

AndrÃ© M H Teixeira

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/234939/publications.pdf>

Version: 2024-02-01

63
papers

3,672
citations

566801

15
h-index

454577

30
g-index

63
all docs

63
docs citations

63
times ranked

2592
citing authors

#	ARTICLE	IF	CITATIONS
1	A Switching Multiplicative Watermarking Scheme for Detection of Stealthy Cyber-Attacks. IEEE Transactions on Automatic Control, 2021, 66, 2558-2573.	3.6	34
2	Security Metrics for Control Systems. Lecture Notes in Control and Information Sciences, 2021, , 99-121.	0.6	2
3	Introduction to the Book. Lecture Notes in Control and Information Sciences, 2021, , 1-8.	0.6	0
4	Detection of Cyber-Attacks: A Multiplicative Watermarking Scheme. Lecture Notes in Control and Information Sciences, 2021, , 173-201.	0.6	4
5	Bayesian network model to distinguish between intentional attacks and accidental technical failures: a case study of floodgates. Cybersecurity, 2021, 4, .	3.1	6
6	Privatized Distributed Anomaly Detection for Large-Scale Nonlinear Uncertain Systems. IEEE Transactions on Automatic Control, 2021, 66, 5299-5313.	3.6	4
7	Stealthy Cyber-Attack Design Using Dynamic Programming. , 2021, , .		3
8	Design of multiplicative watermarking against covert attacks. , 2021, , .		2
9	Security measure allocation for industrial control systems: Exploiting systematic search techniques and submodularity. International Journal of Robust and Nonlinear Control, 2020, 30, 4278-4302.	2.1	5
10	Actuator Security Indices Based on Perfect Undetectability: Computation, Robustness, and Sensor Placement. IEEE Transactions on Automatic Control, 2020, 65, 3816-3831.	3.6	17
11	Joint controller and detector design against data injection attacks on actuators. IFAC-PapersOnLine, 2020, 53, 7439-7445.	0.5	4
12	A Tutorial Introduction to Security and Privacy for Cyber-Physical Systems. , 2019, , .		73
13	Combining Bayesian Networks and Fishbone Diagrams to Distinguish Between Intentional Attacks and Accidental Technical Failures. Lecture Notes in Computer Science, 2019, , 31-50.	1.0	3
14	Effects of Jamming Attacks on a Control System With Energy Harvesting. , 2019, 3, 829-834.		6
15	Data Injection Attacks against Feedforward Controllers. , 2019, , .		0
16	Optimal stealthy attacks on actuators for strictly proper systems. , 2019, , .		7
17	On the Confidentiality of Linear Anomaly Detector States. , 2019, , .		2
18	Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation. IEEE Transactions on Smart Grid, 2019, 10, 3044-3056.	6.2	71

#	ARTICLE	IF	CITATIONS
19	Distributed Sensor and Actuator Reconfiguration for Fault-Tolerant Networked Control Systems. IEEE Transactions on Control of Network Systems, 2018, 5, 1517-1528.	2.4	15
20	Differentially-Private Distributed Fault Diagnosis for Large-Scale Nonlinear Uncertain Systems. IFAC-PapersOnLine, 2018, 51, 975-982.	0.5	5
21	Detection of Sensor Data Injection Attacks with Multiplicative Watermarking. , 2018, , .		10
22	Estimation With Strategic Sensors. IEEE Transactions on Automatic Control, 2017, 62, 724-739.	3.6	44
23	Voltage Control in Distributed Generation under Measurement Falsification Attacks * *This work is sponsored by Chinese Scholarship Council (CSC). IFAC-PapersOnLine, 2017, 50, 8379-8384.	0.5	7
24	Bayesian Network Models in Cyber Security: A Systematic Review. Lecture Notes in Computer Science, 2017, , 105-122.	1.0	25
25	Detection and isolation of routing attacks through sensor watermarking. , 2017, , .		18
26	Detection and Isolation of Replay Attacks through Sensor Watermarking * *This work has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 608224 and from H2020 Programme under grant no. 707546 (SURE).. IFAC-PapersOnLine, 2017, 50, 7363-7368.	0.5	44
27	Co-simulation for cyber security analysis: Data attacks against energy management system. , 2017, , .		20
28	Data attacks on power system state estimation: Limited adversarial knowledge vs. limited attack resources. , 2017, , .		6
29	Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. Lecture Notes in Computer Science, 2017, , 50-62.	1.0	26
30	Combined data integrity and availability attacks on state estimation in cyber-physical power grids. , 2016, , .		9
31	Cybersecurity as a Politikum. , 2016, , .		5
32	From control system security indices to attack identifiability. , 2016, , .		16
33	Cyber-Physical-Security Framework for Building Energy Management System. , 2016, , .		15
34	The ADMM Algorithm for Distributed Quadratic Problems: Parameter Selection and Constraint Preconditioning. IEEE Transactions on Signal Processing, 2016, 64, 290-305.	3.2	26
35	Cyber-Secure and Resilient Architectures for Industrial Control Systems. , 2015, , 149-183.		5
36	Strategic stealthy attacks: The output-to-output $\hat{\sigma}_2$ -gain. , 2015, , .		14

#	ARTICLE	IF	CITATIONS
37	Secure Control Systems: A Quantitative Risk Management Approach. IEEE Control Systems, 2015, 35, 24-45.	1.0	226
38	Voltage control for interconnected microgrids under adversarial actions. , 2015, , .		31
39	A secure control framework for resource-limited adversaries. Automatica, 2015, 51, 135-148.	3.0	833
40	Optimal Parameter Selection for the Alternating Direction Method of Multipliers (ADMM): Quadratic Problems. IEEE Transactions on Automatic Control, 2015, 60, 644-658.	3.6	342
41	The ADMM algorithm for distributed averaging: Convergence rates and optimal parameter selection. , 2014, , .		7
42	Distributed coordination of household electricity consumption. , 2014, , .		0
43	A down-sampled controller to reduce network usage with guaranteed closed-loop performance. , 2014, , .		15
44	Distributed Fault Detection and Isolation Resilient to Network Model Uncertainties. IEEE Transactions on Cybernetics, 2014, 44, 2024-2037.	6.2	131
45	Gaussian cheap talk game with quadratic cost functions: When herding between strategic senders is a virtue. , 2014, , .		10
46	Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures. , 2014, , .		47
47	Optimal scaling of the ADMM algorithm for distributed quadratic programming. , 2013, , .		18
48	Distributed actuator reconfiguration in networked control systems*. IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2013, 46, 61-68.	0.4	10
49	Quantifying Cyber-Security for Networked Control Systems. Lecture Notes in Control and Information Sciences, 2013, , 123-142.	0.6	16
50	Distributed Fault Detection and Isolation with imprecise network models. , 2012, , .		9
51	Revealing stealthy attacks in control systems. , 2012, , .		189
52	Optimal power flow: Closing the loop over corrupted data. , 2012, , .		20
53	Attack models and scenarios for networked control systems. , 2012, , .		315
54	On the Optimal Step-size Selection for the Alternating Direction Method of Multipliers. IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2012, 45, 139-144.	0.4	14

#	ARTICLE	IF	CITATIONS
55	Fault Detection and Mitigation in Kirchhoff Networks. IEEE Signal Processing Letters, 2012, 19, 749-752.	2.1	3
56	Agents misbehaving in a network: a vice or a virtue?. IEEE Network, 2012, 26, 35-40.	4.9	15
57	Cyber-security of SCADA systems. , 2012, , .		10
58	A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator*. IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2011, 44, 11271-11277.	0.4	56
59	Distributed fault detection for interconnected second-order systems. Automatica, 2011, 47, 2757-2764.	3.0	357
60	Dynamical system decomposition using dissipation inequalities. , 2011, , .		6
61	Distributed Leader Selection without Direct Inter-agent Communication. IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2010, 43, 221-226.	0.4	10
62	Networked control systems under cyber attacks with applications to power networks. , 2010, , .		153
63	Cyber security analysis of state estimators in electric power systems. , 2010, , .		276