Covert Attacks in Cyber-Physical Control Systems

DOI: 10.1109/tii.2017.2676005
IEEE Transactions on Industrial Informatics, 2017, 13, 1641-16

#	Paper	IF	Citations
75	. **2017**,		2
74	A controller design for mitigation of passive system identification attacks in networked control systems. *Journal of Internet Services and Applications*, **2018**, 9,	2.6	5
73	Simultaneous Trajectory Planning and Tracking Using an MPC Method for Cyber-Physical Systems: A Case Study of Obstacle Avoidance for an Intelligent Vehicle. *IEEE Transactions on Industrial Informatics*, **2018**, 14, 4273-4283	11.9	99
72	A Risk-Theoretical Approach to $mathcal{H}_{2}$-Optimal Control Under Covert Attacks. **2018**,		1
71	Detection and Mitigation of False Data Injection Attacks for Secure Interactive Networked Control Systems. **2018**,		6
70	Security Aspects of Cyber Physical Systems. **2018**,		4
69	Evaluation on Passive System Identification and Covert Misappropriation Attacks in Large Pressurized Heavy Water Reactors. **2018**,		
68	Measuring and Enhancing Microgrid Resiliency Against Cyber Threats. *IEEE Transactions on Industry Applications*, **2019**, 55, 6303-6312	4.3	18
67	Security and Quality in Cyber-Physical Systems Engineering. **2019**,		6
66	Detection and Compensation of Covert Service-Degrading Intrusions in Cyber Physical Systems through Intelligent Adaptive Control. **2019**,		4
65	. *IEEE Access*, **2019**, 7, 97052-97093	3.5	49
64	Countermeasure for Identification of Controlled Data Injection Attacks in Networked Control Systems. **2019**,		
63	Distributed Detection of Covert Attacks for Interconnected Systems. **2019**,		9
62	Bibliographical review on cyber attacks from a control oriented perspective. *Annual Reviews in Control*, **2019**, 48, 103-128	10.3	37
61	Securing the testing process for industrial automation software. *Computers and Security*, **2019**, 85, 156-180	3.9	7
60	. **2019**,		3
59	A Covert System Identification Attack on Constant Setpoint Control Systems. **2019**,		1

58	Real-Time Monitoring and Control of Industrial Cyberphysical Systems: With Integrated Plant-Wide Monitoring and Control Framework. *IEEE Industrial Electronics Magazine*, **2019**, 13, 38-47	6.2	100
57	An Attribute Credential Based Public Key Scheme for Fog Computing in Digital Manufacturing. *IEEE Transactions on Industrial Informatics*, **2019**, 15, 2297-2307	11.9	28
56	Optimal Switching Integrity Attacks on Sensors in Industrial Control Systems. *Journal of Systems Science and Complexity*, **2019**, 32, 1290-1305	1	5
55	Cyberattack-Resilient Hybrid Controller Design with Application to UAS. *Unmanned System Technologies*, **2019**, 33-56	0.4	
54	Bio-inspired Active System Identification: a Cyber-Physical Intelligence Attack in Networked Control Systems. *Mobile Networks and Applications*, **2020**, 25, 1944-1957	2.9	7
53	Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 2716-2725	11.9	120
52	Distributed Screening of Hijacking Attacks in DC Microgrids. *IEEE Transactions on Power Electronics*, **2020**, 35, 7574-7582	7.2	25
51	. **2020**,		
50	A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems. *Energies*, **2020**, 13, 3860	3.1	22
49	Resilient Distributed Fuzzy Load Frequency Regulation for Power Systems Under Cross-Layer Random Denial-of-Service Attacks. *IEEE Transactions on Cybernetics*, **2020**, PP,	10.2	17
48	. **2020**,		1
47	Detection of Covert Cyber-Attacks in Interconnected Systems: A Distributed Model-Based Approach. *IEEE Transactions on Automatic Control*, **2020**, 65, 3728-3741	5.9	20
46	BLCS: Brain-Like Distributed Control Security in Cyber Physical Systems. *IEEE Network*, **2020**, 34, 8-15	11.4	22
45	Cyber-Physical System Security. **2020**, 107-119		
44	Distributed fuzzy filtering for load frequency control of non-linear interconnected power systems under cyber-physical attacks. *IET Control Theory and Applications*, **2020**, 14, 527-538	2.5	10
43	Identification of Data Injection Attacks in Networked Control Systems Using Noise Impulse Integration. *Sensors*, **2020**, 20,	3.8	3
42	Data-Driven False Data-Injection Attack Design and Detection in Cyber-Physical Systems. *IEEE Transactions on Cybernetics*, **2020**,	10.2	15
41	. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 5825-5834	11.9	6

40	Model-Based Stealth Attack to Networked Control System Based on Real-Time Ethernet. *IEEE Transactions on Industrial Electronics*, **2021**, 68, 7672-7683	8.9	2
39	A degradation-based detection framework against covert cyberattacks on SCADA systems. *IISE Transactions*, **2021**, 53, 812-829	3.3	4
38	Artificial intelligence for securing industrial-based cyber□physical systems. *Future Generation Computer Systems*, **2021**, 117, 291-298	7.5	48
37	. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	2
36	An Impact of Different Uncertainties and Attacks on the Performance Metrics and Stability of Industrial Control System. *Lecture Notes in Networks and Systems*, **2021**, 557-574	0.5	1
35	Cyber Security Using Machine Learning: Techniques and Business Applications. *Studies in Computational Intelligence*, **2021**, 385-406	0.8	1
34	Artificial Neural Network-Based Stealth Attack on Battery Energy Storage Systems. *IEEE Transactions on Smart Grid*, **2021**, 1-1	10.7	3
33	Metaheuristic Techniques in Attack and Defense Strategies for Cybersecurity: A Systematic Review. *Studies in Computational Intelligence*, **2021**, 449-467	0.8	3
32	. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 775-786	11.9	5
31	Soft Computing Optimization of Stealth Data Loss Attack to Industrial Control Systems. **2021**,		
30	On the Security of Networked Control Systems in Smart Vehicle and Its Adaptive Cruise Control. *IEEE Transactions on Intelligent Transportation Systems*, **2021**, 22, 3824-3831	6.1	8
29	Resilient control of cyber-physical systems under sensor and actuator attacks driven by adaptive sliding mode observer. *International Journal of Robust and Nonlinear Control*, **2021**, 31, 7425-7443	3.6	1
28	Event-triggered control of vehicle platoon under deception attacks. *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering*, 095440702110433	1.4	1
27	Siamese Neural Network Based Few-Shot Learning for Anomaly Detection in Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 5790-5798	11.9	73
26	Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook. **2019**, 383-412		17
25	A Cryptographic Toolbox for Feedback Control Systems. *Modeling, Identification and Control*, **2020**, 41, 313-332	1	1
24	Bio-inspired System Identification Attacks in Noisy Networked Control Systems. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2019**, 28-38	0.2	
23	Dynamic Network Path Provisioning and Selection for the Detection and Mitigation of Data Tampering Attacks in Networked Control Systems. *IEEE Access*, **2021**, 1-1	3.5	1

22	Analysis, prevention, and feasibility assessment of stealthy ageing attacks on dynamical systems. *IET Control Theory and Applications*,	2.5	0
21	Cyber-security in networked and distributed model predictive control. *Annual Reviews in Control*, **2021**,	10.3	0
20	Mode division-based anomaly detection against integrity and availability attacks in industrial cyber-physical systems. *Computers in Industry*, **2022**, 137, 103609	11.6	3
19	Resilient observer-based event-triggered control for cyber-physical systems under asynchronous denial-of-service attacks. *Science China Information Sciences*, **2022**, 65, 1	3.4	0
18	Digital Estimation of Three-tank System over Networks with Packets Loss based on TrueTime. **2021** ,		
17	Data-Driven Covert-Attack Strategies and Countermeasures for Cyber-Physical Systems. **2021**,		0
16	Averting and Mitigating the Effects of Uncertainties with Optimal Control in Industrial Networked Control System. **2021**,		0
15	An Online Approach to Covert Attack Detection and Indentification in Power Systems. *IEEE Transactions on Power Systems*, **2022**, 1-1	7	
14	Using Blockchain for Data Collection in the Automotive Industry Sector: A Literature Review. *Journal of Cybersecurity and Privacy*, **2022**, 2, 257-275	4	0
13	Optimized Control Function with Estimation of System Parameters Against Attack for Networked Control System. *Lecture Notes in Electrical Engineering*, **2022**, 515-528	0.2	
12	ANN-Based Stealth Attack to Battery Energy Storage Systems by Using a Low-Cost Device. **2022**,		
11	Resilient Observer Design for Cyber-Physical Systems with Data-Driven Measurement Pruning. **2022**, 85-117		0
10	Markov-Based Malware Propagation Modeling and Analysis in Multi-Layer Networks. **2022**, 2, 456-478		0
9	Event-triggered Control of Interconnected Nonlinear Systems subjected to Cyber-attacks and Time-varying Coupling. **2022**,		0
8	A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. **2023**, 215, 108975		9
7	Distributed Control Microgrids: Cyber-Attack Models, Impacts and Remedial Strategies. **2022**, 8, 1008-1023		0
6	Stealthy Cyberattacks Detection Based on Control Performance Assessment Methods for the Air Conditioning Industrial Installation. **2023**, 16, 1290		1
5	Incremental Security Enforcement for Cyber-Physical Systems. **2023**, 11, 18475-18498		0

4	Multiplicative Attacks with Essential Stealthiness in Sensor and Actuator Loops against Cyber-Physical Systems. **2023**, 23, 1957	0
3	Adaptive Control for Security and Resilience of Networked Cyber-Physical Systems: Where Are We?. **2022**,	0
2	An error neighborhood-based detection mechanism to improve the performance of anomaly detection in industrial control systems. **2022**,	0
1	How to protect smart and autonomous vehicles from stealth viruses and worms. **2023**,	0