

CITATION REPORT

List of articles citing

Secure estimation for cyber-physical systems with adversarial attacks and unknown inputs: An L2-gain method

DOI: 10.1002/rnc.4007

International Journal of Robust and Nonlinear Control
, 2018, 28, 2131-2143.

Source: <https://exaly.com/paper-pdf/69671517/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
26	Secure Luenberger-like observers for cyberphysical systems under sparse actuator and sensor attacks. <i>Automatica</i> , 2018 , 98, 124-129	5.7	32
25	Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks. <i>International Journal of Robust and Nonlinear Control</i> , 2019 , 29, 4797-4811	3.6	27
24	State estimation for linear systems with unknown input and random false data injection attack. <i>IET Control Theory and Applications</i> , 2019 , 13, 823-831	2.5	11
23	Secure interval observer for linear continuous-time systems with discrete measurements subject to cyber-attacks. 2019 ,		1
22	State Estimation and Event-Triggered Control for Cyber-Physical Systems under Malicious Attack. <i>Mathematical Problems in Engineering</i> , 2019 , 2019, 1-10	1.1	
21	Adaptive control for nonlinear cyber-physical systems under false data injection attacks through sensor networks. <i>International Journal of Robust and Nonlinear Control</i> , 2020 , 30, 65-79	3.6	35
20	Event-based distributed state estimation for linear systems under unknown input and false data injection attack. <i>Signal Processing</i> , 2020 , 170, 107423	4.4	12
19	Robust Adaptive Control for a Class of Disturbed Cyber-Physical Systems with Denial of Service. 2020 ,		1
18	Flow-based attack detection and accommodation for networked control systems. <i>International Journal of Control</i> , 2021 , 94, 834-847	1.5	1
17	Resilient adaptive control of switched nonlinear cyber-physical systems under uncertain deception attacks. <i>Information Sciences</i> , 2021 , 543, 398-409	7.7	17
16	Three-stage forgetting factor stochastic gradient parameter estimation methods for a class of nonlinear systems. <i>International Journal of Robust and Nonlinear Control</i> , 2021 , 31, 971-987	3.6	40
15	Online Secure State Estimation of Multiagent Systems Using Average Consensus. <i>IEEE Transactions on Systems, Man, and Cybernetics: Systems</i> , 2021 , 1-13	7.3	3
14	. <i>IEEE Transactions on Systems, Man, and Cybernetics: Systems</i> , 2021 , 51, 176-190	7.3	120
13	Resilient control of cyber-physical systems under sensor and actuator attacks driven by adaptive sliding mode observer. <i>International Journal of Robust and Nonlinear Control</i> , 2021 , 31, 7425-7443	3.6	1
12	Secure State Estimation of Multiagent Systems With Homologous Attacks Using Average Consensus. <i>IEEE Transactions on Control of Network Systems</i> , 2021 , 8, 1293-1303	4	5
11	Robust adaptive estimation and tracking control for perturbed cyber-physical systems against denial of service. <i>Applied Mathematics and Computation</i> , 2021 , 404, 126255	2.7	5
10	Finite-Time Secure Dynamic State Estimation for Cyber-Physical Systems Under Unknown Inputs and Sensor Attacks. <i>IEEE Transactions on Systems, Man, and Cybernetics: Systems</i> , 2021 , 1-10	7.3	3

9	A survey on attack detection, estimation and control of industrial cyber-physical systems. <i>ISA Transactions</i> , 2021 , 116, 1-16	5.5	33
8	A secure state estimation algorithm for nonlinear systems under sensor attacks. 2020 ,		o
7	Asymptotic Stabilization of High-order Nonlinear Systems Subject to Actuator and Sensor Attacks. 2020 ,		
6	Unknown input estimation algorithms for a class of LPV/nonlinear systems with application to wastewater treatment process. <i>Proceedings of the Institution of Mechanical Engineers Part I: Journal of Systems and Control Engineering</i> , 095965182210837	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	Distributed filtering for nonlinear systems under false data injection attack. 2022 , 145, 110521		
2	Minimum structural sensor placement for switched linear time-invariant systems and unknown inputs. 2022 , 146, 110557		o
1	Attack detection and fault-tolerant control of interconnected cyber-physical systems against simultaneous replayed time-delay and false-data injection attacks.		o