Performance Analysis of PCA Based Machine Learning Approaches on FDIA Detection

Kübra BİTİRGEN[1], Ümmühan BAŞARAN FİLİK[2]

[1]Department of Electronics & Communication Technology, National Defence University, Balıkesir, Turkey
[2] Department of Electrical and Electronics Engineering, Eskişehir Technical University, Eskişehir, Turkey
Corresponding Author: kubrabitirgen@eskisehir.edu.tr

Research Paper Received: 13.09.2022 Revised: 27.11.2022 Accepted: 28.11.2022

Abstract—Smart grid (SG) and its specific structures are widely taken notice of by many researchers studying power systems. This paper compares and analyzes the performance of five machine learning approaches combined with principal component analysis (PCA) to do the task of false data injection attack (FDIA) detection of an SG. For this purpose, PCA method combinations are presented and tested by using labeled data. Phasor measurement unit (PMU) data is a critical source of monitoring of progress and performance of an SG system. PMUs are perniciously influenced by FDIAs trying to manipulate the measurements without being noticed by the bad data detector (BDD) of the SG system. In one sense, the selected PMU data consisting of various features which play an important role in the control system of SG is used to analyze the characteristics of the SG system. The results show that FDIA detection is effectively accomplished. The efficiency of the proposed hybrid PCA-based various machine learning approaches is illustrated on a real measured PMU dataset. As empirical results show, Random Forest (RF) with PCA achieves the entire accuracy of 95% in FDIA detection.

Keywords—False data injection attack (FDIA), Phasor measurement unit (PMU), Principle component analysis (PCA), Smart grid (SG)

1. Introduction

1.1. Motivation and Background

The rising electricity demands, along with some attempts by electricity sellers to compete in the electricity markets, forced them to operate the electricity grids close to their physical limits. Thus, these systems are prone to serious contingencies causing serious faults [1]. SGs are advanced digital two-way power flow electrical networks being sustainable, resilient, and adaptive. They are also capable of self-healing and have good foresight for state estimation under various uncertainties. These specific properties depend on advanced tools and networks such as wide area networks, neighborhood area networks, home access networks, local area networks, wide area measurement systems (WAMS), PMUs, intelligent electronic devices, and, more [2]. However, these advanced structures of SGs are in danger because of FDIAs against these layers. Well-coordinated FDIAs are launched by unauthorized access. They can intrude into various cyber layers of the SG systems, ranging from sensing and mon-

itoring devices such as PMUs [3].

PMUs are an essential measurable unit of WAMS and are deployed in the SG communication topology [4]. PMUs are programmable to store data triggered by over/under frequency, current, or voltage events. Data collected from PMUs are transmitted to phasor data concentrators (PDCs). The PDC correlates all data into a single dataset. The dataset is streamed to the third layer that is WAMS via the applications data buffer. WAMS builds upon PMUs and has a powerful interconnection between communication links. WAMS is successfully constituted as advanced control and monitoring infrastructure. Comprehensive research is required to indicate advantages in synchrophasor measurements, miscellaneous applications of PMUs, a multitude of challenges, designing of PMU structure, placements of PMUs, and a variety of WAMS multifunctionalities. These functionalities and design issues of PMUs and WAMS should be considered from local and SG perspectives. Furthermore, IEEE standards for installation, testing, calibration, and synchronization of PMUs and PDC requirements are clarified to guide researchers [5], [6]. They also indicate the functional and performance characteristics of typical PMUs and PDCs.

1.2. Relevant Literature

An accurate state estimation for SGs equipped with PMU is a challenging issue [7]. Information Technology protocols and networks constitute the basis of the PMU networks. Various types of cyber attacks pose a problem for these kinds of systems [8] and they may falsify the control center of SGs by leading to inaccurate control decisions [9]. Learning-based methods [10], X^2 detector [11], and sum detectors [12] are important examples of detection of these kinds of attacks. Although these methods effectively detect FDIAs at determined locations of the SGs, they have not the ability for localizing the attack and correcting falsified measurements.

In [13], synchrophasor-based island mode detection systems are thought of as reliable and fast detection providers. To handle controlling networks, phasor data-based controlling for resynchronization is used [14]. Reported rates of most types of PMUs generally do not exceed the frequency of electrical grids, i.e., 50 or 60 Hz, such as relay-embedded PMUs, SEL standalone [15], and Arbiter 1133A [16].

Continuously reliable and stable operations in SGs depend on accurate state estimations. Nevertheless, synthesized FDIAs wisely circumvent conventionally BDD by initiating interim or continuous errors to state estimation mechanisms to severely damage the entire network performance and operation. To protect the system from especially such kinds of attacks, PMUs are placed at selected locations. They are generally installed on buses, substations, and transformers. They are thought of as advanced measurement units measuring phasor components of networks. The main capability of PMUs is obtaining accurate real-time synchronous phasor measurements in large area networks [17]. They are accepted as robust systems for attackers. However, it is not possible to place a PMU on each bus of the system due to the high budget requirement of the placement. For this reason, PMU placements should depend on a strategy. For instance, week locations especially some buses connected with generators need more protection. They are vulnerable to adverse attacks and physical malfunctions. In [18], the system is observed by installing PMUs at sparse locations and the remainder non PMU locations are equipped with SCADA systems. PMU outputs generally are damaged by these reasons i) an attacker attempts presented as intentional manip-

ulations or, ii) digital data processing, information retrieval stage, and storage can cause unintentional distortion [19]. However, traffic analysis attacks [20] and Reconnaissance attacks [21] are significant examples of such kind of these attack types. Serious challenges derived from the widespread usage of PMUs and the cyber security of communication networks are explained in [21]. System communication from IP addresses or open ports of PMUs and PDCs is captured by attackers. Furthermore, falsified data from the system is injected as correct data.

Synchronized PMUs play key roles to detect FDIAs and protect SG systems. Authors in [22], the Margin Setting Algorithm is used for FDIA detection based on PMU data. In the study, FDIA is built as a time and playback attack: in a time attack, measurements are resampled while in a playback attack, they are played back in reverse. Nevertheless, traditional defense strategies against FDIA are not organized by taking into account data challenges that emerged from the geographically large deployment of PMUs. Large-scale data generated by PMUs cause real-time computational and storage difficulties [23]. Against this challenge, machine learning models for the detection of FDIAs give highly satisfying results. These models are implemented to supply cyber security for SGs and sensor networks [24], [25]. The main reason for the high usage of this kind of approach depends on the fact that cyber security has become more complex and sophisticated than before. In this case, manual and traditional based models give no longer have accurate results [26].

By taking into account the Supervisory control data system, an approach that depends on sparse optimization is proposed to detect FDIA [27]. Different attack strategies against PMUs and Remote Terminal Units are discussed in [28]. To recover falsified measurements of PMUs, Alternating Direction Method of Multipliers is selected in [29]. This method can be used in larger networks but the selected parameters can change the accuracy of the recovery of the measurement.

Generally, the usage of PMUs in SGs aims to reduce the vulnerability of the grids against cyber attacks. However, some recent studies show that PMUs are not entirely in safe condition against the novel FDIAs [29], [30].

SG system operators monitor and control the system's state for the reliable and safe operation of the system. Measurements of power flow are a key underlying operation for the control system. From meter measurements, they give the system state variables. Bus voltage angles and magnitudes are the state variables. The quality of PMU voltage measurements is superior than traditional measurements. Therefore, active/reactive power injection and flow measurements, and PMUs measurements are different in the weighted least square algorithm.

1.3. Contributions and Organization

This paper outlines how these specific contributions of the study models provide better opportunities to improve the FDIA detection of an SG system.

The objective of this study is to develop a robust FDIA detection model. The selected dataset consists of attacked and unattacked events. The contributions of this paper are presented as follows:

- The selected machine learning models with PCA is proposed and validated using the selected dataset for binary class classification.
- The study highlights the contributions and benefits of the improvements in the machine learning models as complex models by adding different approaches in preprocessing stage.

The paper is organized as follows. In Section II, the method used to detect FDIA is presented.

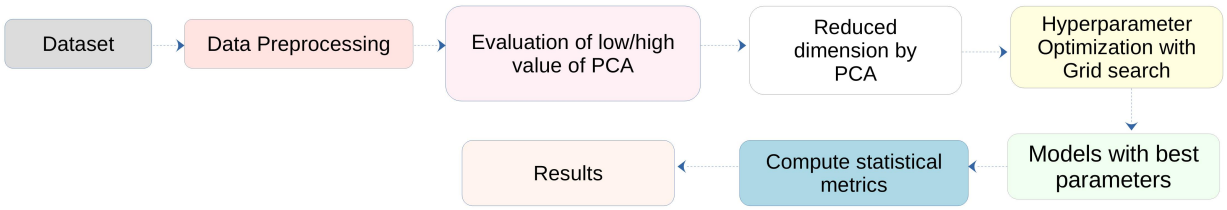

Figure 1. Work-flow of the study.

Section II also describes the selected data and proposed algorithms implemented. Then, the results for the FDIA detection system are shown in Section III. Finally, Section IV summarises the main results and ideas for the paper.

2. Methodology

As shown in Fig. 1, the methodology process is composed of important parts, data preprocessing, PCA for reducing the feature dimension, Grid search for hyperparameter optimization, implementation of the selected models, and evaluation of the models' results based on the statistical metrics. More details of this benchmark are explained below.

2.1. Description of case study

Time-synchronized data consists of PMU measurements and the status of the devices. It enables monitoring of the SG system state. Synchrophasor technology contributes to the safety of the cyber-physical environment for the data flow of the SG system. The data used in this study is taken from open-source simulated power system data [31].

The system has 4 synchrophasors measuring 29 features each for 116 PMU measurements. Three different log types exist relay logs, snort logs, and control panel logs for each PMU for an additional 12 features and 128 features in total. Table I presents a short description of each PMU and the extracted features [32].

Table 1.
Feature Description of The PMU Dataset [31].

Feature	Description
PM1 : V - PM3 - V	Magnitude of Voltage in A - C Phase
PA1 : VH - PA3 : VH	Phase Angle of Voltage in A - C Phase
PM4 : I - PM6 : I	Magnitude of Current in A - C Phase
PA4 : IH - PA6 : IH	Phase Angle of Current in A - C Phase
PA7 : VII - PA9 : VII	Phase Angle of Zero, Neg., Pos., Voltage
PA7 : V - PA9 : V	Magnitude of Zero, Neg., Pos., Voltage
PA10 : VH - PA12 : VH	Phase Angle of Zero, Neg., Pos., Current
PA10 : V - PA12 : V	Magnitude of Zero, Neg., Pos., Current
F	Frequency for relays
DF	Frequency Delta for relays
PA:Z	Apparent Impedans seen by relays
PA:ZH	Apparent Impedans Angles seen by relays
S	Status Flag for relays

The dataset [31] includes thousands of measure-

ments throughout the SG. In the selected PMU dataset, each sample is labeled as "No attacked" and "Attacked". The classification scheme is simple to discriminate the instances of samples. The scenario is run sequentially, the integrated PCA and selected machine learning models perfectly classify the data.

2.2. Mathematical background of PCA

Kernel principal component analysis (kernel PCA) is defined as a nonlinear extension of PCA in [33]. In that study, the method of PCA is presented as having high efficiency in two real-world data sets: breast-cancer cytology, handwritten digits and two-dimensional synthetic distributions. In [34], PCA is combined with a short-term wind power prediction model based LSTM model to reduce the data dimension. Reducing initial variables' dimensionality is the main purpose of the PCA. Input vectors of PCA is represented as $\mathbf{r} = [r_1, r_2, ..., r_m]$ and each vector includes n features. Feature space S and the mapping function f can be expressed as follow [35]:

$$f : r \epsilon R^n \rightarrow f(r) \epsilon S \tag{1}$$

The covariance matrix represented as C of $f(r_i)$ is computed by using (2) when the equation of $\Sigma_{i=1}^{m} f(r_i)$ equals to 0.

$$C = \frac{1}{m} \Sigma_{i=1}^{m} (f(r_i) - mean)(f(r_i) - mean)^T \tag{2}$$

The C with nonnegative λ called eigenvalues can be diagonalized where mean = $\frac{1}{m} \Sigma_{i=1}^{m} f(r_i)$. The following equation should be satisfied with values of the λ.

$$Cr = \lambda_i r \tag{3}$$

Each eigenvector r of C is easily expanded by a linearly expression, the expansion of each eigen vector r of C is seen in (4).

$$r = a_i \Sigma_{i=1}^{m} f(r_i) \tag{4}$$

To calculate the quotiety a_i, a kernel matrix K with size mxm is defined and its elements are computed as following:

$$K_{ij} = f(r_i)^T f(r_i) = f(r_i).f(r_j) = k(r_i, r_j) \tag{5}$$

The two vectors' inner product in space S is $k(r_i, r_j) =< f(r_i), f(r_j) >$. The kernel matrix K is substituted with K' called the Gram matrix as value of projected dataset $f(r_i)$ is not zero mean. K' is expressed as in the following:

$$K' = K - MK - KM + MKM \tag{6}$$

The M matrix has mxm dimension and consists of $\frac{1}{m}$ elements. To calculate the eigen value problem in (3), K' is updated in (7).

$$K'a = m\lambda a \tag{7}$$

The orthonormal eigen vectors of K regarding to the p highest positive eigenvalues $\lambda_1 \geq \lambda_2 \geq .... \geq \lambda_p$ are the vectors of a. Therefore, r_i is names as the orthonormal eigen vectors of C expressed in the (8).

$$r_i = \frac{1}{\sqrt{\lambda_i}} f(r_i) a_i \tag{8}$$

r_{new} called mapping function and r_{new} for a new vector sample to the feature space is represented as $f(r_{new})$. The projection of r_{new} onto eigen vectors r_i is calculated by (9):

$$t = (r_1, r_2, ..., r_p)^T f_{new} \tag{9}$$

The t_i that is i^{th} transformed feature of kernel PCA is computed as the following:

$$t_i = r_i^T f(r_{new}) = \frac{1}{\sqrt{\lambda_i}} a_i^T k(r_i, r_{new}) \tag{10}$$

In an attempt to construct the kernel matrix, training data will be used. Until this time, various types of kernel functions are proposed in many studies in the literature. Generally, the most preferred kernel function is the Gaussian kernel function. In this study, it is selected as the kernel function defined as follow:

$$k(x, y) = e^{-|x-y|^2/2.\sigma^2} \tag{11}$$

2.3. Machine Learning Classification with PCA

In this study, the main objective is to further observe whether the defined projections based on PCA delivers a separable space of attacked and normal (with contingencies) samples. The FDIA detection procedure depends on a binary classification algorithm. Five different machine learning models that are effectively used in literature are implemented to solve this problem.

From this dataset, each feature is involved in the preprocessing. Missing data patterns including the null values in some features describe which value is missing and observed in a dataset. As discussed in [36], there is no standard procedure for missing data patterns in the recent literature. Data preprocessing is a combination of important steps to obtain high-quality data, including data cleansing and data sampling. In the preprocessing, based on the three missing data patterns which exist mostly in the studies that are non-monotone, univariate, and monotone [37]. Data is analyzed to indicate whether missing data and unrelated parameters are in the measurements. During this process, we also perform normalization on all datasets. In the training phase, attack detection is used to generate a classifier based on the selected models, which preserves the attack feature of input vectors and classifies the attack from normal data. After training, the classifier is used to detect the attacked values.

2.3.1 Support Vector Machine

Support vector machine (SVM) has a strong learning and generalization ability, so it is generally used to solve classification problems. To separate a given set of binary labeled data, a hyperplane which is maximally distant from samples, i.e. with maximized margin is drawn [38].

$$\begin{cases} w^T \phi(si) + b = 1, y_i = +1 \\ w^T \phi(si) + b = -1, y_i = -1 \end{cases} \tag{12}$$

Each sample in the data is represented as s_i. ϕ can be defined as a projection function of s_i into a linearly separable space and a normal orthogonal vector to the hyperplanes is also represented as **w.** In this study, where σ is a scaling parameter, a Gaussian kernel realized as $\phi(s.s') = exp(-||s - s'||^2/2\sigma)$ is considered as a projection function. By minimizing the reciprocal while maintaining $y_i(w^T \phi(si) + b) \geq 1$ $\forall_i$, the distance between the two hyperplanes (i.e. $margin = 2/w^2$) in (12) is maximized to enable a decent classification process by using additional offset constant b.

2.3.2 K-Nearest Neighbours

k-nearest neighbor (kNN) is a well-known classification algorithm. The main function of this classifier is to assign a sample to the nearest possible class of K neighbors (i.e., either normal or attacked labeled measurements) [39]. In spite of its simple structure, classifier has proven high accuracy in complex classification problems.

$$d_{ij} = ||s_i - s_j||, s_j \epsilon S \tag{13}$$

where s_i and s correspond to unlabelled and prelabeled samples respectively. Based on the majority of neighbours, data is classified for $k > 1$. Various k values are tested and cross validated to increase the implementation accuracy.

2.3.3 Logistic Regression

In linearly separable data calculations, logistic regression (LR) is a classification model which has generally high certainty. It develops an idea from the statistic field where a logistic model is used to discern probability of an event or true/false class. This algorithm can also be used in multiple classes of events. The sum of all probabilities is unity. Thus in the dataset is assigned a value between 0 and 1. Based on maximum likelihood estimation, LR algorithm coefficients are determined from the training step which is done. The best coefficients are accumulated and the model estimates a value. It is for the default class if the value is very close to 1. Otherwise, for the other class, the value is very close to 0 [40].

2.3.4 Decision Tree

To solve complex classification problems, DT is a powerful machine learning algorithm. Therefore, its learning capability is successfully applied to fulfill classification and complex regression tasks in different domains of islanding detection, intrusion detection, transient stability, power systems, and cybersecurity [41]. To designate a particular class for the input, a DT determines all the possible mapping in feature space. Easier real time implementation and accurate interpretation are allowed by logical operations to correlate features with the classes. As a scenario-based normal/attack state, a binary the classification problem is addressed using DT.

2.3.5 Random Forest

RF is an ensemble classifier that consists of more than a single decision tree. Compared to other traditional classification algorithms, it has low computation error. Significant features, minimum node size, and constructed trees are used for splitting each node. There are some advantages of RF presented in the following [42]:

1) For future reference, generated forests can be saved.
2) RF overcomes the overfitting problem.
3) Variable importance and accuracy are automatically generated.

The best node is selected to split by applying randomization when constructing individual trees in RF. RF generates multiple noisy trees affecting wrong decisions and accuracy for new samples.

2.4. Hyperparameter Optimization

Hyperparameter optimization has high importance for performance of machine learning models

due to controlling the progression of the training phase. There are various hyperparameter optimization methods such as Grid search, Bayesian optimization, Random search, and Manual search. In this study, Grid search method is selected to optimize the hyperparameters.

The Grid search algorithm is widely chosen to identify hyperparameter configuration space and shows possible optimum values of hyperparameters [43]. Grid search performs by evaluating the Cartesian-product of a finite set of values selected manually. As part of this algorithm, the below steps are required to fulfill substantially to determine the global optimums:

- To search and obtain phase scale, the algorithm is implemented in a large space.
- Based on the search space experience of well-performed hyperparameter space, the search space and phase scale are narrowed.
- Step 2 is repeated several times before the optimum value is determined.

2.5. Evaluation metrics

Based on input data, machine learning classification models predict class labels as output. A definition of True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) for binary classification is given from the confusion matrix. The confusion matrix discovers the correct and incorrectly classified illustrations from the dataset samples. It consists of four categories shown in Table 2.

After completion of construction and application of the models, four evaluation metrics as accuracy, precision, recall, and F1-score are calculated. They show the effectiveness and efficiency of models used in a study. The percentage of total correct predictions is called accuracy. Precision can be defined as a percentage of correct positive predictions. A percentage of positive labeled instances predicted as positive is called recall. F1-score is a weighted average of recall and precision. The following metrics derived from the confusion matrix are used to evaluate the models in this study [40].

Table 2.
The Confusion Matrix of Binary Classification.

Actual class	Predicted class	
	Normal	Attack
Normal	TN	FP
Attack	FN	TP

1. Accuracy = (TP + TN) / Total
2. Precision = TP / (FP + TP)
3. Recall = TP / (TP + FN)
4. F1 - score = 2 TP / (2 TN + FP + FN)

3. Implementation and Result Analysis

3.1. Application Effect of PCA with the Machine Learning Models

The selected dataset consists of PMU current measurements, snort log, control panel log, and relay trip status. The information on SG operating conditions is read by an intrusion detection system to monitor the working conditions of the SG system. This study presents a machine learning-based fault diagnosis and also system monitoring in SGs. Many valuable approaches and technics have been proposed related to this issue.

In this study, the algorithm of PCA is used in combination with various machine learning approaches such as SVM, kNN, LR, RF, and DT. FDIA detection is performed via PCA and selected algorithms.

Table 3.
The machine learning models hyperparameter configuration space.

Model	Hyperparameter with search space	Optimized Parameter
SVM	$C : (0.1, 100)$	$C : 0.1$
	$kernel$: [linear, rbf]	$kernel$: rbf
	$gamma$: (0.0001, 10)	$gamma$: 0.5
kNN	$n_{neighbors}$: (3,20)	$n_{neighbors}$: 5
	$leaf_{size}$: [1, 5]	$leaf_{size}$: 1
	$weights$: [uniform, distance]	$weights$: distance
	$algorithm$: [$ball_{tree}$, $brute$, $auto$, kd_{tree}]	$algorithm$: $ball_{tree}$
LR	$penalty$: [l1, l2]	$penalty$: l2
	C: [0.001, 0.01, 0.1, 1, 10, 100, 1000]	C:1
	max_{iter} : [1000]	max_{iter}: 1000
DT	$max_{features}$: [auto, sqrt, log2]	$max_{features}$: auto
	$min_{samplessplit}$: (2,16)	$min_{samplessplit}$: 2
	$min_{samplesleaf}$: (1,12)	$min_{samplesleaf}$: 10
	$random_{state}$: [42]	$random_{state}$: 42
RF	$criterion$: [gini, entropy]	$criterion$: gini
	$random_{state}$: [42]	$random_{state}$: 42
	$n_{estimators}$: [10, 15, 20]	$n_{estimators}$: 20
	$min_{samplesleaf}$: [1, 2, 3]	$min_{samplesleaf}$: 3
	$min_{samplessplit}$: (3,8)	$min_{samplessplit}$: 7
	$max_{features}$: [sqrt, auto, log2]	$max_{features}$: sqrt

Table 4.
Results of The Hybrid Models with added PCA.

Metrics	**Single Classifiers**					**Classifiers with PCA**				
	SVM	**kNN**	**LR**	**DT**	**RF**	**SVM**	**kNN**	**LR**	**DT**	**RF**
Accuracy	0.78	0.88	0.73	0.89	0.90	0.85	0.93	0.77	0.91	0.95
Precision	0.91	0.91	0.98	0.91	0.97	0.95	0.95	0.99	0.93	0.97
Recall	0.85	0.92	0.71	0.91	0.92	0.87	0.98	0.75	0.93	0.95
F1 Score	0.89	0.93	0.88	0.93	0.95	0.91	0.95	0.83	0.94	0.97

This study is the beginning of systems to be developed for FDIA detection and protection systems and models. The defined approach deals with the entire time-series data. The dataset has two classes due to this, there is a simple decision mechanism. This proposed mechanism can give higher accuracy by using PCA to reduce the dimension of the inputs.

The effect of hyperparameter optimization on the detection performance is high and varies by the algorithm. The performance differences of the models with PCA are higher than single algorithms. Although hyperparameter optimization certainly increased the detection performance for SVM, kNN, and RF, in that case, the increment rate depends on the characteristics of the dataset and the meaningful defaults of the respective algorithm. Table 3 shows

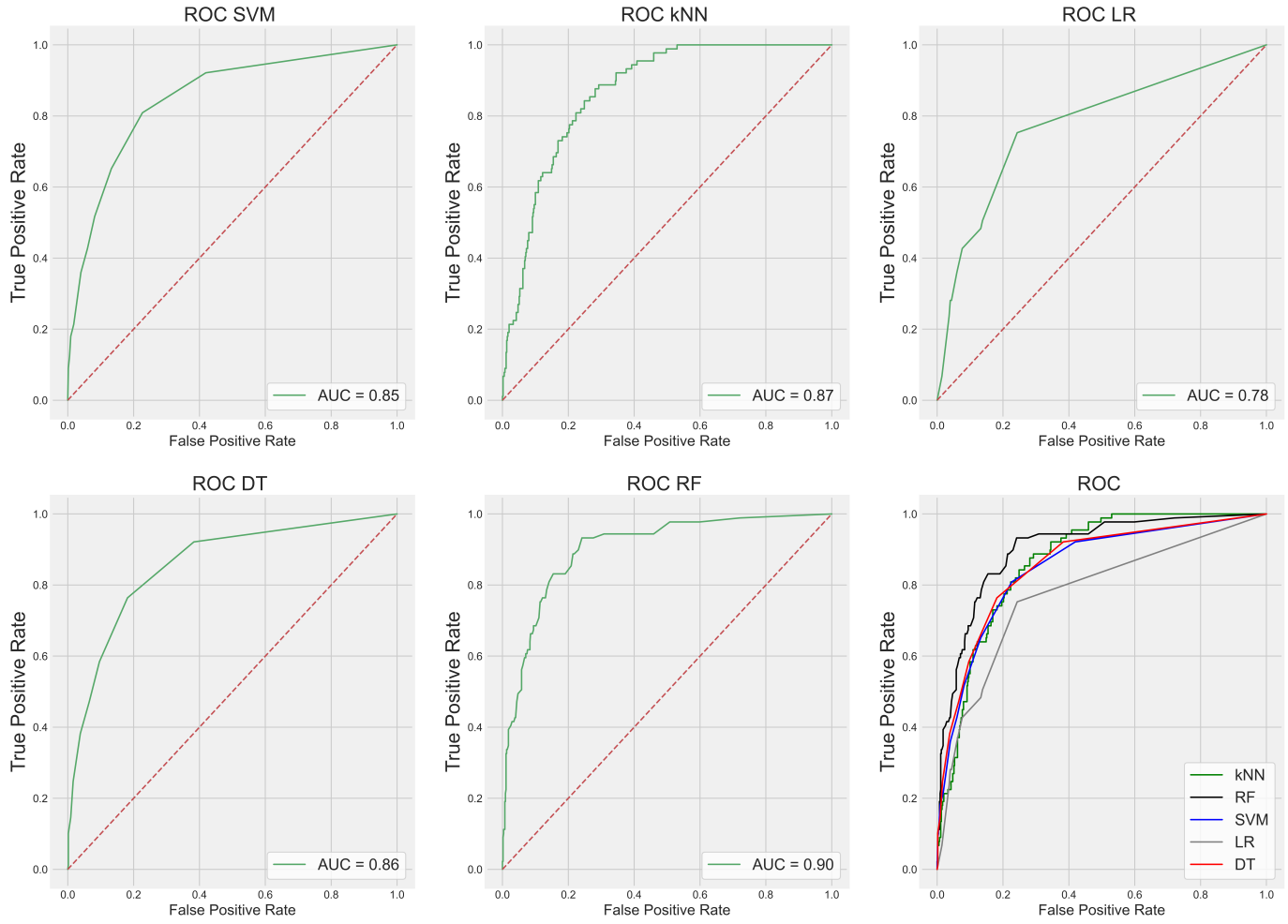

Figure 2. The comparison of the machine learning models using AUC-ROC Curve.

the hyperparameters with search space and their optimized values.

The main idea of the SVM transform the data to higher dimensional feature space and draw an optimal hyperplane maximizing the margin between the two classes. Based on the idea of proximity, kNN presents good performance and its optimized hyperparameters enhance its predictive ability. Although LR has not had a well-performed result, the grid search effect can be seen most in this model. However, most models have promising results apart from the LR model based on the AUC-ROC comparison seen in Fig.2. RF model gives the highest AUC-ROC rate and the results are 0.90. In addition, the least AUC-ROC results are obtained by LR and the results are 0.78. The results show that Grid search has an immense effect to improve the results.

The statistical results of the classifiers are shown in Table II. The evaluation of the learners is observed while accuracy gives a general indication of model performance. Based on the rate of detection accuracy, the model comparison is made. Comparative results are obtained by testing the PCA+SVM, PCA+kNN, PCA+LR, PCA+DT, PCA+RF algorithms. According to four different evaluation criteria which are precision, recall, F measure, and

accuracy, RF has the highest results. LR has the lowest accuracy and implementation performance compared. In this study, the number of samples is increased during the implementations. And then the results are observed in detail. In general, more samples need more computing time but give more realistic results. Between the four approaches, SVM has a stable increase in performance but another three approaches which are DT, kNN, and, RF surpass its performance when more amount of additional data are added. The discriminant function of some steps overlaps other functions because the main theory of SVM assumes a hyperplane separating the data points. Thus, under such inputs, it is difficult to obtain maximum performance from linear SVM. Therefore, it is concluded that for the binary classification of FDIA, the most convenient method among these selected approaches is combining RF with PCA.

The block diagram of the real-time FDIA detection scheme used in the explained approach is shown in Figure 1. An expert system can be constructed with these models to anticipate FDIA more effectively. Afterward, this investigation with exceeding calculations as PCA is all the more precise with kNN and RF calculations in the future.

The studied PCA-based machine learning models are compared with other recent detection approaches. Also, considering that the datasets are collected from a wide variety of dimensions of SG systems. For different system layers and networks, detection rates of the recent studies are between 90 and 99% [44], [45]. Deep learning methods and SVM are highly used model for FDIA detection and has different performances in FDIA detection in various studies [46], [47]. For 13-bus and 123-bus systems, the SVM model [48] presents a worse performance with a detection accuracy of less than 80% and kNN method [49] has better performance. In [49], the proposed model also reduces noise on disturbances and the masking effect of the oscillatory trends. In [50], an improved ANN-based classification model using softmax layer and ensembling supplies an effective training. This model achieves a 92% accuracy rate. In [51], knowledge discovery in databases process based on ANN is proposed. As overall 87.17% classification accuracy is achieved for the classification of fraudsters and non-fraudsters, for low-voltage consumers. In [52], for electricity theft detection, a combination of long short-term memory and convolutional neural network is used and reaches 89% accuracy. As a result, the studied model surpasses the performances of many existing approaches in the literature. However, the superiority of the proposed model compared with other models will give a more accurate result for the PMU dataset of the same system.

4. Conclusion

In conclusion, as machine learning models are very promising to detect the FDIA for safety-critical power networks, hybrid models can also be their primary FDIA detection mechanism. In this paper, PCA method combinations are presented and tested by using a labeled dataset. The main objective of this implementation is to present the performance of some machine learning models by integrating the PCA algorithm. It can be seen that the selected models give high-accuracy results but it is just a classification determining whether there is an event or not. The results show that attack detection is easily actualized but the current problem is to classify multi-labeled measurements which different kinds of cyber-attacks and power system disturbances. Ideas about FDIA detection and discrimination of the attacks will be proposed in the following studies. Furthermore, multi-labeled measurements which mean different cyber attacks

and power system disturbances will be studied. This study and its complementary studies are to be carried out in the future, both physical and cyber structures of SG systems will be taken into account by making a detailed analysis to develop effectively FDIA detection mechanisms.

5. Acknowledgements

This work was supported by the Scientific Research Projects Commission of Eskişehir Technical University under the general purpose [grant numbers 22DRP192 and 22ADP141].

References

[1] U. Adhikari, T. Morris, and S. Pan, "Wams cyber-physical test bed for power system, cybersecurity study, and data mining," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2744–2753, 2016.

[2] G. Dileep, "A survey on smart grid technologies and applications," *Renew. Energy*, vol. 146, pp. 2589–2625, 2020.

[3] M. A. Hasnat and M. Rahnamay-Naeini, "A graph signal processing framework for detecting and locating cyber and physical stresses in smart grids," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3688–3699, 2022.

[4] P. Shaw and M. K. Jena, "A novel event detection and classification scheme using wide-area frequency measurements," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2320–2330, 2020.

[5] I. P. . E. Society, IEEE *guide for synchronization, calibration, testing, and installation of phasor measurement units (PMUs) for power system protection and control*. IEEE Standards Association, 2013.

[6] P. S. R. Committee *et al.*, "IEEE guide for phasor data concentrator requirements for power system protection, control, and monitoring," *IEEE: Piscataway, NJ, USA*, 2013.

[7] Y. Chakhchoukh, H. Lei, and B. K. Johnson, "Diagnosis of outliers and cyber attacks in dynamic PMU-based power state estimation," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1188–1197, 2019.

[8] S. Siamak, M. Dehghani, and M. Mohammadi, "Dynamic GPS spoofing attack detection, localization, and measurement correction exploiting PMU and SCADA," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2531–2540, 2020.

[9] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 9, no. 5, pp. 5326–5340, 2019.

[10] K. Bitirgen and Ü. B. Filik, "A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid," *Int. J. Crit. Infrastruct. Prot.*, p. 100582, 2022.

[11] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, 2014.

[12] D. Ye and T.-Y. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2338–2345, 2019.

[13] R. Franco, C. Sena, G. N. Taranto, and A. Giusto, "Using synchrophasors for controlled islanding-A prospective application for the Uruguayan power system," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 2016–2024, 2012.

[14] T. M. L. Assis and G. N. Taranto, "Automatic reconnection from intentional islanding based on remote sensing of voltage and frequency signals," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1877–1884, 2012.

[15] Schweitzer Engineering Laboratories, "Synchrophasors." Accessed Sept. 18, 2022. [Online]. Available: https://selinc.com/solutions/synchrophasors/

[16] Arbiter Systems, "Arbiter 1133A." Accessed Sept. 18, 2022. [Online]. Available: https://www.arbiter.com/catalog/product/model-1133a-power-sentinel.php#tabs-2

[17] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[18] R. Sodhi, S. Srivastava, and S. Singh, "Multi-criteria decision-making approach for multi-stage optimal placement of phasor measurement units," *IET Gener. Transm. Distrib.*, vol. 5, no. 2, pp. 181–190, 2011.

[19] G. Khare, A. Mohapatra, and S. Singh, "A real-time approach for detection and correction of false data in PMU measurements," *Electr. Power Syst. Res.*, vol. 191, p. 106866, 2021.

[20] B. Sikdar and J. H. Chow, "Defending synchrophasor data networks against traffic analysis attacks," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 819–826, 2011.

[21] T. H. Morris, S. Pan, and U. Adhikari, "Cyber security recommendations for wide area monitoring, protection, and control systems," in *2012 IEEE Pow. Ener. Soc.*, 2012, pp. 1–6.

[22] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26 022–26 033, 2017.

[23] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*. IEEE, 2016, pp. 1–6.

[24] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS one*, vol. 11, no. 6, p. e0155781, 2016.

[25] T. Ma, F. Wang, J. Cheng, Y. Yu, and X. Chen, "A hybrid

spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks," *Sensors*, vol. 16, no. 10, p. 1701, 2016.

[26] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[27] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[28] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Trans. Industr. Inform.*, vol. 13, no. 2, pp. 411–423, 2016.

[29] M. Liao, D. Shi, Z. Yu, Z. Yi, Z. Wang, and Y. Xiang, "An alternating direction method of multipliers based approach for pmu data recovery," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4554–4565, 2018.

[30] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, 2018.

[31] Mississippi State University Critical Infrastructure Protection Center, "Industrial Control System Cyber Attack Data Set." Accessed Sept. 18, 2022. [Online]. Available: http://www.ece.msstate.edu/wiki/index.php/ICS-Attack-Dataset

[32] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *2014 7th International symposium on resilient control systems (ISRCS)*. IEEE, 2014, pp. 1–8.

[33] H. Hoffmann, "Kernel PCA for novelty detection," *Pattern Recognit.*, vol. 40, no. 3, pp. 863–874, 2007.

[34] F. Meng, Y. Fu, and F. Lou, "A network threat analysis method combined with kernel PCA and LSTM-RNN," in *2018 Tenth Int. Conf. Adv. Comput. Intel. (ICACI)*. IEEE, 2018, pp. 508–513.

[35] F. Meng, Y. Fu, F. Lou, and Z. Chen, "An effective network attack detection method based on kernel PCA and LSTM-RNN," in *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*. IEEE, 2018, pp. 568–572.

[36] D. B. Rubin and R. J. Little, *Statistical analysis with missing data*. John Wiley & Sons, 2019.

[37] T. Emmanuel, T. Maupong, D. Mpoeleng, T. Semong, B. Mphago, and O. Tabona, "A survey on missing data in machine learning," *J. Big Data*, vol. 8, no. 1, pp. 1–37, 2021.

[38] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, 2014.

[39] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in *2019 IEEE 7th international conference on smart energy grid engineering (SEGE)*, 2019, pp. 108–112.

[40] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in iot sensors in iot sites using machine learning approaches," *IEEE Internet Things J.*, vol. 7, p. 100059, 2019.

[41] P. K. Jena, S. Ghosh, E. Koley, and M. Manohar, "An ensemble classifier based scheme for detection of false data attacks aiming at disruption of electricity market operation," *J. Netw. Syst. Manag.*, vol. 29, no. 4, pp. 1–26, 2021.

[42] N. Farnaaz and M. Jabbar, "Random forest modeling for network intrusion detection system," *Procedia Comput. Sci.*, vol. 89, pp. 213–217, 2016.

[43] J. Waring, C. Lindvall, and R. Umeton, "Automated machine learning: Review of the state-of-the-art and opportunities for healthcare," *Artif. Intell. Med.*, vol. 104, p. 101822, 2020.

[44] A. Tabakhpour and M. M. Abdelaziz, "Neural network model for false data detection in power system state estimation," in *2019 IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*. IEEE, 2019, pp. 1–5.

[45] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network," *Int. J. Electr. Power Energy Syst.*, vol. 107, pp. 690–702, 2019.

[46] A. Sayghe, J. Zhao, and C. Konstantinou, "Evasion attacks with adversarial deep learning against power system state estimation," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2020, pp. 1–5.

[47] C. Konstantinou and M. Maniatakos, "A data-based detection method against false data injection attacks," *IEEE Des. Test*, vol. 37, no. 5, pp. 67–74, 2019.

[48] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, 2015.

[49] L. Cai, N. F. Thornhill, S. Kuenzel, and B. C. Pal, "Wide-area monitoring of power systems using principal component analysis and k-nearest neighbor analysis," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4913–4923, 2018.

[50] S. Manocha, V. Bansal, I. Kaushal, and A. Bhat, "Efficient power theft detection using smart meter data in advanced metering infrastructure," in *2020 4th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*. IEEE, 2020, pp. 765–770.

[51] B. C. Costa, B. L. Alberto, A. M. Portela, W. Maduro, and E. O. Eler, "Fraud detection in electric power distribution networks using an ann-based knowledge-discovery process," *Int. J. Artif. Intell.*, vol. 4, no. 6, p. 17, 2013.

[52] M. N. Hasan, R. N. Toma, A.-A. Nahid, M. M. Islam, and J.-M. Kim, "Electricity theft detection in smart grid systems: A CNN-LSTM based approach," *Energies*, vol. 12, no. 17, p. 3310, 2019.