False data injection attacks against state estimation in e

ACM Transactions on Information and System Security

14, 1-33

DOI: 10.1145/1952982.1952995

Citation Report

#	Article	IF	Citations
1	A passivity-based framework for composing attacks on networked control systems. , 2012, , .		9
2	Power flow cyber attacks and perturbation-based defense. , 2012, , .		59
3	A game theoretic approach for adversarial pipeline monitoring using Wireless Sensor Networks. , 2012, , .		3
4	SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures. IEEE Transactions on Smart Grid, 2012, 3, 1790-1799.	6.2	155
5	Topology Perturbation for Detecting Malicious Data Injection. , 2012, , .		68
6	Monitoring and Optimization for Power Grids: A Signal Processing Perspective. IEEE Signal Processing Magazine, 2013, 30, 107-128.	4.6	207
7	Jamming attack on Cyber-Physical Systems: A game-theoretic approach. , 2013, , .		28
8	TSB: Trusted sensing base for the power grid. , 2013, , .		2
9	Robust collaborative state estimation for smart grid monitoring. , 2013, , .		1
10	Robust Decentralized State Estimation and Tracking for Power Systems via Network Gossiping. IEEE Journal on Selected Areas in Communications, 2013, 31, 1184-1194.	9.7	51
11	Confidentiality-preserving obfuscation for cloud-based power system contingency analysis. , 2013, , .		8
12	Automated scheduling of deferrable PEV/PHEV load by power-profile unevenness. , 2013, , .		2
13	Distributed state estimation with lossy measurement compression in smart grid. , 2013, , .		1
14	Clustering of smart meter data for disaggregation. , 2013, , .		16
15	Blind topology identification for power systems. , 2013, , .		43
16	Cyber physical system approach for design of power grids: A survey. , 2013, , .		43
17	Impact analysis of transient stability due to cyber attack on FACTS devices. , 2013, , .		18
18	Modeling and verification of security properties for critical infrastructure protection. , 2013, , .		1

#	Article	IF	Citations
19	Addressing the challenges of anomaly detection for cyber physical energy grid systems. , 2013, , .		5
20	Malicious data detection in state estimation leveraging system losses &amp;amp; estimation of perturbed parameters. , 2013, , .		9
21	Fundamental limits of cyber-physical security in smart power grids. , 2013, , .		8
22	Analysis of Optimal False Data Injection Attacks in Unmanned Aerial Systems. , 2013, , .		2
23	Secure Detection Using Binary Sensors. IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2013, 46, 160-167.	0.4	1
24	Confirmation of Theoretical Results Regarding Control Theoretic Cyber Attacks on Controllers. IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2013, 46, 702-707.	0.4	4
25	Improving Wiki Article Quality Through Crowd Coordination. International Journal on Semantic Web and Information Systems, 2013, 9, 105-125.	2.2	6
26	Grid topology identification using electricity prices. , 2014, , .		35
27	Cyber-secure communication architecture for active power distribution networks. , 2014, , .		12
28	Software/Hardware-in-the-Loop Analysis of Cyberattacks on Unmanned Aerial Systems. Journal of Aerospace Information Systems, 2014, 11, 337-343.	1.0	15
29	Identification of &amp;#x201C;unobservable&amp;#x201D; cyber data attacks on power grids. , 2014, , .		5
30	Detecting, locating, &amp;amp; quantifying false data injections utilizing grid topology through optimized D-FACTS device placement. , 2014, , .		5
31	Stealthy attacks in power systems: Limitations on manipulating the estimation deviations caused by switching network topologies. , 2014, , .		1
32	Under the radar attacks in dynamical systems: Adversarial privacy utility tradeoffs. , 2014, , .		2
33	Controller-aware false data injection against programmable logic controllers. , 2014, , .		14
34	A secure distributed consensus scheme for wireless sensor networks against data falsification. , 2014, , .		0
35	Effective measurement design for cyber security. , 2014, , .		3
36	Energy price matrix factorization. , 2014, , .		0

#	Article	IF	Citations
37	Control Systems for the Power Grid and Their Resiliency to Attacks. IEEE Security and Privacy, 2014, 12, 15-23.	1.5	12
38	False Logic Attacks on SCADA Control System. , 2014, , .		4
39	Moving Target Defense for Hardening the Security of the Power System State Estimation. , 2014, , .		65
40	Resilient distributed parameter estimation in heterogeneous time-varying networks. , 2014, , .		21
41	Security Threat Analytics and Countermeasure Synthesis for Power System State Estimation. , 2014, , .		10
42	On Kalman filtering in the presence of a compromised sensor: Fundamental performance bounds. , 2014, , .		45
43	An abrupt change detection heuristic with applications to cyber data attacks on power systems. , 2014, , .		10
44	Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter. IEEE Transactions on Control of Network Systems, 2014, 1, 370-379.	2.4	560
45	Attacks/faults detection and isolation in the Smart Grid using Kalman Filter. , 2014, , .		6
46	On detection of cyber attacks against voltage control in distribution power grids. , 2014, , .		11
47	Extended Distributed State Estimation: A Detection Method against Tolerable False Data Injection Attacks in Smart Grids. Energies, 2014, 7, 1517-1538.	1.6	71
48	Security concepts for the dynamics of autonomous vehicle networks. Automatica, 2014, 50, 852-857.	3.0	58
49	On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures. IEEE Transactions on Parallel and Distributed Systems, 2014, 25, 717-729.	4.0	326
50	A Reputation-Based Secure Distributed Control Methodology in D-NCS. IEEE Transactions on Industrial Electronics, 2014, 61, 6294-6303.	5.2	40
51	Resilient Distributed Control in the Presence of Misbehaving Agents in Networked Control Systems. IEEE Transactions on Cybernetics, 2014, 44, 2038-2049.	6.2	113
52	Impact Analysis of Topology Poisoning Attacks on Economic Operation of the Smart Power Grid. , 2014, , .		29
53	Adversary dynamics and smart grid security: A multiagent system approach. , 2014, , .		4
54	Combating False Data Injection Attacks in Smart Grid using Kalman Filter. , 2014, , .		23

#	Article	IF	Citations
55	A formal model for verifying the impact of stealthy attacks on optimal power flow in power grids. , 2014, , .		28
56	Phasor measurement unit selection for unobservable electric power data integrity attack detection. International Journal of Critical Infrastructure Protection, 2014, 7, 155-164.	2.9	25
57	Stealthy false data injection attacks against state estimation in power systems: Switching network topologies. , 2014, , .		15
58	Privacy-Preserving Power Request in Smart Grid Networks. IEEE Systems Journal, 2014, 8, 441-449.	2.9	31
59	Qualitative Behavioral Analyzer for Fault Detection and Cyber Security of Control Networks. , 2014, , .		0
60	Towards Efficient and Secured Real-Time Pricing in the Smart Grid. , 2014, , .		0
61	Online Monitoring of a Cyber Physical System Against Control Aware Cyber Attacks. Procedia Computer Science, 2015, 70, 238-244.	1.2	10
62	Towards Efficient and Secured Real-Time Pricing in the Smart Grid. , 2015, , .		2
63	Economic impact of data integrity attacks on distributed DC optimal power flow algorithm. , 2015, , .		14
64	Complete observation against attack vulnerability for cyber-physical systems with application to power grids. , 2015, , .		4
65	Smart grid data injection attacks: To defend or not?. , 2015, , .		10
66	Matrix partition-based detection scheme for false data injection in smart grid. International Journal of Wireless and Mobile Computing, 2015, 9, 250.	0.1	2
67	False Data Injection Attacks and detection scenarios in the power system. , 2015, , .		1
68	Efficient solution of large sparse linear systems in modern hardware. , 2015, , .		1
69	Cyber Risk Assessment of Transmission Lines in Smart Grids. Energies, 2015, 8, 13796-13810.	1.6	9
70	A Study of Sparse Matrix Methods on New Hardware. International Journal of Monitoring and Surveillance Technologies Research, 2015, 3, 1-19.	0.3	0
71	Secure Communications in Smart Grid: Networking and Protocols. , 2015, , 113-148.		8
72	Security Challenges in Smart Grid Implementation. SpringerBriefs in Cybersecurity, 2015, , 1-39.	0.2	28

#	Article	IF	Citations
73	Joint Cyber and Physical Attacks on Power Grids. , 2015, , .		21
75	Empirical Development of a Trusted Sensing Base for Power System Infrastructures. IEEE Transactions on Smart Grid, 2015, 6, 2454-2463.	6.2	10
76	Likelihood of cyber data injection attacks to power systems. , 2015, , .		3
77	Fake-acknowledgment attack on ACK-based sensor power schedule for remote state estimation. , 2015, , .		9
78	Data Framing Attacks against Nonlinear State Estimation in Smart Grid. , 2015, , .		3
79	Stealthy control signal attacks in scalar LQG systems. , 2015, , .		4
80	Automated vulnerability analysis of AC state estimation under constrained false data injection in electric power systems. , 2015, , .		15
81	Defending against Energy Dispatching Data integrity attacks in smart grid. , 2015, , .		1
82	Observability of linear systems under adversarial attacks. , 2015, , .		151
83	An algebraic detection approach for control systems under multiple stochastic cyber-attacks. IEEE/CAA Journal of Automatica Sinica, 2015, 2, 258-266.	8.5	10
84	A controller design method for unidentifiable linear SISO systems. , 2015, , .		0
85	Some discussions about data in the new environment of power systems. , 2015, , .		0
86	Towards resilient cyber-physical control systems. , 2015, , .		2
87	Cybersecurity for product lifecycle management a research roadmap. , 2015, , .		2
88	Robust fault detection of linearized power grid network system. , 2015, , .		0
89	Response and reconfiguration of cyber-physical control systems: A survey. , 2015, , .		28
90	Robust fault diagnosis of power grid network system. , 2015, , .		2
91	Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication. IEEE Transactions on Smart Grid, 2015, , 1-10.	6.2	27

#	Article	IF	Citations
92	Security in stochastic control systems: Fundamental limitations and performance bounds. , 2015, , .		75
93	An intrusion-resilient distributed optimization algorithm for modal estimation in power systems. , 2015, , .		9
94	Securing DC and hybrid microgrids. , 2015, , .		5
95	Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems. IEEE Control Systems, 2015, 35, 110-127.	1.0	286
96	Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs. IEEE Control Systems, 2015, 35, 93-109.	1.0	349
97	Detection of false data injection attacks in smart-grid systems. , 2015, 53, 206-213.		88
98	A Real-Time Attack Localization Algorithm for Large Power System Networks Using Graph-Theoretic Techniques. IEEE Transactions on Smart Grid, 2015, 6, 2551-2559.	6.2	33
99	Dynamic load altering attacks in smart grid. , 2015, , .		46
100	Detecting Malicious Data Injections in Event Detection Wireless Sensor Networks. IEEE Transactions on Network and Service Management, 2015, 12, 496-510.	3.2	31
101	Statistical Structure Learning to Ensure Data Integrity in Smart Grid. IEEE Transactions on Smart Grid, 2015, 6, 1924-1933.	6.2	54
102	Detection of False Data Injection Attacks in Smart Grid Communication Systems. IEEE Signal Processing Letters, 2015, 22, 1652-1656.	2.1	186
103	Risk-Sensitive Control Under Markov Modulated Denial-of-Service (DoS) Attack Strategies. IEEE Transactions on Automatic Control, 2015, 60, 3299-3304.	3.6	189
104	A Low-Rank Matrix Approach for the Analysis of Large Amounts of Power System Synchrophasor Data. , 2015, , .		31
105	Information-Theoretic Security in Stochastic Control Systems. Proceedings of the IEEE, 2015, 103, 1914-1931.	16.4	20
106	Secure detection with correlated binary sensors. , 2015, , .		0
107	Modeling security policies for mitigating the risk of load altering attacks on smart grid systems. , 2015, , .		1
108	A new method for detection of fake data in measurements at smart grids state estimation. IET Science, Measurement and Technology, 2015, 9, 765-773.	0.9	4
109	A resilient distributed energy management algorithm for economic dispatch in the presence of misbehaving generation units. , 2015, , .		2

#	Article	IF	Citations
110	Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks. , 2015, , .		2
111	Power system adequacy assessment with load redistribution attacks. , 2015, , .		4
112	A comprehensive assessment of cloud computing for smart grid applications: A multi-perspectives framework. , 2015, , .		10
113	Smart grid data integrity attacks: Observable islands. , 2015, , .		5
114	Integrity Attacks on Real-Time Pricing in Electric Power Grids. ACM Transactions on Information and System Security, 2015, 18, 1-33.	4.5	25
115	Optimum node selection for protection under power grid state estimation. , 2015, , .		0
116	Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: Observer-based combinatorial approach. , 2015, , .		34
117	Enabling the big data analysis in the smart grid. , 2015, , .		16
118	On false data injection attacks against the dynamic microgrid partition in the smart grid. , 2015, , .		18
119	A game-theoretic approach to optimal defense strategy against load redistribution attack. , 2015, , .		3
120	Using spy node to identify cyber-attack in power systems as a novel approach. , 2015, , .		2
121	Distributed Real-Time Anomaly Detection in Networked Industrial Sensing Systems. IEEE Transactions on Industrial Electronics, 2015, 62, 3832-3842.	5.2	107
122	Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid. Information Systems, 2015, 53, 201-212.	2.4	73
123	EAPA: An efficient authentication protocol against pollution attack for smart grid. Peer-to-Peer Networking and Applications, 2015, 8, 1082-1089.	2.6	10
124	Abnormal traffic-indexed state estimation: A cyberâ€"physical fusion approach for Smart Grid attack detection. Future Generation Computer Systems, 2015, 49, 94-103.	4.9	77
125	A Secure Scheme for Distributed Consensus Estimation against Data Falsification in Heterogeneous Wireless Sensor Networks. Sensors, 2016, 16, 252.	2.1	6
126	Resilient decentralized consensus-based state estimation for smart grid in presence of false data. , 2016, , .		21
127	Improved protection scheme for data attack on strategic buses in the Smart Grid. , 2016, , .		1

#	Article	IF	Citations
128	Identifying covert data-manipulators in power system estimation loops. , 2016, , .		4
129	Joint cyber and physical attacks against topology of electric grids. , 2016, , .		1
130	Securing Power System State Estimation. , 2016, , .		1
131	Detection of false data injection attacks in smart grid under colored Gaussian noise. , 2016, , .		28
132	Resilient distribution grids â€" cyber threat scenarios and test environment. , 2016, , .		8
133	Zero-stealthy attack for sampled-data control systems: The case of faster actuation than sensing. , 2016, , .		10
134	Undetectable sensor and actuator attacks for observer based controlled Cyber-Physical Systems. , 2016, , .		4
135	Cyberâ€physical attacks and defences in the smart grid: a survey. IET Cyber-Physical Systems: Theory and Applications, 2016, 1, 13-27.	1.9	332
136	Impact of network topology optimization on power system reliability. , 2016, , .		4
137	Estimation of smart grid topology using SCADA measurements. , 2016, , .		11
138	A Brief Survey of Security Approaches for Cyber-Physical Systems. , 2016, , .		23
139	A new framework of electrical cyber physical systems. , 2016, , .		1
140	Limiting the Impact of Stealthy Attacks on Industrial Control Systems. , 2016, , .		214
141	Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors. , 2016, , .		17
142	Electric vehicle technology as an exploit for cyber attacks on the next generation of electric power systems. , 2016, , .		14
143	Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems. , 2016, , .		16
144	A Resilient Algorithm for Power System Mode Estimation using Synchrophasors. , 2016, , .		4
145	Worst-case analysis of innovation-based linear attack on remote state estimation with resource constraint. , 2016, , .		10

#	Article	IF	Citations
146	Stealthy control signal attacks in vector LQG systems. , 2016, , .		9
147	Protecting critical buses in power-grid against data attacks: Adaptive protection schemes for smart cities. , 2016, , .		0
148	A Round-Robin ADMM algorithm for identifying data-manipulators in power system estimation. , 2016, , .		2
149	Multi-agent System for Detecting False Data Injection Attacks Against the Power Grid. , 2016, , .		4
150	Bid Modification Attack in Smart Grid for Monetary Benefits. , 2016, , .		5
151	Stochastic Detector against linear deception attacks on remote state estimation. , 2016, , .		12
152	Anomaly detection in diurnal CPS monitoring data using a local density approach. , 2016, , .		1
153	Data integrity attacks against the distributed real-time pricing in the smart grid. , 2016, , .		10
154	On modeling of electrical cyber-physical systems considering cyber security. Frontiers of Information Technology and Electronic Engineering, 2016, 17, 465-478.	1.5	43
155	Data-Driven Stealthy Injection Attacks on Smart Grid with Incomplete Measurements. Lecture Notes in Computer Science, 2016, , 180-192.	1.0	22
156	Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective. IEEE Transactions on Smart Grid, 2016, 7, 2038-2049.	6.2	109
158	Energy Big Data Analytics and Security: Challenges and Opportunities. IEEE Transactions on Smart Grid, 2016, 7, 2423-2436.	6.2	172
159	Power system static state estimation using a least winsorized square robust estimator. Neurocomputing, 2016, 207, 457-468.	3.5	20
160	Study on Tradeoffs in Detection of Malicious Data Injections in Wireless Sensor Networks. Procedia Technology, 2016, 25, 378-383.	1.1	0
161	A study of packet-reordering integrity attack on remote state estimation. , 2016, , .		4
162	Detecting and Isolating Attacks of Deception in Networked Control Systems. , 2016, , .		5
163	Recovery after attacks of deception on Networked Control Systems. , 2016, , .		5
164	Vulnerabilities in two-area Automatic Generation Control systems under cyberattack. , 2016, , .		12

#	Article	IF	Citations
165	Feasibility and mitigation of false data injection attacks in smart grid. , 2016, , .		9
166	Towards a unified resilience analysis: State estimation against integrity attacks. , 2016, , .		5
167	Investigating the impact of intrusion detection system performance on communication latency and power system stability. , 2016, , .		3
168	Impact analysis of false data injection attacks on power system static security assessment. Journal of Modern Power Systems and Clean Energy, 2016, 4, 496-505.	3.3	58
169	A Game-Theoretic Approach to Jamming Attacks on Remote State Estimation in Cyber-Physical Systems. , 2016, , 3-30.		1
170	A Game-Theoretic Approach to Jamming Attacks on Remote State Estimation in Cyber-Physical Systems. , 2016, , 13-40.		0
171	Detection of cyber attacks with access to partial data in power system using spy nodes. , 2016, , .		1
172	Data integrity attack in smart grid: optimised attack to gain momentary economic profit. IET Generation, Transmission and Distribution, 2016, 10, 4032-4039.	1.4	24
173	A Case Study on Implementing False Data Injection Attacks Against Nonlinear State Estimation. , 2016, , .		31
174	Cyber attacks, detection and protection in smart grid state estimation. , 2016, , .		10
175	Bad data detection for smart grid state estimation. , 2016, , .		4
176	Quantifying the influence of local load redistribution attack on power supply adequacy. , 2016, , .		2
177	A polynomial-time method to find the sparsest unobservable attacks in power networks. , 2016, , .		1
178	Adaptive cyberâ€physical system attack detection and reconstruction with application to power systems. IET Control Theory and Applications, 2016, 10, 1458-1468.	1.2	128
179	Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation. IEEE Transactions on Smart Grid, 2016, , 1-1.	6.2	158
180	Identification of Successive â€œUnobservableâ€• Cyber Data Attacks in Power Systems Through Matrix Decomposition. IEEE Transactions on Signal Processing, 2016, 64, 5557-5570.	3.2	45
181	Investigation of control theoretic cyber attacks on controllers. International Journal of Systems, Control and Communications, 2016, 7, 273.	0.2	2
182	Compensation of attacks on consensus networks. , 2016, , .		1

#	Article	IF	Citations
183	Power grid resilience against false data injection attacks. , 2016, , .		12
184	On Attacker Models and Profiles for Cyber-Physical Systems. Lecture Notes in Computer Science, 2016, , 427-449.	1.0	48
185	On identifying vulnerable nodes for power systems in the presence of undetectable cyber-attacks. , 2016, , .		5
186	Detection of false data attacks in smart grid with supervised learning. , 2016, , .		74
187	IA<sup>2</sup>P: Intrusion-Tolerant Malicious Data Injection Attack Analysis and Processing in Traffic Flow Data Collection Based on VANETs. International Journal of Distributed Sensor Networks, 2016, 12, 5159739.	1.3	2
188	Attack path reconstruction from adverse consequences on power grids with a focus on Monitoring-Layer attacks. , 2016, , .		2
189	A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids. , 2016, , .		44
190	Power System Reliability Evaluation Considering Load Redistribution Attacks. IEEE Transactions on Smart Grid, 2016, , 1-1.	6.2	50
191	A comprehensive overview of cyber-physical systems: from perspective of feedback system. IEEE/CAA Journal of Automatica Sinica, 2016, 3, 1-14.	8.5	85
192	DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System. IEEE Transactions on Information Forensics and Security, 2016, 11, 2415-2425.	4.5	70
193	Forecasting-Aided Imperfect False Data Injection Attacks Against Power System Nonlinear State Estimation. IEEE Transactions on Smart Grid, 2016, 7, 6-8.	6.2	81
194	BLITHE: Behavior Rule-Based Insider Threat Detection for Smart Grid. IEEE Internet of Things Journal, 2016, 3, 190-205.	5.5	33
195	Enabling multi-layer cyber-security assessment of Industrial Control Systems through Hardware-In-The-Loop testbeds. , 2016, , .		9
196	Security Assessment of Time Synchronization Mechanisms for the Smart Grid. IEEE Communications Surveys and Tutorials, 2016, 18, 1952-1973.	24.8	32
197	Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems. IEEE Transactions on Smart Grid, 2016, 7, 2260-2272.	6.2	185
198	Security system architecture for data integrity based on a virtual smart meter overlay in a smart grid system. Soft Computing, 2016, 20, 1829-1840.	2.1	4
199	Line Outage Localization Using Phasor Measurement Data in Transient State. IEEE Transactions on Power Systems, 2016, 31, 3019-3027.	4.6	28
200	An Event-Triggered Approach to State Estimation for a Class of Complex Networks With Mixed Time Delays and Nonlinearities. IEEE Transactions on Cybernetics, 2016, 46, 2497-2508.	6.2	178

#	Article	IF	Citations
201	Online Energy Price Matrix Factorization for Power Grid Topology Tracking. IEEE Transactions on Smart Grid, 2016, 7, 1239-1248.	6.2	41
202	Transmission Line Rating Attack in Two-Settlement Electricity Markets. IEEE Transactions on Smart Grid, 2016, 7, 1346-1355.	6.2	48
203	Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids With PVs. IEEE Transactions on Smart Grid, 2016, 7, 1824-1835.	6.2	118
204	On Data Integrity Attacks Against Real-Time Pricing in Energy-Based Cyber-Physical Systems. IEEE Transactions on Parallel and Distributed Systems, 2017, 28, 170-187.	4.0	36
205	Effects of Switching Network Topologies on Stealthy False Data Injection Attacks Against State Estimation in Power Networks. IEEE Systems Journal, 2017, 11, 2640-2651.	2.9	25
206	Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks. IEEE Transactions on Smart Grid, 2017, 8, 1580-1590.	6.2	161
207	Dynamic Games With Asymmetric Information and Resource Constrained Players With Applications to Security of Cyberphysical Systems. IEEE Transactions on Control of Network Systems, 2017, 4, 71-81.	2.4	31
208	Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. Journal of Computer and System Sciences, 2017, 83, 58-72.	0.9	63
209	Optimal Linear Cyber-Attack on Remote State Estimation. IEEE Transactions on Control of Network Systems, 2017, 4, 4-13.	2.4	324
210	A Review of False Data Injection Attacks Against Modern Power Systems. IEEE Transactions on Smart Grid, 2017, 8, 1630-1638.	6.2	652
211	Secure and efficient protection of consumer privacy in Advanced Metering Infrastructure supporting fine-grained data analysis. Journal of Computer and System Sciences, 2017, 83, 84-100.	0.9	16
212	Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids. IEEE Transactions on Industrial Informatics, 2017, 13, 2693-2703.	7.2	211
213	Improved sensor fault detection, isolation, and mitigation using multiple observers approach. Systems Science and Control Engineering, 2017, 5, 70-96.	1.8	14
214	Stealthy Control Signal Attacks in Linear Quadratic Gaussian Control Systems: Detectability Reward Tradeoff. IEEE Transactions on Information Forensics and Security, 2017, 12, 1555-1570.	4.5	58
215	Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. IEEE Transactions on Smart Grid, 2017, 8, 2505-2516.	6.2	580
216	A statistical unsupervised method against false data injection attacks: A visualization-based approach. Expert Systems With Applications, 2017, 84, 242-261.	4.4	53
217	Transient stability enhancement of power grid by neural network controlled BFCL considering cyber-attacks. , 2017, , .		4
218	Cyber-Physical Systems Securityâ€"A Survey. IEEE Internet of Things Journal, 2017, 4, 1802-1831.	5.5	672

#	Article	IF	Citations
219	Spatio-Temporal Correlations in Cyber-Physical Systems. , 2017, , .		2
220	Towards a framework for cyber attack impact analysis of electric cyber physical systems. , 2017, , .		4
221	A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities. Pervasive and Mobile Computing, 2017, 39, 52-64.	2.1	22
222	Physical Intrusion Gamesâ€"Optimizing Surveillance by Simulation and Game Theory. IEEE Access, 2017, 5, 8394-8407.	2.6	32
223	The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. IEEE Transactions on Power Systems, 2017, 32, 3317-3318.	4.6	783
224	Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs. Automatica, 2017, 82, 251-260.	3.0	160
225	Security of SCADA systems against cyberâ€"physical attacks. IEEE Aerospace and Electronic Systems Magazine, 2017, 32, 28-45.	2.3	84
226	En-Route Filtering Techniques in Wireless Sensor Networks: A Survey. Wireless Personal Communications, 2017, 96, 697-739.	1.8	18
227	SEDEA: State Estimation-Based Dynamic Encryption and Authentication in Smart Grid. IEEE Access, 2017, 5, 15682-15693.	2.6	23
228	Cybersecurity in Distributed Power Systems. Proceedings of the IEEE, 2017, 105, 1367-1388.	16.4	146
229	Confiscating Flight Control System by Stealthy Output Injection Attack. Journal of Aerospace Information Systems, 2017, 14, 203-213.	1.0	6
230	Delayed unknown input observers for discrete-time linear systems with guaranteed performance. Systems and Control Letters, 2017, 103, 9-15.	1.3	28
231	Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. Journal of Parallel and Distributed Computing, 2017, 103, 32-41.	2.7	109
232	Minimum Sparsity of Unobservable Power Network Attacks. IEEE Transactions on Automatic Control, 2017, 62, 3354-3368.	3.6	27
233	Analysis of Consensus-Based Distributed Economic Dispatch Under Stealthy Attacks. IEEE Transactions on Industrial Electronics, 2017, 64, 5107-5117.	5.2	107
234	Biâ€level modelling of false data injection attacks on security constrained optimal power flow. IET Generation, Transmission and Distribution, 2017, 11, 3586-3593.	1.4	33
236	Kalman filter with diffusion strategies for detecting power grid false data injection attacks. , 2017, , .		11
237	Cascading Failure Attacks in the Power System: A Stochastic Game Perspective. IEEE Internet of Things Journal, 2017, 4, 2247-2259.	5.5	53

#	Article	IF	Citations
238	Hidden Moving Target Defense in Smart Grids. , 2017, , .		17
239	Cyber-Physical Security and Privacy in the Electric Smart Grid. Synthesis Lectures on Information Security Privacy and Trust, 2017, 9, 1-64.	0.3	9
240	A brief overview on secure control of networked systems. Advances in Manufacturing, 2017, 5, 243-250.	3.2	8
241	Achieving Efficient Detection Against False Data Injection Attacks in Smart Grid. IEEE Access, 2017, 5, 13787-13798.	2.6	90
242	Towards a secure network architecture for smart grids in 5G era. , 2017, , .		21
243	Improvements to the Smart Energy Profile security. , 2017, , .		2
244	On the optimization of energy storage system placement for protecting power transmission grids against dynamic load altering attacks. , 2017, , .		14
245	Detecting Time Synchronization Attacks in Cyber-Physical Systems with Machine Learning Techniques. , 2017, , .		24
246	Cognitive radio testbed for Digital Beamforming of satellite communication. , 2017, , .		5
247	Impact of Cyber Attacks on Data Integrity in Transient Stability Control. , 2017, , .		2
248	A transient stability control adaptive to measurements uncertainties. , 2017, , .		1
250	Review of cyber attacks on power system operations. , 2017, , .		32
251	Replay attack detection in a multi agent system using stability analysis and loss effective watermarking. , 2017, , .		21
252	Strategic Trust in Cloud-Enabled Cyber-Physical Systems With an Application to Glucose Control. IEEE Transactions on Information Forensics and Security, 2017, 12, 2906-2919.	4.5	54
253	Attack-resilient estimation of switched nonlinear cyber-physical systems. , 2017, , .		15
254	Profiting from attacks on real-time price communications in smart grids. , 2017, , .		3
255	Coupling analysis-based false monitoring information identification of production system in process industry. Science China Technological Sciences, 2017, 60, 807-817.	2.0	3
256	Controls for Smart Grids: Architectures and Applications. Proceedings of the IEEE, 2017, 105, 2244-2261.	16.4	61

#	Article	IF	Citations
257	On the Impact of Cyber Attacks on Data Integrity in Storage-Based Transient Stability Control. IEEE Transactions on Industrial Informatics, 2017, 13, 3322-3333.	7.2	40
258	A Joint Data Compression and Encryption Approach for Wireless Energy Auditing Networks. ACM Transactions on Sensor Networks, 2017, 13, 1-32.	2.3	17
259	Stealthy Attacks in Dynamical Systems: Tradeoffs Between Utility and Detectability With Application in Anonymous Systems. IEEE Transactions on Information Forensics and Security, 2017, 12, 779-792.	4.5	9
260	Stealthy output injection attacks on control systems with bounded variables. International Journal of Control, 2017, 90, 1389-1402.	1.2	7
261	Consensus estimationâ€based target localization in underwater acoustic sensor networks. International Journal of Robust and Nonlinear Control, 2017, 27, 1607-1627.	2.1	47
262	Q-Learning-Based Vulnerability Analysis of Smart Grid Against Sequential Topology Attacks. IEEE Transactions on Information Forensics and Security, 2017, 12, 200-210.	4.5	185
263	Standardization and Security for Smart Grid Communications Based on Cognitive Radio Technologiesâ€"A Comprehensive Survey. IEEE Communications Surveys and Tutorials, 2017, 19, 423-445.	24.8	43
264	False Data Injection on State Estimation in Power Systemsâ€"Attacks, Impacts, and Defense: A Survey. IEEE Transactions on Industrial Informatics, 2017, 13, 411-423.	7.2	403
265	Robust Detection of Cyber Attacks on State Estimators Using Phasor Measurements. IEEE Transactions on Power Systems, 2017, 32, 2468-2470.	4.6	36
266	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.	1.6	39
267	Event-triggered resilient control of a class of cyber-physical systems under denial-of-service. , 2017, , .		6
268	PReSS towards a secure smart grid: Protection recommendations against smart spoofing. , 2017, , .		0
269	On detecting false data injection with limited network information using transformation based statistical techniques. , 2017, , .		8
270	A new watermarking approach for replay attack detection in LQG systems. , 2017, , .		23
271	Exploiting Submodularity in Security Measure Allocation for Industrial Control Systems. , 2017, , .		4
272	IoT-enabled distributed cyber-attacks on transmission and distribution grids. , 2017, , .		27
273	On the impact of empirical attack models targeting marine transportation. , 2017, , .		14
274	Compromising Security of Economic Dispatch in Power System Operations. , 2017, , .		12

#	Article	IF	Citations
275	Strong Structural Input and State Observability of LTV Network Systems with Multiple Unknown Inputs. IFAC-PapersOnLine, 2017, 50, 7357-7362.	0.5	6
276	Protecting Positive and Second-Order Systems against Undetectable Attacks * *This research is supported in part by the Hong Kong RGC under the grant number CityU 11260016, in part by Knut and Alice Wallenberg Foundation, Swedish Research Council, and Swedish Foundation for Strategic Research and in part by the Research Grants Council of Hong Kong Special Administrative Region, China, under the Theme-Based Research Scheme T23-701/14-N.. IFAC-PapersOnLine, 2017, 50, 8373-8378.	0.5	4
277	Analysis and Mitigation of Bias Injection Attacks Against a Kalman Filter * *This work was supported by the Swedish Civil Contingencies Agency through the CERCES project, the Swedish Research Council, Knut and Alice Wallenberg Foundation, and the Swedish Foundation for Strategic Research. IFAC-PapersOnLine, 2017, 50, 8393-8398.	0.5	14
278	Consequence Analysis of Innovation-based Integrity Attacks with Side Information on Remote State Estimation * *The work by Z. Guo and L. Shi is supported by an HKUST KTH Partnership FP804. The work by D. Shi is supported by Natural Science Foundation of China (61503027). The work by K.H. Johansson is supported by the Knut and Alice Wallenberg Foundation and the Swedish Research Council.. IFAC-PapersOnLine, 2017, 50, 8399-8404.	0.5	5
279	Watch Me, but Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations. , 2017, , .		64
280	Approximate Power Grid Protection Against False Data Injection Attacks. , 2017, , .		2
281	Communication systems and security issues in smart microgrids. , 2017, , .		11
282	Cross-Level Detection Framework for Attacks on Cyber-Physical Systems. Journal of Hardware and Systems Security, 2017, 1, 356-369.	0.8	5
283	False data injection attacks targeting DC model-based state estimation. , 2017, , .		7
284	Attack tolerant finite-time consensus for multi-agent networks. , 2017, , .		3
285	Recent advances on state estimation for power grids with unconventional measurements. IET Control Theory and Applications, 2017, 11, 3221-3232.	1.2	18
286	Using simulators to assess knowledge and behavior of â€œnoviceâ€•operators of critical infrastructure under cyberattack events. , 2017, , .		9
287	Physical Attestation in the Smart Grid for Distributed State Verification. , 2017, , .		5
288	Composite FDIA and topology attack on the electricity market. , 2017, , .		4
289	Securing networked control systems: Modeling attacks and defenses. , 2017, , .		9
290	Efficient detection of false data injection attacks on AC state estimation in smart grids. , 2017, , .		10
291	Resilient control under denial-of-service via dynamic event triggering. , 2017, , .		3
292	A game theoretic approach to analyze false data injection and detection in LQG system. , 2017, , .		6

#	Article	IF	Citations
293	A framework for modeling load redistribution attacks coordinating with switching attacks. , 2017, , .		2
294	Game theory for secure critical interdependent gas-power-water infrastructure. , 2017, , .		10
295	Context-aware local Intrusion Detection in SCADA systems: A testbed and two showcases. , 2017, , .		10
296	Vulnerability analysis of electrical cyber physical systems using a simulation platform. , 2017, , .		7
297	AC sparse modeling for false data injection attack on smart gird. , 2017, , .		2
298	Intrusion detection for stochastic task allocation in robot swarms. , 2017, , .		2
299	Detection of false data injection attack on load frequency control in distributed power systems. , 2017, , .		15
300	Active detection for exposing intelligent attacks in control systems. , 2017, , .		13
301	Resilient transactive control in microgrids under dynamic load altering attacks. , 2017, , .		6
302	Robust optimal protection strategy against false data injection attacks in power grids. , 2017, , .		3
303	F-DDIA: A Framework for Detecting Data Injection Attacks in Nonlinear Cyber-Physical Systems. Security and Communication Networks, 2017, 2017, 1-12.	1.0	3
304	Dynamic multi-arm bandit game based multi-agents spectrum sharing strategy design. , 2017, , .		5
305	Securing cyber-physical systems with adaptive commensurate response. , 2017, , .		7
306	A semidefinite programming relaxation under false data injection attacks against power grid AC state estimation. , 2017, , .		11
307	A secure communication architecture in the smart grid. , 2017, , .		3
308	Electric grid power flow model camouflage against topology leaking attacks. , 2017, , .		7
309	Toward a practical storage-based control scheme for transient stability applications. , 2017, , .		1
310	Physical watermarking for securing cyber physical systems via packet drop injections. , 2017, , .		8

#	Article	IF	Citations
311	A Bayesian Game-Theoretic Defense Strategy for False Data Injection Attacks in Smart Grid. , 2017, , .		1
313	Optimal Tree Construction Model for Cyber-Attacks to Wide Area Measurement Systems. IEEE Transactions on Smart Grid, 2018, 9, 25-34.	6.2	15
314	Secure and Resilient Industrial Control Systems. IEEE Design and Test, 2018, 35, 90-94.	1.1	11
315	Determining Resilience Gains From Anomaly Detection for Event Integrity in Wireless Sensor Networks. ACM Transactions on Sensor Networks, 2018, 14, 1-35.	2.3	8
316	Structural and Strongly Structural Input and State Observability of Linear Network Systems. IEEE Transactions on Control of Network Systems, 2018, 5, 2062-2072.	2.4	13
317	Security Challenges of Networked Control Systems. Studies in Systems, Decision and Control, 2018, , 77-95.	0.8	23
318	Novel Detection Scheme Design Considering Cyber Attacks on Load Frequency Control. IEEE Transactions on Industrial Informatics, 2018, 14, 1932-1941.	7.2	83
319	Finite time attack detection and supervised secure state estimation for CPSs with malicious adversaries. Information Sciences, 2018, 451-452, 67-82.	4.0	25
320	Smart grids security challenges: Classification by sources of threats. Journal of Electrical Systems and Information Technology, 2018, 5, 468-483.	1.2	164
321	False Data Injection Attacks on Networked Control Systems: A Stackelberg Game Analysis. IEEE Transactions on Automatic Control, 2018, 63, 3503-3509.	3.6	122
322	A Generalized False Data Injection Attacks Against Power System Nonlinear State Estimator and Countermeasures. IEEE Transactions on Power Systems, 2018, 33, 4868-4877.	4.6	132
323	Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. Proceedings of the IEEE, 2018, 106, 9-20.	16.4	174
324	Reservoir Computing Meets Smart Grids: Attack Detection Using Delayed Feedback Networks. IEEE Transactions on Industrial Informatics, 2018, 14, 734-743.	7.2	101
325	Identification of False Data Injection Attacks With Considering the Impact of Wind Generation and Topology Reconfigurations. IEEE Transactions on Sustainable Energy, 2018, 9, 1349-1364.	5.9	46
326	Worst-case stealthy innovation-based linear attack on remote state estimation. Automatica, 2018, 89, 117-124.	3.0	177
327	ARMET: Behavior-Based Secure and Resilient Industrial Control Systems. Proceedings of the IEEE, 2018, 106, 129-143.	16.4	31
328	Attack under Disguise. , 2018, , .		39
329	Reliable Control Policy of Cyber-Physical Systems Against a Class of Frequency-Constrained Sensor and Actuator Attacks. IEEE Transactions on Cybernetics, 2018, 48, 3432-3439.	6.2	97

#	Article	IF	Citations
330	AIâ€based approach to identify compromised meters in data integrity attacks on smart grid. IET Generation, Transmission and Distribution, 2018, 12, 1052-1066.	1.4	62
331	Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption. IEEE Access, 2018, 6, 24325-24339.	2.6	88
332	Designing Safe and Secure Industrial Control Systems: A Tutorial Review. IEEE Design and Test, 2018, 35, 73-88.	1.1	10
333	Model-based approach for cyber-physical attack detection in water distribution systems. Water Research, 2018, 139, 132-143.	5.3	63
334	Distributed Kalman filtering for robust state estimation over wireless sensor networks under malicious cyber attacks. , 2018, 78, 92-97.		28
335	Physical Attestation in the Smart Grid for Distributed State Verification. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 275-288.	3.7	8
336	A Cyber-Physical Control Framework for Transient Stability in Smart Grids. IEEE Transactions on Smart Grid, 2018, 9, 1205-1215.	6.2	95
337	Analyzing Locally Coordinated Cyber-Physical Attacks for Undetectable Line Outages. IEEE Transactions on Smart Grid, 2018, 9, 35-47.	6.2	71
338	Power Grid State Estimation Following a Joint Cyber and Physical Attack. IEEE Transactions on Control of Network Systems, 2018, 5, 499-512.	2.4	57
339	Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. IEEE Transactions on Smart Grid, 2018, 9, 2862-2872.	6.2	133
340	Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack. IEEE Transactions on Smart Grid, 2018, 9, 3543-3552.	6.2	67
341	Opportunities for Price Manipulation by Aggregators in Electricity Markets. IEEE Transactions on Smart Grid, 2018, 9, 5687-5698.	6.2	43
342	Detection Against Linear Deception Attacks on Multi-Sensor Remote State Estimation. IEEE Transactions on Control of Network Systems, 2018, 5, 846-856.	2.4	161
343	A Robustness-Oriented Power Grid Operation Strategy Considering Attacks. IEEE Transactions on Smart Grid, 2018, 9, 4248-4261.	6.2	23
344	A Class of Switching Exploits Based on Inter-Area Oscillations. IEEE Transactions on Smart Grid, 2018, 9, 4659-4668.	6.2	14
345	Generalized FDIA-Based Cyber Topology Attack With Application to the Australian Electricity Market Trading Mechanism. IEEE Transactions on Smart Grid, 2018, 9, 3820-3829.	6.2	68
346	Experimental Comparison of Multicast Authentication for Wide Area Monitoring Systems. IEEE Transactions on Smart Grid, 2018, 9, 4394-4404.	6.2	18
347	Causality Countermeasures for Anomaly Detection in Cyber-Physical Systems. IEEE Transactions on Automatic Control, 2018, 63, 386-401.	3.6	52

#	Article	IF	Citations
348	Enabling Sustainable Cyber Physical Security Systems through Neuromorphic Computing. IEEE Transactions on Sustainable Computing, 2018, 3, 112-125.	2.2	13
349	A Distributed Control Paradigm for Smart Grid to Address Attacks on Data Integrity and Availability. IEEE Transactions on Signal and Information Processing Over Networks, 2018, 4, 70-81.	1.6	23
350	Joint-Transformation-Based Detection of False Data Injection Attacks in Smart Grid. IEEE Transactions on Industrial Informatics, 2018, 14, 89-97.	7.2	113
351	Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems. Neurocomputing, 2018, 272, 571-583.	3.5	33
352	Benchmarking robustness of load forecasting models under data integrity attacks. International Journal of Forecasting, 2018, 34, 89-104.	3.9	97
353	Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks. IEEE Transactions on Signal and Information Processing Over Networks, 2018, 4, 48-59.	1.6	231
354	Adequacy evaluation of electric power grids considering substation cyber vulnerabilities. International Journal of Electrical Power and Energy Systems, 2018, 96, 368-379.	3.3	27
355	Analysis of Cyber-Physical Security in Electric Smart Grid : Survey and challenges. , 2018, , .		2
356	Crystal (ball). , 2018, , .		6
357	Distinguishing Between Cyber Injection and Faults Using Machine Learning Algorithms. , 2018, , .		7
358	Quantifying the Impact of Cyber-Attack Strategies for Control Systems Equipped With an Anomaly Detector. , 2018, , .		12
359	A Novel Sparse False Data Injection Attack Method in Smart Grids with Incomplete Power Network Information. Complexity, 2018, 2018, 1-16.	0.9	14
360	Going Dark. , 2018, , .		0
361	Detection of False Data Injection Attacks in Power Systems with Graph Fourier Transform. , 2018, , .		26
362	Highly Assured Safety and Security of e-Health Applications. , 2018, , .		3
363	Impact of GPS Spoofing on Synchrophasor Assisted Load Shedding. , 2018, , .		1
364	Hidden Moving Target Defense against False Data Injection in Distribution Network Reconfiguration. , 2018, , .		18
365	Impact of False Data Detection on Cloud Hosted Linear State Estimator Performance. , 2018, , .		1

#	Article	IF	Citations
366	AVAIL: Assured Volt-AmpÃ¨re Information Ledger. , 2018, , .		1
367	Cyberattack Detection in Intelligent Grids Using Non-linear Filtering. , 2018, , .		6
368	Cyber Attack Detection and Isolation for Smart Grids via Unknown Input Observer. , 2018, , .		12
369	Power System Equipment Cyber-Physical Risk Assessment Based on Architecture and Critical Clearing Time. , 2018, , .		5
370	An Efficient Data-Driven False Data Injection Attack in Smart Grids. , 2018, , .		6
371	A Survey on the Effects of False Data Injection Attack on Energy Market. , 2018, , .		3
372	Collaborative Attacks on Autonomous Vehicle Platooning. , 2018, , .		6
373	Incorporating Unidentifiable Cyberattacks into Power System Reliability Assessment. , 2018, , .		7
374	Local Identification of Sensor Attack and Distributed Resilient State Estimation for Linear Systems. , 2018, , .		10
375	A Multiplicative Coordinated Stealthy Attack and its Detection for Cyber Physical Systems. , 2018, , .		11
376	PAMA: A Proactive Approach to Mitigate False Data Injection Attacks in Smart Grids. , 2018, , .		9
377	Modelling and Countermeasures of False Data Injection Attacks Against State Estimation in Power Systems. , 2018, , .		0
378	Subset Level Detection of False Data Injection Attacks in Smart Grids. , 2018, , .		8
379	Secure Sensor Design for Resiliency of Control Systems Prior to Attack Detection. , 2018, , .		0
380	A Multi-Observer Approach for Attack Detection and Isolation of Discrete-Time Nonlinear Systems. , 2018, , .		3
381	Statistical Approach to Detection of Attacks for Stochastic Cyber-Physical Systems. IFAC-PapersOnLine, 2018, 51, 178-183.	0.5	4
382	A Robust Circle-criterion Observer-based Estimator for Discrete-time Nonlinear Systems in the Presence of Sensor Attacks. , 2018, , .		10
383	Cyber-Security Problems in Smart Grid Cyber Attacks Detecting Methods and Modelling Attack Scenarios on Electric Power Systems. , 2018, , .		7

#	Article	IF	Citations
384	Tuning Windowed Chi-Squared Detectors for Sensor Attacks. , 2018, , .		5
385	Event-Driven Synchronization of Lur'e System Subject to Cyber Attack. , 2018, , .		1
386	An integrated testbed for locally monitoring SCADA systems in smart grids. Energy Informatics, 2018, 1, .	1.4	13
387	Economic-Driven FDI Attack in Electricity Market. Lecture Notes in Computer Science, 2018, , 216-224.	1.0	1
388	Data-Driven False Data Injection Attacks on State Estimation in Smart Grid. , 2018, , .		2
389	Identification of the Attacker in Cyber-Physical Systems with an Application to Vehicular Platooning in Adversarial Environment. , 2018, , .		20
390	Is Machine Learning in Power Systems Vulnerable?. , 2018, , .		46
391	Comparing Kalman Filters and Observers for Power System Dynamic State Estimation With Model Uncertainty and Malicious Cyber Attacks. IEEE Access, 2018, 6, 77155-77168.	2.6	61
392	Establishing Data Integrity in Networks of Cyber-Physical Systems. , 2018, , .		2
393	A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. IEEE Access, 2018, 6, 78238-78259.	2.6	384
394	Securing industrial control system environments: the missing piece. Journal of Cyber Security Technology, 2018, 2, 131-163.	1.8	5
395	Deterministic En-Route Filtering of False Reports: A Combinatorial Design Based Approach. IEEE Access, 2018, 6, 74494-74505.	2.6	4
396	Impacts of Modeling Errors and Randomness on Topology Identification of Electric Distribution Network. , 2018, , .		3
397	Truth Will Out. , 2018, , .		58
398	Analysis and Computation of Adaptive Defense Strategies Against Advanced Persistent Threats for Cyber-Physical Systems. Lecture Notes in Computer Science, 2018, , 205-226.	1.0	26
399	Named Data Networkingâ€™s Intrinsic Cyber-Resilience for Vehicular CPS. IEEE Access, 2018, 6, 60570-60585.	2.6	19
400	Low Latency Detection of Sparse False Data Injections in Smart Grids. IEEE Access, 2018, 6, 58564-58573.	2.6	11
401	Data-Driven and Low-Sparsity False Data Injection Attacks in Smart Grid. Security and Communication Networks, 2018, 2018, 1-11.	1.0	19

#	Article	IF	Citations
402	Trade-offs in Data-Driven False Data Injection Attacks Against the Power Grid. , 2018, , .		7
403	Graph theoretical defense mechanisms against false data injection attacks in smart grids. Journal of Modern Power Systems and Clean Energy, 2018, 6, 860-871.	3.3	23
404	Towards an Iterated Game Model with Multiple Adversaries in Smart-World Systems. Sensors, 2018, 18, 674.	2.1	3
405	From Wired to Wireless: Challenges of False Data Injection Attacks Against Smart Grid Sensor Networks. , 2018, , .		2
406	False Data Injection Attacks Against State Estimation in Smart Grids: Challenges and Opportunities. , 2018, , .		10
407	Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning. , 2018, , .		40
408	Attacks on Authentication and Authorization Models in Smart Grid. Advances in Information Security, 2018, , 53-70.	0.9	4
409	Robust protection scheme against cyberâ€physical attacks in power systems. IET Control Theory and Applications, 2018, 12, 1792-1801.	1.2	13
410	Support Vector Machine Detection of Data Framing Attack in Smart Grid. , 2018, , .		3
411	An Overview of Cyber Security for Smart Grid. , 2018, , .		12
412	A New Classification of Attacks against the Cyber-Physical Security of Smart Grids. , 2018, , .		11
413	A Secure and Scalable Data Communication Scheme in Smart Grids. Wireless Communications and Mobile Computing, 2018, 2018, 1-17.	0.8	6
414	Towards Data Poisoning Attacks in Crowd Sensing Systems. , 2018, , .		47
415	A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. ACM Computing Surveys, 2019, 51, 1-36.	16.1	257
417	Algorithmic Attack Synthesis Using Hybrid Dynamics of Power Grid Critical Infrastructures. , 2018, , .		7
418	Smart Grid Security Security and Privacy of Customer-Side Networks. Springer Briefs in Electrical and Computer Engineering, 2018, , 27-64.	0.3	2
419	Smart Grid Security Protection Against False Data Injection (FDI) Attacks. Springer Briefs in Electrical and Computer Engineering, 2018, , 91-112.	0.3	0
420	TABOR. , 2018, , .		93

#	Article	IF	Citations
421	Designing three indicators to detect false data injection attacks on smart grid by dynamic state estimation. Journal of Intelligent and Fuzzy Systems, 2018, 35, 5593-5604.	0.8	2
422	Vulnerability Assessment of Electrical Cyber-Physical Systems against Cyber Attacks. Applied Sciences (Switzerland), 2018, 8, 768.	1.3	6
423	Covert Cyber Assault Detection in Smart Grid Networks Utilizing Feature Selection and Euclidean Distance-Based Machine Learning. Applied Sciences (Switzerland), 2018, 8, 772.	1.3	23
424	Taxonomy Analysis of Security Aspects in Cyber Physical Systems Applications. , 2018, , .		9
425	Switching and Data Injection Attacks on Stochastic Cyber-Physical Systems. ACM Transactions on Cyber-Physical Systems, 2018, 2, 1-2.	1.9	30
426	Detection of false data injection attacks in smart grids using Recurrent Neural Networks. , 2018, , .		63
427	A stochastic game approach to cyber-physical security with applications to smart grid. , 2018, , .		5
428	Resilient power grid state estimation under false data injection attacks. , 2018, , .		9
429	Vulnerability analysis of power systems based on cyber-attack and defense models. , 2018, , .		9
430	Feature Selectionâ€"Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning. IEEE Access, 2018, 6, 27518-27529.	2.6	71
431	False Data Injection Attacks in Healthcare. Communications in Computer and Information Science, 2018, , 192-202.	0.4	9
432	Linear Quadratic Gaussian Control Under False Data Injection Attacks. , 2018, , .		8
433	Consensus-Based Intrusion Detection for the Electric Power Grid Control System. , 2018, , .		1
434	Cyber security considerations on PMU-based state estimation. , 2018, , .		3
435	Coupled Cyber and Physical Systems: Embracing Smart Cities with Multistream Data Flow. IEEE Electrification Magazine, 2018, 6, 73-83.	1.8	9
437	Machine learning based false data injection in smart grid. , 2018, , .		9
438	Noncircular Attacks on Phasor Measurement Units for State Estimation in Smart Grid. IEEE Journal on Selected Topics in Signal Processing, 2018, 12, 777-789.	7.3	10
439	Observerâ€based attackâ€resilient control for linear systems against FDI attacks on communication links from controller to actuators. International Journal of Robust and Nonlinear Control, 2018, 28, 4382-4403.	2.1	35

#	Article	IF	Citations
440	Secure estimation based Kalman Filter for cyberâ€"physical systems against sensor attacks. Automatica, 2018, 95, 399-412.	3.0	85
441	Adaptive integral slidingâ€mode control strategy of dataâ€driven cyberâ€physical systems against a class of actuator attacks. IET Control Theory and Applications, 2018, 12, 1440-1447.	1.2	62
442	An Investigation of Coordinated Attack on Load Frequency Control. IEEE Access, 2018, 6, 30414-30423.	2.6	28
443	Detection and Characterization of Intrusions to Network Parameter Data in Electric Power Systems. IEEE Transactions on Smart Grid, 2019, 10, 3919-3928.	6.2	18
444	Detection of Sensor Attack and Resilient State Estimation for Uniformly Observable Nonlinear Systems having Redundant Sensors. IEEE Transactions on Automatic Control, 2019, 64, 1162-1169.	3.6	51
445	On Redundant Observability: From Security Index to Attack Detection and Resilient State Estimation. IEEE Transactions on Automatic Control, 2019, 64, 775-782.	3.6	42
446	A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios. IEEE Transactions on Smart Grid, 2019, 10, 1704-1712.	6.2	77
447	REACT to Cyber Attacks on Power Grids. IEEE Transactions on Network Science and Engineering, 2019, 6, 459-473.	4.1	34
448	EXPOSE the Line Failures Following a Cyber-Physical Attack on the Power Grid. IEEE Transactions on Control of Network Systems, 2019, 6, 451-461.	2.4	19
449	Power Grid AC-Based State Estimation: Vulnerability Analysis Against Cyber Attacks. IEEE Transactions on Automatic Control, 2019, 64, 1784-1799.	3.6	68
450	False Data Injection Attacks in Internet of Things. EAI/Springer Innovations in Communication and Computing, 2019, , 47-58.	0.9	15
451	A two-layer game theoretical attack-defense model for a false data injection attack against power systems. International Journal of Electrical Power and Energy Systems, 2019, 104, 169-177.	3.3	69
452	Resilient PMU Network Design in the Face of GPS Spoofing Attacks. , 2019, , .		2
453	Detection and isolation of false data injection attack for smart grids via unknown input observers. IET Generation, Transmission and Distribution, 2019, 13, 1277-1286.	1.4	31
454	Design of a FDIA Resilient Protection Scheme for Power Networks by Securing Minimal Sensor Set. Lecture Notes in Computer Science, 2019, , 156-171.	1.0	1
455	Detection and Isolation of False Data Injection Attacks in Smart Grids via Nonlinear Interval Observer. IEEE Internet of Things Journal, 2019, 6, 6498-6512.	5.5	43
456	Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning. , 2019, , .		63
457	A Resilient Attitude Tracking Algorithm for Mechanical Systems. IEEE/ASME Transactions on Mechatronics, 2019, 24, 2550-2561.	3.7	14

#	Article	IF	Citations
458	Defending Against Data Integrity Attacks in Smart Grid: A Deep Reinforcement Learning-Based Approach. IEEE Access, 2019, 7, 110835-110845.	2.6	60
459	Detection of Stealthy attacks on Electric Grids Using Transient Analysis. , 2019, , .		0
460	Towards insider threats detection in smart grid communication systems. IET Communications, 2019, 13, 1728-1736.	1.5	10
461	Real Time Security Assessment of the Power System Using a Hybrid Support Vector Machine and Multilayer Perceptron Neural Network Algorithms. Sustainability, 2019, 11, 3586.	1.6	29
462	Review of the false data injection attack against the cyberâ€physical power system. IET Cyber-Physical Systems: Theory and Applications, 2019, 4, 101-107.	1.9	71
463	Optimal Strategy of Attack-Defense Interaction Over Load Frequency Control Considering Incomplete Information. IEEE Access, 2019, 7, 75342-75349.	2.6	17
464	Recovery of Missing Data in Correlated Smart Grid Datasets. , 2019, , .		2
465	Data Quality Management Framework for Smart Grid Systems. Lecture Notes in Business Information Processing, 2019, , 299-310.	0.8	10
466	Real-Time Identification of False Data Injection Attacks: A Novel Dynamic-Static Parallel State Estimation Based Mechanism. IEEE Access, 2019, 7, 95812-95824.	2.6	12
467	Distributed Data-Selective DLMS Estimation Under Channel Attacks. IEEE Access, 2019, 7, 83863-83872.	2.6	6
468	Exploiting Vulnerabilities of Load Forecasting Through Adversarial Attacks. , 2019, , .		45
469	Managing False Data Injection Attacks During Contingency of Secured Meters. IEEE Transactions on Smart Grid, 2019, 10, 6945-6953.	6.2	10
470	Mitigating the Impacts of Covert Cyber Attacks in Smart Grids Via Reconstruction of Measurement Data Utilizing Deep Denoising Autoencoders. Energies, 2019, 12, 3091.	1.6	19
471	Intelligent Anomaly Detection for Large-scale Smart Grids. , 2019, , .		29
472	A Countermeasure against Zero-dynamics Sensor Attack via Generalized Hold Feedback. , 2019, , .		2
473	Cognitive Risk Control for Mitigating Cyber-Attack in Smart Grid. IEEE Access, 2019, 7, 125806-125826.	2.6	24
474	Dynamic State Estimation of Generators Under Cyber Attacks. IEEE Access, 2019, 7, 125253-125267.	2.6	32
475	Prevention of false data injections in smart infrastructures. , 2019, , .		14

#	Article	IF	Citations
476	Intrusion Detection in Smart Grid Measurement Infrastructures Based on Principal Component Analysis. , 2019, , .		2
477	Quickest Detection of False Data Injection Attacks in Smart Grid with Dynamic Models. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2022, 10, 1292-1302.	3.7	12
478	A Tutorial on Detecting Security Attacks on Cyber-Physical Systems. , 2019, , .		21
479	Detection and Compensation of Covert Service-Degrading Intrusions in Cyber Physical Systems through Intelligent Adaptive Control. , 2019, , .		11
480	On Effectiveness of Detecting FDI Attacks on Power Grid using Moving Target Defense. , 2019, , .		5
481	Cyber-Physical Security of State Estimation Against Attacks on Wide-Area Load Shedding Protection Schemes. , 2019, , .		4
482	A Robust Control Architecture for Mitigating Sensor and Actuator Attacks on PV Converter. , 2019, , .		5
483	Secure Fusion Filtering and Clustering for Distributed Wireless Sensor Networks. , 2019, , .		3
484	Bibliographical review on cyber attacks from a control oriented perspective. Annual Reviews in Control, 2019, 48, 103-128.	4.4	79
485	Kalman Filtering Based Interval State Estimation For Attack Detection. Energy Procedia, 2019, 158, 6589-6594.	1.8	7
486	A Decentralized State Estimation Algorithm for Building Electrical Distribution Network Based on ADMM. , 2019, , .		0
487	Security control for networked control systems with randomly occurring integrity check protection subject to randomly occurring zero-value attacks. Journal of the Franklin Institute, 2019, 356, 11456-11472.	1.9	4
488	False data injection attacks against smart gird state estimation: Construction, detection and defense. Science China Technological Sciences, 2019, 62, 2077-2087.	2.0	43
489	Distributed filtering under false data injection attacks. Automatica, 2019, 102, 34-44.	3.0	130
490	Online Identification and Data Recovery for PMU Data Manipulation Attack. IEEE Transactions on Smart Grid, 2019, 10, 5889-5898.	6.2	55
491	Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. IEEE Access, 2019, 7, 13960-13988.	2.6	298
492	Entropy-Based Proactive and Reactive Cyber-Physical Security. Advances in Information Security, 2019, , 59-83.	0.9	3
493	Cognitive Dynamic System for Control and Cyber-Attack Detection in Smart Grid. IEEE Access, 2019, 7, 78320-78335.	2.6	20

#	Article	IF	Citations
494	A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids. IEEE Access, 2019, 7, 80778-80788.	2.6	224
495	A business that canâ€™t lose: Investing in attacks against the Colombian power grid. International Journal of Critical Infrastructure Protection, 2019, 26, 100303.	2.9	1
496	A Review on Active Distribution System State Estimation. , 2019, , .		6
497	A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation. Energies, 2019, 12, 2209.	1.6	53
498	Design and Realization of Testbeds for Security Research in the Industrial Internet of Things. Advanced Sciences and Technologies for Security Applications, 2019, , 287-310.	0.4	3
499	Detecting stealthy attacks against industrial control systems based on residual skewness analysis. Eurasip Journal on Wireless Communications and Networking, 2019, 2019, .	1.5	31
500	A modeling framework for critical infrastructure and its application in detecting cyber-attacks on a water distribution system. International Journal of Critical Infrastructure Protection, 2019, 26, 100298.	2.9	16
501	Line Failure Detection After a Cyber-Physical Attack on the Grid Using Bayesian Regression. IEEE Transactions on Power Systems, 2019, 34, 3758-3768.	4.6	27
502	Quickest Detection of Time-varying False Data Injection Attacks in Dynamic Smart Grids. , 2019, , .		4
503	Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks, 2019, 160, 165-191.	3.2	133
504	Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest. IEEE Transactions on Information Forensics and Security, 2019, 14, 2765-2777.	4.5	170
505	Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Communications Surveys and Tutorials, 2019, 21, 2702-2733.	24.8	468
506	On the Security of MIL-STD-1553 Communication Bus. Lecture Notes in Computer Science, 2019, , 153-171.	1.0	4
507	A Collaborative Intrusion Detection Approach Using Blockchain for Multimicrogrid Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 49, 1720-1730.	5.9	63
508	Stability of Transactive Energy Market-Based Power Distribution System Under Data Integrity Attack. IEEE Transactions on Industrial Informatics, 2019, 15, 5541-5550.	7.2	35
509	Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers. International Journal of Electrical Power and Energy Systems, 2019, 110, 208-222.	3.3	41
510	Secure Distributed State Estimation for Networked Microgrids. IEEE Internet of Things Journal, 2019, 6, 8046-8055.	5.5	29
511	A Low Power WSNs Attack Detection and Isolation Mechanism for Critical Smart Grid Applications. IEEE Sensors Journal, 2019, 19, 5315-5324.	2.4	28

#	Article	IF	Citations
512	Network Constrained Unit Commitment Under Cyber Attacks Driven Overloads. IEEE Transactions on Smart Grid, 2019, 10, 6449-6460.	6.2	29
513	Dynamic Security Assessment for Power System Under Cyber-Attack. Journal of Electrical Engineering and Technology, 2019, 14, 549-559.	1.2	5
514	Security design against stealthy attacks on power system state estimation: A formal approach. Computers and Security, 2019, 84, 301-317.	4.0	2
515	Partial grid false data injection attacks against state estimation. International Journal of Electrical Power and Energy Systems, 2019, 110, 623-629.	3.3	33
516	Supporting Sustainable Maintenance of Substations under Cyber-Threats: An Evaluation Method of Cybersecurity Risk for Power CPS. Sustainability, 2019, 11, 982.	1.6	12
517	Distribution system state estimation: an overview of recent developments. Frontiers of Information Technology and Electronic Engineering, 2019, 20, 4-17.	1.5	59
518	A Review of Cyber-Attack Methods in Cyber-Physical Power System. , 2019, , .		35
519	Detection of False Data Injection Attacks in Cyber-Physical Systems using Dynamic Invariants. , 2019, , .		1
520	Blind Topology Identification for Smart Grid Based on Dictionary Learning. , 2019, , .		5
521	Real-time Detecting False Data Injection Attacks Based on Spatial and Temporal Correlations. , 2019, , .		4
522	Semantic-Based Detection Architectures Against Monitoring-Control Attacks in Power Grids. , 2019, , .		2
523	Location of False Data Injection Attacks in Power System. , 2019, , .		2
524	An Optimal Defense Strategy Against Data Integrity Attacks In Smart Grids. , 2019, , .		0
525	Identifying an Exploitable Structure for the Core Problem of Load-Redistribution Attack Problems. , 2019, , .		4
526	The Economic Impacts of Household Level Smart Meter Manipulation Attack. , 2019, , .		0
527	Malicious data injection attacks: A relaxed physics model based strategy for real-time monitoring. , 2019, , .		1
528	Linearized Attack Vector Formulation against AC State Estimator. , 2019, , .		5
529	Data Multiple Interpolation Technique Based on Convolutional Neural Networks. , 2019, , .		0

#	Article	IF	Citations
530	MILP Modeling of Targeted False Load Data Injection Cyberattacks to Overflow Transmission Lines in Smart Grids. , 2019, , .		17
531	Data Attack Method in Completely Distributed Control Mode Based on DC-OPF. , 2019, , .		0
532	A Methodology for Detecting Stealthy Transformer Tap Command Injection Attacks in Smart Grids. , 2019, , .		0
533	LQG Reference Tracking with Safety and Reachability Guarantees under False Data Injection Attacks. , 2019, , .		7
534	Physics-Guided Deep Learning for Time-Series State Estimation Against False Data Injection Attacks. , 2019, , .		6
535	Learning-Guided Network Fuzzing for Testing Cyber-Physical System Defences. , 2019, , .		35
536	Detection of False Data Injection Attack Using Graph Signal Processing for the Power Grid. , 2019, , .		20
537	A Machine Learning Approach to Distinguish Faults and Cyberattacks in Smart Buildings. , 2019, , .		9
538	False Data Detection in Distributed Oscillation Mode Estimation using Hierarchical k-means. , 2019, , .		1
539	A Framework for the Integration of ICT-relevant Data in Power System Applications. , 2019, , .		12
540	Kalman Filter Based Secure State Estimation and Individual Attacked Sensor Detection in Cyber-Physical Systems. , 2019, , .		11
541	Distributed Fusion Estimation for Linear Time-varying Systems under DoS Attacks and Bounded Noises. , 2019, , .		1
542	Optimal Attack Strategy for Multi-Transmission Line Congestion in Cyber-Physical Smart Grids. , 2019, , .		9
543	Resilient Trajectory Planning in Adversarial Environments. , 2019, , .		2
544	Attack-resilient Estimation for Linear Discrete-time Stochastic Systems with Input and State Constraints. , 2019, , .		9
545	Towards Robust and Scalable Power System State Estimation. , 2019, , .		1
546	Z Table: Cost-Optimized Attack on Reinforcement Learning. , 2019, , .		1
547	Finding the Worse Case: Undetectable False Data Injection with Minimized Knowledge and Resource. , 2019, , .		0

#	Article	IF	Citations
548	Data-Driven Measurement Tampering Detection Considering Spatial-Temporal Correlations. , 2019, , .		2
549	Enabling Secure Grid Information Sharing through Hash Calendar-based Blockchain Infrastructures. , 2019, , .		1
550	A Novel Detection Method for Abnormal PMU Amplitude Data Obtained in Both Ends of Transmission Line. , 2019, , .		1
551	SAâ€“Based PMU Network Upgrade for Detectability of GPS Spoofing Attacks. , 2019, , .		2
552	An Overview About Detection of Cyber-Attacks on Power SCADA Systems. , 2019, , .		2
553	Research on Situational Sensing Method of Grid Cyber-Physical System under Network Attack. , 2019, , .		0
554	Trust in control: a trust model for power system network assessment. EPJ Web of Conferences, 2019, 217, 01008.	0.1	2
555	Stealthy and Sparse False Data Injection Attacks Based on Machine Learning. Lecture Notes in Computer Science, 2019, , 337-347.	1.0	2
556	Detection of False Data Injection Attacks in Smart Grids: A Real-Time Principle Component Analysis. , 2019, , .		10
557	A review of various modern strategies for mitigation of cyber attacks in smart grids. , 2019, , .		1
558	Resilient Control Design for Vehicular Platooning in an Adversarial Environment. , 2019, , .		13
559	Stealthy Attack Mitigation of Consensus-based Distributed Economic Dispatch. , 2019, , .		1
560	A Test Bed for Detecting False Data Injection Attacks in Systems With Distributed Energy Resources. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2022, 10, 1303-1315.	3.7	16
561	Secure interval observer for linear continuous-time systems with discrete measurements subject to cyber-attacks. , 2019, , .		2
562	Distributed Optimal Dynamic State Estimation for Cyber Intrusion Detection in Networked DC Microgrids. , 2019, , .		4
563	Transient Model-Based Detection Scheme for False Data Injection Attacks in Microgrids. , 2019, , .		4
564	Impact of Cyber-Attacks on Power Grids with Distributed Energy Storage Systems. , 2019, , .		6
565	Real-time Detection of False Data Injection Attacks Based on Load Forecasting in Smart Grid. , 2019, , .		8

#	Article	IF	Citations
566	Detection of False Data Injection Attack in Smart Grids via Interval Observer. , 2019, , .		1
567	Creating Meta Attack Language Instances using ArchiMate: Applied to Electric Power and Energy System Cases. , 2019, , .		15
568	Nonzero-Dynamics Stealthy Attack and Its Impacts Analysis in DC Microgrids. , 2019, , .		3
569	Distributed Control Methods and Impact of Communication Failure in AC Microgrids: A Comparative Review. Electronics (Switzerland), 2019, 8, 1265.	1.8	33
570	Risk-Based Mitigation of Load Curtailment Cyber Attack Using Intelligent Agents in a Shipboard Power System. IEEE Transactions on Smart Grid, 2019, 10, 4741-4750.	6.2	42
571	On Reliability Analysis of Smart Grids under Topology Attacks. ACM Transactions on Cyber-Physical Systems, 2019, 3, 1-25.	1.9	11
572	Toward a spoof-tolerant PMU network architecture. International Journal of Electrical Power and Energy Systems, 2019, 107, 311-320.	3.3	6
573	A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 49, 1554-1569.	5.9	240
574	A Stealth Cyber-Attack Detection Strategy for DC Microgrids. IEEE Transactions on Power Electronics, 2019, 34, 8162-8174.	5.4	169
575	Secure State Estimation Against Integrity Attacks: A Gaussian Mixture Model Approach. IEEE Transactions on Signal Processing, 2019, 67, 194-207.	3.2	52
576	Review of major approaches to analyze vulnerability in power system. Reliability Engineering and System Safety, 2019, 183, 153-172.	5.1	134
577	Transmission Scheduling for Remote State Estimation Over Packet Dropping Links in the Presence of an Eavesdropper. IEEE Transactions on Automatic Control, 2019, 64, 3732-3739.	3.6	60
578	Convex Optimization Based State Estimation Against Sparse Integrity Attacks. IEEE Transactions on Automatic Control, 2019, 64, 2383-2395.	3.6	27
579	Multilevel Programming-Based Coordinated Cyber Physical Attacks and Countermeasures in Smart Grid. IEEE Access, 2019, 7, 9836-9847.	2.6	31
580	Robust Power System State Estimation From Rank-One Measurements. IEEE Transactions on Control of Network Systems, 2019, 6, 1391-1403.	2.4	11
581	Cyber Security for Power System State Estimation. Power Electronics and Power Systems, 2019, , 241-256.	0.6	2
582	State of the art of cyber-physical systems security: An automatic control perspective. Journal of Systems and Software, 2019, 149, 174-216.	3.3	125
583	Security in Smart Cyber-Physical Systems: A Case Study on Smart Grids and Smart Cars. , 2019, , 147-163.		12

#	Article	IF	Citations
584	A new model approach of electrical cyber physical systems considering cyber security. IEEJ Transactions on Electrical and Electronic Engineering, 2019, 14, 201-213.	0.8	10
585	Challenges and Opportunities: Cyber-Physical Security in the Smart Grid. Power Electronics and Power Systems, 2019, , 257-273.	0.6	18
586	Enhanced Hidden Moving Target Defense in Smart Grids. IEEE Transactions on Smart Grid, 2019, 10, 2208-2223.	6.2	88
587	Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks. IEEE Transactions on Smart Grid, 2019, 10, 3162-3173.	6.2	272
588	Worst-Case Innovation-Based Integrity Attacks With Side Information on Remote State Estimation. IEEE Transactions on Control of Network Systems, 2019, 6, 48-59.	2.4	47
589	Financially Motivated FDI on SCED in Real-Time Electricity Markets: Attacks and Mitigation. IEEE Transactions on Smart Grid, 2019, 10, 1949-1959.	6.2	47
590	Impact of Stealthy Attacks on Optimal Power Flow: A Simulink-Driven Formal Analysis. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	3.7	1
591	Distributed Load Sharing Under False Data Injection Attack in an Inverter-Based Microgrid. IEEE Transactions on Industrial Electronics, 2019, 66, 1543-1551.	5.2	131
592	Minimax-Regret Robust Defensive Strategy Against False Data Injection Attacks. IEEE Transactions on Smart Grid, 2019, 10, 2068-2079.	6.2	39
593	Optimization Algorithms for Catching Data Manipulators in Power System Estimation Loops. IEEE Transactions on Control Systems Technology, 2019, 27, 1203-1218.	3.2	13
594	Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks. Information Fusion, 2019, 46, 44-50.	11.7	43
595	Distributed H_infty Estimation in Sensor Networks With Two-Channel Stochastic Attacks. IEEE Transactions on Cybernetics, 2020, 50, 465-475.	6.2	49
596	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
597	Reliable Leader-to-Follower Formation Control of Multiagent Systems Under Communication Quantization and Attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 50, 89-99.	5.9	82
598	A Moving Target Defense Control Framework for Cyber-Physical Systems. IEEE Transactions on Automatic Control, 2020, 65, 1029-1043.	3.6	58
599	Crossâ€layer security design for encrypted CPS based on modified security signalling game. Asian Journal of Control, 2020, 22, 956-975.	1.9	3
600	False Data Injection and Detection in LQG Systems: A Game Theoretic Approach. IEEE Transactions on Control of Network Systems, 2020, 7, 338-348.	2.4	31
601	Input-to-State Stabilization of Interval Type-2 Fuzzy Systems Subject to Cyberattacks: An Observer-Based Adaptive Sliding Mode Approach. IEEE Transactions on Fuzzy Systems, 2020, 28, 190-203.	6.5	91

#	Article	IF	Citations
602	Securely Solving Linear Algebraic Equations in a Distributed Framework Enhanced With Communication-Efficient Algorithms. IEEE Transactions on Network Science and Engineering, 2020, 7, 1027-1042.	4.1	2
603	Detecting stealthy attacks on industrial control systems using a permutation entropy-based method. Future Generation Computer Systems, 2020, 108, 1230-1240.	4.9	21
604	Resilient Control Design for Load Frequency Control System Under False Data Injection Attacks. IEEE Transactions on Industrial Electronics, 2020, 67, 7951-7962.	5.2	113
605	Resilient Output Containment of Heterogeneous Cooperative and Adversarial Multigroup Systems. IEEE Transactions on Automatic Control, 2020, 65, 3104-3111.	3.6	22
606	False data injection attacks against state estimation in the presence of sensor failures. Information Sciences, 2020, 508, 92-104.	4.0	43
607	Enhancing Power System Cyber-Security With Systematic Two-Stage Detection Strategy. IEEE Transactions on Power Systems, 2020, 35, 1549-1561.	4.6	27
608	Moving Target Defense Approach to Detecting Stuxnet-Like Attacks. IEEE Transactions on Smart Grid, 2020, 11, 291-300.	6.2	65
609	On Feasibility and Limitations of Detecting False Data Injection Attacks on Power Grid State Estimation Using D-FACTS Devices. IEEE Transactions on Industrial Informatics, 2020, 16, 854-864.	7.2	123
610	Enhanced Resilient State Estimation Using Data-Driven Auxiliary Models. IEEE Transactions on Industrial Informatics, 2020, 16, 639-647.	7.2	38
611	Analysis of Moving Target Defense Against False Data Injection Attacks on Power Grid. IEEE Transactions on Information Forensics and Security, 2020, 15, 2320-2335.	4.5	82
612	Security attacks on smart grid scheduling and their defences: a game-theoretic approach. International Journal of Information Security, 2020, 19, 427-443.	2.3	18
613	Attack Identification and Correction for PMU GPS Spoofing in Unbalanced Distribution Systems. IEEE Transactions on Smart Grid, 2020, 11, 762-773.	6.2	40
614	Priority-Based Protection Against the Malicious Data Injection Attacks on State Estimation. IEEE Systems Journal, 2020, 14, 1945-1952.	2.9	12
615	Protecting the Grid Against MAD Attacks. IEEE Transactions on Network Science and Engineering, 2020, 7, 1310-1326.	4.1	15
616	Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes. IEEE Transactions on Power Systems, 2020, 35, 440-450.	4.6	47
617	Diagnosis of Outliers and Cyber Attacks in Dynamic PMU-Based Power State Estimation. IEEE Transactions on Power Systems, 2020, 35, 1188-1197.	4.6	40
618	A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. IEEE Transactions on Smart Grid, 2020, 11, 2218-2234.	6.2	361
619	Fast Nonconvex SDP Solvers for Large-Scale Power System State Estimation. IEEE Transactions on Power Systems, 2020, 35, 2412-2421.	4.6	5

#	Article	IF	Citations
620	A penalty-based adaptive secure estimation for power systems under false data injection attacks. Information Sciences, 2020, 508, 380-392.	4.0	10
621	Recursive Filtering of Distributed Cyber-Physical Systems With Attack Detection. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51, 6466-6476.	5.9	51
622	Resilient Consensus-Based Distributed Filtering: Convergence Analysis Under Stealthy Attacks. IEEE Transactions on Industrial Informatics, 2020, 16, 4878-4888.	7.2	25
623	Data-Driven Output-Feedback LQ Secure Control for Unknown Cyber-Physical Systems Against Sparse Actuator Attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51, 5708-5720.	5.9	19
624	Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 2020, 105, 581-606.	4.9	144
625	Scalable and Robust State Estimation From Abundant But Untrusted Data. IEEE Transactions on Smart Grid, 2020, 11, 1880-1894.	6.2	3
626	Cyber Security in Control of Grid-Tied Power Electronic Convertersâ€"Challenges and Vulnerabilities. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021, 9, 5326-5340.	3.7	90
627	Attack-Resilient Event-Triggered Controller Design of DC Microgrids Under DoS Attacks. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67, 699-710.	3.5	112
628	Stealthy Actuator Signal Attacks in Stochastic Control Systems: Performance and Limitations. IEEE Transactions on Automatic Control, 2020, 65, 3927-3934.	3.6	35
629	Neutralizing zero dynamics attack on sampled-data systems via generalized holds. Automatica, 2020, 113, 108778.	3.0	16
630	Detection and Mitigation of Data Manipulation Attacks in AC Microgrids. IEEE Transactions on Smart Grid, 2020, 11, 2588-2603.	6.2	59
631	Detecting Dynamic Attacks in Smart Grids Using Reservoir Computing: A Spiking Delayed Feedback Reservoir Based Approach. IEEE Transactions on Emerging Topics in Computational Intelligence, 2020, 4, 253-264.	3.4	24
632	A Data-Based Detection Method Against False Data Injection Attacks. IEEE Design and Test, 2020, 37, 67-74.	1.1	7
633	State-Saturated Recursive Filter Design for Stochastic Time-Varying Nonlinear Complex Networks Under Deception Attacks. IEEE Transactions on Neural Networks and Learning Systems, 2020, 31, 3788-3800.	7.2	175
634	Sparse Undetectable Sensor Attacks Against Cyber-Physical Systems: A Subspace Approach. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67, 2517-2521.	2.2	16
635	Transactive Energy to Thwart Load Altering Attacks on Power Distribution Systems. Future Internet, 2020, 12, 4.	2.4	9
636	The Effect of SMiShing Attack on Security of Demand Response Programs. Energies, 2020, 13, 4542.	1.6	8
637	Interdependence-Aware Game-Theoretic Framework for Secure Intelligent Transportation Systems. IEEE Internet of Things Journal, 2021, 8, 16395-16405.	5.5	7

#	Article	IF	Citations
638	False data injection attacks detection on power systems with convolutional neural network. Journal of Physics: Conference Series, 2020, 1633, 012134.	0.3	5
639	Adaptive Compensation Control under Constant False Data Injection Attack. IOP Conference Series: Materials Science and Engineering, 2020, 782, 032072.	0.3	0
640	Robust localized cyber-attack detection for key equipment in nuclear power plants. Progress in Nuclear Energy, 2020, 128, 103446.	1.3	11
641	A3D: Attention-based auto-encoder anomaly detector for false data injection attacks. Electric Power Systems Research, 2020, 189, 106795.	2.1	24
642	Cyberâ€“physical security for onâ€going smart grid initiatives: a survey. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 233-244.	1.9	29
643	Effect of Communication Failures on State Estimation of 5G-Enabled Smart Grid. IEEE Access, 2020, 8, 112642-112658.	2.6	40
644	A Hybrid Cyber Attack Model for Cyber-Physical Power Systems. IEEE Access, 2020, 8, 114876-114883.	2.6	28
645	Formal Synthesis of Monitoring and Detection Systems for Secure CPS Implementations. , 2020, , .		7
646	Smart Grid Data Security using Practical CP-ABE with Obfuscated Policy and Outsourcing Decryption. , 2020, , .		2
647	False Data Injection Attacks against State Estimation in AC-DC Hybrid Power System. , 2020, , .		3
648	A multilevel hybrid anomaly detection scheme for industrial wireless sensor networks. International Journal of Network Management, 2020, 31, e2144.	1.4	6
650	A Distributed Observer-Based Cyber-Attack Identification Scheme in Cooperative Networked Systems under Switching Communication Topologies. Electronics (Switzerland), 2020, 9, 1912.	1.8	6
651	Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning. Computers and Security, 2020, 97, 101994.	4.0	66
652	Robust distribution system state estimation with hybrid measurements. IET Generation, Transmission and Distribution, 2020, 14, 3250-3259.	1.4	21
653	Robustness of Short-Term Wind Power Forecasting against False Data Injection Attacks. Energies, 2020, 13, 3780.	1.6	19
654	Attack Detection and Isolation for Distributed Load Shedding Algorithm in Microgrid Systems. IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 2020, 1, 102-110.	3.0	15
655	Data Integrity Attack Detection for Node Voltage in Cyber-Physical Power System. Arabian Journal for Science and Engineering, 2020, 45, 10591-10603.	1.7	1
656	A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems. Energies, 2020, 13, 3860.	1.6	60

#	Article	IF	Citations
657	Resilient Sensor Placement for Kalman Filtering in Networked Systems: Complexity and Algorithms. IEEE Transactions on Control of Network Systems, 2020, 7, 1870-1881.	2.4	10
658	Resilient decentralized sampled-data <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si25.svg"><mml:mrow><mml:msub><mml:mrow><mml:mi>H</mml:mi></mml:mrow><mml:mrow><mml:mi>âˆž</mml:mi></m filter design for linear interconnected systems subject to denial-of-service attacks. Information Sciences, 2020, 538, 467-485.	4.0	12
659	Cyber Attack Detection for a Nonlinear Binary Crude Oil Distillation Column. , 2020, , .		1
660	An integrated state-estimation framework for interdependent water and energy systems. Journal of Hydrology, 2020, 590, 125393.	2.3	5
661	Real-Time Implementation of Secure Distributed State Estimation for Networked Microgrids. , 2020, , .		2
662	Semi-Supervised Domain-Adversarial Training for Intrusion Detection against False Data Injection in the Smart Grid. , 2020, , .		9
663	False data injection attacks and detection on electricity markets with partial information in a microâ€gridâ€based smart grid system. International Transactions on Electrical Energy Systems, 2020, 30, e12661.	1.2	4
664	Impact of injection attacks on sensor-based continuous authentication for smartphones. Computer Communications, 2020, 163, 150-161.	3.1	10
665	A Double-Layer Cyber Physical Cooperative Emergency Control Strategy Modification Method for Cyber-Attacks Against Power System. , 2020, , .		2
666	Multi-Model Resilient Observer under False Data Injection Attacks. , 2020, , .		3
667	A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. IEEE Access, 2020, 8, 177447-177470.	2.6	80
668	Physical Layer Detection of Malicious Relays in LTE-A Network Using Unsupervised Learning. IEEE Access, 2020, 8, 154713-154726.	2.6	2
669	Mitigating the Impacts of False Data Injection Attacks in Smart Grids using Deep Convolutional Neural Networks. , 2020, , .		2
670	Power Systems Decomposition for Robustifying State Estimation Under Cyber Attacks. IEEE Transactions on Power Systems, 2021, 36, 1922-1933.	4.6	14
671	Model-Based Secure Load Frequency Control of Smart Grids Against Data Integrity Attack. IEEE Access, 2020, 8, 159672-159682.	2.6	7
672	CPFuzz: Combining Fuzzing and Falsification of Cyber-Physical Systems. IEEE Access, 2020, 8, 166951-166962.	2.6	4
673	Designing false data injection attacks penetrating ACâ€based bad data detection system and FDI dataset generation. Concurrency Computation Practice and Experience, 2022, 34, e5956.	1.4	4
674	Detection of False Data Injection Attacks Using the Autoencoder Approach. , 2020, , .		20

#	Article	IF	Citations
675	Test Data Generation for False Data Injection Attack Testing in Air Traffic Surveillance. , 2020, , .		4
676	Anomaly Detection using Clustered Deep One-Class Classification. , 2020, , .		4
677	Secure impulsive synchronization in Lipschitz-type multi-agent systems subject to deception attacks. IEEE/CAA Journal of Automatica Sinica, 2020, 7, 1326-1334.	8.5	47
678	Detection and Differentiation of Replay Attack and Equipment Faults in SCADA Systems. IEEE Transactions on Automation Science and Engineering, 2021, 18, 1626-1639.	3.4	28
679	Real-time False Data Injection Attack Detection in Connected Vehicle Systems with PDE modeling. , 2020, , .		10
680	Multi-Objective Evolutionary Optimization for Worst-Case Analysis of False Data Injection Attacks in the Smart Grid. , 2020, , .		4
681	Q-Learning for Securing Cyber-Physical Systems : A survey. , 2020, , .		10
682	Approaching Optimal Power Flow From Attackerâ€™s Standpoint To Launch False Data Injection Cyberattack. , 2020, , .		10
683	Literature Review on False Data Injection Attacks Against Power System. , 2020, , .		0
684	Coordinated False Data Injection Attacks in AGC System and Its Countermeasure. IEEE Access, 2020, 8, 194640-194651.	2.6	19
685	Fusion Estimation for FDI Sensor Attacks in Distributed Systems. , 2020, , .		3
686	On Data Integrity Attacks against Industrial Internet of Things. , 2020, , .		7
687	An Event-Triggered Ï‡<sup>2</sup>-Detector for Cyber-Physical Systems under False Data Injection Attacks. , 2020, , .		0
688	A multilayer perceptron model for anomaly detection in water treatment plants. International Journal of Critical Infrastructure Protection, 2020, 31, 100393.	2.9	28
689	Cyber-Physical Microgrids: Toward Future Resilient Communities. IEEE Industrial Electronics Magazine, 2020, 14, 4-17.	2.3	29
690	Learning-based switched reliable control of cyber-physical systems with intermittent communication faults. IEEE/CAA Journal of Automatica Sinica, 2020, 7, 711-724.	8.5	7
691	Data-Centric Edge Computing to Defend Power Grids Against IoT-Based Attacks. Computer, 2020, 53, 35-43.	1.2	11
692	An Event-Driven Resilient Control Strategy for DC Microgrids. IEEE Transactions on Power Electronics, 2020, 35, 13714-13724.	5.4	49

#	Article	IF	Citations
693	A Game-Theoretic Approach to Secure Estimation and Control for Cyber-Physical Systems with a Digital Twin. , 2020, , .		6
694	Stealthy attack detection using convex optimization-based RPCA algorithm. Electric Power Systems Research, 2020, 187, 106418.	2.1	0
695	Adversarial Examples on Power Systems State Estimation. , 2020, , .		18
696	A Literature Review: Intrusion Detection Systems in Internet of Things. Journal of Physics: Conference Series, 2020, 1518, 012040.	0.3	4
697	Security Challenges &amp; Controls in Cyber Physical System. , 2020, , .		6
698	Distributed Resilient Secondary Control of DC Microgrids Against Unbounded Attacks. IEEE Transactions on Smart Grid, 2020, 11, 3850-3859.	6.2	59
699	A Secure Distributed Information Sharing Algorithm Based on Attack Detection in Multi-Task Networks. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67, 5125-5138.	3.5	14
700	Interval Functional Observers Design for Time-Delay Systems Under Stealthy Attacks. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67, 5101-5112.	3.5	14
701	Efficient detection of false data injection attack with invertible automatic encoder and longâ€shortâ€term memory. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 110-118.	1.9	8
702	Control Behavior Integrity for Distributed Cyber-Physical Systems. , 2020, , .		18
703	Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. Journal of Information Security and Applications, 2020, 54, 102518.	1.8	36
704	On Detection of False Data in Cooperative DC Microgridsâ€"A Discordant Element Approach. IEEE Transactions on Industrial Electronics, 2020, 67, 6562-6571.	5.2	109
705	Ship Security Relative Integrated Navigation with Injected Fault Measurement Attack and Unknown Statistical Property Noises. Journal of Marine Science and Engineering, 2020, 8, 305.	1.2	1
706	Attribute-Based Data Security with Obfuscated Access Policy for Smart Grid Applications. , 2020, , .		1
707	Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. International Journal of Electrical Power and Energy Systems, 2020, 119, 105947.	3.3	57
708	Optimal D-FACTS Placement in Moving Target Defense Against False Data Injection Attacks. IEEE Transactions on Smart Grid, 2020, 11, 4345-4357.	6.2	35
709	Detection of integrity loss in networked control systems using an interval finite memory observer. International Journal of Control, 2021, 94, 2640-2649.	1.2	1
710	Actuator Security Indices Based on Perfect Undetectability: Computation, Robustness, and Sensor Placement. IEEE Transactions on Automatic Control, 2020, 65, 3816-3831.	3.6	17

#	Article	IF	Citations
711	Recovery-based Model Predictive Control for Cascade Mitigation under Cyber-Physical Attacks. , 2020, , .		11
712	<i>iFinger</i>: Intrusion Detection in Industrial Control Systems via Register-Based Fingerprinting. IEEE Journal on Selected Areas in Communications, 2020, 38, 955-967.	9.7	22
713	Locational Detection of the False Data Injection Attack in a Smart Grid: A Multilabel Classification Approach. IEEE Internet of Things Journal, 2020, 7, 8218-8227.	5.5	96
714	Secure State Estimation With Byzantine Sensors: A Probabilistic Approach. IEEE Transactions on Automatic Control, 2020, 65, 3742-3757.	3.6	17
715	Overloaded Branch Chains Induced by False Data Injection Attack in Smart Grid. IEEE Signal Processing Letters, 2020, 27, 426-430.	2.1	11
716	Detection of Hidden Transformer Tap Change Command Attacks in Transmission Networks. IEEE Transactions on Smart Grid, 2020, 11, 5161-5173.	6.2	9
717	A resilient framework for sensor-based attacks on cyberâ€“physical systems using trust-based consensus and self-triggered control. Control Engineering Practice, 2020, 101, 104509.	3.2	12
718	A Novel Sparse Attack Vector Construction Method for False Data Injection in Smart Grids. Energies, 2020, 13, 2940.	1.6	3
719	False data injection against state estimation in power systems with multiple cooperative attackers. ISA Transactions, 2020, 101, 225-233.	3.1	20
720	Almost Sure Stability of Nonlinear Systems Under Random and Impulsive Sequential Attacks. IEEE Transactions on Automatic Control, 2020, 65, 3879-3886.	3.6	84
721	Cyber risks of PMU networks with observation errors: Assessment and mitigation. Reliability Engineering and System Safety, 2020, 198, 106873.	5.1	7
722	Adversarial Attacks and Defenses on Cyberâ€“Physical Systems: A Survey. IEEE Internet of Things Journal, 2020, 7, 5103-5115.	5.5	45
723	Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants. Reliability Engineering and System Safety, 2020, 201, 106878.	5.1	26
724	A Methodology for Security Classification applied to Smart Grid Infrastructures. International Journal of Critical Infrastructure Protection, 2020, 28, 100342.	2.9	45
725	Data-Driven False Data-Injection Attack Design and Detection in Cyber-Physical Systems. IEEE Transactions on Cybernetics, 2021, 51, 6179-6187.	6.2	42
726	A Secure Hybrid Dynamic-State Estimation Approach for Power Systems Under False Data Injection Attacks. IEEE Transactions on Industrial Informatics, 2020, 16, 7275-7286.	7.2	58
727	Blockchain for Internet of Energy management: Review, solutions, and challenges. Computer Communications, 2020, 151, 395-418.	3.1	207
728	Detection of False Data Injection Cyber-Attacks in DC Microgrids Based on Recurrent Neural Networks. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021, 9, 5294-5310.	3.7	114

#	Article	IF	Citations
729	Deep Reinforcement Learning for Partially Observable Data Poisoning Attack in Crowdsensing Systems. IEEE Internet of Things Journal, 2020, 7, 6266-6278.	5.5	98
730	Detection and Isolation of False Data Injection Attacks in Smart Grid via Unknown Input Interval Observer. IEEE Internet of Things Journal, 2020, 7, 3214-3229.	5.5	33
731	Extremely Randomized Trees-Based Scheme for Stealthy Cyber-Attack Detection in Smart Grid Networks. IEEE Access, 2020, 8, 19921-19933.	2.6	84
732	PMU Placement Optimization for Efficient State Estimation in Smart Grid. IEEE Journal on Selected Areas in Communications, 2020, 38, 71-83.	9.7	23
733	Cloud control systems venture. , 2020, , 19-49.		0
734	SMSâ€“A Security Management System for Steam Turbines Using a Multisensor Array. IEEE Systems Journal, 2020, 14, 3813-3824.	2.9	11
735	On the Silent Perturbation of State Estimation in Smart Grid. IEEE Transactions on Industry Applications, 2020, , 1-1.	3.3	7
737	False data injection attacks on inverter-based microgrid in autonomous mode. , 2020, , 125-146.		6
738	Resilient model-free adaptive control for cyber-physical systems against jamming attack. Neurocomputing, 2020, 413, 422-430.	3.5	41
739	False data injection attacks and countermeasures in smart microgrid systems. , 2020, , 263-279.		1
740	A Robust Dynamic Compensation Approach for Cyber-Physical Systems Against Multiple Types of Actuator Attacks. Applied Mathematics and Computation, 2020, 380, 125284.	1.4	16
741	Statistical Approach to Detection of Attacks for Stochastic Cyber-Physical Systems. IEEE Transactions on Automatic Control, 2021, 66, 849-856.	3.6	9
742	Event-Based Formation Control for Nonlinear Multiagent Systems Under DoS Attacks. IEEE Transactions on Automatic Control, 2021, 66, 452-459.	3.6	141
743	Secure Information Fusion using Local Posterior for Distributed Cyber-Physical Systems. IEEE Transactions on Mobile Computing, 2021, 20, 2041-2054.	3.9	2
744	The Vulnerability of Cyber-Physical System Under Stealthy Attacks. IEEE Transactions on Automatic Control, 2021, 66, 637-650.	3.6	69
745	Time Synchronization Attack and Countermeasure for Multisystem Scheduling in Remote Estimation. IEEE Transactions on Automatic Control, 2021, 66, 916-923.	3.6	8
746	Interval Observer-Based Detection and Localization Against False Data Injection Attack in Smart Grids. IEEE Internet of Things Journal, 2021, 8, 657-671.	5.5	32
747	Smart Grid Security Enhancement by Using Belief Propagation. IEEE Systems Journal, 2021, 15, 2046-2057.	2.9	8

#	Article	IF	Citations
748	Distributed Attack Detection in a Water Treatment Plant: Method and Case Study. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 86-99.	3.7	82
749	A novel trust-based false data detection method for power systems under false data injection attacks. Journal of the Franklin Institute, 2021, 358, 56-73.	1.9	12
750	Timely detection and mitigation of IoT-based cyberattacks in the smart grid. Journal of the Franklin Institute, 2021, 358, 172-192.	1.9	17
751	Optimal Ïµ -stealthy attack in cyber-physical systems. Journal of the Franklin Institute, 2021, 358, 151-171.	1.9	8
752	R-Print: A System Residuals-Based Fingerprinting for Attack Detection in Industrial Cyber-Physical Systems. IEEE Transactions on Industrial Electronics, 2021, 68, 11458-11469.	5.2	7
753	Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach. IEEE Transactions on Smart Grid, 2021, 12, 623-634.	6.2	123
754	TOTAL: Optimal Protection Strategy Against Perfect and Imperfect False Data Injection Attacks on Power Grid Cyberâ€“Physical Systems. IEEE Internet of Things Journal, 2021, 8, 1001-1015.	5.5	19
755	A degradation-based detection framework against covert cyberattacks on SCADA systems. IISE Transactions, 2021, 53, 812-829.	1.6	10
756	Data-Driven Attack Detection for Linear Systems. , 2021, 5, 671-676.		14
757	Data-Driven False Data Injection Attacks Against Power Grids: A Random Matrix Approach. IEEE Transactions on Smart Grid, 2021, 12, 635-646.	6.2	38
758	On the Complexity and Approximability of Optimal Sensor Selection and Attack for Kalman Filtering. IEEE Transactions on Automatic Control, 2021, 66, 2146-2161.	3.6	15
759	A Moving Target Defense for Securing Cyber-Physical Systems. IEEE Transactions on Automatic Control, 2021, 66, 2016-2031.	3.6	38
760	A secure distributed ledger for transactive energy: The Electron Volt Exchange (EVE) blockchain. Applied Energy, 2021, 282, 116208.	5.1	24
761	Security of Power Line Communication systems: Issues, limitations and existing solutions. Computer Science Review, 2021, 39, 100331.	10.2	20
762	A Descriptor System design framework for false data injection attack toward power systems. Electric Power Systems Research, 2021, 192, 106932.	2.1	10
763	A Binary-Optimization-Based Coordinated Cyber-Physical Attack for Disrupting Electricity Market Operation. IEEE Systems Journal, 2021, 15, 2619-2629.	2.9	4
764	Secure State Estimation Using Hybrid Homomorphic Encryption Scheme. IEEE Transactions on Control Systems Technology, 2021, 29, 1704-1720.	3.2	20
765	Stealthy MTD Against Unsupervised Learning-Based Blind FDI Attacks in Power Systems. IEEE Transactions on Information Forensics and Security, 2021, 16, 1275-1287.	4.5	26

#	Article	IF	Citations
766	Cybersecurity of Wide Area Monitoring, Protection, and Control Systems for HVDC Applications. IEEE Transactions on Power Systems, 2021, 36, 592-602.	4.6	25
767	Distributed Data-Driven Intrusion Detection for Sparse Stealthy FDI Attacks in Smart Grids. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68, 993-997.	2.2	26
768	A Detection Mechanism Against Load-Redistribution Attacks in Smart Grids. IEEE Transactions on Smart Grid, 2021, 12, 704-714.	6.2	37
769	Detecting Generalized Replay Attacks via Time-Varying Dynamic Watermarking. IEEE Transactions on Automatic Control, 2021, 66, 3502-3517.	3.6	36
770	Data Integrity Attacks Against Outage Management Systems. IEEE Transactions on Engineering Management, 2022, 69, 765-772.	2.4	5
771	A two-step trace model for the detection of UVI attacks against power grids in the wireless network. Soft Computing, 2021, 25, 5199-5207.	2.1	0
772	Privacy-Preserving Schemes for Safeguarding Heterogeneous Data Sources in Cyber-Physical Systems. IEEE Access, 2021, 9, 55077-55097.	2.6	25
773	How to Employ Competitive Smart Home Retailers to React to Cyberattacks in Smart Cities?. Power Systems, 2021, , 63-92.	0.3	1
774	Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack. IEEE Access, 2021, 9, 16488-16507.	2.6	32
775	Cyberattack Detection for Converter-Based Distributed dc Microgrids: Observer-Based Approaches. IEEE Industrial Electronics Magazine, 2022, 16, 67-77.	2.3	17
776	Smart Grid Cyber-Physical Attack and Defense: A Review. IEEE Access, 2021, 9, 29641-29659.	2.6	108
777	A Secured Advanced Management Architecture in Peer-to-Peer Energy Trading for Multi-Microgrid in the Stochastic Environment. IEEE Access, 2021, 9, 92083-92100.	2.6	45
778	Active Detection Against Replay Attack: A Survey on Watermark Design for Cyber-Physical Systems. Lecture Notes in Control and Information Sciences, 2021, , 145-171.	0.6	7
779	Intrusion Detection Against MMS-Based Measurement Attacks at Digital Substations. IEEE Access, 2021, 9, 1240-1249.	2.6	9
780	Cyber security in power electronic systems. , 2021, , 199-220.		1
781	Blockchain-Based Decentralized Replay Attack Detection for Large-Scale Power Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52, 4727-4739.	5.9	23
782	A Review of Cyberâ€“Physical Security for Photovoltaic Systems. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2022, 10, 4879-4901.	3.7	47
783	Detection of Stealthy Cyber Intrusion in Smart Electric Grid Using Advanced State Estimation. , 2021, , .		1

#	Article	IF	Citations
784	Confidence-aware collaborative detection mechanism for false data attacks in smart grids. Soft Computing, 2021, 25, 5607-5618.	2.1	4
785	False Data Injection Attack in a Platoon of CACC: Real-Time Detection and Isolation With a PDE Approach. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 8692-8703.	4.7	18
786	An Optimal PMU Placement Scheme for Detection of Malicious Attacks in Smart Grid. , 2021, , .		0
787	A brief review on attack design and detection strategies for networked cyber-physical systems. Turkish Journal of Engineering, 2021, 5, 1-7.	0.7	1
788	State estimation in electric power systems. , 2021, , 1-8.		0
789	Security Analysis for Dynamic State Estimation of Power Systems With Measurement Delays. IEEE Transactions on Cybernetics, 2023, 53, 2087-2096.	6.2	29
790	A Subgrid-Oriented Privacy-Preserving Microservice Framework Based on Deep Neural Network for False Data Injection Attack Detection in Smart Grids. IEEE Transactions on Industrial Informatics, 2022, 18, 1957-1967.	7.2	32
791	Distributed Event-Triggered Consensus-Based Control of DC Microgrids in Presence of DoS Cyber Attacks. IEEE Access, 2021, 9, 54009-54021.	2.6	13
792	A Federated Learning Framework for Detecting False Data Injection Attacks in Solar Farms. IEEE Transactions on Power Electronics, 2022, 37, 2496-2501.	5.4	26
793	A Bibliometric Analysis of Power System Planning Research During 1971â€“2020. IEEE Transactions on Power Systems, 2022, 37, 2283-2296.	4.6	9
794	Resilient Collaborative Distributed AC Optimal Power Flow Against False Data Injection Attacks: A Theoretical Framework. IEEE Transactions on Smart Grid, 2022, 13, 795-806.	6.2	4
795	A Remedial Action Scheme Against False Data Injection Cyberattacks in Smart Transmission Systems: Application of Thyristor-Controlled Series Capacitor (TCSC). IEEE Transactions on Industrial Informatics, 2022, 18, 2297-2309.	7.2	16
796	Leader-Following Consensus of Multiple Euler-Lagrange Systems Under Deception Attacks. IEEE Access, 2021, 9, 100548-100557.	2.6	4
797	Boundary Defense Against Cyber Threat for Power System State Estimation. IEEE Transactions on Information Forensics and Security, 2021, 16, 1752-1767.	4.5	13
799	Revealing a New Vulnerability of Distributed State Estimation: A Data Integrity Attack and an Unsupervised Detection Algorithm. IEEE Transactions on Control of Network Systems, 2022, 9, 706-718.	2.4	10
800	Metaheuristic Techniques in Attack and Defense Strategies for Cybersecurity: AÂSystematic Review. Studies in Computational Intelligence, 2021, , 449-467.	0.7	5
801	Cyber Attack Detection and Correction Mechanism in Distributed DC Microgrid. IEEE Transactions on Power Electronics, 2021, , 1-1.	5.4	11
802	Lyapunov-Based Control of a Nonlinear Multiagent System With a Time-Varying Input Delay Under False-Data-Injection Attacks. IEEE Transactions on Industrial Informatics, 2022, 18, 2693-2703.	7.2	28

#	Article	IF	Citations
803	Distributed Detection and Mitigation of Biasing Attacks Over Multi-Agent Networks. IEEE Transactions on Network Science and Engineering, 2021, 8, 3465-3477.	4.1	5
804	Secure Dynamic Nonlinear Heterogeneous Vehicle Platooning: Denial-of-Service Cyber-Attack Case. Studies in Systems, Decision and Control, 2021, , 287-315.	0.8	4
805	Convex Optimization of Cyberattacks Overflowing Multiple Lines in Cyber-Physical Power Systems. IEEE Systems Journal, 2022, 16, 5224-5233.	2.9	0
806	Sparse Actuator and Sensor Attacks Reconstruction for Linear Cyber-Physical Systems With Sliding Mode Observer. IEEE Transactions on Industrial Informatics, 2022, 18, 3873-3884.	7.2	20
807	Cyber Attack Detection Scheme for a Load Frequency Control System Based on Dual-Source Data of Compromised Variables. Applied Sciences (Switzerland), 2021, 11, 1584.	1.3	6
808	DIACS: A Blockchain-based Model for Systematic Data Integrity Assessment and Control. , 2021, , .		0
809	Analyzing the effects of cyberattacks on distribution system state estimation. , 2021, , .		2
810	Coordinated Control of Virtual Power Plants to Improve Power System Short-Term Dynamics. Energies, 2021, 14, 1182.	1.6	20
811	Design and Development of a Cyber Security Framework for National Time Dissemination. SN Computer Science, 2021, 2, 1.	2.3	0
812	The safety region-based model predictive control for discrete-time systems under deception attacks. International Journal of Systems Science, 2021, 52, 2144-2160.	3.7	5
813	A domain-specific language to design false data injection tests for air traffic control systems. International Journal on Software Tools for Technology Transfer, 2022, 24, 127-158.	1.7	3
814	Social Collective Attack Model and Procedures for Large-Scale Cyber-Physical Systems. Sensors, 2021, 21, 991.	2.1	3
815	Revealing Structural and Functional Vulnerability of Power Grids to Cascading Failures. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2021, 11, 133-143.	2.7	16
816	A Data-Driven Model Predictive Control for Alleviating Thermal Overloads in the Presence of Possible False Data. IEEE Transactions on Industry Applications, 2021, 57, 1872-1881.	3.3	15
817	Cyberattacks identification in IEC 61850 based substation using proximal support vector machine. Journal of Intelligent and Fuzzy Systems, 2022, 42, 1213-1222.	0.8	7
818	Based on random game Petri net model CPS risk assessment and defense decision of distribution network. , 2021, , .		3
819	Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecurity, 2021, 4, .	3.1	7
820	Review of Design Elements within Power Infrastructure Cyberâ€"Physical Test Beds as Threat Analysis Environments. Energies, 2021, 14, 1409.	1.6	5

#	Article	IF	Citations
821	Low-Complexity Quickest Change Detection in Linear Systems With Unknown Time-Varying Pre- and Post-Change Distributions. IEEE Transactions on Information Theory, 2021, 67, 1804-1824.	1.5	8
822	Data trustworthiness signatures for nuclear reactor dynamics simulation. Progress in Nuclear Energy, 2021, 133, 103612.	1.3	5
823	Enhanced cyberâ€physical security using attackâ€resistant cyber nodes and eventâ€triggered moving target defence. IET Cyber-Physical Systems: Theory and Applications, 2021, 6, 12-26.	1.9	4
824	Detection of False Data Injection Attacks Based on Kalman Filter and Controller Design in Power System LFC. Journal of Physics: Conference Series, 2021, 1861, 012120.	0.3	3
825	Advanced Network Sampling with Heterogeneous Multiple Chains. Sensors, 2021, 21, 1905.	2.1	0
826	A combined survey on distribution system state estimation and false data injection in cyberâ€physical power distribution networks. IET Cyber-Physical Systems: Theory and Applications, 2021, 6, 41-62.	1.9	14
827	False Data Injection Attack Detection in Power Systems Based on Cyber-Physical Attack Genes. Frontiers in Energy Research, 2021, 9, .	1.2	21
828	Cyber Attacks and Faults Discrimination in Intelligent Electronic Device-Based Energy Management Systems. Electronics (Switzerland), 2021, 10, 650.	1.8	6
829	Validation of Covert Cognizance Active Defenses. Nuclear Science and Engineering, 2021, 195, 977-989.	0.5	0
830	Detection and localization of biased load attacks in smart grids via interval observer. Information Sciences, 2021, 552, 291-309.	4.0	9
831	Observer-Based Attack Detection and Mitigation for Cyberphysical Systems: A Review. IEEE Systems, Man, and Cybernetics Magazine, 2021, 7, 35-60.	1.2	35
832	Attack detection design for dc microgrid using eigenvalue assignment approach. Energy Reports, 2021, 7, 469-476.	2.5	18
833	Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. Electrical Engineering, 2022, 104, 259-282.	1.2	32
834	Towards Secure Fog Computing: A Survey on Trust Management, Privacy, Authentication, Threats and Access Control. Electronics (Switzerland), 2021, 10, 1171.	1.8	30
835	Systematic planning of moving target defence for maximising detection effectiveness against false data injection attacks in smart grid. IET Cyber-Physical Systems: Theory and Applications, 2021, 6, 151-163.	1.9	6
836	A Secure Control Design for Networked Control System with Nonlinear Dynamics under False-Data-Injection Attacks. , 2021, , .		3
837	Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation. Energies, 2021, 14, 2657.	1.6	17
838	Spatial-Temporal Correlation-Concerned Measurement Manipulation Detection Based on Gramian Angular Summation Field and Convolutional Neural Networks. , 2021, , .		1

#	Article	IF	Citations
839	Distributed nonlinear state estimation using adaptive penalty parameters with load characteristics in the Electricity Reliability Council of Texas. Journal of Industrial Information Integration, 2021, 24, 100223.	4.3	3
840	Review of Cyber-Physical Attacks in Smart Grids: A System-Theoretic Perspective. Electronics (Switzerland), 2021, 10, 1153.	1.8	15
841	Hierarchical Clustering Detection Based Secure Fusion Filtering for Multiple False Data Injection Attacks. , 2021, , .		0
842	Reinforcement Learning based Multistage Optimal PMU Placement Against Data Integrity Attacks in Smart Grid. , 2021, , .		2
843	Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method. Computers and Electrical Engineering, 2021, 91, 107058.	3.0	16
844	Data-Driven Probabilistic Anomaly Detection for Electricity Market under Cyber Attacks. , 2021, , .		1
845	Key-Leakage Resilient Encrypted Data Aggregation With Lightweight Verification in Fog-Assisted Smart Grids. IEEE Internet of Things Journal, 2021, 8, 8234-8245.	5.5	10
846	Optimal Linear FDI Attacks with Side Information: A Comparative Study. , 2021, , .		8
847	Designing Constraint-Based False Data-Injection Attacks Against the Unbalanced Distribution Smart Grids. IEEE Internet of Things Journal, 2021, 8, 9422-9435.	5.5	19
848	Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids. Sustainable Cities and Society, 2021, 75, 103116.	5.1	35
849	A Deep Learning-Based Classification Scheme for False Data Injection Attack Detection in Power System. Electronics (Switzerland), 2021, 10, 1459.	1.8	9
850	On the security of ANN-based AC state estimation in smart grid. Computers and Security, 2021, 105, 102265.	4.0	6
851	Adversarial Classification of the Attacks on Smart Grids Using Game Theory and Deep Learning. , 2021, , .		0
852	Deep Learning-based Anomaly Detection in Cyber-physical Systems. ACM Computing Surveys, 2022, 54, 1-36.	16.1	101
853	A Systematic Literature Review on Malicious Use of Reinforcement Learning. , 2021, , .		1
854	An Ensemble Classifier Based Scheme for Detection of False Data Attacks Aiming at Disruption of Electricity Market Operation. Journal of Network and Systems Management, 2021, 29, 1.	3.3	4
855	On the Security of Networked Control Systems in Smart Vehicle and Its Adaptive Cruise Control. IEEE Transactions on Intelligent Transportation Systems, 2021, 22, 3824-3831.	4.7	28
856	Detection of attacks and intrusions on automotive engine IoT sensors. , 2021, , .		2

#	Article	IF	Citations
857	Trust in Power System State Variables based on Trust in Measurements. , 2021, , .		1
858	Synchrophasor Data Under GPS Spoofing: Attack Detection and Mitigation Using Residuals. IEEE Transactions on Smart Grid, 2021, 12, 3415-3424.	6.2	11
859	DDAF: Deceptive Data Acquisition Framework against Stealthy Attacks in Cyber-Physical Systems. , 2021, , .		0
860	A Bi-Level Model for Detecting and Correcting Parameter Cyber-Attacks in Power System State Estimation. Applied Sciences (Switzerland), 2021, 11, 6540.	1.3	9
861	Spoofing Resilient State Estimation for the Power Grid Using an Extended Kalman Filter. IEEE Transactions on Smart Grid, 2021, 12, 3404-3414.	6.2	7
862	False Data Injection Attacks Detection in Smart Grid: A Structural Sparse Matrix Separation Method. IEEE Transactions on Network Science and Engineering, 2021, 8, 2545-2558.	4.1	30
863	Stacked Autoencoder Framework of False Data Injection Attack Detection in Smart Grid. Mathematical Problems in Engineering, 2021, 2021, 1-8.	0.6	3
864	An Artificial Intelligence Empowered Cyber Physical Ecosystem for Energy Efficiency and Occupation Health and Safety. Energies, 2021, 14, 4214.	1.6	2
865	State-of-the-Art of Optimal Active and Reactive Power Flow: A Comprehensive Review from Various Standpoints. Processes, 2021, 9, 1319.	1.3	33
866	Decentralized Coordinated Cyberattack Detection and Mitigation Strategy in DC Microgrids Based on Artificial Neural Networks. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021, 9, 4629-4638.	3.7	51
867	A Bayesian Rule Learning Based Intrusion Detection System for the MQTT Communication Protocol. , 2021, , .		3
868	Strategic PMU placement to alleviate power system vulnerability against cyber attacks. Energy Conversion and Economics, 2021, 2, 212-220.	1.9	6
869	Integrating Security Behavior into Attack Simulations. , 2021, , .		5
870	Triâ€level defense strategy for <scp>electricityâ€gas</scp> integrated systems against load redistribution attacks. International Transactions on Electrical Energy Systems, 2021, 31, e13062.	1.2	1
871	A Network Parameter Database False Data Injection Correction Physics-Based Model: A Machine Learning Synthetic Measurement-Based Approach. Applied Sciences (Switzerland), 2021, 11, 8074.	1.3	4
872	Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. Applied Sciences (Switzerland), 2021, 11, 7228.	1.3	10
873	Cyber-Resilience Enhancement and Protection for Uneconomic Power Dispatch Under Cyber-Attacks. IEEE Transactions on Power Delivery, 2021, 36, 2253-2263.	2.9	11
874	Dynamic State Estimation of Smart Grid Based on CKF under False Data Injection Attacks. , 2021, , .		0

#	Article	IF	Citations
875	A Novel Technique to Detect False Data Injection Attacks on Phasor Measurement Units. Sensors, 2021, 21, 5791.	2.1	7
876	Advancements and Research Trends in Microgrids Cybersecurity. Applied Sciences (Switzerland), 2021, 11, 7363.	1.3	16
877	Mitigating Concurrent False Data Injection Attacks in Cooperative DC Microgrids. IEEE Transactions on Power Electronics, 2021, 36, 9637-9647.	5.4	39
878	A deep learningâ€based classification scheme for cyberâ€attack detection in power system. IET Energy Systems Integration, 2021, 3, 274-284.	1.1	5
879	Physical layer attack identification and localization in cyberâ€“physical grid: An ensemble deep learning based approach. Physical Communication, 2021, 47, 101394.	1.2	17
880	Iterative State Estimation With Weight Tuning and Pseudo-Measurement Generation. IEEE Systems Journal, 2021, 15, 3165-3172.	2.9	2
881	A tri-level optimization model for power grid defense with the consideration of post-allocated DGs against coordinated cyber-physical attacks. International Journal of Electrical Power and Energy Systems, 2021, 130, 106903.	3.3	19
882	Cyber Risks to Critical Smart Grid Assets of Industrial Control Systems. Energies, 2021, 14, 5501.	1.6	9
883	Analysis of false data injection attacks in power systems: A dynamic Bayesian game-theoretic approach. ISA Transactions, 2021, 115, 108-123.	3.1	15
884	A secure strategy for a cyber physical system with multi-sensor under linear deception attack. Journal of the Franklin Institute, 2021, 358, 6666-6683.	1.9	14
885	Design of a coordinated cyber-physical attack in IoT based smart grid under limited intruder accessibility. International Journal of Critical Infrastructure Protection, 2021, 35, 100484.	2.9	5
886	Zero-dynamics attacks on networked control systems. Journal of Process Control, 2021, 105, 99-107.	1.7	3
887	Mahalanobis distance-based robust approaches against false data injection attacks on dynamic power state estimation. Computers and Security, 2021, 108, 102326.	4.0	0
888	Machine learning based false data injection in smart grid. International Journal of Electrical Power and Energy Systems, 2021, 130, 106819.	3.3	22
889	Optimal Planning and Operation of Hidden Moving Target Defense for Maximal Detection Effectiveness. IEEE Transactions on Smart Grid, 2021, 12, 4447-4459.	6.2	22
890	Cybersecurity in Power Grids: Challenges and Opportunities. Sensors, 2021, 21, 6225.	2.1	55
891	Defending against false data injection attack on demand response program: A bi-level strategy. Sustainable Energy, Grids and Networks, 2021, 27, 100506.	2.3	13
892	CPMTD: Cyber-physical moving target defense for hardening the security of power system against false data injected attack. Computers and Security, 2021, 111, 102465.	4.0	15

#	Article	IF	Citations
893	Real-time Attack-recovery for Cyber-physical Systems Using Linear-quadratic Regulator. Transactions on Embedded Computing Systems, 2021, 20, 1-24.	2.1	10
894	A novel secure observer-based controller and attack detection scheme for Networked Control Systems. Information Sciences, 2021, 575, 185-205.	4.0	4
895	Integrated Cyber and Physical Anomaly Location and Classification in Power Distribution Systems. IEEE Transactions on Industrial Informatics, 2021, 17, 7040-7049.	7.2	26
896	Real-Time Detection of Cyber-Physical False Data Injection Attacks on Power Systems. IEEE Transactions on Industrial Informatics, 2021, 17, 6810-6819.	7.2	17
897	The vulnerability of distributed state estimator under stealthy attacks. Automatica, 2021, 133, 109869.	3.0	18
898	Multi-objective cost-effective optimization for defending against false data injection attacks in power system operation. Electric Power Systems Research, 2021, 200, 107469.	2.1	3
899	A remedial action framework against cyberattacks targeting energy hubs integrated with distributed energy resources. Applied Energy, 2021, 304, 117895.	5.1	17
900	Optimal Attack Strategy Against Fault Detectors for Linear Cyber-Physical Systems. Information Sciences, 2021, 581, 390-402.	4.0	8
901	Distributed dynamic state-input estimation for power networks of Microgrids and active distribution systems with unknown inputs. Electric Power Systems Research, 2021, 201, 107510.	2.1	10
902	Protection of large-scale smart grids against false data injection cyberattacks leading to blackouts. International Journal of Critical Infrastructure Protection, 2021, 35, 100457.	2.9	13
903	CShield: Enabling code privacy for Cyberâ€"Physical systems. Future Generation Computer Systems, 2021, 125, 564-574.	4.9	3
904	Data-Driven Resilient Automatic Generation Control Against False Data Injection Attacks. IEEE Transactions on Industrial Informatics, 2021, 17, 8092-8101.	7.2	51
905	On Joint Reconstruction of State and Input-Output Injection Attacks for Nonlinear Systems. , 2022, 6, 554-559.		2
906	Measurement-driven blind topology estimation for sparse data injection attack in energy system. Electric Power Systems Research, 2022, 202, 107593.	2.1	4
907	Stochastic Denial-of-Service Attack Allocation in Leader-Following Multiagent Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52, 2848-2857.	5.9	9
908	Spatio-Temporal Correlation-Based False Data Injection Attack Detection Using Deep Convolutional Neural Network. IEEE Transactions on Smart Grid, 2022, 13, 750-761.	6.2	21
909	A New AC False Data Injection Attack Method Without Network Information. IEEE Transactions on Smart Grid, 2021, 12, 5280-5289.	6.2	17
910	Detection of Attacks in Cyber-Physical Systems: Theory and Applications. Lecture Notes in Control and Information Sciences, 2021, , 79-98.	0.6	1

#	Article	IF	Citations
911	Intrusion Detection, Measurement Correction, and Attack Localization of PMU Networks. IEEE Transactions on Industrial Electronics, 2022, 69, 4697-4706.	5.2	11
912	Gross error processing in measurements. , 2021, , 161-182.		0
914	Profit-Oriented False Data Injection Attack Against Wind Farms and Countermeasures. IEEE Systems Journal, 2022, 16, 3700-3710.	2.9	4
915	KFRNN: An Effective False Data Injection Attack Detection in Smart Grid Based on Kalman Filter and Recurrent Neural Network. IEEE Internet of Things Journal, 2022, 9, 6893-6904.	5.5	34
916	A Spatiotemporal and Multivariate Attribute Correlation Extraction Scheme for Detecting Abnormal Nodes in WSNs. IEEE Access, 2021, 9, 135266-135284.	2.6	7
918	Map-Based Localization Under Adversarial Attacks. Springer Proceedings in Advanced Robotics, 2020, , 775-790.	0.9	6
919	Preserving User Privacy in the Smart Grid by Hiding Appliance Load Characteristics. Lecture Notes in Computer Science, 2013, , 67-80.	1.0	3
920	SRID: State Relation Based Intrusion Detection for False Data Injection Attacks in SCADA. Lecture Notes in Computer Science, 2014, , 401-418.	1.0	48
922	Super Resolution Perception for Improving Data Completeness in Smart Grid State Estimation. Engineering, 2020, 6, 789-800.	3.2	22
923	Cyber attacks in smart grid â€" dynamic impacts, analyses and recommendations. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 321-329.	1.9	11
924	Stochastic games for power grid coordinated defence against coordinated attacks. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 292-300.	1.9	5
925	Wyner wiretapâ€like encoding scheme for cyberâ€physical systems. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 359-365.	1.9	3
926	Deep learning based method for false data injection attack detection in AC smart islands. IET Generation, Transmission and Distribution, 2020, 14, 5756-5765.	1.4	47
927	Resilient wireless sensor networks for cyber-physical systems. , 2016, , 239-267.		5
928	Detecting Cyber-Physical Attacks in Water Distribution Systems: One-Class Classifier Approach. Journal of Water Resources Planning and Management - ASCE, 2020, 146, .	1.3	11
929	Electric Power Grid Resilience to Cyber Adversaries: State of the Art. IEEE Access, 2020, 8, 87592-87608.	2.6	56
930	Deep Learning Based Covert Attack Identification for Industrial Control Systems. , 2020, , .		8
931	Net Load Redistribution Attacks on Nodal Voltage Magnitude Estimation in AC Distribution Networks. , 2020, , .		7

#	Article	IF	Citations
932	Brief Survey on Attack Detection Methods for Cyber-Physical Systems. IEEE Systems Journal, 2020, 14, 5329-5339.	2.9	101
933	False Data Injection Cyber Range of Modernized Substation System. , 2020, , .		9
934	Robust and Adaptive Sequential Submodular Optimization. IEEE Transactions on Automatic Control, 2022, 67, 89-104.	3.6	6
935	Joint Cyber and Physical Attacks on Power Grids. Performance Evaluation Review, 2015, 43, 361-374.	0.4	6
936	A Data-Driven Approach to Distinguish Cyber-Attacks from Physical Faults in a Smart Grid. , 2015, , .		21
937	LiS: Lightweight Signature Schemes for Continuous Message Authentication in Cyber-Physical Systems. , 2020, , .		10
938	Analyzing Cyber-Physical Systems from the Perspective of Artificial Intelligence. , 2019, , .		9
939	Active fuzzing for testing and securing cyber-physical systems. , 2020, , .		15
940	DIDEROT. , 2020, , .		23
941	Constrained Concealment Attacks against Reconstruction-based Anomaly Detectors in Industrial Control Systems. , 2020, , .		28
942	A survey of methods supporting cyber situational awareness in the context of smart cities. Journal of Big Data, 2020, 7, .	6.9	19
943	powerLang: a probabilistic attack simulation language for the power domain. Energy Informatics, 2020, 3, .	1.4	18
944	Smart Cities: A Survey on Security Concerns. International Journal of Advanced Computer Science and Applications, 2016, 7, .	0.5	81
945	Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis. , 2017, , .		53
946	Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit. , 2017, , .		108
947	IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT. , 2019, , .		125
948	DefRec: Establishing Physical Function Virtualization to Disrupt Reconnaissance of Power Grids' Cyber-Physical Infrastructures. , 2020, , .		9
949	Enhancing Security for Voltage Control of Distribution Systems Under Data Falsification Attacks. , 2019, , .		3

#	Article	IF	Citations
950	Critical Infrastructure Security. Advances in Information Security, Privacy, and Ethics Book Series, 2020, , 134-162.	0.4	4
951	Climate Change and Energy Management Strategies. Computational Water Energy and Environmental Engineering, 2017, 06, 143-153.	0.4	2
952	A Fog Computing based Smart Grid Cloud Data Security. International Journal of Applied Information Systems, 2016, 10, 1-6.	0.1	3
953	Protection Strategies Against False Data Injection Attacks with Uncertain Information on Electric Power Grids. Journal of Electrical Engineering and Technology, 2017, 12, 19-28.	1.2	5
954	Accurate Detection of False Data Injection Attacks in Renewable Power Systems Using Deep Learning. IEEE Access, 2021, 9, 135774-135789.	2.6	11
955	Bayesian Approximation Filtering With False Data Attack on Network. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58, 976-988.	2.6	5
956	Joint Detection and Localization of Stealth False Data Injection Attacks in Smart Grids Using Graph Neural Networks. IEEE Transactions on Smart Grid, 2022, 13, 807-819.	6.2	39
957	Cyber attacks targeting electronic devices of power systems and countermeasures. IEICE Electronics Express, 2021, 18, 20210406-20210406.	0.3	0
958	Privacy-Preserving Computation for Large-Scale Security-Constrained Optimal Power Flow Problem in Smart Grid. IEEE Access, 2021, 9, 148144-148155.	2.6	2
959	Event-based adaptive compensation control of nonlinear cyber-physical systems under actuator failure and false data injection attack. , 2021, , .		3
960	Real-time Identification of False Data Injection Attack in Smart Grid. , 2021, , .		8
961	Personalized Privacy Preservation for Smart Grid. , 2021, , .		1
962	Security weakness of dynamic watermarking-based detection for generalised replay attacks. International Journal of Systems Science, 2022, 53, 948-966.	3.7	6
963	Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research. Energy Reports, 2021, 7, 6530-6564.	2.5	58
964	A Survey of Research on Smart Grid Security. Communications in Computer and Information Science, 2012, , 395-405.	0.4	5
968	Biologically Inspired Hierarchical Cyber-Physical Multi-agent Distributed Control Framework for Sustainable Smart Grids. Power Systems, 2015, , 219-259.	0.3	4
969	System-state-free false data injection attack for nonlinear state estimation in smart grid. International Journal of Smart Grid and Clean Energy, 2015, , .	0.4	2
971	Cloud Computing for Transportation Cyber-Physical Systems. , 2015, , 370-389.		7

#	Article	IF	Citations
972	A Survey on the Cyber Attacks Against Non-linear State Estimation in Smart Grids. Lecture Notes in Computer Science, 2016, , 40-56.	1.0	2
973	An Encryption Traffic Analysis Countermeasure Model Based on Game Theory. Lecture Notes in Computer Science, 2018, , 285-292.	1.0	0
974	State Estimation of Electric Power System under DOS-attacks on SCADA system and WAMS. , 2018, , .		2
975	Adversarial False Data Injection Attack Against Nonlinear AC State Estimation with ANN in Smart Grid. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2019, , 365-379.	0.2	7
976	Overview of Data Aggregation Schemes in a Smart Grid AMI Network. Journal of Communications, 2019, , 787-801.	1.3	2
977	A Framework for Joint Attack Detection and Control Under False Data Injection. Lecture Notes in Computer Science, 2019, , 352-363.	1.0	4
978	Trust-Based Control and Scheduling for UGV Platoon under Cyber Attacks. , 0, , .		9
979	Dynamic Attacks Against Inverter-Based Microgrids. , 2019, , .		4
980	Protecting the grid topology and user consumption patterns during state estimation in smart grids based on data obfuscation. Energy Informatics, 2019, 2, .	1.4	1
981	Butterfly Attack: Adversarial Manipulation of Temporal Properties of Cyber-Physical Systems. , 2019, , .		6
982	Taxonomy of IoT Vulnerabilities. , 2020, , 7-58.		2
983	Cascading Failure Attacks in the Power System. , 2020, , 53-79.		0
984	Overview of Security for Smart Cyber-Physical Systems. , 2020, , 5-24.		8
985	SPNTA: Reliability Analysis Under Topology Attacksâ€"A Stochastic Petri Net Approach. Wireless Networks, 2020, , 41-74.	0.3	0
986	Detecting a Stealthy Attack in Distributed Control for Microgrids using Machine Learning Algorithms. , 2020, , .		8
987	Cyber-Attack Mitigation on Low Voltage Distribution Grids by Using a Novel Distribution System State Estimation Approach. Lecture Notes in Electrical Engineering, 2021, , 107-116.	0.3	0
988	Enhancing Cyber-Security of Distributed Robust State Estimation: Identification of Data Integrity Attacks in Multi-Operator Power System. , 2020, , .		1
989	Evasion Attacks with Adversarial Deep Learning Against Power System State Estimation. , 2020, , .		29

#	Article	IF	Citations
990	Method of amplitude data recovery in PMU measurements that considers synchronisation errors. IET Generation, Transmission and Distribution, 2020, 14, 5746-5755.	1.4	5
991	Effective Energy Management via False Data Detection Scheme for the Interconnected Smart Energy Hubâ€"Microgrid System under Stochastic Framework. Sustainability, 2021, 13, 11836.	1.6	25
992	Enhanced distributed state estimation with resilience to multiple disturbances and false data injection attacks. International Journal of Robust and Nonlinear Control, 2022, 32, 1075-1092.	2.1	10
993	A zonotopic set-invariance analysis of replay attacks affecting the supervisory layer. Systems and Control Letters, 2021, 157, 105056.	1.3	10
994	Bi-level Adversary-Operator Cyberattack Framework and Algorithms for Transmission Networks in Smart Grids. Advances in Intelligent Systems and Computing, 2020, , 183-202.	0.5	4
995	Protected Control System with RSA Encryption. Smart Innovation, Systems and Technologies, 2020, , 113-125.	0.5	1
996	Fundamentals and Related Literature. Wireless Networks, 2020, , 23-40.	0.3	0
997	Machine Learning Enabled Secure Collection of Phasor Data in Smart Power Grid Networks. , 2020, , .		1
999	Modelling Financially Motivated Cyber Attacks on Electricity Markets Using Mixed Integer Linear Programming. , 2020, , .		0
1000	Elliptic Envelope Based Detection of Stealthy False Data Injection Attacks in Smart Grid Control Systems. , 2020, , .		9
1001	Cyber Security Enhancement of Smart Grids Via Machine Learning - A Review. , 2020, , .		3
1002	A Stackelberg Security Investment Game for Voltage Stability of Power Systems. , 2020, , .		8
1003	Measurement Unit Placement Against Injection Attacks for the Secured Operation of an IIoT-Based Smart Grid. , 2020, , .		2
1004	Smart Grid Security: Attack Modeling from a CPS Perspective. , 2020, , .		1
1005	Real-Time Attack-Recovery for Cyber-Physical Systems Using Linear Approximations. , 2020, , .		25
1006	False Data Injection Attacks in Smart Grid Using Gaussian Mixture Model. , 2020, , .		0
1007	Stealthy monitoring-control attacks to disrupt power system operations. Electric Power Systems Research, 2022, 203, 107636.	2.1	1
1009	Cyber-Physical Security of Air Traffic Surveillance Systems. IFIP Advances in Information and Communication Technology, 2020, , 3-23.	0.5	0

#	Article	IF	Citations
1010	iDDAF: An Intelligent Deceptive Data Acquisition Framework for Secure Cyber-Physical Systems. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 338-359.	0.2	2
1012	Cyber Security for Voltage Control of Distribution Systems Under Data Falsification Attacks. Power Electronics and Power Systems, 2020, , 145-165.	0.6	0
1013	Distributed Bias Detection in Cyber-Physical Systems. IFIP Advances in Information and Communication Technology, 2020, , 245-260.	0.5	0
1014	Impact Analysis of False Data Injection Attack on Smart Grid State Estimation Under Random Packet Losses. Communications in Computer and Information Science, 2020, , 61-75.	0.4	2
1015	DHCD: Distributed Host-Based Collaborative Detection for FmDI Attacks. Wireless Networks, 2020, , 75-97.	0.3	0
1016	Secure Estimation of CPS with a Digital Twin. Advances in Information Security, 2020, , 115-138.	0.9	0
1017	Customized Attack Detection Under Power Industrial Control System. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2020, , 96-106.	0.2	1
1018	PFDD: On Feasibility and Limitations of Detecting FmDI Attacks Using D-FACTS. Wireless Networks, 2020, , 123-148.	0.3	0
1019	Anomaly Detection in Smart Grids using Machine Learning Techniques. , 2020, , .		22
1020	Semantic analysis framework for protecting the power grid against monitoringâ€control attacks. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 119-126.	1.9	5
1021	Data integrity attack detection in smart grid: a deep learning approach. International Journal of Security and Networks, 2020, 15, 15.	0.1	0
1023	Detecting Cyber-Physical-Attacks in AC microgrids using artificial neural networks. , 2021, , .		3
1024	Cyber Attack Estimation of Nonlinear DC Microgrids with Noisy Measurements: Spherical Simplex Radial CKF Approach. , 2021, , .		2
1025	Accuracy improvement of electrical load forecasting against new cyber-attack architectures. Sustainable Cities and Society, 2022, 77, 103523.	5.1	7
1026	Attack detection based on set-membership estimation. , 2020, , .		0
1027	Trust assessment of power system states. Energy Informatics, 2020, 3, .	1.4	5
1028	Model-Agnostic Algorithm for Real-Time Attack Identification in Power Grid using Koopman Modes. , 2020, , .		13
1029	Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods. IEEE Access, 2021, 9, 159291-159312.	2.6	10

#	Article	IF	Citations
1030	Joint Adversarial Example and False Data Injection Attacks for State Estimation in Power Systems. IEEE Transactions on Cybernetics, 2022, 52, 13699-13713.	6.2	26
1031	Attack Detection in Power Distribution Systems Using a Cyber-Physical Real-Time Reference Model. IEEE Transactions on Smart Grid, 2022, 13, 1490-1499.	6.2	17
1032	Malicious adversaries against secure state estimation: Sparse sensor attack design. Automatica, 2022, 136, 110037.	3.0	7
1033	Event-triggered adaptive compensation control for nonlinear cyber-physical systems under false data injection attacks. , 2021, , .		0
1034	A Data Driven Threat-Maximizing False Data Injection Attack Detection Method with Spatio-Temporal Correlation. , 2021, , .		0
1035	Deep learning-based probabilistic anomaly detection for solar forecasting under cyberattacks. International Journal of Electrical Power and Energy Systems, 2022, 137, 107752.	3.3	11
1036	Resiliency Improvement of an AC/DC Power Grid with Embedded LCC-HVDC Using Robust Power System State Estimation. Energies, 2021, 14, 7847.	1.6	5
1038	A modified model predictive control method for frequency regulation of microgrids under status feedback attacks and time-delay attacks. International Journal of Electrical Power and Energy Systems, 2022, 137, 107713.	3.3	11
1040	State Estimation Under Joint False Data Injection Attacks: Dealing With Constraints and Insecurity. IEEE Transactions on Automatic Control, 2022, 67, 6745-6753.	3.6	23
1041	Stealthy Hacking and Secrecy of Controlled State Estimation Systems With Random Dropouts. IEEE Transactions on Automatic Control, 2023, 68, 31-46.	3.6	4
1042	Electromagnetic Transients-Based Detection of Data Manipulation Attacks in Three Phase Radial Distribution Networks. IEEE Transactions on Industry Applications, 2022, 58, 667-677.	3.3	1
1043	Graph Neural Networks Based Detection of Stealth False Data Injection Attacks in Smart Grids. IEEE Systems Journal, 2022, 16, 2946-2957.	2.9	37
1044	Secure Control of DC Microgrids for Instant Detection and Mitigation of Cyber-Attacks Based on Artificial Intelligence. IEEE Systems Journal, 2022, 16, 2580-2591.	2.9	20
1045	Cyber Physical Systems: Analyses, challenges and possible solutions. Internet of Things and Cyber-physical Systems, 2021, 1, 22-33.	4.6	42
1046	Constrained-Differential-Evolution-Based Stealthy Sparse Cyber-Attack and Countermeasure in an AC Smart Grid. IEEE Transactions on Industrial Informatics, 2022, 18, 5275-5285.	7.2	30
1047	Cyber-Attack Detection for Photovoltaic Farms Based on Power-Electronics-Enabled Harmonic State Space Modeling. IEEE Transactions on Smart Grid, 2022, 13, 3929-3942.	6.2	11
1049	Online Characterization and Detection of False Data Injection Attacks in Wide-Area Monitoring Systems. IEEE Transactions on Power Systems, 2022, 37, 2549-2562.	4.6	5
1050	A planned scheduling process of cloud computing by an effective job allocation and fault-tolerant mechanism. Journal of Ambient Intelligence and Humanized Computing, 2022, 13, 1153-1171.	3.3	5

#	Article	IF	Citations
1051	Stealthy and profitable data injection attack on real time electricity market with network model uncertainties. Electric Power Systems Research, 2022, 205, 107742.	2.1	3
1052	Design of AC state estimation based cyber-physical attack for disrupting electricity market operation under limited sensor information. Electric Power Systems Research, 2022, 205, 107732.	2.1	8
1053	Design of False Data Injection Attack for Automatic Generation Control. , 2020, , .		0
1054	Training Strategies for Autoencoder-based Detection of False Data Injection Attacks. , 2020, , .		2
1055	Special Session: Noninvasive Sensor-Spoofing Attacks on Embedded and Cyber-Physical Systems. , 2020, , .		11
1056	Identification of Smart Grid Attacks via State Vector Estimator and Support Vector Machine Methods. , 2020, , .		0
1057	Cascading Failures of Power System with the Consideration of Cyber Attacks. , 2020, , .		1
1058	Generation of False Data Injection Attacks using Conditional Generative Adversarial Networks. , 2020, , .		7
1059	A Novel Design of Concurrent Cyber Attacks in Cooperative DC Microgrids. , 2020, , .		2
1060	Computation of Worst-case Operation Scenarios against False Data Injection Attacks Considering Load Demand and Generation Uncertainties. , 2020, , .		1
1061	Detection of False Data Injection Attack Based on Improved Distortion Index Method. , 2020, , .		1
1062	Detection of Undesired Events on Real-World SCADA Power System through Process Monitoring. , 2020, , .		2
1063	LSTM-Based False Data Injection Attack Detection in Smart Grids. , 2020, , .		6
1064	FDIA Detection through an Adaptive Multi-Level Features Classification in Smart Grids. , 2020, , .		1
1065	Detecting Cyber Attack Under Quantitative Impact of Demand Side Management. , 2020, , .		0
1066	Ranking Cyber Attack Vulnerability of Nodes in Power Transmission Network. , 2020, , .		0
1067	Detection Method for Tolerable False Data Injection Attack Based on Deep Learning Framework. , 2020, , .		5
1068	A Hybrid Security Solution for Mitigating Cyber-Attacks on Info-Communication Systems. , 2020, , .		3

#	Article	IF	Citations
1069	Power Grid State Estimation under General Cyber-Physical Attacks. , 2020, , .		2
1070	Information Theoretic Data Injection Attacks with Sparsity Constraints. , 2020, , .		2
1071	Energy Based Optimal Dynamic Stealth False Data Injection Attacks on the Smart Grid. , 2020, , .		0
1072	Statistical Techniques-based Characterization of FDIA in Smart Grids Considering Grid Contingencies. , 2020, , .		0
1073	Quantized Reservoir Computing on Edge Devices for Communication Applications. , 2020, , .		2
1074	Power Systems Intrusion Detection Using Novel Wrapped Feature Selection Framework. , 2020, , .		1
1075	The Impact of Cybersecurity on Siting Distributed Generation Units in AC Power Systems. , 2020, , .		0
1076	Detection of False Data Injection Attacks on Smart Grids: A Resilience-Enhanced Scheme. IEEE Transactions on Power Systems, 2022, 37, 2679-2692.	4.6	14
1077	An Enhanced Energy Management System Including a Real-Time Load-Redistribution Threat Analysis Tool and Cyber-Physical SCED. IEEE Transactions on Power Systems, 2022, 37, 3346-3358.	4.6	8
1078	False Data Injection Attack Against Power System Small-Signal Stability. , 2021, , .		5
1079	Topology Learning Aided False Data Injection Attack without Prior Topology Information. , 2021, , .		5
1080	Real-time Mitigation of Effects of False Data in Smart Grid: A Data Diode Approach. , 2021, , .		0
1081	A Novel Real-Time False Data Detection Strategy for Smart Grid. , 2021, , .		2
1082	Attack Detection and Localization in Smart Grid with Image-based Deep Learning. , 2021, , .		9
1083	CHIMERA: A Hybrid Estimation Approach to Limit the Effects of False Data Injection Attacks. , 2021, , .		2
1084	A Resilient Scheme for Mitigating False Data Injection Attacks in Distributed DC Microgrids. , 2021, , .		1
1085	Vulnerabilities of Power System Operations to Load Forecasting Data Injection Attacks. , 2021, , .		1
1086	An XGBoost-Based Vulnerability Analysis of Smart Grid Cascading Failures under Topology Attacks. , 2021, , .		1

#	Article	IF	Citations
1087	Exploring Targeted and Stealthy False Data Injection Attacks via Adversarial Machine Learning. IEEE Internet of Things Journal, 2022, 9, 14116-14125.	5.5	9
1088	Stealthy Attack Detection Method Based on Multi-Feature Long Short-Term Memory Prediction Model. SSRN Electronic Journal, 0, , .	0.4	0
1089	Data-Driven False Data Injection Attack: A Low-Rank Approach. IEEE Transactions on Smart Grid, 2022, 13, 2479-2482.	6.2	14
1090	Relentless False Data Injection Attacks Against Kalman-Filter-Based Detection in Smart Grid. IEEE Transactions on Control of Network Systems, 2022, 9, 1238-1250.	2.4	12
1091	Cyber-Attacks in Modular Multilevel Converters. IEEE Transactions on Power Electronics, 2022, 37, 8488-8501.	5.4	21
1092	Blind false data injection attacks in smart grids subject to measurement outliers. Journal of Control and Decision, 2022, 9, 445-454.	0.7	3
1093	Distributed Energy Management for Port Power System under False Data Injection Attacks. Complexity, 2022, 2022, 1-15.	0.9	3
1094	Real-Time Monitoring for Detection of Adversarial Subtle Process Variations. Nuclear Science and Engineering, 2022, 196, 544-567.	0.5	4
1095	The usage of power system multi-model forecasting aided state estimation for cyber attack detection. Power Engineering Research Equipment Technology, 2022, 23, 13-23.	0.1	0
1096	State-of-the-art survey of artificial intelligent techniques for IoT security. Computer Networks, 2022, 206, 108771.	3.2	37
1097	Monte-Carlo-based data injection attack on electricity markets with network parametric and topology uncertainties. International Journal of Electrical Power and Energy Systems, 2022, 138, 107915.	3.3	4
1098	Data-Driven Detection of Stealthy False Data Injection Attack Against Power System State Estimation. IEEE Transactions on Industrial Informatics, 2022, 18, 8467-8476.	7.2	16
1099	CAE: Contextual auto-encoder for multivariate time-series anomaly detection in air transportation. Computers and Security, 2022, 116, 102652.	4.0	11
1100	IGDT-based dynamic programming of smart distribution network expansion planning against cyber-attack. International Journal of Electrical Power and Energy Systems, 2022, 139, 108006.	3.3	4
1101	Identification of strategic sensor locations for intrusion detection and classification in smart grid networks. International Journal of Electrical Power and Energy Systems, 2022, 139, 107970.	3.3	1
1102	Integrating model-driven and data-driven methods for fast state estimation. International Journal of Electrical Power and Energy Systems, 2022, 139, 107982.	3.3	9
1103	Unmanned Ground Vehicle Platooning Under Cyber Attacks: A Human-Robot Interaction Framework. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 18113-18128.	4.7	5
1105	Cybersecurity Enhancement for Multi-Infeed High-Voltage DC Systems. IEEE Transactions on Smart Grid, 2022, 13, 3227-3240.	6.2	8

#	Article	IF	Citations
1106	LQG Reference Tracking With Safety and Reachability Guarantees Under Unknown False Data Injection Attacks. IEEE Transactions on Automatic Control, 2023, 68, 1245-1252.	3.6	0
1108	Resilience of Smart Integrated Energy Systems. , 2022, , 1-27.		1
1109	Cyber-Physical Attack Conduction and Detection in Decentralized Power Systems. IEEE Access, 2022, 10, 29277-29286.	2.6	7
1110	Blind False Data Injection Attacks Against State Estimation Based on Matrix Reconstruction. IEEE Transactions on Smart Grid, 2022, 13, 3174-3187.	6.2	8
1111	Explicit Analysis on Effectiveness and Hiddenness of Moving Target Defense in AC Power Systems. IEEE Transactions on Power Systems, 2022, 37, 4732-4746.	4.6	14
1113	A Novel Bilevel False Data Injection Attack Model Based on Pre- and Post- Dispatch. IEEE Transactions on Smart Grid, 2022, 13, 2487-2490.	6.2	3
1114	Secure Control Design for Networked Control Systems With Nonlinear Dynamics Under Time-Delay-Switch Attacks. IEEE Transactions on Automatic Control, 2023, 68, 798-811.	3.6	8
1115	Relaxed Connected Dominating Set Problem for Power System Cyberâ€“Physical Security. IEEE Transactions on Control of Network Systems, 2022, 9, 1780-1792.	2.4	1
1116	Secure Estimation With Privacy Protection. IEEE Transactions on Cybernetics, 2023, 53, 4947-4961.	6.2	5
1117	Low Latency Cyberattack Detection in Smart Grids with Deep Reinforcement Learning. SSRN Electronic Journal, 0, , .	0.4	1
1118	Bayesian robust hankel matrix completion with uncertainty modeling for synchrophasor data recovery. , 2022, 2, 1-19.		1
1119	Secure predictor-based neural dynamic surface control of nonlinear cyberâ€“physical systems against sensor and actuator attacks. ISA Transactions, 2022, 127, 120-132.	3.1	3
1120	Vulnerability assessment and defence strategy to site distributed generation in smart grid. IET Smart Grid, 2022, 5, 161-176.	1.5	2
1121	Earth-Mover-Distance-Based Detection of False Data Injection Attacks in Smart Grids. Energies, 2022, 15, 1733.	1.6	3
1122	Reachability-Based False Data Injection Attacks and Defence Mechanisms for Cyberpower System. Energies, 2022, 15, 1754.	1.6	5
1123	Digital Twinâ€"Cyber Replica of Physical Things: Architecture, Applications and Future Research Directions. Future Internet, 2022, 14, 64.	2.4	46
1124	A rule-based model for electricity theft prevention in advanced metering infrastructure. Journal of Electrical Systems and Information Technology, 2022, 9, .	1.2	3
1125	Toward Optimal False Data Injection Attack against Selfâ€Triggered Model Predictive Controllers. Advanced Theory and Simulations, 0, , 2200025.	1.3	1

#	Article	IF	Citations
1126	Realâ€time pricing response attack in smart grid. IET Generation, Transmission and Distribution, 2022, 16, 2441-2454.	1.4	1
1127	Periodic zeroâ€dynamics attacks for discreteâ€time secondâ€order multiâ€agent systems. International Journal of Robust and Nonlinear Control, 2022, 32, 5619-5636.	2.1	4
1128	Denoising Algorithm for Subtle Anomaly Detection. Nuclear Technology, 2022, 208, 1365-1381.	0.7	3
1129	Detection of false data injection attacks leading to line congestions using Neural networks. Sustainable Cities and Society, 2022, 82, 103861.	5.1	8
1130	Geometrical Characterization of Sensor Placement for Cone-Invariant and Multi-Agent Systems against Undetectable Zero-Dynamics Attacks. SIAM Journal on Control and Optimization, 2022, 60, 890-916.	1.1	1
1131	A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. Renewable Energy, 2022, 189, 1383-1406.	4.3	27
1132	An effective intrusion-resilient mechanism for programmable logic controllers against data tampering attacks. Computers in Industry, 2022, 138, 103613.	5.7	6
1133	A clustering-based framework for searching vulnerabilities in the operation dynamics of Cyber-Physical Energy Systems. Reliability Engineering and System Safety, 2022, 222, 108400.	5.1	5
1134	An overview of structural systems theory. Automatica, 2022, 140, 110229.	3.0	15
1135	Detection of false data injection attack in power information physical system based on SVMâ€"GAB algorithm. Energy Reports, 2022, 8, 1156-1164.	2.5	13
1136	A novel strategy for locational detection of false data injection attack. Sustainable Energy, Grids and Networks, 2022, 31, 100702.	2.3	7
1137	A Detection-Estimation Strategy for Delayed Systems under Spoofing Attack. , 2021, , .		0
1138	State Estimation for Cyber-Seaport Microgrid under False Data Injection Attacks. , 2021, , .		0
1139	Dynamic Phasor Estimation Method Considering False Data Injection Attack. , 2021, , .		0
1140	Privacy, Security, and Utility Analysis of Differentially Private CPES Data. , 2021, , .		9
1141	Square-root Extended Kalman Filter-based Detection of False Data Injection Attack in Smart Grids. , 2021, , .		1
1142	Cyber-physical security analysis of smart inverters under the pricing attacks. , 2021, , .		2
1143	Blockchain Checksum for Establishing Secure Communications for Digital Twin Technology. , 2021, , .		0

#	Article	IF	Citations
1144	Research on key node identification scheme for power system considering malicious data attacks. Energy Reports, 2021, 7, 1289-1296.	2.5	3
1145	A global approach to fault detection in multi-agent systems with switching topologies subject to cyber-attacks. , 2021, , .		0
1146	Detection of Cyber Attacks on Railway Autotransformer Traction Power Systems. , 2021, , .		1
1147	Impact of Brute Force Based False Data Injection Attack on Distribution System State Estimation. , 2021, , .		2
1148	A Novel Deep Learning Framework to Identify False Data Injection Attack in Power Sector. , 2021, , .		0
1149	Stealthy False Data Injection Attacks against Extended Kalman Filter Detection in Power Grids. , 2021, , .		2
1150	Deep Learning Based Real-Time Detection of False Data Injection Attacks in Power Grids. , 2021, , .		2
1151	A Reinforcement Learning-Based Detection Method for False Data Injection Attack in Distributed Smart Grid. , 2021, , .		0
1152	Detection and Prevention of False Data Injection Attack in Cyber Physical Power System. , 2021, , .		0
1153	An Online Approach to Covert Attack Detection and Identification in Power Systems. IEEE Transactions on Power Systems, 2023, 38, 267-277.	4.6	4
1154	A Generalized Hold Based Countermeasure Against Zero-Dynamics Attack With Application to DC-DC Converter. IEEE Access, 2022, 10, 44923-44933.	2.6	1
1155	Reachability Analysis Plus Satisfiability Modulo Theories: An Adversary-Proof Control Method for Connected and Autonomous Vehicles. IEEE Transactions on Industrial Electronics, 2023, 70, 2982-2992.	5.2	3
1156	Attack and defence methods in cyberâ€physical power system. IET Energy Systems Integration, 2022, 4, 159-170.	1.1	13
1157	Event-based fuzzy resilient control of nonlinear DC Microgrids under denial-of-service attacks. ISA Transactions, 2022, 127, 206-215.	3.1	8
1158	False Data Injection Detection for Phasor Measurement Units. Sensors, 2022, 22, 3146.	2.1	7
1159	Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and) Tj ETQq1 1 0.784314 rgBT /Overlock 10 T	2.6	16
1160	Attack-Resilient Optimal PMU Placement via Reinforcement Learning Guided Tree Search in Smart Grids. IEEE Transactions on Information Forensics and Security, 2022, 17, 1919-1929.	4.5	18
1161	Feature Construction to Detect and Locate FDIAs Using PNN and SVM models. , 2022, , .		0

#	Article	IF	Citations
1163	Physics-Constrained Robustness Evaluation of Intelligent Security Assessment for Power Systems. IEEE Transactions on Power Systems, 2023, 38, 872-884.	4.6	5
1164	Reliable control strategy based on sliding mode observer against FDI attacks in smart grid. Asian Journal of Control, 2023, 25, 910-920.	1.9	5
1165	An Accurate False Data Injection Attack (FDIA) Detection in Renewable-Rich Power Grids. , 2022, , .		6
1166	Improved Wasserstein Generative Adversarial Networks Defense Method against Data Integrity Attack on Smart Grid. Recent Advances in Electrical and Electronic Engineering, 2022, 15, .	0.2	0
1167	Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts. Renewable and Sustainable Energy Reviews, 2022, 163, 112423.	8.2	58
1168	Vulnerability analysis of cyber physical systems under the false alarm cyber attacks. Physica A: Statistical Mechanics and Its Applications, 2022, 599, 127416.	1.2	3
1169	Low latency cyberattack detection in smart grids with deep reinforcement learning. International Journal of Electrical Power and Energy Systems, 2022, 142, 108265.	3.3	5
1170	Voltage Stability Constrained Moving Target Defense Against Net Load Redistribution Attacks. IEEE Transactions on Smart Grid, 2022, 13, 3748-3759.	6.2	8
1171	An ${H_infty }$ Load Frequency Control Scheme for Multi-Area Power System Under Cyber-Attacks and Time-Varying Delays. IEEE Transactions on Power Systems, 2023, 38, 1336-1349.	4.6	8
1172	Link State Estimation Under Cyber-Physical Attacks: Theory and Algorithms. IEEE Transactions on Smart Grid, 2022, 13, 3760-3773.	6.2	2
1173	Data-Driven Cyber-Attack Detection of Intelligent Attacks in Islanded DC Microgrids. IEEE Transactions on Industrial Electronics, 2023, 70, 4293-4299.	5.2	15
1174	Dense Overload Subgraph Induced by Cyberâ€"Physical Attacks in Smart Grid. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70, 611-615.	2.2	1
1175	Economic Loss Utilized Probabilistic Defense against Load Redistribution AttacksÂby Selecting Optimal Critical Measuring Units. Technology and Economics of Smart Grids and Sustainable Energy, 2022, 7, .	1.8	0
1176	Detection and Prevention of False Data Injection Attacks in the Measurement Infrastructure of Smart Grids. Sustainability, 2022, 14, 6407.	1.6	7
1177	Mitigating Cyber Vulnerabilities in Distribution-Level Electricity Markets. SSRN Electronic Journal, 0, , .	0.4	0
1178	Towards Quantum Artificial Intelligence Electromagnetic Prediction Models for Ladder Logic Bombs and Faults in Programmable Logic Controllers. , 2022, , .		2
1179	Sequential Detection of Microgrid Bad Data via a Data-Driven Approach Combining Online Machine Learning With Statistical Analysis. Frontiers in Energy Research, 0, 10, .	1.2	3
1180	Detecting Cyberattacks on Electrical Storage Systems through Neural Network Based Anomaly Detection Algorithm. Sensors, 2022, 22, 3933.	2.1	8

#	Article	IF	Citations
1181	Research on Cyber-attacks and Defensive Measures of Power Communication Network. IEEE Internet of Things Journal, 2022, , 1-1.	5.5	0
1182	Multi-Objective False Data Injection Attacks of Cyberâ€"Physical Power Systems. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69, 3924-3928.	2.2	12
1183	PMU Angle Deviation Detection and Correction Using Line Reactive Power Measurements. IEEE Transactions on Power Systems, 2023, 38, 2679-2689.	4.6	1
1184	Learning-Based Vulnerability Analysis of Cyber-Physical Systems. , 2022, , .		8
1185	A Review of Cognitive Dynamic Systems and Its Overarching Functions. , 2022, , .		1
1186	Distributed Secondary Control Strategy Against Bounded FDI Attacks for Microgrid With Layered Communication Network. Frontiers in Energy Research, 0, 10, .	1.2	3
1187	Designing a robust cyberâ€attack detection and identification algorithm for DC microgrids based on Kalman filter with unknown input observer. IET Generation, Transmission and Distribution, 2022, 16, 3230-3244.	1.4	3
1188	Data-driven modeling of the temporal evolution of breakersâ€™ states in the French electrical transmission grid. Nonlinear Analysis: Hybrid Systems, 2022, 46, 101215.	2.1	1
1189	A Hybrid Deep Sensor Anomaly Detection for Autonomous Vehicles in 6G-V2X Environment. IEEE Transactions on Network Science and Engineering, 2023, 10, 1246-1255.	4.1	13
1190	Analysis ofÂMachine Learning andÂDeep Learning inÂCyber-Physical System Security. Lecture Notes in Networks and Systems, 2022, , 355-363.	0.5	1
1191	Smart distribution system state estimation. , 2022, , 45-55.		0
1192	Divergence-Based Transferability Analysis for Self-Adaptive Smart Grid Intrusion Detection With Transfer Learning. IEEE Access, 2022, 10, 68807-68818.	2.6	4
1193	Prediction of Power Measurements Using Adaptive Filters. , 2022, , .		0
1194	A Bagging MLP-based Autoencoder for Detection of False Data Injection Attack in Smart Grid. , 2022, , .		1
1195	Robust Autoencoder-based State Estimation in Power Systems. , 2022, , .		0
1196	Detection of Stealthy False Data Injection Attacks in Unobservable Distribution Networks. , 2022, , .		1
1197	Control over Blockchain for Data-Driven Fault Tolerant Control in Industry 4.0. , 2022, , .		2
1198	A Cyber Attack Taxonomy for Microgrid Systems. , 2022, , .		5

#	Article	IF	Citations
1199	Combating False Data Injection Attacks on Human-Centric Sensing Applications. , 2022, 6, 1-22.		1
1200	Datadriven false data injection attacks against cyber-physical power systems. Computers and Security, 2022, 121, 102836.	4.0	8
1201	Data recovery via covert cognizance for unattended operational resilience. Progress in Nuclear Energy, 2022, 151, 104317.	1.3	1
1202	Stochastic detection against deception attacks in CPS: Performance evaluation and game-theoretic analysis. Automatica, 2022, 144, 110461.	3.0	18
1203	Real-Time Locational Detection of Stealthy False Data Injection Attack in Smart Grid: Using Multivariate-Based Multi-Label Classification Approach. Energies, 2022, 15, 5312.	1.6	15
1204	Resilient iterative learning control for a class of discreteâ€time nonlinear systems under hybrid attacks. Asian Journal of Control, 0, , .	1.9	0
1205	Physics-Constrained Vulnerability Assessment of Deep Reinforcement Learning-Based SCOPF. IEEE Transactions on Power Systems, 2023, 38, 2690-2704.	4.6	8
1206	Detection of False Data Injection Attacks in Unobservable Power Systems by Laplacian Regularization. , 2022, , .		2
1208	Secure and Privacy-Preserving Consensus for Multi-Agent Networks under Deception Attacks. , 2022, , .		1
1209	Optimal linear attack for multi-sensor network against state estimation. Journal of the Franklin Institute, 2022, 359, 9220-9240.	1.9	1
1210	Modeling and Analysis of Explanation for Secure Industrial Control Systems. ACM Transactions on Autonomous and Adaptive Systems, 2022, 17, 1-26.	0.4	0
1211	Discrete-time resilient-distributed secondary control strategy against unbounded attacks in polymorphic microgrid. Frontiers in Energy Research, 0, 10, .	1.2	1
1212	Impact of cyberâ€attack on coordinated voltage control in low voltage grids. IET Renewable Power Generation, 0, , .	1.7	0
1213	Resilience enhancement of multi-agent reinforcement learning-based demand response against adversarial attacks. Applied Energy, 2022, 324, 119688.	5.1	11
1214	Stealthy attack detection method based on Multi-feature long short-term memory prediction model. Future Generation Computer Systems, 2022, 137, 248-259.	4.9	4
1215	Review of active defense methods against power CPS false data injection attacks from the multiple spatiotemporal perspective. Energy Reports, 2022, 8, 11235-11248.	2.5	6
1216	Structural-Constrained Methods for the Identification of False Data Injection Attacks in Power Systems. IEEE Access, 2022, 10, 94169-94185.	2.6	6
1217	Chance-Constrained OPF: A Distributed Method With Confidentiality Preservation. IEEE Transactions on Power Systems, 2022, , 1-13.	4.6	1

#	Article	IF	Citations
1218	False Data Injection Attacks on Smart Grid Voltage Regulation With Stochastic Communication Model. IEEE Transactions on Industrial Informatics, 2023, 19, 7122-7132.	7.2	4
1219	A Novel False Data Injection Attack Formulation Based on CUR Low-Rank Decomposition Method. IEEE Transactions on Smart Grid, 2022, 13, 4965-4968.	6.2	4
1220	Semi-supervised False Data Injection Attacks Detection in Smart Grid. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2022, , 189-200.	0.2	0
1221	Robust Moving Target Defence Against False Data Injection Attacks in Power Grids. IEEE Transactions on Information Forensics and Security, 2023, 18, 29-40.	4.5	6
1222	Resilient Observer Design for Cyber-Physical Systems with Data-Driven Measurement Pruning. , 2022, , 85-117.		2
1223	A Novel ZSV-Based Detection Scheme for FDIAs in Multiphase Power Distribution Systems. IEEE Transactions on Smart Grid, 2023, 14, 1236-1248.	6.2	1
1224	Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach. IEEE Transactions on Smart Grid, 2022, 13, 4862-4872.	6.2	90
1225	PowerFDNet: Deep Learning-Based Stealthy False Data Injection Attack Detection for AC-Model Transmission Systems. IEEE Open Journal of the Computer Society, 2022, 3, 149-161.	5.2	4
1226	Adversarial Models Towards Data Availability and Integrity of Distributed State Estimation for Industrial Iot-Based Smart Grid. SSRN Electronic Journal, 0, , .	0.4	0
1227	Small-Signal Angle Stability-Oriented False Data Injection Cyber-Attacks on Power Systems. IEEE Transactions on Smart Grid, 2023, 14, 635-648.	6.2	4
1228	Attack Power System State Estimation by Implicitly Learning the Underlying Models. IEEE Transactions on Smart Grid, 2023, 14, 649-662.	6.2	4
1229	Preventing False Data Injection Attacks in LFC System via the Attack-Detection Evolutionary Game Model and KF Algorithm. IEEE Transactions on Network Science and Engineering, 2022, 9, 4349-4362.	4.1	6
1230	Resilient State Estimation andÂAttack Mitigation inÂCyber-Physical Systems. , 2022, , 149-185.		1
1231	Modeling Cascading Failures in Coupled Smart Grid Networks. IEEE Access, 2022, 10, 81054-81070.	2.6	5
1232	Submodularity-based False Data Injection Attack Scheme in Multi-agent Dynamical Systems. , 2022, , .		4
1233	Detection of cyber attacks on smart grids. Advances in Computational Intelligence, 2022, 2, .	0.7	0
1234	Detection Scheme for Tampering Behavior on Distributed Controller of Electric-Thermal Integrated Energy System Based on Relation Network. Computational Intelligence and Neuroscience, 2022, 2022, 1-16.	1.1	0
1235	Vector Auto-Regression-Based False Data Injection Attack Detection Method in Edge Computing Environment. Sensors, 2022, 22, 6789.	2.1	5

#	Article	IF	Citations
1236	Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. Energies, 2022, 15, 6799.	1.6	24
1237	Attack estimationâ€"based resilient control for cyber-physical power systems. Transactions of the Institute of Measurement and Control, 0, , 014233122211224.	1.1	0
1238	Drivers for increasing attractiveness of commercial centers. International Journal of Construction Management, 0, , 1-12.	2.2	0
1239	Guaranteed performance impulsive tracking control of multi-agents systems under discrete-time deception attacks. Communications in Nonlinear Science and Numerical Simulation, 2023, 117, 106905.	1.7	7
1240	Observability Decomposition-Based Decentralized Kalman Filter and Its Application to Resilient State Estimation under Sensor Attacks. Sensors, 2022, 22, 6909.	2.1	1
1241	Real-Time Detection of Cyber-Attacks in Modern Power Grids with Uncertainty using Deep Learning. , 2022, , .		3
1242	Comparison of encrypted control approaches and tutorial on dynamic systems using Learning With Errors-based homomorphic encryption. Annual Reviews in Control, 2022, 54, 200-218.	4.4	9
1243	A Cross-Layer Defense Method for Blockchain Empowered CBTC Systems Against Data Tampering Attacks. IEEE Transactions on Intelligent Transportation Systems, 2023, 24, 501-515.	4.7	14
1244	Distributed Tracking Control of Nonlinear Multi-agent Systems Against False Data Injection Attacks. , 2022, , .		0
1245	Active Defense Research against False Data Injection Attacks of Power CPS Based on Data-Driven Algorithms. Energies, 2022, 15, 7432.	1.6	3
1246	State vulnerability assessment against false data injection attacks in AC state estimators. Energy Conversion and Economics, 2022, 3, 319-332.	1.9	3
1247	Adaptive Resilient Control of AC Microgrids under Unbounded Actuator Attacks. Energies, 2022, 15, 7458.	1.6	2
1248	Deep learning-based identification of false data injection attacks on modern smart grids. Energy Reports, 2022, 8, 919-930.	2.5	10
1249	Cyberâ€"physical risk assessment for false data injection attacks considering moving target defences. International Journal of Information Security, 2023, 22, 579-589.	2.3	5
1250	Observable Placement of Phasor Measurement Units for Defense against Data Integrity Attacks in Real Time Power Markets. Reliability Engineering and System Safety, 2022, , 108957.	5.1	2
1251	A Review on Distribution System State Estimation Algorithms. Applied Sciences (Switzerland), 2022, 12, 11073.	1.3	10
1252	Graph-based detection for false data injection attacks in power grid. Energy, 2023, 263, 125865.	4.5	10
1253	The Optimal Distributed Weighted Least-Squares Estimation in Finite Steps for Networked Systems. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70, 1069-1073.	2.2	0

#	Article	IF	Citations
1254	Completely Stealthy FDI Attack Against State Estimation in Networked Control Systems. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70, 1114-1118.	2.2	2
1255	Cyber Brittleness of Smart Cities. , 2022, , 19-40.		3
1256	Prevention and Detection of Coordinated False Data Injection Attacks on Integrated Power and Gas Systems. IEEE Transactions on Power Systems, 2023, 38, 4252-4268.	4.6	6
1257	Detection and Identification of Sparse Sensor Attacks in Cyber-Physical Systems With Side Information. IEEE Transactions on Automatic Control, 2023, 68, 5349-5364.	3.6	5
1258	Effective Factors and Policies in Electrical Energy Security. , 2022, , 1-31.		1
1259	Differential Evolution-Based Three Stage Dynamic Cyber-Attack of Cyber-Physical Power Systems. IEEE/ASME Transactions on Mechatronics, 2023, 28, 1137-1148.	3.7	38
1260	Extended Moving Target Defense for AC State Estimation in Smart Grids. IEEE Transactions on Smart Grid, 2023, 14, 2313-2325.	6.2	5
1261	False Data Injection Attack on Atmospheric Electric Field in Thunderstorm Warning. , 2022, , .		1
1262	Stealth Attacks on the SADI with Prior Information on the State Covariance Matrix. , 2022, , .		1
1263	False data injection attacks detection based on Laguerre function in nonlinear Cyberâ€Physical systems. Internet Technology Letters, 2023, 6, .	1.4	2
1264	Event-triggered <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" display="inline" id="d1e87" altimg="si2.svg"><mml:msub><mml:mrow><mml:mi>H</mml:mi></mml:mrow><mml:mrow><mml:mi>âˆž</mml:mi></mml:mrow></m consensus for nonlinear multi-agent systems with semi-Markov switching topologies under DoS attacks. , 2023, 2, 100006.		3
1265	Security Enhancement of Network Constraint Grid-Edge Energy Management System. , 2022, , .		0
1266	Analytical Risk Assessment of Communication Cyber Attacks on Automatic Generation Control. , 2022, , .		0
1267	Impact Analysis of Sensor Cyber-Attacks on Grid-Tied Variable Speed Hydropower Plants. , 2022, , .		2
1268	Resilient Defense of False Data Injection Attacks in Smart Grids via Virtual Hidden Networks. IEEE Internet of Things Journal, 2023, 10, 6474-6490.	5.5	1
1269	Optimal deception attacks on remote state estimators equipped with interval anomaly detectors. Automatica, 2023, 148, 110723.	3.0	2
1270	A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research, 2023, 215, 108975.	2.1	153
1271	Data Mining Applications in Smart Grid System (SGS). , 2022, , 1-17.		0

#	Article	IF	Citations
1272	Fine-Tuned RNN-Based Detector for Electricity Theft Attacks in Smart Grid Generation Domain. IEEE Open Journal of the Industrial Electronics Society, 2022, 3, 733-750.	4.8	5
1273	Optimal Deception Attacks Against Remote State Estimation: An Information-Based Approach. IEEE Transactions on Automatic Control, 2022, , 1-16.	3.6	1
1274	Robust Monitor for Industrial IoT Condition Prediction. IEEE Internet of Things Journal, 2022, , 1-1.	5.5	0
1275	Reinforcement Learning-Based Adaptive Feature Boosting for Smart Grid Intrusion Detection. IEEE Transactions on Smart Grid, 2023, 14, 3150-3163.	6.2	2
1276	Active Interdiction Defence Scheme Against False Data-Injection Attacks: A Stackelberg Game Perspective. IEEE Transactions on Cybernetics, 2024, 54, 162-172.	6.2	2
1277	Analysis of Targeted Coordinated Attacks on Decomposition-Based Robust State Estimation. IEEE Open Access Journal of Power and Energy, 2023, 10, 116-127.	2.5	0
1278	An Ensemble Learning-Based Cyber-Attacks Detection Method of Cyber-Physical Power Systems. , 2022, , .		1
1279	Detection of cyber attack in smart grid: A Comparative Study. , 2022, , .		3
1280	Physical Verification of Data-Driven Cyberattack Detector in Power System: An MTD Approach. , 2022, , .		1
1281	Attacks Detection and Security Control Against False Data Injection Attacks Based on Interval Type-2 Fuzzy System. , 2022, , .		0
1282	Load Redistribution Attacks in Multi-Terminal DC Grids. , 2022, , .		1
1283	False Data Injection Attacks on Sensor Systems. , 2022, , .		0
1284	Detecting Cyber Attacks in Smart Grids with Massive Unlabeled Sensing Data. , 2022, , .		1
1285	Localization of Coordinated Cyber-Physical Attacks in Power Grids Using Moving Target Defense and Deep Learning. , 2022, , .		3
1286	Vulnerability of Distributed Inverter VAR Control in PV Distributed Energy System. , 2022, , .		1
1287	Smart retrofitting of buildings: a bibliometric study. IOP Conference Series: Earth and Environmental Science, 2022, 1101, 022013.	0.2	0
1288	Defending Smart Electrical Power Grids against Cyberattacks with Deep <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" display="inline" overflow="scroll"><mml:mi>Q</mml:mi></mml:math> -Learning. , 2022, 1, .		11
1290	Defense Strategy against False Data Injection Attacks in Ship DC Microgrids. Journal of Marine Science and Engineering, 2022, 10, 1930.	1.2	3

#	Article	IF	Citations
1291	DRAGON: Deep Reinforcement Learning for Autonomous Grid Operation and Attack Detection. , 2022, , .		2
1292	Fail-Safe: Securing Cyber-Physical Systems against Hidden Sensor Attacks. , 2022, , .		4
1293	Resilienceâ€based output containment control of heterogeneous MAS against unbounded attacks. IET Control Theory and Applications, 2023, 17, 757-768.	1.2	0
1294	BayesImposter: Bayesian Estimation Based.bss Imposter Attack on Industrial Control Systems. , 2022, , .		1
1295	Distributed Control Microgrids: Cyber-Attack Models, Impacts and Remedial Strategies. IEEE Transactions on Signal and Information Processing Over Networks, 2022, 8, 1008-1023.	1.6	6
1296	Generalized Graph Neural Network-Based Detection of False Data Injection Attacks in Smart Grids. IEEE Transactions on Emerging Topics in Computational Intelligence, 2023, 7, 618-630.	3.4	6
1297	Detection of false data injection attacks in cyberâ€"physical systems using graph convolutional network. Electric Power Systems Research, 2023, 217, 109118.	2.1	11
1298	Assessing cyber attacks on local electricity markets using simulation analysis: Impacts and possible mitigations. Sustainable Energy, Grids and Networks, 2023, 34, 100993.	2.3	3
1299	Critical Load Identification for Load Redistribution Attacks. , 2022, , .		0
1300	Moving Target Defense Oriented D-FACTS Deployment and Operation. , 2022, , .		0
1301	Distributed Optimal and Self-Tuning Filters Based on Compressed Data for Networked Stochastic Uncertain Systems with Deception Attacks. Sensors, 2023, 23, 335.	2.1	6
1302	Barrier Certificate based Safe Control for LiDAR-based Systems under Sensor Faults and Attacks. , 2022, , .		1
1303	Optimal Myopic Attacks on Nonlinear Estimation. , 2022, , .		2
1304	A Model-free False Data Injection Attack Strategy in Networked Control Systems. , 2022, , .		2
1305	Resilient Synchronization of Heterogeneous MAS Against Correlated Sensor Attacks. , 2022, , .		0
1306	A Secure Time-Based Bad Data Detection Algorithm for State Estimation. , 2022, , .		0
1307	Abstraction-Free Control Synthesis to Satisfy Temporal Logic Constraints under Sensor Faults and Attacks. , 2022, , .		0
1308	Hybrid Physics-Based and Data-Driven Mitigation Strategy for Automatic Generation Control Under Cyber Attack. Power Systems, 2023, , 135-160.	0.3	0

#	Article	IF	Citations
1309	False data injection attack in smart grid: Attack model and reinforcement learning-based detection method. Frontiers in Energy Research, 0, 10, .	1.2	2
1310	A Comprehensive Review on Cyber-Attack Detection and Control of Microgrid Systems. Power Systems, 2023, , 1-45.	0.3	2
1311	A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things. Computational Intelligence and Neuroscience, 2023, 2023, 1-24.	1.1	18
1312	Thinking in Systems, Sifting Through Simulations: A Way Ahead for Cyber Resilience Assessment. IEEE Access, 2023, 11, 11430-11450.	2.6	4
1313	Stealth Data Injection Attacks with Sparsity Constraints. IEEE Transactions on Smart Grid, 2023, , 1-1.	6.2	0
1314	Super-Resolution Perception Assisted Spatiotemporal Graph Deep Learning Against False Data Injection Attacks in Smart Grid. IEEE Transactions on Smart Grid, 2023, 14, 4035-4046.	6.2	6
1316	Cyber-Attacks on Smart Grid System: A Review. , 2022, , .		4
1317	CNN-GRU based fake data injection attack detection method for power grid. , 2022, , .		1
1318	Feature Selection based False Data Detection Scheme using Machine Learning for Power System. , 2022, , .		0
1319	Localizing False Data Injection Attacks in Smart Grid: A Spectrum-Based Neural Network Approach. IEEE Transactions on Smart Grid, 2023, 14, 4827-4838.	6.2	2
1320	Research communities in cyber security vulnerability assessments: A comprehensive literature review. Computer Science Review, 2023, 48, 100551.	10.2	3
1321	Detection of data-driven blind cyber-attacks on smart grid: A deep learning approach. Sustainable Cities and Society, 2023, 92, 104475.	5.1	3
1322	Resilient distributed estimation against FDI attacks: A correntropy-based approach. Information Sciences, 2023, 635, 236-256.	4.0	2
1324	Letter Detecting the One-Shot Dummy Attack on the Power Industrial Control Processes With an Unsupervised Data-Driven Approach. IEEE/CAA Journal of Automatica Sinica, 2023, 10, 550-553.	8.5	1
1325	Multi-Agent Distributed Deep Learning Algorithm to Detect Cyber-Attacks in Distance Relays. IEEE Access, 2023, 11, 10842-10849.	2.6	2
1326	Generalized Likelyhood Ratio based Detection on Cyber-Attacks. , 2022, , .		0
1327	A novel cyberâ€attack modelling and detection in overcurrent protection relays based on wavelet signature analysis. IET Generation, Transmission and Distribution, 2023, 17, 1585-1600.	1.4	4
1328	Random Bad State Estimator to Address False Data Injection in Critical Infrastructures. , 2022, , .		0

#	Article	IF	Citations
1329	XTM: A Novel Transformer and LSTM-Based Model for Detection and Localization of Formally Verified FDI Attack in Smart Grid. Electronics (Switzerland), 2023, 12, 797.	1.8	6
1330	Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. Energies, 2023, 16, 1651.	1.6	10
1331	Detection and reconstruction of measurements against false data injection and DoS attacks in distribution system state estimation: A deep learning approach. Measurement: Journal of the International Measurement Confederation, 2023, 210, 112565.	2.5	4
1332	False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction. Computers and Electrical Engineering, 2023, 107, 108638.	3.0	25
1333	Distributed Resilient Secondary Control for AC Microgrid Under FDI Attacks. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70, 2570-2574.	2.2	1
1334	MMTD: Multistage Moving Target Defense for Security-Enhanced D-FACTS Operation. IEEE Internet of Things Journal, 2023, 10, 12234-12247.	5.5	1
1335	Distribution System State Estimation and False Data Injection Attack Detection with a Multi-Output Deep Neural Network. Energies, 2023, 16, 2288.	1.6	8
1336	Model-Measurement Data Integrity Attacks. IEEE Transactions on Smart Grid, 2023, 14, 4741-4757.	6.2	0
1337	Resilient Consensus Control for Multi-Agent Systems: A Comparative Survey. Sensors, 2023, 23, 2904.	2.1	3
1338	False data injection attack detection in power system with non-convex principal component analysis. , 2022, , .		0
1339	Attack Detection based on Alternating Direction Multiplier Method for Distributed State Estimation in Smart Grid. , 2022, , .		0
1340	A Deep Learning-Based Attack Detection Mechanism Against Potential Cascading Failure Induced by Load Redistribution Attacks. IEEE Transactions on Smart Grid, 2023, 14, 4772-4783.	6.2	10
1341	Learning new attack vectors from misuse cases with deep reinforcement learning. Frontiers in Energy Research, 0, 11, .	1.2	1
1342	An error neighborhood-based detection mechanism to improve the performance of anomaly detection in industrial control systems. , 2022, , .		0
1343	On Information Fusion in Optimal Linear FDI Attacks Against Remote State Estimation. IEEE Transactions on Control of Network Systems, 2023, 10, 2085-2096.	2.4	1
1344	Adaptive unknown input observer-based detection and identification method for intelligent transportation under malicious attack. Measurement and Control, 0, , 002029402311591.	0.9	0
1345	A Temporal Graph Neural Network for Cyber Attack Detection and Localization in Smart Grids. , 2023, , .		8
1346	Deep Adversary based Stealthy False Data Injection Attacks against AC state estimation. , 2022, , .		1

#	Article	IF	Citations
1347	Anomaly Detection Method For Interactive Data of Third-Party Load Aggregation Platform Based on Multidimensional Feature Information Fusion. , 2022, , .		0
1348	Real-time detection of deception attacks in cyber-physical systems. International Journal of Information Security, 2023, 22, 1099-1114.	2.3	1
1349	Wavelet analysis and consensus algorithm-based fault-tolerant control for smart grids. Frontiers in Energy Research, 0, 11, .	1.2	0
1350	Locational Detection of False Data Injection Attack in Smart Grid Based on Multilabel Machine Learning Classification Methods. , 2023, , .		1
1351	A Resilient Controller for Frequency Regulation of Power Grids against Cyber Attacks. , 2023, , .		0
1352	Detection of false data injection attacks on power systems using graph edge-conditioned convolutional networks. Protection and Control of Modern Power Systems, 2023, 8, .	4.3	8
1353	Optimal Power Flow. , 2023, , 1-10.		0
1354	Static Detection of False Data in the Power Grid by Fusing Structure and Attributes of Node. Journal of Electrical Engineering and Technology, 0, , .	1.2	1
1355	Cybersecurity Analysis of Data-Driven Power System Stability Assessment. IEEE Internet of Things Journal, 2023, 10, 15723-15735.	5.5	1
1356	Modified Matrix Completion-Based Detection of Stealthy Data Manipulation Attacks in Low Observable Distribution Systems. IEEE Transactions on Smart Grid, 2023, 14, 4851-4862.	6.2	0
1357	A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids. ACM Computing Surveys, 2023, 55, 1-37.	16.1	4
1358	Study of Cyber Attackâ€™s Impact on LCC-HVDC System With False Data Injection. IEEE Transactions on Smart Grid, 2023, 14, 3220-3231.	6.2	3
1359	A Brief Survey of Recent Advances and Methodologies for the Security Control of Complex Cyberâ€"Physical Networks. Sensors, 2023, 23, 4013.	2.1	1
1360	Optimal Defense Strategy Against Load Redistribution Attacks under Attackerâ€™s Resource Uncertainty: A Trilevel Optimization Approach. , 2023, , .		1
1364	Effective Factors and Policies in Electrical Energy Security. , 2023, , 129-159.		0
1366	Synchrophasor Big Data Architectures, Platforms and Applications: A Review. , 2022, , .		0
1368	Data Integrity Attack Strategy against State Estimation Results of Distributed Power System. , 2023, , .		0
1369	Stealthy attacks formalized as STL formulas for Falsification of CPS Security. , 2023, , .		1

#	Article	IF	Citations
1376	Security and Privacy in the Internet of Medical Things (IoMT). Advances in Healthcare Information Systems and Administration Book Series, 2023, , 1-27.	0.2	1
1378	Adversarial Attacks on Machine Learning-Based State Estimation in Power Distribution Systems. , 2023, , .		0
1379	Load Altering Attacks- a Review of Impact and Mitigation Strategies. , 2023, , .		1
1381	Method for Detecting FDI Attacks on Intelligent Power Networks. Lecture Notes on Data Engineering and Communications Technologies, 2023, , 715-731.	0.5	0
1388	Comparative Analysis of Game-Based Defense Strategies against False Data Injection Attacks under Complete and Incomplete Information Conditions. , 2022, , .		0
1389	A Detection Based on OMES and MTAD-GAT for False Data Injection Attack in Smart Grid. , 2022, , .		0
1390	An Adaptive LQR-Based Defense Strategy against False Data Injection Attack in Smart Grids. , 2022, , .		0
1393	Secure Control Loop Execution of Cyber-Physical Devices Using Predictive State Space Checks. , 2023, , .		0
1394	Comparative Study of ML Algorithms for Load Redistribution Attack Detection. , 2022, , .		0
1395	Deep learning-based hybrid detection model for false data injection attacks in smart grid. , 2023, , .		0
1396	On the Economic Vulnerability Analysis of Power Grids to False Data Injection Attacks Against Wide Area Measurement Systems. , 2022, , .		0
1397	Detection of False Data Injection Attacks in Distribution System State Estimation. , 2022, , .		0
1400	Distributed Load Sharing Under Cyber Attacks. , 2023, , 181-200.		0
1401	Comparing Kalman Filters and Observers Against Cyber Attacks. , 2023, , 99-124.		0
1403	Robust Defense against Load Redistribution Attacks in Power Grids based on Reactance Control. , 2023, , .		0
1406	Detection Localization and Recovery of False Data Injection Attacks on Power Grids Based on SA-DCNN and AE-LSTM. , 2023, , .		0
1407	Effective Factors and Policies in Electrical Energy Security. , 2023, , 1-31.		0
1412	Mapping the Knowledge of Cybersecurity in the Manufacturing Industry. Applied Innovation and Technology Management, 2023, , 239-266.	0.3	0

#	Article	IF	Citations
1413	Differential Aggregation against General Colluding Attackers. , 2023, , .		1
1414	From Tactics to Techniques: A Systematic Attack Modeling for Advanced Persistent Threats in Industrial Control Systems. , 2023, , .		0
1415	Comprehensively Analyzing the Impact of Cyberattacks on Power Grids. , 2023, , .		5
1416	Detection and Localization of Stealth False Data Injection Attacks in Active Power Distribution Systems Using an Ensemble of Deep CNNs. , 2023, , .		0
1417	Resilience of Smart Integrated Energy Systems. , 2023, , 1887-1913.		0
1418	Data Mining Applications in Smart Grid System (SGS). , 2023, , 1557-1573.		0
1420	Detection of e-Mobility-Based Attacks on the Power Grid. , 2023, , .		2
1425	Data-driven FDI Attacks: A Stealthy Approach to Subvert SVM Detectors in Power System. , 2023, , .		0
1429	Implementation of IEEE C37.118 Packet Manipulation Tool, pySynphasor for Power System Security Evaluation. , 2023, , .		0
1436	ICSML: Industrial Control Systems ML Framework for native inference using IEC 61131-3 code. , 2023, , .		0
1437	Security Framework for Cloud Control Systems Against False Data Injection Attacks. , 2023, , .		0
1438	Shedding Light on Inconsistencies in Grid Cybersecurity: Disconnects and Recommendations. , 2023, , .		1
1447	Identification of Malicious Data Attacks in a Smart Grid Network Using Spectral Clustering. , 2023, , .		0
1449	Optimal False Data Injection Attack on EV Chargers and DGs in Active Distribution Networks. , 2023, , .		0
1450	Data-driven Vulnerability Analysis of Networked Pipeline System. , 2023, , .		0
1451	Interpretable Detection and Localization of False Data Injection Attacks Based on Causal Learning. , 2023, , .		0
1452	LF Radio Receiver For Substation Intrusion Deterrent and Measurement Validation. , 2023, , .		0
1455	Minimizing the Risk of Attacks in Electric Power Systems via Effective Grid Reinforcement of Counter Threat Technologies. , 2023, , .		0

#	Article	IF	Citations
1456	Input-to-State Stability ofÂCyber-Physical Systems Under Denial ofÂService Attacks. Lecture Notes in Electrical Engineering, 2023, , 91-103.	0.3	0
1457	Performance Analysis of Chi-square Detection for False Data Injection Attack. , 2023, , .		0
1458	Invited Paper: Detection ofÂFalse Data Injection Attacks inÂPower Systems Using aÂSecured-Sensors andÂGraph-Based Method. Lecture Notes in Computer Science, 2023, , 240-258.	1.0	0
1459	A Novel False Data Injection Method Targeting on Time-series analysis in Smart Grid. , 2023, , .		0
1460	FDI Attack-Resilient Distributed Cooperative Control forÂMicrogrids viaÂTwo-Hop Communication. Lecture Notes in Electrical Engineering, 2023, , 831-841.	0.3	0
1467	Machine Learning Assisted Bad Data Detection for High-Throughput Substation Communication. , 2023, , .		0
1477	A Defensive Mechanism Against Load Redistribution Attacks with Sequential Outage Potential Using Encrypted PMUs. , 2023, , .		1
1478	False Data Injection Attack Detection for Control Systems Based on Correlation Analysis. , 2023, , .		0
1480	Resilient Control of Smart Microgrids Based on Reliable Estimation. , 2023, , .		0
1485	Watermarking-based Discrete LQG Systems for Detecting Replay Attacks. , 2023, , .		0
1487	Detection of False Data Injection Attacks in Smart Grids Under Power Fluctuation Uncertainty Based on Deep Learning. , 2023, , .		1
1488	Industrial Network Protocol Security Enhancement Using Programmable Switches. , 2023, , .		0
1491	Protection of Power System State Estimation against False Data Injection Attacks. , 2023, , .		1
1492	A Smart Grid Ontology: Vulnerabilities, Attacks, and Security Policies. , 2023, , .		0
1493	Distributed Optimal Filter for Networked Stochastic Uncertain Systems with Correlated Noises and Fading Deception Attacks. , 2023, , .		0
1497	False Data Injection Attack Diminishing the Performance of Controllable Devices in Active Distribution Networks. , 2023, , .		0
1498	Bad-Data-Resilient Dynamic State Estimation for Power Systems with Partially Known Models. , 2023, , .		0
1500	Optimal Sequential False Data Injection Attack Scheme: Finite-Time Inverse Convergence. , 2023, , .		0

#	Article	IF	Citations
1501	Optimal Linear Attack in Cyber-Physical Systems with Periodic Detection. , 2023, , .		1
1502	Effects of Quantization on Zero-Dynamics Attacks to Closed-Loop Sampled-Data Control Systems. , 2023, , .		0
1506	Real-Time and Experimental Reactive and Proactive Defense in a Multi-Agent Scenario. , 2024, , .		0
1508	Dynamic State Estimation based Cyber Attack Detection scheme to Supervise Distance Relay Operation in Transmission line. , 2023, , .		0
1509	Detection of False Data Injection in Cyber Physical Power Systems using Extended Kalman Filter. , 2023, , .		0
1510	Catch You if Pay Attention: Temporal Sensor Attack Diagnosis Using Attention Mechanisms for Cyber-Physical Systems. , 2023, , .		1
1514	A detection method for false data injection attacks in power systems based on artificial fish swarm K-means clustering algorithm. , 2023, , .		0
1515	Unveiling a New Vulnerability in Modern Power Systems: Leveraging Publicly-Available LMPs for Crafting Cyber-Attacks. , 2023, , .		0
1516	Cyber Attack-Aware Security Hardening of Time Synchronization Technologies in WAMPAC Systems. , 2023, , .		0
1520	METRICS: A Methodology forÂEvaluating andÂTesting theÂResilience ofÂIndustrial Control Systems toÂCyberattacks. Lecture Notes in Computer Science, 2024, , 25-45.	1.0	0
1522	Risk and vulnerability assessment in power systems. , 2024, , 23-66.		0
1523	Strategic deployment of advanced measuring instruments to enhance robustness of state estimation in smart grid against cyberattacks. , 2024, , 169-185.		0
1526	An Overview of E-Mobility-Based Threats to the Power Grid. Advances in Mechatronics and Mechanical Engineering, 2024, , 142-155.	1.0	0
1530	Spatial-Temporal Graph Neural Network for Detecting and Localizing Anomalies in PMU Networks. Communications in Computer and Information Science, 2024, , 75-82.	0.4	0
1532	Modeling High Concealment LR Attack Based on Linearization of Signal Space Projection. Lecture Notes in Electrical Engineering, 2024, , 665-673.	0.3	0