Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids

DOI: 10.1109/tii.2017.2656905
IEEE Transactions on Industrial Informatics, 2017, 13, 2693-27

#	Paper	IF	Citations
170	Ensuring Data Integrity of OPF Module and Energy Database by Detecting Changes in Power Flow Patterns in Smart Grids. *IEEE Transactions on Industrial Informatics*, **2017**, 13, 3299-3311	11.9	23
169	Interval state estimation based defense mechanism against cyber attack on power systems. **2017**,		1
168	Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks. *IEEE Transactions on Industrial Informatics*, **2018**, 14, 4766-4778	11.9	106
167	. **2018**, 66, 3280-3295		6
166	Robust Bad Data Detection Method for Microgrid Using Improved ELM and DBSCAN Algorithm. **2018**, 144, 04018026		7
165	Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks. *IEEE Transactions on Industrial Informatics*, **2018**, 14, 3271-3280	11.9	109
164	False Data Injection Attacks on Contingency Analysis: Attack Strategies and Impact Assessment. **2018**, 6, 8841-8851		18
163	Optimal Prevention and Control Strategy Against Preconceive Faults in Electric Cyber-Physical System. **2018**,		1
162	Physical-Model-Checking to Detect Switching-Related Attacks in Power Systems. **2018**, 18,		3
161	Cyber Physical Energy Systems Modules for Power Sharing Controllers in Inverter Based Microgrids. **2018**, 3, 66		6
160	A data-driven covert attack strategy in the closed-loop cyber-physical systems. **2018**, 355, 6454-6468		7
159	Impact of Cyber Attacks on High Voltage DC Transmission Damping Control. **2018**, 11, 1046		9
158	False Data Injection Attack Based on Hyperplane Migration of Support Vector Machine in Transmission Network of the Smart Grid. **2018**, 10, 165		3
157	Event-triggered hybrid control strategy based on hybrid automata and decision tree for microgrid. **2019**, 13, 3066-3077		1
156	Detection Scheme Against Cyber-Physical Attacks on Load Frequency Control Based on Dynamic Characteristics Analysis. *IEEE Systems Journal*, **2019**, 13, 2859-2868	4.3	14
155	Unscented Kalman Filter based interval state estimation of cyber physical energy system for detection of dynamic attack. **2019**, 188, 116036		9
154	A Parallel Control Framework of Analog Proportional Integral and Digital Model Predictive Controllers for Enhancing Power Converters Cybersecurity. **2019**, 1-1		1

153	Online Identification and Data Recovery for PMU Data Manipulation Attack. *IEEE Transactions on Smart Grid*, **2019**, 10, 5889-5898	10.7	40
152	Design of data-injection attacks for cyber-physical systems based on Kullback□eibler divergence. **2019**, 361, 77-84		6
151	Resilience Analysis of DC Microgrids Under Denial of Service Threats. **2019**, 34, 3199-3208		34
150	An Optimal Defense Strategy Against Data Integrity Attacks In Smart Grids. **2019**,		
149	. **2019**,		2
148	An Ensembled ELMs Based Defense Mechanism Against Cyber Attack on Power Systems. **2019**,		0
147	Detection and Identification of Cyber and Physical Attacks on Distribution Power Grids with PVs: An Online High-Dimensional Data-driven Approach. **2019**, 1-1		16
146	Distributed Optimal Dynamic State Estimation for Cyber Intrusion Detection in Networked DC Microgrids. **2019**,		2
145	Transient Model-Based Detection Scheme for False Data Injection Attacks in Microgrids. **2019**,		2
144	Nonzero-Dynamics Stealthy Attack and Its Impacts Analysis in DC Microgrids. **2019**,		2
143	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	10.7	21
142	A Stealth Cyber-Attack Detection Strategy for DC Microgrids. *IEEE Transactions on Power Electronics*, **2019**, 34, 8162-8174	7.2	87
141	Networked Microgrids: State-of-the-Art and Future Perspectives. *IEEE Transactions on Industrial Informatics*, **2019**, 15, 1238-1250	11.9	91
140	State of the art of cyber-physical systems security: An automatic control perspective. **2019**, 149, 174-216		66
139	Stochastic Stability Analysis and Control of Secondary Frequency Regulation for Islanded Microgrids Under Random Denial of Service Attacks. *IEEE Transactions on Industrial Informatics*, **2019**, 15, 4066-4075	11.9	50
138	. *IEEE Transactions on Industrial Electronics*, **2019**, 66, 1543-1551	8.9	80
137	Signal Temporal Logic-Based Attack Detection in DC Microgrids. *IEEE Transactions on Smart Grid*, **2019**, 10, 3585-3595	10.7	50
136	Online Generative Adversary Network Based Measurement Recovery in False Data Injection Attacks: A Cyber-Physical Approach. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 2031-2043	11.9	30

135	Resilient Output Containment of Heterogeneous Cooperative and Adversarial Multigroup Systems. **2020**, 65, 3104-3111		7
134	Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 2716-2725	11.9	120
133	Detection and Mitigation of Data Manipulation Attacks in AC Microgrids. *IEEE Transactions on Smart Grid*, **2020**, 11, 2588-2603	10.7	25
132	Distributed Screening of Hijacking Attacks in DC Microgrids. *IEEE Transactions on Power Electronics*, **2020**, 35, 7574-7582	7.2	25
131	The data dimensionality reduction and bad data detection in the process of smart grid reconstruction through machine learning. **2020**, 15, e0237994		1
130	A review on microgrid architecture, cyber security threats and standards. **2020**,		6
129	A systematic review of cyber-resilience assessment frameworks. **2020**, 97, 101996		11
128	Microgrid Cyber-Security: Review and Challenges toward Resilience. **2020**, 10, 5649		16
127	Distributed Resilient Voltage and Reactive Power Control for Islanded Microgrids under False Data Injection Attacks. **2020**, 13, 3828		4
126	. **2020**, 22, 2586-2633		80
125	Cyber□physical attacks on power distribution systems. **2020**, 5, 218-225		8
124	Performance assessment of reverse droop control for multi-DER cooperative DC microgrid. **2020**,		
123	Distributed Resilient Secondary Control of DC Microgrids Against Unbounded Attacks. *IEEE Transactions on Smart Grid*, **2020**, 11, 3850-3859	10.7	24
122	On Detection of False Data in Cooperative DC Microgrids□A Discordant Element Approach. *IEEE Transactions on Industrial Electronics*, **2020**, 67, 6562-6571	8.9	56
121	A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids. *IEEE Transactions on Smart Grid*, **2020**, 11, 3690-3701	10.7	44
120	A novel protection scheme for low voltage DC microgrid using inductance estimation. *International Journal of Electrical Power and Energy Systems*, **2020**, 120, 105992	5.1	14
119	A Data-Driven Attack Detection Approach for DC Servo Motor Systems Based on Mixed Optimization Strategy. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 5806-5813	11.9	29
118	False data injection attacks on inverter-based microgrid in autonomous mode. **2020**, 125-146		2

117	False data injection attacks and countermeasures in smart microgrid systems. **2020**, 263-279		1
116	Extreme Learning Machine-Based State Reconstruction for Automatic Attack Filtering in Cyber Physical Power System. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 1892-1904	11.9	10
115	Distributed Resilient Control for Energy Storage Systems in Cyber-Physical Microgrids. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 1331-1341	11.9	38
114	False Data Injection Cyber-Attacks Mitigation in Parallel DC/DC Converters Based on Artificial Neural Networks. **2021**, 68, 717-721		19
113	Detection and Diagnosis of Data Integrity Attacks in Solar Farms Based on Multilayer Long Short-Term Memory Network. *IEEE Transactions on Power Electronics*, **2021**, 36, 2495-2498	7.2	21
112	Distributed Observer-Based Finite-Time Control of AC Microgrid Under Attack. *IEEE Transactions on Smart Grid*, **2021**, 12, 157-168	10.7	7
111	Cyber-Resilient Cooperative Control of Bidirectional Interlinking Converters in Networked AC/DC Microgrids. *IEEE Transactions on Industrial Electronics*, **2021**, 68, 9707-9718	8.9	7
110	A Cyber-Secure Distributed Control Architecture for Autonomous AC Microgrid. *IEEE Systems Journal*, **2021**, 15, 3324-3335	4.3	11
109	Mitigation of Motor Stalling and FIDVR via Energy Storage Systems With Signal Temporal Logic. **2021**, 36, 1164-1174		2
108	A Machine-Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 650-658	11.9	28
107	Securing Microgrid Optimal Energy Management Using Deep Generative Model. **2021**, 9, 63377-63387		2
106	. **2021**, 9, 16488-16507		9
105	Cyber security in power electronic systems. **2021**, 199-220		0
104	A Review of Cyber-Physical Security for Photovoltaic Systems. **2021**, 1-1		7
103	Reinforcement Learning Based Penetration Testing of a Microgrid Control Algorithm. **2021**,		2
102	Stability-Oriented Design of Cyberattack-Resilient Controllers for Cooperative DC Microgrids. *IEEE Transactions on Power Electronics*, **2021**, 1-1	7.2	5
101	Resilient Containment of Multi-Group Systems Against Unknown Unbounded FDI attacks. *IEEE Transactions on Industrial Electronics*, **2021**, 1-1	8.9	8
100	A Sub-grid-oriented Privacy-Preserving Microservice Framework based on Deep Neural Network for False Data Injection Attack Detection in Smart Grids. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	7

99	Communication Constraints for Distributed Secondary Control of Heterogenous Microgrids: A Survey. **2021**, 1-1		9
98	Cyber Attack Detection and Correction Mechanisms in a Distributed DC Microgrid. *IEEE Transactions on Power Electronics*, **2021**, 1-1	7.2	2
97	A Network Attack Detection Model of Smart Grid Based on XGBoost Algorithm. **2021**, 481-488		
96	A NDO Based Attack Detection Observer and Isolation Strategy in Distributed DC Microgrid with FDIA. **2021**, 1754, 012011		2
95	A Resilient Control Method Against False Data Injection Attack in DC Microgrids. **2021**,		
94	Performance and Vulnerability of Distributed Secondary Control of AC Microgrids under Cyber-Attack. **2021**,		
93	Deriving invariant checkers for critical infrastructure using axiomatic design principles. **2021**, 4,		2
92	Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. 1		5
91	A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids. *IEEE Transactions on Smart Grid*, **2021**, 12, 1929-1938	10.7	16
90	. *IEEE Internet of Things Journal*, **2021**, 8, 9422-9435	10.7	5
89	A Dynamic Reconfiguration-based Approach to Resilient State Estimation. **2021**,		
88	Using modified prediction interval-based machine learning model to mitigate data attack in microgrid. *International Journal of Electrical Power and Energy Systems*, **2021**, 129, 106847	5.1	2
87	Dynamic defenses in cyber security: Techniques, methods and challenges. **2021**,		3
86	Siamese Neural Network Based Few-Shot Learning for Anomaly Detection in Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 5790-5798	11.9	73
85	Mitigating Concurrent False Data Injection Attacks in Cooperative DC Microgrids. *IEEE Transactions on Power Electronics*, **2021**, 36, 9637-9647	7.2	8
84	Resilient Economic Control for Distributed Microgrids Under False Data Injection Attacks. *IEEE Transactions on Smart Grid*, **2021**, 12, 4435-4446	10.7	2
83	Resilient Control and Analysis for DC Microgrid System Under DoS and Impulsive FDI Attacks. *IEEE Transactions on Smart Grid*, **2021**, 12, 3742-3754	10.7	15
82	On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective. **2021**, 152, 111642		8

81	Threat Modelling of Cyber-Physical Systems Using an Applied Calculus. **2021**, 35, 100466		2
80	Cyber-Resilient Cooperative Control of DC Microgrid Clusters. *IEEE Systems Journal*, **2021**, 1-12	4.3	7
79	Concept Drift Analysis by Dynamic Residual Projection for effectively Detecting Botnet Cyber-attacks in IoT scenarios. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	1
78	Secure MPC/ANN-Based False Data Injection Cyber-Attack Detection and Mitigation in DC Microgrids. *IEEE Systems Journal*, **2021**, 1-12	4.3	9
77	Frequency Injection Based HVDC Attack-Defense Control Via Squeeze-Excitation Double CNN. **2021** , 1-1		17
76	BMI-Based Load Frequency Control in Microgrids Under False Data Injection Attacks. *IEEE Systems Journal*, **2021**, 1-11	4.3	10
75	Survey on automated symbolic verification and its application for synthesising cyber-physical systems. **2020**, 5, 1-24		6
74	Switching attacks on smart grid using non-linear sliding surface. **2019**, 4, 382-392		5
73	Mitigating zero dynamic attack in communication link-enabled droop-controlled hybrid AC/DC microgrids. **2020**, 5, 207-217		1
72	Survey of machine learning methods for detecting false data injection attacks in power systems. **2020**, 3, 581-595		26
71	Cyber-Security of Smart Microgrids: A Survey. **2021**, 14, 27		31
70	Hierarchical View on Detection of Attacks in Closed Loop Control Systems. *Lecture Notes on Data Engineering and Communications Technologies*, **2019**, 220-226	0.4	
69	Layered management and hybrid control strategy based on hybrid automata and random forest for microgrid. *IET Renewable Power Generation*, **2019**, 13, 3113-3123	2.9	3
68	Analyzing the Resiliency of Microgrid Control Algorithms Against Malicious Input. **2020**,		
67	An Enhanced Blockchain-Based Data Management Scheme for Microgrids. *Advances in Intelligent Systems and Computing*, **2020**, 766-775	0.4	1
66	Distributed Control of Parallel DC-DC Converters Under FDI Attacks on Actuators. *IEEE Transactions on Industrial Electronics*, **2021**, 1-1	8.9	1
65	Real-time distributed economic dispatch scheme of grid-connected microgrid considering cyberattacks. *IET Renewable Power Generation*, **2020**, 14, 2750-2758	2.9	2
64	Vulnerability Identification and Remediation of FDI Attacks in Islanded DC Microgrids Using Multi-agent Reinforcement Learning. *IEEE Transactions on Power Electronics*, **2021**, 1-1	7.2	3

63	Distributed synchronous detection for false data injection attack in cyber-physical microgrids. *International Journal of Electrical Power and Energy Systems*, **2022**, 137, 107788	5.1	2
62	Stability Investigation of DC Microgrids Under Stealth Cyber Attacks. **2021**,		0
61	Secure Control of DC Microgrids for Instant Detection and Mitigation of Cyber-Attacks Based on Artificial Intelligence. *IEEE Systems Journal*, **2021**, 1-12	4.3	2
60	Cyber-attack Detection for Photovoltaic Farms based on Power-Electronics-Enabled Harmonic State Space Modeling. *IEEE Transactions on Smart Grid*, **2021**, 1-1	10.7	0
59	Detection of Malicious Attacks in Autonomous Cyber-Physical Inverter-Based Microgrids. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	1
58	Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, **2022**, 43, 100452	8.3	8
57	Coordinated ancillary services, market participation and communication of multi-microgrids: A review. *Applied Energy*, **2022**, 308, 118332	10.7	6
56	Novel Hybrid Model for Intrusion Prediction on Cyber Physical Systems Communication Networks based on Bio-inspired Deep Neural Network Structure. *Journal of Information Security and Applications*, **2022**, 65, 103107	3.5	1
55	Secure Control of DC Microgrids under Cyber-Attacks based on Recurrent Neural Networks. **2020**,		4
54	A Novel Design of Concurrent Cyber Attacks in Cooperative DC Microgrids. **2020**,		0
53	Detection of False-Data Injection Attacks in Supercapacitor Charging Systems. **2020**,		1
52	A Periodic Event-Triggering Reactive Power Sharing Control in an Islanded Microgrid considering DoS Attacks. **2020**,		1
51	Research on Security Estimation and Control of Cyber-Physical System. **2020**,		
50	Attack-Resilient Distributed Control in DC Microgrids. **2021**,		
49	False Relay Operation Attacks in Power Systems with High Renewables. **2021**,		0
48	A Resilient Scheme for Mitigating False Data Injection Attacks in Distributed DC Microgrids. **2021**,		0
47	A Data-Driven Detection strategy of False Data in Cooperative DC Microgrids. **2021**,		0
46	Quantum-Key-Distribution Based Microgrid Control for Cybersecurity Enhancement. **2021**,		1

45	Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wireless Communications and Mobile Computing*, **2022**, 2022, 1-26	1.9	9
44	An Inertia-based Data Recovery Scheme for False Data Injection Attack. *IEEE Transactions on Industrial Informatics*, **2022**, 1-1	11.9	3
43	CONGO2: Scalable Online Anomaly Detection and Localization in Power Electronics Networks. *IEEE Internet of Things Journal*, **2022**, 1-1	10.7	0
42	False Data Injection Cyber-Attacks Detection for Multiple DC Microgrid Clusters. *Applied Energy*, **2022**, 310, 118425	10.7	3
41	Blockchain Protocol-based Predictive Secure Control for Networked Systems. *IEEE Transactions on Industrial Electronics*, **2022**, 1-1	8.9	3
40	Secure consensus control for multi-agent systems against attacks on actuators and sensors. *International Journal of Robust and Nonlinear Control*,	3.6	0
39	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	5.1	
38	SIEMS: A Secure Intelligent Energy Management System for Industrial IoT applications. *IEEE Transactions on Industrial Informatics*, **2022**, 1-1	11.9	1
37	A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. *Renewable Energy*, **2022**, 189, 1383-1406	8.1	2
36	A novel strategy for locational detection of false data injection attack. *Sustainable Energy, Grids and Networks*, **2022**, 31, 100702	3.6	1
35	Optimal Chi-squared Detector of Replay Attacks on Cyber-Physical Systems. **2021**,		
34	Small-signal stability and robustness analysis for microgrids under time-constrained DoS attacks and a mitigation adaptive secondary control method. *Science China Information Sciences*, **2022**, 65, 1	3.4	3
33	Secure Data Transmission and Trustworthiness Judgement Approaches Against Cyber-Physical Attacks in an Integrated Data-Driven Framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, **2022**, 1-11	7.3	0
32	Optimal Communication Network Design of Microgrids Considering Cyber-Attacks and Time-Delays. *IEEE Transactions on Smart Grid*, **2022**, 1-1	10.7	3
31	The Control Strategy for Power CPS Microgrid under Network Attack. **2022**,		
30	False Data Injection-and Propagation-Aware Game Theoretical Approach for Microgrids. *IEEE Transactions on Smart Grid*, **2022**, 1-1	10.7	
29	Data-driven Cyber-attack Detection of Intelligent Attacks in Islanded DC Microgrids. *IEEE Transactions on Industrial Electronics*, **2022**, 1-1	8.9	1
28	Cyber-Attack Detection for Active Neutral Point Clamped (ANPC) Photovoltaic (PV) Converter using Kalman Filter. **2022**,		

27	Sequential Detection of Microgrid Bad Data via a Data-Driven Approach Combining Online Machine Learning With Statistical Analysis. *Frontiers in Energy Research*, 10,	3.8	1
26	Security of digitalized process systems. *Methods in Chemical Process Safety*, **2022**,	1.1	0
25	Distributed Secondary Control Strategy Against Bounded FDI Attacks for Microgrid With Layered Communication Network. *Frontiers in Energy Research*, 10,	3.8	
24	Data-Driven Detection of Stealth Cyber-Attacks in DC Microgrids. *IEEE Systems Journal*, **2022**, 1-10	4.3	1
23	Fault and Attack Detection and Diagnosis by Analysis of Electrical Waveforms of Power Networks. **2022**,		
22	Distributed event-triggered secondary frequency control of islanded AC microgrids under cyber attacks with input time delay. **2022**, 143, 108506		0
21	PowerFDNet: Deep Learning-Based Stealthy False Data Injection Attack Detection for AC-Model Transmission Systems. **2022**, 3, 149-161		0
20	Resilient operation of DC microgrid against FDI attack: A GRU based framework. **2023**, 145, 108586		0
19	A Novel Attack Identification Mechanism in IoT-Based Converter-Composed DC Grids. **2022**, 1-1		0
18	Resilient Operation of BESS in a Cooperative DC Microgrid under Data Manipulation Attacks. **2022**,		0
17	Distributed Data Recovery Against False Data Injection Attacks in DC Microgrids. **2022**,		0
16	Detection of False Data Injection Cyberattacks: Experimental Validation on a Lab-scale Microgrid. **2022**,		0
15	Distributed Mitigation Layers for Voltages and Currents Cyber-Attacks on DC Microgrids Interfacing Converters. **2022**, 15, 9426		0
14	Defense Strategy against False Data Injection Attacks in Ship DC Microgrids. **2022**, 10, 1930		0
13	Resilience-based output containment control of heterogeneous MAS against unbounded attacks.		0
12	Distributed Control Microgrids: Cyber-Attack Models, Impacts and Remedial Strategies. **2022**, 8, 1008-1023		0
11	Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey.		0
10	Customization of Bookkeeping system for Blockchain System Analysis: A Review. **2022**,		0

9	Comparative Evaluation of Cyber-Attacks on AC Microgrid Secondary Control. **2022**,	0
8	Cybersecurity Challenges in Microgrids: Inverter-Based Resources and Electric Vehicles. **2023**, 91-114	0
7	Incremental Security Enforcement for Cyber-Physical Systems. **2023**, 11, 18475-18498	0
6	Analysis of safety and security challenges and opportunities related to cyber-physical systems. **2023**, 173, 384-413	0
5	Consensus-based Frequency Control of a Cyber-physical Power System under Two Types of DDoS Attacks. **2022**,	0
4	False Data Injection Attacks in Power Systems. 1-15	0
3	A Learning-Based Tolerance Method for False Data Injection Attacks in Microgrid Secondary Control. **2022**,	0
2	Wavelet analysis and consensus algorithm-based fault-tolerant control for smart grids. 11,	0
1	A hierarchical framework for distributed resilient control of islanded AC microgrids under false data injection attacks. **2023**,	0