Detecting Hidden Attackers in Photovoltaic Systems Using Machine Learning

Suman Sourav1,2, Partha P. Biswas2, Binbin Chen1,2, and Daisuke Mashima2

1Singapore University of Technology and Design, Singapore; e-mail: [suman_sourav, binbin_chen]@sutd.edu.sg
2Advanced Digital Sciences Center, Singapore; e-mail: [partha.b, daisuke.m]@adsc-create.edu.sg

Abstract—In modern smart grids, the proliferation of communication enabled distributed energy resource (DER) systems has increased the surface of possible cyber-physical attacks. Attacks originating from the distributed edge devices of DER system, such as photovoltaic (PV) system, is often difficult to detect. An attacker may change the control configurations or various setpoints of the PV inverters to destabilize the power grid, damage devices, or for the purpose of economic gain. A more powerful attacker may even manipulate the PV system metering data transmitted for remote monitoring, so that (s)he can remain hidden. In this paper, we consider a case where PV systems operating in different control modes can be simultaneously attacked and the attacker has the ability to manipulate individual PV bus measurements to avoid detection. We show that even in such a scenario, with just the aggregated measurements (that the attacker cannot manipulate), machine learning (ML) techniques are able to detect the attack in a fast and accurate manner. We use a standard radial distribution network, together with real smart home electricity consumption data and solar power data in our experimental setup. We test the performance of several ML algorithms to detect attacks on the PV system. Our detailed evaluations show that the proposed intrusion detection system (IDS) is highly effective and efficient in detecting attacks on PV inverter control modes.

I. INTRODUCTION

The fast depletion of fossil fuels, environmental regulation and imposition of carbon tax in some cases compelled many countries to quickly adopt alternate and replenishable sources of energy. Solar energy, a form of renewable energy, is harnessed by the well-established PV system technology. Globally, the growth in PV system installed capacity has been phenomenal in the last couple of decades, and just in the year 2019, about 109GW PV capacity was installed [1]. Together with the high penetration of renewable energy, modern grids are accommodating internet-of-things (IoT) devices for efficient control and management of the grid. Though sophisticated information technology network facilitates faster communication and overall performance enhancement of the grid, it also opens up channels for cyberattackers to intrude into the power system and perform any offensive manoeuvre that makes the system behave undesirably.

Grid or transmission system operator usually do not have visibility of DER plants (e.g., solar plants), and in most cases the monitoring of the plant is restricted to the local distribution substation level. Furthermore, renewable sources are inherently variable. Limited visibility as well as uncertainty in renewable sources can easily be exploited by an attacker to launch attacks through the edge devices of the PV systems [2]. The variability in system performance and output would even make it harder to distinguish between an actual attack and a regular change in system parameter. Attack on PV system control characteristics may jeopardise the system voltage. The impact of the attack would be severe if a majority of the PVs connected to the system are manipulated (to give reduced output or fully disconnected) or the attack is launched during peak-loading scenarios of the network. Such an attack would have economic consequences as well. Lowering the PV system active power setpoint would force the consumers to draw more active power from the thermal generator(s) connected to the grid, thereby increasing both fuel cost and emission. As an example, a change of setpoint even by 0.1 MW (lower) would incur an additional fuel cost of anywhere between $0.175 to $0.325 per hour depending on the type of fossil fuel used by the generator [3]. The cost follows quadratic relationship with the active power, implying even more commercial impact if the setpoint is lowered further.

In a distribution network, different PVs can operate in different control modes, and they can be attacked simultaneously. Most of the existing studies [2], [4], [5] considered attack only on single mode of operation, i.e., where all the PV systems are operating in the same mode. In contrast, here we consider and aim to highlight the case of a combined attack on multiple, different modes. We discuss the impact of such an attack and propose a method to detect it. Moreover, we consider a sophisticated attacker who tries to stay hidden by manipulating the PV bus measurements, i.e., by sending PV bus measurements as if there is no attack. Such hidden attackers often target to gain information by observing the system and/or to disrupt the system on a specific planned time.

A cyber rule-based intrusion detection system (IDS) might not be able to detect such attacks on the edge devices of PV system. Therefore, we need to leverage physical system data to analyze and detect. The adoption of machine intelligence in detecting cyberattacks in smart grid on various aspects is widespread. Several machine learning (ML) algorithms have also been tested in the context of PV systems [2], [4]. In a supervised ML method, the algorithm is trained with system-wide data for both normal and attack scenarios in the network.
considering variable load demand and solar power. Based on the training imparted, the algorithm is expected to classify a new set of data in the category of normal or attacked data. The method is fast and quite accurate. Also, the ML-based detection algorithm works in a non-invasive manner as it does not interfere with the normal power system operation. In a power grid, measurement data from some metering instruments might be missing occasionally due to communication loss or faulty instruments. A trained ML-model might still be able to correctly classify a set of measurement data as normal or malicious even when parts of the dataset are missing. We leverage such characteristics of the ML method in our IDS to detect attacks, especially the control mode related attacks on the PV system. We simulate the PV control modes to run power flow using the power simulator MATPOWER [6] and generate exhaustive datasets for our study. We test several ML algorithms and compare their performance. The contributions of our work can be summarized as below:

- We give one of the first studies where simultaneous attacks on PVs operating in different control modes are considered, under a strong attacker model which assumes capability of manipulating individual PV bus measurements to remain hidden.
- For the various configurations, we create several baseline datasets using a standard test distribution network with real-world PV generation and load demand data (where small errors of the energy meter readings are unavoidable). We make these datasets publicly available to facilitate further research in this direction.
- We evaluate the performance of many ML algorithms by conducting extensive experiments including cases where parts of measurement data are missing. The results show that the ML-based techniques, specifically multi-layer perceptron and random forest algorithms are effective and efficient in detecting attacks on various PV control modes (accuracy of around 95% even with missing data).

II. LITERATURE REVIEW

Cyberattack scenarios in the broader context of smart grid have been well studied in the literature. Study on DER integrated grids has also been popular among the energy and cybersecurity research communities. Qi et al. [5] suggested a holistic framework for defence against cyberattacks in a network with high DER penetrations. The resilience design aspects at cyber, physical device and utility levels had been broadly discussed. In the same vein, Johnson et al. [7] proposed engineering design control of the DER devices and enclaving (i.e., segmentation) of the network with several DERs to enhance the cyberattack resiliency. In [8], the authors summarized the current industry practices for DER cybersecurity and also suggested some strategies to improve the security postures. Specifically for IDS, signature-based and behavioural-based solutions were studied in [9] to detect few types of attacks on PV inverters. For voltage control manipulation in low voltage distribution grid, [10] gives a contextual anomaly detection method based on an artificial neural network. Chavez et al. [11] showed the importance of physical system features, in addition to the network traffic features, to identify certain types of attacks in a distribution network. They collect and use a combination of cyber-security data and power system and control information to propose a hybrid IDS for DER systems. Unsupervised [2] ML algorithms have been tested on a proposed edge-based IDS for PV system security. In [4], a more conventional approach of supervised learning ML methods were used to detect attacks, considering synchronized data from PV systems.

In a different direction, Li et al. [12] use raw electrical waveform data and a high-dimensional data-driven approach to detect and identify cyber-physical attacks in distribution power grids with PVs. Another approach that has been widely studied in the power system context is the application of physics-based techniques for attack detection [13], [14]. However, these solutions rely quite heavily on the availability and accuracy of all measurement data. For cases with missing measurements or meter reading errors, the performance and accuracy of such solutions would be limited.

Overall, most of these works discussed here focus on single operating mode and the attacker doesn’t particularly focus on remaining hidden. In contrast, here we consider simultaneous attacks on PVs operating in different control modes where the attacker manipulates PV bus measurements to remain hidden.

III. THREAT MODEL AND ATTACK MODES

Before we discuss in detail the possible threats on PV unit operations, we briefly describe the various possible operating modes of a PV unit. Once the attacker gets control, it actively tries to stay hidden by manipulating the measurement data of the bus associated with the DER by sending data as if the DER were not attacked. As such, an analysis of individual PV bus measurements wouldn’t reveal any attack.

A. PV Operating Modes

We consider three PV operating modes, namely, limit active power mode (Max P), Constant power factor (PF) mode, and voltage-reactive power mode (volt-var). Due to variability in solar irradiance, the active power output from the PV unit changes and it is limited by the capacity of PV unit and associated inverters.

In limit active power mode (Max P), a DER is set to deliver a defined maximum amount of active power. In constant power factor (PF) mode, the active power output is proportional to the reactive power output. Lastly, the voltage-reactive power mode (volt-var mode) of operation is an important regulation mode where the DER reactive power output is a function of the voltage at the point of common coupling (PCC) or the DER terminal for a standalone unit. PV inverter can be set to operate at any characteristics between the most and least aggressive curves defined as per UL 1741, and depicted in Fig. 1. Our default setting (blue line in Fig. 1) is as per the interconnection Rule 21 of California Public Utilities Commission, and also per the PV inverter application guide [15].
B. PV Attack Modes

As the penetration of DERs including PVs into the grid is becoming high, any maloperation in the PV control modes would hamper the grid operation and may inflict economic loss. A direct attack on PV operation is to disconnect the unit from grid. An attacker may also manipulate the configuration (the control curve) of a PV inverter to change the amount of reactive power absorbed from or injected into the grid. This may incur additional system losses, affect the voltage stability and even permanently damage power system components. We briefly discuss about the possible attacks on PV systems.

**Power curtailment attack:** When the DER operates in ‘limit active power mode’, an adversary could lower the active power set point (or reduce it to zero) so that the actual power injected by the DER is lower than what it is capable of delivering. This type of attack may not have immediate significant impact on the grid, however, this type of attack is difficult to detect as the DER output is inherently variable and the attacker could hide within the fluctuating PV output.

**Disconnect attack:** Disconnect attack is also an attack on active power output (usually zero power output) of the DERs when the attacker is able to control a large number of PVs in the network. The disconnection of several DERs at once would increase the amount of power drawn from the grid, which may eventually lead to line overload, voltage and frequency fluctuations. The attack may also affect the grid planning as the DER owner would be unable to sell power to the utility.

**Constant power factor (PF) mode attack:** An attacker might change the actual power factor setting to make it more capacitive or inductive resulting in poor voltage regulation, power quality and/or higher losses in the power system.

**Volt-var attack:** Smart DER inverters can be utilized to control voltage at certain point in the network (e.g., point of common coupling) by absorbing or injecting certain amount of reactive power. When an adversary gains knowledge of the control algorithm or the volt-var characteristic, (s)he can change the characteristic or even invert it to absorb or inject an arbitrary amount of reactive power. This would greatly hamper the voltage control application, and would affect the voltage level at the grid.

**Reverse power flow attack:** Modern households are equipped with smart appliances that adopt communication channel for remote control and monitoring. An attacker could exploit any weak links in the communication channel to turn the devices off. When the DER generation is high, such an event would result in supplying excess power to the grid instead of local consumption. If a large number of loads are under control of the attacker, the cumulative effect would impact the voltage regulation and protection coordination of the grid.

IV. PHYSICS-BASED VS ML-BASED APPROACH

In this section, we discuss why we focus on ML-based detection of attacks on DER systems instead of physics-based method. From a given datapoint the objective of either approach is to determine the presence/absence of an attack. In real distribution networks, the differences in overall generation and consumption data denotes the inherent ‘loss’ in the network, occurring primarily due to the impedance of the distribution lines. When the PV system is attacked and the associated PV system meter readings are manipulated (to maintain the pretence of non attack at individual level), the apparent overall loss value would be different from the actual system loss. Furthermore, small meter errors (maximum ±1%) are unavoidable and such cumulative errors of numerous meters would make it even harder to calculate the actual system losses, even if there is no attack. We evaluate the performance of physics-based study, i.e., power flow study, in detecting attacks on the PV system.

Fig 2 shows the plot of a form of network ‘losses’ for the normal and attack datapoints. The attack cases consider PV control mode attacks, PV system meter data manipulation and inherent meter errors, while the normal datapoints have only the meter errors. As observed from the plot, a large number of normal and attack datapoints overlap, and it would not be easy to delimit an appropriate boundary between the two types of datapoints by some thresholding technique. Therefore, we resort to the supervised ML models that can learn from the available data and help develop a mechanism to identify attacks on the PV system. The ML-based detector can also function with some missing measurement data in the system. The power flow study would give incorrect results or may even fail to converge if some measurement data are unavailable.
V. ML-BASED IDS

We make use of several well-known and popular machine learning algorithms/classifiers to evaluate the accuracy of those models as an IDS. Most of the algorithms we consider here are simple supervised ML algorithms and once trained, for any given input can output whether or not there exists an attack. As these algorithms are quite well-known and well-used in literature [16], [17], [18] we only provide a brief description. These classifiers were implemented in python using the sklearn library with a 5-fold cross validation. To make our results reproducible, we provide the tuned hyper-parameters for the generated datasets (in section VI-B) for each of the algorithms.

**Logistic Regression (LR):** LR is one of the simpler and widely used ML algorithms for binary classification and is typically used as a baseline for performance comparison. It estimates the relationship between the independent variables (features) and target binary variable (label). Based on a grid search, we obtain the optimal hyper-parameters for LR to be \( C=100, \text{max}_\text{iter}=1000, \text{penalty}='\text{l1}', \) and solver='liblinear'.

**Support Vector Machine (SVM):** For SVM, the classification is performed by determining a hyperplane that differentiates two classes to the largest extent (or by a maximum margin). Our grid search determines the optimal parameters to be \( C=1000, \gamma=1, \text{and kernel='rbf}'. \)

**k Nearest Neighbors (KNN):** KNN works on the basic assumption that similar things/data-points exist in close proximity of one another and the classification is based on majority voting by the neighbors. The optimal parameters obtained through a grid search in this case was metric='minkowski', \( n\_\text{neighbors}=2, \) and weights='uniform'.

**Gradient boosting (GBT):** GBT creates the prediction model in a sequence of steps, where in each step, it minimizes a predefined loss function by adding a tree, while keeping the existing trees unchanged. The grid search in this case yielded learning_rate=0.01, max_depth=4, max_features='sqrt', \( n\_\text{estimators}=1750, \text{random}\_\text{state}=10, \) and subsample=1 as the optimal parameters.

**Random Forest (RF):** RF is another ensemble ML method consisting of many uncorrelated decision trees. For classification, the output of the RF classifier is the class selected by most trees. In this case, the grid search yields max_depth=100, max_features=3, min_samples_leaf=3, min_samples_split=12 as the set of optimal parameters.

**Multi-layer Perceptron (MLP):** MLP is a feed-forward artificial neural network based classifier where each neural network layer is fully connected to the following one. Neurons have nonlinear activation functions, except for those of the input layer. The optimal model was obtained after a grid search that gave the parameters activation='tanh', alpha=0.0001, hidden_layer_sizes=(50, 100, 50), learning_rate='adaptive', max_iter=1000, and solver='adam'.

VI. CASE STUDIES AND EVALUATIONS

We evaluate the performance of our proposed IDS on a standard distribution network where PV systems, domestic and small scale commercial consumers are connected. Real world data for PV generation and domestic household demands of every single minute over a period of one month has been considered for training and testing purpose of the several ML algorithms, and to assess the overall performance of the IDS.

### A. Test Network

We consider the 69-bus 12.66kV distribution network proposed by Baran and Wu [19], and reproduced here in Fig. 3. The network has been widely adopted by the research community to study optimal placement of DERs and shunt capacitors [20], [21], as well as for optimal network reconfiguration [22]. We use the default base configuration and branch data as in the original proposed network. Bus load data is altered as described herein.

**Load data:** For bus loading, we consider the variable domestic household consumption data provided in Smart∗ [23] dataset. Smart∗ contains every minute energy consumption data for three real homes - Home A, Home B and Home C, for several months and years. We use the data for the month of June in the year 2012. While assigning these data to the network buses, we consider that a minimum of 4 and maximum 10 houses (of any combination of home types selected randomly) are connected to each bus. While doing so, we also ensure that the network load at any moment does not exceed the total load originally proposed in [19], i.e., 3802.19 kW and 2964.6 kvar. In our power system study, we ignore the branch-line or cable required to interconnect all houses connected to each bus, and assume that the load at the point of common coupling is balanced. Also, one smart meter shall be able to transmit energy consumption data of all the homes connected to a single bus. We do not consider any load at substation bus 1, bus 2, bus 3 (as in the original network), and also at the buses where PV plants are connected. A summary of the network is provided in Table I. The average power factor for the household loads is considered to be 0.78 lagging, in line with the detailed study performed in [24]. We publicly share the synthesized time-series consumption data in GitHub repository.

---

1https://github.com/suman-nus/Synthesized-DER-Data
PV system data: We consider 4 nos. PV plants in our test network. Singapore PV generation data for selected 4 plants are incorporated in our study. The data contains PV generation of every minute for the month of May in the year 2020 (data from 1st-30th May, 2020 are considered in study). In a distribution network, the location of the PV is decided based on the load demand at various buses of the network. In our test case, placement of the PV units closer to the farthest points of the radial feeders would provide voltage support, as well as would help reduce the network losses. Therefore, we consider the 4 PV units that are connected to bus 25, bus 32, bus 45 and bus 62 (refer to Fig. 3) with maximum kW capacities as mentioned in Table I. Although the choice of PV locations in our experimental set up is somewhat arbitrary, finding optimal siting for the same is outside the scope of this work.

B. Datasets for the Machine Learning Algorithm

We consider consumption and generation data per minute for 12 hours each day for a month-long period. The purpose of our study is to detect attacks on PV system control functions. Grid connected PVs could be turned off during night, and to have meaningful gain, the attack would likely be carried out during daytime when the PV generation is at substantial level. Now, out of approximately 21600 total datapoints over a month, 80% of the datapoints are used to train the ML algorithm, while the remaining are utilized to test it. Both training and testing datasets have normal and attack datapoints. Normal datapoints are for the naturally variable demand data and the PV generation data. 3-different settings of the network, based on operating modes of the 4 PV units, are considered in our study as detailed in Table II. For all the settings, the attack datapoints are created in the following manner.

- 20% of the total datapoints are randomly selected so that they can be corrupted to generate attack datapoints.
- Each DER is assumed to operate in one of the 3 operating modes: constant power factor, limit active power (Max P) and volt-var control.
- One or multiple DERs, operating all in same or different modes, may be attacked. The attack scenarios considered in our study for different settings of the network are provided in Table II.
- In each attack datapoint either 1 PV, 2 PVs or all the 4 PVs are considered under attack (randomly chosen).

In the context of the PV attack modes discussed in section III-B, it may be noted that the effect of power curtailment attack, disconnect attack and reverse power flow attack can be simulated with the change in setpoint of active power \( P \) when the PV is operating in limit active power (i.e., Max \( P \)) mode. For both normal and attack datasets, each datapoint contains active power \( (P) \) and reactive power \( (Q) \) for all buses. We consider measurement error of up to \( \pm 1\% \). The standard IEEE C57.13.6 defines high accuracy classes of instrument transformers such as 0.15S, 0.3S, 0.5S, etc. to have maximum errors of \( \pm 0.15\% \), \( \pm 0.3\% \) and \( \pm 0.5\% \), respectively. Moreover, metering instrument accuracy classes of 0.2, 0.5, etc. are also stipulated in ANSI standard C12.20. Therefore, our assumption of maximum error level of up to \( \pm 1\% \) is well justified if the metering instruments are of high accuracy class. In case of an attack on DER control mode, we presume that the attacker manipulates the DER settings (or control characteristics), as well as the measurement data of the bus associated with the DER as if the DER were not attacked. Therefore, the attacker can remain hidden in the system as the PV bus measurements won’t reveal any anomaly. We add all \( P \) and \( Q \) received from all the load buses. In the dataset, we have a total of 6 features for the machine learning models: sum of all \( P \) and \( Q \) readings (say, \( P_{d} \) and \( Q_{d} \), respectively) obtained from load buses, substation bus-1 \( P \) and \( Q \) measurement data (say, \( P_{gen} \) and \( Q_{gen} \), respectively), and the differences of these values, i.e., \( (P_{gen} - P_{d}) \) and \( (Q_{gen} - Q_{d}) \).

**Missing Measurement data:** In a large distribution network numerous smart meters would send measurement data to an aggregator or a nearby substation. In the process, it is likely that some measurement data would be missed due to a faulty meter or a communication loss. We create datasets to account for such cases and evaluate the performance of our IDS on these datasets. In the measurement datasets, we consider 20% of the total datapoints have missing data where in each datapoint, maximum 10% of the bus data (both \( P \) and \( Q \) data for the buses) are missing. For example, if a measurement datapoint has meter readings from 60 buses of the network, readings of 6 buses would be missing (total 12 missing meter readings considering both \( P \) and \( Q \)). Now, if we have a total of 1000 measurement datapoints, 200 of them would have such missing data. Similar to the earlier case, we sum all the available bus \( P \) and \( Q \) data with missing data treated as 0.

C. Performance of various ML algorithms

To more accurately simulate different real world settings, we consider three training/testing schemes as shown in Table III where we consider inputs with/without missing measurement data. We evaluate the performance of three schemes under different PV operating modes and attack scenarios using several different evaluation metrics. Thereafter, we discuss how the ML algorithms performs in these cases.

To get a holistic view of the performance, we calculate several different well known evaluation metrics like Accuracy, Precision, Recall, AUC (area under the ROC curve), PR AUC (precision recall curve) and Jaccard score. In the interest of space, we refer the reader to [25], [26] for details regarding the evaluation metrics. For each of the evaluation metrics, the

| Items | Quantity | Details |
|-------|----------|---------|
| Buses | 69       | Base voltage: 12.66 kV [19] |
| Branches | 73 | Open branches: 69 to 73; Branch data [19] |
| PV units | 4 | Bus 25 (420 kW), Bus 32 (180 kW), Bus 45 (330 kW), Bus 62 (390 kW) |
| Loads | - | Consumption data: [23]; No load: Buses 1, 2, 3, 25, 32, 45, 62 |
possible values ranges from 0 to 1, with a value closer to 1 implying better performance. See Tables IV, V, VI, and VII for the performance of the ML algorithms in each scenario.

We observe that the performance of all the algorithms are better when trained and tested on similar datasets (either with all available data, or with missing data) as compared to the case where training is done on all available data and testing is done with missing data. However, even in this case the ML algorithms, especially RF and MLP perform reasonably well.

Overall, the best performing algorithms in most cases are also the MLP algorithm and the RF algorithm. These dominate the top results (shown in bold font in Tables IV, V, VI, and VII) or are a close second in most cases. The decision tree based algorithms (RF and GBT) perform in nearly identical fashion with RF holding the edge in many cases. However, the difference in many cases is quite insignificant and can possibly be attributed to fine grained hyper-parameter tuning.

**VII. CONCLUSION**

In this work, we present an ML-based IDS solution for various possible attack modes on PV system controls. For study purpose, we develop a test distribution network incorporating real-world PV generation data and consumption data. We observe that the MLP and the RF algorithms exhibit the most superior performance with attack detection accuracy up to around 95% for most scenarios. We believe that this obtained accuracy is sufficient for most cases and more sophisticated ML algorithms like RNN and transformers can perform even better at the cost of additional time and resources for training. In general, the ML-based approach can detect even a small attack that does not significantly impact the grid operation.

**ACKNOWLEDGEMENTS**

This research is supported in part by the National Research Foundation, Singapore, under its National Satellite of Excellence Programme “Design Science and Technology for Secure Critical Infrastructure” (Award Number: NSoE_DeST-SCI2019-0008), and in part by the National Research Foundation, Prime Minister’s Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme, and in part by the SUTD Start-up Research Grant (SRG Award No: SRG ISTD 2020 157). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

**REFERENCES**

[1] “IEA (2020), Renewables 2020, IEA, Paris,” Oct 2021. [Online]. Available: https://www.iea.org/reports/renewables-2020

[2] D. M. Shilay, K. G. Lorey, T. Weiz, T. Lovetty, and Y. Cheng, “Catching anomalous distributed photovoltaics: An edge-based multimodal anomaly detection,” arXiv preprint arXiv:1709.08830, 2017.

[3] P. P. Biswas, P. Suganthan, and G. A. Amarattunga, “Optimal power flow solutions incorporating stochastic wind and solar power,” Energy Conversion and Management, vol. 148, pp. 1194–1207, 2017.

[4] Q. Li, F. Li, J. Zhang, J. Ye, W. Song, and A. Mantoth, “Data-driven cyberattack detection for photovoltaic (pv) systems through analyzing micro-pmu data,” in 2020 IEEE Energy Conversion Congress and Exposition (ECCE). IEEE, 2020, pp. 431–436.

[5] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, “Cybersecurity for distributed energy resources and smart inverters,” IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 28–39, 2016.

[6] R. D. Zimmerman, C. E. Marrillo-Sánchez, and D. Gan, “Matpower,” PSERC[Online], Software Available at: http://www.pserc.cornell.edu/matpower, 1997.

[7] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, “Power system effects and mitigation recommendations for der cyberattacks,” IET Cyber-Physical Systems: Theory & Applications, vol. 4, no. 3, pp. 240–249, 2019.

[8] R. S. de Carvalho and D. Saleem, “Recommended functionalities for improving cybersecurity of distributed energy resources,” in 2019 Resilience Week (RWS), vol. 1, 2019, pp. 226–231.

[9] C. B. Jones, A. R. Chavez, R. Darbari-Zamora, and S. Hossain-McKenzie, “Implementation of intrusion detection methods for distributed photovoltaic inverters at the grid-edge,” in IEEE ISGT, 2020.

[10] A. M. Kosek, “Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model,” in CPSR-SG. IEEE, 2016, pp. 1–6.

[11] A. Chavez, C. Lai, N. Jacobs, S. Hossain-McKenzie, C. B. Jones, J. Johnson, and A. Summers, “Hybrid intrusion detection system design for distributed energy resource systems,” in 2019 IEEE CyberPELS (CyberPELS). IEEE, 2019, pp. 1–6.

[12] F. Li, R. Xue, Y. Yang, L. Gou, P. Ma, J. Shi, J. Ye, and W. Song, “Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach,” IEEE Journal of Emerging and Selected Topics in Power Electronics, 2019.

[13] D. Mashima, B. Chen, T. Zhou, R. Rajendran, and B. Sikdar, “Securing substations through command authentication using on-the-fly simulation of power system dynamics,” in IEEE SmartgridComm, 2018, pp. 1–7.
### TABLE IV
RESULTS OF DIFFERENT ML ALGORITHMS FOR NETWORK SETTING 1 (ALL PVs ARE IN CONSTANT PF = 1 MODE)

| Scheme | LR | SVM | KNN | RF | GBT | MLP |
|--------|----|-----|-----|----|-----|-----|
| Accuracy | 0.859 | 0.936 | 0.929 | 0.963 | 0.963 | 0.962 |
| Precision | 0.8 | 0.835 | 0.830 | 0.921 | 0.972 | 0.934 |
| Recall | 0.926 | 0.681 | 0.662 | 0.821 | 0.822 | 0.823 |
| F1 Score | 0.857 | 0.81 | 0.79 | 0.899 | 0.899 | 0.897 |
| AUC | 0.713 | 0.933 | 0.871 | 0.957 | 0.963 | 0.965 |
| PR AUC | 0.697 | 0.899 | 0.924 | 0.949 | 0.932 | 0.933 |
| Jaccard | 0.826 | 0.681 | 0.653 | 0.817 | 0.816 | 0.813 |

### TABLE V
RESULTS OF DIFFERENT ML ALGORITHMS FOR NETWORK SETTING 2 (ALL PVs ARE IN MAX P MODE)

| Scheme | LR | SVM | KNN | RF | GBT | MLP |
|--------|----|-----|-----|----|-----|-----|
| Accuracy | 0.956 | 0.963 | 0.948 | 0.968 | 0.969 | 0.969 |
| Precision | 0.949 | 1 | 0.969 | 0.991 | 0.991 | 1 |
| Recall | 0.924 | 0.816 | 0.75 | 0.849 | 0.85 | 0.844 |
| F1 Score | 0.872 | 0.899 | 0.853 | 0.914 | 0.915 | 0.915 |
| AUC | 0.979 | 0.984 | 0.91 | 0.983 | 0.984 | 0.986 |
| PR AUC | 0.945 | 0.958 | 0.902 | 0.959 | 0.958 | 0.958 |
| Jaccard | 0.79 | 0.816 | 0.744 | 0.842 | 0.843 | 0.844 |

### TABLE VI
RESULTS OF DIFFERENT ML ALGORITHMS FOR NETWORK SETTING 3 (ALL PVs ARE IN VOLT-VAR CONTROL MODE)

| Scheme | LR | SVM | KNN | RF | GBT | MLP |
|--------|----|-----|-----|----|-----|-----|
| Accuracy | 0.838 | 0.932 | 0.915 | 0.957 | 0.958 | 0.962 |
| Precision | 0.949 | 1 | 0.969 | 0.991 | 0.991 | 1 |
| Recall | 0.988 | 0.816 | 0.75 | 0.849 | 0.85 | 0.844 |
| F1 Score | 0.906 | 0.996 | 0.948 | 0.985 | 0.986 | 0.989 |
| AUC | 0.995 | 0.958 | 0.902 | 0.959 | 0.958 | 0.958 |
| PR AUC | 0.962 | 0.904 | 0.824 | 0.93 | 0.935 | 0.936 |
| Jaccard | 0.78 | 0.662 | 0.588 | 0.802 | 0.795 | 0.812 |

### TABLE VII
RESULTS OF DIFFERENT ML ALGORITHMS FOR NETWORK SETTING 4 (PVs ARE IN DIFFERENT OPERATING MODES)

| Scheme | LR | SVM | KNN | RF | GBT | MLP |
|--------|----|-----|-----|----|-----|-----|
| Accuracy | 0.889 | 0.942 | 0.924 | 0.964 | 0.963 | 0.962 |
| Precision | 0.949 | 0.997 | 0.975 | 0.985 | 0.982 | 0.976 |
| Recall | 0.409 | 0.712 | 0.833 | 0.833 | 0.829 | 0.833 |
| F1 Score | 0.628 | 0.831 | 0.699 | 0.902 | 0.899 | 0.897 |
| AUC | 0.809 | 0.952 | 0.869 | 0.973 | 0.973 | 0.973 |
| PR AUC | 0.725 | 0.92 | 0.847 | 0.943 | 0.943 | 0.946 |
| Jaccard | 0.457 | 0.71 | 0.625 | 0.821 | 0.817 | 0.813 |

[14] D. Mashima, P. Gunathilaka, and B. Chen, “Artificial command delaying for secure substation remote control: Design and implementation,” IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 471–482, 2017.

[15] “Grid support function application protocol for UNDM & TRIO-TM inverters,” Oct 2021. [Online]. Available: https://search.abb.com/library

[16] B. E. Boser, I. M. Guyon, and V. N. Vapnik, “A training algorithm for optimal margin classifiers,” in Proceedings of the fifth annual workshop on Computational learning theory. ACM, 1992, pp. 144–152.

[17] Y. Cheng, C. Xu, D. Mashima, P. P. Biswas, G. Chhipurapalli, B. Zhou, and Y. Wu, “Powernet: a smart energy forecasting architecture based on neural networks,” IET Smart Cities, 2020.

[18] K. Shah, H. Patel, D. Sanghvi, and M. Shah, “A comparative analysis of logistic regression, random forest and knn models for the text classification,” Augmented Human Research, vol. 5, pp. 1–16, 2020.

[19] M. E. Baran and F. F. Wu, “Optimal capacitor placement on radial distribution systems,” IEEE Transactions on power delivery, vol. 4, no. 1, pp. 725–734, 1989.

[20] P. P. Biswas, R. Mallipeddi, P. N. Suganthan, and G. A. Amarasinghe, “A multiobjective approach for optimal placement and sizing of distributed generators and capacitors in distribution network,” Applied soft computing, vol. 60, pp. 268–280, 2017.

[21] E. A. Almabsout, R. A. El-Sehiny, O. N. U. An, and O. Bayat, “A hybrid local search-genetic algorithm for simultaneous placement of dg units and shunt capacitors in radial distribution systems,” IEEE Access, vol. 8, pp. 54465–54481, 2020.

[22] P. P. Biswas, P. N. Suganthan, and G. A. Amarasinghe, “Distribution network reconfiguration together with distributed generator and shunt capacitor allocation for loss minimization,” in 2018 IEEE Congress on Evolutionary Computation (CEC). IEEE, 2018, pp. 1–7.

[23] S. Barker, A. Mishra, D. Irwin, E. Cechet, P. Shenyi, J. Albrecht et al., “Smart*: An open data set and tools for enabling research in sustainable homes,” SmartKDD, August, vol. 111, no. 122, p. 108, 2012.

[24] A. Ahmad, S. A. R. Khashif, M. A. Saqib, A. Ashraf, and U. T. Shami, “Tariff for reactive energy consumption in household appliances,” Energy, vol. 186, p. 115188, 2019.

[25] N. Japkowitz and M. Shih, Evaluating Learning Algorithms: A Classification Perspective. USA: Cambridge University Press, 2011.

[26] G. I. Iwenko and S. A. Honov, “On the jaccard similarity test,” Journal of Mathematical Sciences, vol. 88, no. 6, pp. 789–794, 1998.