Elliptic Envelope Based Detection of Stealthy False Data Injection Attacks in Smart Grid Control Systems

Mohammad Ashrafuzzaman
Department of Computer Science
University of Idaho
Moscow, ID, USA
ORCID: 0000-0002-2882-3821

Saikat Das
Department of Computer Science
University of Memphis
Memphis, TN, USA
ORCID: 0000-0003-1142-8259

Ananth A. Jillepalli
Department of Computer Science
University of Idaho
Moscow, ID, USA
ORCID: 0000-0003-0089-8263

Yacine Chakhchoukh
Department of Electrical and Computer Engineering
University of Idaho
Moscow, ID, USA
ORCID: 0000-0001-7263-2419

Frederick T. Sheldon
Department of Computer Science
University of Idaho
Moscow, ID, USA
ORCID: 0000-0003-1241-2750

***Abstract*—State estimation is an important process in power transmission systems. Stealthy false data injection attacks (SFDIA) against state estimation may cause electricity theft, minor disturbances or even outages. Accurate and precise detection of these attacks are very important to prevent or minimize damages. In this paper, we propose an unsupervised learning based scheme to detect SFDIA on the state estimation. The scheme uses random forest classifier for dimensionality reduction and elliptic envelope for detecting these attacks as anomalies. We compare the performance of the elliptic envelope method with four other unsupervised methods. All five models are trained and then tested with a dataset from a simulated IEEE 14-bus system. The results demonstrate that the elliptic envelope based approach provides the best detection rate and least false alarm rate among these five unsupervised methods.**

***Index Terms*—Smart grid security, False data injection attack, unsupervised learning, elliptic envelope.**

I. Introduction

Incorporation of cyber capabilities into smart power grids functionality has made these cyber-physical systems (CPS) and critical infrastructures susceptible to cybersecurity threats [1, 2]. One of the many ways a smart power grid can be attacked over the cyber network is using stealthy false data injection attacks (SFDIA) on the state estimation (SE) process in the transmission systems [3]. SE collects measurement data from sensors in remote terminal units (RTUs) in the power transmission buses through the supervisory control and data acquisition (SCADA) systems and computes voltage magnitudes and phase angles for all the buses in the transmission system [4]. A cyber-attacker can intelligently modify this measurement data after compromising RTUs or intruding into the communication channels. The falsely injected measurement data can affect the outcome of the SE and can potentially mislead operators at the power control centers to take erroneous corrective actions, which may disrupt the operation of the grid. This so-called stealthy false data injection attacks (SFDIA), a class of CPS attack, may take an important role in a coordinated attack on the power grid [5]. For example, a coordinated cyber-attack that included SFDIA components caused a power outage for about 225,000 Ukrainians in December 2015 [6].

Detection of SFDIA is an active research area. Detection methods using traditional statistical approaches and physics of state estimation have been proposed. Lately, use of data-driven machine learning-based approaches are gaining popularity [7].

A. Motivation

SFDIA are subtle modifications of bus measurement data and happen very sparsely. Therefore, SFDIA can be considered anomalies compared to measurement data corresponding to the normal grid operation. Hence, the problem can be reduced to an anomaly or an outlier detection task that can be handled by machine learning schemes.

Among many machine learning methods, the unsupervised methods are particularly suited for anomalies and outliers detection [8, 9]. Also, unsupervised learning can be applied to a wider range of datasets because they do not need labeled data for training. While it may not be very difficult to collect data during normal operation of transmission systems, "attack" data is very rarely available because attacks do not happen often. In addition to that the process of curating the data to create labeled datasets is an onerous task. Instead of being trained on data labeled with ground truth, unsupervised models work by finding the hidden similarities in different data components and attempt to group similar data instances in regions or clusters. For bi-modal data like SE measurement

978-1-7281-2547-3/20/$31.00 ©2020 IEEE

data with sparse attacks, unsupervised models create one cluster fitting most of the non-attack data (major data) and treat instances lying far outside the cluster as anomalies. Therefore, unsupervised models are particularly well-suited to discover zero-day attacks never before encountered. Elliptic envelope algorithm is an unsupervised machine learning method that uses covariance estimation on Gaussian distribution data [10]. Elliptic envelope tries to make an elliptical cluster and fits the major class instances in that. Instances far away from the cluster are then considered as anomalies. Therefore, elliptic envelope is suitable for Gaussian SE measurement data with sparse SFDIA.

B. Contributions

In this paper, we present an elliptic envelope based approach for detection of SFDIA. We fine-tune hyper-parameter values to find the model having the best detection rate with minimum false alarms. We generate datasets from a simulated IEEE 14-bus system using MATPOWER. We reduce the number of features in data to improve speed of training by utilizing importance-based feature ordering capability of random forest classifier (RFC) and selecting only the most important features. We run elliptic envelope method with different parameter values and identify the best performing model. In addition, we run four other unsupervised machine learning algorithms, namely one-class support vector machine (OCSVM) with linear kernel, OCSVM with polynomial kernel, isolation forest and local outlier factor with the dataset, and compare results from the elliptic envelope based model with those from the four other models. We find that the elliptic envelope method performs far better than other four methods.

C. Paper Organization

The remainder of this paper is organized as follows. Section II summarizes the related works. Section III briefly describes the state estimation and stealthy FDI attack. Section IV presents the elliptic envelope based SFDIA detection scheme. A set of experiments with this scheme along with the results are presented in Section V. Conclusions are presented in Section VI, followed by an acknowledgment and the references.

II. Related Work

A number of machine learning based approaches, using supervised, unsupervised, and semi-supervised learning models, have been developed to detect SFDIA on the state estimation in power transmission systems. Most machine learning based SFDIA detection considered supervised methods [11]–[17]. In this section, a few works that are based on unsupervised learning are discussed.

Ahmed et al. [18] utilized unsupervised learning method isolation forest (ISOF) to detect FDI attacks using simulated data generated by MATPOWER. They reduced the dimensionality of the data using principal component analysis (PCA). To demonstrate that ISOF performs better, they compared their results with those of a few other learning methods namely support vector machine (SVM), k-nearest neighbors (k-NN), naive Bayes (NB) and multilayer perceptron (MLP). They did not report how long it took to train the models. They reported only accuracy, precision and F1-score values. It is surprising that their results of ISOF are better than the other models which are all supervised models. Generally, supervised models perform better in terms of accuracy and precision than unsupervised models on the same dataset because they are trained with labeled data. In a separate work, Ahmed et al. [16] proposed a Euclidean distance-based anomaly detection scheme. The authors used a genetic algorithm for feature selection. They tested the proposed methods on IEEE 14-, 39-, 57- and 118-bus systems using MATPOWER generated data.

Yang et al. [19] used one-class SVM (OCSVM), robust covariance, ISOF and local outlier factor (LOF) methods. They ran these methods using data from a simulated IEEE 14-bus system. However, the dataset used has only 1000 set of measurements. They reported only accuracy and precision values for the algorithms which can be misleading metrics for anomaly detection. The most relevant metrics for sparse attack detection are sensitivity or recall, specificity, and F1-score.

Hao et al. [20] used a sparse PCA-approximation based method to detect SFDIA. Identification of real measurements with the availability of sparse datasets is achieved by using recovery functions. The recovery function's accuracy is inversely proportional to the sparsity of available data. As such, this model falls short in identifying SFDIA when data is too sparse to produce reliably accurate recovery functions. They evaluated their approach on IEEE 9-, 14-, and 57-bus systems simulated with MATPOWER.

Chaojun et al. [21] used the Kullback–Leibler distance (KLD) to calculate the distance between two probability distributions derived from variations in measurement data. When SFDIA are introduced into the measurement matrix, the probability distributions of the measurement variations will deviate from the historical data, thus leading to a larger KLD. If this deviation is larger than a threshold value then it will detect presence of SFDIA.

Ashrafuzzaman et al. [22] developed a scheme that used an ensemble of supervised methods and another ensemble of unsupervised methods. In the unsupervised ensemble, they used OCSVM, elliptic envelope, ISOF, and LOF. The ensemble-based approach gave a detection rate of 72% with a false alarm rate of 3%. They tested the scheme using simulated dataset from an IEEE 14-bus system. The main drawback of the scheme was that it takes a lot of time to train.

From the discussion above, we can see that there had been only a few works based on unsupervised learning to detect SFDIA on the state estimation in power transmission systems. In our work we are investigating the efficacy of elliptic envelope method and also determining the hyper-parameter value for optimized performance. We are also using RFC to reduce the feature dimensionality for speedy training and possible improvement in detection performance.

III. Stealthy False Data Injection Attacks on State Estimation

This section briefly describes the state estimation process in power transmission system and the SFDIA on SE.

A. State Estimation in Power Transmission Systems

State estimation is an important part of the energy management systems (EMS) at power transmission control centers. Measurement data, e.g., power flows, voltage magnitudes, and power injections, from all the buses in the system are collected by the EMS via SCADA system. Using these measurement data, SE computes the best estimation of the values of the system's unknown state variables, i.e., voltage magnitudes and phase angles for all of the different buses [4]. SE is run every few seconds to a few minutes. SE identifies and corrects contamination in the data, removes any bad data that emanate randomly from communication errors, and refines the measurements. Finally, SE provides a set of values for the state variables that are acceptable to the operator. These values are then used as inputs to other computational programs within EMS including optimal power flow, contingency analysis, unit commitment, and locational marginal pricing [23].

B. Stealthy False Data Injection Attacks on State Estimation

The SE process uses a residual-based approach to detect any anomaly or corruption in the measurement data. This residual is the difference between measurements from the sensors and the corresponding estimated values at the power control center. The residual should be zero under ideal condition which is seldom the case and a residual within a small threshold value is acceptable by the system. If the residual is above this tolerance limit then the presence of random errors due to disturbances in communication channels or sensor malfunctions are assumed. In this case, either the erroneous values are adjusted or the set of measurement data is discarded and the next set of data is analyzed.

If the change in measurement data, which may include falsely injected data by a cyber-attacker, causes the residual to be above the threshold, then those modifications are caught by the bad-data detector as part of the SE. However, if the attacker has knowledge of the power system topology, then they can modify the measurement values in such a way that the residual remains within the threshold. Obviously, these attacks will not be identified by the bad-data detector. These attacks that cannot be detected using the conventional methods based on residual analysis are called *stealthy FDI attacks* [3].

In executing an SFDI attack, the attacker first compromises the power transmission system's communication network and figures out the topology of the system. Then they compromise one or more of the sensors in the RTUs, and modify some of the measurements in a way that the changes will not be discerned by the SE process. The SE process will assume that the data is valid and will compute the state variables based on this data. The power control center operators will work with these variables and will inadvertently cause malfunctions or disruptions in the grid.

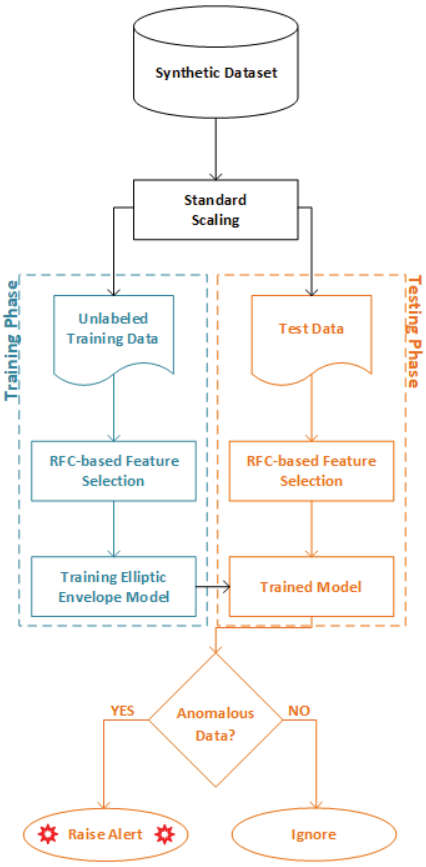

Fig. 1. The process flow diagram of the elliptic envelope based SFDIA detection scheme.

IV. Elliptic Envelope Based Detection of Stealthy FDI Attacks

This section provides an overview of the unsupervised elliptic envelope based SFDIA detection scheme. The schematic diagram depicting the process flow is given in Figure 1. The synthetic state estimation measurement data is normalized using standard scaling. Then, the dataset is split into training and testing subsets. For training phase, we employ random forest classifier (RFC) for feature reduction, and then train the model using elliptic envelope method. During the testing phase, the test data is also feature-reduced using RFC and then the model trained by elliptic envelope method is used to detect anomalous data indicating occurrence of an attack.

A. Feature Selection using Random Forest Classifier Method

The complexity and time for model training increase sharply with increase in number of features in the dataset, because of the so-called "curse of dimensionality" [24]. The number of data items, i.e., features, in SE measurement data increases with the number of buses in the system. For example, the number of features in the measurement data for an IEEE 9-bus system is 27, for an IEEE 14-bus system it is 122, and for an IEEE 300-bus system it is 1122.

It is often observed that not all the features in a dataset contribute equally in training the models. Hence, the features with the least discriminating properties can be safely eliminated from the dataset without compromising the model performance. Feature selection may lead the trained model to maximizing its performance while minimizing its running time.

In this scheme, we use random forest classifier (RFC) [25] to rank and select the features in the SE measurement dataset according to their importance in model training. Random forest is an ensemble of a large number of decision trees. Each node in the trees represents a condition on a single feature in the dataset. The dataset is split into two depending on the response to the condition. Instances with same responses end up in the same set. A measure of how much each feature contributes in making this decision is taken at the time of the split. This measure is used in ranking the features according to their contribution or importance. Then, the most important features are retained while the others are discarded from the dataset to obtain a feature-reduced dataset.

B. Attack Detection using Elliptic Envelope Method

In this scheme, unsupervised machine learning method elliptic envelope is used as an anomaly detector to diagnose SFDIA on state estimation in power transmission systems. The elliptic envelope method models data as a high dimensional Gaussian distribution with possible covariances between data-features. It attempts to delineate an ellipse so that majority of the data instances fit into the ellipse. Data instances lying far outside the ellipse are then considered anomalies or outliers and, for the current context, are marked as an attack.

The elliptic envelope method uses the FAST-minimum covariance determinant (FAST-MCD) [26] to estimate the shape and size of the ellipse. The FAST-MCD algorithm selects non-intersecting sub-sets of data and computes the mean μ, and the covariance matrix C, in each data-feature for each sub-set. The Mahalanobis distance, d_{MH}, a measure of the distance between a point P and a distribution D, is computed for each multidimensional data vector x, in each sub-set and the data are ordered in ascending order by d_{MH}. The Mahalanobis distance obtained from this estimate is used to define the threshold for determining outliers or anomalies. The Mahalanobis distance is defined by Mahalanobis [27] as:

$$d_{MH} = \sqrt{(x-\mu)^T C^{-1}(x-\mu)} \tag{1}$$

where C is the covariance matrix. If the covariance matrix is the identity matrix, then d_{MH} reduces to the Euclidean distance and to the normalized Euclidean distance if the covariance matrix is diagonal. In essence, the Mahalanobis distance measures how many σ (standard deviation) a data point is from the mean of a distribution. The FAST-MCD algorithm selects sub-sets from the original dataset, with small values of d_{MH}. Then computes mean, covariance, and the values of d_{MH} of the sub-sets. This procedure is iterated until the determinate of the covariance matrix converges. The covariance matrix with the smallest determinate from all sub-set forms an ellipse which encloses majority of the data.

In this paper, we used an implementation of elliptic envelope method provided by the scikit-learn Python package [28].

V. Experiments and Results

This section presents an experiment with the proposed approach that uses RFC for feature selection and elliptic envelope for anomaly detection, and discusses the results. This experiment evaluates the performance of the proposed detection scheme.

A. Attack Model

In this experiment, SFDIA targeting the static AC state estimation are considered. The attacker is assumed to be capable of changing the communicated data such as voltages, currents and power magnitudes in the measurement matrix. The adversary needs only selected partial knowledge of the network topology to allow them to generate a stealthy attack on a single bus. The considered attack model assumes that only one fixed bus is targeted for the entire duration of an attack.

B. Simulation and Data Generation

We used simulation of the standard IEEE 14-bus system, as shown in Figure 2, for generating data. The measurements are obtained from solving power flows using the MATPOWER toolbox [30] and adding Gaussian measurement noise. The measurements are 40 active power-flows, 14 active power-injections, 40 reactive power flows, 14 reactive power-injections and 14 voltage magnitudes giving a total of 122 measurements comprising the feature set. The dataset consists of 100,000 sets of measurement data.

C. Data Preprocessing

The synthetic dataset did not have any missing data or invalid data; so we did not have to perform any data cleaning.

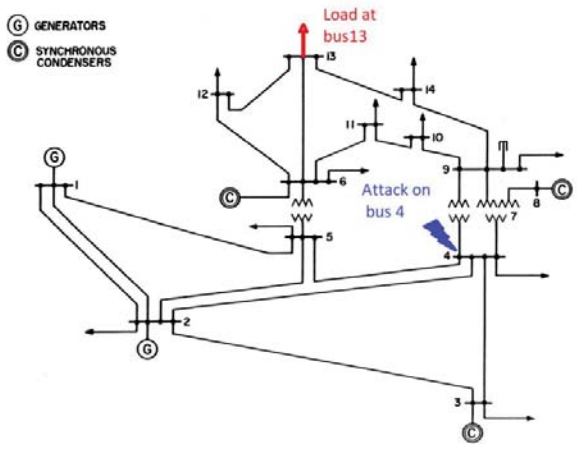

Fig. 2. Diagram of a standard IEEE 14-bus system (adapted from [29]) showing an attack that targets bus number 4.

However, we applied standard scaling to normalize the data by scaling the values in one feature to unit variance.

The dataset generated contains 90% "normal" data and 10% "attack" data implying that the dataset is imbalanced. Since the unsupervised models function as outlier or anomaly detectors, the dataset did not need balancing.

D. Feature Selection

We used the random forest algorithm on the dataset to order the features according to their contribution levels in training the machine learning model learn the data characteristics. The first 21 features in the ordered feature list have the largest variances, and therefore only these features were retained in the dataset as the predictor variables and the other features are discarded.

E. Model Training

To find an optimized elliptic envelope model, we trained the model with varying values for the hyper-parameter "contamination rate". Contamination rate represents the proportion of anomalies or outliers in the dataset. The contamination rate describes approximately how much of the data instances should sit outside of the enclosing high-dimensional ellipse that contains the majority of the data instances. In this experiment, the values of contamination rate was started at 0.001 and was gradually increased to 0.5.

To validate the effectiveness of elliptic envelope in detecting the stealthy FDI attacks, we have trained and evaluated four other popular unsupervised anomaly detection methods, namely one-class SVM with linear kernel (OCSVM_L), one-class SVM with polynomial kernel (OCSVM_P), isolation forest (ISOF) and local outlier factor (LOF).

The dataset was split in 7:3 ratio into training subset and test subset retaining the same distribution of normal and attack data. To obtain robust models without over-fitting, we used 10-fold cross-validation over randomly divided sub-sets of training data during training of the models. Then we used the test data for prediction and for measuring model performance.

F. Evaluation Metrics

Six metrics were used to evaluate the performance of the method. *Accuracy* is the percentage of true identification of both normal and attack instances over total population. *Precision*, also known as the positive predictive value, represents how often the model correctly identifies an attack. *Sensitivity*, also known as Recall, true-positive rate, or detection rate, indicates how many of the attacks the model does correctly identify. Sensitivity intuitively gives the ability of the model to detect all the attacks and precision gives the ability of the model not to mark a non-attack as an attack. *F1-score* provides the weighted average of precision and sensitivity. *False positive rate* is the rate at which the model misidentifies a non-attack as an attack and thereby raises a false alarm. *Specificity* is the inverse of FPR and measures the proportion of actual negatives or non-attacks that are correctly marked as negatives.

In an anomaly detection problem where the goal is to detect the minor class occurrences, the most important metrics are F1-score and sensitivity which, in our case, measures the proportion of "attacks" that are correctly identified as such and the FPR which measures the proportion of "non-attacks" that are incorrectly identified as "attacks" raising a false alarm.

The evaluation metrics are defined as [31]:

1) Accuracy $= (TP + TN)/Total$
2) Precision $= TP/(FP + TP)$
3) Sensitivity $= TP/(FN + TP)$
4) False Positive Rate (FPR) $= FP/(FP + TN)$
5) Specificity $= TN/(FP + TN)$ or (1 - FPR)
6) F1-Score $= 2TP/(2TN + FP + FN)$

where 1) True positive (TP): when the model correctly identifies an attack instance, 2) True negative (TN): when it correctly identifies a normal or non-attack instance, 3) False positive (FP): when a non-attack is incorrectly identified as an attack instance, and 4) False negatives (FN): when an attack is incorrectly identified as a non-attack instance.

In addition to these six metrics, the receiver operating characteristic (ROC) curve's area under the curve (AUC) score, a measure of the diagnostic ability of binary classifier systems, is reported. The ROC curves are plotted to demonstrate the detection performance of different models over all possible thresholds. The ROC curve is a graph of false positive rate (FPR) versus true positive rate (TPR).

The run times (i.e., elapsed times) for training the models were measured for comparing the speed of different models running the all-feature dataset versus the reduced-feature dataset.

G. Discussion of Results

In this section we present and discuss the results from the experiment in terms of the evaluation metrics.

We trained the elliptic envelope model with different contamination rates. The line-graph in Figure 3 shows the effect

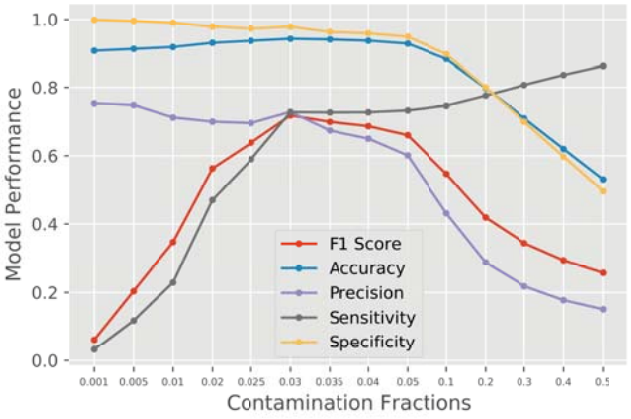

Fig. 3. Plot showing the effect of contamination rate on model performance.

TABLE I
EVALUATION METRICS VALUES FOR THE MODELS USING THE TEST DATASET WITH 21 FEATURES.

Models	F1-Score	Accuracy	Precision	Sensitivity	FPR	Specificity	ROC AUC	Elapsed Time (in seconds) 21 Features	122 Features
OCSVM_P	0.0557	0.4702	0.0332	0.1716	0.4998	0.5002	0.3358	283.16	7962.59
OCSVM_L	0.2948	0.6455	0.1800	0.8133	0.3713	0.6287	0.7210	692.14	2799.61
LOF	0.1025	0.7192	0.0723	0.1760	0.2262	0.7738	0.4748	326.25	3047.92
ISOF	0.2488	0.5318	0.1457	0.8514	0.5002	0.4998	0.6756	562.87	1919.34
EE	0.7181	0.9432	0.72.86	0.7259	0.0204	0.9796	0.7897	14.39	45.20

of contamination rate on the model performance. The models were trained with the dataset after the features were reduced to 21 from 122 using the random forest classifier. The performance numbers are gathered when the models were tested using the test dataset. We started with a contamination rate of 0.001. At this point, the accuracy and precision values are high but the most important metrics for anomaly detection, namely sensitivity and F1-score, are close to zero. With increasing contamination rates, F1-score and sensitivity increase with decreasing precision. The lines for F1-score, sensitivity and precision meet together at the 0.03 contamination rate value. This is the maximum point for both accuracy and F1-score. After the cross-over point at 0.03, sensitivity value increases but both F1-score and precision go down. Therefore, we can say that the best hyper-parameter value for contamination rate is 0.03, i.e., the model is most robust with 0.03 contamination rate. At this point, the values of F1-score is 72%, and sensitivity and precision is 73%, which means that the best optimized elliptic envelope model can reliably detect 73% of attacks, and will raise a false alarm only 2% times. The corresponding accuracy of the model is 94.32% and ROC AUC is 79%. This demonstrates that the fine-tuned model is robust, reliable, accurate and fairly strong in its detection capability. The model takes an average of 14 seconds to train with 70,000 data samples using 10-fold cross validation.

To give a comparative study of how the elliptic envelope model performs compared to other popular anomaly detection models, we trained and tested four unsupervised models mentioned above. We trained these models using the feature-reduced dataset with 21 features. The performance data is for testing with the trained models. Table I and the corresponding line-graph in Figure 4 show the values for the evaluation metrics for the five unsupervised models for the 21-feature dataset. They show that the elliptic envelope model outperforms the other four models in accuracy, precision, F1-score and specificity. ISOF has better sensitivity value than elliptic envelope. But the F1-score, precision, and specificity are very poor for ISOF; hence the model is neither robust nor reliable, and has an exorbitantly high false alarm rate of 50%.

In an additional experiment, the dataset with all 122 features were used for training the five models. It was observed that the performance numbers do not improve or degrade when the models are trained with 122 features. However, as shown by columns 9 and 10 of Table I, training with a full-feature dataset takes an average of 400% more time compared to the training time using only a 21-feature dataset.

Figure 5 shows the ROC curves for the five models. ROC curve plots false positive rate versus true positive rate. The curve corresponding to elliptic envelope has the highest AUC value of 0.79 followed closely by OCSVM_L with 0.72. OCSVM_P and LOF perform worse than random.

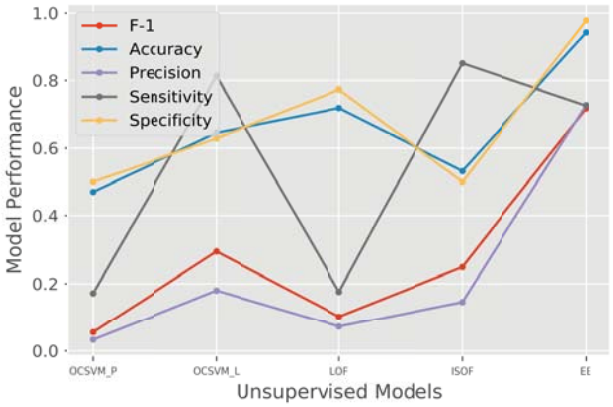

Fig. 4. Performance comparison for the five unsupervised models.

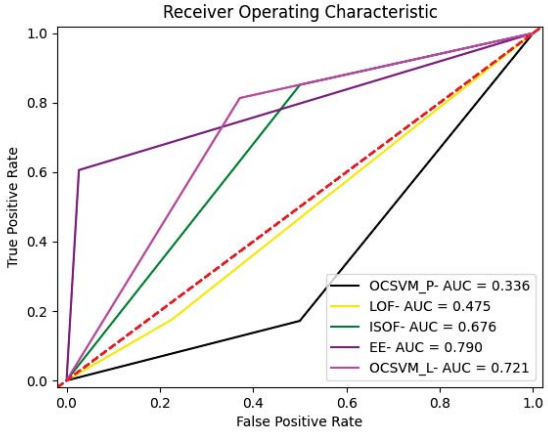

Fig. 5. ROC curves for the five unsupervised models.

VI. Conclusion

Stealthy false data injection attacks on the state estimation of a power transmission system can have severe consequences. Early, accurate and precise detection of these types of attacks are critical to prevent significant economic losses and potentially catastrophic outages. In this paper, we developed and tested a scheme for detecting SFDIA using an unsupervised machine learning method, namely elliptic envelope. We implemented the scheme using the Python machine learning libraries and tested it using a synthetic dataset from the simulation of standard IEEE 14-bus system by MATPOWER. We fine-tuned the elliptic envelope model for best performance using different contamination rates and found that the model performs best with a contamination rate of 0.03. The best model can correctly and reliably detect 73% of the attacks and will falsely raise an alarm at a rate of only 2%. We also compared the performance of elliptic envelope model with four other unsupervised models and found that elliptic envelope out-performs the other four.

Acknowledgment

This research was partially supported by an Idaho Global Entrepreneurial Mission (IGEM) Grant for Security Management of Cyber-Physical Control Systems, 2016 (Grant Number IGEM17-001).

References

[1] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[2] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45 – 56, 2018.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 13:1–13:33, 2011.

[4] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation*. New York: CRC Press, 2004.

[5] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156–168, 2017.

[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[7] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.

[8] K. Leung and C. Leckie, "Unsupervised anomaly detection in network intrusion detection using clusters," in *Proceedings of the 28th Australasian Conference on Computer Science*, vol. 38, pp. 333–342, 2005.

[9] S. Das, D. Venugopal, and S. Shiva, "A holistic approach for detecting DDoS attacks by using ensemble unsupervised machine learning," in *Future of Information and Communication Conference*, pp. 721–738, Springer, 2020.

[10] P. J. Rousseeuw, "Least median of squares regression," *Journal of the American statistical association*, vol. 79, no. 388, pp. 871–880, 1984.

[11] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2017.

[12] 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 Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, 2015.

[13] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, 2017.

[14] Y. Wang, M. Amin, J. Fu, and H. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, 2017.

[15] M. Ashrafuzzaman, Y. Chakhchoukh, A. Jillepalli, P. Tosic, D. Conte de Leon, F. Sheldon, and B. Johnson, "Detecting stealthy false data injection attacks in power grids using deep learning," in *Wireless Communications and Mobile Computing Conference (IWCMC), 14th International*, pp. 219–225, IEEE, 2018.

[16] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Covert cyber assault detection in smart grid networks utilizing feature selection and Euclidean distance-based machine learning," *Applied Sciences*, vol. 8, no. 5, pp. 772–792, 2018.

[17] M. Mohammadpourfard, Y. Weng, M. Pechenizkiy, M. Tajdinian, and B. Mohammadi-Ivatloo, "Ensuring cybersecurity of smart grid against data integrity attacks under concept drift," *International Journal of Electrical Power & Energy Systems*, vol. 119, p. 105947, 2020.

[18] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2765–2777, 2019.

[19] C. Yang, Y. Wang, Y. Zhou, J. Ruan, and W. Liu, "False data injection attacks detection in power system using machine learning method," *Journal of Computer and Communications*, vol. 6, no. 11, p. 276, 2018.

[20] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 5, pp. 1–12, 2015.

[21] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[22] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. Shiva, and F. T. Sheldon, "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning," *Computers & Security*, vol. 97, p. 101994, 2020.

[23] M. S. Thomas and J. D. McDonald, *Power System SCADA and Smart Grids*. CRC press, 2015.

[24] M. Verleysen and D. François, "The curse of dimensionality in data mining and time series prediction," in *International Work-Conference on Artificial Neural Networks*, pp. 758–770, Springer, 2005.

[25] T. K. Ho, "Random decision forests," in *Proceedings of 3rd international conference on document analysis and recognition*, vol. 1, pp. 278–282, IEEE, 1995.

[26] P. J. Rousseeuw and K. V. Driessen, "A fast algorithm for the minimum covariance determinant estimator," *Technometrics*, vol. 41, no. 3, pp. 212–223, 1999.

[27] P. C. Mahalanobis, "On the generalized distance in statistics," in *Proceedings of the National Institute of Sciences of India*, vol. 2:1, pp. 49–55, National Institute of Science of India, 1936.

[28] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[29] University of Washington, *Power System Test Case Archive*. [Online]. Available: http://www.ee.washington.edu/research/pstca/, 2018.

[30] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.

[31] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Information Processing & Management*, vol. 45, no. 4, pp. 427–437, 2009.