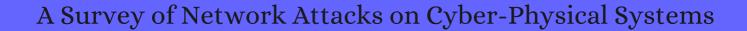
CITATION REPORT List of articles citing



DOI: 10.1109/access.2020.2977423 IEEE Access, 2020, 8, 44219-44227.

Source: https://exaly.com/paper-pdf/76918410/citation-report.pdf

Version: 2024-04-09

This report has been generated based on the citations recorded by exaly.com for the above article. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

#	Paper	IF	Citations
39	. IEEE Access, 2020 , 8, 68883-68894	3.5	8
38	Homomorphic Encryption of Supervisory Control Systems Using Automata. <i>IEEE Access</i> , 2020 , 8, 14718	5- <u>4</u> . 4 71	98 0
37	On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems. <i>IEEE Access</i> , 2021 , 9, 41787-41798	3.5	4
36	Zero Assignment via Generalized Sampler: A Countermeasure Against Zero-Dynamics Attack. <i>IEEE Access</i> , 2021 , 9, 109932-109942	3.5	1
35	CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review. <i>IEEE Access</i> , 2021 , 9, 38571-38601	3.5	5
34	Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. <i>Sustainability</i> , 2021 , 13, 3196	3.6	12
33	Universal Zero Dynamics: The SISO Case. 2021 ,		O
32	Cyberattack Resilient Control for Power Electronics Dominated Grid with Minimal Communication. 2021 ,		1
31	Detection and Isolation of DoS and Integrity Cyber Attacks in Cyber-Physical Systems with a Neural Network-Based Architecture. <i>Electronics (Switzerland)</i> , 2021 , 10, 2238	2.6	4
30	A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications. <i>IEEE Communications Surveys and Tutorials</i> , 2021 , 23, 1125-1159	37.1	18
29	Feature Selection Improves Tree-based Classification for Wireless Intrusion Detection. 2020,		2
28	GPU-based Classification for Wireless Intrusion Detection. 2020,		0
27	3C3C Model of Distribution Internet of Things Based on MQTT. 2020 ,		
26	A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid. <i>International Journal of Electrical Power and Energy Systems</i> , 2022 , 136, 10)7 72 0	3
25	A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid [Part []: Background on CPPS and necessity of CPPS testbeds. <i>International Journal of Electrical Power and Energy Systems</i> , 2022 , 136, 107718	5.1	6
24	Optimization-Based Assessment of Initial-State Opacity in Petri Nets. AIRO Springer Series, 2021, 127-1	3& .3	1
23	Novel Hybrid Model for Intrusion Prediction on Cyber Physical Systems©ommunication Networks based on Bio-inspired Deep Neural Network Structure. <i>Journal of Information Security and Applications</i> , 2022 , 65, 103107	3.5	1

22	An optimization-based approach to assess non-interference in labeled and bounded Petri net systems. <i>Nonlinear Analysis: Hybrid Systems</i> , 2022 , 44, 101153	4.5	1
21	A Survey on Dynamic Corrective Control of Asynchronous Sequential Machines. <i>Applied Sciences</i> (Switzerland), 2022 , 12, 2562	2.6	
20	Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems. <i>Computer Communications</i> , 2022 ,	5.1	O
19	Recommendation Method of Honeynet Trapping Component Based on LSTM. 2021,		
18	A Generalized Comprehensive Security Architecture Framework for IoT Applications Against Cyber-Attacks. <i>Lecture Notes in Electrical Engineering</i> , 2022 , 455-471	0.2	
17	Event-triggered model-free adaptive control for nonlinear cyber-physical systems with false data injection attacks. <i>International Journal of Robust and Nonlinear Control</i> , 2022 , 32, 2442-2452	3.6	1
16	Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures). <i>IEEE Access</i> , 2022 , 1-1	3.5	О
15	A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. <i>IEEE/CAA Journal of Automatica Sinica</i> , 2022 , 9, 784-800	7	12
14	Design and implementation of robust corrective control systems with permanent sensor faults. <i>Information Sciences</i> , 2022 ,	7.7	
13	A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design. <i>IEEE Communications Surveys and Tutorials</i> , 2022 , 1-1	37.1	3
12	Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope. <i>Computer Communications</i> , 2022 ,	5.1	
11	Secret Inference and Attacktability Analysis of Discrete Event Systems. Information Sciences, 2022,	7.7	
10	Universal Zero Dynamics Attacks Using Only Input-Output Data. 2022,		О
9	State-Feedback Control for Cyber-Physical Discrete-Time Systems under Replay Attacks: An LMI Approach. 2022 , 2022, 1-9		Ο
8	Robust input/output model matching of asynchronous sequential machines under intermittent actuator faults. 2022 ,		О
7	Multi-loop networked control system design subject to interchange attack.		O
6	Intrusion Response Systems for Cyber-Physical Systems: A Comprehensive Survey. 2022 , 102984		О
5	DDoS Attacks on Smart Manufacturing Systems: A Cross-Domain Taxonomy and Attack Vectors. 2022 ,		O

Cyber Physical System: Security Challenges in Internet of Things System. 2022,

Modular Supervisory Control for the Coordination of a Manufacturing Cell with Observable Faults.
2023, 23, 163

An Improved Light Weight Countermeasure Scheme to Efficiently Mitigate TCP Attacks in SDN.
2022, 501-511

Towards Secure Consensus of Multi-Agent Systems via a Virtual Network and Heterogeneous Controller Gains. 2022, 55, 236-241