An analysis on Proficiency in Securing Cyber Physical Systems and current research directions

Preeti Prasada[1*], Dr. Srinivas Prasad[2]

[1a]Research Scholar, Dept of CSE GITAM School of Technology, GITAM (Deemed to be University), Vishakhapatnam
[1b]Senior Assistant Professor, CSE-AIML, Geethanjali College of Engineering and Technology, Hyderabad
*preeti.preetu11@gmail.com

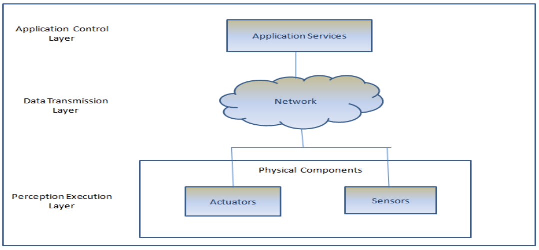
[2]Professor, Dept of CSE GITAM School of Technology, GITAM (Deemed to be University), Vishakhapatnam
sprasad@gitam.edu

Abstract. Cyber Physical Systems are the talk of the trending globe today, also the security of CPSs in equally important. While CPS has become a part of our life; in form of a health monitoring implant, home automation or a self-driving car, and the advancing adversary attacks that could affect lives by attacking CPSs bother the user of CPSs. There are numerous different stealthy attacks that have been undertaken against CPSs, and there are also many different security measures available. Future research has a lot of potential in creating security systems that can fend off sneaky attacks using tools like block chains and deep learning.

Keywords: Cyber Physical Systems (CPSs), block chain, deep learning

1. Introduction

Internet today has led to many achievements and developments; due to this advancement we have witnessed a tremendous growth in the field of technology as well. According to ITU, web penetration is directly corelated to the employment of a common man and economic growth rates of a nation [2]. The extension of the Internet of Things has been a recent development in today's world, leading to systems such as the Internet of Vehicles, Industrial Internet of Things, and Consumer Internet of Things, among others. These systems are commonly referred to as CPSs (Cyber Physical Systems), and they are used in a variety of industrial forms and fields, just as manufacturing, power systems, military warfare, health care, education, home automation, and agriculture. In other words, CPS integrates, monitors, and manages a system's activities while reducing the need for human interaction through automation of the processes [16]. NASA made the proposal for CPS in 1992. The CPS can be separated into three strata; the execution layer, the data transmission layer, and the application control layer [3] [4], as shown in figure-1 and 2.



K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_125

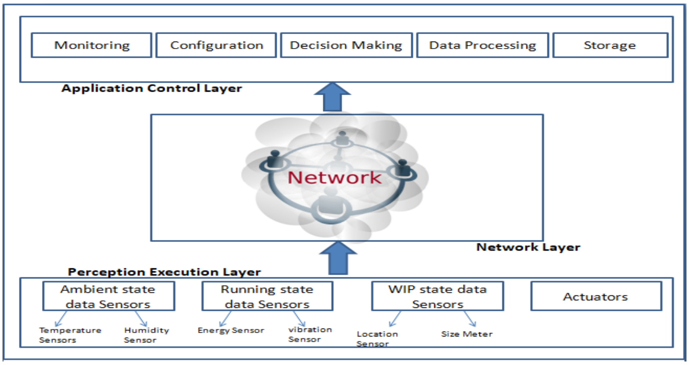


Figure-2 Elaboration of Layers in CPS

All physical parts, including sensors that recognize environmental changes or events, gather the relevant data, and then translate that data into the necessary action that will be carried out using mechanical force by actuators, are found in the perception execution layer, which is the lowest layer. The intermediate layer, or the layer of data transfer, is in charge of the system's data flow. Managing user-system interactions is within the purview of the top layer, control layer. The user is provided with the necessary services [17]. CPSs have a wide range of applications and advantages, but they are also open to security threats. Though there are protective measures with respect to the use of anti-viruses, IDS, firewalls, etc. The continuous data flow between the sensors, actuators and controllers makes it vulnerable to adversarial attacks. To improve the efficiency of such systems and making these systems secure AI and ML algorithms have been used widely [9],[11]. Each and every-day the kinds of attacks on CPSs are improving, which could cause a heavy damage to the infrastructure, human life, financial aspect etc. To have a defense strategy against these attacks that are rapidly improving, we need to know the kind of advancements in attacks; dark-web: one such platform which can give us an insight of current trends in adversarial attacks [10]. As mentioned in Figure 1. We see the different layers in CPS, adversaries can occur on any of the layers [17]. In section-II will describe regarding the different categories and different patterns of attacks on each of these layers.

2. Taxonomy

In addition to evaluating past research on Cyber Physical System security, this paper aims to categorise attacks and their impact on system behaviour. The paper is organized across the remainder sections as: Section-III describes the various security attacks that can occur on Cyber Physical Systems, Section IV tells about various defense strategies against these attacks. Section V lists a few existing methodologies to secure CPSs from stealthy attacks. Subsequent sections like section VI and VII and gives a brief of review work done for the analysis of the work done by researchers and future scope of research. Table -2 gives a summary of the research review. Figure-4 gives a diagrammatic view of the structure of the paper.

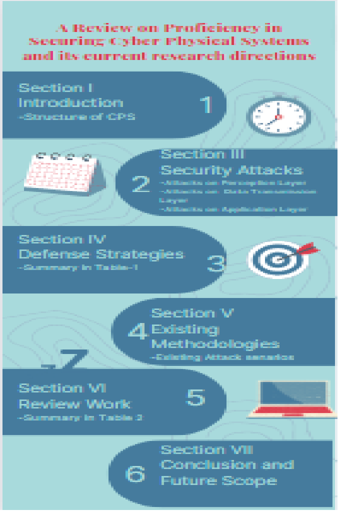

A Review on Proficiency in Securing Cyber Physical Systems and its current research directions
Section I
Introduction
-Structure of CPS
1
Section III
Security Attacks
-Attacks on Perception Layer
-Attacks on Data Transmission Layer
-Attacks on Application Layer
2
Section IV
Defense Strategies
-Summary in Table-1
3
Section V
Existing Methodologies
-Existing Attack senarios
4
Section VI
Review Work
-Summary in Table 2
5
Section VII
Conclusion and Future Scope
6

Figure-3 structure of paper

3. SECURITY ATTACKS

Liwei Cao etal. [17] described attacks can be categorized layer wise for a better understanding of how attacks could hamper the system. At the Perception Execution strata, the kinds of attacks that could occur are that could alter the sensor data, delete the sensor data, and insert counterfeited data to the sensor data. Similarly with respect to actuators, attacks could be like enabling and disabling actuators. These attacks are namely Sensor Insertion attacks, Sensor Erasure attacks, Actuation device Enablement attack, Actuator Disablement attack etc [17]. Attacks on Data Transmission layer could be the general kind of attacks that happen to any network layer in any networking. MIM and DoS assaults are the most frequent attacks seen in this layer, according to [17] for CPSs. An example of a MIM attack on CPS is shown in Figure 3. Figure 5 illustrates a DoS attack on the CPS. Such assaults affect the system in various ways leading system to be out of control, not providing any service or destruction of the system.

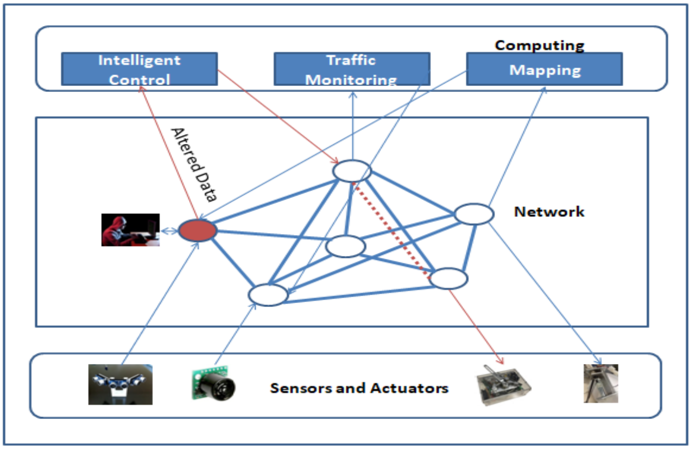


Figure-4: MIM attack in CPS

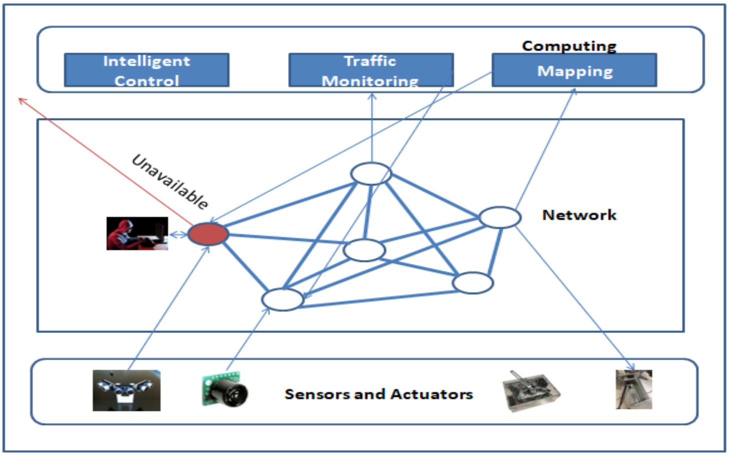


Figure-5: Denial of Service attack in CPS

The DoS attack in Figure-5 describes how a controller is being made unavailable to the physical component of the system, ultimately the system would not respond as required [17].The DoS attack could lead to three different situations overloading the controller or the sensors, sending invalid data to the controller or traffic could be blocked. DoS attack can be avoided to some extent by injecting PS-Poll frame. Figure-7 describes how a PS-Poll frame could work. At Application control strata the kind of attacks that are possible are stealing application related data from databases; by attacking the databases or attacking on users private information [17].K. Aarika et al [18] defined various attacks on CPS as Jamming, Tampering, Exhaustion, Collision and unfairness; these attacks most commonly occur in wireless sensor networks. Figure-5 shows the general attacks on CPSs.

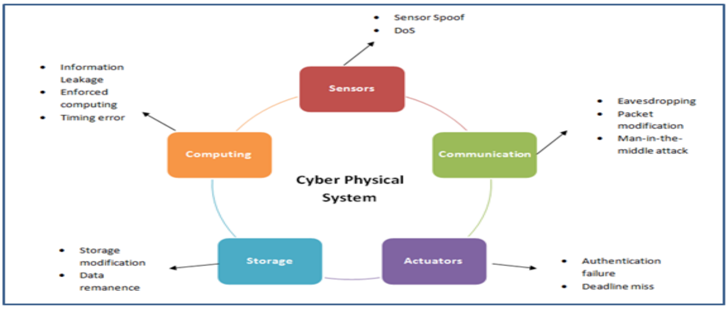


Figure-6: General Attacks on CPS

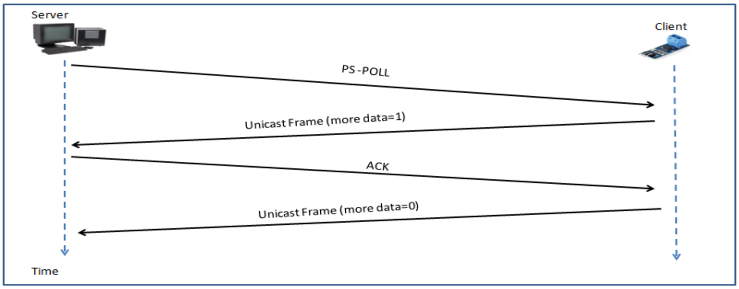


Figure-7: Explaining PS-Poll

4. Defense Strategies

Section II describes the assualts layer wise, the defense strategies in this section would be discussed layer wise. At the bottom most layer of CPS, i.e., Perception Execution layer attacks are generally on the sensors and actuators. Table-1 shows the consolidation of all the layers with respect to their attacks and defense mechanisms.

4.1. Attacks and Defense mechanisms on Perception Execution Layer

The sensor data can be altered and hence the system could be misled by the attacker. Goes et al. [5] proposed the idea of Insertion Deletion Structure, which captures the interactions between the system and the attacker. The Insertion Deletion Structure can predict all the actions of an adversary and to what state the system might lead to.

H. Jeon et al. [13] described a very stealthy attack on the sensors called as the Pole Dynamics Attack. Even the attacker hardly has any knowledge regarding the system still with the help of Pole-Dynamics Attack the attacker can creep into the system and stays sneaky till the attack has affected. In Pole Dynamics Attack fake data is injected into the sensor data ultimately causing the controller to take a wrong decision, leading to system failure or corruption. As per Liwei Cao [17], there can be ways which is similar to Disturbance Observer, where the technique makes an observation between the actual and expected dynamics of the system. The problem with this technique is that, the attacker also could make use of the same technique (DOB) and could understand the deviations between the actual and the expected system dynamics, using which the attacker can make sure the attack remains stealthy until the attack is successful.

Another way to defend is by developing a model-based approach to predict the system's behavior. According to W. L. Duo [25] a finite automaton can be used as a model to identify or predict the system state. [25] Describes the model as the states of the model to be X; wherein the states are {Initial state, S1, S2,..,Sn, Denial of service, illegal access}; inputs to the system are {E1,E2,E3,…En, Grant access, De-authorize}; where E1,E2,….,En, exploits made by the attacker [25]. The initial state of the model is a clean state wherein the attacker has not performed any action, but in the subsequent phase the action of the attacker could lead to a damaging state. Figure-7 shows the finite automaton of an attack on a CPS. Figure-8 demonstrates how the system could reach to out of control state ultimately causing Denial of service attack or providing illegal access to the attacker. Therefore, safe and unsafe states of a CPS can be predicted using finite automata when the system is under assault. Petri nets are a different method to evaluate the dangers that could harm CPSs, according to Y. Fu [8].Identification of various threats on CPS gets difficult as increase in the assaults.

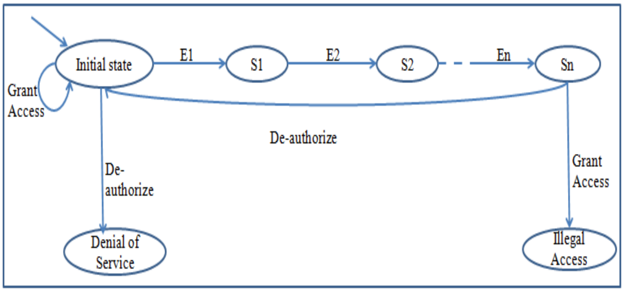


Figure-8: Automaton of an attack on CPS

4.2 Attacks and Defense mechanisms on Data Transmission Layer

In CPS, the most common attacks in this layer are MIM and DoS. According to Yassine [14], to prevent MIM attack, we could use the most common security that is cryptographic measures like Message Digest, Digital Signature, and MAC Biometrics. Lima [6], presented a module called NA safe Controllability; which would mean Network Attack Safe Controllability mainly used to prevent the system damage caused by Man in the Middle attack. When the system is under an attack in a closed loop, then a supervisory control that identifies that the system could reach an unsafe state takes an immediate action to block the system state [6]. S. Liu et al. [7] has designed a mixed strategy to defend the DoS attack. The mix strategy includes the combination of zero-sum game and investigation of the feedback controller using LMI tool box.

4.3 Attacks and Defense mechanisms on Application Control Layer

In contrast to other CPS layers, this layer is less vulnerable to attacks. The concern here is data loss, which may be avoided with the aid of cryptographic techniques like public key encryption and error correction codes, among others.

Table-1 Attacks and Defense strategies on CPSs

Layer	**Attack**	**Defense**
Perception Execution Layer	SI, SE, AE, AD, Pole-Dynamics attack	IDA, Model based Approach, DOB
Data Transmission Layer	MIM, DOS	NA Safe Controllability, Stochastic Game theory
Application Control Layer	Data loss	Public Key Cryptography

5. Existing Methods/Techniques

As per Sravanthi et al. [15] Cyber Physical Systems generate a huge amount of data on a daily basis, due to the sensors that generate data and hence only data analysis tools can help understand this vast data. When it comes to securing CPSs, instead of making use of mathematical models, Machine learning algorithms can be used for quick decision making. Z. N. Zarandi et al. [19] discussed in his paper about the 2 major kinds of attacks happening on CPSs, i.e. DoS, Deception attacks and in both the category of attacks, Machine learning methods are the best way to analyze and detect these attacks. [19] Mentions in his paper regarding the simulating tools for CPS security. [19] Makes use of a Neural Network Library called Keras, MATLAB software for generating datasets and evaluation of the detection of attacks. We could also make use of SVM to evaluate the system performance [19]. John S. Baras [22], has mentioned about Model Based Systems Engineering for CPS, this model is a combination of SysML, Modelica, and MATLAB tools.

6. Review Work

Sangjun Kim et al. [26] mentioned a few recent assaults on CPS as re-play attack, few sneaky ways to manipulate information from sensors and control input data: zero dynamics attack, pole dynamics attack, and covert attack. Focus should be on detection of such stealthy attacks unlike in the conventional information security where the focus is on eavesdropping and encryption. Due to the presence of physical dynamics in CPSs eavesdropping would not affect the behavior of the physical component [1], [26]. Table 2 gives a brief of my Research. The present focus should be on detection of stealthy attacks that attack the behaviour of the components of CPS [1],[26]. Table-2 gives a brief of my research review.

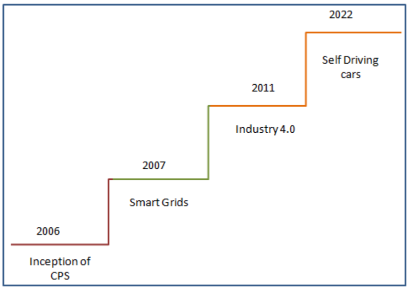
Table 2: Review of Research

Title of the paper	**Journal/Publisher**	**Year**	**Advantages/ Disadvantages**	**Algorithm/Technology used**
A survey of cyber attacks on Cyber Physical Systems: Recent Advances and Challenges [25]	IEEE/ CAA Journal of Automatica Sinica	2022	The study explores model-based security and lists various attacks against CPSs. They also emphasized the need for DoS attack defense systems.	Model based security
Design Analysis and Implementation of a security Assessment/Enhancement platform for Cyber Physical Systems [24]	IEEE / IEEE Transactions On Industrial Informatics	2022	The authors proposed and experimented on security enhancement modules with respect to an architecture for CPS	Layer based security
Can Block chain be Trusted in Industry 4.0? Study of a Novel Misleading Attack on Bit coin [28]	IEEE/ IEEE Transactions on Industrial Informatics	2022	The author proposed misleading attacks on blocks and its future scope, which can hamper the security in Industry-4.0	Block-chain, Mis-leading attack
Active Security Control Approach Against DoS Attacks in Cyber-Physical Systems [23]	IEEE/ IEEE Transactions on Automatic Control	2021	The author simulated a network and created DoS attack and designed an active security control against DoS.	Stable controller design based on Predictive control theory
A Literature Review on Block chain-enabled Security and Operation of	IEEE/ IEEE 46th Annual Computers,	2022	This paper describes about the use of	-------

[27]	Applications Conference		securing CPSs in different sectors like Health care, Transportation, smart-grids etc.	
Design and Analysis of Cyber Physical Systems [20]	IEEE / IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering	2021	The paper proposes BI system design and data security using transformations on data.The author stressed on analysis of data	Design of Business Intelligence System
Recent Developments on CPSs [21]	IEEE/ International Conference on Communication, Control and Information Sciences	2021	The paper presented various kinds of CPSs with popular real time examples. The authors introduced the concept of hybrid automata or verification in CPSs.	Automata for verification of CPS
A survey of Network Attacks on Cyber Physical Systems [17]	IEEE/ Special Section on Intelligent Information Services	2020	The paper is a research on various types of attacks on CPSs and defense mechanisms.	------
Perception layer security in internet of things [18]	Procedia Computer Science	2020	Research was based on the perception layer attacks and defense strategies	Layer based defense mechanisms
CPS Information Security Risk Evaluation system based on Petri nets [8]	IEEE / IEEE Second International Conference on Data Science in Cyberspace	2017	This paper gave an insight on securing CPSs using Petri nets.	Petri nets

7. Conclusion and Future work

Today's globe has many different types of CPSs since technological breakthroughs occur frequently. Households have received CPSs as well. Since there are security dangers to the Cyber Physical Systems that cannot be disregarded, the security of CPSs has become increasingly obvious. There are several strategies created for this goal, but we must all agree that since the enemies are getting better every day, our security measures also need to get better. Different systems' security procedures are designed using a variety of machine learning and deep learning methods. Creating machine learning modules for CPS security has a lot of potential in the future. Graph 1 displays the increase in research and development on Cyber Physical Systems since 2006.



Graph-1: Development in CPS

Future Work: Several researchers have published papers on Cyber Physical Systems and related security based on Block chain Technology [29]. Few essential factors in CPS are control, storage and trust; all the mentioned factors can be secured with various implementations of Block chain Technology [29]. Blockchain provides the necessary security in various ways, there is a huge gap to be filled in this context, research in this direction could benefit CPS.

8. References

1. Y. Mo and B. Sinopoli, “Secure control against replay attacks,” in Proc. Allerton Conf. Commun. Control Comput. (Allerton), 2009, pp. 911–918.
2. R. Katz, “The impact of broadband on the economy: Research to date and policy issues,” Broadband Series, 2012.
3. T. Lu, B. Xu, X. Guo, L. Zhao, and F. Xie, “A new multilevel framework for cyber-physical system security,” in Proc. 1st Int. Workshop Swarm Edge Cloud, pp. 1_2, 2013,
4. Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu,”Review on cyber-physical systems,” IEEE/CAA J. Autom. Sinica, vol. 4, no. 1, pp. 27_40, Jan. 2017.
5. R. M. Goes, E. Kang, R. Kwong, and S. Lafortune, ”Stealthy deception attacks for cyber-physical systems,”in Proc. IEEE 56th Annu. Conf. Decis. Control (CDC), Melbourne, VIC, Australia, pp. 4224_4230, Dec. 2017.
6. Subba Rao Polamuri, Dr. Kudipudi Srinivas, Dr. A. Krishna Mohan, Multi-Model Generative Adversarial Network Hybrid Prediction Algorithm (MMGAN-HPA) for stock market prices prediction, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9, 2022, Pages 7433-7444,https://doi.org/10.1016/j.jksuci.2021.07.001
7. S. Liu, B. Xu, S. Li and Y. Liu, "Resilient control strategy of cyber-physical system under DoS attacks," 2017 36th Chinese Control Conference (CCC), 2017, pp. 7760-7765, doi: 10.23919/ChiCC.2017.8028584.
8. Avanija, J., K. E. Kumar, Ch Usha Kumari, G. Naga Jyothi, K. Srujan Raju, and K. Reddy Madhavi. "Enhancing Network Forensic and Deep Learning Mechanism for Internet of Things Networks." (2023).
9. C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, “Generalization of deep learning for cyber-physical system security: A survey,” in IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, pp. 745–751, IEEE, 2018.
10. Masashi KADOGUCHI, Shota HAYASHI, Masaki HASHIMOTO, Akira OTSUKA, ”Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning” in IEEE 978-1-7281-2504-6/19, 2019
11. C. Li and M. Qiu, “Reinforcement Learning for Cyber-Physical Systems: with Cyber security Case Studies”. Chapman and Hall/CRC, 2019.

layer security in Internet of Things", in Future Generation Computer Systems, Elsevier ,Volume 100 pg. 144-164, November 2019

13. H. Jeon and Y. Eun, "A stealthy sensor attack for uncertain cyber-physical systems", IEEE Internet Things J., vol. 6, no. 4, pp. 6345_6352, Aug. 2019.
14. Yassine, Maleh & Shojafar, Mohammad & Haqiq, Abdelkrim & Darwish, Ashraf. Cyber security and Privacy in Cyber Physical Systems, 2019
15. Sravanthi, K. & Tyagi, Amit &shamila.m,. (2019). Cyber physical systems: The role of machine learning and cyber security in present and future. 5. 66-80.
16. Felix O. Olowononi, Danda B. Rawat, and Chunmei Liu "Resilient Machine Learning for Networked Cyber Physical Systems: ASurvey for Machine Learning Security to Securing Machine Learning for CPS" in IEEE Communications Surveys & Tutorials, DOI 10.1109/COMST.2020.3036778, 2020
17. Liwei Cao, Xiaoning Jiang, Yumei Zhao, Shouguang Wang, Dan You, And Xianli Xu, "A Survey of Network Attacks on Cyber-Physical Systems", Special Section on Intelligent Information Services,IEEE Access Digital Object Identifier 10.1109/ACCESS.2020.2977423, March 2020
18. K. Aarika, M. Bouhlal, R. Ait Abdelouahid, S. Elfilali, E. Benlahmar, "Perception layer security in the internet of things" , Procedia Computer Science, Volume 175, Pages 591-596, ISSN 1877-0509, 2020.
19. Z. N. Zarandi and I. Sharifi, "Detection and Identification of Cyber-Attacks in Cyber-Physical Systems Based on Machine Learning Methods," 2020 11th International Conference on Information and Knowledge Technology (IKT), 2020, pp. 107-112, doi: 10.1109/IKT51791.2020.9345627.
20. Dmitriy P. Plakhotnikov, Elena E. Kotova, "Design and Analysis of Cyber-Physical Systems", in IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, 978-1-6654-0476-1/20, 2021
21. Prince V Jose, K. S. Sunil,"Recent Developments on Cyber-Physical Systems" in International Conference on Communication, Control and Information Sciences (ICCISc) | 978-1-6654-0295-8/20 IEEE | DOI: 10.1109/ICCISc52257.2021.9484983, 2021
22. John S. Baras," Formal Methods and Tool-Suites for CPS Security, Safety and Verification" NATO Science for Peace and Security Series - D: Information and Communication Security, Volume53: Engineering Secure and Dependable Software Systems, 2021,pg 1 – 7, doi: 10.3233/978-1-61499-977-5-1
23. T. Li, B. Chen, L. Yu and W. -A. Zhang, "Active Security Control Approach Against DoS Attacks in Cyber-Physical Systems," in IEEE Transactions on Automatic Control, vol. 66, no. 9, pp. 4303-4310, Sept. 2021, doi: 10.1109/TAC.2020.3032598.
24. Xirong Ning and Jin Jiang, "Design, Analysis and Implementation of a Security Assessment/Enhancement Platform for Cyber-Physical Systems"in IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 18, 2022
25. W. L. Duo, M. C. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," IEEE/CAA J. Autom. Sinica, vol. 9, no. 5, pp. 784–800, May 2022. Doi: 10.1109/JAS.2022.105548 ,2022
26. S. Kim, K. -J. Park and C. Lu, "A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design," in IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1534-1573, third quarter 2022, doi: 10.1109/COMST.2022.3187531.
27. A. A. Khalil, J. Franco, I. Parvez, S. Uluagac, H. Shahriar and M. A. Rahman, "A Literature Review on Blockchain-enabled Security and Operation of Cyber-Physical Systems," 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 2022, pp. 1774-1779, doi: 10.1109/COMPSAC54236.2022.00282.
28. G. Ebrahimpour, M. S. Haghighi and M. Alazab, "Can Blockchain be Trusted in Industry 4.0? Study of a Novel Misleading Attack on Bitcoin," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8307-8315, Nov. 2022, doi: 10.1109/TII.2022.3142036.
29. A. A. Khalil, J. Franco, I. Parvez, S. Uluagac, H. Shahriar and M. A. Rahman, "A Literature Review on Blockchain-enabled Security and Operation of Cyber-Physical Systems," 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 2022, pp. 1774-1779, doi: 10.1109/COMPSAC54236.2022.00282.