Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest

Saeed Ahmed, YoungDoo Lee, Seung-Ho Hyun, and Insoo Koo

***Abstract*— Being one of the most multifaceted cyber-physical systems, smart grids (SGs) are arguably more prone to cyber-threats. A covert data integrity assault (CDIA) on a communications network may be lethal to the reliability and safety of SG operations. They are intelligently designed to sidestep the traditional bad data detector in power control centers, and this type of assault can compromise the integrity of the data, causing a false estimation of the state that further severely distresses the entire power system operation. In this paper, we propose an unsupervised machine learning-based scheme to detect CDIAs in SG communications networks utilizing non-labeled data. The proposed scheme employs a state-of-the-art algorithm, called isolation forest, and detects CDIAs based on the hypothesis that the assault has the shortest average path length in a constructed random forest. To tackle the dimensionality issue from the growth in power systems, we use a principal component analysis-based feature extraction technique. The evaluation of the proposed scheme is carried out through standard IEEE 14-bus, 39-bus, 57-bus, and 118-bus systems. The simulation results show that the proposed scheme is proficient at handling non-labeled historical measurement datasets and results in a significant improvement in attack detection accuracy.**

***Index Terms*— Cyber-security, cyber-assaults, machine learning, principal component analysis, state estimation, smart grids, isolation forest.**

I. Introduction

THE emerging concept of the smart grid (SG), one of the most complex cyber-physical systems (CPSs) ever built in history, encompasses complex systems of electrical power, sensors, actuators, smart meters, computing, and state-of-the-art communications technologies. The huge dependency of power systems on a heterogeneous communications architecture in SGs heightens potential challenges to its cyber-security and resilience [1]–[6]. As depicted in Figure 1, remote terminal units (RTUs), consisting of smart meters, sensors, and actuators, are deployed to collect measurements. Conventionally, at the power control center (PCC), a device termed as bad data detector (BDD) is employed to check the consistency of the estimated measurements. A malicious user can intrude into the physical security of RTUs to retrieve and alter the classified-grid and user data. Intelligently crafting the attack vector, an intruder can compromise the integrity of the smart grid by inserting biased values into the measurement data to dodge and bypass a conventional BDD with a false, yet feasible system state [7]. Thus, initiating such a covert data integrity assault (CDIA) through deceitful measurements may result in economic loss, a partial or complete outage of the power system, or a combination of economic loss and system outages. CDIAs and their subsequent impact on the reliability of power system operations have been broadly discussed in [7]–[9]. Owing to the severe consequences of such attacks on reliable and safe operations of SGs, the need to establish a defense mechanism against CDIAs is imminent.

A. Literature Review

Extensive investigations in academia and the industry on cyber-security of smart grids have resulted in the various defense strategies. Broadly, the defense mechanism suggested in the literature can be arranged into three tiers: protection, detection, and alleviation.

Typically, protection (serving as the first tier of the defense) can avert a majority of cyber-assaults employing shielded communications and safeguarding critical data or measurements. State-of-the-art secure communications technologies and innovative protocols can be employed to alleviate the vulnerabilities [10]–[28].

If the protection tier is compromised, the attacker faces the intrusion detection system (IDS) as the second-tier defense. Detection acts as an early cautionary system, and signals operators to initiate a quick and appropriate response measure against the attack. In the literature, a detection-based defense mechanism was suggested in multiple directions. Several CDIA detection methods, which are not based on machine learning (ML) rules have been proposed [29]–[38]. Recently, efficient ML-based IDSs have been proposed in the literature in the context of CDIAs [38]–[45]. Alleviation, the third defense tier, is activated for the restoration of reliable operations once the cyber-physical (CP) assault detection alarm is received at the power control center. Numerous solutions, including bi- and tri-level optimization, game-theoretic techniques, and minimal cost solutions, have been reported in the literature to CP attack's impacts [46]–[51].

Manuscript received September 25, 2018; revised January 13, 2019 and February 24, 2019; accepted February 27, 2019. Date of publication March 5, 2019; date of current version June 14, 2019. This work was supported by the National Research Foundation of Korea (NRF) grant through the Korean Government (MSIT) under Grant NRF-2018R1A2B6001714. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Guofei Gu. *(Corresponding author: Seung-Ho Hyun.)*

The authors are with the University of Ulsan, Ulsan 44610, South Korea (e-mail: takeitez@ulsan.ac.kr).

Digital Object Identifier 10.1109/TIFS.2019.2902822

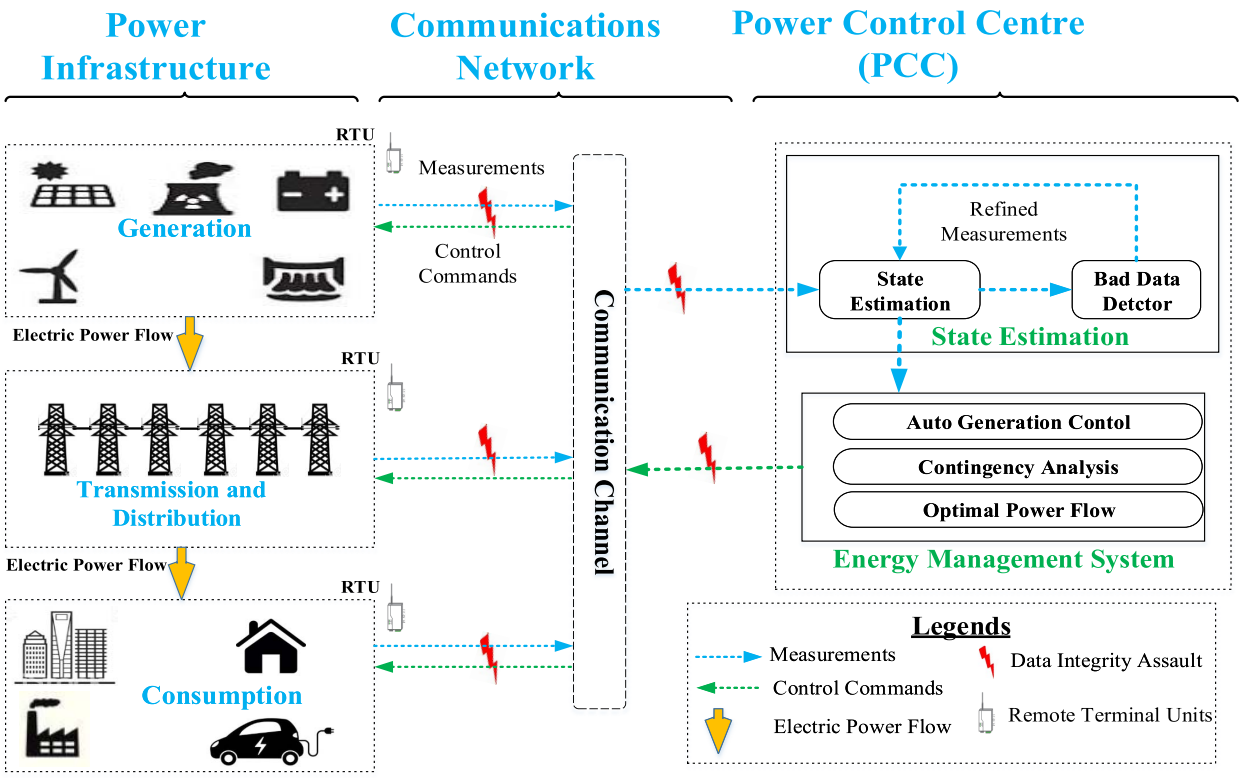

Fig. 1. Cyber-assault threat to a communications network in a smart grid.

For the detection tier in the security mechanism of SGs, ML-based approaches are becoming popular in the research community owing to their efficiency in identifying the data that have different underlying distributions. Machine learning algorithms have proven their effectiveness in the detection of intrusions and abnormalities in many fields, and we find their applications in the field of SG security as well. Identifying the malicious user activity in SG communications utilizing ML algorithms was studied in the literature [38], [39]. Ozay *et al.* [40] used several ML-based algorithms to detect CDIA on SG communications at the physical layer. They processed the samples in small sizes; however, they did not use dimension reduction (DR) methods employing the labeled data [40]. Esmalifalak *et al.* [41] employed a feature extraction (FE) method for DR and suggested a support vector machine (SVM)-based supervised learning mechanism for labeled data. Wang *et al.* [42] suggested an ML-based scheme to identify time synchronization assault in SG measurements, in which the attackers target to change the time stamps of the measured data. Ahmed *et al.* [43] employed feature selection (FS) and Euclidean-distance based supervised learning techniques to detect the CDIA in SG networks. Ahmed *et al.* [44] suggested a genetic algorithm (GA)-based feature selection (FS) technique combined with one-class, fine-tuned SVM to detect covert cyber assaults in supervised data. Table I summarizes the various defense tiers reported in the literature. In summary, ML-based CDIA detection reported in the literature mostly considered supervised ML algorithms to detect assaults on labeled data. In this paper, considering a more realistic scenario of an unlabeled, historical SE-MF data, we propose an unsupervised ML-based scheme that employs a state-of-the-art ML technique, which we call an isolation forest (*iForest*).

B. Motivation

The historical SE-MF data in the PCC is non-labeled. Furthermore, SE-MF data not affected by the CDIA are consistent with physical laws such as Kirchhoff's laws and Ohm's law, whereas the data that are compromised by a CDIA contradict with these laws. This underlying distinction, between normal and compromised data, inspires employing the *iForest*-based unsupervised anomaly detection (AD) scheme, which is considered more influential at separating anomalies from normal data with low complexity. It works on the idea of separating each point in the dataset and splits them into compromised or normal data. Because there are fewer compromised data points than normal data points, they can be isolated easily. The computational burden at PCC can be reduced by adopting a suitable DR method. Persuaded by its better performance with uniformly distributed SE-MF dataset as compared to the other unsupervised DR schemes like independent component analysis (ICA), we employed principal component analysis (PCA) for DR.

C. Contributions

In practical scenarios, the historical SE-MF database has no class labels. Labeling the archival data is a cumbersome task and needs manual effort. Therefore, in this paper, we focus on the improvement of detection accuracy for CDIAs in the

TABLE I
DEFENSE TIERS IN SG COMMUNICATIONS NETWORK AGAINST THE COVERT DATA INTEGRITY ASSAULTS

Tier	Aim	Proposed Methods	Reference
Protection	- Shield communication - Protect critical data - Reduce vulnerabilities	- Secure technologies, innovative protocols - Test beds for developed technologies - Greedy algorithms and graph-based methods to identify critical locations - Finding critical subsets of measurements - Encrypted devices at critical locations - Attack and defense cost calculations via game-theoretic approaches - Preservation and rearrangement of crucial information to hide topology - Development of distributed state estimation systems - Secure key management and distribution in AMI - Meter encryption.	[10]–[28]
Detection	Employ IDS to take quick measures against CDIA	**CDIA Detection Without Utilizing Machine Learning** - Model- and game-theoretic methods for security - Physical watermarking of control inputs - Integration of run-time semantic analysis with efficient look-ahead PF analysis - Model-based IDS system to tackle attacks on auto generation control - Integration of host-based and network-based detection - Generic use of PMU data considering whitelist/ behavior and network topology - IDS to detect PMU data assaulted by the GPS spoofing - Detection of CP assaults on AMI systems based on behavior - Distributed multi-layered IDS and early warning system - Identification with cumulative sum and quickest detection **CDIA Detection Utilizing Machine Learning:** - Utilizing supervised and semi-supervised classifiers - IDS utilizing feature selection and machine learning to improve accuracy - IDS utilizing distance-, model-, and statistics-based anomaly detection methods - Joint transformation-based detection using KullbackLeibler distance	[29]–[45]
Alleviation	Activate restore mechanism for reliable operations	- Bi-level and tri-level optimiztion - Game-theory (zero-sum, attacker-defender, zero-sum Markov games) - Line switching in the lower level of bi-level optimization - Minimal cost solutions with GA, Benders decomposition,	[45]–[50]

non-labeled SE-MF dataset. We considered an intelligently crafted CDIA in an SG communications network, which is capable of dodging the conventional BDD. To detect the CDIA, we employed a state-of-the-art anomaly detection method: the *iForest*. Additionally, we used PCA to tackle the dimensionality issue when the size of the power systems increase. The major technical contributions of this paper are summarized as follows.

- We investigate a smartly crafted CDIA on SG measurements and study how such an assault can bypass a BDD in conventional power systems.
- We compare the performance of PCA with those of other unsupervised DR methods such as ICA, to handle the rising computational intricacies in the uniformly distributed SE-MF dataset owing to the increasing sizes of power systems. PCA is found more effective to reduce multidimensional data to lower dimensions while retaining most of the information.
- Supervised machine learning algorithms are not useful in the detection of compromised unlabeled data. Therefore, we propose an unsupervised ML-based scheme to detect the presence of anomalies in the SE-MF dataset. Our scheme utilizes a cutting-edge ML algorithm: the *iForest*.
- We use standard IEEE 14-bus, 39-bus, 57-bus, and 118-bus test systems [52], [53] to evaluate the efficiency of the proposed detection scheme. Performance evaluation depicts that the proposed scheme results in higher accuracy, in comparison to binary-class SVM and other existing AD-based schemes.

D. Paper Organization

Organization of this paper is as follows. In Section II, electric power network, conventional bad data detection, and the nature of a CDIA in SG networks are explained sequentially. In Section III, we first explain the PCA-based FE mechanism, and we then present the proposed CDIA detection method. Simulation results are presented in Section IV. The concluding remarks of this paper are presented in Section V. The all abbreviations used throughout the paper are listed in Table II.

II. SYSTEM MODEL

A. Electric Power Network

The power transmission system links multiple numbers of electric generators to the consumers across a vast geographical area. Multiple lines and paths contribute to ensuring the routing of the power from any generating source to any consumer considering the frugality and expenses of the transmission path. A communication network that connects the power system and devices to the power control center (PCC), is employed for efficient control and monitoring of power system as like Figure 1.

TABLE II
NOMENCLATURE

Abbreviation	Term	Abbreviation	Term
AC	alternating current	*iForest*	Isolation Forest
AD	anomaly detection	IDS	intrusion detection system
AE	autoencoder	*k*NN	*k* nearest neighbor
AGC	auto generation control	LDA	linear discriminant analysis
AMI	advanced metering infrastructure	MF	measurement features
BDD	bad-data detection	ML	machine learning
CDIA	covert data integrity assault	MLP	multi-layer perceptron
CP	cyber-physical	NB	naive Bayes
CPS	cyber-physical system	OPF	optimal power flow
DC	direct current	PCA	principle component analysis
DR	dimension reduction	PMU	phase measurement unit
EMS	energy management system	ROC	receiver operating characteristic
FE	feature extraction	RTU	remote terminal unit
FPR	false positive rate	SE	state estimation
FP	false positive	SVD	singular value decomposition
FS	feature selection	SVM	support vector machine
GA	genetic algorithm	SG	smart grid
GPS	global positioning system	TP	true positive
ICS	independent component analysis	TPR	true positive rate
ID	intrusion detection	WLS	weighted least square

B. State Estimation

To enable viable and stable operation of a power system, state estimation (SE) serves as an essential tool, continuously monitoring system components. The smart meters or sensors deployed in RTUs report their measurements to the PCC via the communications network. At the PCC, the states (bus voltage angles and magnitudes) of the power system are estimated using meter measurements as like Figure 1.

The state estimation task is to estimate the state variables, $\theta = [\theta_1, \theta_2, \ldots, \theta_m]^T$, taking into account the meter measurements $M = [M_1, M_2, \ldots, M_n]^T$ of the power system, where n and m are positive integers, and $\theta_i, M_j \in \mathbb{R}$ for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. More precisely, the state variable vector θ is associated with the measurements M, in a non-linear or alternating current (AC) power flow model [51], [54] as follows:

$$M = h(\theta) + e, \tag{1}$$

where $e = [e_1, e_2, \ldots, e_m]^T$ is a zero-mean Gaussian measurement noise vector. The solution of AC power flow model involves high computational complexity. Therefore, with a small sacrifice of accuracy, power engineers adopt a fast and robust linear regression model, termed as direct current (DC) model under the assumption that the voltage magnitude at each bus remains close to its rated value [7], [19], [51], [54]. Thus, the model in (1) can be represented using linear regression or DC model as follows:

$$M = H\theta + \mathrm{e}, \tag{2}$$

where H is the Jacobian matrix composed of topology and impedance data in DC power flow problems and is approximated as follows [51], [54]:

$$H = \left.\frac{\partial h(\theta)}{\partial \theta}\right|_{\theta=0}. \tag{3}$$

To find the estimated state, $\hat{\theta}$ that is the best fit of the measurements, weighted least square (WLS) criteria [51] can be employed. Thus, the estimated voltage phase angle is given as

$$\hat{\theta} = (H^T \Delta H)^{-1} H^T \Delta M = WM, \tag{4}$$

where $W = (H^T \Delta H)^{-1} H^T \Delta$ and Δ is a diagonal matrix where the elements are reciprocals of the variances of sensors or meters errors.

C. Conventional Bad Data Detection

The sensor measurements may become corrupted due to many reasons such as sensor malfunctions, environmental noise, and malicious user assaults. Under the normal conditions, the sensor measurements result in an estimate of the states approaching their actual values, while a malicious assault may result in shifted away from state variables introducing a contrariety among the normal and assaulted measurements. Traditional power systems utilize a residual-based detector termed as bad data detector (BDD), to identify the corruption in the sensor measurements [51], [54]. The residual R is the difference between collected sensors measurements M and the estimated measurements $\hat{M}$ at the PCC, and it is expressed as follows:

$$R = M - \hat{M} = M - H\hat{\theta}. \tag{5}$$

Then $\left\| M - H\hat{\theta} \right\|$ is compared with a carefully selected threshold τ [51] to detect the presence of bad measurements, where $\|.\|$ denotes the L2-norm. Therefore, the hypothesis of not being assaulted is accepted if we have

$$\max_i |R_i| < \tau, \tag{6}$$

where R_i is the component of the residual vector R, τ is the threshold, and $|.|$ is the operator for taking the absolute value. Otherwise, an alarm of the presence of bad measurements is raised.

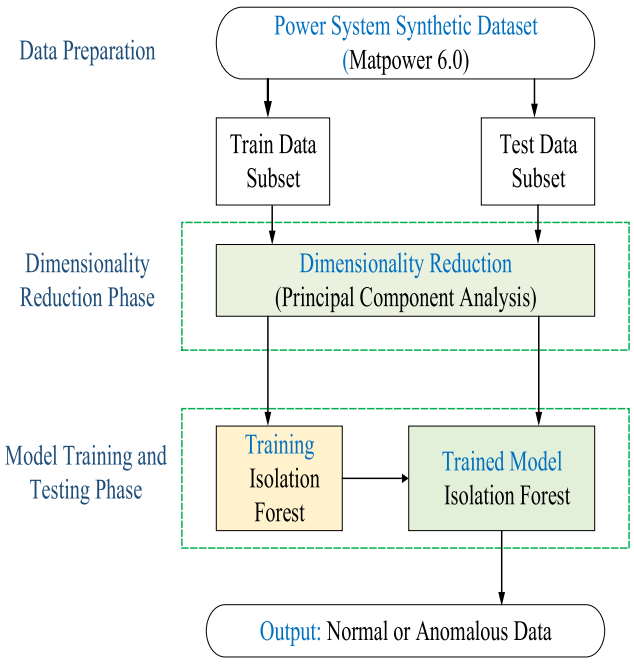

Fig. 2. A flowchart of the proposed CDIA detection scheme.

D. Covert Data Integrity Assault (CDIA)

A smart and intelligent assaulter can inject a biased value into the meter or sensor measurements by forming an assault vector, a, which sidesteps the bad data detector in the PCC [55].

If $\left\|\left(M - H\hat{\theta}\right)\right\| \leq \tau$, an assault vector, $a = \mathrm{Hc}$, can deceive the bad data detector in the PCC as follows:

$$\begin{aligned} &\left\|(M+a) - H(\hat{\theta}+c)\right\| \\ &= \left\|\left(M - H\hat{\theta}\right) + (a - Hc)\right\| \\ &= \left\|M - H\hat{\theta}\right\| \leq \tau, \end{aligned} \tag{7}$$

where assault vector a is a linear combination of the column vector of H, and τ is a pre-defined threshold. Generally, the CDIAs are categorized into two classes; load change assaults and load redistribution assaults. The design aim of both assault classes is to target one or more state variables. However, the final objective of these attacks is to dodge the legacy bad data detector in the PCC. In this paper, we assume that the assaulter has sufficient information about the topology of the SG network.

III. Machine Learning-Based Detection of CDIA

In this section, we present the proposed CDIA detection scheme. A flowchart of the proposed detection mechanism is in Figure 2. We employ PCA first for DR of SE-MF data, and then, we utilize the *iForest*-based detection scheme. PCA transforms the data into a new domain. The compromised data can be tackled effectively in this new domain compared to the original domain.

TABLE III
Dimensions of Various Standard IEEE Bus Systems

System	Variable States	Features/ Dimensions
IEEE 9-bus	8	27
IEEE 14-bus	13	54
IEEE 39-bus	38	131
IEEE 57-bus	56	217
IEEE 118-bus	117	490
IEEE 145-bus	144	1051
IEEE 300-bus	299	1122

A. Tackling the Dimensionality Issue

The SE-MF dataset, considered in this paper, consists of the features such as the active power flowing through each line and active power injected into the buses. With the increasing sizes of the power systems, the features or dimensions of SE-MF dataset increase, escalating the complexity, as shown in Table III. Therefore, visualization, analysis, and apprehension about load profile behavior become more challenging. Broadly, the techniques reported in the literature to handle the curse of dimensionality, are divided into two classes: feature selection (FS); and feature extraction (FE) [56].

The FS methods can be utilized to eliminate the least discriminating features; however, many measurements are dependent on each other or an underlying unknown variable. A single measurement may represent a combination of information about connected buses in power systems. Thus removing such a measurement would remove more information than needed.

The FE is another interesting way of analyzing load profile behavior in which we first utilize the redundant data from the power network, and we then find out the fascinating characteristics. However, FE is highly subjective, and it depends not only on the nature of the problem but also on the type of data under consideration. There is no generic FE scheme which works well in all cases. The FE techniques are further categorized as supervised, such as linear discriminant analysis (LDA) and unsupervised methods such as PCA and ICA [57]. For the unsupervised data, PCA and ICA are the candidate dimension reduction (DR) choices. The SE-MF dataset, employed in this paper, exhibits a uniform distribution and the sensor or meter measurement noise also follows the Gaussian distribution [41], [44]. The PCA is considered more suitable for the data with Gaussian distribution. Additionally, PCA provides a bit more freedom to choose the number of components to represent the dynamics of data from the variance criteria [58], [59]. Therefore, PCA is a better FE choice for Gaussian distributed SE-MF data. Conversely, ICA is considered as a good FE choice for non-Gaussian distribution of data. Contrary to PCA, there exist no criteria in the ICA method for determining the number of components that represent the dynamics of data [58], [60]. Recently, autoencoder (AE)-based DR utilizing unsupervised data [61] has gained popularity among the researchers. Development of AE-based FE and IDS may be a promising and appealing direction for future works on SG security.

PCA is a statistical tool employed to transform m-dimensional space to n-dimensional space where $m \geq n$.

The new data still contain most of the information in the large dataset. The significant point in this process is that there is no more correlation between the new data and the features are arranged by the importance of the information they carry. Maximum possible variability in the data lies in the first principal component, and then each successive component accounts for as much of the remaining variability as possible.

Mathematically, PCA is invoked to perform eigendecomposition of the co-variance matrix $\left(M^T M\right)$, which results in an ordered $(m \times m)$ eigenvector W, and eigenvalue λ. The columns of vector W are called loadings, or principal components. Finally, the transformed dataset M_T, into $(m \times r)$ dimensions, is given as follows:

$$M_T = M W_r, \tag{8}$$

where W_r is the eigen-vector with r selected columns or principal components.

Singular value decomposition (SVD), which is mathematically identical to PCA, is computationally easier, and is widely used to calculate the eigendecomposition. Performing SVD, the SE-MF dataset M is decomposed into three vectors, as follows:

$$M = U \Sigma V^*, \tag{9}$$

where U is an $(m \times n)$ unitary matrix, V is an $(n \times n)$ unitary matrix (identical to W_r), and Σ is an $(m \times n)$ rectangular diagonal matrix. The ordered and positive real entries on the diagonal of V are known as singular values of M. Now, transformed data matrix M_T is obtained as follows:

$$M_T = MV = (U \Sigma V^*)V = U \Sigma. \tag{10}$$

The truncated transformed data matrix is realized by selecting the first r columns that contain most of the information such that we have

$$M_T = U\,(:, 1:r)\,\Sigma. \tag{11}$$

B. Unsupervised Learning-Based Isolation Forest Algorithm

A CDIA on an SG communications network results in abnormal behavior of critically important information, which can be considered anomalies or outliers in the SE-MF dataset. Consistent with [62], an anomaly is a data point in time where a measurement from an RTU is significantly weird while conflicting with physical laws such as Kirchhoff's laws and Ohm's law. Predominantly, the model-based anomaly detection schemes reported in the literature, such as statistical-, clustering-, and classification-based mechanisms [63]–[65], first establish a profile of normal samples and then identify instances that vary from the normal profile as attacks. Unlike the existing approaches, the *iForest* algorithm [59], [66] is a state-of-the-art CDIA detection scheme that isolates anomalies without constructing profiles of normal data. The *iForest* algorithm is based on the fact that anomalies are data points that are few and different from other data.

Capitalizing on the facts that: 1) an assaulter would compromise only a few measurement samples in order to maintain its covertness; and 2) the compromised samples are different from the normal samples, in this paper, we propose the CDIA detection scheme based on *iForest*, called *iForest*-based CDIA detection scheme. The *iForest*-based CDIA detection scheme first sets up a powerful ensemble of isolation tree hierarchy that can isolate every single sample. Here we denote isolation tree as *iTree*. Being perceptible to isolation, the compromised RTU measurements are isolated closer to the root of the tree. On the other hand, normal measurements are isolated near the leaves of the tree. For a data-driven random tree, segregation of the data is repeated recursively until isolation of all instances. As illustrated in Figure 3, this random segregation yields considerably shorter paths for anomalous data because anomalous data are fewer in number and different from normal data. Because recursive segregation is represented by a tree structure, the path length from the root node to a terminating node determines the number of segregations to isolate a measurement sample. Individual trees are created with various sets of partitions, because each partition is created randomly. To rank a measurement in the SE-MF dataset employing the *iForest* algorithm as normal or compromised, we explain the hierarchy of *iTrees*, the concept of the path length, and the anomaly score, as follows:

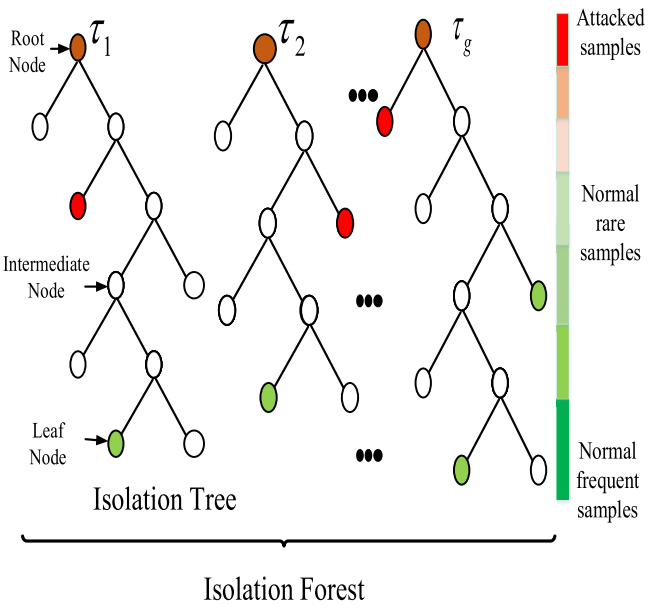

Fig. 3. Isolation forest architecture.

1) Isolation Tree: An *iTree* is a complete binary tree, with each node explicitly branched into zero or two child nodes. An *iTree* isolates each distinct instance to a leaf node after it is grown entirely as like Figure 3. Let $M_T = [M_1, M_2, \ldots, M_n]$ be the transformed SE-MF dataset after applying PCA, consisting of n measurement samples where each sample consists of r features. To construct an *i*Tree, we utilize a subset of the SE-MF dataset, $M'_T \subset M_T$, consisting of ψ instances, and perform a test by randomly selecting a feature, x_j where $j \in \{1, 2, \ldots, r\}$, and a split value, y such that the test $x_j < y$ can divide the data points into two child nodes, T_e and T_w. This procedure is recursively repeated until one of the following conditions is met: (1) $\left|M'_T\right| = 1$, the tree

TABLE IV
SYMBOLS AND NOTATIONS UTILIZED IN *iForest* ALGORITHM

Symbol	Description
M_T	transformed SE-MF dataset consisting of r features
M_j	measurement sample j, where $j \in \{1, 2, ..., n\}$
n	number of measurements in SE-MF dataset, $n = \|M_j\|$
ρ	sub-sampling size
$P(M_j)$	path length of sample M_j
x_j	a random feature, $j \in \{1, 2, ..., r\}$
τ	a tree or a node
s	a function to get the anomaly score
ψ	total number of instances in a subset
$c(\psi)$	average path length of unsuccessful searches in a BST for a given ψ
$E\left(P\left(M_j\right)\right)$	path length averaged over a collection of *i*Trees

cannot grow any more, (2) all the data in M'_T carry the same values. Thus, the number of internal nodes is $\psi - 1$, the number of leaf nodes in an *iTree* is ψ, and the total number of nodes is $2\psi - 1$. Therefore, memory space increases linearly with ψ. The description of symbols and notations utilized to explain the *iTree* are illustrated in Table IV. The anomaly detection scheme determines a ranking that depicts the degree of anomaly. The points that are ranked at the top of the list are considered anomalies. Next, we discuss the path length and anomaly score which construct the basis for the detection of the anomalous data.

2) Path Length: The number of edges that a sample point, M_j, passes through in an *iTree* from the root node to the terminating node is termed the path length, $h(x)$. In other words, the number of splittings needed to isolate a sample is the path length starting from the root node and terminating at the leaf node during recursive splitting in a tree hierarchy. This path length, averaged over a forest of such random trees, is a measure of normality. In this paper, we utilize the path length as a metric of the degree of susceptibility to isolation. For particular samples in a random forest, the following points hold:

- a deep path length corresponds to low susceptibility to isolation, and
- measurement samples with shorter path lengths correspond to high susceptibility to isolation.

3) Anomaly Score: Like other anomaly detection methods, an anomaly score is required to make a decision about a measurement sample in *iTree*. In an *iTree*, the maximum feasible height increases on the order of ψ, but the average height increases on the order of $\log(\psi)$. Normalization of the path lengths from models of different sub-sampling sizes utilizing ψ or $\log(\psi)$ is not bounded, and direct comparison of path lengths is not possible. Taking advantage of their complete identical structure with *i*Trees, we borrow analysis form binary search trees to estimate the average path length, $c(\psi)$, of an *i*Tree [66]–[68]. Anomaly score s of instance M_j is defined as follows [67]:

$$s\left(\psi, M_j\right) = 2^{-\frac{E\left(P\left(M_j\right)\right)}{c(\psi)}}, \tag{12}$$

where $P(M_j)$ is the path length of sample M_j, $E(P(M_j))$ is the path length averaged over a collection of *iTrees*, and $c(\psi)$ is the average path length of unsuccessful searches in a binary search tree for a given ψ. The exclusive relationships between the average path length over a collection of *iTrees* $E(P(M_j))$, and values of the anomaly score are given as follows:

- when $E\left(P\left(M_j\right)\right) \to 0, s \to 1$
- when $E\left(P\left(M_j\right)\right) \to \psi - 1, s \to 0$
- when $E\left(P\left(M_j\right)\right) \to c\left(\psi\right), s \to 0.5$.

Utilizing the anomaly score s, we can make a value judgment about the instances. The instances are regarded as compromised if they return an anomaly score closer to 1; the instances are safely categorized as normal if they have much smaller anomaly score than 0.5; the entire sample has no clear or distinct anomaly when all the instances return an anomaly score of 0.5. In the paper, we use $s = 0.5$ as the value of the anomaly score since it serves as the best threshold to achieve the highest accuracy.

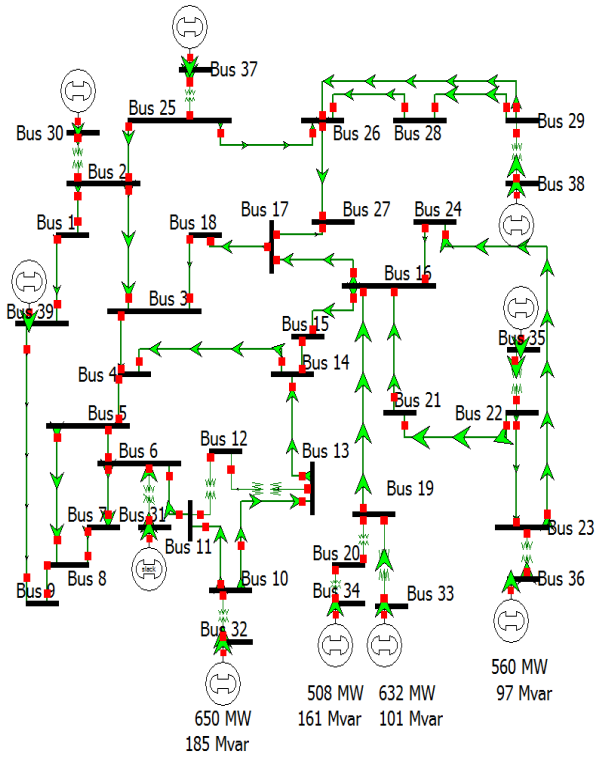

Fig. 4. Standard IEEE 39-bus system [53].

IV. EXPERIMENTAL RESULTS

In this section, we evaluate the performance of the proposed *iForest*-based CDIA detection scheme.

A. Power System Data Generation

We employed standard IEEE 14-, 39-, 57-, and 118-bus systems to validate the efficiency of the proposed algorithm. Experiment results were averaged over 10 iterations for each bus system. To generate the configuration of these standard IEEE test systems and specifically the Jacobian matrix, we utilized the MATPOWER 6.0 toolbox [52]. The measurements M, are generated using the operating points of the test systems

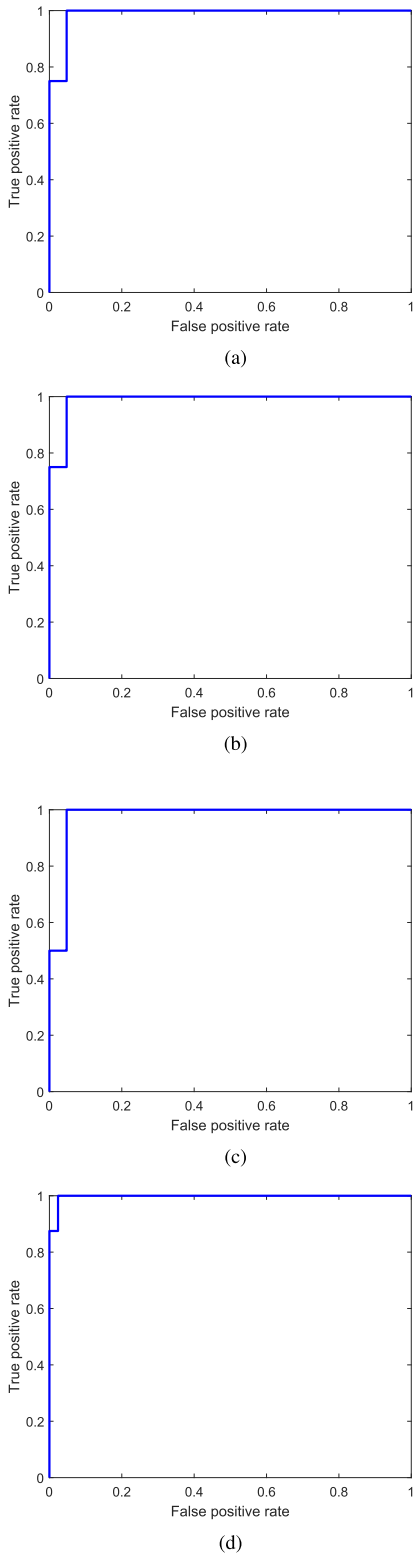

Fig. 5. The ROC curves of the proposed *iForest*-based CDIA detection scheme in standard IEEE 14-, 39-, 57- and 118-bus systems. (a) IEEE 14-bus system. (b) IEEE 39-bus system. (c) IEEE 57-bus system. (d) IEEE 118-bus system.

provided in MATPOWER case files. We used the DC power flow analysis to approximate the state vectors employed in the AC power flow model. The state variable vector θ, for a κ-bus system, consists of $(\kappa - 1)$ bus voltage phase angles, and the measurement vector M is composed of active power flows in the lines and active power injections into the buses. To carry out an impartial comparison with a real-world power grid scenario, we used stochastic loads with uniform load distributions similar to [41], i.e., ranging between $[0.9 \times L_0 - 1.1 \times L_0]$, where L_0 is the base load. Active power flow in the branches and active power injections into the buses are the features employed in these simulations. To generate the attack, we followed the attack model utilized in [55] by assuming that the assaulter has complete information about the power grid topology and can access a limited number of meters or sensors. Figure 4 illustrates the IEEE 39-bus system [53]. Owing to the limited space, we did not include the figures of the other IEEE bus systems employed this work.

B. Parameter Tuning for Detection Models

For *iForest* implementation, we divided the simulation into two stages: training the *iForest* model and evaluating it. To train the model, we utilized 80% of the SE-MF data encompassing both normal and compromised measurements. We utilized 20% of the data to test the trained model. The subsampling size, ψ and ensemble size (or the number of trees, t) are the important input parameters to improve detection accuracy. We observed that *i*Forest reliably detects CDIAs in the SE-MF dataset at $\psi = 256$. A further increase in ψ did not improve the detection accuracy. Similarly, we use $t = 100$ as the number of trees since the path lengths converge well before this value.

To validate its effectiveness in the detection of CDIA in SGs, we compared the proposed scheme with numerous ML algorithms discussed in the literature such as SVM, *k*NN, NB, and MLP [12], [40], [41], [43], [44]. Each detection algorithm has different tuning parameters, which play an essential role in producing high accuracy. In the tuning process, we tested a series of values and determined optimal parameters based on the highest overall detection accuracy for each reference model. In this paper, the accuracy and F_1 score results under the optimal parameters of each model were used as performance metrics. For the SVM, radial basis function (RBF) kernel shows good performance and is generally utilized [41], [45]. We, therefore, employed the RBF kernel to implement the SVM algorithm. We used Bayesian optimization to choose from an extensive range of values, i.e., between 10^{-5} and 10^5, to search optimal values for the kernel width parameter σ and penalty parameter C. Applying this procedure to all standard IEEE bus systems utilized in this paper, we found the optimal values of $C = 5.648$ and $\sigma = 6.67$ for the standard IEEE 118-bus system, $C = 10.8$ and $\sigma = 8.28$ for the standard IEEE 57-bus system, $C = 11.97$ and $\sigma = 9.25$ for standard IEEE 39-bus system, and $C = 13.8$ and $\sigma = 8.76$ for the 14-bus system. The *k*NN approach calibrates the dataset, by finding a group of k samples that have the shortest distance to the unknown sample. The label of unknown samples is determined from these k samples, by exploiting the average of the class attributes of the k nearest neighbors. After examining the k values from 1 to 10 to find out the optimal k value for all

TABLE V

ACCURACY AND F_1 SCORE OF THE PROPOSED DETECTION SCHEME WITH DIFFERENT DIMENSION OF PCA FOR STANDARD IEEE 14-, 39-, 57- AND 118-BUS SYSTEMS

System	Dimensions/ PCs	Accuracy (%)	F_1 score
IEEE 14-bus	2	93.84	0.9341
	3	93.35	0.9310
	4	93.00	0.9291
	5	77.85	0.7800
	6	62.95	0.6121
IEEE 39-bus	2	93.89	0.9351
	3	93.32	0.9313
	4	92.02	0.9200
	5	78.43	0.7843
	6	63.95	0.6291
IEEE 57-bus	2	94.20	0.9366
	3	93.65	0.9324
	4	93.23	0.9312
	5	77.75	0.7785
	6	58.99	0.5542
IEEE 118-bus	2	95.06	0.9516
	3	93.54	0.9260
	4	91.16	0.9167
	5	77.75	0.7734
	6	75.45	0.7552

training sample sets, the number of neighbors is considered 6 due to better accuracy. The selection of a suitable distance criterion is one of the critical parameters in the *k*NN algorithm. We utilized the Manhattan distance [59] to implement *k*NN algorithm. We also compared the proposed scheme with multilayer perceptron (MLP) utilizing the default parameters values provided in the algorithm [69].

C. Dimension Reduction With PCA

Exploiting the fact that the SE-MF data are highly correlated, a suitable DR technique like PCA can adequately lessen the number of dimensions. In this subsection, first, we analyze the accuracy and F_1 score of the proposed scheme for different dimensions of PCA. Then, we compare the performance of the proposed detection scheme with PCA and ICA for various dimensions.

From Table V, we see that for standard IEEE 14-, 39-, 57-, and 118-bus systems, the reduced space representation with first two principal components (PCs) exhibits good detection accuracy and F_1 score for the proposed scheme. It is also apparent that the addition of more PCs does not contribute to improving the detection accuracy of the proposed scheme. Maximum information about the original data resides in the first PC and then in the second PC. Therefore, it is a compelling choice to select the first two PCs for the proposed detection scheme. In the simulated dataset, maximum variance (99%) is retained employing only a two to three principal components. Next, we compare the performance of PCA and ICA for the detection accuracy and F_1 score of the proposed detection scheme. It is evident from the Table VI that the proposed detection scheme has higher performance with the PCA than with the ICA for standard IEE 14-, 39-, 57-, and 118-bus systems. Without the loss of generality, the SE-MF dataset has a uniform distribution, and measurement noise also follows the Gaussian distribution. Therefore, PCA might be a preferable DR approach for the SE-MF dataset.

TABLE VI

PERFORMANCE COMPARISON BETWEEN PCA AND ICA FOR CDIA DETECTION

System	PCA-based detection			ICA-based detection		
	PCs	Accuracy	F_1 score	ICs	Accuracy	F_1 score
14-bus	2	93.84	0.9341	2	93.01	0.9313
	3	93.15	0.9310	3	92.98	0.9301
39-bus	2	93.89	0.9351	2	92.92	0.9311
	3	93.32	0.9313	3	92.35	0.9221
57-bus	2	94.20	0.9366	2	93.10	0.9316
	3	93.65	0.9324	3	92.25	0.9175
118-bus	2	94.67	0.9441	2	93.36	0.9341
	3	93.54	0.9260	3	92.12	0.9214

D. ROC Curves

The ROC curve summarizes the performance of a detection scheme over all possible thresholds. The ROC curve is realized by plotting the false positive rate (FPR) against the true positive rate (TPR) employing the confusion matrix. The confusion matrix interprets the performance of the detection model for a test dataset in which the true or actual values are known.

- The probability that normal data are incorrectly classified as attacked is FPR. It serves as a measure of specificity for the proposed detection scheme.
- The probability that attacked data are correctly identified as attacked data is the TPR, and it is used as a measure of sensitivity.

Figure 5 illustrates the ROC curves for the proposed assault detection scheme, utilizing the standard IEEE 14-, 39-, 57-, and 118-bus systems. Figures 5(a), (b), (c), and (d) show that the area under the curve is closer to 1 in all test bus cases. A detection accuracy near 1 validates the good performance of the proposed scheme. In the next subsections, we present the detection accuracy and F_1 score achieved by the proposed scheme.

E. Accuracy and F_1 Score

A standard way to gauge the efficiency of the anomaly detection algorithm is by calculating the accuracy of the scheme. It is a single-number performance metric of the detection algorithm, and can be calculated as follows:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{Total Population}}, \tag{13}$$

where true positive (TP) are the points that the proposed algorithm detects as positive samples and that are, in fact, positive. Similarly, true negatives (TN) are the samples that the proposed algorithm detects as negative samples and that are, in fact, negative.

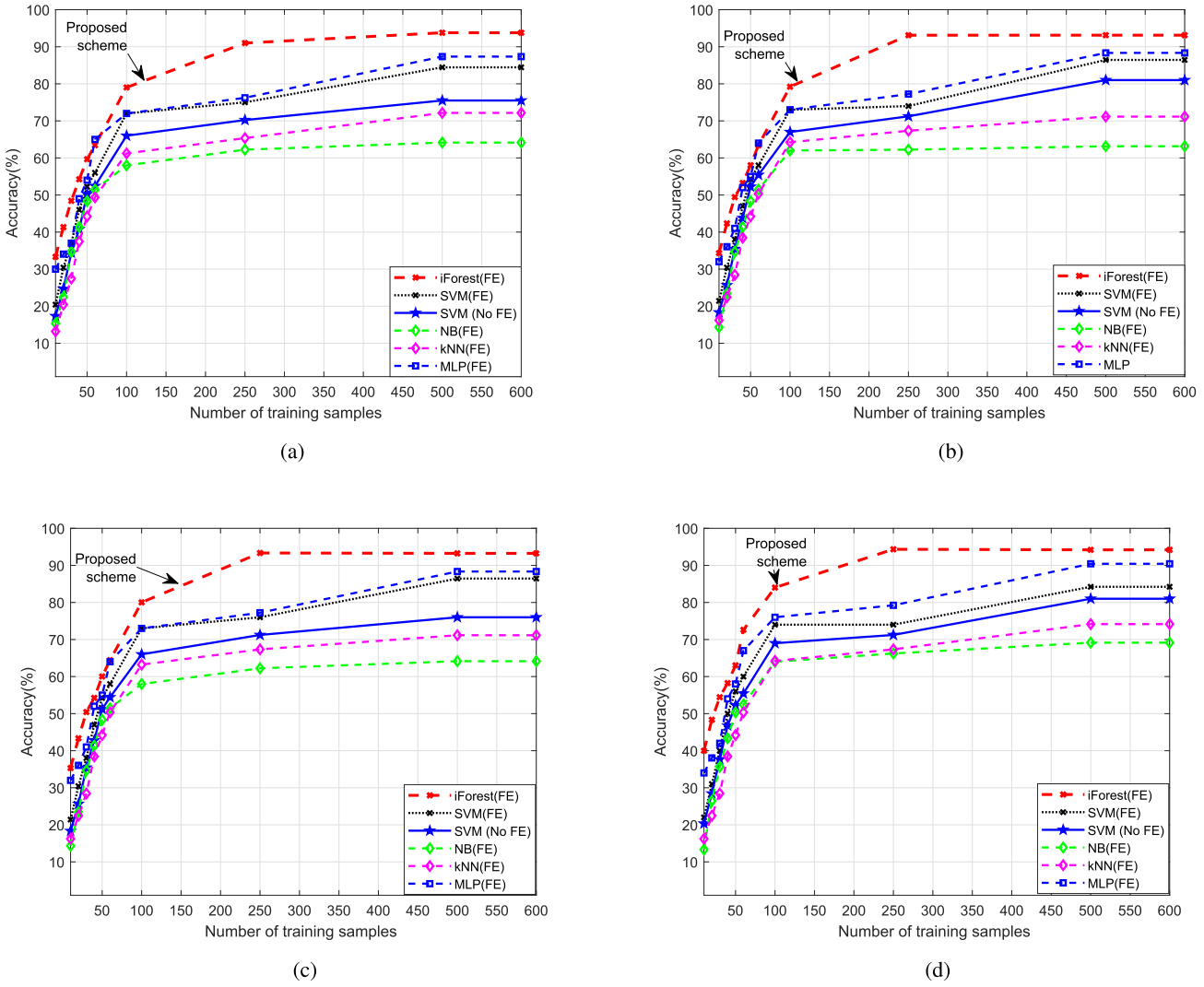

Fig. 6. The accuracy of the proposed *i*Forest-based CDIA detection scheme with varying numbers of training samples. (a) IEEE 14-bus system. (b) IEEE 39-bus system. (c) IEEE 57-bus system. (d) IEEE 118-bus system.

The F_1 score is a gauge of precise detection of the subject dataset. The F_1 score is obtained as follows:

$$F_1 = 2\left(\frac{P_r R_e}{P_r + R_e}\right) \tag{14}$$

where P_r is precision and is calculated as follows:

$$P_r = \left(\frac{\text{TP}}{\text{Predicted Positive}}\right). \tag{15}$$

The samples that the proposed algorithm detects as positive samples, and that are, in actual, positive are termed true positive (TP). Predicted positives may include both attacked and normal sample points, but the algorithm detects them all as positive. R_e is recall, calculated as follows:

$$R_e = \left(\frac{\text{TP}}{\text{Actual Positive}}\right). \tag{16}$$

Figures 6 and 7 show the comparison of accuracy and the F_1 score between the proposed *iForest*-based CDIA detection scheme and existing ML schemes for various IEEE standard bus systems based on varying the number of training samples. From Figures 6 and 7, it is observed that the proposed *iForest*-based scheme with fine-tuned parameters outperforms other schemes and requires fewer training samples to attain a higher accuracy and F_1 score. It is also evident from Figures 6 and 7 that the performance of the learning model can be enhanced by increasing the amount of learning data.

MLP shows good CDIA detection accuracy and F_1 score, and its performance is improved moderately by increasing the number of training data. Nonetheless, MLP has a slow training speed and is hard to tune.

The SVM has a lower detection accuracy and F_1 score compared to the proposed scheme. It is also evident that a large number of training samples are required to train the model to achieve good accuracy with SVM. It can be seen from Figures 6 and 7 that *k*NN is more sensitive to feature size, and exhibits a low detection efficiency when the increasing the size of the power system. Finally, the NB-based detection algorithm shows low performance.

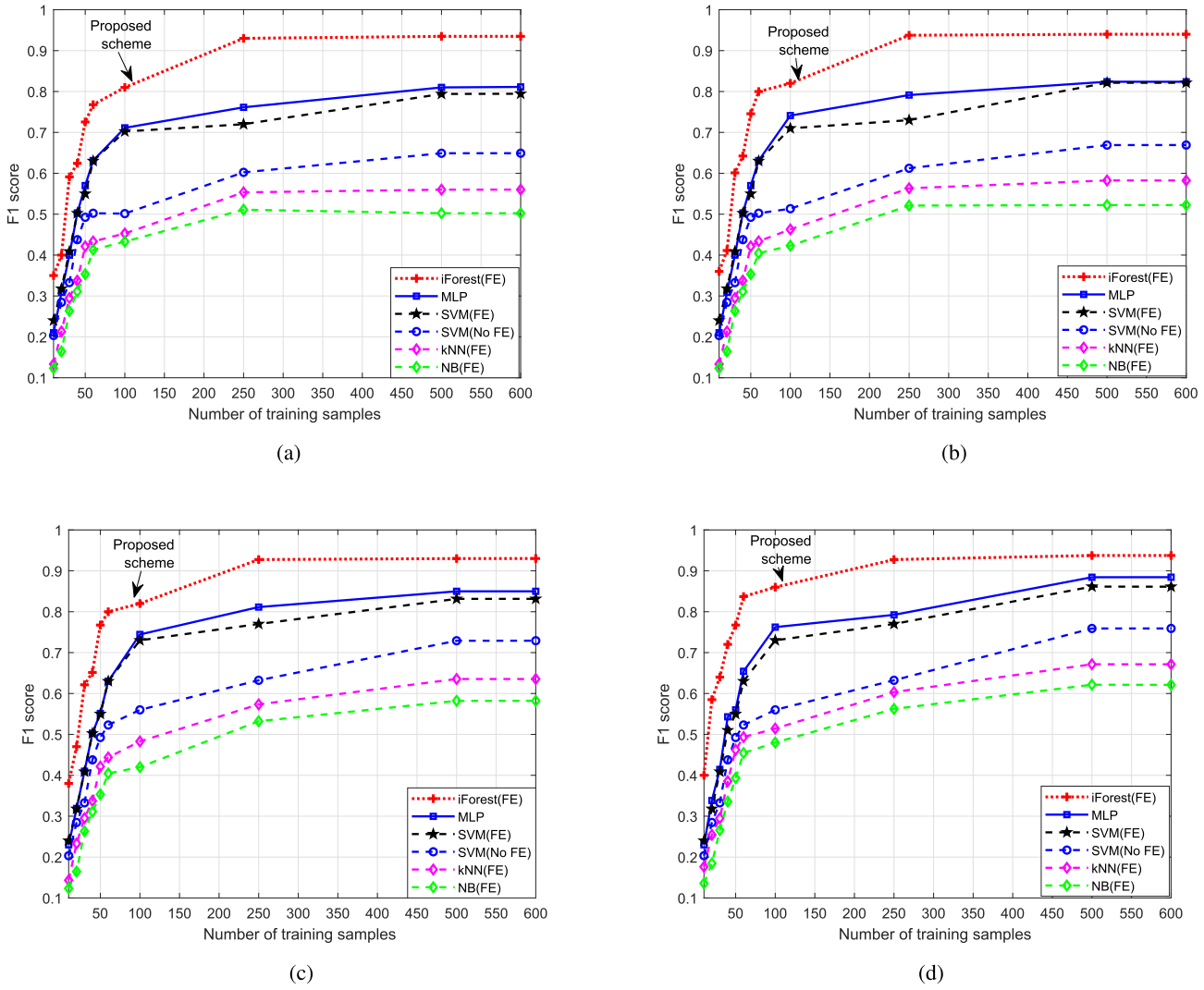

Fig. 7. The F_1 score of the proposed *i*Forest-based CDIA detection scheme with varying numbers of training samples. (a) IEEE 14-bus system. (b) IEEE 39-bus system. (c) IEEE 57-bus system. (d) IEEE 118-bus system.

TABLE VII

AVERAGE CDIA DETECTION ACCURACY COMPARISON BETWEEN THE PROPOSED *iForest*-BASED CDIA DETECTION AND EXISTING ML SCHEMES

	IEEE 14-Bus System		**IEEE 39-Bus System**		**IEEE 57-Bus System**		**IEEE 118-Bus System**	
Detection Scheme	Accuracy (%)	F_1 score	Accuracy (%)	F_1 score	Accuracy (%)	F_1 score	Accuracy (%)	F_1 score
***i*Forest**	93.012	0.923	93.421	0.929	94.016	0.930	94.518	0.941
SVM (FE)	85.323	0.842	85.112	0.837	86.004	0.851	86.999	0.852
SVM (No FE)	69.563	0.687	69.943	0.663	67.564	0.667	68.876	0.657
***k*NN (FE)**	67.643	0.641	66.723	0.602	61.723	0.598	58.234	0.563
NB (FE)	62.321	0.644	66.543	0.645	60.321	0.611	60.000	0.587
MLP (FE)	89.743	0.873	90.142	0.882	90.723	0.906	90.353	0.924

The significant point is that the proposed scheme is based on unsupervised ML algorithm where labels are not utilized. Conversely, reference schemes are supervised and require target labels for CDIA detection. The proposed scheme exhibits considerably good performance at low computational cost [59]. Furthermore, the average CDIA detection performance of the proposed scheme in comparison to the existing ML–based schemes, is given in the Table VII. It can be seen from Table VII, that the average accuracy and the F_1 score of the proposed scheme for detecting CDIAs is better than the existing ML-based schemes for all the test bus cases.

V. CONCLUSION

In this paper, we propose an unsupervised scheme for detection of CDIAs in SG communications networks considering a realistic scenario of a non-labeled, historical SE-MF dataset

in the PCC of a power network. The proposed scheme is based on a state-of-the-art algorithm called *i*Forest. To tackle the growing complexity from the increasing sizes of power systems, we employ a PCA-based FE mechanism to transform high-dimensional space into a low-dimensional space where the data points can easily be separated without compromising accuracy. The transformed data are used as input for the unsupervised *i*Forest-based anomaly detection scheme. The performance of the proposed scheme was evaluated by employing standard IEEE 14-bus, 39-bus, 57-bus, and 118-bus systems. Active power injections into the buses and active power flow measurements in the branches are the main features of the dataset. We compared the performance of the proposed scheme with those of numerous machine learning schemes reported in the literature. The test results show that the proposed *i*Forest-based detection scheme reasonably improves detection accuracy in the occasional operational environment. The low-computational complexity of the proposed scheme enables the identification of outliers or anomalies in a short time. In the future, we will remodel our work by considering more diverse attack scenarios, and we will incorporate more machine-learning algorithms to improve the detection accuracy.

REFERENCES

[1] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[2] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58–66, Jan./Feb. 2012.

[3] Y. Mo *et al.*, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[4] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys & Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart. 2012.

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

[6] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, 4th Quart. 2012.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. 13, 2011.

[8] A. Lee, "Guidelines for smart grid cyber security," NIST, Gaithersburg, MD, USA, Tech. Rep. 7628 Rev 1, 2010.

[9] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCS)*, Jun. 2008, pp. 495–500.

[10] S. Ahmed, Y. D. Lee, S. H. Hyun, and I. Koo, "A cognitive radio-based energy-efficient system for power transmission line monitoring in smart grids," *J. Sensors*, vol. 2017, Nov. 2017, Art. no. 3862375.

[11] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart. 2012.

[13] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 36–46, Mar. 2013.

[14] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[15] R. C. Qiu *et al.*, "Cognitive radio network for the smart grid: Experimental system architecture, control algorithms, security, and microgrid testbed," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 724–740, Dec. 2011.

[16] C. Queiroz, A. Mahmood, and Z. Tari, "SCADAsima—Framework for building SCADA simulations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 589–597, Dec. 2011.

[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, Jun. 2011.

[18] D. Deka, R. Baldick, and S. Vishwanath, "Data attack on strategic buses in the power grid: Design and protection," in *Proc. IEEE PES Gen. Meeting Conf. Expo.*, Jul. 2014, pp. 1–5.

[19] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[20] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.

[21] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, Jul. 2016.

[22] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[23] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[24] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1471–1485, Jul. 2014.

[25] M. Talebi, J. Wang, and Z. Qu, "Secure power systems against malicious cyber-physical data attacks: Protection and identification," in *Proc. Int. Conf. Power Syst. Eng.*, 2012, pp. 11–12.

[26] R. H. Etemad and F. Lahouti, "Resilient decentralized consensus-based state estimation for smart grid in presence of false data," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2016, pp. 3466–3470.

[27] Z. Ismail, J. Leneutre, D. Bateman, and L. Chen, "A game theoretical analysis of data confidentiality attacks on smart-grid AMI," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1486–1499, Jul. 2014.

[28] Y. Guo, C.-W. Ten, S. Hu, and W. W. Weaver, "Preventive maintenance for advanced metering infrastructure against malware propagation," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1314–1328, May 2016.

[29] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.

[30] K. G. Vamvoudakis, J. P. Hespanha, B. Sinopoli, and Y. Mo, "Detection in adversarial environments," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3209–3223, Dec. 2014.

[31] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Syst.*, vol. 35, no. 1, pp. 93–109, Feb. 2015.

[32] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 163–178, Jan. 2016.

[33] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC61850 automated substations," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2376–2383, Oct. 2010.

[34] S. Pal and B. Sikdar, "A mechanism for detecting data manipulation attacks on PMU data," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Nov. 2014, pp. 253–257.

[35] S. Pal, B. Sikdar, and J. H. Chow, "Detecting malicious manipulation of synchrophasor data," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2015, pp. 145–150.

[36] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov. 2015.

[37] R. Mitchell and I.-R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1254–1263, Sep. 2013.

[38] Y. Zhang, L. Wang, W. Sun, R. C. Green, II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[39] Z. M. Fadlullah, M. M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," *IEEE Netw.*, vol. 25, no. 5, pp. 50–55, Sep./Oct. 2011.

[40] 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, Aug. 2016.
[41] 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, Sep. 2017.
[42] J. Wang, W. Tu, L. C. Hui, S. M. Yiu, and E. K. Wang, "Detecting time synchronization attacks in cyber-physical systems with machine learning techniques," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 2246–2251.
[43] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning," *IEEE Access*, vol. 6, pp. 27518–27529, 2018.
[44] 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," *Appl. Sci.*, vol. 8, no. 5, p. 772, 2018.
[45] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1000–1009, Aug. 2011.
[46] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24–29, Aug. 2012.
[47] C. Y. T. Ma, D. K. Y. Yau, X. Lou, and N. S. V. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1676–1686, May 2013.
[48] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Trilevel optimization in power network defense," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 4, pp. 712–718, Jul. 2007.
[49] J. M. Arroyo and F. J. Fernández, "A genetic algorithm approach for the analysis of electric grid interdiction with line switching," in *Proc. IEEE 15th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP)*, Nov. 2009, pp. 1–6.
[50] L. Zhao and B. Zeng, "Vulnerability analysis of power grids with line switching," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2727–2736, Aug. 2013.
[51] A. Gomez-Exposito and A. Abur, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.
[52] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[53] *Illinois Center for a Smarter Electric Grid (ICSEG)*. Accessed: Apr. 2, 2018. [Online]. Available: http://icseg.iti.illinois.edu/ieee-39-bus-system/
[54] J. Casazza, J. Casazza, and F. Delea, *Understanding Electric Power Systems: An Overview of the Technology and the Marketplace*, vol. 13. Hoboken, NJ, USA: Wiley, 2003.
[55] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 1, pp. 89–97, Jan. 2018.
[56] S. Abe, "Feature selection and extraction," in *Support Vector Machines for Pattern Classification*. New York, NY, USA: Springer, 2010, pp. 331–341.
[57] A. Jain and B. Chandrasekaran, *Dimensionality and Sample Size Considerations in Pattern Recognition Practice, Handbook of Statistics*, vol. 2, P. R. Krishnaiah and L. Kanal, Eds. Amsterdam, The Netherlands: Elsevier, 1982.
[58] M. Ivanov. (Sep. 29, 2017). *Comparison of PCA with ICA from Data Distribution Perspective*. [Online]. Available: https://arxiv.org/abs/1709.10222
[59] R. Domingues, M. Filippone, P. Michiardi, and J. Zouaoui, "A comparative evaluation of outlier detection algorithms: Experiments and analyses," *Pattern Recognit.*, vol. 74, pp. 406–421, Feb. 2018.
[60] D. A. Tibaduiza, L. E. Mujica, M. Anaya, J. Rodellar, and A. Güemes, "Principal component analysis vs independent component analysis for damage detection," in *Proc. 6th Eur. Workshop Structural Health Monitor.*, vol. 2, 2012, pp. 3–6.
[61] Q. Meng, D. Catchpoole, D. Skillicom, and P. J. Kennedy, "Relational autoencoder for feature extraction," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, May 2017, pp. 364–371.
[62] V. Chandola, V. Mithal, and V. Kumar, "Comparative evaluation of anomaly detection techniques for sequence data," in *Proc. 8th IEEE Int. Conf. Data Mining (ICDM)*, Dec. 2008, pp. 743–748.
[63] N. Abe, B. Zadrozny, and J. Langford, "Outlier detection by active learning," in *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (ACM)*, 2006, pp. 504–509.
[64] Z. He, X. Xu, and S. Deng, "Discovering cluster-based local outliers," *Pattern Recognit. Lett.*, vol. 24, nos. 9–10, pp. 1641–1650, Jun. 2003.
[65] P. J. Rousseeuw and K. Van Driessen, "A fast algorithm for the minimum covariance determinant estimator," *Technometrics*, vol. 41, no. 3, pp. 212–223, 1999.
[66] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *Proc. 8th Int. Conf. Data Mining*, 2008, pp. 413–422.
[67] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation-based anomaly detection," *ACM Trans. Knowl. Discovery Data*, vol. 6, no. 1, p. 3, 2012.
[68] B. R. Preiss, *Data Structures and Algorithms*. Hoboken, NJ, USA: Wiley, 1999.
[69] F. Pedregosa *et al.*, "Scikit-learn: Machine learning in python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, Oct. 2011.

Saeed Ahmed received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Azad Jammu and Kashmir, Pakistan, in 2005 and 2010, respectively. He is currently pursuing the Ph.D. degree with the University of Ulsan, South Korea. He served as a Transmission Planning Engineer in the telecom industry from 2005 to 2012 and has experience in planning, surveying, deploying, and troubleshooting of the microwave and optical fiber-based core and access PDH/SDH/SONET/DWDM networks. He joined the Mirpur University of Science and Technology (MUST), Mirpur, Pakistan, as an Assistant Professor in 2012. His research area includes energy-efficient resource allocation in cognitive radios, smart grid (SG) communication technologies, smart grid security, and Internet of Things (IoT).

YoungDoo Lee received the B.E., M.E., and Ph.D. degrees from the School of Electrical Engineering, University of Ulsan, South Korea, in 2007, 2009, and 2013, respectively, where he has been a Research Fellow since 2013. His current research interests include artificial intelligent-based networks, cognitive radio networks, underwater sensor networks, beacon-based service networks, RFID, IoT-based service system, and next-generation communication systems.

Seung-Ho Hyun received the B.E., M.S., and Ph.D. degrees in electrical engineering from Seoul National University, South Korea, in 1991, 1993, and 1996, respectively. His work experience includes the Korea Railroad Research Institute and Myongji University. He has been an Associate Professor with the University of Ulsan, South Korea, since 2004. His major research field is power system control, protection, and renewable energy.

Insoo Koo received the B.E. degree from Konkuk University, Seoul, South Korea, in 1996, and the M.S. and Ph.D. degrees from the Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 1998 and 2002, respectively. From 2002 to 2004, he was with the Ultrafast Fiber-Optic Networks (UFON) Research Center, GIST, as a Research Professor. In 2003, he was a Visiting Scholar with the Royal Institute of Science and Technology, Sweden. In 2005, he joined the University of Ulsan, where he is currently a Full Professor. His research interests include next-generation wireless communication systems and wireless sensor networks.