Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks

DOI: 10.1109/tii.2018.2825243
IEEE Transactions on Industrial Informatics, 2018, 14, 3271-32

#	Paper	IF	Citations
158	Subset Level Detection of False Data Injection Attacks in Smart Grids. **2018**,		4
157	Delay aware transient stability assessment with synchrophasor recovery and prediction framework. **2018**, 322, 187-194		9
156	Physical-Model-Checking to Detect Switching-Related Attacks in Power Systems. **2018**, 18,		3
155	Real-Time Identification of False Data Injection Attacks: A Novel Dynamic-Static Parallel State Estimation Based Mechanism. **2019**, 7, 95812-95824		7
154	Genetic similarity of biological samples to counter bio-hacking of DNA-sequencing functionality. **2019**, 9, 8684		1
153	Quickest Detection of False Data Injection Attacks in Smart Grid with Dynamic Models. **2019**, 1-1		6
152	Detection of the False Data Injection Attack in Home Area Networks using ANN. **2019**,		2
151	False data injection attacks against smart gird state estimation: Construction, detection and defense. **2019**, 62, 2077-2087		26
150	Dynamic Data Injection Attack Detection of Cyber Physical Power Systems With Uncertainties. *IEEE Transactions on Industrial Informatics*, **2019**, 15, 5505-5518	11.9	40
149	Toward a Lightweight Intrusion Detection System for the Internet of Things. **2019**, 7, 42450-42471		81
148	Synchrophasor Recovery and Prediction: A Graph-Based Deep Learning Approach. *IEEE Internet of Things Journal*, **2019**, 6, 7348-7359	10.7	18
147	Non-intrusive Runtime Monitoring for Power System Intelligent Terminal Based on Improved Deep Belief Networks (I-DBN). **2019**,		
146	An Industrial Network Intrusion Detection Algorithm Based on Multifeature Data Clustering Optimization Model. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 2063-2071	11.9	86
145	A Network Attack Detection Method Using SDA and Deep Neural Network Based on Internet of Things. **2020**, 27, 209-214		2
144	Load Disaggregation Using One-Directional Convolutional Stacked Long Short-Term Memory Recurrent Neural Network. **2020**, 14, 1395-1404		14
143	Sensor attack detection for cyber-physical systems based on frequency domain partition. **2020**, 14, 1452-1466		7
142	Local False Data Injection Attack Theory Considering Isolation Physical-Protection in Power Systems. **2020**, 8, 103285-103290		5

(2021-2020)

141	Active Learning-Based XGBoost for Cyber Physical System Against Generic AC False Data Injection Attacks. **2020**, 8, 144575-144584		8
140	Real-Time Intrusion Detection in Wireless Network: A Deep Learning-Based Intelligent Mechanism. **2020**, 8, 170128-170139		5
139	Mitigating the Impacts of False Data Injection Attacks in Smart Grids using Deep Convolutional Neural Networks. **2020**,		
138	Detection of False Data Injection Attacks Using the Autoencoder Approach. **2020**,		8
137	Fusion Estimation for FDI Sensor Attacks in Distributed Systems. **2020**,		1
136	. **2020**, 14, 4-17		13
135	A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network. **2020**, 8, 89337-89350		36
134	Detecting bi-level false data injection attack based on time series analysis method in smart grid. *Computers and Security*, **2020**, 96, 101899	4.9	1
133	A Novel False Data Injection Attack Detection Model of the Cyber-Physical Power System. **2020**, 8, 95109-95125		19
132	Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. **2020**, 54, 102518		19
131	. *IEEE Internet of Things Journal*, **2020**, 7, 8218-8227	10.7	25
130	A Secure Hybrid Dynamic-State Estimation Approach for Power Systems Under False Data Injection Attacks. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 7275-7286	11.9	29
129	Semi-supervised deep ensemble learning for travel mode identification. **2020**, 112, 120-135		12
128	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
127	Secure Information Fusion using Local Posterior for Distributed Cyber-Physical Systems. **2021**, 20, 2041-2054		0
126	A Graph Theory-Based Approach to Detect False Data Injection Attacks in Power System AC State Estimation. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 2465-2475	11.9	14
125	Markov Game for Securing Wide-Area Damping Control Against False Data Injection Attacks. **2021**, 15, 1356-1365		3
124	. **2021**, 15, 2046-2057		2

123	Perturbation-Based Diagnosis of False Data Injection Attack Using Distributed Energy Resources. *IEEE Transactions on Smart Grid*, **2021**, 12, 1589-1601	10.7	8
122	Active resilient control for two-dimensional systems under denial-of-service attacks. **2021**, 31, 759-771		1
121	Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach. *IEEE Transactions on Smart Grid*, **2021**, 12, 623-634	10.7	42
120	On the Resiliency of Power and Gas Integration Resources Against Cyber Attacks. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 3099-3110	11.9	6
119	Distributed Data-Driven Intrusion Detection for Sparse Stealthy FDI Attacks in Smart Grids. **2021**, 68, 993-997		11
118	Travel Mode Identification With GPS Trajectories Using Wavelet Transform and Deep Learning. **2021**, 22, 1093-1103		13
117	Cyber-Physical Anomaly Detection in Microgrids Using Time-Frequency Logic Formalism. **2021**, 9, 20012-20021		5
116	. **2021**, 9, 16488-16507		9
115	Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. **2021**, 9, 29775-29818		40
114	AI Methods for Neutralizing Cyber Threats at Unmanned Vehicular Ecosystem of Smart City. **2021**, 157-171		1
113	An abnormal traffic detection method in smart substations based on coupling field extraction and DBSCAN. **2021**, 260, 02005		
112	Security Analysis for Dynamic State Estimation of Power Systems With Measurement Delays. **2021**, PP,		9
111	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
110	A Federated Learning Framework for Detecting False Data Injection Attacks in Solar Farms. **2021**, 1-1		6
109	Establishing a detection model data attacks in power distribution system. **2021**, 257, 01082		
108	Deep Learning-Assisted Short-Term Load Forecasting for Sustainable Management of Energy in Microgrid. **2021**, 6, 15		12
107	Sequential Perturbation-based Attack Detection using DERs for Unbalanced Distribution System. **2021**,		0
106	Cyber Attacks and Faults Discrimination in Intelligent Electronic Device-Based Energy Management Systems. **2021**, 10, 650		3

105	Research on Power Planning Considering Power Grid Security. **2021**,		1
104	Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. 1		5
103	ConAML: Constrained Adversarial Machine Learning for Cyber-Physical Systems. **2021**,		5
102	Consensus-Based Distributed Target Tracking with False Data Injection Attacks over Radar Network. *Applied Sciences (Switzerland)*, **2021**, 11, 4564	2.6	1
101	Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids. **2021**, 103116		10
100	A Deep Learning-Based Classification Scheme for False Data Injection Attack Detection in Power System. **2021**, 10, 1459		1
99	On the security of ANN-based AC state estimation in smart grid. *Computers and Security*, **2021**, 105, 102265	4.9	1
98	Fourier Singular Values-Based False Data Injection Attack Detection in AC Smart-Grids. *Applied Sciences (Switzerland)*, **2021**, 11, 5706	2.6	7
97	Deep-learning-based data-manipulation attack resilient supervisory backup protection of transmission lines. 1		1
96	Computational intelligence technologies stack for protecting the critical digital infrastructures against security intrusions. **2021**,		0
95	Generalized attack separation scheme in cyber physical smart grid based on robust interval state estimation. *International Journal of Electrical Power and Energy Systems*, **2021**, 129, 106741	5.1	4
94	Stacked Autoencoder Framework of False Data Injection Attack Detection in Smart Grid. **2021**, 2021, 1-8		0
93	Network-based multidimensional moving target defense against false data injection attack in power system. *Computers and Security*, **2021**, 107, 102283	4.9	4
92	Semi-supervised anomaly detection in dynamic communication networks. **2021**, 571, 527-542		2
91	Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled CyberPhysical Systems. *IEEE Internet of Things Journal*, **2021**, 8, 13712-13722	10.7	14
90	Deep learning for online AC False Data Injection Attack detection in smart grids: An approach using LSTM-Autoencoder. **2021**, 193, 103178		2
89	Deep Learning-Based Reliable Routing Attack Detection Mechanism for Industrial Internet of Things. **2021**, 123, 102661		3
88	Parameter tampering cyberattack and event-trigger detection in game-based interactive demand response. *International Journal of Electrical Power and Energy Systems*, **2022**, 135, 107550	5.1	2

87	Wavelet probability distribution mapping for detection and correction of dynamic data injection attacks in WAMS. *International Journal of Electrical Power and Energy Systems*, **2022**, 134, 107447	5.1	0
86	. **2021**, 9, 119118-119138		4
85	Spatio-Temporal Correlation-Based False Data Injection Attack Detection Using Deep Convolutional Neural Network. *IEEE Transactions on Smart Grid*, **2021**, 1-1	10.7	3
84	Deep Representation Learning for Cyber-Attack Detection in Industrial IoT. **2021**, 139-162		1
83	Detection of False Data Injection Attacks in Smart Grid Based on Machine Learning. **2021**, 191-203		
82	BMI-Based Load Frequency Control in Microgrids Under False Data Injection Attacks. **2021**, 1-11		10
81	Survey of machine learning methods for detecting false data injection attacks in power systems. **2020**, 3, 581-595		26
80	Cyber-Security of Smart Microgrids: A Survey. **2021**, 14, 27		31
79	Accurate Detection of False Data Injection Attacks in Renewable Power Systems Using Deep Learning. **2021**, 9, 135774-135789		4
78	Introduction to Machine Learning Methods in Energy Engineering. **2021**, 61-82		0
77	Introduction and Literature Review of Power System Challenges and Issues. **2021**, 19-43		1
76	@PAD. **2020**,		
75	Identification and Correction of False Data Injection Attacks against AC State Estimation using Deep Learning. **2020**,		
74	False Data Injection Attacks in Smart Grid Using Gaussian Mixture Model. **2020**,		
73	A Simple Cyber Attack Detection Scheme for Smart Grid Cyber Security Enhancement. **2020**,		
72	A cyber-attack detection method for load control system based on cyber and physical layer crosscheck mechanism.		
71	False Data Injection Attack Detection and Improved WLS Power System State Estimation Based on Node Trust. 1		0
70	. *IEEE Transactions on Smart Grid*, **2021**, 1-1	10.7	0

69	Adaptive sliding-mode tracking control of networked control systems with false data injection attacks. **2022**, 585, 194-208		4
68	A Data Driven Threat-Maximizing False Data Injection Attack Detection Method with Spatio-Temporal Correlation. **2021**,		
67	An enhanced UAV safety control scheme against attacks on desired trajectory. **2021**, 119, 107212		0
66	Detection of Malicious Attacks in Autonomous Cyber-Physical Inverter-Based Microgrids. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	1
65	A New Explainable Deep Learning Framework for Cyber Threat Discovery in Industrial IoT Networks. *IEEE Internet of Things Journal*, **2021**, 1-1	10.7	2
64	Experience Driven Attack Design and Federated Learning Based Intrusion Detection in Industry 4.0. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	2
63	Optimized cyber-attack detection method of power systems using sliding mode observer. **2022**, 205, 107745		1
62	An integrated data-driven scheme for the defense of typical cyber▯physical attacks. **2022**, 220, 108257		1
61	Training Strategies for Autoencoder-based Detection of False Data Injection Attacks. **2020**,		1
60	A Novel Design of Concurrent Cyber Attacks in Cooperative DC Microgrids. **2020**,		0
59	FDIA Detection through an Adaptive Multi-Level Features Classification in Smart Grids. **2020**,		0
58	A Highly Discriminative Detector against False Data Injection Attacks in AC State Estimation. *IEEE Transactions on Smart Grid*, **2022**, 1-1	10.7	1
57	A Proof-of-Authority Blockchain Based Distributed Control System for Islanded Microgrids. *IEEE Transactions on Industrial Informatics*, **2022**, 1-1	11.9	3
56	Auto-Starting Semi-Supervised Learning-Based Identification of Synchrophasor Data Anomalies. *IEEE Internet of Things Journal*, **2022**, 1-1	10.7	
55	Data-Driven Detection of Stealthy False Data Injection Attack Against Power System State Estimation. *IEEE Transactions on Industrial Informatics*, **2022**, 1-1	11.9	4
54	CAE: Contextual auto-encoder for multivariate time-series anomaly detection in air transportation. *Computers and Security*, **2022**, 116, 102652	4.9	1
53	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	
52	Hierarchical Blockchain Design for Distributed Control and Energy Trading within Microgrids. *IEEE Transactions on Smart Grid*, **2022**, 1-1	10.7	2

51	Data Integrity Attack in Dynamic State Estimation of Smart Grid: Attack Model and Countermeasures. *IEEE Transactions on Automation Science and Engineering*, **2022**, 1-14	4.9	0
50	Low Latency Cyberattack Detection in Smart Grids with Deep Reinforcement Learning. *SSRN Electronic Journal*,	1	0
49	A novel strategy for locational detection of false data injection attack. *Sustainable Energy, Grids and Networks*, **2022**, 31, 100702	3.6	1
48	Detection of False Data Injection Attacks Using Cross Wavelet Transform and Machine Learning. **2021**,		
47	A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithm. *Expert Systems*,	2.1	2
46	Fake Data Injection Attack Detection in AMI System Using a Hybrid Method. **2021**,		
45	Cyber Attack Detection in PMU Networks Exploiting the Combination of Machine Learning and State Estimation-Based Methods. **2021**,		0
44	Deep learning-based defense and detection scheme against eavesdropping and typical cyber-physical attacks. **2021**,		
43	Deep Federated Learning-Based Cyber-Attack Detection in Industrial Control Systems. **2021**,		0
42	Intelligent GPS Spoofing Attack Detection in Power Grid. **2021**,		1
41	Detection and Prediction of FDI Attacks in IoT Systems via Hidden Markov Model. *IEEE Transactions on Network Science and Engineering*, **2022**, 1-1	4.9	0
40	Model-free predictive control of nonlinear systems under False Data Injection attacks. *Computers and Electrical Engineering*, **2022**, 100, 107977	4.3	
39	Malicious data injection attacks risk mitigation strategy of cyber▯physical power system based on hybrid measurements attack detection and risk propagation. *International Journal of Electrical Power and Energy Systems*, **2022**, 142, 108241	5.1	
38	Low latency cyberattack detection in smart grids with deep reinforcement learning. *International Journal of Electrical Power and Energy Systems*, **2022**, 142, 108265	5.1	1
37	False Data Injection Attack Detection Based on Wavelet Packet Decomposition and Random Forest in Smart Grid. **2021**,		
36	Network Attack Detection Method of the Cyber-Physical Power System Based on Ensemble Learning. *Applied Sciences (Switzerland)*, **2022**, 12, 6498	2.6	2
35	Impact Assessment and Defense for Smart Grids with FDIA Against AMI. **2022**, 1-13		
34	Online routing for smart electricity network under hybrid uncertainty. **2022**, 145, 110538		0

(2023-2022)

33	Review of active defense methods against power CPS false data injection attacks from the multiple spatiotemporal perspective. **2022**, 8, 11235-11248	0
32	PowerFDNet: Deep Learning-Based Stealthy False Data Injection Attack Detection for AC-Model Transmission Systems. **2022**, 3, 149-161	0
31	Hybrid-AI Blockchain Supported Protection Framework for Smart Grids. **2022**, 646-659	1
30	False data injection attack detection in dynamic power grid: A recurrent neural network-based method. 10,	0
29	Detection of Cyber-Attacks in Smart Power Transmission System using Mathematical Morphology and Autoencoder. **2022**,	0
28	Active Defense Research against False Data Injection Attacks of Power CPS Based on Data-Driven Algorithms. **2022**, 15, 7432	1
27	A secure forecasting-aided state estimation framework for power distribution systems against false data injection attacks. **2022**, 328, 120107	0
26	Graph-based detection for false data injection attacks in power grid. **2023**, 263, 125865	1
25	A Novel Attack Identification Mechanism in IoT-Based Converter-Composed DC Grids. **2022**, 1-1	0
24	Security Enhancement of Network Constraint Grid-Edge Energy Management System. **2022**,	0
23	A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. **2023**, 40, 100582	0
22	Research on Security Defense of Coupled Transportation and Cyber-Physical Power System Based on the Static Bayesian Game. **2022**, 1-13	0
21	An Ensemble Learning-Based Cyber-Attacks Detection Method of Cyber-Physical Power Systems. **2022**,	0
20	False Data Injection Attacks Detection in Real Smart Grid with Edge Computing. **2022**,	0
19	A Proactive Attack Detection for Heating, Ventilation, and Air Conditioning (HVAC) System Using Explainable Extreme Gradient Boosting Model (XGBoost). **2022**, 22, 9235	1
18	Fast economic dispatch with false data injection attack in electricity-gas cyber-physical system: A data-driven approach. **2022**,	0
17	Review on the Microgrid Concept, Structures, Components, Communication Systems, and Control Methods. **2023**, 16, 484	3
16	Hybrid Physics-Based and Data-Driven Mitigation Strategy for Automatic Generation Control Under Cyber Attack. **2023**, 135-160	0

15	Detection of False Data Injection Attacks in Smart Grids Based on Expectation Maximization. **2023**, 23, 1683	0
14	CNN-GRU based fake data injection attack detection method for power grid. **2022**,	0
13	Hybrid Machine Learning based False Data Injection Attack Detection and Mitigation Model for Waste Water Treatment Plant. **2022**,	0
12	Machine Learning Approaches in Cyber Attack Detection and Characterization in IoT enabled Cyber-Physical Systems. **2023**,	0
11	Detection of data-driven blind cyber-attacks on smart grid: A deep learning approach. **2023**, 92, 104475	0
10	Random Bad State Estimator to Address False Data Injection in Critical Infrastructures. **2022**,	0
9	Detection and reconstruction of measurements against false data injection and DoS attacks in distribution system state estimation: A deep learning approach. **2023**, 210, 112565	0
8	Robust and Secure Quality Monitoring for Welding through Platform-as-a-Service: A Resistance and Submerged Arc Welding Study. **2023**, 11, 298	0
7	Robust Kalman Filter for Position Estimation of Automated Guided Vehicles Under Cyberattacks. **2023**, 72, 1-12	0
6	Bespoke Mitigation Framework for False Data Injection Attack-Induced Contingency Events. **2023**,	0
5	An Optimization-Based Robust Dynamic State Estimation for Power Systems with Synchronized Phasor Measurement Units, Involving Disturbance Rejection. **2023**, 2023, 1-22	0
4	Privacy-Preserving Truth Discovery with Truth Transparency. **2023**, 109-142	0
3	Detection of false data injection attacks on power systems using graph edge-conditioned convolutional networks. **2023**, 8,	0
2	A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids.	0
1	Detection and Prevention of Cyber-Attacks in Cyber-Physical Systems based on Nature Inspired Algorithm. **2023**,	0