Electrical Engineering
https://doi.org/10.1007/s00202-022-01601-9

ORIGINAL PAPER

Analysis of deceptive data attacks with adversarial machine learning for solar photovoltaic power generation forecasting

Murat Kuzlu[1] · Salih Sarp[2] · Ferhat Ozgur Catak[3] · Umit Cali[4] · Yanxiao Zhao[2] · Onur Elma[5] · Ozgur Guler[6]

Received: 13 January 2022 / Accepted: 15 June 2022

Abstract

The solar photovoltaics (PV) energy resources have become more important with their significant contribution to the current power grid among renewable energy resources. However, the integration of the solar PV causes reliability issues in the power grid due to its high dependence on the weather condition. The predictability and stability of forecasting are critical for fully utilizing solar power. This study presents an Artificial Neural Network (ANN)-based solar PV power generation forecasting using a public dataset to form a basis experimental testbed to demonstrate analysis and impact of deceptive data attacks with adversarial machine learning. In addition, it evaluates the algorithms' performance using the Root Mean Squared Error (RMSE), Mean Squared Error (MSE), and Mean Average Error (MAE) metrics for two main cases, i.e., with and without adversarial machine learning attacks. The results show that the ANN-based models are vulnerable to adversarial attacks.

Keywords Solar PV energy generation forecasting · Adversarial machine learning attacks · Forecasting

1 Introduction

Reliability is the most critical parameter to maintain grid stability and operation. The real-time power supply and load balance are key factors for the power system's reliability. However, the electric energy cannot be stored in large quantities due to the architecture of the current power system. Power plants generate the electrical energy to be consumed immediately without storing the energy. In addition, the power grids are undergoing rapid change with increased penetration of Distributed Energy Resources (DER), i.e., wind turbines, solar photovoltaics (PV), fuel cells, microturbines, combustion turbines, cogeneration, and energy storage systems [1]. Among these energy resources, solar PV has shown unprecedented growth in the USA during recent decades. The integration of renewable energy technologies into the existing grid requires robust performing forecasting algorithms due to their weather dependencies. At present, there are more than 1 million solar PV installations across the USA, representing 71.3 GW of operating PV capacity. The increase in residential installations helped the US solar market grow 45% year-over-year [2]. In recent years, solar power was

Murat Kuzlu, Ferhat Ozgur Catak, Umit Cali, Yanxiao Zhao, Onur Elma and Ozgur Guler have contributed equally to this work.

✉ Salih Sarp
sarps@vcu.edu

Murat Kuzlu
mkuzlu@odu.edu

Ferhat Ozgur Catak
f.ozgur.catak@uis.no

Umit Cali
umit.cali@ntnu.no

Yanxiao Zhao
yzhao7@vcu.edu

Onur Elma
onurelma@comu.edu.tr

Ozgur Guler
oguler@ekareinc.com

[1] Engineering Technology, Old Dominion University, Norfolk, VA, USA

[2] Electrical and Computer Engineering, Virginia Commonwealth University, Richmond, VA, USA

[3] Electrical Engineering and Computer Science, University of Stavanger, Stavanger, Norway

[4] Department of Electric Power Engineering, Norwegian University of Science and Technology, Trondheim, Norway

[5] Electronics Engineering, Canakkale Onsekiz Mart University, Canakkale, Turkey

[6] R&D, eKare Inc, Merrifield, VA, USA

Published online: 22 July 2022

significantly increased when compared to other fuel types, its share of total US electrical generation—from just 0.1% in 2010 to nearly 4% today [3,4]. Solar energy is one of the best alternative energy resources to fuel types. However, the grid integration of solar PVs being weather-dependent power generation technology has its own challenges due to fluctuations in power generation [5]. Emerging technologies are utilized to realize the potential of smart grids [6,7]. Artificial intelligence (AI)-based energy forecasting methods have been the most promising techniques to increase the grid integration capabilities of solar PV resources [8–10]. These forecasting methods have been used in the energy domain, especially solar PV generation, due to their success in extracting the complex underlying structure of the solar data [11]. The Deep Learning (DL) algorithm—the most popular AI-based method—is applied to solar forecasting without feature engineering, i.e., less sensitive to missing data [12]. Machine Learning (ML) techniques such as Linear Regression (LR), K-Nearest Neighbor (KNN), Decision Trees (DT), Gaussian Process Regression (GPR), Gradient Boosting Regression Trees (GBRT), Support Vector Regression (SVR), and Multilayer Perceptron Regression (MLPR) are used for many energy generation forecasts. Prior efforts for forecasting PV power generation include developing a power generation prediction system using wavelet transformation and AI combinations [13]. A deep Convolutional Neural Network (CNN) model, i.e., SolarNet, is proposed for solar radiation forecasting in [14]. In [15], a CNN-based framework for the solar prediction model is proposed. The authors proposed a Long Short-Term Memory (LSTM) model for the solar PV generation forecast with the utilization of the Principal Component Analysis (PCA) to reduce the training time and improve the generalization ability of the model in [16]. The authors in [17] review time series and Artificial Neural Networks (ANN) for short-term PV power generation forecasting across five different sites, while the authors in [18] review recent AI applications on solar power generation forecasting, focusing on DL techniques. The study [19] provides a PV power forecasting model using weather classification in combination with ANN using an additional aerosol index feature. A Random Forest algorithm optimized by Differential Evolution Grey Wolf Optimizer [20] is used to forecast the PV power generation. The authors in [21] proposed the hour-ahead PV power generation forecast using SVR, Polynomial Regression, and Lasso. The study [22] summarizes the solar power generation forecasting performance of ANN, SVR, and GPR with sensitivity analysis for parameter tuning.

Another important aspect of forecasting using AI is its security. DL models are vulnerable to attacks that can hinder their potential of the models and put it at risk [23]. One of the studies done by the authors in [24] analyzed the model training and adversarial attack aspects for solar PV generation forecasting. The results indicated that adversarial attacks could reduce the performance of short-term forecasting methods, especially LSTM and Temporal Convolutional Network (TCN). Another study [25] emphasizes that AI-based models can be used to forecast the generation capacity of solar PV. However, these models are vulnerable to adversarial attacks at the same time, i.e., the forecasting error under attack highly increased when compared to the forecasting error in non-attacked conditions. It also discusses mitigating the adversarial attacks to reduce the damage to the forecasting model accuracy by detecting and discarding adversarial examples. The study [26] presents the effect of data integrity attacks on the performance of four different load forecasting models, i.e., multiple linear regression, SVR, ANN, and fuzzy interaction regression. A study by Chen et al. [27] discusses the vulnerability of the power systems and load forecasting models. Their findings indicate that forecasting models are exposed to high-security risks against black-box attacks. The impact of adversarial attacks on solar power generation is examined by the authors in [28]. Findings suggest that adversarial attacks pose serious threats to regression tasks.

In our previous study [29], several AI-based solar PV power generation forecasting models were investigated along with the impact of false data injection in terms of performance metrics, such as the Root Mean Squared Error (RMSE), Mean Squared Error (MSE), and Mean Average Error (MAE). This study focuses on adversarial machine learning attacks, which is a technique attempting to fool models with deceptive data.

Researchers have shown that existing Deep Neural Networks (DNN) models are vulnerable to carefully crafted attacks [30–32]. These techniques are called adversarial machine learning attacks [33]. Adversarial machine learning attacks are based on perturbation of the input instances in a direction that maximizes the chances of wrong decision making, resulting in false predictions [34]. Adversarial machine learning attacks are of two types: i) the first type of attack is called *classical*, where the adversary attempts to make the target misclassify a specific example, while the second type is called *contextual*, where the adversary attempts to make the target misclassify examples from a particular class, distributed according to a specific pattern [35]. The well-known adversarial machine learning attacks are the fast-gradient sign method (FGSM), projected gradient descent (PGD), basic iterative method (BIM), and Carlini&Wagner (C&W) attacks. In this paper, we modified the original classification-based FGSM attack into the regression models. The proposed attack uses the MSE loss function instead of categorical cross-entropy. The MSE loss function is more suitable than the categorical cross-entropy function for the regression models. The regression-based attack is called Regression-Based Fast Gradient Sign Method Attack (R-FGSM). The proposed attack can be implemented in a single forward pass, the same way as the original FGSM attack.

The results show that the proposed attack is more efficient than the original FGSM attack. The results also show that the modified attack can fool the DNN models when the data samples are perturbed in a specific direction.

The contributions are:

(i) The development of an ANN-based PV power generation forecasting model,
(ii) Validation of the selected ANN-based models in terms of RMSE, MSE, and MAE metrics,
(iii) Analysis of deceptive data attacks with adversarial machine learning for ANN-based solar PV forecasting models.

2 Methodology

Machine Learning methods have been quite popular in the field of solar power forecasting field. The current studies focus on the AI-based models of machine learning with the goal to find robust solar power generation forecasting. In this study, the Artificial Neural Network (ANN) model is experimented with and investigated in terms of the model performance with and without deceptive data attacks. Biological neurons inspired researchers who created the ANN algorithms, which aim to mimic human cognitive features such as learning and decision-making. This process is accomplished after mathematical modeling and using the software domain. Perceptrons, activation functions, input, output, and hidden layers are the main components of typical ANNs. Signals represented as real numbers are forwarded from one layer to the next one via synapses from the input to the output layer. The output of each layer is determined by the weighted sum of inputs. Most the ANN algorithms are designed to process the data by splitting it into two main categories: training and testing, respectively. Some ANN models can also be designed with a validation dataset. The training dataset is utilized to fit the weights of, for instance, a classifier, while the testing dataset is an independent dataset, which is used to quantify the performance of the ANN algorithm. Furthermore, a validation dataset is used to tune the architecture of a classifier. As indicated, the utilization of ANN models is not limited to classification. During the training stage, all weights in a given ANN and the corresponding threshold are set as random numbers. Weights and thresholds are adjusted to the same data labels to yield similar outcomes during this stage. Activation functions are responsible to determine the behavior and output of the neuron by also using some normalization functions. Normalization usually occurs between 0 and 1 or -1 and 1 limits. Activation functions can be in the form of linear, unit step, sigmoid or hyperbolic tangent, depending on the need, which also acts as a kind of gatekeeper. The corresponding neuron's gate is opened to transmit the number coming from the previous neurons if the same number is above the threshold boundaries of the particular activation function. The broadcasting of the signal transmission from input to output layer via hidden layer or layers is repeated [36].

The general overview of this study is shown in Fig. 1. The proposed framework focuses on ANN-based solar power generation forecasting models and hosts only one adversarial attack, i.e., FGSM. The framework works with the following four steps: (1) Solar PV Data Collection and Processing, (2) Adversarial Noise, (3) ANN-based Forecasting Models, and (4) Performance Metrics.

- Solar PV Data Collection and Processing: The first step is to collect data from publicly available data resources or manual user upload. The framework stores time-series data, i.e., solar power generation. Then, the quality of the collected data will be improved by pre-processing for robust analysis and decision. This process includes removing or filling in the missing values, detecting outliers, and normalizing the data. In this study, the data are collected from a publicly available data resource.
- Adversarial Noise: The framework hosts one of the first and most popular adversarial attack models, i.e., Fast Gradient Sign Method (FGSM), to generate the adversarial noise. It attempts to fool solar power generation models by supplying craftily manipulated input with a slight difference. This step is performed only for adversarial attack cases.
- ANN-based Forecasting Model(s): Classification, forecasting, and regression analysis are among the most popular application areas of ANNs. The framework hosts an ANN-based model for solar power generation forecasting. This step also includes the training and the testing phase, respectively.
- Performance Metrics: The main objective of this step is to evaluate and measure the model performance with and without adversarial attacks in terms of model accuracy, i.e., MSE, RMSE, and MAE.

Regarding the experiments, the framework supports two types of use cases. The first, the dataset without deceptive data attacks, i.e., ignoring the adversarial noise step, is used with a forecasting model using the ANN technique, and results are evaluated with performance metrics, i.e., RMSE, MSE, and MAE. The second, the same model is run under deceptive data attacks, i.e., including the adversarial noise step, and the performance of the ANN model is analyzed using the same performance metrics again.

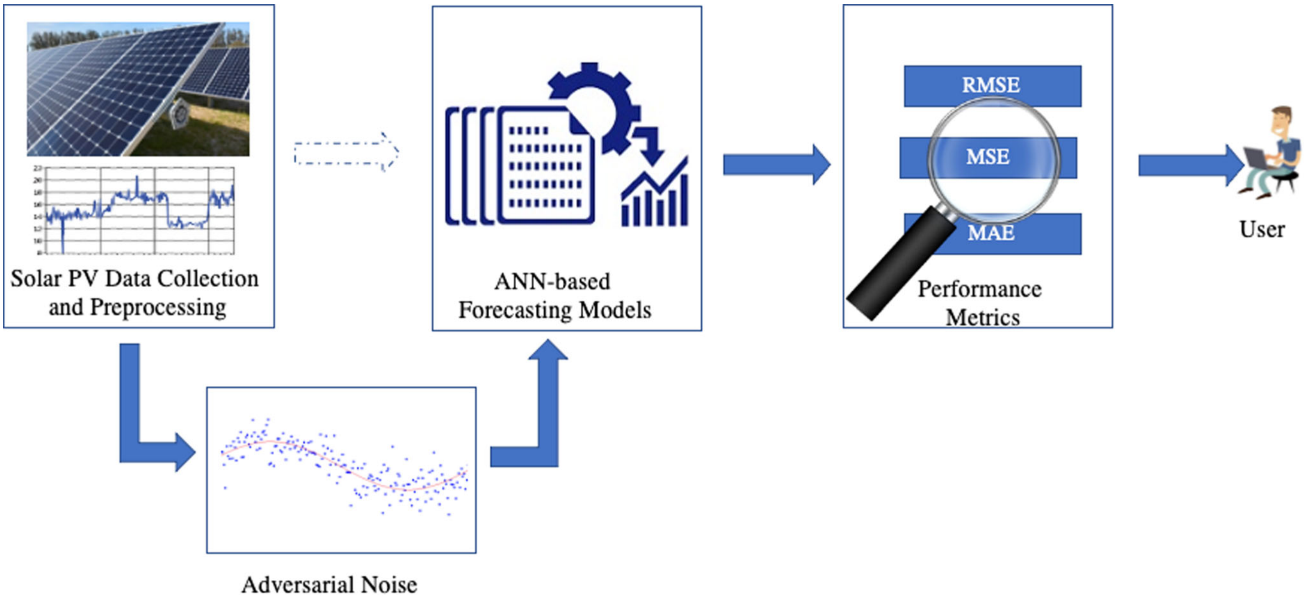

Solar PV Data Collection and Preprocessing
ANN-based Forecasting Models
RMSE
MSE
MAE
Performance Metrics
User
Adversarial Noise

Fig. 1 The framework of the solar PV power generation forecasting model

3 Data collection, preprocessing, validation, and adversarial attack method

3.1 Dataset collection

An open-source benchmark dataset is used for this work, which is obtained from the Global Energy Forecasting Competition (GEFCOM) held in 2014 [37]. The dataset consists of hourly PV power generation data and corresponding numerical weather forecasts from April 2012 to July 2014, and contains the following 12 weather variables from the European Centre for Medium-Range Weather Forecasts (ECMWF):

1. Total column liquid water (*kg m**-2*)
2. Total column ice water (*kg m**-2*)
3. Surface pressure (*Pa*)
4. Relative humidity (%)
5. Total cloud cover (0-1)
6. 10-meter U wind component (*m s**-1*)
7. 10-meter V wind component (*m s**-1*)
8. 2-meter temperature (*K*)
9. Surface solar rad down (*J m-2*)
10. Surface thermal rad down (*J m-2*)
11. Top net solar rad (*J m-2*)
12. Total precipitation (*m*)

3.2 Train/test dataset and validation

The dataset is split into training and testing subsets with a ratio of 0.8 and 0.2, respectively. The randomized split is needed to obtain the same division for further validation of the model.

Several performance metrics are used to evaluate and compare different ML models. The RMSE metric gives the same level of error as the prediction, which makes the interpretation easier. Moreover, the RMSE metric gives smaller values, which are widely preferred for simplicity. The RMSE equation is shown in equation (1). Another metric that is used in this study is MAE, which quantifies the accuracy of our model by calculating the average absolute difference between actual and predicted values in equation (2).

$$\text{RMSE} = \sqrt{\frac{\sum (Y_t - \hat{Y}_t)^2}{n}} \tag{1}$$

$$\text{MAE} = \frac{1}{n}\sum_{t=0}^{n} |Y_t - \hat{Y}_t| \tag{2}$$

where Y_t: The actual *t*th instance. $\hat{Y}_t$: The forecasted *t*th instance. *n*: The total number of testing instance.

The MSE scores are utilized for further analyses of the model using the same calculation as in equation (1), without a square root of the overall computation. MAE also has the same unit as the prediction.

3.3 Fast gradient sign method

Fast Gradient Sign Method (FGSM) [38] is one of the earliest and most popular adversarial attacks in machine learning. FGSM utilizes the derivative of the model's loss function with respect to the input image to determine in which direction the pixel values of the input image should be altered to minimize the loss function of the model. Once this direction is extracted, it changes all pixels simultaneously in the direction to maximize the loss value of the prediction. For a model with the classification loss function described as $L(\theta, \mathbf{x}, y)$ where θ represents the parameters of the model, $\mathbf{x}$ is the benign input to the model (sample input image in our case), y_{true} is the actual label of our input, we can generate adversarial samples using the formula below:

$$\mathbf{x}^* = \mathbf{x} + \epsilon \cdot sign\left(\nabla_x L(\theta, \mathbf{x}, y_{true})\right) \tag{3}$$

where $\mathbf{x}$ is the clean input, $\mathbf{x}^*$ is the malicious input, L is the MSE loss function, θ is the weights of the ANN model, and ϵ controls the magnitude of the perturbation.

One last key point about FGSM is that it is not designed to be optimal but fast. That means it is not designed to produce the minimum required adversarial perturbation. Besides, the method's success ratio is relatively low in small ϵ values compared to other attack types.

4 Implementation of solar PV generation forecasting models and their validation

This paper aims to employ an ANN-based model for solar PV generation forecasting to evaluate and analyze the model performance on a regular and deceptive attack dataset so that the PV power generation will be broadly utilized in smart grid applications with higher acceptance. The ANN model is trained using the training set, and the performance is evaluated through the test set. The variation between predicted and actual values is compared using different performance metrics, such as RMSE, MSE, and MAE. In the second run, the dataset is modified with adversarial noise, and the ANN model is evaluated with the same performance metrics as in the first case.

4.1 Solar PV power generation forecasting

The PV power generation forecasting has critical importance as the integration of solar panels into the power grid depends on stable and predictable power generation. This study provides the performance of the ANN-based model in terms of RMSE, MSE, and MAE. The performance of the ANN model is calculated and shown in Table 1, i.e., RMSE (0.0874), MSE (0.0076), and MAE (0.0425) scores. A lower score is a better performance for the evaluation.

Table 1 The performance of the ANN-based model in terms of RMSE, MSE, and MAE

Model	RMSE	MSE	MAE
ANN	0.0874	0.0076	0.0425

The demonstrated PV solar forecasting model is an hour ahead of prediction. Figure 2 shows the observation and the forecast values. The red line shows the observation data and the forecast values are shown by the green line, and the filled area shows the difference between the forecast and the observation. The modeling performance is calculated by the area between the red and green lines. The better performance is in the lower area. The ANN model has the obvious advantage for PV power generation forecasting.

The best hyper-parameter settings are shown in Table 2. The table shows the details of the PV power generation forecasting ANN model architecture with the number of layers, neurons, and activation functions. We applied grid-search to find the best hyperparameters for the ANN model.

4.2 Adversarial machine learning attack against solar PV power generation forecasting

The deceptive data attack on PV power generation forecasting is important to evaluate the robustness of forecasting models. The collected data come from various sources using many sensors exposed to adversarial attacks. The performance of each model is evaluated through RMSE, MAE, and MSE metrics in the previous section. This paper investigates only the ANN model as a use case for simplicity. Table 3 shows the impact of a specific ϵ value on the RMSE/MSE/MAE performance metrics of the ANN model. ϵ is the attack power multiplication factor which is shown in equation 3. The value of ϵ ranges from 0 to 0.9. The higher the value of ϵ means the more powerful attack on the solar PV power generation forecasting. Table 3 shows that the RMSE metric is more sensitive than MSE and MAE. The RMSE value of the ANN model reaches about 0.77 when the data are modified by the attack with $\epsilon = 0.5$. The MSE and MAE values are about 0.59 and 0.68, respectively.

In this study, it is assumed that the solar PV generation, i.e., observed and forecasted, is ”0” during evening and night times. Figure 3a–c shows the observed and the forecasted data with FGSM generated deceptive inputs for $\epsilon = 0.01$, $\epsilon = 0.02$, and $\epsilon = 0.20$, respectively. The red line shows the observed data in the figure, while the green line shows the forecasted data. Figure 3a–c obviously shows that the attack power, i.e., especially a high ϵ with a low solar PV generation, causes a serious malfunction in the ANN model results.

It is assumed that it is acceptable to RMSE up to 0.1. According to Fig. 4, the solar PV forecasting model can resist any FGSM attack with $\epsilon = 0.01$. Results also indicate that the solar PV forecasting model is vulnerable to the FGSM attack. For example, the RMSE performance result with $\epsilon = 0.5$

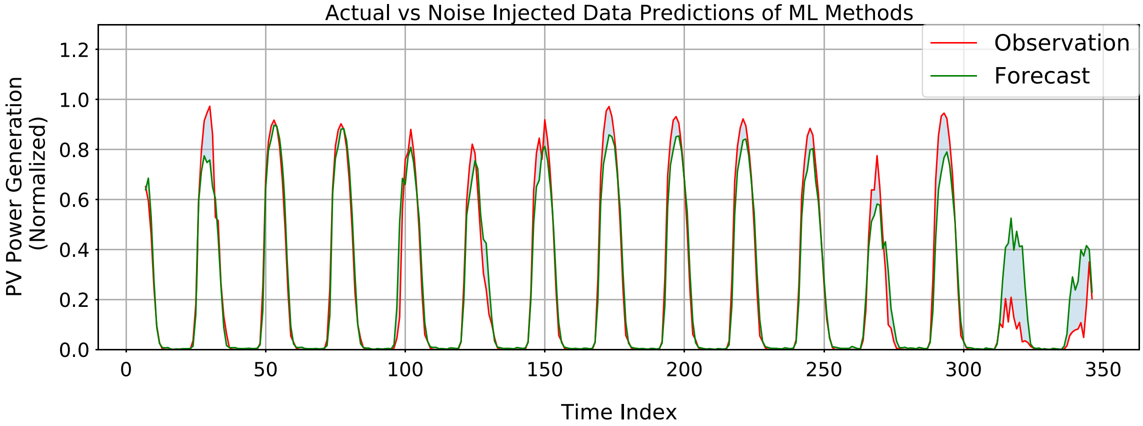


Fig. 2 ANN model forecast results with observed data

is approximately 8.85 (i.e., $\frac{0.774029(Attacked)}{0.087452(Normal)} \approx 8.85$) times more vulnerable to FGSM attack.

Table 2 The best hyper-parameters for the PV power generation forecasting ANN model

Parameter		Value
Layers	# of Neurons - 1	266
	# of Neurons - 2	42
	# of Neurons - 3	10
	# of Neurons - 4	266
	Activation	elu
	Last layer activation	Softplus
	Dropout	0.2
	Optimizer	Adam

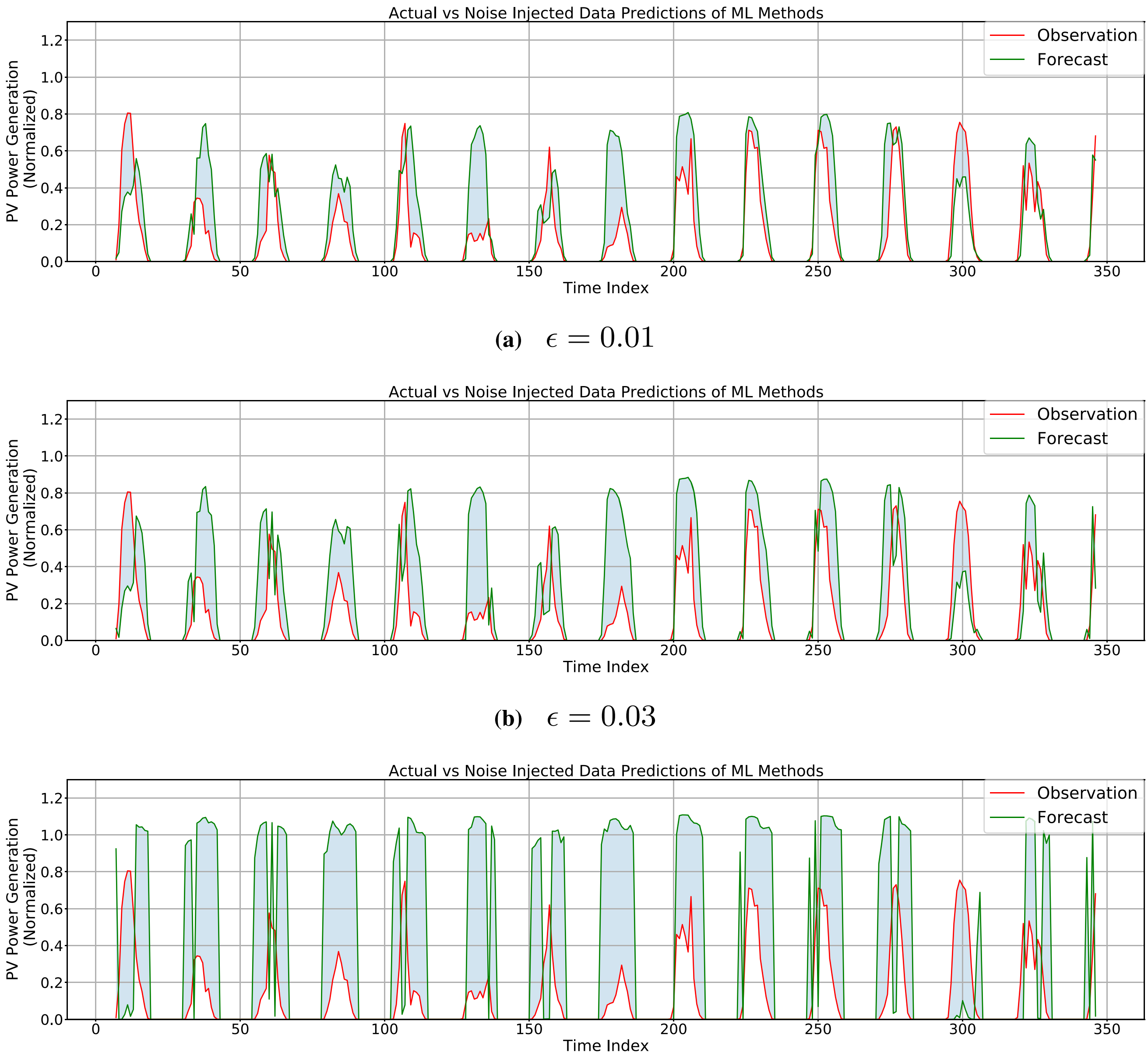
Table 3 RMSE/MSE/MAE scores of AN model for a specific ϵ value

Epsilon	RMSE	MSE	MAE
0.00	0.087452	0.007648	0.042553
0.01	0.114608	0.013135	0.064512
0.02	0.144627	0.020917	0.087192
0.03	0.176092	0.031008	0.112340
0.06	0.287484	0.082647	0.231236
0.09	0.395761	0.156627	0.342055
0.12	0.478345	0.228814	0.420943
0.16	0.561352	0.315116	0.497979
0.19	0.608172	0.369873	0.540815
0.22	0.645133	0.416197	0.574374
0.25	0.674541	0.455005	0.600870
0.28	0.698070	0.487302	0.621923
0.31	0.716937	0.513998	0.638706
0.34	0.732049	0.535896	0.652083
0.37	0.744125	0.553722	0.662733
0.40	0.753776	0.568179	0.671224
0.43	0.761485	0.579860	0.678000
0.47	0.769426	0.592017	0.684982
0.50	0.774029	0.599120	0.689034
0.53	0.777739	0.604878	0.692307
0.56	0.780742	0.609558	0.694963
0.59	0.783188	0.613383	0.697134
0.62	0.785192	0.616527	0.698922
0.65	0.786847	0.619127	0.700404
0.68	0.788220	0.621291	0.701641
0.71	0.789369	0.623104	0.702682
0.74	0.790337	0.624632	0.703563
0.78	0.791403	0.626318	0.704540
0.81	0.792068	0.627372	0.705154
0.84	0.792641	0.628280	0.705687
0.87	0.793138	0.629068	0.706151
0.90	0.793572	0.629756	0.706558

5 Results and discussion

This study demonstrated the analysis and impact of deceptive data attacks with adversarial ML on solar PV generation forecasting models. The results show that the ANN-based model without any deceptive data attacks, i.e., FGSM, provides reasonable performance for forecasting solar PV power generation. i.e., 0.0874, 0.0076, and 0.0425 in terms of the RMSE, MSE, and MAE, respectively. However, the model is very sensitive to FGSM attacks. For example, the RMSE value can go up to 0.793 under a heavy deceptive data attack, i.e., $\epsilon = 0.5$.

Figure 3a demonstrates the PV solar energy forecasting time series with respect to measured or observed solar energy data. Once the deceptive data attacks are applied to the reference time series case, as indicated in Fig. 3b, the impacts can be identified using forecasting performance metrics like RMSE, MSE, and MAE but still difficult to visually see the difference where $\epsilon = 0.3$. The impacts of massive deceptive



(a) $\epsilon = 0.01$

(b) $\epsilon = 0.03$

(c) $\epsilon = 0.20$

Fig. 3 The model predictions for the test and malicious inputs

data attacks can be observed in Fig. 3c very clearly. Figure 4 summarizes the sensitivity of the performed deceptive data attacks on the energy forecast accuracy and the boundaries between the successful and unsuccessful attacks in terms of RMSE, MSE, and MAE.

Observations derived from the results of solar PV power generation forecasting and the adversarial attack impact are outlined below:

Observation 1: ANN-based models have great potential to forecast solar PV power generation.

Observation 2: Adversarial attacks may significantly affect the performance of the forecasting models.

Observation 3: ANN-based models have a higher sensitivity to adversarial attacks, such as FSGM type.

Observation 4: It is needed to develop defense algorithms to mitigate the vulnerability of ANN-based models.

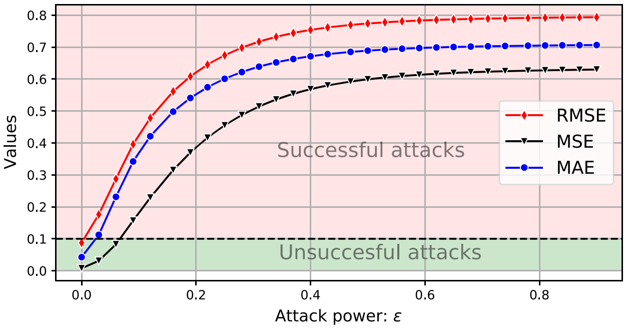


Fig. 4 Prediction performance changes with different ϵ values

6 Conclusion

Digitalization of power markets and systems has been an integral part of the power sector, where AI and ML-based implementations play an important role. Besides various advantages of such digitalization practices such as AI-based energy forecasting, such processes are getting open targets for cyber-crimes and attacks. This paper presents solar PV power generation forecasting models by utilizing widely used AI methods and investigates the impact of deceptive data attacks on solar PV generation forecast accuracy. All models are also evaluated in terms of performance metrics, i.e., RMSE, MSE, and MAE.

In the first part of the study, the proposed ANN-based models use the PV power generation and weather data to forecast the generated power from solar PV to demonstrate the reference case where no cyber attack is applied. In the second step, a set of deceptive data attacks with various levels are performed to characterize the impact of the cyberattacks on the forecast accuracy as a comprehensive sensitivity analysis to analyze the impacts of deceptive data attacks. The attack parameter, i.e., ϵ, is systematically applied to the energy forecast testing environment between 0 and .90 levels. $\epsilon = 0$ represents the case without any cyberattack, and $\epsilon = 0.9$ represents the heaviest cyberattack. According to the findings, the imposed deceptive data attacks are becoming more effective right after $\epsilon = 0.01$.

The manipulated energy forecasts might cause massive damage to the power systems and market operations depending on the importance of the application. Therefore, it is essential to identify and mitigate such kinds of cyberattacks to eliminate or minimize unwanted social, economic, and technical damages. This study demonstrated that the ANN-based method could be applied successfully to any solar PV power generation forecast model or similar energy forecasting models, while they can suffer from deceptive data attacks. It is expected that this study could be useful for engineers and researchers working on the smart grid domain who are working on a data-driven ecosystem.

Acknowledgements This work was supported in part by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development in Virginia. For more information about CCI, visit cyberinitiative.org.

References

1. US. Department of Energy FE (2002) Using distributed energy resources-a how-to guide for federal energy managers. Cogener Compet Power J 17(4):37–68
2. U.S. Solar Market and 15 States See Best Quarter Ever for Residential Solar, https://www.seia.org/news/us-solar-market-and-15-states-see-best-quarter-ever-residential-solar. Retrieved: December 2021
3. Solar Market Insight Report 2019 Q4, http://www.seia.org/research-resources/solar-market-insight-report-2019-q4, Retrieved: September 2021
4. Solar Industry Research Data, https://www.seia.org/solar-industry-research-data, Retrieved: September 2021
5. Ahmed Razin et al (2020) A review and evaluation of the state-of-the-art in PV solar power forecasting: Techniques and optimization. Renew Sustain Energy Rev 124:109792
6. Bayindir R, Colak I, Fulli G, Demirtas K (2016) Smart grid technologies and applications. Renew Sustain Energy Rev 66:499–516
7. Kuzlu M, Sarp S, Pipattanasomporn M, Cali U (2020) Realizing the potential of blockchain technology in smart grid applications. In: 2020 IEEE power and energy society innovative smart grid technologies conference (ISGT), pp 1–5. IEEE
8. Cali U, Kuzlu M, Pipattanasomporn M, Kempf J, Bai L (2021) Applications of artificial intelligence in the energy domain. In: Digitalization of power markets and systems using energy informatics. Springer, Cham. https://doi.org/10.1007/978-3-030-83301-5_7
9. Onen A (2021) Role of artificial intelligence in smart grids. Electr Eng, pp 1–1
10. Sarp S, Kuzlu M, Cali U, Elma O, Guler O (2021) An interpretable solar photovoltaic power generation forecasting approach using an explainable artificial intelligence tool In: IEEE power and energy society innovative smart grid technologies conference (ISGT), pp 1–5, https://doi.org/10.1109/ISGT49243.2021.9372263
11. Wang Huaizhi et al (2020) Taxonomy research of artificial intelligence for deterministic solar power forecasting. Energy Convers Manage 214:112909
12. Radian B (2013) Artificial intelligence techniques for solar energy and photovoltaic applications. Handbook of Research on Solar Energy Systems and Technologies. IGI Global, pp 376–436
13. Mandal Paras et al (2012) Forecasting power output of solar photovoltaic system using wavelet transform and artificial intelligence techniques. Proc Comput Sci 12:332–337
14. Kuo Ping-Huan, Huang Chiou-Jye (2018) A green energy application in energy management systems by an artificial intelligence-based solar radiation forecasting model. Energies 11(4):819
15. Dong N, Chang JF, Wu AG, Gao ZK (2020) A novel convolutional neural network framework based solar irradiance prediction method. Int J Electr Power Energy Syst 114:105411
16. Zhang J, Chi Y, Xiao L (2018) Solar power generation forecast based on LSTM, In: 2018 IEEE 9th international conference on software engineering and service science (ICSESS), Beijing, China, pp 869–872
17. Isaksson E, Karpe Conde M (2018) Solar power forecasting with machine learning techniques
18. Mellit Adel et al (2020) Advanced methods for photovoltaic output power forecasting: a review. Appl Sci 10(2):487
19. Kou J, et al (2013) Photovoltaic power forecasting based on artificial neural network and meteorological data, In: 2013 IEEE

international conference of IEEE region 10 (TENCON 2013), Xi'an, pp 1–4

20. Liu D, Sun K (2019) Random forest solar power forecast based on classification optimization. Energy 187:115940
21. Alfadda A, Adhikari R, Kuzlu M, Rahman S (2017) Hour-ahead solar PV power forecasting using SVR based approach. In: 2017 IEEE power and energy society innovative smart grid technologies conference (ISGT), Washington, DC, pp 1–5
22. Sharifzadeh Mahdi, Sikinioti-Lock Alexandra, Shah Nilay (2019) Machine-learning methods for integrated renewable power generation: A comparative study of artificial neural networks, support vector regression, and Gaussian Process Regression. Renew Sustain Energy Rev 108:513–538
23. Yuan X, He P, Zhu Q, Li X (2019) Adversarial examples: attacks and defenses for deep learning. IEEE Trans Neural Netw Learn Syst 30(9):2805–2824
24. Santana EJ, Silva RP, Zarpelão BB, Junior SB (2020) Photovoltaic generation forecast: model training and adversarial attack aspects. In: Brazilian conference on intelligent systems 2020 Oct 20, pp 634–649. Springer, Cham
25. Santana EJ, Silva RP, Zarpelão BB, Barbon Junior S (2021) Detecting and mitigating adversarial examples in regression tasks: a photovoltaic power generation forecasting case study. Information 12(10):394
26. Luo J, Hong T, Fang S (2018) Benchmarking robustness of load forecasting models under data integrity attacks. Int J Forecast 34(1):89–104
27. Chen Y, Tan Y, Zhang B (2019, June) Exploiting vulnerabilities of load forecasting through adversarial attacks. In: Proceedings of the tenth ACM international conference on future energy systems, pp 1–11
28. Tang N, Mao S, Nelms RM (2021) Adversarial attacks to solar power forecast. In: Proceedings of the IEEE GLOBECOM
29. Sarp S, Kuzlu M, Cali U, Elma O, Guler O (2021) Analysis of false data injection impact on AI based solar photovoltaic power generation forecasting. arXiv preprint arXiv:2110.09948
30. Tuna OF, Catak FO, Eskil T (2021) Exploiting epistemic uncertainty of the deep learning models to generate adversarial samples. arXiv preprint arXiv:2102.04150
31. Unsal DB, Ustun TS, Hussain SM, Onen A (2021) Enhancing cybersecurity in smart grids: false data injection and its mitigation. Energies 14(9):2657
32. Aladag M, Catak FO, Gul E (2019) Preventing data poisoning attacks by using generative models, In: International informatics and software engineering conference (UBMYK), pp 1–5, https://doi.org/10.1109/UBMYK48245.2019.8965459
33. Kurakin A, Goodfellow I, Bengio S (2016) Adversarial machine learning at scale. arXiv preprint arXiv:1611.01236
34. Rosenberg I, Shabtai A, Elovici Y, Rokach L (2021) Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Comput Surv (CSUR) 54(5):1–36
35. Catak FO, Kuzlu M, Catak E, Cali U, Unal D (2022) Security concerns on machine learning solutions for 6G networks in mmWave beam prediction. Phys Commun, p 101626
36. Cali U, Kuzlu M, Pipattanasomporn M, Kempf J, Bai L (2021) Foundations of big data, machine learning, and artificial intelligence and explainable artificial intelligence. In: Digitalization of power markets and systems using energy informatics. Springer, Cham. https://doi.org/10.1007/978-3-030-83301-5_6
37. Hong Tao, Pinson Pierre, Fan Shu, Zareipour Hamidreza, Troccoli Alberto, Hyndman Rob J (2016) Probabilistic energy forecasting: global energy forecasting competition 2014 and beyond. Int J Forecast 32(3):896–913
38. Goodfellow IJ, Shlens J, Szegedy C (2014) Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572