

Yuzhe Li

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/1746899/publications.pdf>

Version: 2024-02-01

42
papers

1,640
citations

516710

16
h-index

377865

34
g-index

42
all docs

42
docs citations

42
times ranked

1073
citing authors

#	ARTICLE	IF	CITATIONS
1	Learning-Based DoS Attack Power Allocation in Multiprocess Systems. IEEE Transactions on Neural Networks and Learning Systems, 2023, 34, 8017-8030.	11.3	3
2	Watermark-Based Proactive Defense Strategy Design for Cyber-Physical Systems With Unknown-but-Bounded Noises. IEEE Transactions on Automatic Control, 2023, 68, 3300-3315.	5.7	6
3	False-Data-Injection Attacks on Remote Distributed Consensus Estimation. IEEE Transactions on Cybernetics, 2022, 52, 433-443.	9.5	17
4	A Novel Attack Detection for Linear Systems With Unknown-But-Bounded Noises. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52, 4223-4232.	9.3	4
5	Distributed state estimation for linear time-invariant dynamical systems: A review of theories and algorithms. Chinese Journal of Aeronautics, 2022, 35, 1-17.	5.3	2
6	Proportional Tracking Control of Positive Linear Systems. , 2022, 6, 1670-1675.		5
7	Event-Triggered Control and Proactive Defense for Cyber-Physical Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52, 6305-6313.	9.3	7
8	Joint Power Allocation for Remote State Estimation With SWIPT. IEEE Transactions on Signal Processing, 2022, 70, 1434-1447.	5.3	11
9	Strategic DoS Attack in Continuous Space for Cyber-Physical Systems Over Wireless Networks. IEEE Transactions on Signal and Information Processing Over Networks, 2022, 8, 421-432.	2.8	3
10	Stealthy multiplicative attacks against cyber-physical systems: A gap metric approach. International Journal of Robust and Nonlinear Control, 2022, 32, 7336-7347.	3.7	2
11	Stochastic detection against deception attacks in CPS: Performance evaluation and game-theoretic analysis. Automatica, 2022, 144, 110461.	5.0	18
12	Data-Driven False Data-Injection Attack Design and Detection in Cyber-Physical Systems. IEEE Transactions on Cybernetics, 2021, 51, 6179-6187.	9.5	42
13	Optimal DoS Attack Against LQR Control Channels. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68, 1348-1352.	3.0	22
14	Optimal unbiased linear sensor fusion over multiple lossy channels with collective observability. Automatica, 2021, 128, 109568.	5.0	4
15	Security analysis for cyber-physical systems under undetectable attacks: A geometric approach. International Journal of Robust and Nonlinear Control, 2020, 30, 4359-4370.	3.7	19
16	Secure analysis of dynamic networks under pinning attacks against synchronization. Automatica, 2020, 111, 108576.	5.0	15
17	Sparse Undetectable Sensor Attacks Against Cyber-Physical Systems: A Subspace Approach. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67, 2517-2521.	3.0	16
18	Efficient Linear Sensor Fusion Over Multiple Lossy Channels With Local Observability. , 2019, 3, 721-726.		3

#	ARTICLE	IF	CITATIONS
19	Power control for multi-sensor remote state estimation over interference channel. Systems and Control Letters, 2019, 126, 1-7.	2.3	16
20	Multi-sensor transmission power control for remote estimation through a SINR-based communication channel. Automatica, 2019, 101, 78-86.	5.0	25
21	False Data Injection Attacks on Networked Control Systems: A Stackelberg Game Analysis. IEEE Transactions on Automatic Control, 2018, 63, 3503-3509.	5.7	122
22	Detection Against Linear Deception Attacks on Multi-Sensor Remote State Estimation. IEEE Transactions on Control of Network Systems, 2018, 5, 846-856.	3.7	161
23	An Intrusion Detection System for Cyber Attacks in Wireless Networked Control Systems. IEEE Transactions on Circuits and Systems II: Express Briefs, 2018, 65, 1049-1053.	3.0	36
24	Transmit power control and remote state estimation with sensor networks: A Bayesian inference approach. Automatica, 2018, 97, 292-300.	5.0	22
25	Power Control of an Energy Harvesting Sensor for Remote State Estimation. IEEE Transactions on Automatic Control, 2017, 62, 277-290.	5.7	61
26	SINR-Based DoS Attack on Remote State Estimation: A Game-Theoretic Approach. IEEE Transactions on Control of Network Systems, 2017, 4, 632-642.	3.7	227
27	A multi-channel transmission schedule for remote state estimation under DoS attacks. Automatica, 2017, 78, 194-201.	5.0	178
28	Improved results on transmission power control for remote state estimation. Systems and Control Letters, 2017, 107, 44-48.	2.3	6
29	A Game-Theoretic Approach to Fake-Acknowledgment Attack on Cyber-Physical Systems. IEEE Transactions on Signal and Information Processing Over Networks, 2017, 3, 1-11.	2.8	39
30	A Game-theoretic Approach to Remote State Estimation in Presence of a DoS Attacker. IFAC-PapersOnLine, 2017, 50, 2595-2600.	0.9	11
31	A Randomized Variance-based Sensor Scheduling for Remote State Estimation. IFAC-PapersOnLine, 2017, 50, 6385-6390.	0.9	4
32	Multi-sensor Transmission Management for Remote State Estimation under Coordination. IFAC-PapersOnLine, 2017, 50, 3829-3834.	0.9	10
33	Stochastic Detector against linear deception attacks on remote state estimation. , 2016, , .		12
34	A Game-Theoretic Approach to Jamming Attacks on Remote State Estimation in Cyber-Physical Systems. , 2016, , 3-30.		1
35	Fake-acknowledgment attack on ACK-based sensor power schedule for remote state estimation. , 2015, , .		9
36	Data-driven power control for state estimation: A Bayesian inference approach. Automatica, 2015, 54, 332-339.	5.0	34

#	ARTICLE	IF	CITATIONS
37	Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach. IEEE Transactions on Automatic Control, 2015, 60, 2831-2836.	5.7	346
38	Transmission Power Scheduling for Energy Harvesting Sensor in Remote State Estimation. IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2014, 47, 122-127.	0.4	7
39	Multi-sensor transmission power scheduling for remote state estimation under SINR model. , 2014, , .		14
40	Jamming attack on Cyber-Physical Systems: A game-theoretic approach. , 2013, , .		28
41	Optimal Periodic Transmission Power Schedules for Remote Estimation of ARMA Processes. IEEE Transactions on Signal Processing, 2013, 61, 6164-6174.	5.3	54
42	Online sensor transmission power schedule for remote state estimation. , 2013, , .		18