IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 30, 2021, accepted September 8, 2021, date of publication October 4, 2021, date of current version October 11, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3117230

Accurate Detection of False Data Injection Attacks in Renewable Power Systems Using Deep Learning

FAYHA ALMUTAIRY[1,2], LAZAR SCEKIC[3], RAMADAN ELMOUDI[4], AND SAFWAN WSHAH[2], (Member, IEEE)

[1]Department of Computer Science, Shaqra University, Shaqra 11961, Saudi Arabia
[2]Department of Computer Science, University of Vermont, Burlington, VT 05405, USA
[3]Faculty of Electrical Engineering, University of Montenegro, 81000 Podgorica, Montenegro
[4]New York Power Authority (NYPA), White Plains, NY 10601, USA

Corresponding author: Fayha Almutairy (fayha.almutairy@gmail.com)

ABSTRACT The rapid development of technology in the past decades created a society heavily dependent on electricity, where even short disturbances in the power supply can result in grave socio-economic consequences. Therefore, assuring a safe and reliable operation of the power system has become of utmost importance. False data injection attacks (FDIAs) represent a class of cyber-attacks targeting the power system state estimation. FDIAs alter the perspective of the power system's state which can lead to inappropriate control actions. Thus, a reliable method for detecting FDIAs represents the main prerequisite to the safe operation of the power system in the context of cybersecurity. Noticing the scarce literature analyzing the detection of FDIAs in power systems with a high share of renewable energy sources, this paper demonstrates that the performance of the existing methods deteriorates when faced with the volatile nature of renewable energy sources. This paper presents a deep learning approach for detecting stealthy FDIAs concerning the power systems with high penetration of renewable energy sources. The performance of the proposed method is validated through different scenarios based on the modified versions of the IEEE 14-bus system and the IEEE 118-bus system. The proposed method is able to detect most of the attacks under different test scenarios, outperforming the benchmark techniques with an average detection rate of 99% for the IEEE 14-bus system and 97% for the IEEE 118-bus system.

INDEX TERMS False data injection attacks, cyber-attack detection, state estimation, renewable energy sources, deep learning.

I. INTRODUCTION

Power systems are critical components in our modern infrastructure. Most of our daily activities depend on the security of power systems [1]. Therefore, it is of utmost importance to ensure both their physical and cybersecurity. Cybersecurity stands for the security of Information and Communication Technologies (ICT) that support the operation of electric power systems [2]. Following the coordinated cyber-attack that led to the Ukraine Blackout in 2015, cybersecurity of electric power systems is recognized as one of the crucial challenges facing power and energy authorities [3].

There are several reasons for the increasing importance of cybersecurity. First, with advances in computing technology, power systems have been upgraded with networking capabilities that facilitate their monitoring and control, but also transform them into cyber systems [4]. Second, smart grids require sophisticated and decentralized control methods to ensure their continuous and stable operation. Therefore, uninterrupted communication between physically separated entities is required. Such reliance on communication technologies makes smart grids more vulnerable to cyber-attacks [5]. Third, the addition of Phasor Measurement Units (PMUs) that rely on communication technologies has further increased the potential for cyber-attacks in power systems [6].

Various types of cyber-attacks, such as reconnaissance attacks, packet injection attacks, denial-of-service

The associate editor coordinating the review of this manuscript and approving it for publication was Fabio Mottola.

TABLE 1. Related work.

Category	Reference	Method	State estimation	Test system	Evaluation metrics	RES
Statistical	[7]	KLD	**AC**	14	detection rate	no
	[8]	SO	DC	57, 118, 2383	detection rate, false positive rate	no
	[9]	GLRT	DC	14	detection rate, false positive rate	no
	[10]	AD	DC	14	detection rate, false positive rate, F1-score	**yes**
Machine learning	[11], [12]	SVM	DC	9, 57, 118	precision, recall, accuracy, F1-score	no
	[13]	KNN	DC	30	accuracy, F1-score	no
	[14]	GMM	DC	118	F1-score	no
Deep learning	[15]	CNN	DC	39	accuracy	no
	[16]	CDBN	DC	118, 300	detection accuracy, false positive rate	no
	[17]	DNN	AC	118, 300	detection accuracy, false positive rate	no
	[18]	BLSTM	DC/**AC**	118, 300	detection accuracy, F1-score	no
	this paper	TCN Vanilla WaveNet Proposed WaveNet	**AC**	14, 118	detection rate, false positive rate, F1-score	**yes**

attacks [19], energy thefts [20], [21] and False Data Injection Attacks (FDIAs) threaten power systems. FDIAs represent a new class of cyber-attacks that targets the power system state estimation by manipulating the measurement data transmitted over communication lines [4], [22]. In FDIAs, the adversary compromises power system measurements aiming to alter the estimated state of the power system. Ultimately, this can lead to control actions that can compromise the secure and economical operation of the power system [5]. FDIAs can bypass the existing Bad Data Detection (BDD) techniques and pose a serious threat to power system operation and control [23]. In addition, FDIAs can disrupt deregulated energy markets and cause severe economic and financial losses [1].

A variety of different strategies have been proposed in the literature to protect the power system from FDIAs. They can be classified into two main categories, namely: protection-based strategies and detection-based strategies. The protection-based strategies are based on ensuring the security of measurements through different mechanisms. Ideally, the highest security could be achieved by protecting all meter measurements. However, applying this approach to large systems would entail significant investment costs. Motivated by this problem, the authors proved in [24] that it is necessary and sufficient to protect a set of basic measurements that ensures that no undetectable FDIAs can be launched. The main drawback of the proposed approach is that the number of basic measurements is equal to the number of variables in the state estimation problem. To overcome this problem, the authors in [25] have proposed exact and approximate methods to determine the minimum set of measurements required to protect a given subset of state variables. This approach extends the protection-based scheme to large-scale systems. While previous works are mostly based on identifying the set of critical measurements, in [26] the authors proposed a greedy algorithm for strategically placing PMUs to defend against FDIAs. Apart from the high cost of PMUs, their deployment is also associated with an increased risk of another type of cyber-attacks, namely GPS spoofing attacks [27]. Although efficient, protection-based strategies require the expansion of information and communication infrastructure, which imposes additional costs. Therefore, the focus of this paper is on detection-based strategies. However, for a detailed overview of protection-based strategies, the reader is referred to [28].

Extensive literature presents a wide variety of detection-based strategies applied to detect FDIAs. These can be broadly divided into three categories, namely: statistical, machine learning, and deep learning methods. Table 1 features some of the most notable papers from each category summarizing the proposed detection methods, employed state estimation approaches (DC, AC, or both), as well as the test system used to validate the proposed method and the employed evaluation metrics. Apart from these, Table 1 also notes whether renewable energy sources (RES) have been considered in the performed studies or not. The earliest methods applied to detect FDIAs on the power system state estimation were mostly statistical. In [7], the authors proposed an efficient method based on the Kullback-Leibler distance (KLD) between two probability distributions: distribution of measurement variation from historical data, and distribution of measurement variation between two subsequent time-steps. FDIAs lead to a sudden increase of distance index, which makes it easy to distinguish from normal operating conditions. In [8], the authors formulated the detection problem as a sparse optimization (SO) problem. The optimization problem was solved using nuclear norm minimization and low rank matrix factorization, where the latter is proven to provide superior performance. In [9], the authors proposed a generalized likelihood ratio test (GLRT) detector which was proven to provide high accuracy in detecting sparse FDIAs. In particular application, GLRT requires solving a nonconvex

combinatorial optimization problem. Therefore, the authors performed convex regularization of the optimization problem which leads to higher computational efficiency, but also to somewhat worse performance. In [10], the authors proposed an anomaly detection (AD) method that employs an F-test to compare the current state vector with its recent forms. After determining a suspicious state vector, a residual vector is formed by subtracting the average of the recent states from the suspicious vector. Afterwards, various algorithms are applied to the residual vector with the aim of detecting and localizing the attack.

The idea of employing machine learning methods for the detection of FDIAs is attributed to Ozay *et al.* [11]. In their pioneering work, the authors investigated the performance of several supervised and semi-supervised learning algorithms for the detection of FDIAs. Through numerical experiments, it was concluded that Support Vector Machine (SVM) outperforms k-Nearest Neighbor (KNN) and perceptron by a significant margin, especially for larger systems. In addition, it was concluded that the performance of SVM is heavily dependent on the selection of the kernel type. Superior performance of SVM over KNN and its modified version, namely Extended Nearest Neighbor (ENN) was later confirmed by analyzing different test scenarios [13]. The employment of SVM was also analyzed in [12], where it was concluded that computational complexity can be reduced by applying the principal component analysis (PCA) to select the main sample features. In [14], the authors proposed a semi-supervised learning approach based on a Gaussian mixture model (GMM). Through numerical experiments, it was concluded that the proposed method outperforms SVM and multi-layered perceptron in terms of detection accuracy, training time, and testing time.

With the availability of advanced computational resources and their successful application in various fields, many researchers have analyzed the possibility of using deep learning methods for the detection of FDIAs. In [15], the authors developed a two-stage detection technique combining Convolutional Neural Networks (CNNs) with Long Short Term Memory (LSTM) to detect FDIAs with high accuracy. Although promising results were obtained, the proposed method was only applied in simple scenarios. In particular, uncoordinated FDIAs were generated by introducing random Gaussian noise into the measurements. Therefore, it remains unclear whether the proposed method is applicable to stealthy coordinated attacks. In [16], the authors employed Conditional Deep Belief Networks (CDBNs) to extract the behavioural features of stealthy FDIAs that evade conventional BDD techniques. The extracted features were then used to detect potential FDIAs that affect real-time measurements. In contrast, Discrete Wavelet Transform (DWT) was combined with Deep Neural Networks (DNNs) to extract temporal features of system states [17]. The spatiotemporal technique proved to be an efficient and scalable solution for detecting stealthy FDIAs. To address the scalability issue, in [18], the authors employed an Invertible Automatic Encoder (IAE) that reduces the dimension of the measurement set. The set of characteristic measurements was further processed using an LSTM network, which outperforms SVM and Deep Belief Network (DBN).

Although high detection accuracy is shown when tested on standard test scenarios, the literature does not answer whether the existing detection methods can be applied to power systems with a high share of RES. Recently, governments have prioritized RES over fossil fuel-based power generation aiming towards climate neutrality. It is expected that by 2030, more than 35 percent of the total energy demand will be met by RES [29]. Although the RES play an important role in reducing the carbon footprint of the electricity sector, their volatile nature leads to inevitable power and voltage fluctuations. Apart from causing major technical challenges, such fluctuations alter the underlying distribution of measurements and system states. Therefore, it remains unclear whether the performance of existing methods is affected by the addition of RES. To the best of our knowledge, the detection of FDIAs in renewable power systems has been analyzed only in [10]. Although the aforementioned work addresses the addition of RES and topology changes, the research was limited to DC state estimation. To test the performance of the proposed method on AC state estimation, the authors have only analyzed FDIAs targeting the voltage magnitudes. As will be shown in the following sections, these types of attacks are easily detected due to relatively small voltage magnitude deviations under normal operating conditions. Moreover, the authors considered only one integration scenario where RES can account for only 5 percent of the peak demand. Therefore, the correlation between different penetration levels and the performance indicators of FDIA detection methods was not identified. Naturally, increasing the penetration of variable RES leads to higher power and voltage fluctuations, which increases the spatiotemporal complexity of the system states. As will be shown in the following sections, this heavily affects the performance of the existing methods.

Considering the existing gap in the literature, this paper focuses on investigating the impact of non-dispatchable RES on the performance of the existing detection methods. As will be shown, the introduction of RES increases the likelihood of FDIAs remaining undetected. Unfortunately, this makes the existing methods unreliable. Therefore, an advanced deep learning architecture is proposed that is shown to outperform the existing methods in the detection of FDIAs.

The main contributions of this paper are as follows:

1) This work pioneers in studying the effect of different levels of renewable penetration on the accuracy of the existing methods for the detection of stealthy FDIAs affecting AC state estimation.
2) Instead of using Recurrent family models widely employed in the literature, this paper analyzes the possibility of using Auto-regressive models such as WaveNet and TCN for the detection of FDIAs.

3) The conventional architecture of WaveNet is modified in order to offer an efficient and scalable method for the detection of FDIAs.

The rest of the paper is organized as follows. Section II presents a brief theoretical overview of FDIAs in the context of power system state estimation. In addition, Section II also features a simple test scenario justifying the existing gap in the literature. Section III explains the proposed methodology for the detection of FDIAs. Section IV illustrates the numerical results and the validation of the proposed approach simulated on the modified versions of the IEEE 14-bus system and the IEEE 118-bus system. Section IV also features the correlation between the accuracy of the proposed method and the severity of the attack scenarios. In the end, the conclusions are drawn in Section V.

II. FALSE DATA INJECTION ATTACKS IN THE CONTEXT OF POWER SYSTEM STATE ESTIMATION

In this section, a mathematical model of a weighted least-squares state estimator is presented, and a mathematical model of stealthy FDIAs that bypass conventional residual-based bad data detection techniques is introduced. Furthermore, the performance evaluation of existing detection techniques is also presented using a simple test scenario.

A. STATE ESTIMATION

Following the work of the pioneer of state estimation, Fred Schweppe, a state estimator can be defined as a data processing algorithm for converting redundant measurement data and other available data on the power system into an accurate estimate of the system state [30]. Based on the power flow model used in the problem formulation, three main types of state estimators have been developed in the literature: AC, decoupled, and DC state estimators. As mentioned in the previous section, most related work in the area of FDIAs focuses on the DC state estimator. The DC state estimator is widely used in daily power system operation due to its low computational burden, however, the accuracy of the DC power flow analysis is highly case-dependent and under certain conditions, it introduces alarmingly inaccurate results for the critical power flows [31]. Moreover, with the increasing computational power of modern computers, the advantages of using DC over the AC state estimator may become negligible in terms of computational burden. Therefore, a state estimator based on AC power flow equations is used in this paper.

The AC state estimator is based on the nonlinear measurement model:

$$z = h(x) + e \tag{1}$$

where $z = (z_1, z_2, \ldots, z_m)^T$ is the measurement vector, $x = (x_1, x_2, \ldots, x_n)^T$ is the state vector, h is a nonlinear vector function relating the measurements with the system states, and $e = (e_1, e_2, \ldots, e_m)^T$ is the vector of random measurement errors following a Gaussian distribution with a 0 mean, and a corresponding variance matrix $R_z = diag(\sigma_1^2, \sigma_2^2, \ldots \sigma_m^2)$.

The state estimation problem is usually solved as an overdetermined ($m > n$) weighted least squares problem which can be mathematically formulated as:

$$\min_x J(x) = \sum_{i=1}^{m} \left(\frac{z_i - h_i(x)}{\sigma_i} \right)^2 \tag{2}$$

After applying the first-order optimality condition to the performance index $J(x)$, an iterative Gauss-Newton scheme arises, yielding the optimal estimate of the system state $\hat{x}$.

B. BAD DATA DETECTION AND FALSE DATA INJECTION ATTACKS

The weighted least squares approach assumes that the measurement errors follow a Gaussian distribution. However, since the power system represents a dynamic environment with a large number of uncontrollable impacting factors, the occurrence of large errors in the input data is not uncommon. To cope with the occurrence of bad data, a wide range of different BDD techniques have been developed. The most commonly employed BDD techniques rely on the analysis of the residual vector r. After determining the optimal estimate of the system state, the residual vector $r = (r_1, r_2, \ldots, r_m)^T$ can be determined as:

$$r = z - h(\hat{x}) \tag{3}$$

The measurements subject to high noise, inverse polarity or meter failures are characterized by high values of the residual, making them easy to identify and exclude from the process of state estimation.

FDIAs can be defined as those in which the adversary alters the readings of one or more meters, thereby changing the estimated value of the system state variables. FDIAs can be either random or targeted [24]. In random attacks, the adversary injects arbitrary errors into the estimates of the state variables, while in targeted attacks, specific errors are injected into the estimates of specific state variables. However, a more significant categorization is based on the extent of the adversary's knowledge about the system prior to performing the attack. As such, FDIAs can be either complete or incomplete [17]. As the name implies, in complete FDIAs, the adversary has complete knowledge of the power system. Complete FDIAs represent a critical scenario over the incomplete since they lead to inaccurate estimates of the system states while bypassing the conventional residual-based BDD techniques. This may subsequently lead the system operators towards control actions that may jeopardize the secure operation of the power system. Due to their covert nature, this type of FDIAs is often denoted as ''stealthy''.

While the assumptions regarding the knowledge and capabilities of the adversary required in order to launch a stealthy FDIA may seem strong, the 2015 Ukraine blackout states otherwise. The coordinated cyber-attack leading to the blackout was performed by orchestrating numerous attacks which served as a decoy while the adversary group hijacked the SCADA system. In [3], the authors employed this example

to justify the feasibility of stealthy FDIAs. The necessary conditions for launching complete FDIAs against DC state estimation have been introduced to the literature in [32]. The same concept was later extended to AC state estimation in [33]. The mathematical model of stealthy FDIAs against AC state estimation is as follows.

Let $\hat{x}_a$ denote the estimate of the system state determined by processing the compromised set of measurements $z_a = z + a$. The attack vector $a = (a_1, a_2, \ldots, a_m)^T$ represents measurement deviations introduced by an FDIA. Under FDIAs, the residual vector can be determined as:

$$\begin{aligned} r_a &= z_a - h(\hat{x}_a) \\ &= z + a - h(\hat{x}_a) + h(\hat{x}) - h(\hat{x}) \\ &= z - h(\hat{x}) + a - h(\hat{x}_a) + h(\hat{x}) \\ &= r + a - h(\hat{x}_a) + h(\hat{x}) \end{aligned} \tag{4}$$

which in general differs from the normal residual vector. However, if the attack vector is constructed as:

$$a = h(\hat{x}_a) - h(\hat{x}), \tag{5}$$

the residual vector remains unchanged in comparison with the normal scenario ($r_a = r$). In other words, when the nonlinear vector function $h(\cdot)$ is known along with the system state estimate $\hat{x}$, the adversary can construct an attack vector which leads to the false estimate of the system state $\hat{x}_a$, bypassing the conventional residual-based BDD techniques.

C. TRADITIONAL AND DEEP LEARNING METHODS FOR THE DETECTION OF FALSE DATA INJECTION ATTACKS

As introduced in the previous section, it remains unclear whether the methods proposed in the literature can be used to a high extent in power systems with a high share of RES. As such, this section discusses the performance of two groups of FDIA detection methods, namely machine learning and deep learning methods on a simple, tailored case study. The analyzed test system is a simple 2-bus system consisting of a synchronous generator supplying the consumer through a short power line. Apart from that, the consumer has installed a wind generator for supplying a part of its load which varies according to a realistic load profile. Furthermore, the wind generator is assigned a realistic generation profile. The 3-month period was simulated on a 5-minute resolution leading to a dataset of around 25 thousand samples where each sample represents a state vector arising from the state estimation process. Throughout the 3-month period, stealthy FDIAs are performed randomly with around 25% of the samples being corrupted. From the group of machine learning methods, three techniques commonly used in the literature have been considered, namely SVM, KNN, and Random Forest (RF) [34]. The deep learning methods discussed in detail in the previous section, namely [15], [17], and [18], have proven to be of high complexity for a simple Proof-of-Concept as it was extremely hard to train them due to a small number of features in the dataset. Therefore, Gated Recurrent Unit (GRU) and LSTM proposed in [17] and [18] respectively, have been chosen from the category of deep learning methods.[1]

In the absence of wind generation, SVM, KNN, and RF were able to detect the attacks with high accuracy, as shown in Table 2. The same applies to the deep learning techniques of LSTM and GRU. However, in the presence of wind generation which doesn't exceed 40% of the load active power, the performance of the machine learning detection methods deteriorates significantly while deep learning methods exhibit superior performance.

TABLE 2. False data injection attack detection rate.

	Detection rate [%]	
Detection method	No wind generation	Wind generation
SVM	100.00	1.69
KNN	99.90	76.79
RF	99.80	40.35
GRU	100	82.33
LSTM	100	82.11

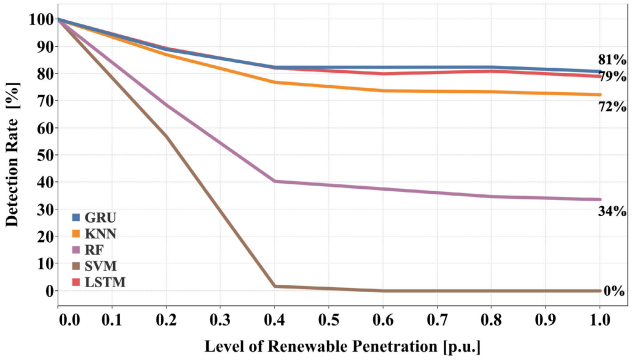


FIGURE 1. Correlation between the level of renewable penetration and the accuracy of the existing detection techniques.

The accuracy of the analyzed methods would be further compromised since realistic power systems are characterized by higher complexity and frequent topology changes. Furthermore, it was found that the performance of the analyzed methods is dependent on the level of installed RES capacity. Figure 1 leads to an important conclusion: increasing the level of variable renewable generation decreases the accuracy of both machine learning and deep learning methods aimed at the detection of FDIAs. Following the renewable energy transition and the global targets to reduce the carbon footprint of the electricity sector, it becomes clear that the existing machine learning methods represent an unreliable solution

[1]The experiments were conducted with the following sets of parameters: **SVM:** Kernel type = Polynomial; **KNN:** number of neighbours = 1; **RF:** 10 Trees, Depth of 2; **GRU:** 128 hidden unit size followed by 1 feedforward layer of 64 hidden units; **LSTM:** 2 Layers of 32 hidden unit size followed by 1 Feedforward layer of 32 hidden units.

for the detection of FDIAs in modern power systems while deep learning methods seem to be more robust. As such, the next section features a deep auto-regressive method powered with residual blocks personalized for the detection of FDIAs.

III. PROPOSED METHOD

This paper introduces an architecture modification of WaveNet, a deep neural network previously used in audio processing, to make it suitable for the detection of FDIAs. WaveNet was originally used to generate raw speech signals which took the probabilistic form of predicting the next waveform given k previous ones as:

$$p(x) = \prod_{i=t-k}^{t+1} p(x_{t+1}|x_{t-k}, x_{t-k+1}, \ldots, x_t) \tag{6}$$

Generation is always perceived as a harder task than classification as a continuous distribution conditioned on previous time steps needs to be generated. Following WaveNet's original formulation [35], the task was divided into next sample prediction (regression) and frame classification. To leverage WaveNet's architecture to make it suitable for the detection of FDIAs, the problem can be reformulated as follows: given a sequence of k readings, predict the presence of the attack. The new formulation leads to the following equation:

$$p(y_t) = p(y_t|x_{t-k}, x_{t-k+1}, \ldots, x_t) \tag{7}$$

where y indicates the probability of an attack.

The following subsections will elaborate on the performed architecture modifications enabling WaveNet's use in the field of FDIA detection.

A. CAUSAL AND DILATED CONVOLUTION

The dilated causal convolution is the backbone operation of WaveNet. It performs both spatial and temporal information extraction through the dilated use of standard convolutions kernels (1×1). Dilated convolution increases the convolution operation's receptive field allowing the learning process to capture long-term dependencies without an increase in computation. Stacked dilated convolutions enable networks to have very large receptive fields with just a few layers while preserving the input resolution throughout the network as well as computational efficiency. This work employs the same dilation factor used in the original architecture while increasing the depth up to 10 layers. In other words, the dilation is doubled for every layer up to a certain limit and then repeated (e.g. 1,2,4,…,512,1024; 1,2,4,…,512,1024; 1,2,4,…,512,1024). The intuition behind this configuration is that exponentially increasing the dilation factor results in an exponential growth of the receptive field with depth [35], [36]. Second, stacking these blocks further increases the model capacity and the receptive field size [35]. Furthermore, the dilated convolutions capture a compact representation in a hierarchy rather than the normal convolution operations.

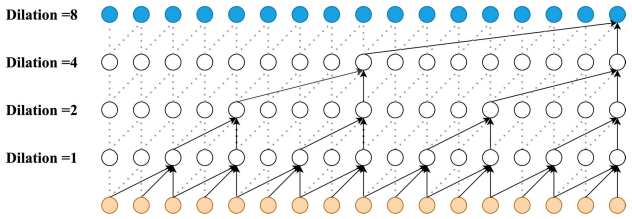


FIGURE 2. Dilated Convolution with kernel size = 3.

As shown in Figure 2, each input passes through a different hidden unit in each dilation layer, giving the model a diversified representation of learning. As shown in Figure 2, the filters skip a step every layer allowing parallel computation of past time steps and modeling both short and long-term dependencies as the dilation rate in powers of two increases the layer depth.

On the other hand, causal convolution makes sure the network does not violate the input order as the output prediction depends solely on previous time steps. In this paper, the causal convolution is applied to each time step separately with 32 filters to create a dense representation of each time step in a higher-dimensional space. In addition, each compact sequence is treated as either an attacked sequence or normal sequence, where the prediction $p(y_t|x_{t-k}, x_{t-k+1} \ldots, x_t)$ emitted by the model at time step t with sequence length equaling k.

The hierarchy structure of dilated causal convolutions mimics the sequence processing power in RNNs, LSTMs, and GRUs as the output has a quite large receptive field with no extra computations [37]. The original version of WaveNet is quite similar to LSTMs and GRUs as the dilated convolutions are followed by two gates, namely one activation gate and one binary gate similar to the two gates in LSTM. The ''Tanh'' gate is similar to the Input Update Gate, and the ''Sigmoid'' gate is similar to the Forget Gate. However, the dilated convolutions are considered better, as LSTMs have to back-propagate through a large number of steps which leads to the problem of vanishing gradients among other problems [38]. As such, training dilated convolutions is incomparably simpler. Furthermore, a major difference between RNNs and dilated convolutions is the shared parameters in RNN architecture, where the same parameters are used in each time step. In dilated convolutions, a set of parameters change throughout different intervals of the input time-series data. Accompanied with different filters, this can be understood as having different representations for the same time intervals which aid the network in capturing different variations of attacks.

B. RESIDUAL BLOCKS

Vanishing gradients represent a major issue in deep neural networks, where gradients of earlier blocks in the network die out as more blocks are stacked after it. In [35], the authors used residual blocks to solve the issue of vanishing gradients by feeding the output of the causal convolution layer deeper

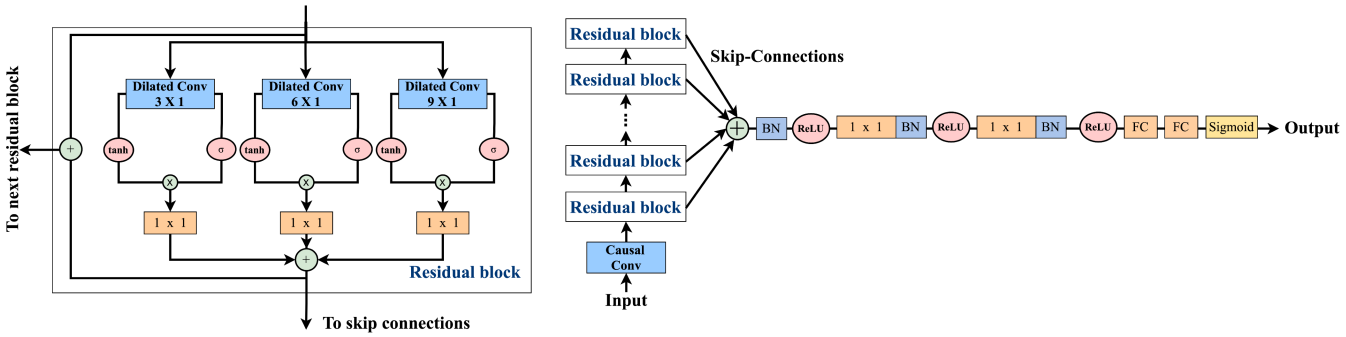


FIGURE 3. Overview of the residual block and the architecture of the proposed method.

into the network. This shortcut connection allows the input to bypass the dilated convolution operation, where both the shortcut connection and the dilated convolution output are then added together to form the output of the whole residual block, facilitating gradient backpropagation throughout the network. Residual blocks mitigate the vanishing gradient problem, accelerating and stabilizing training. In addition, the Residual connection passes the raw input information, which aids the convergence of the training process for a deep network.

Due to the complexity of the dataset, the original WaveNet architecture is adjusted as shown in Figure 3. The proposed model has three different internal branches inside the residual block to capture different inter-feature dependency ranges. Each branch has dilated convolution kernels with varying sizes as follows: 3, 6 and 9, respectively. Figure 2 shows the dilated causal convolution with a kernel size of 3, which is different from the one used in the original paper.

C. HYPERPARAMETER TUNING

In order to efficiently train the proposed model, several hyperparameters were considered, namely: optimizer type, learning rate, batch size, model depth and the sequence size. The tuning process was started by initializing the weights with a Glorot Uniform Distribution [39]. Based on the convergence of the training process and the probability of overfitting, the optimal number of epochs was set to 30. Five different optimizers were considered in the tuning process, namely: Adam [40], AdaGrad [41], AdaDelta [42], RMSprop [43], and SGD [44]. The possible learning rates were set to 10^{-2}, 10^{-3}, 10^{-4} and 10^{-5}, while the batch sizes of 16, 32, 64, 128 and 256 were considered. Model depths ranging from 9 to 16 with the step size of 1 were considered. Candidate sequence sizes were given as 4, 8, 16, 32 and 64. After defining the search space, the Random Search method [45] was used to create possible combinations and select the best combination of hyperparameters for training and validating the model. This is both time- and memory-efficient and more controllable than using grid search to test each combination of hyperparameter values. The best performing optimizer was found to be Adam, with a learning rate of 10^{-4}, batch size of 128, sequence size of 32, and depth (number of blocks) of 10.

IV. TEST RESULTS

In order to show the effectiveness of the proposed method, three additional methods were trained: a machine learning algorithm, SVM [46], along with three deep learning algorithms namely Bidirectional Long Short-Term Memory (BLSTM) [47], Temporal Convolutional Network (TCN) [48], and the original WaveNet often denoted as the Vanilla WaveNet. SVM is known as one of the most efficient supervised machine learning algorithms. The main disadvantage of SVM is that it completely neglects the temporal dependencies in the input data. On the other hand, BLSTM has the ability to capture long and short-term dependencies in sequential data. BLSTM has proven to be a successful choice and a strong baseline for time series problems and it was previously employed in the literature for the detection of FDIAs [15]. TCN is another version of Auto-regressive models which shares many characteristics with WaveNet, such as causal and dilated convolutions. However, as will be shown in the forthcoming case studies, both, the original WaveNet and the proposed method proved superiority over TCN.

To validate the proposed approach and compare it with the benchmark methods, four different case studies based on the modified versions of the IEEE 14-bus system are analyzed in this section. As will be seen, in the base scenario with no renewable generation, all of the employed algorithms exhibit excellent performance in terms of their ability to detect FDIAs. However, with the addition of RES, the situation changes drastically, leading to low detection rates depending on the analyzed scenario. This section also features the correlation between the magnitude of FDIAs and the accuracy of the proposed method. Furthermore, to prove its scalability, the performance of the proposed method is analyzed on a modified version of the IEEE 118-bus system.

A. TEST SYSTEM

The test system used to validate the proposed method represents a modified version of the IEEE 14-bus system shown

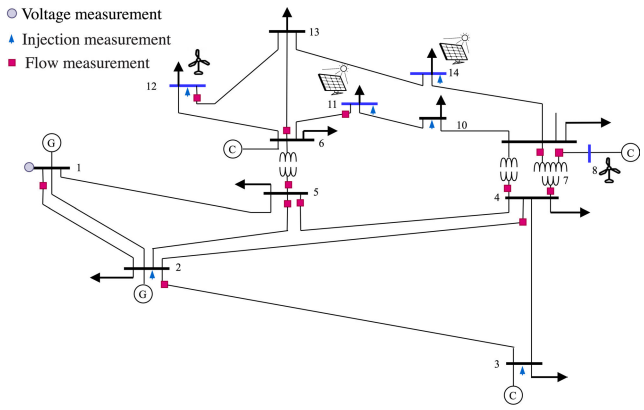


FIGURE 4. IEEE 14-bus system.

in Figure 4. Originally, the IEEE 14-bus system represents a simple approximation of the American power system as of February 1962, consisting of 14 buses, two synchronous generators, three synchronous condensers, and 11 loads [49]. Following the approach outlined in [7] and [10], the original version of the IEEE 14-bus system was modified by assigning each load a specific zone of the New York Independent System Operator (NYISO) [50]. This modification aims to create a realistic environment for validating the proposed model by assigning a realistic variation pattern to each load.

NYISO provides the zonal load data at a 5-minute resolution, resulting in 288 samples for 24 hours. Unlike in [10] where the 7-day cycle was used for validation, the deep learning models used in this paper require a larger training dataset to achieve peak performance. Therefore, the zonal load data for the first three months of 2019 was used for training and validation, resulting in 25920 samples, with 80% of the data used for training and 20% of the data used for validation. The dataset was split to ensure that the model is tested on unseen data to prove its generalization ability and to ensure that no overfitting occurs. In addition, the amount of data generated is sufficient to prevent overfitting that can occur when training complex models. The zonal load data was normalized using the peak load for each zone and scaled with the nominal active and reactive power demand of each load to keep the system close to its nominal operating regime. The load data and their characteristics are summarized in Appendix A.

Apart from the above modification, RES will be added to different buses in the upcoming case studies to analyze the impact of renewable generation on the detection rate and accuracy of the developed models. The renewable generation profiles for the three-month period were extracted from the generation mix also provided by NYISO with a 5-minute resolution. Some of the key features of the renewable generation profiles are also summarized in Appendix A. The locations for connecting RES are determined based on the impact that the generator connection has on the rest of the system. Specifically, buses introducing the highest variability in the system states following the connection of RES are selected. The justification for this approach is that the introduction of fluctuating wind and solar generation leads to higher variability in system states. As a result, the expected range of the system states increases, which means that the state subjected to a FDIA may still be within the expected range of values, making it difficult for existing models to detect the attack. In other words, RES are connected in a way that increases the spatiotemporal complexity of the system states. Sensitivity analysis is used to identify the buses that have the greatest impact on the power system. The analysis has highlighted buses 8, 11, 12 and 14 as the critical buses, so they will be used as the connection points of the RES in the upcoming case studies. The procedure behind the sensitivity analysis and its detailed results are presented in Appendix B.

B. DATA GENERATION AND SIMULATION OF FALSE DATA INJECTION ATTACKS

The procedure used to create a realistic environment for the training and validation of the detection methods is shown in Figure 5. In the first step, using the system data alongside the demand and generation profiles, a power flow analysis is performed to determine the measurements required for the state estimation. After determining the measurements, a vector of Gaussian noise with a zero mean and a standard deviation of 0.02 is added to the measurements to mimic the occurrence of inevitable measurement errors. The noisy measurements are sent to the state estimator, providing the final estimation of the system states. As described in Section II, to alter the perspective of a certain state, the adversary needs to be able to manipulate all the measurements dependent on that state. Assuming this to hold true, a FDIA can be simulated by simply changing the value of a certain state after the

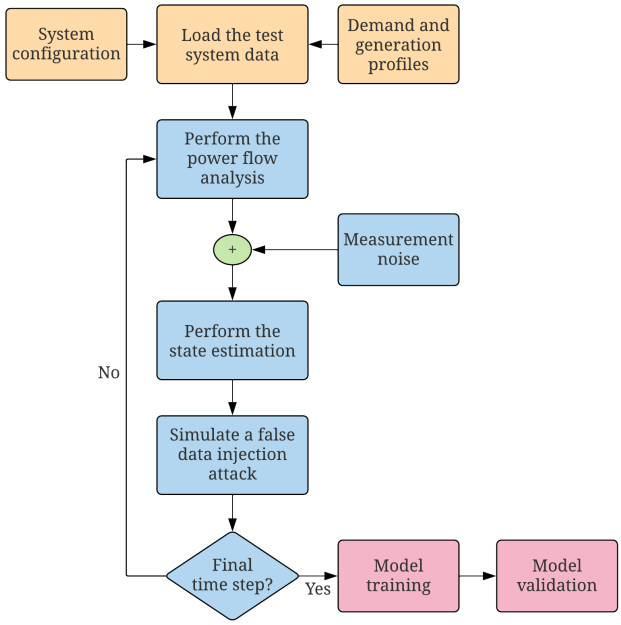


FIGURE 5. Data generation flowchart.

state estimation is performed. In this paper, we have analyzed the ability of the discussed methods to detect the attacks manifested by a 10% decrease in one of the system states $(\theta_2, \theta_3, \ldots, \theta_N, V_1, V_2, \ldots, V_N)$ along with several scenarios of multiple simultaneous attacks [7], [10]. The same attack scenarios are considered in all of the case studies where FDIAs are performed every fifth day. In order to confirm that both peak and off-peak load conditions are considered, attacks are performed between 1-6 am, between 12-5 pm, or on the whole day randomly. The complete dataset consisting of 25920 observations of the system states is used to train and validate the performance of the analyzed methods. The power system simulations including the power flow analysis, state estimation, and the simulation of FDIAs have been performed in MATLAB. On the other hand, the benchmark detection techniques and the proposed method were implemented using Keras, a top-level library built on top of TensorFlow. All experiments were conducted on a workstation with Nvidia K-80 GPU and 16 GB of RAM.

C. EVALUATION METRICS

In compliance with the related work, the most commonly noted evaluation metrics have been employed to test the performance of the proposed method, namely:

1) F1-score (F1), which provides more insight into the ability of the model to classify each sample as normal or attacked. F1 represents a suitable measure for models tested on imbalanced datasets [51], and it can be calculated as:

$$Precision = \frac{TP}{TP + FP} \tag{8}$$

$$Recall = \frac{TP}{TP + FN} \tag{9}$$

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall} \tag{10}$$

where TP denotes the number of true positives representing the number of correctly detected attacked samples, FP denotes the number of false positives or the number of normal samples falsely classified as attacked, and FN denotes the number of false negatives or the number of the attacked samples not detected by the model.

2) Detection rate (DR), which represents the number of attacks detected by the model divided by the total number of the performed attacks, shows the model's ability to recognize the attacked samples.
3) False Positive Rate (FPR), which represents the ratio between the number of normal samples falsely categorized as attacked and the total number of actual normal samples.

D. CASE STUDY I: POWER SYSTEM WITHOUT RENEWABLE ENERGY SOURCES

As the title suggests, the first case study analyzes the performance of the employed detection algorithms in a traditional power system without RES. In all of the analyzed scenarios, all of the deployed algorithms were able to detect the attacks. Furthermore, in all of the case studies analyzed in this paper, when the attacks are performed to the voltage magnitudes, all of the deployed algorithms are able to detect the attacks with an accuracy of almost 100%. The main reason for that is that under normal operating conditions, voltage magnitudes are close to their nominal values with small fluctuations throughout the day, meaning that any significant deviation due to FDIAs is easily detected. On the other hand, as will be seen, FDIAs affecting voltage phase angles are more likely to remain undetected. As such, in the forthcoming case studies, the test results will be shown only when the FDIAs affect the voltage phase angles.

E. CASE STUDY II: POWER SYSTEM WITH A SOLAR POWER PLANT

In the second case study, the effect of one solar power plant on the accuracy of the detection methods is analyzed. The solar power plant with 100MW of capacity is connected to the 8^{th} bus, which proved to have the largest effects on the whole system. The detection rate and the F1 score of different methods for all of the test scenarios are shown in Table 3. As can be seen, the addition of the solar power plant with a variable output power severely affects the performance of SVM, while BLSTM, TCN, and original WaveNet experienced a slight deterioration in the performance, based on the analyzed scenario. Table 3 leads to an important conclusion: a FDIA has the biggest chance of staying undetected if it indirectly targets the phase angle corresponding to the bus representing the connection point of variable RES. In this case, when the attacks are performed to the phase angle of the 8^{th} bus, SVM shows the worst performance, being able to detect only 59.86% of the attacks. BLSTM, TCN, and Vanilla WaveNet were able to detect 95.78%, 97.47%, and 97.98% of the attacks, respectively, while the proposed method demonstrated the highest detection rate.

F. CASE STUDY III: POWER SYSTEM WITH A WIND POWER PLANT

In the third case study, the performance of the detection methods is analyzed when faced with high variability of wind generation. Similar to the second case study, the wind power plant with 100MW of capacity is connected to the 8^{th} bus. Table 4 features the evaluation metrics for the selected techniques under different test scenarios. As can be seen, the addition of the wind power plant of the same capacity leads to an even higher deterioration of the performance of SVM and BLSTM, while TCN, Vanilla WaveNet, and the proposed method are only slightly affected. The reason for this lies in the fact that wind generation is characterized by frequent turbulent changes in the output power leading to turbulent changes in the system states. As a consequence, when the attacks are performed on some of the system states, the reference methods attribute these state fluctuations to the variable wind generation rather than to the attacks. As in the second case

TABLE 3. Summary of test results - Case Study II.

	SVM			BLSTM			TCN			Vanilla WaveNet			Proposed Method		
Inject	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%
θ_2	97.50	99.51	0.11	98.33	99.51	0.09	99.62	99.84	0.11	99.62	**99.88**	**0.07**	**99.74**	**99.88**	**0.07**
θ_3	98.41	99.63	0.22	99.81	99.8	0.02	99.29	99.82	0.11	99.29	99.82	0.11	**99.82**	**99.98**	**0**
θ_4	99.15	99.82	**0.07**	98.85	99.72	0.18	98.89	99.76	0.09	99.31	99.74	0.18	**99.86**	**99.88**	**0.07**
θ_5	98.69	99.74	**0.05**	**99.76**	**99.84**	**0.05**	99.65	99.80	0.16	99.42	99.84	0.09	99.53	**99.84**	0.07
θ_6	**100**	**100**	**0**	**100**	**100**	**0**	**100**	**100**	**0**	**100**	**100**	**0**	**100**	**100**	**0**
θ_7	93.35	98.86	**0.02**	97.19	99.28	0.30	98.64	99.57	0.07	98.24	99.63	0.09	**99.29**	**99.72**	0.09
θ_8	59.86	92.75	01.04	95.78	99.26	0.25	97.47	99.47	0.18	97.98	99.47	0.27	**99.59**	**99.73**	**0.11**
θ_9	97.53	99.55	0.15	99.38	99.82	0.11	99.21	99.82	0.09	99.21	99.80	0.11	**99.53**	**99.88**	**0.07**
θ_{10}	97.04	99.43	0.11	97.88	99.67	0.36	97.97	99.40	0.34	**99.62**	99.82	0.14	99.36	99.78	**0.09**
θ_{11}	96.93	99.30	0.29	96.11	99.35	**0.09**	99.19	99.76	0.14	99.59	99.50	0.52	**99.19**	**99.76**	**0.09**
θ_{12}	99.24	99.76	0.14	98.65	99.67	0.14	99.62	99.86	0.09	98.89	99.76	0.07	**99.50**	**99.78**	**0.07**
θ_{13}	98.24	99.55	0.26	98.78	99.72	0.15	98.87	99.67	0.09	**99.83**	97.14	03.37	99.50	**99.90**	**0.04**
θ_{14}	94.49	98.70	0.73	97.82	99.53	0.20	98.09	99.49	0.27	98.85	99.69	0.16	**99.48**	**99.88**	**0.05**
$\theta_{7,8}$	72.34	94.7	01.26	97.09	99.55	0.20	98.69	99.78	**0.02**	98.04	99.76	0.11	**99.86**	**99.76**	0.09
$\theta_{12,14}$	98.59	99.74	0.11	98.91	99.74	**0.09**	99.50	99.80	0.14	99.75	99.80	0.18	**99.75**	**99.88**	**0.09**

TABLE 4. Summary of test results - Case Study III.

	SVM			BLSTM			TCN			Vanilla WaveNet			Proposed Method		
Inject	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%
θ_2	90.15	98.27	0.79	96.10	99.32	0.28	97.13	99.63	0.06	99.10	99.76	0.15	**99.10**	**99.80**	**0.05**
θ_3	98.09	99.44	0.32	98.36	99.63	**0.14**	99.00	99.71	0.16	**99.25**	**99.74**	0.16	**99.25**	**99.74**	0.16
θ_4	93.76	98.75	0.38	95.30	99.24	**0.09**	97.45	98.43	0.20	98.92	99.61	0.27	**99.06**	**99.78**	**0.09**
θ_5	93.05	98.13	0.77	97.14	99.26	0.30	98.79	99.69	0.12	99.23	99.78	0.09	**99.56**	**99.86**	**0.07**
θ_6	96.29	98.82	0.69	90.04	98.26	**0.07**	98.31	99.43	0.14	**99.76**	**99.90**	**0.07**	99.53	99.84	0.09
θ_7	40.95	91.21	**0.02**	91.77	98.63	0.33	98.41	99.63	0.20	98.85	99.39	0.18	**99.20**	**99.80**	0.07
θ_8	38.47	92.25	**0.06**	83.90	98.23	0.09	96.36	99.47	0.17	97.00	99.67	0.12	**99.04**	**99.78**	0.11
θ_9	68.26	94.79	0.11	95.92	98.44	01.13	97.40	99.55	0.19	97.76	99.43	0.27	**99.47**	**99.80**	**0.04**
θ_{10}	88.85	97.78	0.30	96.46	99.35	0.02	98.08	99.59	0.1	99.33	99.40	0.59	**99.44**	**99.86**	**0.01**
θ_{11}	88.36	97.31	0.92	96.48	99.09	0.55	99.28	99.42	0.15	**99.40**	**99.82**	0.09	99.28	99.80	**0.05**
θ_{12}	90.45	97.99	0.84	98.80	99.72	0.13	98.65	99.72	0.11	98.75	99.74	0.1	**99.55**	**99.86**	**0.09**
θ_{13}	87.54	97.60	01.05	98.02	99.70	**0.07**	**99.67**	**99.88**	0.09	99.08	99.59	0.18	**99.67**	**99.88**	0.09
θ_{14}	70.46	93.94	01.30	96.48	99.09	0.50	97.68	99.43	0.23	97.92	99.55	0.14	**99.38**	**99.80**	**0.11**
$\theta_{7,8}$	44.23	93.07	0.13	93.10	99.17	0.13	98.46	99.78	**0.06**	98.66	99.78	**0.06**	**99.23**	**99.84**	0.09
$\theta_{12,14}$	89.72	97.89	0.84	96.55	99.43	0.13	97.15	99.49	0.16	98.08	99.59	0.18	**99.55**	**99.84**	**0.11**

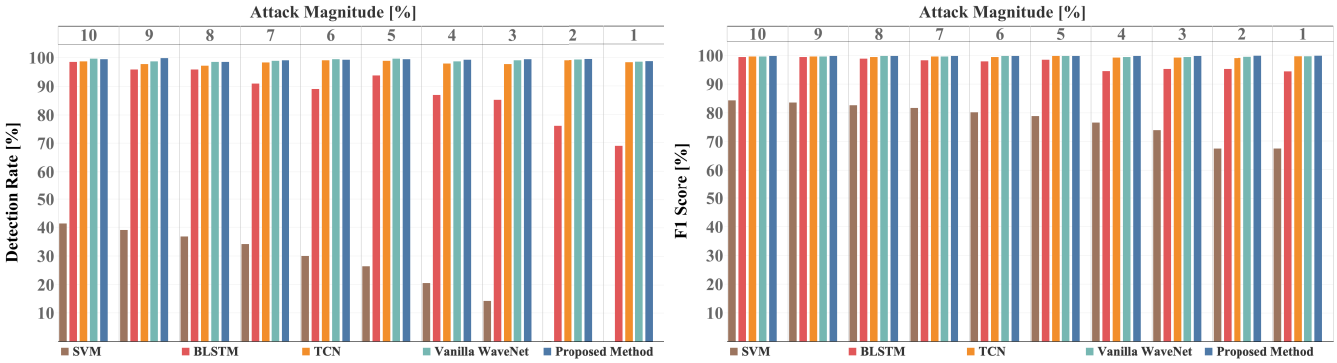
study, when the attacks are performed to the phase angle of the 8^{th} bus, SVM exhibits the worst performance, being able to detect only 38.47% of the attacks. BLSTM, TCN, and Vanilla WaveNet are outperforming SVM; however, their performance is also affected up to a certain extent by the addition of the wind power plant. In the end, the performance of the proposed method is only slightly affected by the addition of the wind power plant, proving its superiority over the reference methods in most of the analyzed scenarios.

G. CASE STUDY IV: POWER SYSTEM WITH A HIGH PENETRATION OF RENEWABLE ENERGY SOURCES

Power system scenarios analyzed in the first three case studies represent realistic scenarios that can be found in present power systems. However, aiming to reduce the carbon footprint of the electricity sector, it is expected that the power systems will reach extremely high levels of renewable penetration. Therefore, it seemed appropriate to analyze the performance of the proposed algorithm in such an environment. In this case study, two wind power plants with a nominal capacity of 50MW are connected to buses 8 and 12, along with two solar power plants with a nominal capacity of 50MW connected to buses 11 and 14. Since the peak load in the system is around 250MW, the installed renewable capacity can account for almost 80% of the power supply, depending on the availability. The results for all of the test scenarios are shown in Table 6. As can be seen, SVM is unreliable in a highly volatile environment. Similarly, the high penetration of RES poses problems to the performance of

TABLE 5. Summary of test results - Case Study IV.

	SVM			BLSTM			TCN			Vanilla WaveNet			Proposed Method		
Inject	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%	DR%	F1%	FPR%
θ_2	80.20	96.18	0.75	90.78	98.35	0.25	98.51	99.60	0.19	98.86	99.71	0.14	**99.49**	**99.84**	**0.09**
θ_3	95.16	98.97	0.38	97.61	99.49	0.18	97.73	99.53	0.16	98.26	99.57	0.15	**99.46**	**99.84**	**0.09**
θ_4	94.03	98.81	0.19	98.07	99.61	0.19	98.34	99.61	0.12	**99.66**	99.73	0.10	99.33	**99.80**	**0.09**
θ_5	79.95	96.36	0.39	99.02	99.71	0.16	96.10	99.28	0.11	99.12	99.78	0.09	**99.39**	**99.84**	**0.07**
θ_6	52.35	93.06	**0.07**	97.03	99.55	0.09	99.21	99.74	0.18	98.91	99.60	0.19	**99.53**	**99.78**	0.18
θ_7	47.05	88.63	0.21	90.77	97.96	0.38	98.07	99.61	0.29	99.16	99.44	0.50	**99.79**	**99.76**	**0.14**
θ_8	7.05	78.03	0.29	94.92	98.94	0.19	98.63	99.39	0.15	98.78	99.67	0.14	**99.77**	**99.86**	**0.12**
θ_9	74.21	95.94	**0.02**	95.01	98.85	0.35	97.49	99.22	0.48	98.56	99.43	0.07	**99.07**	**99.67**	0.23
θ_{10}	67.56	94.42	**0.02**	97.10	98.94	0.73	98.74	99.7	0.11	99.07	99.70	0.11	**99.49**	**99.86**	0.07
θ_{11}	52.69	92.47	0.27	95.59	99.18	0.25	99.00	99.71	**0.18**	99.20	99.61	**0.18**	**99.43**	**99.74**	0.20
θ_{12}	23.85	87.67	**0.02**	89.93	97.93	0.82	99.23	99.80	0.1	99.30	99.80	0.09	**99.80**	**99.82**	0.09
θ_{13}	42.82	89.42	0.14	95.16	98.91	0.39	99.38	99.88	**0.02**	99.02	99.78	0.07	**99.87**	**99.92**	0.03
θ_{14}	39.95	88.51	0.34	89.05	97.83	0.48	97.17	99.24	0.37	98.22	99.29	0.17	**99.13**	**99.76**	**0.07**
$\theta_{7,8}$	55.63	90.03	01.97	98.67	99.65	0.14	99.55	99.80	0.13	99.34	99.67	0.16	**99.66**	**99.82**	**0.11**
$\theta_{12,14}$	27.37	88.45	**0**	96.79	98.77	0.95	99.23	99.78	0.13	99.43	99.74	0.13	**99.69**	**99.86**	0.12



(a) Detection rate

(b) F1-score

FIGURE 6. Summary of test results - Case Study V.

BLSTM and TCN. In contrast, both the Vanilla WaveNet and the proposed method represent a reliable tool for the detection of FDIAs, with slight superiority of the proposed method.

H. CASE STUDY V: CORRELATION BETWEEN ATTACK MAGNITUDE AND EVALUATION METRICS

For simplicity, the previous case studies employed an approach widely used in the literature where FDIAs are manifested in a 10% decrease in one or multiple system states at a time. In practice, having the ability to manipulate multiple meters at the same time, the adversary will slowly increase the magnitude of the attack over time in order to avoid turbulent change in the system states which can be easily detected under certain conditions. As such, it is necessary to determine the threshold of the attack magnitude at which the proposed method fails to detect most of the attacks. To demonstrate the performance of the analyzed methods under different attack magnitudes, the estimated states obtained in the previous case study were used to generate 10 attack scenarios with attack magnitudes ranging from 1% to 10%. The attacks with a random duration of up to 2 hours (24 samples) are performed randomly affecting the phase angle of the 8^{th} bus. The test results containing the detection rate and the F1-score are shown in Figure 6. As can be seen, as the magnitude of the attack decreases, the performance of SVM deteriorates significantly. As the magnitude of the attack approaches 2%, SVM is not able to differentiate between normal and attacked samples. BLSTM follows a similar pattern, however, it's still outperforming SVM by a significant margin. On the other hand, decreasing the magnitude of the attack even up to 1% doesn't affect TCN and WaveNet at all, with WaveNet slightly outperforming TCN. Since FDIAs with attack magnitudes lower than 1% aren't regarded as severe threats, it is safe to conclude that the proposed method presents an efficient solution for the detection of realistic stealthy FDIAs.

TABLE 6. Summary of test results - Case Study VI.

	SVM		BLSTM		TCN		Vanilla WaveNet		Proposed Method	
Scenario	DR%	F1%	DR%	F1%	DR%	F1%	DR%	F1%	DR%	F1%
Without RES	89.66	94.13	94.31	94.78	95.27	94.72	95.92	95.22	**97.47**	**96.70**
With RES	84.01	87.04	93.69	94.49	95.87	94.90	95.21	94.76	**96.74**	**95.49**

I. CASE STUDY VI: SCALABILITY ANALYSIS

Modern power systems are large-scale dynamic systems consisting of up to several hundreds of buses. Although providing promising results on a simple 14-bus test system, the proposed method needs to be tested for its scalability. As such, this case study features the performance analysis of the proposed method on an extended version of the IEEE 118-bus system proposed in [52]. Two characteristic scenarios have been analyzed, namely the scenario without renewable generation, where the total demand in the system is supplied by conventional generation capacities, and the test system version explicitly proposed in [52]. The test system incorporates 54 buses with installed different types of generation capacities. The publicly available database provides time-synchronized data for active and reactive power demand, wind, solar, and hydro generation on an hourly level. For the purpose of the analysis, the time-synchronized data were downscaled to a 5-minute interval, and a 6 month period was simulated leading to more than 50 thousand samples of 235 states. During the observed period, multiple simultaneous FDIAs of different magnitude (ranging from 1 to 10%) have been performed to randomly selected states. The test results are shown in Table 6. As can be seen, the trend from the previous case studies continued regardless of the different attack scenarios and a larger system. SVM is proven to be an inferior technique for the detection of FDIAs in contrast with employed deep learning techniques. The proposed method has proven superior performance over the benchmark techniques in terms of its high accuracy. In terms of its performance after the addition of RES, TCN and WaveNet are proven to be more robust since they experienced only a slight performance drop.

V. DISCUSSION AND CONCLUSION

With the rapid development of smart grids and their dependence on communication technologies, cybersecurity of power systems is becoming increasingly important. FDIAs represent a class of cyber-attacks that targets the power system state estimation. Many recent studies present a variety of statistical, machine learning, and deep learning methods aimed at detecting FDIAs. However, the literature does not answer whether the existing methods can be applied to power systems with a high share of variable renewable energy sources.

In general, the output power of variable renewable energy sources is subject to uncertainty and it is usually difficult to predict in advance with high accuracy. This uncertainty leads to inherent power and voltage fluctuations that alter the underlying distribution of measurements and system states. In other words, the addition of variable renewable energy sources increases the spatiotemporal complexity of the system states. Therefore, methods aimed at detecting FDIAs must show robustness to the unpredictable nature of renewable energy sources.

By performing numerical simulations, a strong correlation between the level of installed renewable capacity and the accuracy of existing methods was found. Specifically, the accuracy of existing methods decreases as the installed renewable capacity increases. To overcome this problem, this paper proposed the use of an Auto-regressive model called WaveNet for achieving accurate detection of FDIAs in renewable power systems. In addition, an architecture modification of WaveNet is introduced which further improves its performance.

WaveNet is a deep neural network previously used in audio processing to generate raw speech signals. The core concept of WaveNet is the use of dilated causal convolutions, allowing the spatiotemporal features of the input data to be captured by expanding the receptive field without increasing the number of parameters of the model. In this study, we have explored how depth and width in the architecture of WaveNet affect the performance of the model. In this regard, the depth of the model was varied between 9 and 16 residual blocks, and the width of the model was varied between 1 and 3 branches inside each block respectively. In general, increasing the depth and width of the model improves its performance. However, as the depth/width of the model increases, the complexity of the model increases as well. Therefore, finding the optimal architecture is crucial in order to avoid overfitting, which may occur in the early epochs unless a stronger regularization is used. From numerical experiments, it was concluded that increasing the depth of the model improves its performance only up to the point where the receptive field exceeds the size of the input sequence. The best sequence size was found to be 32 samples in which 10 residual blocks are enough to cover the input field. Further increasing the depth of the model does not improve its performance. On the other hand, it was concluded that widening consistently improves the performance of the model across different depths. Therefore, it is more efficient to increase the width of the model upon reaching the depth of 10 residual blocks. This is in compliance with recent

research in which width has shown better performance than depth in many applications [53]. Increasing the depth or the width of the model inherently increases its complexity. Nevertheless, increasing the complexity of the model for even a slight improvement in its performance is worth it from the perspective of cybersecurity, because if there exists a probability of launching a successful stealthy FDIA, the power system is exposed to a constant threat. To demonstrate that the proposed architecture modification does not impose any practical limitations, the average recorded computation time for training and testing the proposed method are reported in Table 7. The time required to train the proposed model is not an important indicator, because the model can be trained offline and later used real-time to detect the presence of FDIAs. On the other hand, the computation time of the model needs to be significantly lower in comparison with the update rate of state estimation. Considering the update rate of the practical SCADA systems, the proposed method can be used to a high extent to ensure the cybersecurity of state estimation in real-time. Furthermore, the recorded results suggest that the computation time is almost independent of the size of the test system, meaning that the proposed method can be used for large-scale systems.

TABLE 7. Computation time of the proposed method.

Computation time	14 bus system	118 bus system
Training	469 ms/iteration	479 ms/iteration
Testing	77 ms/sample	80 ms/sample

The proposed method was tested on the modified versions of the IEEE 14-bus system and the IEEE 118-bus system, and its performance was compared with machine learning and deep learning models, namely SVM, BLSTM, TCN, and the Vanilla WaveNet. Using benchmark techniques in six different case studies, the superiority of the proposed method was confirmed in terms of the highest detection rate, highest F1-score and lowest false positive rate. The proposed method was able to detect most of the attacks under different test scenarios with an average detection rate of 99%, outperforming the benchmark techniques due to its capability of capturing long-term dependencies in the input data. In order to examine how uncertainty affects the performance of the suggested architecture, real-time generation profiles of renewable energy sources have been used. The results show that the proposed method is robust to the unpredictable nature of renewable energy sources due to its power to extract more abstract features and obtain a higher receptive field. Even though the accuracy of the proposed method would decline due to the existence of uncertain renewable energy sources, this accuracy drop is not significant enough to make the prediction unreliable. In fact, the reported results prove the reliability of the proposed method in various energy supply structures.

Since the analysis laid down in this paper assumes a fixed system topology, further work will focus on adapting the proposed method to accommodate frequent topology changes. Moreover, like other detection-based strategies, the proposed method is not intended to identify the compromised measurements. Therefore, further work will involve extending the proposed method with this functionality to provide accurate estimates of the system states even under FDIAs. The proposed method will also be extended to different types of cyber-attacks to develop an efficient solution that ensures the security of power system state estimation.

APPENDIX A

Since the subject of this paper is data classification in the context of FDIAs targeting the power system state estimation, it seemed appropriate to mention the characteristics of data used for training and validation of the employed models. Therefore, Appendix A contains a brief summary of the main characteristics of regional loads and renewable energy sources.

As mentioned in Section 4, to create a realistic environment for the training and validation of the employed models, the standard version of the IEEE 14-bus system was modified by assigning each load a certain region of the New York Independent System Operator. Table 8 summarizes the main characteristics of each region and their corresponding buses in the system. As can be seen, the largest portion of the system load is concentrated in the central region related to the third bus in the system. As a consequence of a large number of consumers, the central region is also showing the highest variability during the observed three-month period leading to a relatively high standard deviation. The regional load profiles described here are employed in all of the presented case studies.

TABLE 8. Main characteristics of the regional loads.

Region	Bus	Nominal load [MW]	Mean load [MW]	Standard deviation [MW]
CAPITL	2	21.7	13.11	1.72
CENTRL	3	94.2	67.68	8.18
DUNWOD	4	47.8	22.92	3.14
GENESE	5	7.6	4.55	0.59
HUD VL	6	11.2	5.44	0.73
LONGIL	9	29.5	11.97	1.72
MHK VL	10	9	6.37	0.86
MILL WD	11	3.5	1.70	0.27
N.Y.C.	12	6.1	3.21	0.44
NORTH	13	13.5	9.53	0.75
WEST	14	14.9	9.97	0.94

Case Studies II and IV feature the addition of solar power plants to different system buses. Since different levels of solar penetration were used, Figure 7 presents the normalized solar generation profile in the analyzed period. The daily solar generation profiles follow the typical Gaussian curve

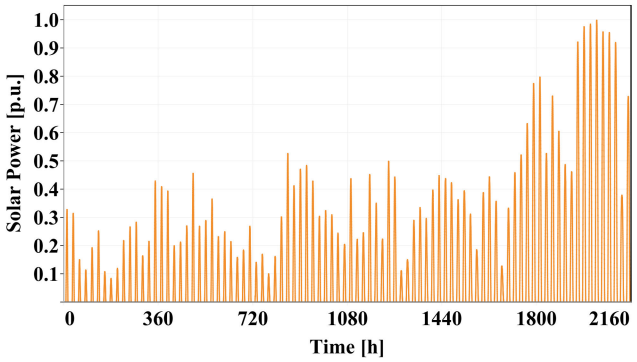


FIGURE 7. Solar generation profile.

with different peak values for each day. It can be seen that the available solar generation increases towards the end of the observed period. Mathematically, since solar generation is available only during the day, the solar generation profile is characterized by a relatively low mean power of only 0.098 [p.u.] and a standard deviation of 0.18 [p.u.].

Apart from solar power plants, Case Studies III and IV feature the addition of wind power plants with the normalized wind generation profile shown in Figure 8. In contrast with solar generation, wind generation is characterized by more turbulent changes, with some days having almost no wind generation at all. As shown in the case studies, this variability of wind generation poses serious challenges to the existing methods employed for detecting FDIAs. Mathematically, the employed wind generation profile is characterized by a mean power of 0.4 [p.u.] and a standard deviation of 0.28 [p.u.], also proving the higher variability of wind in contrast with solar generation.

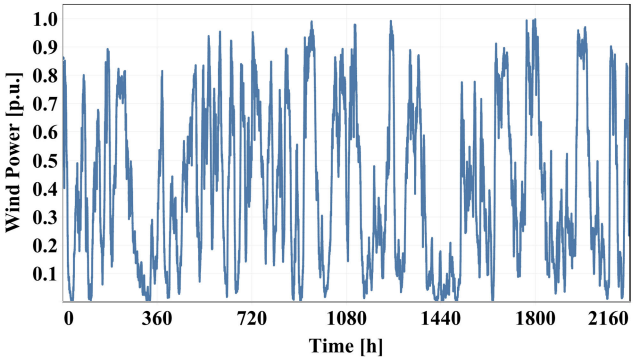


FIGURE 8. Wind generation profile.

APPENDIX B

To further justify the reasoning behind the bus-selection approach used in this paper, Appendix B summarizes the procedure behind the conducted sensitivity analysis and its results. The sensitivity analysis is an iterative procedure which can be described through 4 simple steps:

1) Perform the power flow analysis for the modified power system with renewable generation connected at the k-th bus.
2) After normalizing the system states with respect to their temporal variations, the variance of the state vector at each time step i is calculated as:

$$\sigma_i = \sum_{j=1}^{n} (x_j - \mu_i)^2 \tag{11}$$

where x_j represents the j^{th} state in the state vector, and μ_i represents the average value of the system states at current time-step. Completing this procedure for every time step, the average variance of the state vector σ_{avg}^{k} is calculated.
3) The same procedure described in steps 1 and 2 is performed for every bus k=1,2,...,N, yielding their respective average variances of the state vector.
4) The location providing the highest average variance of the state vector is chosen as the critical location for the connection of renewable energy sources.

The results of the sensitivity analysis are shown in Figure 9, where it can be seen that buses 8, 12, 11 and 14 exhibit the highest influence on the power system, respectively. Furthermore, this influence is reflected to the accuracy and the detection rate of employed methods for the detection of FDIAs, which is demonstrated using SVM. Figure 9 leads to an important conclusion: buses exhibiting the highest influence on the variance of the state vector after the connection of renewable energy sources lead to the lowest detection rate of FDIAs.

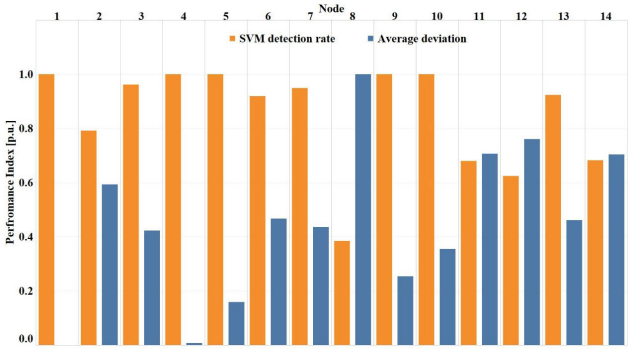


FIGURE 9. Detailed results of the sensitivity analysis.

REFERENCES

[1] K. Khanna, B. K. Panigrahi, and A. Joshi, "AI-based approach to identify compromised meters in data integrity attacks on smart grid," *IET Gener. Transmiss. Distrib.*, vol. 12, no. 5, pp. 1052–1066, Mar. 2018.
[2] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.
[3] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[4] M. Ashrafuzzaman, Y. Chakhchoukh, A. A. Jillepalli, P. T. Tosic, D. C. de Leon, F. T. Sheldon, and B. K. Johnson, "Detecting stealthy false data injection attacks in power grids using deep learning," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 219–225.
[5] A. Ayad, H. E. Z. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using recurrent neural networks," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2018, pp. 1–5.
[6] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *Proc. Joint Workshop Cyber- Phys. Secur. Resilience Smart Grids (CPSR-SG)*, Apr. 2016, pp. 1–6.
[7] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.
[8] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.
[9] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
[10] M. Mohammadpourfard, A. Sami, and Y. Weng, "Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations," *IEEE Trans. Sustain. Energy*, vol. 9, no. 3, pp. 1349–1364, Jul. 2018.
[11] 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.
[12] M. Esmalifalak, R. Zheng, and L. Liu, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Aug. 2014.
[13] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2016, pp. 1395–1402.
[14] A. Foroutan and F. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 161–171, Jul. 2017.
[15] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2019, pp. 1–6.
[16] 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 Trans. Smart Grid.*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.
[17] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3271–3280, Jul. 2018.
[18] Y. Li, W. Huo, R. Qiu, and J. Zeng, "Efficient detection of false data injection attack with invertible automatic encoder and long-short-term memory," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 1, pp. 110–118, Mar. 2020.
[19] T. H. Morris, S. Pan, and U. Adhikari, "Cyber security recommendations for wide area monitoring, protection, and control systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2012, pp. 1–6.
[20] D. Syed, H. Abu-Rub, S. S. Refaat, and L. Xie, "Detection of energy theft in smart grids using electricity consumption patterns," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 4059–4064.
[21] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2326–2329, Mar. 2019.
[22] R. Nawaz, M. A. Shahid, I. M. Qureshi, and M. H. Mehmood, "Machine learning based false data injection in smart grid," in *Proc. 1st Int. Conf. Power, Energy Smart Grid (ICPESG)*, Apr. 2018, pp. 1–6.
[23] S. Basumallik, S. Eftekharnejad, N. Davis, and B. K. Johnson, "Impact of false data injection attacks on PMU-based state estimation," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–6.
[24] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Proc. 1st Workshop Secure Control Syst. (CPSWEEK)*, Stockholm, Sweden, Apr. 2010. [Online]. Available: https://cps-vo.org/content/proceedings-first-workshop-secure-control-systems
[25] 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.
[26] 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.
[27] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Critical Infrastruct. Protection*, vol. 5, no. 3, pp. 146–153, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548212000480
[28] S. Aoufi, A. Derhab, and M. Guerroumi, "Survey of false data injection in smart power grid: Attacks, countermeasures and challenges," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102518.
[29] *Remap 2030: A Renewable Energy Roadmap*, IRENA, Int. Renew. Energy Agency, Abu Dhabi, United Arab Emirates, 2014.
[30] F. Schweppe and J. Wildes, "Power system static-state estimation—Part I: Exact model," *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 120–125, Jan. 1970.
[31] B. Stott, J. Jardim, and O. Alsac, "DC power flow revisited," *IEEE Trans. Power Syst.*, vol. 24, no. 3, pp. 1290–1300, Aug. 2009.
[32] 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, pp. 1–33, May 2011, doi: 10.1145/1952982.1952995.
[33] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.
[34] 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.
[35] A. van den Oord, S. Dieleman, H. Zen, K. Simonyan, O. Vinyals, A. Graves, N. Kalchbrenner, A. Senior, and K. Kavukcuoglu, "Wavenet: A generative model for raw audio," 2016, *arXiv:1609.03499*. [Online]. Available: https://arxiv.org/abs/1609.03499
[36] F. Yu and V. Koltun, "Multi-scale context aggregation by dilated convolutions," 2016, *arXiv:1511.07122*. [Online]. Available: https://arxiv.org/abs/1511.07122
[37] A. Sherstinsky, "Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network," *Phys. D, Nonlinear Phenomena*, vol. 404, Mar. 2020, Art. no. 132306.
[38] R. Pascanu, T. Mikolov, and Y. Bengio, "On the difficulty of training recurrent neural networks," in *Proc. Int. Conf. Mach. Learn.*, 2013, pp. 1310–1318.
[39] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proc. 13th Int. Conf. Artif. Intell. Statist.*, 2010, pp. 249–256.
[40] K. DP and J. Ba, "Adam: A method for stochastic optimization," in *Proc. 3rd Int. Conf. Learn. Represent. (ICLR)*, 2015, pp. 1–15.
[41] J. Duchi, E. Hazan, and Y. Singer, "Adaptive subgradient methods for online learning and stochastic optimization," *J. Mach. Learn. Res.*, vol. 12, no. 7, pp. 2121–2159, 2011.
[42] M. D. Zeiler, "ADADELTA: An adaptive learning rate method," 2012, *arXiv:1212.5701*. [Online]. Available: https://arxiv.org/abs/1212.5701
[43] T. Tieleman and G. Hinton, "Lecture 6.5-RMSPROP: Divide the gradient by a running average of its recent magnitude," *COURSERA, Neural Netw. Mach. Learn.*, vol. 4, no. 2, pp. 26–31, 2012.
[44] S. Ruder, "An overview of gradient descent optimization algorithms," 2016, *arXiv:1609.04747*. [Online]. Available: http://arxiv.org/abs/1609.04747
[45] J. Bergstra and Y. Bengio, "Random search for hyper-parameter optimization," *J. Mach. Learn. Res.*, vol. 13, no. 2, pp. 281–305, 2012.
[46] J. Han, J. Pei, and M. Kamber, *Data Mining: Concepts and Techniques*. Amsterdam, The Netherlands: Elsevier, 2011.
[47] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks," *IEEE Trans. Signal Process.*, vol. 45, no. 11, pp. 2673–2681, Nov. 1997.
[48] C. Lea, R. Vidal, A. Reiter, and G. D. Hager, "Temporal convolutional networks: A unified approach to action segmentation," in *Proc. Comput. Vis. ECCV Workshops*, G. Hua and H. Jégou, Eds. MA, USA: Springer, Oct. 2016, pp. 47–54.
[49] (2016). *14 Bus Power Flow Test Case*. [Online]. Available: http://labs.ece.uw.edu/pstca/pf14/pg_tca14bus.htm
[50] New York ISO Independent Operator. (2016). *Load Data Profile*. [Online]. Available: http://www.nyiso.com

[51] S. Kotsiantis, D. Kanellopoulos, and P. Pintelas, "Handling imbalanced datasets: A review," *GESTS Int. Trans. Comput. Sci. Eng.*, vol. 30, no. 1, pp. 25–36, 2006.
[52] I. Pena, C. B. Martinez-Anido, and B.-M. Hodge, "An extended IEEE 118-bus test system with high renewable penetration," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 281–289, Jan. 2018.
[53] S. Zagoruyko and N. Komodakis, "Wide residual networks," 2016, *arXiv:1605.07146*. [Online]. Available: http://arxiv.org/abs/1605.07146

FAYHA ALMUTAIRY received the B.S. and M.S. degrees in computer science from King Saud University, Riyadh, Saudi Arabia. She is currently pursuing the Ph.D. degree in computer science with the University of Vermont. She is also a Lecturer with Shaqra University. Her research interests include machine learning, smart grids, and cyber security.

LAZAR SCEKIC was born in Niksic, Montenegro, in February 1998. He received the B.S. degree in electrical engineering with specialization in power systems from the Faculty of Electrical Engineering, University of Montenegro, Podgorica, Montenegro, in 2019, where he is currently pursuing the M.S. degree. His research interests include power system analysis, control, and energy storage.

RAMADAN ELMOUDI received the Ph.D. degree in electrical engineering from the State University of New York at Buffalo. He is currently with the Research and Development Group, New York Power Authority, where he manages many projects in New York state concerning implementation of electric grid innovations, asset management, and power system data analytics. He has more than 25 years of industrial experience in power sector. His research interests include power systems modeling and control, artificial intelligence (AI) applications in smart grids, power electronics for smart grids, and advanced protection and automation centers.

SAFWAN WSHAH (Member, IEEE) received the Ph.D. degree in computer science and engineering from the State University of New York at Buffalo. He has a broad experience in deep learning, computer vision, data analytics, and image processing. He has received ten issued U.S. patents with four additional patents pending. He is the author of six journal publications and 23 conference proceedings. He has served on the organizing committee for top conferences and serves as a reviewer/referee for several journals and conferences.