

Can Attackers With Limited Information Exploit Historical Data Injection Attacks on Power Systems?

IEEE Transactions on Power Systems

33, 4775-4786

DOI: [10.1109/tpwrs.2018.2818746](https://doi.org/10.1109/tpwrs.2018.2818746)

Citation Report

#	ARTICLE	IF	CITATIONS
1	Unobservable False Data Injection Attacks against PMUs: Feasible Conditions and Multiplicative Attacks. , 2018, , .		9
2	Intelligent data attacks against power systems using incomplete network information: a review. Journal of Modern Power Systems and Clean Energy, 2018, 6, 630-641.	3.3	21
3	Fast Screening of High-Risk Lines Under False Data Injection Attacks. IEEE Transactions on Smart Grid, 2019, 10, 4003-4014.	6.2	35
4	Modelling and Vulnerability Analysis of Cyber-Physical Power Systems Based on Interdependent Networks. Energies, 2019, 12, 3439.	1.6	20
5	False data injection attacks against smart grid state estimation: Construction, detection and defense. Science China Technological Sciences, 2019, 62, 2077-2087.	2.0	43
6	Intrusion Detection Systems: A Cross-Domain Overview. IEEE Communications Surveys and Tutorials, 2019, 21, 3639-3681.	24.8	61
7	Dynamic Data Injection Attack Detection of Cyber Physical Power Systems With Uncertainties. IEEE Transactions on Industrial Informatics, 2019, 15, 5505-5518.	7.2	71
8	Modeling and Analysis Cyber Threats in Power Systems Using Architecture Analysis & Design Language (AADL). , 2019, , .		1
9	The data dimensionality reduction and bad data detection in the process of smart grid reconstruction through machine learning. PLoS ONE, 2020, 15, e0237994.	1.1	5
10	Local False Data Injection Attack Theory Considering Isolation Physical-Protection in Power Systems. IEEE Access, 2020, 8, 103285-103290.	2.6	10
11	Microgrid Cyber-Security: Review and Challenges toward Resilience. Applied Sciences (Switzerland), 2020, 10, 5649.	1.3	44
12	Power Systems Decomposition for Robustifying State Estimation Under Cyber Attacks. IEEE Transactions on Power Systems, 2021, 36, 1922-1933.	4.6	14
13	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.	7.2	48
14	Smart Grid Security Enhancement by Using Belief Propagation. IEEE Systems Journal, 2021, 15, 2046-2057.	2.9	8
15	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
16	An Optimization-Based Approach to Recover the Detected Attacked Grid Variables After False Data Injection Attack. IEEE Transactions on Smart Grid, 2021, 12, 5322-5334.	6.2	11
17	Network Parameter Coordinated False Data Injection Attacks Against Power System AC State Estimation. IEEE Transactions on Smart Grid, 2021, 12, 1626-1639.	6.2	32
18	Zero-Parameter-Information Data Integrity Attacks and Countermeasures in IoT-Based Smart Grid. IEEE Internet of Things Journal, 2021, 8, 6608-6623.	5.5	32

#	ARTICLE	IF	CITATIONS
19	Review of Cyber-Physical Attacks in Smart Grids: A System-Theoretic Perspective. Electronics (Switzerland), 2021, 10, 1153.	1.8	15
20	Observer-based reconstruction for smart grid cyber attack detection. , 2021, , .		2
21	A Cyber-Secured Operation for Water-Energy Nexus. IEEE Transactions on Power Systems, 2021, 36, 3105-3117.	4.6	12
22	Tri-level defense strategy for electricity-gas integrated systems against load redistribution attacks. International Transactions on Electrical Energy Systems, 2021, 31, e13062.	1.2	1
23	Deep learning algorithms for cyber security applications: A survey. Journal of Computer Security, 2021, 29, 447-471.	0.5	9
24	\$N-1\$ Reliability Makes It Difficult for False Data Injection Attacks to Cause Physical Consequences. IEEE Transactions on Power Systems, 2021, 36, 3897-3906.	4.6	8
25	Cyber Security of Market-Based Congestion Management Methods in Power Distribution Systems. IEEE Transactions on Industrial Informatics, 2021, 17, 8142-8153.	7.2	5
26	Parameter tampering cyberattack and event-trigger detection in game-based interactive demand response. International Journal of Electrical Power and Energy Systems, 2022, 135, 107550.	3.3	4
27	Cyber attacks in smart grid – dynamic impacts, analyses and recommendations. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 321-329.	1.9	11
28	Stochastic games for power grid coordinated defence against coordinated attacks. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 292-300.	1.9	5
29	Operations research in optimal power flow: A guide to recent and emerging methodologies and applications. European Journal of Operational Research, 2022, 300, 387-404.	3.5	29
30	Accuracy improvement of electrical load forecasting against new cyber-attack architectures. Sustainable Cities and Society, 2022, 77, 103523.	5.1	7
31	Unified Detection of Attacks Involving Injection of False Control Commands and Measurements in Transmission Systems of Smart Grids. IEEE Transactions on Smart Grid, 2022, 13, 1598-1610.	6.2	6
32	Computation of Worst-case Operation Scenarios against False Data Injection Attacks Considering Load Demand and Generation Uncertainties. , 2020, , .		1
33	Power Systems Intrusion Detection Using Novel Wrapped Feature Selection Framework. , 2020, , .		1
34	An Inertia-Based Data Recovery Scheme for False Data Injection Attack. IEEE Transactions on Industrial Informatics, 2022, 18, 7814-7823.	7.2	21
35	A GAN-Based Data Injection Attack Method on Data-Driven Strategies in Power Systems. IEEE Transactions on Smart Grid, 2022, 13, 3203-3213.	6.2	5
36	Blind False Data Injection Attacks Against State Estimation Based on Matrix Reconstruction. IEEE Transactions on Smart Grid, 2022, 13, 3174-3187.	6.2	8

#	ARTICLE	IF	CITATIONS
37	A Deep Learning Approach to Anomaly Sequence Detection for High-Resolution Monitoring of Power Systems. IEEE Transactions on Power Systems, 2023, 38, 4-13.	4.6	2
38	Revealing Vulnerability of N-1 Secure Power Systems to Coordinated Cyber-Physical Attacks. IEEE Transactions on Power Systems, 2023, 38, 1044-1057.	4.6	6
40	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
41	Datadriven false data injection attacks against cyber-physical power systems. Computers and Security, 2022, 121, 102836.	4.0	8
42	Cyber-physical risk modeling with imperfect cyber-attackers. Electric Power Systems Research, 2022, 211, 108437.	2.1	8
43	False data injection threats in active distribution systems: A comprehensive survey. Future Generation Computer Systems, 2023, 140, 344-364.	4.9	9
44	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
46	A Review on Defense Mechanism against the Denial of Service and False Data Injection in Cyber-Physical Power Systems. , 2023, , .		1
50	A Poisoning Attack for Data-Driven Strategies in Power Systems. , 2023, , .		0
52	A Stream-Based Approach to Intrusion Detection. , 2024, , 253-291.		0