Machine Learning in Generation, Detection, and Mitigation of Cyberattacks in Smart Grid: A Survey

Nur Imtiazul Haque, Md Hasan Shahriar, Md Golam Dastgir, Anjan Debnath, Imtiaz Parvez, Arif Sarwat, Mohammad Ashiqur Rahman
Department of Electrical and Computer Engineering
Florida International University, Miami, USA
{nhaqu004, mshah068, mdast001, adebn001, iparv001, asarwat, marahman}@fiu.edu

Abstract—Smart grid (SG) is a complex cyber-physical system that utilizes modern cyber and physical equipment to run at an optimal operating point. Cyberattacks are the principal threats confronting the usage and advancement of the state-of-the-art systems. The advancement of SG has added a wide range of technologies, equipment, and tools to make the system more reliable, efficient, and cost-effective. Despite attaining these goals, the threat space for the adversarial attacks has also been expanded because of the extensive implementation of the cyber networks. Due to the promising computational and reasoning capability, machine learning (ML) is being used to exploit and defend the cyberattacks in SG by the attackers and system operators, respectively. In this paper, we perform a comprehensive summary of cyberattacks generation, detection, and mitigation schemes by reviewing state-of-the-art research in the SG domain. Additionally, we have summarized the current research in a structured way using tabular format. We also present the shortcomings of the existing works and possible future research direction based on our investigation.

Index Terms—Cyber-physical systems; cyberattacks; smart grid; anomaly detection system; machine learning.

I. INTRODUCTION

In the modern power system, a vast amount of intelligent devices form a cyber network to monitor, control, and protect the physical network. The cyber-physical (CP) networks’ interdependency is the backbone of the modern smart grid (SG). Fig. 1 illustrates the typical multi-layer architecture of SG, composed of physical, data acquisition, communication, and application layers. The physical layer consists of generation, transmission, and distribution networks [1]–[3]. SG incorporates distributed energy resources (DERs) such as solar, wind, hydro, etc., connected to the grid with converters for extracting maximum power [4]–[7]. The data acquisition layer consists of smart sensors and measurement devices, where the smart devices collect data and transmit them to the communication layer. The communication layer includes a wide variety of wired/wireless technologies and network devices, which transmits data to the energy management system (EMS) that optimizes, monitors, and sends control signals to the actuators.

Though the cyber layers improve the efficiency of the SG, they might put the system at higher risk by expanding the attack space. An attacker can compromise the vulnerable points, disrupting the monitoring and controlling of the physical equipment [8]–[11]. Additionally, demand response, energy efficiency, dynamic electricity market, distributed automation, etc. are the key features of the SG network [12]–[14]. All these salient features nominate the SG, a very complex network. Machine learning (ML) is a ubiquitous prominent tool with capability of extracting patterns in any complex network data without being explicitly programmed. Recently, a lot of researchers are using ML to analyze the cybersecurity of SG.
TABLE I
CLASSIFICATION OF ML-BASED ATTACK GENERATION TECHNIQUES IN SMART GRID

| Reference       | Institution                 | Year | Attack Type       | Attack Goal                     | Category         | ML Algorithm | Performance       | Testbed            |
|-----------------|-----------------------------|------|-------------------|---------------------------------|------------------|---------------|------------------|--------------------|
| Paul et al. [15]| South Dakota State University, USA | 2019 | Line Switching    | Generation loss, Line outage    | Unsupervised     | K-means       | Line outage-63, Generation loss-12029 MW | W&W 6, IEEE 7, 8, 300 bus |
| Ni et al. [16]  | South Dakota State University, USA | 2019 | Line Switching    | Optimal Multistage Attack Sequence for Line outage | Reinforcement     | Q-learning     | Line outage-50%, Generation loss-60% | W&W 6 bus and IEEE 39 bus |
| Ni et al. [17]  | South Dakota State University, USA | 2017 | Line Switching    | Optimal Attack Sequence for Blackout | Reinforcement     | Q-learning     | Generation loss-160.1278 MW and blackout | W&W 6 bus and IEEE 30 bus |
| Yan et al. [18] | University of Rhode Island, USA | 2016 | Line Switching    | Optimal Attack Sequence for Blackout | Reinforcement     | Q-learning     | Voltage sag- 0.5 pu | IEEE 39 bus |
| Chen et al. [19]| Tsinghua University, China   | 2019 | Line Switching    | Disrupt Automatic Voltage Control | Reinforcement     | Q-learning     | Voltage sag- 0.5 pu | IEEE 39 bus |
| Ahmadian et al. [20]| University of Houston, USA    | 2018 | Line Switching    | Maximize Cost                   | Unsupervised     | GAN           | Generated fake load data | IEEE 5 bus |
| Nawaz et al. [21]| Air University, Pakistan     | 2018 | Line Switching    | State Estimation                | Supervised       | LR            | Generated stealthy FDI attack vectors | IEEE 5 bus |

attack in the SG. K-means and Q-learning algorithms are used to launch the line switching attacks. In contrast, Q-learning, generative adversarial networks (GAN), and linear regression (LR) models are used to generate false data injection (FDI) attacks.

Paul et al. used load ranking and K-means clustering algorithms as two different approaches to attack SG for selecting the most vulnerable transmission lines to create contingencies [15]. They found that clustering-based algorithms perform better in tripping transmission lines. On the other hand, load ranking shows better results to gain higher generation loss. In [18], Yan et al. proposed Q-learning-based cyberattacks in different buses of the system that leads the system to blackout. Ni et al. proposed another reinforcement learning-based sequential line switching attack to initiate blackout [17]. They recently proposed a multistage game using a Q-learning algorithm to create transmission line outage and generation loss [16]. Nawaz et al. proposed an LR-based FDI attack generator against the state estimation of the SG. They implemented and evaluated their model on IEEE 5 bus system [21]. Ahmadian et al. presented a GAN-based false load data generator in [20]. The attacker’s goal was to maximize the generation cost by injecting that false load data into the system. Recently, Chen et al. also presented a Q-learning-based FDI attack generator against the automatic voltage control using partially observable Markov decision process and was able to create a voltage sag on IEEE 39 bus system [24].

III. MACHINE LEARNING BASED ATTACK DETECTION

A wide range of research has been conducted to detect various attacks in SG leveraging ML approaches. In this section, we review the existing research efforts of ML-based attack detection in various segments of the SG, as summarized in Table II. In the following subsections, we discuss the detection techniques of a few prevalent cyberattacks.

A. False Data Injection Attack

Most of the research efforts attempted to detect stealthy FDI attacks using ML. Esmalifalak et al. attempted to detect stealthy FDI attacks using a support vector machine (SVM)-based technique and a statistical anomaly detection approach [25]. They showed that SVM outperforms the statistical approach when the model is trained with sufficient data. He et al. proposed a conditional deep belief network (CDBN)-based detection scheme that extracts temporal features from distributed sensor measurements [34]. The proposed detection scheme is robust against various attacked measurements and environmental noise levels. Moreover, it can perform better than SVM and artificial neural network (ANN)-based detection mechanisms. Karimipour et al. proposed a continuous, computationally efficient, and independent mechanism using feature extraction scheme and time series partitioning method to detect FDI attacks [36]. This paper used dynamic bayesian networks (DBsN) concept and Boltzmann machine-based learning algorithms to detect unobservable attacks. Valdes et al. presented a novel intrusion detection system (IDS) utilizing adaptive resonance theory (ART) and self-organizing maps (SOM) to differentiate normal, fault, and attack states in a distribution substation system [46]. Yan et al. viewed the FDI attack detection problem as a binary classification problem and attempted to solve it using three different algorithms: SVM, K-nearest neighbor (KNN), and extended nearest neighbor (ENN) [26]. Their experimental analysis showed that all these algorithms could be tuned to attain optimal performance against FDI attack detection. Ayad et al. examined the use of a recurrent neural network (RNN)-based method that deals with temporal and spatial correlations between the measurements, unlike other learning methods, to recognize FDI attacks in SG [44]. Niu et al. presented a deep learning-based framework combining a convolutional neural network (CNN) and a long short term memory (LSTM) network to detect novel FDI attacks [45]. Sakhinni et al. analyzed three different algorithms (e.g., ANN, KNN, and SVM) that incorporate different feature selection (FS) techniques and used a genetic algorithm (GA) as optimal FS method for power systems. The authors of [43] proposed a nonlinear autoregressive exogenous (NARX) neural networks to estimate DC current and voltage to detect
| Category | ML Algorithm | Attack | Number of Features | Data Collection | Testbed | Performance | Reference |
|----------|--------------|--------|--------------------|----------------|---------|------------|-----------|
| SVM      | FDI          | 304    | MATPOWER simulation tool | IEEE 118 bus | 99% accuracy | [25] |
|          | NA           | NA     | MATPOWER simulation tool | IEEE 30 bus | 96.1% accuracy | [26] |
|          | IL           | 34     | MATPOWER simulation tool | IEEE 14 bus | 90.79% accuracy | [27] |
|          | CC           | 233    | SE-MF datasets | IEEE 14, 39-, 57- and 118-bus systems | 99.954% accuracy and 0.939 F1-score | [29] |
|          | DoS, R2L, and U2R | NA | NSL-KDD dataset | NA | 0.67% TPR and 2.15% FNR | [30] |
| KNN      | FDI          | 34     | MATPOWER simulation tool | IEEE 14 bus | 85.59% accuracy | [27] |
|          | CC           | 233    | SE-MF datasets | IEEE 14, 39-, 57- and 118-bus systems | 77.234% accuracy | [29] |
| ENN      | FDI          | NA     | NA | IEEE 30 bus | 100% accuracy | [26] |
|          | DoS          | 2      | N/A | N/A | 100% | [32] |
|          | DoS/DDoS     | 80     | CIC-IDS2017 dataset | NA | 99.9% accuracy | [31] |
|          | CDB/N        | FDI    | NA | MATPOWER simulation tool | IEEE 118, 300 bus | 98% accuracy | [34] |
|          | CC           | 233    | SE-MF datasets | IEEE 14, 39-, 57- and 118-bus systems | 90% accuracy | [38] |
|          | XGBBoost     | XNS, SQLI, DDoS, PS, etc. | 71 | CIC-IDS2018 dataset | NA | 99.8% precision and 99.75% recall | [39] |
|          | DT           | ET     | NA | NA | 92.5% accuracy | [40] |
|          | Adaboost     | CC     | NA | NA | 92.5% accuracy | [40] |
|          | AIRS         | DoS, R2L, U2R, and PA | NA | NSL-KDD dataset | NA | 1.3% FPR, and 26.32% FNR | [30] |
|          | Multi-SVM    | DoS    | NA | N/A | 90% accuracy | [41] |
|          | Autoencoder ANN | FDI | 339 | NA | IEEE 118 bus | 95.05% accuracy | [42] |
|          | NARX ANN     | FDL    | NA | OPAL-RF simulator | DC microgrid system | 95.05% accuracy | [43] |
| RNN      | FDI          | 112    | MATPOWER simulation tool | IEEE 30 bus | 99% accuracy, 91.529% precision, and 85.02% recall | [44] |
|          | Statistical  | FDI    | 304 | MATPOWER simulation tool | IEEE 118 bus | 99% accuracy | [25] |
|          | ART and SOM based classifier (Novel) | FDI | 24 | Real-time digital Simulator(RTDS) | RTDS hardware in the loop testbed | 90% accuracy | [46] |
|          | CLONALG      | DoS, R2L, U2R | NA | NSL-KDD dataset | NA | 0.8% FPR and 21.02% FNR | [30] |
|          | iForest      | CC     | 233 | SE-MF datasets | IEEE 14, 39-, 57- and 118-bus systems | 90% accuracy | [47] |

FDI attacks in DC microgrid and showed that the proposed method has successfully identified FDI attacks during transient and steady-state conditions. The autoencoder ANN-based FDI attack detection mechanism has also been investigated by Wang et al. [42].

**B. Covert Cyber Attack**

Ahmed et al. tried to detect covert cyber (CC) attacks in their several research efforts. In one of their works, they proposed two euclidean distance-based abnormality recognition scheme for detecting anomalies in the state estimation measurement features (SE-MF) dataset [38]. In their another work, they leveraged several ML methods (KNN, SVM, multi-layer perceptron (MLP), naïve bayes (NB), and adaboost) to identify a CC attack in the SE information that is gathered through a communication network of smart grid [29] along with a GA for optimizing the features. Their discovery revealed that KNN has low CC attack detection performance than the other ML methods. They also proposed an unsupervised
ML-based mechanism utilizing a state-of-the-art algorithm, called isolation forest (iForest) to distinguish CC attacks in SG systems using non-labeled information. The proposed mechanism can sensibly improve detection performance in the periodic operational condition [47].

C. Electricity Theft

Energy Theft (ET) detection in SG mostly leverages supervised ML algorithms. Ford et al. examined a novel utilization of ANN and smart meter fine-grained information to report energy fraud, accomplishing a higher energy theft detection rate [35]. Jindal et al. proposed an extensive top-down scheme utilizing a decision tree (DT) and SVM. In contrast to other works, the proposed scheme is sufficiently proficient in accurately distinguishing and detecting constant power theft at each level in the power transmission system [40].

D. Denial of Service Attack

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack detection has got a significant research focus. Vijayanand et al. proposed a novel DoS attack detection framework utilizing diverse multi-layer deep learning algorithms for precisely identifying the attacks by analyzing smart meter traffic [37]. In another work, they have used another novel approach named as multi-SVM for DoS attack detection [41]. Zhang et al. attempted to detect anomalies in diverse layer network structure using SVM, clonal selection algorithm (CLONALG), and artificial immune recognition system (AIRS). According to their performance analysis, SVM based IDS outperforms CLONALG and AIRS [30]. Radoglou et al. proposed a novel IDS for AMI using DT [31]. Boumkheld et al. proposed an NB classifier based centralized IDS for accumulating all information sent by data collector that requires massive memory and computational resources. Roy et al. used extreme gradient boosting (XGBoost), random forest (RF) on CIC-IDS2018 dataset for detecting various SG cyberattacks, including DoS [39].

Moreover, the ML-based detection of cross-site scripting (XSS) and SQL injection (SQLI), unknown routing attack (URA), brute force (BF), information leakage (IL), port scanning (PS), remote to local (R2L), the user to root (U2R) attacks also gained some attention in the recent research.

IV. MACHINE LEARNING BASED ATTACK MITIGATION

Attack mitigation is the strategy to minimize the effect of malicious attacks maintaining the functionality of the system. Table III summarizes the ML-based attack mitigation in SG.

Wei et al. proposed a deep belief network (DBfN)-based cyber-physical model to identify and mitigate the FDI attack while maintaining the transient stability of wide-area monitoring systems (WAMSs) [49]. An et al. modeled a deep-Q-network (DQN) detection scheme to defend against data integrity attacks (DIA) in AC power systems [50] and showed that the DQN detection outperforms the baseline schemes in terms of detection accuracy and rapidity. Chen et al. presented a Q-learning-based mitigation technique for FDI attacks in automatic voltage controller [24]. They replaced the suspected data with their maximum likelihood estimation (MLE) values to enhance the securities of the state estimation and OPF-based controls. In [52], Maharjan et al. proposed an SVM based resilient SG network with DERs to mitigate the data unavailability attack (DUA). Parvez et al. proposed a localization-based key management system using the KNN algorithm for node/meter authentication in AMI networks [51]. They showed that the source meter could be authenticated accurately by the KNN algorithm utilizing the pattern of sending frequency, packet size, and distance between two meters. Ren et al. proposed a GAN model that predicts the missing/unavailable PMU data even without observability and network topology [53]. Shahriar et al. proposed a GAN-based approach to generate a synthetic attack dataset from the existing attack data. They achieved up to 91% f1 score in detecting different cyberattacks for the emerging smart grid technologies [54]. In another work, Ying et al. proposed a similar GAN-based approach achieving a 4% increase in the attack detection accuracy [55]. Li et al. proposed another GAN based model to defend against FDI attacks [48] that provides the predicted deviation of the measurements and recovers the compromised sensors.
V. FUTURE RESEARCH DIRECTION

Fig. 2 shows the pie-chart of ML techniques used in attack generation, detection, and mitigation for the SG network. Fig. 2(b) illustrates that a lot of research have been conducted towards the application of different ML algorithms in attack-detection, whereas, generation and mitigation fields are comparatively less explored. As SG is dynamic and intermittent in nature, researchers are mostly applying Q-learning to generate real-time attacks, as shown in Fig. 2(a). On the other hand, GAN has the capability of generating missing data with considerable accuracy, thus, as shown in Fig. 2(c), it is prominently used in attack mitigation strategies. However, GAN also has the potential to generate attack data considering the system’s topology and states. Hence, future researchers can focus on GAN and the other less explored algorithms such as ANN, RNN, KNN, DT, etc. in the attack generation and mitigation strategies.

VI. CONCLUSION

ML has been creating new dimensions for both attackers and defenders with respect to scalability and accuracy due to its wide range of applications in SG. Therefore, it draws attention to the researchers for conducting security-related investigations applying emerging ML algorithms. In this paper, we review current research works, related to the potential ML-based attack generation, detection, and mitigation schemes for future researchers. In addition, we present a tabular form summarizing the existing studies in an organized way that would help future researchers to emphasize the unfocused areas.

VII. ACKNOWLEDGEMENT

This research was supported in part by the U.S. National Science Foundation under awards #1553494 and #1929183.

REFERENCES

[1] Anjan Debnath, Temitayo O Olowu, Imitiaz Parvez, Md Golam Dastgir, and Arif Sarwat. A novel module independent straight-line-based fast maximum power point tracking algorithm for photovoltaic systems. *Energies*, 13(12):3233, 2020.

[2] Chitta Ranjan Saha, M Nazmul Huda, Asim Mumtaz, Anjan Debnath, Sanju Thomas, and Robert Jinks. Photovoltaic (pv) and thermo-electric energy harvesters for charging applications. *Microelectronics Journal*, 96:104685, 2020.

[3] Mohamadsaleh Jafari, Temitayo O Olowu, Arif I Sarwat, and Mohammad Ashiqur Rahman. Study of smart grid protection challenges with high photovoltaic penetration. In *2019 North American Power Symposium (NAPS)*, pages 1–6. IEEE, 2019.

[4] Anjan Debnath, Sukanta Roy, M Nazmul Huda, and M Ziaur Rahman Khan. Fast maximum power point tracker for photovoltaic arrays. In *2012 7th International Conference on Electrical and Computer Engineering*, pages 912–915. IEEE, 2012.

[5] N. Akbar, M. Islam, S. S. Ahmed, and A. A. Hye. Dynamic model of battery charging. In *TENCON 2015 - 2015 IEEE Region 10 Conference*, pages 1–4, Nov 2015.

[6] Anjan Debnath, Imitiaz Parvez, Md Golam Dastgir, Asim Nabi, Temitayo Olowu, Hugo Riggis, and Arif Sarwat. Voltage regulation of photovoltaic system with varying loads. In *IEEE SoutheastCon, Raleigh,NC, USA, 12–15 March*, pages 1–7, 2020.

[7] Md Hasan Shahriar, Md Jawwad Sadiq, and Md Forkan Uddin. Stability analysis of grid connected pv array under maximum power point tracking. In *2016 9th International Conference on Electrical and Computer Engineering (ICECE)*, pages 499–502. IEEE, 2016.

[8] Anibal Sanj, Walid Saad, Ismail Guvenc, Arif Sarwat, and Soroj Biswas. Smart grid security: Threats, challenges, and solutions. *arXiv preprint arXiv:1606.06992*, 2016.

[9] AKM Iqtiidar Newaz, Amit Kumar Sikder, Mohammad Ashiqur Rahman, and A Selcuk Uluagac. Healthguard: A machine learning-based security framework for smart healthcare systems. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, pages 389–396. IEEE, 2019.

[10] AKM Iqtiidar Newaz, Amit Kumar Sikder, Leonardo Babun, and A Selcuk Uluagac. Heka: A novel intrusion detection system for attacks to personal medical devices. In *2020 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2020.

[11] Mohammad Ashiqur Rahman, Md Hasan Shahriar, Mohamadsaleh Jafari, and Rahat Masum. Novel attacks against contingency analysis in power grids. *arXiv preprint arXiv:1911.00928*, 2019.

[12] Muhammad Faheem, Syed Bilal Hussain Shah, Rizwan Aslam Butt, Basit Raza, Muhammad Anwar, Muhammad Waqar Ashraf, Md A Nadi, and Vehbi C Gunog. Smart grid communication and information technologies in the perspective of industry 4.0: Opportunities and challenges. *Computer Science Review*, 30:1–30, 2018.

[13] Imitiaz Parvez, Arif Sarwat, Anjan Debnath, Temitayo Olowu, and Md Golam Dastgir. Multi-layer perceptron based photovoltaic forecasting for rooftop pv applications in smart grid. In *IEEE SoutheastCon, Raleigh,NC, USA, 12–15 March*, pages 1–6, 2020.

[14] M Ashiqur Rahman, Md Hasan Shahriar, and Rahat Masum. False data injection attacks against contingency analysis in power grids: Poster. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 343–344, 2019.

[15] Shuva Paul, Md Rashidul Haq, Avijit Das, and Zhen Ni. A comparative study of smart grid security based on unsupervised learning and load ranking. In *2019 IEEE International Conference on Electro Information Technology (EIT)*, pages 310–315. IEEE, 2019.

[16] Zhen Ni and Shuva Paul. A multistage game in smart grid security: A reinforcement learning solution. *IEEE transactions on neural networks and learning systems*, 30(9):2684–2695, 2019.

[17] Zhen Ni, Shuva Paul, Xiangnan Zhong, and Qinglai Wei. A reinforcement learning approach for sequential decision-making process of attacks in smart grid. In *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1–8. IEEE, 2017.
Saeed Ahmadian, Heidar Malki, and Zhu Han. Cyber attacks on smart grids using generative adversarial networks. In 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP), pages 942–946. IEEE, 2018.

Rehan Nawaz, Muhammad Awais Shahid, Ijaz Mansoor Qureshi, and Rehaman Habib Mehlood. Machine learning based false data injection in smart grid. In 2018 1st International Conference on Power, Energy and Smart Grid (ICPESG), pages 1–6. IEEE, 2018.

Ahmed S Musleh, Guo Chen, and Zhao Yang Dong. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Transactions on Smart Grid, 11(3):2218–2234, 2020.

Eklas Hossain, Intiijh Khan, Fuad Un-Noor, Sarder Shazali Sikander, and Md Samiul Haque Sunny. Application of big data and machine learning in smart grid, and associated security concerns: A review. IEEE Access, 7:130–13888, 2019.

Ying Chen, Shaowei Huang, Feng Liu, Zhisheng Wang, and Xinwei Sun. Evaluation of reinforcement learning-based false data injection attack to automatic voltage control. IEEE Transactions on Smart Grid, 10(2):218–2169, 2018.

Mohammad Esmaillalak, Lanchao Liu, Nam Nguyen, Rong Zheng, and Zhu Han. Detecting stealthy false data injection using machine learning in smart grid. IEEE Systems Journal, 11(3):1644–1652, 2017.

Jun Yan, Bo Tang, and Haibo He. Detection of false data attacks in smart grid with supervised learning. In 2016 International Joint Conference on Neural Networks (IJCNN), pages 1395–1402. IEEE, 2016.

Jacob Sakhnini, Hadis Karimipour, and Ali Dehghantanha. Smart grid cyber attacks detection using supervised learning and heuristic feature selection. In 2018 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), pages 108–112. IEEE, 2019.

Cengiz Kaygusuz, Leonardo Babun, Hidayet Aksu, and A Selcuk Ulugac. Detection of compromised smart grid devices with machine learning and convolution techniques. In 2018 IEEE International Conference on Communications (ICC), pages 1–6. IEEE, 2018.

Saeed Ahmed, YoungDoo Lee, Seung-Ho Hyun, and Insoo Koo. Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning. IEEE Access, 6:27518–27529, 2018.

Yichi Zhang, Lingfeng Wang, Weiqing Wang, Robert C Green II, and Yuancheng Li, Yuanyuan Wang, and Shiyan Hu. Online generative adversarial networks for power grid with supervised learning. In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pages 790–793. IEEE, 2019.

Xiangyu Niu, Jiayi Niu, Jinjuan Sun, and Kevin Tomson. Dynamic detection of false data injection attack in smart grid using deep learning. In 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pages 1–5. IEEE, 2019.

Alfonso Valdes, Richard Macwan, and Matthew Backes. Anomaly detection in electrical substation circuits via unsupervised machine learning. In 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), pages 500–505. IEEE, 2016.

Saeed Ahmed, YoungDoo Lee, Seung-Ho Hyun, and Insoo Koo. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. IEEE Transactions on Industrial Informatics, 14(10):2765–2777, 2019.

Dou An, Qingsong Peng, Chenyang Yang, and Shiyuan Hu. Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach. IEEE Transactions on Industrial Informatics, 16(3):2031–2043, 2019.

Chenguang Wang, Simon Tindemans, Kaikai Pan, and Peter Palensky. Detection of false data injection attacks using the autoencoder approach. arXiv preprint arXiv:2003.02229, 2020.

Chengwei Wang, Simon Tindemans, Kaikai Pan, and Peter Palensky. Detection of false data injection attacks using the autoencoder approach. arXiv preprint arXiv:2003.02229, 2020.

Gautham Prasad, Yinjia Huo, Lutz Lampe, and Victor CM Leung. Machine learning based physical-layer intrusion detection and location for the smart grid. In 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pages 1–6. IEEE, 2019.

Md Raqibull Hasan, Yanxiao Zhao, Guodong Wang, Yu Luo, Lina Pu, and Rui Wang. Supervised machine learning based routing detection for smart meter network. In 12th EAI International Conference on Mobile Multimedia Communications, Mobimedia 2019. European Alliance for Innovation (EAI), 2019.

Nadia Boumkheld, Mounir Ghoghoh, and Mohammed El Koubi. Intrusion detection system for the detection of blackhole attacks in a smart grid. In 2016 4th International Symposium on Computational and Business Intelligence (ISCBI), pages 108–111. IEEE, 2016.

Youhbiao He, Gihan J Mendis, and Jin Wei. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. IEEE Transactions on Smart Grid, 9(5):2505–2516, 2017.

Vitaly Ford, Ambareen Siraj, and William Eberle. Smart grid energy fraud detection using artificial neural networks. In 2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG), pages 1–6. IEEE, 2014.

Hadi Karimipour, Ali Dehghantanha, Reza M Parizi, Kim-Kwang Raymond Choo, and Henry Leung. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. IEEE Access, 7:80778–80788, 2019.