LQ Secure Control for Cyber-Physical Systems Against Sparse Sensor and Actuator Attacks

DOI: 10.1109/tcns.2018.2878507
IEEE Transactions on Control of Network Systems, 2019, 6, 833-841.

#	Paper	IF	Citations
33	On modeling and secure control of cyber-physical systems with attacks/faults changing system dynamics: An average dwell-time approach. *International Journal of Robust and Nonlinear Control*, **2019**, 29, 5481-5498	3.6	4
32	Vector Recovery for a Linear System Corrupted by Unknown Sparse Error Vectors With Applications to Secure State Estimation. **2019**, 3, 895-900		4
31	Dynamic Output Feedback Control of Cyber-Physical Systems Under DoS Attacks. *IEEE Access*, **2019**, 7, 181032-181040	3.5	12
30	Data-Driven Output-Feedback LQ Secure Control for Unknown Cyber-Physical Systems Against Sparse Actuator Attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, **2020**, 1-13	7.3	6
29	Neural-Network-Based Adaptive Resilient Dynamic Surface Control Against Unknown Deception Attacks of Uncertain Nonlinear Time-Delay Cyberphysical Systems. *IEEE Transactions on Neural Networks and Learning Systems*, **2020**, 31, 4341-4353	10.3	23
28	MPC for the Cyber-Physical System with Deception Attacks. **2020**,		1
27	Secure state estimation for cyber-physical systems under sparse data injection attacks: a switched counteraction approach. *International Journal of Control*, **2020**, 1-12	1.5	1
26	Secure bipartite tracking control of a class of nonlinear multi-agent systems with nonsymmetric input constraint against sensor attacks. *Information Sciences*, **2020**, 539, 504-521	7.7	5
25	A Secure Control Learning Framework for Cyber-Physical Systems Under Sensor and Actuator Attacks. *IEEE Transactions on Cybernetics*, **2021**, 51, 4648-4660	10.2	11
24	Output feedback secure control for cyber-physical systems against sparse sensor attacks. *Applied Mathematics and Computation*, **2020**, 384, 125384	2.7	4
23	Event-triggered Output Feedback Resilient Control for NCSs under Deception Attacks. *International Journal of Control, Automation and Systems*, **2020**, 18, 2220-2228	2.9	4
22	Adaptive Control of Second-Order Nonlinear Systems With Injection and Deception Attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, **2020**, 1-8	7.3	11
21	A Robust Dynamic Compensation Approach for Cyber-Physical Systems Against Multiple Types of Actuator Attacks. *Applied Mathematics and Computation*, **2020**, 380, 125284	2.7	7
20	Fault tolerant control of islanded AC microgrids under sensor and communication link faults using online recursive reduced-order estimation. *International Journal of Electrical Power and Energy Systems*, **2021**, 126, 106578	5.1	3
19	. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, **2021**, 51, 176-190	7.3	120
18	Resilient State Estimation and Control of Cyber-Physical Systems Against False Data Injection Attacks on Both Actuator and Sensors. *IEEE Transactions on Control of Network Systems*, **2021**, 1-1	4	1
17	Resilient Predictive Control for Cyber-Physical Systems under Denial-of-Service Attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, **2021**, 1-1	3.5	3

16	Sparse Actuator and Sensor Attacks Reconstruction for Linear Cyber-physical Systems with Sliding Mode Observer. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	4
15	A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems. *Proceedings of the IEEE*, **2021**, 109, 517-541	14.3	21
14	Trust-based fault detection and robust fault-tolerant control of uncertain cyber-physical systems against time-delay injection attacks. *Heliyon*, **2021**, 7, e07294	3.6	0
13	Stochastic model predictive control framework for resilient cyber-physical systems: review and perspectives. *Philosophical Transactions Series A, Mathematical, Physical, and Engineering Sciences*, **2021**, 379, 20200371	3	3
12	A Secure Dynamic Event-Triggered Mechanism for Resilient Control of Multi-Agent Systems Under Sensor and Actuator Attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, **2021**, 1-12	3.9	5
11	ADP-based Remote Secure Control for Networked Control Systems under Unknown Nonlinear Attacks in Sensor and Actuator. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	
10	Reinforcement Learning for feedback-enabled cyber resilience. *Annual Reviews in Control*, **2022**,	10.3	8
9	Resilient Sliding Mode Control for a Class of Cyber-Physical Systems With Multiple Transmission Channels Under Denial-of-Service Attacks. *Journal of the Franklin Institute*, **2022**, 359, 5302-5302	4	
8	Adaptive finite-time control for cyber-physical systems with injection and deception attacks. *Applied Mathematics and Computation*, **2022**, 430, 127316	2.7	0
7	Resilient Load Frequency Control of Islanded AC Microgrids Under Concurrent False Data Injection and Denial-of-Service Attacks. *IEEE Transactions on Smart Grid*, **2022**, 1-1	10.7	0
6	Design of False Data Injection Attacks in Cyber-Physical Systems. *Information Sciences*, **2022**, 608, 825-843	7.7	1
5	Introduction to Cyber-Physical Security and Resilience. **2022**, 9-35		
4	Adaptive output-feedback resilient tracking control using virtual closed-loop reference model for cyber-physical systems with false data injection attacks.		
3	Observer-based decentralized fuzzy control for connected nonlinear vehicle systems.		0
2	Cyber-physical systems subject to false data injections: A model predictive control framework for resilience operations. **2023**, 152, 110957		0
1	Identification of FIR systems with binary-valued observations against denial-of-service attacks. **2023**, 450, 127989		0