IEEE13-AdvAttack A Novel Dataset for Benchmarking the Power of Adversarial Attacks against Fault Prediction Systems in Smart Electrical Grid

Carmelo Ardito
carmelo.ardito@poliba.it
Polytechnic University of Bari
Bari, Italy

Yashar Deldjoo
yashar.deldjoo@poliba.it
Polytechnic University of Bari
Bari, Italy

Tommaso Di Noia
tommaso.dinoia@poliba.it
Polytechnic University of Bari
Bari, Italy

Eugenio Di Sciascio
eugenio.disciascio@poliba.it
Polytechnic University of Bari
Bari, Italy

Fatemeh Nazary*
fatemeh.nazary@poliba.it
Polytechnic University of Bari
Bari, Italy

ABSTRACT

Due to their economic and significant importance, fault detection tasks in intelligent electrical grids are vital. Although numerous smart grid (SG) applications, such as fault detection and load forecasting, have adopted data-driven approaches, the robustness and security of these data-driven algorithms have not been widely examined. One of the greatest obstacles in the research of the security of smart grids is the lack of publicly accessible datasets that permit testing the system's resilience against various types of assault. In this paper, we present **IEEE13-AdvAttack**, a large-scaled simulated dataset based on the IEEE-13 test node feeder suitable for supervised tasks under SG. The dataset includes both conventional and renewable energy resources. We examine the robustness of fault type classification and fault zone classification systems to adversarial attacks. Through the release of datasets, benchmarking, and assessment of smart grid failure prediction systems against adversarial assaults, we seek to encourage the implementation of machine-learned security models in the context of smart grids. The benchmarking data and code for fault prediction are made publicly available on https://bit.ly/3NT5jxG.

CCS CONCEPTS

• **Computing methodologies** → *Machine learning*.

KEYWORDS

Adversarial Machine Learning, Attack, Smart Grid, Fault Classification

*Corresponding author: Fatemeh Nazary. Authors are listed in alphabetical order.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CIKM '22, October 17–21, 2022, Atlanta, GA, USA
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9236-5/22/10…$15.00
https://doi.org/10.1145/3511808.3557612

ACM Reference Format:
Carmelo Ardito, Yashar Deldjoo, Tommaso Di Noia, Eugenio Di Sciascio, and Fatemeh Nazary. 2022. IEEE13-AdvAttack A Novel Dataset for Benchmarking the Power of Adversarial Attacks against Fault Prediction Systems in Smart Electrical Grid. In *Proceedings of the 31st ACM International Conference on Information and Knowledge Management (CIKM '22), October 17–21, 2022, Atlanta, GA, USA.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3511808.3557612

1 INTRODUCTION

According to a statement released by the World Health Organization, at least one in every ten patients experiences suffer as a result of inadequate infrastructure security. Instability or inadequate distribution of electrical energy can directly influence people's lives and societal well-being. The current study is concerned with the "security of power grids", which serve as the country's critical energy infrastructure (CEI) [25]. Conventionally-operated electrical grids have undergone significant alterations and updates in terms of dependability, robustness, and efficiency throughout the years, giving rise to what we now refer to as Smart Grids (SG). One of the most critical aspects of SGs is their application in fault detection, fault classification, and routine examination of the underlying disturbances that cause failures [6]. Power grid networks are naturally susceptible to physical damage, and electrical faults can be produced by natural accidents such as a tree falling on a power line, a bird contacting the line, lightning, or the aging of the equipment.

The dataset we release here focuses on two primary objectives: (i) the classifications of faults and the regions in which they are likely to occur, and (ii) the investigation of adversarial machine-learning attacks directed against fault type and zone classification systems.

Fault zone and type classification in SGs. Fault zone classification (FZC) aims to find the zone (or sometimes the exact location) in which the fault has occurred, while in fault type classification (FCT) the primary objective is to determine the fault's type class. Voltage sags are the main cause of faults, which can manifest as asymmetric phase-to-phase (LL), single-phase-to-ground (LG), or two-phase-to-ground (LLG) or symmetric three-phase-to-ground (LLLG or LLL) faults in both transmission and distribution systems [1, 29]. Previous literature has utilized a combination of tools and techniques from electrical engineering, signal processing, and

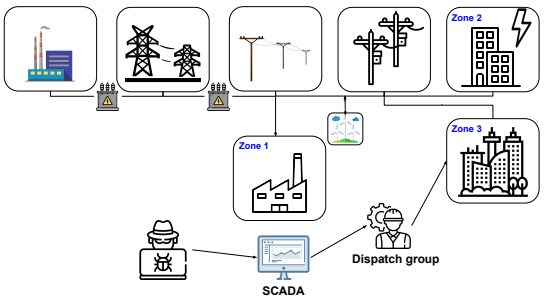

Figure 1: A hypothetical illustration of targeted adversarial attacks against fault zone prediction in smart grids. As a result of an adversarial assault on a fault location prediction system, dispatch recovery groups were inadvertently sent to zone 3 instead of zone 2, where the real fault had occurred.

artificial intelligence (AI) [7, 8, 13, 27, 29] to solve the above fault classification tasks. Among them, machine-learned (ML) models, notably those based on deep learning, have witnessed an increase in their acceptance in the current infrastructure of power systems, owing to the huge amounts of data spanning energy networks.

Adversarial attacks against machine-learned fault classification systems. Despite their excellent efficiency, the complexity of existing (deep) inference methods may be their undoing. These vulnerabilities can be exploited by adversaries to undermine the confidentiality, integrity, or availability of SGs (aka the CIA triad) [15, 33]. Adversarial attacks are operationalized via *adversarial examples* – subtle but non-random perturbations – designed to induce a ML model to produce erroneous outputs (e.g., to misclassify an input sample) [3, 14]. As seen in Figure 1, an attacker can enter the SG system's communication network in order to attack the failure prediction system used in supervisory control and data acquisition (SCADA) [11]. The purpose of the targeted adversarial attack is to induce the SCADA fault classification system's machine learning (ML) model to misclassify an input sample as belonging to a known but incorrect class. To achieve this objective, the attacker in the FZC scenario chooses as (illegitimate) target class label the one that can cause the most harm and suffering, so as to extend the expedition and recovery effort. For instance, the attacker could generate a fake positive signal and direct the rescue squad to more inaccessible and populated places that are actually faultless.

Challenge and contributions. One of the greatest obstacles to the development of advanced machine-learned fault and security defensive mechanisms under smart grids is the apparent lack of comprehensive datasets relating to smart electrical grids that can provide both a large catalog and a set of characteristics defining the electrical grids. Smart grid [19] is associated with large volumes of data from many sources, such as power system operation, energy commodity markets (electricity markets, gas, and oil), the environment, and the weather. These data are distinguished by the variety of their sources, their growth rate, their spatial-temporal resolutions, and their enormous volume. The contributions of the paper, reflected in the released resources, are multi-fold:

- We investigate the impact of adversarial attacks against several key fault classification problems, and their combination on a widely used dataset based on the IEEE-13 test node feeder;
- We analyze adversarial attacks by examining multiple experimental situations with different adversarial goals;
- We release **IEEE13-AdvAttack** dataset, which is a large-scaled dataset that was created using the IEEE-13 test node feeder simulation and code for evaluating both unintentional (fault) and intentional (attack) security threats under SGs.

2 RELATED DATASETS

Under SGs, test grids that simulate the behavior of a real distribution feeder have been established in order to assess various three-phase grid algorithms. Modern test grids also permit the incorporation of renewable energy sources. Following is a list of the most common test grids found in the literature intended for distribution networks.

- **IEEE-13.** This circuit model is very small and used to test common features of distribution analysis software, operating at 4.16 kV. It is characterized by being short, relatively highly loaded, a single voltage regulator at the substation, overhead and underground lines, shunt capacitors, an in-line transformer, and unbalanced loading.
- **IEEE-14.** It represents a simple approximation of the American Electric Power system. It has 14 buses, five generators, and 11 loads.
- **IEEE-33.** It comprises both forms of balanced and unbalanced three-phase power systems, including new details on integrating distributed and renewable generation units, reactive power compensation assets, reconfiguration infrastructures, and appropriate datasets of load and renewable generation profiles for different case studies.
- **IEEE-123.** It operates at a nominal voltage of 4.16 kV. This circuit is described by overhead and underground lines, unbalanced loading with constant current, impedance, power, four voltage regulators, shunt capacitor banks, and switches.

In the electrical industry, a variety of simulation programs exist, which are described here with reference to the study that employed them to solve the problem of fault prediction, they include MATLAB Simulink [31], PSCAD [10, 20, 21], RSCAD [28], PSS/Sincal [2], Opal-RT [16], PST [22, 23], DIgSILENT [17, 24], MATPOWER [18].

To the best of our knowledge, none of the existing research studies have made an attempt to make simulation data from IEEE test node feeders publicly available, despite the widespread adoption of simulation tools for failure prediction systems in SGs. This is a substantial barrier to the development of machine-learned adversarial assaults and failure prediction systems. *To remedy this shortcoming, we construct a comprehensive dataset on smart electrical grids (based on the IEEE-13 test node feeder) that can give both a complete catalog and a set of attributes identifying the electrical networks.*

3 A DATASET FOR SMART-GRID MACHINE-LEARNED SECURITY

3.1 General information

The acquired data in this research is based on IEEE-13 test node feeder. Although other types of node feeders described in Section

2 may be utilized, for the sake of simplicity we selected for IEEE-13 and left the continuation of this work to other node feeders for future investigation. The IEEE-13 node test feeder consists of a 4.16 kVlt voltage generator, 13 buses for fault simulation and measurement of three-phase signals. One may split this distribution system into four crucial zones, zone 1: 632-671, zone 2: 632-633, zone 3: 692-675, and zone 4: 671-680 (refer to the Github repo for the network's schematic diagram).

3.2 Feature extraction and fault Simulation

We utilized the default parameters for the IEEE-13 test node feeder simulation in MATLAB, which included a voltage frequency of 60 Hz and a sample time of $10 - 5$. By inserting fault into the IEEE-13 node test feeder in the Simulink environment of MATLAB, we generated data. We injected 11 distinct fault types with 22 distinct resistances per fault type into the four critical zones next to load flow buses 671, 633, 675, and 680 (lines within the red boxes in Figure IEEE-13). This information is summarized in Table 1. A dataset composed of 11616 faulty samples was created in which 4 (zones)$\times$ 4 (measurement-zone) $\times$ 11 (faults) $\times$ 3 (phases) $\times$ 22 (resistance values) = 11616. For healthy data, we obtained raw healthy signals for 88 different line lengths by measuring from specified four zones and for three phases 88 (Line-length) $\times$ 4 (measurement-zone) $\times$ 3 (phases) = 1056.

Total duration for fault simulation was $t = [0.0 - 0.02]$ and each fault with every resistances were applied at $t = 0.01$ and revoked at $t = 0.02$, thus $t_f = [0.01 - 0.02]$ indicates the fault duration, whereas $t_h = [0 - 0.01]$ indicates the healthy (non-faulty) duration of time. In the GitHub link (shared in the abstract), we provide a Figure depicting the number of samples generated by simulation for both defective and healthy signals. In this study, we selected three types of features utilized in earlier research [1, 12, 26, 30, 32]:

- **Time-domain features.** It refers to the original data measured in time domain. Applying six aggregation functions to the voltage signal $x(t)$ produced a six-dimensional time domain feature vector. They include (mean, standard deviation, skewness, kurtosis) together with the energy and maximum level of the signals.
- **Frequency-domain features.** Voltage signals were also converted to the frequency domain using discrete Fourier transform. The same six aggregation functions used in the time domain were applied to the calculated spectrum to create a six-dimensional frequency-domain feature vector.
- **Discrete Wavelet transform (DWT)**. DWT analyzes digital signals at several resolutions. Multi-resolution analysis uses approximation A_i and detail D_i wavelet coefficients. Motivated by earlier works [1, 32], we utilized a high number of level-decompositions (five) according to A_5, $D_{1:5}$.

Overall, 48 features are extracted, including six time-domain features, six DFT features, and 36 DWT features (five stages of decomposition plus one level of approximation).

3.3 Dataset Structure

In terms of the dataset, the data files are organized in a specified arrangement for easier accessibility. The structure of the dataset is presented in the Github rep. As the main folder, We have a "DataSet-IEEE13-withRE" folder which contains two main sub-folders: (1) "RawTimeSeriesData" contains Raw voltage measurements for both faulty and healthy signals for three phases. (2) "FeatureData" folder that includes features from three domains: time, frequency (discrete Fourier transform DFT), and Discrete wavelet transform are extracted (DWT) for both faulty and healthy signals in three phases.

Table 1: The characteristic of the dataset used for classification and training the machine-learned adversarial attacks in this work.

Item	Details
Fault type	phase to ground AG, BG, CG phase to phase AB, AC, BC phase to phase to ground ABG, ACG, BCG three phase ABC three phase to ground ABCG
Fault location	zone 1 branch 632-671 zone 2 branch 632-633 zone 3 branch 692-675 zone 4 branch 671-680
Fault resistance	0.0010, 0.0273, 0.0535, 0.0798 0.1061, 0.1323 0.1586, 0.1848 0.2111, 0.2374, 0.2636, 0.2899 0.3162, 0.3424, 0.3687, 0.3949 0.4212, 0.4475, 0.4737, 0.5, 1, 2

4 BENCHMARKING

We trained a Multi-layer Perceptron (MLP) neural network for the three classification tasks stated in Section 4.1. An input layer, two dense layers, and an output layer compose the model. The number of neurons in this layer must correspond to the number of output classes in each task, making it the only layer to vary between the three tasks. The tasks require separate training phases, which all take place with the same settings, using 500 Epochs, Adam Optimizer, and fixed learning rate of 10e-3 with a batch-size of 20. The hyper-parameters were obtained after fine-tuning.

We utilized the IBM Adversarial Robustness Toolbox for adversarial attacks due to its complete compatibility with Keras and extensive selection of attacks suited for deep learning models. The employed attacks include FGSM and multi-step attacks (BIM, PGD), in both untargeted and targeted scenarios.

4.1 Fault Classification in Smart Grids

We consider different multi-class classification problems pertinent to fault prediction in smart grids with $K \geq 2$ classes in this paper, in which X is the input space and $y = \{1, 2, ..., K\}$ the output space. Our problem showcases two different target labels for the problems at hand (i) fault location and (ii) fault type. Therefore, the main task is split into three sub-tasks:

(1) Fault location classification (FLC): with $K = 4$ the task aims to classify a given signal into its originating zone as shown in Table 1.
(2) Fault type classification (FTC): with $K = 11$ the task aims to classify a given signal into one of predefined fault types as shown in Table 1.
(3) Joint location and type classification (FLC+FTC) $K = 44$ integrating the both fault class labels in the preceding cases;

Table 2: Result of application of adversarial attacks against fault classification tasks on the presented IEEE-13 dataset.

		Base	Random Noise	Adversarial Attack		
				FGSM	BIM	C&W
Attack goal			$\epsilon = 0.05$	$\epsilon = 0.05$	$\epsilon = 0.05$	
UnTargeted	FZC	0.71	0.556	0.160	0.154	0.281 (ℓ_∞)
UnTargeted	FTC	0.46	0.388	0.075	0.048	0.166 (ℓ_∞)
UnTargeted	Joint	0.45	0.320	0.086	0.023	0.139 (ℓ_∞)
Targeted	FZC	0.71	0.556	0.260	0.265	0.631 (ℓ_2)
Targeted	FTC	0.46	0.388	0.076	0.198	0.388 (ℓ_2)
Targeted	Joint	0.45	0.320	0.030	0.135	0.432 (ℓ_2)

where, (1) and (2) are explicitly contained in the dataset, while (3) is derived by combing each different possible combination of task 1 and task 2. Thus, we can state that the joint task is expected to be a more complex task compared to the former.

4.2 Adversarial Attacks against Fault Classification

The adversary is interested in mis-classifying smart-grid fault classification tasks in each of the three FZC, FTC, and joint sub-tasks through the use of two types of attacks: untargeted vs. targeted.

Adversary knowledge. Our assumption is *white-box* setting where the attacker knows all of the parameters of the feature extraction model used to estimate the perturbation he/she want to estimate. In addition, the attacker has full access to the input features that would be changed as result of the attack. The attacker can also obtain the class labels in targeted attack scenario.

Explored Attacks. The performed attacks consist of the fast gradient sign method (FGSM), basic iterative method (BIM), and Carlini and Wagner (C&W), which FGSM belong to ℓ_∞-norm and C&W belong to ℓ_∞-norm and ℓ_2-norm attack types. FGSM is a white-box attack that employs the sign of the loss function's gradient to learn adversarial perturbations and BIM is the iterative version of the FGSM. Formally, in the untargeted scenario, FGSM aims to generate a perturbation that maximizes the training loss formulated as

$$\delta = \epsilon \cdot \text{sign}(\nabla_x \ell(f(x;\theta), y)) \tag{1}$$

where ϵ (perturbation level) represents the attack strength and ∇_x is the gradient of the loss function w.r.t. input sample $\mathbf{x}$, y is the legitimate label and sign(.) is the sign operator.

The second category of adversarial tracks is Carlini and Wagner. It is a powerful attack model for finding adversarial perturbation under three various distance metrics (ℓ_0, ℓ_2, ℓ_∞). Its key insight is similar to L-BFGS as it transforms the constrained optimization problem into an empirically chosen loss function to form an unconstrained optimization problem as

$$\min_{\delta} \left(\|\delta\|_p^p + c \cdot h(\mathbf{x} + \delta, y_T) \right) \tag{2}$$

where $h(\cdot)$ is the candidate loss function. □

The C&W attack has been used with several norm-type constraints on perturbation ℓ_0, ℓ_2, ℓ_∞ among which the ℓ_2 and ℓ_∞ have been reported to be most effective, and we used in this work [9].

Discussion. In Table 2, we demonstrate the result of benchmarking two security-related scenarios, (i) fault classification, (ii) adversarial attack against fault classification system on the proposed dataset. Before an attack, **Base** displays the outcome of the pure classification system (FZC, FTC, or combined). As the complexity of the job increases from FZC to FTC and then to joint, the classification accuracy can be shown to decrease. We compare the effectiveness of adversarial perturbations generated by different adversarial attack methods (FGSM, BIM, and C&W) compared to random noise. Additionally we consider the performance of attacks change when we alternate between the **attack targets**. As shown in Table 2, the analyzed adversarial attacks FGSM, BIM, and C&W have a much greater impact in untargated scenarios.

For instance, comparing the strength of the three adversarial attack models, BIM is the strongest in all tasks. In the case of (untargeted, Joint), BIM untargeted adversarial attack accuracy reaches 0.023, whilst FGSM and C&W reach 0.086 and 0.139, respectively, under the same condition. The effect of attack target (targeted vs. untargeted) is stronger on BIM and C&W than on FSGM. For example, for the (FTC), the classification accuracy of 0.048 vs. 0.198 (BIM-untrg vs. BIM-trg), however for FGSM the corresponding difference is only 0.075 vs. 0.076 (FGSM-untrg vs. FGSM-trg).

5 CONCLUSIONS

In this study, we studied the security and vulnerability of fault classification systems driven in the context of smart electrical grids by simulating IEEE-13 test feeders with renewable energy and generating corresponding data. We released **IEEE13-AdvAttack**, a large-scale simulated dataset based on the IEEE-13 test node feeder that is suitable for supervised fault classification tasks under SG, for the first time. Traditional and renewable energy sources are represented in the dataset. We examine the resistance of fault type classification and fault zone classification systems to hostile assaults. To defend these systems against alternative adversarial training and detection techniques would require more nuanced and in-depth research, which we hope to pursue in future work. Another interesting future direction consider the privacy of fault-prediction systems such that separate zones do not need to exchange their data with a central server. This could be accomplished via multi-party computation techniques, such as a federated learning solution that trains a privacy-by-design failure prediction solution [4, 5].

ACKNOWLEDGMENTS

This work has been partially funded by *e-distribuzione S.p.A* company, Italy, through a PhD scholarship granted to Fatemeh Nazary.

REFERENCES

[1] Tamer S. Abdelgayed, Walid G. Morsi, and Tarlochan S. Sidhu. 2018. A New Harmony Search Approach for Optimal Wavelets Applied to Fault Classification. *IEEE Trans. Smart Grid* 9, 2 (2018), 521–529. https://doi.org/10.1109/TSG.2016.2555141

[2] Shaik Affijulla and Praveen Tripathy. 2018. A Robust Fault Detection and Discrimination Technique for Transmission Lines. *IEEE Trans. Smart Grid* 9, 6 (2018), 6348–6358.

[3] Vito Walter Anelli, Yashar Deldjoo, Tommaso DiNoia, and Felice Antonio Merra. 2022. Adversarial recommender systems: Attack, defense, and advances. In *Recommender systems handbook*. Springer, 335–379.

[4] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Antonio Ferrara. 2019. Towards effective device-aware federated learning. In *International Conference of the Italian Association for Artificial Intelligence*. Springer, 477–491.

[5] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Antonio Ferrara. 2020. Prioritized multi-criteria federated learning. *Intelligenza Artificiale* 14, 2 (2020), 183–200. https://doi.org/10.3233/IA-200054

[6] Carmelo Ardito, Yashar Deldjoo, Tommaso Di Noia, Eugenio Di Sciascio, and Fatemeh Nazary. 2022. Visual inspection of fault type and zone prediction in electrical grids using interpretable spectrogram-based CNN modeling. *Expert Systems with Applications* (2022), 118368.

[7] Carmelo Ardito, Yashar Deldjoo, Eugenio Di Sciascio, and Fatemeh Nazary. 2021. Revisiting Security Threat on Smart Grids: Accurate and Interpretable Fault Location Prediction and Type Classification. In *Proceedings of the Italian Conference on Cybersecurity, ITASEC 2021, All Digital Event, April 7-9, 2021 (CEUR Workshop Proceedings, Vol. 2940)*, Alessandro Armando and Michele Colajanni (Eds.). CEUR-WS.org, 523–533. http://ceur-ws.org/Vol-2940/paper44.pdf

[8] Carmelo Ardito, Yashar Deldjoo, Eugenio Di Sciascio, Fatemeh Nazary, and Gianluca Sapienza. 2021. ISCADA: Towards a Framework for Interpretable Fault Prediction in Smart Electrical Grids. In *Human-Computer Interaction - INTERACT 2021 - 18th IFIP TC 13 International Conference, Bari, Italy, August 30 - September 3, 2021, Proceedings, Part V (Lecture Notes in Computer Science, Vol. 12936)*. Springer, 270–274. https://doi.org/10.1007/978-3-030-85607-6_20

[9] Nicholas Carlini and David A. Wagner. 2016. Defensive Distillation is Not Robust to Adversarial Examples. *CoRR* abs/1607.04311 (2016). arXiv:1607.04311 http://arxiv.org/abs/1607.04311

[10] Soham Chakraborty and Sarasij Das. 2019. Application of Smart Meters in High Impedance Fault Detection on Distribution Systems. *IEEE Trans. Smart Grid* 10, 3 (2019), 3465–3473.

[11] Lei Cui, Youyang Qu, Longxiang Gao, Gang Xie, and Shui Yu. 2020. Detecting false data attacks using machine learning techniques in smart grid: A survey. *J. Netw. Comput. Appl.* 170 (2020), 102808. https://doi.org/10.1016/j.jnca.2020.102808

[12] Qiushi Cui and Yang Weng. 2020. Enhance High Impedance Fault Detection and Location Accuracy via μ-PMUs. *IEEE Trans. Smart Grid* 11, 1 (2020), 797–809.

[13] Swagata Das, Sundaravaradan Navalpakkam Ananthan, and Surya Santoso. 2019. Estimating Zero-Sequence Line Impedance and Fault Resistance Using Relay Data. *IEEE Trans. Smart Grid* 10, 2 (2019), 1637–1645.

[14] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. 2021. A survey on adversarial recommender systems: from attack/defense strategies to generative adversarial networks. *ACM Computing Surveys (CSUR)* 54, 2 (2021), 1–38.

[15] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. 2016. A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers. *IEEE Trans. Inf. Forensics Secur.* 11, 10 (2016), 2174–2186. https://doi.org/10.1109/TIFS.2016.2578285

[16] Mostafa Gilanifar, Jose Cordova, Hui Wang, Matthias Stifter, Eren Erman Ozguven, Thomas I. Strasser, and Reza Arghandeh. 2020. Multi-Task Logistic Low-Ranked Dirty Model for Fault Detection in Power Distribution System. *IEEE Trans. Smart Grid* 11, 1 (2020), 786–796.

[17] Sayyed Mohammad Hashemi, Majid Sanaye-Pasand, and Mohammad Shahidehpour. 2019. Fault Detection During Power Swings Using the Properties of Fundamental Frequency Phasors. *IEEE Trans. Smart Grid* 10, 2 (2019), 1385–1394.

[18] Miao He and Junshan Zhang. 2011. A Dependency Graph Approach for Fault Detection and Localization Towards Secure Smart Grid. *IEEE Trans. Smart Grid* 2, 2 (2011), 342–351.

[19] Muhammad Sohail Ibrahim, Wei Dong, and Qiang Yang. 2020. Machine learning driven smart electric power systems: Current trends and new perspectives. *Applied Energy* 272 (2020), 115237.

[20] Huaiguang Jiang, Xiaoxiao Dai, David Wenzhong Gao, Jun Jason Zhang, Yingchen Zhang, and Eduard Muljadi. 2016. Spatial-Temporal Synchrophasor Data Characterization and Analytics in Smart Grid Fault Detection, Identification, and Impact Causal Analysis. *IEEE Trans. Smart Grid* 7, 5 (2016), 2525–2536.

[21] Huaiguang Jiang, Jun Jason Zhang, David Wenzhong Gao, and Ziping Wu. 2014. Fault Detection, Identification, and Location in Smart Grid Based on Data-Driven Computational Methods. *IEEE Trans. Smart Grid* 5, 6 (2014), 2947–2956.

[22] Iman Kiaei and Saeed Lotfifard. 2019. A Two-Stage Fault Location Identification Method in Multiarea Power Grids Using Heterogeneous Types of Data. *IEEE Trans. Ind. Informatics* 15, 7 (2019), 4010–4020.

[23] Wenting Li, Deepjyoti Deka, Michael Chertkov, and Meng Wang. 2019. Real-time faulted line localization and pmu placement in power systems through convolutional neural networks. *IEEE Transactions on Power Systems* 34, 6 (2019), 4640–4651.

[24] Mehrdad Majidi, Mehdi Etezadi-Amoli, and Mohammed Sami Fadali. 2017. A Sparse-Data-Driven Approach for Fault Location in Transmission Networks. *IEEE Trans. Smart Grid* 8, 2 (2017), 548–556.

[25] Ijeoma Onyeji, Morgan Bazilian, and Chris Bronk. 2014. Cyber security and critical energy infrastructure. *The Electricity Journal* 27, 2 (2014), 52–60.

[26] Evandro Agostinho Reche, Jeovane Vicente de Sousa, Denis Vinicius Coury, and Ricardo A. S. Fernandes. 2019. Data Mining-Based Method to Reduce Multiple Estimation for Fault Location in Radial Distribution Systems. *IEEE Trans. Smart Grid* 10, 4 (2019), 3612–3619. https://doi.org/10.1109/TSG.2018.2832840

[27] Nikolaos Sapountzoglou, Jesus Lago, Bart De Schutter, and Bertrand Raison. 2020. A generalizable and sensor-independent deep learning method for fault detection and location in low-voltage distribution grids. *Applied Energy* 276 (2020), 115299.

[28] Md Shafiullah and M. A. Abido. 2018. S-Transform Based FFNN Approach for Distribution Grids Fault Detection and Classification. *IEEE Access* 6 (2018), 8080–8088.

[29] Shenxing Shi, Beier Zhu, Sohrab Mirsaeidi, and Xinzhou Dong. 2019. Fault Classification for Transmission Lines Based on Group Sparse Representation. *IEEE Trans. Smart Grid* 10, 4 (2019), 4673–4682. https://doi.org/10.1109/TSG.2018.2866487

[30] Veerapandiyan Veerasamy, Noor Izzri Abdul Wahab, Rajeswari Ramachandran, Mariammal Thirumeni, Chitra Subramanian, Mohammad Lutfi Othman, and Hashim Hizam. 2019. High-impedance fault detection in medium-voltage distribution network using computational intelligence-based classifiers. *Neural Comput. Appl.* 31, 12 (2019), 9127–9143.

[31] Xiaowei Wang, Jie Gao, Xiangxiang Wei, Guobing Song, Lei Wu, Jingwei Liu, Zhihui Zeng, and Mostafa Kheshti. 2019. High Impedance Fault Detection Method Based on Variational Mode Decomposition and Teager-Kaiser Energy Operators for Distribution Network. *IEEE Trans. Smart Grid* 10, 6 (2019), 6041–6054.

[32] James Jian Qiao Yu, Yunhe Hou, Albert Y. S. Lam, and Victor O. K. Li. 2019. Intelligent Fault Detection Scheme for Microgrids With Wavelet-Based Deep Neural Networks. *IEEE Trans. Smart Grid* 10, 2 (2019), 1694–1703. https://doi.org/10.1109/TSG.2017.2776310

[33] Alireza Zarreh, HungDa Wan, Yooneun Lee, Can Saygin, and Rafid Al Janahi. 2019. Risk assessment for cyber security of manufacturing systems: A game theory approach. *Procedia Manufacturing* 38 (2019), 605–612.