(3): 57-61. https://doi.org/10.1109/MC.2020.2966109

[18] Teixeira, A., Pérez, D., Sandberg, H., Johansson, K.H. (2012). Attack models and scenarios for networked control systems. In Proceedings of the 1st international conference on High Confidence Networked Systems, pp. 55-64. https://doi.org/10.1145/2185505.2185515

[19] Khalid, F., Rehman, S., Shafique, M. (2020). Overview of security for smart cyber-physical systems. Security of Cyber-Physical Systems: Vulnerability and Impact, 5-24. https://doi.org/10.1007/978-3-030-45541-5_2

[20] Alladi, T., Chamola, V., Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. Computer Communications, 155: 1-8. https://doi.org/10.1016/j.comcom.2020.03.007

[21] Dibaji, S.M., Pirani, M., Flamholz, D.B., Annaswamy, A.M., Johansson, K.H., Chakrabortty, A. (2019). A systems and control perspective of CPS security. Annual Reviews in Control, 47: 394-411. https://doi.org/10.1016/j.arcontrol.2019.04.011

[22] Wang, T., Liang, Y., Yang, Y., Xu, G., Peng, H., Liu, A., Jia, W. (2020). An intelligent edge-computing-based method to counter coupling problems in cyber-physical systems. IEEE Network, 34(3): 16-22. https://doi.org/10.1109/MNET.011.1900251

[23] Chen, Y., Poskitt, C.M., Sun, J. (2018, May). Learning from mutants: Using code mutation to learn and monitor invariants of a cyber-physical system. In 2018 IEEE

Symposium on Security and Privacy (SP), pp. 648-660. https://doi.org/10.1109/SP.2018.00016

[24] Settanni, G., Skopik, F., Karaj, A., Wurzenberger, M., Fiedler, R. (2018). Protecting cyber physical production systems using anomaly detection to enable self-adaptation. In 2018 IEEE Industrial Cyber-Physical Systems (ICPS), pp. 173-180. https://doi.org/10.1109/ICPHYS.2018.8387655

[25] Hehenberger, P., Vogel-Heuser, B., Bradley, D., Eynard, B., Tomiyama, T., Achiche, S. (2016). Design, modelling, simulation and integration of cyber physical systems: Methods and applications. Computers in Industry, 82: 273-289. https://doi.org/10.1016/j.compind.2016.05.006

[26] Lee, J., Jin, C., Bagheri, B. (2017). Cyber physical systems for predictive production systems. Production Engineering, 11(2): 155-165. https://doi.org/10.1007/s11740-017-0729-4

[27] Farivar, F., Haghighi, M. S., Jolfaei, A., Alazab, M. (2019). Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. IEEE Transactions on Industrial Informatics, 16(4): 2716-2725. https://doi.org/10.1109/TII.2019.2956474

[28] Xu, H., Yu, W., Griffith, D., Golmie, N. (2018). A survey on industrial Internet of Things: A cyber-physical systems perspective. IEEE access, 6: 78238-78259. https://doi.org/10.1109/ACCESS.2018.2884906

[29] Alguliyev, R., Imamverdiyev, Y., Sukhostat, L. (2018). Cyber-physical systems and their security issues. Computers in Industry, 100: 212-223. https://doi.org/10.1016/j.compind.2018.04.017

[30] Sridhar, S., Hahn, A., Govindarasu, M. (2011). Cyber–physical system security for the electric power grid. Proceedings of the IEEE, 100(1): 210-224. https://doi.org/10.1109/JPROC.2011.2165269

[31] Pang, Z.H., Liu, G.P. (2011). Design and implementation of secure networked predictive control systems under deception attacks. IEEE Transactions on Control Systems Technology, 20(5): 1334-1342. https://doi.org/10.1109/TCST.2011.2160543

[32] Li, J., Liu, X., Su, X. (2018). Sliding mode observer-based load frequency control of multi-area power systems under delayed inputs attack. In 2018 Chinese Control and Decision Conference (CCDC), pp. 3716-3720. https://doi.org/10.1109/CCDC.2018.8407768

[33] Ding, D., Han, Q.L., Xiang, Y., Ge, X., Zhang, X.M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 275: 1674-1683. https://doi.org/10.1016/j.neucom.2017.10.009

[34] Ji, P., Ye, J., Mu, Y., Lin, W., Tian, Y., Hens, C., Perc, M., Tang, Y., Sun, J., Kurths, J. (2023). Signal propagation in complex networks. Physics Reports, 1017: 1–96. https://doi.org/10.1016/j.physrep.2023.03.005

[35] Lv, Z., Chen, D., Lou, R., Alazab, A. (2021). Artificial intelligence for securing industrial-based cyber–physical systems. Future Generation Computer Systems, 117: 291-298. https://doi.org/10.1016/j.future.2020.12.001

[36] Tantawy, A., Abdelwahed, S., Erradi, A., Shaban, K. (2020). Model-based risk assessment for cyber physical systems security. Computers & Security, 96: 101864. https://doi.org/10.1016/j.cose.2020.101864

[37] Salahdine, F., Kaabouch, N. (2020). Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey. Physical Communication, 39: 101001. https://doi.org/10.1016/j.phycom.2020.101001

[38] Sargolzaei, A., Crane, C.D., Abbaspour, A., Noei, S. (2016). A machine learning approach for fault detection in vehicular cyber-physical systems. In 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 636-640. https://doi.org/10.1109/ICMLA.2016.0112

[39] Goh, J., Adepu, S., Tan, M., Lee, Z.S. (2017). Anomaly detection in cyber physical systems using recurrent neural networks. In 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 140-145. https://doi.org/10.1109/HASE.2017.36

[40] Yan, W., Mestha, L.K., Abbaszadeh, M. (2019). Attack detection for securing cyber physical systems. IEEE Internet of Things Journal, 6(5): 8471-8481. https://doi.org/10.1109/JIOT.2019.2919635

[41] Junejo, K.N., Goh, J. (2016). Behaviour-based attack detection and classification in cyber physical systems using machine learning. In Proceedings of the 2nd ACM international workshop on cyber-physical system security, pp. 34-43. https://doi.org/10.1145/2899015.2899016

[42] Macas, M., Chunming, W. (2019). Enhanced cyber-physical security through deep learning techniques. In Proc. CPS Summer School Ph. D. Workshop, pp. 72-83

[43] Wang, J., Tu, W., Hui, L.C., Yiu, S.M., Wang, E.K. (2017). Detecting time synchronization attacks in cyber-physical systems with machine learning techniques. In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 2246-2251. https://doi.org/10.1109/ICDCS.2017.25

[44] Shin, J., Baek, Y., Eun, Y., Son, S.H. (2017). Intelligent sensor attack detection and identification for automotive cyber-physical systems. In 2017 IEEE Symposium series on computational intelligence (SSCI), pp. 1-8. https://doi.org/10.1109/SSCI.2017.8280915

[45] Ghafouri, A., Vorobeychik, Y., Koutsoukos, X. (2018). Adversarial regression for detecting attacks in cyber-physical systems. arXiv preprint arXiv:1804.11022. https://arxiv.org/abs/1804.11022

[46] Kholidy, H.A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. Future Generation Computer Systems, 115: 171-187. https://doi.org/10.1016/j.future.2020.09.002

[47] Laprie, J.C. (2008). From dependability to resilience. In 38th IEEE/IFIP Int. Conf. On dependable systems and networks, pp. G8-G9.

[48] Barbeau, M., Carle, G., Garcia-Alfaro, J., Torra, V. (2019). Next generation resilient cyber-physical systems. arXiv preprint arXiv:1907.08849. https://arxiv.org/abs/1907.08849

[49] Khalil, Y.F. (2016). A novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures. Process Safety and Environmental Protection, 102: 473-484. https://doi.org/10.1016/j.psep.2016.05.001

[50] Martins, G., Bhatia, S., Koutsoukos, X., Stouffer, K., Tang, C., Candell, R. (2015). Towards a systematic threat modeling approach for cyber-physical systems. In 2015 Resilience Week (RWS), pp. 1-6. https://doi.org/10.1109/RWEEK.2015.7287428

[51] Mavani, M., Asawa, K. (2017). Modeling and analyses of IP spoofing attack in 6LoWPAN network. Computers & Security, 70: 95-110. https://doi.org/10.1016/j.cose.2017.05.004

[52] Mitchell, R., Chen, R. (2015). Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems. IEEE Transactions on Reliability, 65(1): 350-358. https://doi.org/10.1109/TR.2015.2406860

[53] Genge, B., Siaterlis, C., Hohenadel, M. (2012). Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems. International Journal of Computers Communications & Control, 7(4): 674-687.

[54] Yang, Q., Chang, L., Yu, W. (2016). On false data injection attacks against Kalman filtering in power system dynamic state estimation. Security and Communication Networks, 9(9): 833-849. https://doi.org/10.1002/sec.835

[55] Sakiz, F., Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks, 61: 33-50. https://doi.org/10.1016/j.adhoc.2017.03.006

[56] Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., Poolla, K. (2013). Smart grid data integrity attacks. IEEE Transactions on Smart Grid, 4(3): 1244-1253. https://doi.org/10.1109/TSG.2013.2245155

[57] Mo, Y., Chabukswar, R., Sinopoli, B. (2013). Detecting integrity attacks on SCADA systems. IEEE Transactions on Control Systems Technology, 22(4): 1396-1407. https://doi.org/10.1109/TCST.2013.2280899

[58] Yoo, H., Shon, T. (2016). Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. Future Generation Computer Systems, 61: 128-136. https://doi.org/10.1016/j.future.2015.09.026

[59] Yampolskiy, M., Horváth, P., Koutsoukos, X.D., Xue, Y., Sztipanovits, J. (2015). A language for describing attacks on cyber-physical systems. International Journal of Critical Infrastructure Protection, 8: 40-52. https://doi.org/10.1016/j.ijcip.2014.09.003

[60] Abosuliman, S.S. (2023). Deep learning techniques for securing cyber-physical systems in supply chain 4.0. Computers and Electrical Engineering, 107: 108637. https://doi.org/10.1016/j.compeleceng.2023.108637

[61] Lydia, M., Prem Kumar, G.E., Selvakumar, A.I. (2023). Securing the cyber-physical system: A review. Cyber-Physical Systems, 9(3): 193-223. https://doi.org/10.1080/23335777.2022.2104378

[62] Wu, M., Song, Z., Moon, Y.B. (2019). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. Journal of Intelligent Manufacturing, 30: 1111-1123. https://doi.org/10.1007/s10845-017-1315-5

[63] Adepu, S., Kandasamy, N.K., Mathur, A. (2019). Epic: An electric power testbed for research and training in cyber physical systems security. In Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2, pp. 37-52. https://doi.org/10.1007/978-3-030-12786-2_3