Charalambos Konstantinou

List of Publications by Year
in descending order

76	1,546	430874 18	395702 33
papers	citations	h-index	g-index
78	78	78	886
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	The Cybersecurity Landscape in Industrial Control Systems. Proceedings of the IEEE, 2016, 104, 1039-1057.	21.3	249
2	Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. IEEE Access, 2021, 9, 29775-29818.	4.2	121
3	Survey of machine learning methods for detecting false data injection attacks in power systems. IET Smart Grid, 2020, 3, 581-595.	2.2	74
4	Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. IEEE Internet of Things Journal, 2022, 9, 199-221.	8.7	57
5	ConFirm: Detecting firmware modifications in embedded systems using Hardware Performance Counters. , 2015, , .		55
6	Cyber-physical systems: A security perspective. , 2015, , .		50
7	GPS spoofing effect on phase angle monitoring and control in a realâ€time digital simulatorâ€based hardwareâ€inâ€theâ€loop environment. IET Cyber-Physical Systems: Theory and Applications, 2017, 2, 180-187.	3.3	49
8	A Review of Current Research Trends in Power-Electronic Innovations in Cyberâ€"Physical Systems. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021, 9, 5146-5163.	5.4	48
9	Impact of firmware modification attacks on power systems field devices. , 2015, , .		43
10	Malicious Firmware Detection with Hardware Performance Counters. IEEE Transactions on Multi-Scale Computing Systems, 2016, 2, 160-173.	2.4	40
11	Enhanced Resilient State Estimation Using Data-Driven Auxiliary Models. IEEE Transactions on Industrial Informatics, 2020, 16, 639-647.	11.3	38
12	Blockchain and Autonomous Vehicles: Recent Advances and Future Directions. IEEE Access, 2021, 9, 130264-130328.	4.2	37
13	Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids. Sustainable Cities and Society, 2021, 75, 103116.	10.4	35
14	Deep Reinforcement Learning for Cybersecurity Assessment of Wind Integrated Power Systems. IEEE Access, 2020, 8, 208378-208394.	4.2	32
15	A Case Study on Implementing False Data Injection Attacks Against Nonlinear State Estimation. , 2016, , .		31
16	Toward a Secure and Resilient All-Renewable Energy Grid for Smart Cities. IEEE Consumer Electronics Magazine, 2022, 11, 33-41.	2.3	31
17	Evasion Attacks with Adversarial Deep Learning Against Power System State Estimation. , 2020, , .		29
18	Hardware-Layer Intelligence Collection for Smart Grid Embedded Systems. Journal of Hardware and Systems Security, 2019, 3, 132-146.	1.3	28

#	Article	IF	Citations
19	On the Feasibility of Load-Changing Attacks in Power Systems During the COVID-19 Pandemic. IEEE Access, 2021, 9, 2545-2563.	4.2	28
20	Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids. International Journal of Electrical Power and Energy Systems, 2021, 132, 107150.	5.5	28
21	A resilience-oriented centralised-to-decentralised framework for networked microgrids management. Applied Energy, 2022, 308, 118234.	10.1	26
22	Contactless Technologies for Smart Cities: Big Data, IoT, and Cloud Infrastructures. SN Computer Science, 2021, 2, 334.	3.6	24
23	The Nitric Oxide System in Peripheral Artery Disease: Connection with Oxidative Stress and Biopterins. Antioxidants, 2020, 9, 590.	5.1	23
24	Advanced Techniques for Designing Stealthy Hardware Trojans. , 2014, , .		20
25	Detection of Malicious Attacks in Autonomous Cyber-Physical Inverter-Based Microgrids. IEEE Transactions on Industrial Informatics, 2022, 18, 5815-5826.	11.3	20
26	Adversarial Examples on Power Systems State Estimation. , 2020, , .		18
27	Attacking the smart grid using public information. , 2016, , .		17
28	Blockchain for Distributed Energy Resources Management and Integration. IEEE Access, 2022, 10, 68598-68617.	4.2	16
29	Cyber Insurance Against Cyberattacks on Electric Vehicle Charging Stations. IEEE Transactions on Smart Grid, 2022, 13, 1529-1541.	9.0	14
30	Resilient Cyber-Physical Energy Systems Using Prior Information Based on Gaussian Process. IEEE Transactions on Industrial Informatics, 2022, 18, 2160-2168.	11.3	13
31	Load-Altering Attacks Against Power Grids Under COVID-19 Low-Inertia Conditions. IEEE Open Access Journal of Power and Energy, 2022, 9, 226-240.	3.4	13
32	Taxonomy of firmware Trojans in smart grid devices. , 2016, , .		12
33	Image Processing Based Approach for False Data Injection Attacks Detection in Power Systems. IEEE Access, 2022, 10, 12412-12420.	4.2	12
34	A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain. IEEE Transactions on Industrial Informatics, 2023, 19, 1894-1902.	11.3	11
35	DERauth: A Battery-Based Authentication Scheme for Distributed Energy Resources. , 2020, , .		10
36	Cyber-Physical Systems Security Education Through Hands-on Lab Exercises. IEEE Design and Test, 2020, 37, 47-55.	1.2	10

#	Article	IF	Citations
37	Enabling multi-layer cyber-security assessment of Industrial Control Systems through Hardware-In-The-Loop testbeds. , 2016, , .		9
38	PHYLAX: Snapshot-based profiling of real-time embedded devices via JTAG interface. , 2018, , .		9
39	Reinforcement Learning for Cyber-Physical Security Assessment of Power Systems. , 2019, , .		9
40	Cyber Risks to Critical Smart Grid Assets of Industrial Control Systems. Energies, 2021, 14, 5501.	3.1	9
41	Attack Detection and Localization in Smart Grid with Image-based Deep Learning. , 2021, , .		9
42	Security assessment and impact analysis of cyberattacks in integrated T&D power systems. , 2021, , .		8
43	Datadriven false data injection attacks against cyber-physical power systems. Computers and Security, 2022, 121, 102836.	6.0	8
44	A Data-Based Detection Method Against False Data Injection Attacks. IEEE Design and Test, 2020, 37, 67-74.	1.2	7
45	Cybersecurity for the Smart Grid. Computer, 2020, 53, 10-12.	1.1	7
46	Adversarial attack and defense methods for neural network based state estimation in smart grid. IET Renewable Power Generation, 2022, 16, 3507-3518.	3.1	7
47	A Triggerless Backdoor Attack and Defense Mechanism for Intelligent Task Offloading in Multi-UAV Systems. IEEE Internet of Things Journal, 2023, 10, 5719-5732.	8.7	7
48	Privacy-Preserving Functional IP Verification Utilizing Fully Homomorphic Encryption. , 2015, , .		6
49	A Hardware-based Framework for Secure Firmware Updates on Embedded Systems. , 2019, , .		6
50	Chaos Engineering for Enhanced Resilience of Cyber-Physical Systems. , 2021, , .		6
51	A power loss minimization strategy based on optimal placement and sizing of distributed energy resources. International Journal of Numerical Modelling: Electronic Networks, Devices and Fields, 2022, 35, .	1.9	6
52	FLEP-SGS²: a Flexible and Low-cost Evaluation Platform for Smart Grid Systems Security. , 2019, , .		5
53	Defensive costâ€“benefit analysis of smart grid digital functionalities. International Journal of Critical Infrastructure Protection, 2022, 36, 100489.	4.6	5
54	Stealthy Rootkit Attacks on Cyber-Physical Microgrids. , 2021, , .		4

#	Article	IF	Citations
55	Coordinated control and parameters optimization for PSS, POD and SVC to enhance the transient stability with the integration of DFIG based wind power systems. International Journal of Emerging Electric Power Systems, 2022, 23, 359-379.	0.8	4
56	Distributed Adaptive AC Droop Control in D-Q Coordinates for Inverter-Based Microgrids. , 2020, , .		4
57	Modeling Communication Networks in a Real-Time Simulation Environment for Evaluating Controls of Shipboard Power Systems. , 2020, , .		4
58	Low-budget Energy Sector Cyberattacks via Open Source Exploitation. , 2018, , .		3
59	Multi-Model Resilient Observer under False Data Injection Attacks. , 2020, , .		3
60	Evaluation of Communication Network Models for Shipboard Power Systems. , 2021, , .		3
61	Special Session: Physics- Informed Neural Networks for Securing Water Distribution Systems. , 2020, , .		3
62	Data-Driven Fault-Tolerant Tracking Control for Linear Parameter-Varying Systems. IEEE Access, 2022, 10, 66734-66742.	4.2	3
63	Plug-in electric vehicles demand modeling in smart grids. , 2021, , .		2
64	Special Session: Harness the Power of DERs for Secure Communications in Electric Energy Systems. , 2020, , .		2
65	CHIMERA: A Hybrid Estimation Approach to Limit the Effects of False Data Injection Attacks. , 2021, , .		2
66	Reinforcement of Power System Performance Through Optimal Allotment of Distributed Generators Using Metaheuristic Optimization Algorithms. Journal of Electrical Engineering and Technology, 2022, 17, 2617-2630.	2.0	2
67	SDRE-based primary control of DC Microgrids equipped by a fault detection/isolation mechanism. Energy Reports, 2022, 8, 8215-8224.	5.1	2
68	What Latin Hypercube Is Not. Lecture Notes in Management and Industrial Engineering, 2018, , 1-12.	0.4	1
69	A Modular End-to-End Framework for Secure Firmware Updates on Embedded Systems. ACM Journal on Emerging Technologies in Computing Systems, 2022, 18, 1-19.	2.3	1
70	Faster than real-time simulation. , 2021, , .		1
71	Load Shedding Frequency Management of Microgrids Using Hierarchical Fuzzy Control. , 2021, , .		1
72	Hardware-Enabled Secure Firmware Updates in Embedded Systems. IFIP Advances in Information and Communication Technology, 2020, , 165-185.	0.7	1

#	Article	IF	Citations
73	HPC-Based Malware Detectors Actually Work: Transition to Practice After a Decade of Research. IEEE Design and Test, 2022, 39, 23-32.	1.2	1
74	Assessment of Low-Budget Targeted Cyberattacks Against Power Systems. IFIP Advances in Information and Communication Technology, 2019, , 232-256.	0.7	0
75	UrbanBox: a Low Cost End-to-End Platform for Smart City Sensing. , 2019, , .		0
76	Session details: Session 1: Session 1: CPS&IoT Security. , 2020, , .		0