Piroska Haller

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/5082068/publications.pdf

Version: 2024-02-01

50 papers	545 citations	949033 11 h-index	889612 19 g-index
53 all docs	53 docs citations	53 times ranked	566 citing authors

#	Article	IF	Citations
1	Tampering Detection for Automotive Exhaust Aftertreatment Systems using Long Short-Term Memory Predictive Networks. , 2022, , .		3
2	Privacy-Preserving Tampering Detection in Automotive Systems. Electronics (Switzerland), 2021, 10, 3161.	1.8	10
3	A Security-Enhanced Interoperability Middleware for the Internet of Things. , 2019, , .		0
4	Anomaly Detection in Aging Industrial Internet of Things. IEEE Access, 2019, 7, 74217-74230.	2.6	27
5	Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. International Journal of Critical Infrastructure Protection, 2019, 25, 152-168.	2.9	19
6	Using Side-Channels to Detect Abnormal Behavior in Industrial Control Systems. , 2019, , .		0
7	A lightweight key generation scheme for end-to-end data authentication in Industrial Control Systems. Automatisierungstechnik, 2019, 67, 417-428.	0.4	3
8	Engineering security-aware control applications for data authentication in smart industrial cyberâ€“physical systems. Future Generation Computer Systems, 2019, 91, 206-222.	4.9	17
9	Engineering Edge Security in Industrial Control Systems. Advanced Sciences and Technologies for Security Applications, 2019, , 185-200.	0.4	0
10	On the practical integration of anomaly detection techniques in industrial control applications. International Journal of Critical Infrastructure Protection, 2019, 24, 48-68.	2.9	9
11	GHOST - Safe-Guarding Home IoT Environments with Personalised Real-Time Risk Control. Communications in Computer and Information Science, 2018, , 68-78.	0.4	27
12	Enabling authenticated data exchanges in industrial control systems. , 2018, , .		1
13	Cyber-Security-Aware Network Design of Industrial Control Systems. IEEE Systems Journal, 2017, 11, 1373-1384.	2.9	42
14	Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids. IEEE Transactions on Smart Grid, 2017, 8, 2440-2451.	6.2	16
15	Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems. IEEE Access, 2017, 5, 9336-9347.	2.6	26
16	Optimally scheduled interventions in the presence of vulnerabilities for modern cyber-physical systems. , 2017, , .		1
17	Cross-layer anomaly detection in industrial cyber-physical systems. , 2017, , .		3
18	Design, verification and implementation of a lightweight remote attestation protocol for process control systems. , 2017, , .		0

#	Article	IF	Citations
19	Big Data Processing to Detect Abnormal Behavior in Smart Grids. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2017, , 214-221.	0.2	0
20	SOFTWARE DEFINED RESPONSE AND NETWORK RECONFIGURATION FOR INDUSTRIAL CONTROL SYSTEMS. IFIP Advances in Information and Communication Technology, 2017, , 157-173.	0.5	2
21	Generating high quality data for the protection of modern critical infrastructures. , 2016, , .		2
22	A framework for designing resilient distributed intrusion detection systems for critical infrastructures. International Journal of Critical Infrastructure Protection, 2016, 15, 3-11.	2.9	20
23	A hierarchical control plane for software-defined networks-based industrial control systems. , 2016, , .		18
24	Data transfer regulator for wireless teleoperation. Transactions of the Institute of Measurement and Control, 2016, 38, 141-149.	1.1	2
25	Nonlinear PI Rate Control in Bottleneck Links: Application to Teleoperation Systemsâˆ—â˜—This work was supported by a grant of the Romanian National Authority for Scientific Research, CNCS UEFISCDI, project number PN-II-RU-TE-2011-3-0005.. IFAC-PapersOnLine, 2015, 48, 14-19.	0.5	3
26	Denial of Service Attack Detection in Case of Tennessee Eastman Challenge Process. Procedia Technology, 2015, 19, 835-841.	1.1	13
27	A framework for testing stealthy attacks in energy grids. , 2015, , .		2
28	A clustering-based approach to detect cyber attacks in process control systems. , 2015, , .		38
29	Bilateral Teleoperation in the Presence of Jitter: Communication Performance Evaluation and Control. Studies in Systems, Decision and Control, 2015, , 291-311.	0.8	2
30	Behavior-based critical cyber asset identification in Process Control Systems under Cyber Attacks. , 2015, , .		2
31	A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, 2015, 10, 3-17.	2.9	90
32	Experimental assessment of network design approaches for protecting industrial control systems. International Journal of Critical Infrastructure Protection, 2015, 11, 24-38.	2.9	28
33	Performance Analysis of Wireless Sensor Networks. Procedia Technology, 2015, 19, 842-849.	1.1	7
34	Data clustering-based anomaly detection in industrial control systems. , 2014, , .		50
35	Communication delay and jitter influence on bilateral teleoperation. , 2014, , .		5
36	A connection pattern-based approach to detect network traffic anomalies in critical infrastructures. , 2014, , .		20

#	Article	IF	Citations
37	A survey on cloud-based software platforms to implement secure smart grids. , 2014, , .		17
38	Performance analysis of WLAN based mobile robot teleoperation. , 2013, , .		3
39	Video supported bilateral teleoperation system: Design and implementation. , 2013, , .		1
40	Passive bilateral teleoperation with bounded control signals. , 2013, , .		2
41	Bilateral Teleoperation of Wheeled Mobile Robots Working in Common Workspace. IAES International Journal of Robotics and Automation, 2013, 3, .	0.2	3
42	Extending the BOINC architecture using peer-to-peer application code exchange. , 2011, , .		2
43	A syntactic approach for identifying multi-protocol attacks. , 2009, , .		0
44	Prediction and congestion control algorithm for networked motion tracking. Control Engineering Practice, 2009, 17, 1265-1272.	3.2	3
45	Middleware for Automated Implementation of Security Protocols. Lecture Notes in Computer Science, 2009, , 476-490.	1.0	1
46	Towards Automated Secure Web Service Execution. Lecture Notes in Computer Science, 2009, , 943-954.	1.0	0
47	Term-Based Composition of Security Protocols. , 2008, , .		1
48	Formal verification and implementation of real time operating system based applications. , 2008, , .		0
49	Dynamic Filter Based Prediction for Efficient Networked Motion Tracking. Industrial Informatics, 2009 INDIN 2009 7th IEEE International Conference on, 2007, , .	0.0	0
50	Adaptive Transfer Protocol for Networked Motion Tracking. , 2007, , .		0