Optimal stealthy false data injection attacks in cyber-physical systems

DOI: 10.1016/j.ins.2019.01.001
Information Sciences, 2019, 481, 474-490.

#	Paper	IF	Citations
73	Cooperative attack strategy design via H∞ scheme for linear cyber-physical systems. *International Journal of Robust and Nonlinear Control*, **2020**, 30, 33-50	3.6	5
72	False data injection attacks against state estimation in the presence of sensor failures. *Information Sciences*, **2020**, 508, 92-104	7.7	27
71	Worst-case ?-stealthy false data injection attacks in cyber-physical systems. *Information Sciences*, **2020**, 515, 352-364	7.7	10
70	Event-based distributed state estimation for linear systems under unknown input and false data injection attack. *Signal Processing*, **2020**, 170, 107423	4.4	12
69	Optimal deception attacks against remote state estimation in cyber-physical systems. *Journal of the Franklin Institute*, **2020**, 357, 1832-1852	4	19
68	Sensor attack detection for cyber-physical systems based on frequency domain partition. *IET Control Theory and Applications*, **2020**, 14, 1452-1466	2.5	7
67	A systematic review of cyber-resilience assessment frameworks. *Computers and Security*, **2020**, 97, 101996	4.9	11
66	An asymmetric interdependent networks model for cyber-physical systems. *Chaos*, **2020**, 30, 053135	3.3	9
65	Distributed active disturbance rejection control for Ackermann steering of a four-in-wheel motor drive vehicle with deception attacks on controller area networks. *Information Sciences*, **2020**, 540, 370-389	7.7	13
64	Optimal Stealth Attack Strategy Design for Linear Cyber-Physical Systems. *IEEE Transactions on Cybernetics*, **2020**, PP,	10.2	2
63	Detection of stealthy false data injection attacks against networked control systems via active data modification. *Information Sciences*, **2021**, 546, 192-205	7.7	34
62	Detection, estimation, and compensation of false data injection attack for UAVs. *Information Sciences*, **2021**, 546, 723-741	7.7	14
61	Optimal sensor attacks in cyber-physical systems with Round-Robin protocol. *Information Sciences*, **2021**, 548, 85-100	7.7	15
60	Adaptive fault estimation for cyber-physical systems with intermittent DoS attacks. *Information Sciences*, **2021**, 547, 746-762	7.7	8
59	Secure state estimation for systems under mixed cyber-attacks: Security and performance analysis. *Information Sciences*, **2021**, 546, 943-960	7.7	9
58	Optimal stealthy switching location attacks against remote estimation in cyber-physical systems. *Neurocomputing*, **2021**, 421, 183-194	5.4	4
57	Optimal Allocation of False Data Injection Attacks for Networked Control Systems With Two Communication Channels. *IEEE Transactions on Control of Network Systems*, **2021**, 8, 2-14	4	4

56	Optimal Stealthy Innovation-Based Attacks With Historical Data in Cyber-Physical Systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, **2021**, 51, 3401-3411	7.3	13
55	Optimal Jamming Attack System Against Remote State Estimation in Wireless Network Control Systems. *IEEE Access*, **2021**, 9, 51679-51688	3.5	1
54	Secure State Estimation With Switched Compensation Mechanism Against DoS Attacks. *IEEE Transactions on Cybernetics*, **2021**, PP,	10.2	2
53	Remote State Estimation for Nonlinear Systems via a Fading Channel: A Risk-sensitive Approach. *IEEE Transactions on Cybernetics*, **2021**, PP,	10.2	1
52	Leader-Following Consensus of Multiple Euler-Lagrange Systems Under Deception Attacks. *IEEE Access*, **2021**, 9, 100548-100557	3.5	1
51	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
50	Unified multidisciplinary modeling and simulation analysis of internal power system. *Journal of Computational Methods in Sciences and Engineering*, **2021**, 1-21	0.3	
49	. **2021**,		
48	Permutation entropy based detection scheme of replay attacks in industrial cyber-physical systems. *Journal of the Franklin Institute*, **2021**, 358, 4058-4076	4	4
47	Sliding-mode secure control for jump cyber□physical systems with malicious attacks. *Journal of the Franklin Institute*, **2021**, 358, 3424-3440	4	3
46	. **2021**,		1
45	A case study in the use of attack graphs for predicting the security of cyber-physical systems. **2021**,		3
44	Formulating false data injection cyberattacks on pumps□flow rate resulting in cascading failures in smart water systems. *Sustainable Cities and Society*, **2021**, 75, 103370	10.1	0
43	An Output-Coding-Based Detection Scheme Against Replay Attacks in Cyber-Physical Systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, **2021**, 68, 3306-3310	3.5	6
42	Optimal Attack Strategy Against Fault Detectors for Linear Cyber-Physical Systems. *Information Sciences*, **2021**, 581, 390-402	7.7	2
41	Secure State Estimation of Nonlinear Cyber-Physical Systems Against DoS Attacks: A Multiobserver Approach. *IEEE Transactions on Cybernetics*, **2021**, PP,	10.2	1
40	Adaptive Event-triggered Control for Networked Switched T-S Fuzzy Systems Subject to False Data Injection Attacks. *International Journal of Control, Automation and Systems*, **2020**, 18, 2580-2588	2.9	6
39	. **2021**,		

38	Reachability Analysis of Cyber-Physical Systems Under Stealthy Attacks. *IEEE Transactions on Cybernetics*, **2020**, PP,	10.2	4
37	Adaptive sliding-mode tracking control of networked control systems with false data injection attacks. *Information Sciences*, **2022**, 585, 194-208	7.7	4
36	Worst-Case Stealthy False-Data Injection Attacks on Remote State Estimation. **2021**,		0
35	Worst-Case Stealthy Innovation-based Linear Attacks on Remote State Estimation Under Kullback--Leibler Divergence. *IEEE Transactions on Automatic Control*, **2021**, 1-1	5.9	3
34	How vulnerable is innovation-based remote state estimation: Fundamental limits under linear attacks. *Automatica*, **2022**, 136, 110079	5.7	2
33	Complete stealthiness false data injection attacks against dynamic state estimation in cyber-physical systems. *Information Sciences*, **2022**, 586, 408-423	7.7	3
32	Detection of False Data Injection Attacks in Industrial Wireless Sensor Networks Exploiting Network Numerical Sparsity. *IEEE Transactions on Signal and Information Processing Over Networks*, **2021**, 7, 676-688	2.8	
31	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	
30	Research on cyber-physical system control strategy under false data injection attack perception. *Transactions of the Institute of Measurement and Control*, 014233122110693	1.8	
29	Blind false data injection attacks in smart grids subject to measurement outliers. *Journal of Control and Decision*, 1-10	0.9	1
28	Optimal completely stealthy attacks against remote estimation in cyber-physical systems. *Information Sciences*, **2022**, 590, 15-28	7.7	7
27	Stealthy FDI Attacks against Networked Control Systems Using Two Filters with an Arbitrary Gain. *IEEE Transactions on Circuits and Systems II: Express Briefs*, **2022**, 1-1	3.5	2
26	Stealthy false data injection attacks with resource constraints against multi-sensor estimation systems.. *ISA Transactions*, **2022**,	5.5	2
25	Estimation Performance of Cyber-Physical Systems Attacked by False Data Injection. **2021**,		
24	Watermarking-Based Protection Strategy Against Stealthy Integrity Attack on Distributed State Estimation. *IEEE Transactions on Automatic Control*, **2022**, 1-1	5.9	0
23	Leader-following bipartite consensus of multiple uncertain Euler-Lagrange systems under deception attacks. *Applied Mathematics and Computation*, **2022**, 428, 127227	2.7	2
22	A Secure Encoding Mechanism Against Deception Attacks on Multi-Sensor Remote State Estimation. *IEEE Transactions on Information Forensics and Security*, **2022**, 1-1	8	1
21	Stochastic Stealthy False Data Injection Attacks Against Cyber-Physical Systems. *IEEE Systems Journal*, **2022**, 1-12	4.3	0

20	Optimal innovation-based deception attacks with side information against remote state estimation in cyber-physical systems. *Neurocomputing*, **2022**, 500, 461-470	5.4	0
19	Fusion and detection for multi-sensor systems under false data injection attacks. *ISA Transactions*, **2022**,	5.5	0
18	Detection of Stealthy False Data Injection Attacks Against Cyber-Physical Systems: A Stochastic Coding Scheme.		1
17	Optimal encryption strategy for cyber-physical systems against stealthy attacks with energy constraints: A Stackelberg game approach. **2022**, 610, 674-693		0
16	Measurement-Based Optimal Stealthy Attacks on Remote State Estimation. **2022**, 17, 3365-3374		0
15	Innovation-based optimal linear attacks and detection under K-L divergence detector in cyber-physical systems. **2022**,		0
14	Leader-following consensus of multiple uncertain Euler□agrange systems under denial-of-service attacks.		0
13	Dynamic Leader-Following Bipartite Consensus of Multiple Uncertain Euler-Lagrange Systems Under Deception Attacks. **2022**, 1-1		0
12	Security of networked control systems subject to deception attacks: a survey. 1-22		3
11	Attack detection and fault-tolerant control of interconnected cyber-physical systems against simultaneous replayed time-delay and false-data injection attacks.		0
10	Optimal deception attacks on remote state estimators equipped with interval anomaly detectors. **2023**, 148, 110723		0
9	Deception attacks on Kalman filtering with interval estimation performance loss. **2022**, 55, 7-12		0
8	Game-Theoretic Switching Detection of Malicious Attacks in Switched Systems. **2022**, 1-15		0
7	Analysis of Stealthy False Data Injection Attacks Against Networked Control Systems: Three Case Studies.		1
6	Optimal energy constrained deception attacks in cyber-physical systems with multiple channels: A fusion attack approach. **2023**,		0
5	Detection of false data injection attacks in cyber□hysical systems using graph convolutional network. **2023**, 217, 109118		0
4	Multiplicative Attacks with Essential Stealthiness in Sensor and Actuator Loops against Cyber-Physical Systems. **2023**, 23, 1957		0
3	Abusive adversarial agents and attack strategies in cyber-physical systems. **2023**, 8, 149-165		0

2	Resilient Distributed State Estimation for LTI Systems Under Time-Varying Deception Attacks. **2023**, 10, 381-393	0
1	False data injection attacks on sensors against state estimation in cyber-physical systems. **2023**,	0