Multi Label Deep Learning classification approach for False Data Injection Attacks in Smart Grid

Prasanna Srinivasan.V[1*], Balasubadra.K[2], Saravanan.K[3], Arjun.V.S[4]and Malarkodi.S[5]
[1]Department of Information Technology, R.M.D Engineering College
Kavaraipettai,Tamilnadu,India
[e-mail:vas.sri81@gmail.com]
[2]Department of Information Technology, R.M.D Engineering College
Kavaraipettai,Tamilnadu,India
[e-mail:kbalasubadra@gmail.com]
[3]Department of Information Technology, R.M.D Engineering College
Kavaraipettai,Tamilnadu,India
[e-mail:saravanan_kv@ymail.com]
[4]Masters Student at Montreal Institute of Learning Algorithm (MILA)
Quebec, Canada
[e-mail:innovatorarjun@gmail.com]
[5]Senior Security Analyst, Photon Infotech,
Tamilnadu, Chennai, India
[e-mail:kmalar008@gmail.com]
[*]Correspondingauthor:Prasanna Srinivasan.V

Received January 10, 2021; revised March 25, 2021; accepted June 13, 2021; published June 30, 2021

Abstract

The smart grid replaces the traditional power structure with information inventiveness that contributes to a new physical structure. In such a field, malicious information injection can potentially lead to extreme results. Incorrect, FDI attacks will never be identified by typical residual techniques for false data identification. Most of the work on the detection of FDI attacks is based on the linearized power system model DC and does not detect attacks from the AC model. Also, the overwhelming majority of current FDIA recognition approaches focus on FDIA, whilst significant injection location data cannot be achieved. Building on the continuous developments in deep learning, we propose a Deep Learning based Locational Detection technique to continuously recognize the specific areas of FDIA. In the development area solver gap happiness is a False Data Detector (FDD) that incorporates a Convolutional Neural Network (CNN). The FDD is established enough to catch the fake information. As a multi-label classifier, the following CNN is utilized to evaluate the irregularity and cooccurrence dependency of power flow calculations due to the possible attacks. There are no earlier statistical assumptions in the architecture proposed, as they are "model-free." It is also "cost-accommodating" since it does not alter the current FDD framework and it is only several microseconds on a household computer during the identification procedure. We have shown that ANN-MLP, SVM-RBF, and CNN can conduct locational detection under different noise and attack circumstances through broad experience in IEEE 14, 30, 57, and

http://doi.org/10.3837/tiis.2021.06.013 **ISSN : 1976-7277**

118 bus systems. Moreover, the multi-name classification method used successfully improves the precision of the present identification.

Keywords: Deep learning, False Data Injection Attack, Internet of Things, Machine learning, Multi-label Classification, Power System, Smart grid.

1. Introduction

The ineffectuality of vital cyber-attack systems presents a significant danger to our society's strength and health. Smart grids that integrate the traditional models of the power systems with Information and Communication Technology ICT are seen as defenseless in particular. This developmental challenge has a weakness in conventional defense measures, starting from the ICT domain [1]. The innovation of the Internet of Things (IoT) has changed the conventional power system considerably. Smart grids incorporate new ICT structures that use bright matrices, propelled databases, and correspondence innovations, as other industrial IoT systems are facing incredible security challenges, especially in the face of rising cyber-attack hazards. The state assessment specifies the status of the power grid network based on the raw figures set up by the system of Supervisory Control and Data Acquisition (SCADA). In general, the exchanged state estimation of the network can interfere with power systems activity [2]. Extensive investigation of the effects on state estimates of cyber threats, such as contact barrier, power outage, congestion line, etc.

The real issue of detecting False Data Injection Attacks (FDIA), where the attackers are expected to negotiate network estimates. This FDIA implies that the Power System State Estimation (PSSE) will be affected [3]. The condition of an energy grid is usually defined by the voltage values on all network buses. FDIA concentrates on resolving the calculation of the status of the power grid by inserting false data into meter calculations. The traditional false data detector (FDD) of the present SCADA device may be utilized for a highly structured FDIA. FDIA is known to be one of the state estimate's most offensive threats [4]. Any imperceptible attack may also be created, even if the attacker has insufficient power system design data. The innovative power system cannot be operated without a reliable PSSE and is frequently operated close to its operational cutoff points. Typically, the PSSE has strategies to recognize abnormal false data and residual faults. When the attacker has adequate information regarding the topology of the system, an entirely structured attack may pass the false data detector on residual data and disrupt the PSSE on an ideal scale [5-6]. Those attacks are known as stealth attacks or imperceptibility [7-8]. The consequences of FDI attacks may be dynamic and vary from financial performance to overburden and actual human threat impact.

Simultaneously, a large number of investigative efforts have been devoted to protecting FDIA from the use of certain physically protected systems [9-10], which are largely classified into two classifications, and information subordinate identification calculations [11-12]. For instance, the basic number of sensors to be monitored must be compromised and a convincing estimate for the optimal PMU circumstance should be developed to avoid FDIA. In any event,

an effective system offers an ideal solution for amplifying insurance standards for compulsory assets. Once again, the FDIA discovery question was suggested to be investigated in different knowledge subordinate estimates, for example, the mixing of Gaussian transmission technologies [13], maximum likelihood estimation, Kalman networks, weak development, theory structure, and the arrangement of comparability [14-15]. Used burden-scale statistics, age plans, and information synchro phasers, for example, provide the empirical description of the spectrum between SCADA-based State calculations and conjecture-based perceptions of chances. Nonetheless, knowledge concerning the attack model and power system details is extraordinarily helpful to the feasibility of the vast majority of abandonment function. Data-driven approaches for acknowledgment based on deep learning were late suggested [16-17]. Deep learning strategies help the system to obtain the models genuinely from knowledge planning, not through a pre-characterized paradigm of attack and power systems. Conversely, all the current strategies just stressed the location of the attacks to the fact that we may learn, i.e., that a malignant attack happens. To quickly develop successful countermeasures, it is essential to recognize the area of attack from time to time other than the recognition of nearness [18]. The irregularity and co-occurrence dependency on identified data from the region often provides additional scope to update the application of proximity recognition.

In this paper, we consider a deep learning tool for location detection FDIA to overcome any problems. Specifically, we discuss the problem of FDIA localization as a multi-name problem. To address this issue, we suggest a design that links the CNN to a traditional FDD detector. To evacuate the low-quality content, the standard FDD indicator is used. To identify the anomalies and co-occurrence dependency of the FDIA, the following CNN is used as a multi-name classifier. The design is convenient as it is without a model and does not require the current FDD Framework to be changed [19]. A household computer has a run time detection process of just a few microseconds. In overview, our main endeavors are as follows.

- As far as the literature survey performed, this paper is one of the first to create an FDIA power system, deep-learning locational detection portion. In specific, it links a deep-neural network with a typical FDD detector, referred to as the " Convolutional Neural Network - Locational Detection (CNN-LD). CNN-LD architecture can apply to the range of hidden attacks and topology models with updated network parameters.
- We formulate the FDIA location detection problem as a multi-label classification problem and use CNN as a classifier to extract power flow correlation functionality and increase location detection ability. We have carefully planned the structure of the network (for example, making pooling layers) and the loss functions according to FDIA's specific architectures.
- We performed comprehensive tests of open-source material and technology to test and evaluate the suggested program. To determine the demonstration and prediction potential of the conceptual structures, border-impact studies are also carried out.

2. Related Work

Ongoing improvements demonstrate that, in FDI attacks, false or malignant data are injected with meters and sensors by sensitively framing the attack vector, that fills the system operator from a feasible, yet off-base system condition. Many experiments have been carried out to establish effective countermeasures to defend against attacks by FDI [20]. Such ventures are commonly classified into two categories: liability security and exposed-based defense, which

defend against FDI attacks. There are also two forms of exposed-based protection. The main thing is for smart meters or sensors to be secured, because the estimating elements, supported by meters or sensors, take on a major influence in the smart grid that is fit for cyber-attacks. The next sort is to ensure that the power system is created. The number and location of measuring meters needed to be secured are important to determine the principal type of protection-based defense that can prevent the estimated meter from being compromised. From the protection perspective of estimate meters, the least expensive method of strategy to guarantee the power system besides FDI attacks has also extended it to explore picking which protection meters and to adopt the financial plan of guards to carry on each of these meters. The authors in [21-22] suggested both accurate and approximate calculations, using the graphical strategies, to choose the basic number estimates besides system protection of many FDI attacks by state factors. For the next sort, the establishment of the power structure is important to the attacker's earlier knowledge. Therefore, securing the data set up of power systems, which becomes necessary to avoid FDI attacks. In [22], the authors investigated FDI safeguard tools using surreptitious topological data.

The FDI attack problem when the attacker provided incorrect information on transmission line admittances. Also, a new vulnerability action has been established to compare and classify grid topologies with incomplete information against FDI attacks. Though this protection-based security will take on a particular duty of preventing FDI attacks, it is hard to ensure that the configuration details and the safeguarded procedures are preserved in the finest condition. Throughout the end of 2015, Ukraine was seen to experience a generous cyberattack [23] professorial collapse, and experts unchanged disperse attackers were able to obtain the lead throughout screaming and the criteria that followed to traverse the everlasting tracking along with observing power system. Enabling authorities to have 5G access to energy consumption monitoring services might also provide them with the information needed to have comprehensive and insightful information about public utilities (e.g., streetlights, traffic cameras, building heaters, others). Optimizing city energy management can be done by identifying the primary energy sources it is also important to invest in methods that enable both safer and more secure communications as well as providing end-to-to-end (end-to-to-end) visibility. From this, we have seen a paradigm shift from dedicated resources for dedicated functions to virtual, orchestration, and automation, and software networking for shared resources; moreover, 5G and beyond will see virtual, orchestration, and automation, cloudification, and software network composition for shared resources. Anomaly detection in a lack of security is more damaging to network stability and user data than if the protocols cannot only detect and attack threats in real-time but able to do not respond to them (with minimum delay). Threat/ anomaly such time-sensitive data requires the assistance of AI and ML [25]. In comparison, the protection-based strategy is increasingly material for a limited power network or only very simple smart meters or sensors and associated tests owing to the exorbitant expenses of ensuring that any single genius meter or sensor is put in frameworks. Based on the breaking of the harsh estimates, the detection obstacle against an FDI attack is conducted.

Similarly, Kullback-Leibler Distance (KLD) will be employed toward classifying FDI attacks by utilizing in such a way to greater KLDs were formed when injected false data was applied to the force structures and estimate varieties were possibly misleading [26]. The quality of identification was therefore partial through the constant limit for this technique. It can be observed that the power grid measurements are of inherently small dimensions and the sparse nature of FDI attacks and mechanisms. To solve the problem, they have been utilizing methods of reducing nuclear requirements and low-grade matrix factorization. In either

scenario, the FDI attacks detection techniques for a broad electricity grid, suggested with the well-developed multifaceted complexity of computational technology [26-27]. Instead of the state estimates which might attain efficient FDI attack locations in four individual situations [28], a distributed host scheme was suggested based on collaborative determinations: single, sparse, random, and dense four kinds of appropriations for false measurement data.

3. POWER SYSTEM NETWORKS

1. AC State Estimation

State estimates are extremely critical for various usage of power systems, such as the ideally suited power flow, load determination, possibility analysis, and currency dispatch, which are all based on state estimate results. AC State estimates utilize non-linear tasks between estimates and system state [29-30], not the same as DC State estimates. The model for comparison is shown as following equation 1.

$$x = h(n) + m\_er \tag{1}$$

Where x is a vector of estimates which includes each actual *Pij* power as well as the reactive power of *Qij* delivered by any two associated buses *i, j* upon this power system topology, and also the actual power injection P_i, and its reactive power injection *Qi* in bus *i*, through $i, j \in N$ where N means the structure of power system buses. n has been the vector for state factors like transportation voltage sizes and stage points where n contains $2\| N \| - 1$ state factors as the slack bus phase angle is continuously set to 0 with $\| N \|$ the sense cardinal to set N, i.e. $n = [\theta_1, \theta_2, \cdots \theta_N, U_1, U_2, \cdots U_N]^T$, where m_er is the measurement errors, and *h(n)* is a nonlinear capability between the vector n and the system state vector n [31] as seen in equation (2)

$$\text{x}\, H\left(x_j \mid n, \delta_j^2\right) = \frac{1}{\delta_j \sqrt{2\pi}} \exp\left\{\frac{\left[x_j - h_j(n)^2\right]}{2\delta_j^2}\right\} \tag{2}$$

2. AC State Estimate FDI Attacks

Usual innovation in false data detection depends on the $ra = m\_er - h(\hat{n})$ residual test. The state calculation value was quite similar to the real system value. False data is acknowledged if the residual is more significant than a certain limit τ, i.e., $\| m\_er - h(\hat{n}) \| > \tau$ Assume each attacker is aware of h(•), just let $\hat{n}_{bad}$ and $m\_er_{bad} = m\_er + bd$ indicate that after the FDI, the system status is incorrect and that the measurement checked is comparable. The corresponding residual from the FDI attacks is obtained in equation 3.

$$\begin{aligned} ra_{bad} &= m\_er_{bad} - h(\hat{n}_{bad}) \\ &= m\_er + a - h(\hat{n}_{bad}) + h(\hat{n}) - h(\hat{n}) \\ &= ra + a - h(\hat{n}_{bad}) + h(\hat{n}) \end{aligned} \tag{3}$$

See from (3) for faults applied to the calculation in AC status reports, if $bd = h(\hat{n}_{bad}) - h(\hat{n})$, it could be passed on false data details [32]. In detail, it is important to monitor certain system state variables when the attacker needs to inject false data in an AC state estimate. It is

a permanent cost and exercise for attackers to collect all data of *h*. Now and then it can take just a few meters to create a good subtle FDIA. In reality, an ideal stealthy attack may also be effectively established with incomplete knowledge of system parameters.

3. The estimation of power states

Estimation of the operational state of a power system through available metering devices In this paper, we consider microgrids, which are preferred due to their advantages of greater reliability, simpler control, and better integration with renewable sources and energy storage units. The relationship between the n-dimensional measurement $z=\left(z_1,z_2,z_3,\cdots,z_n\right)^T$ and the system state $x=\left(x_1,x_2,x_3,\cdots,x_n\right)^T$ can be expressed as equation 4

$$z=Hx+e \tag{4}$$

where error $e=\left(e_1,e_2,e_3,\cdots,e_n\right)^T$ and **H** is the measurement noise and Jacobian represents the uncertainty in Jacobian Conventional 2-norm comparison of measurement error with a minimum-quality threshold τ is made to determine whether or not measurements are bad, that is, compromised. Because this is, in this case, the detector will only signal an attack as long as an attack is presented in equation 5.

$$R=\left\|z-Hx\right\|_2^2\geq\tau \tag{5}$$

4. Locational Detection

The presence of FDIA is numerically proportional to the characterization, for example, *x*, in two classes, of the whole vector estimate: there is or not. For machine learning [33] this is a single label classification problem. However, it identifies the location of the attack in two classes of each element of the vector of estimation, i.e.,x_i. This is, from a machine learning perspective, the issue of locational detection is a multi-label order issue. Since this progress of deep learning in a single label classification over the previous decade has been incredible, multi-label classification is still very exploratory because of its complexity and its broad relevance. Apart from single-label classification, a vast number of meaning indicators, sometimes contradictory in design, can estimate problems relevant to the multi-label classification. The properties of multi-label issues are typically remarkably inconsistent, and the single-label equilibrium methods would hence not work. We design the proposed neural network configuration carefully to isolate and present similar data to generate adequate performances in multi-label classes to solve the problem [34]. In contrast, in our empirical studies, we will even evaluate the improvements to the single label approaches.

5. Convolutional Neural Network

The successful generalization category of Neural Networks (CNN or ConvNets) in the domain of image and video processing in real-time. CNN describes the multi-node, multi-layered neural network. We construct a CNN by using three basic layers: convolution, pooling, and fully connected. In this way, CNN converts the first input layer to the final output which is given as a score. In particular, each convolutional layer and fully connected layers modify both the weights and the biases/activations in the volume. Gradient descent will be used to train the CNN to minimize the difference between the outputs and the dataset class labels [35].

4. PROPOSED MULTI-LABEL LD CLASSIFICATION APPROACH

The system is provided with estimates of discreet time examples from back-to-back, i.e., the time in which the usual estimates occur and the proposed locational detection of FDIA is presented in the **Fig. 1**. Besides, in the process of preparing the CNN classifier, the proposed techniques do not use any earlier factual presumptions (for example, ***H***). This requires estimates and ground truth names. In a sample time *t*, the detail is first observed by the FDD detector (continuous estimation). As seen in Equation. (2), by computing the '2-standard of the remaining and contrasting estimation and the foreordained edge τ, FDD evaluates the quality in measurement data. The current meter is reported by FDD to be undermined or upsetting when $R \geq \tau$. 2 Inspecting and communication errors as a consequence of their strong residual characteristics may be recognized viable as potential unstructured FDIA [36]. Should approximate data pass the FDD, the closeness and region of ordered FDIAs will be calculated by the CNN-based multi-label classifier, by breaking down the anomalies and the co-occurrence dependency including its data.

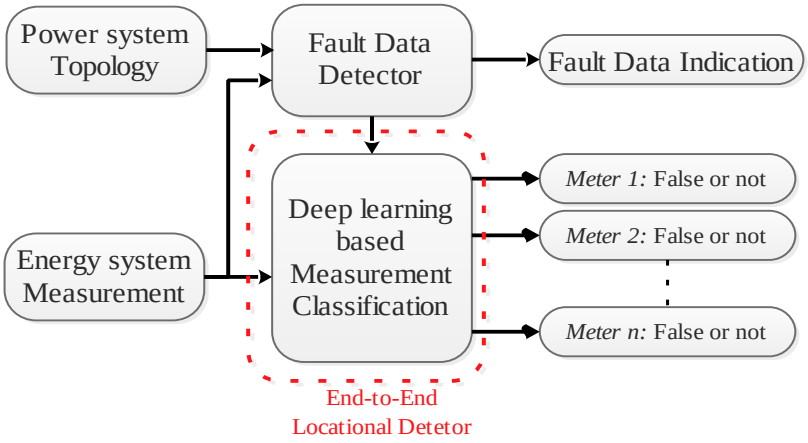


Fig. 1. Proposed FDIA-LD Technique

The CNN-LD hypothesis suggests uses CNN to isolate and analyze the FDIA's high dimensional contextual highlights. They denote the data (i.e., the estimates), ground truth labels (i.e. meter classes), and yields (i.e. CNN period t classifications) as $x^t = (x_1^t, x_2^t, \cdots, x_n^t)$ $m^t = (m_1^t, m_2^t, \cdots, m_n^t)$ $\hat{m}^t = (\hat{m}_1^t, \hat{m}_2^t, \cdots, \hat{m}_n^t)$and, any one of them. The input and output data components are 19 for IEEE 14-bus, in consideration of the fact that 19 measurements occur in our reconstruction settings within the 14-bus system. Meter *i* name for ground reality at time *t* is calculated by the guideline:

$$m_i^t = \begin{cases} 1, & the\ meter\ \ i\ \ at\ time\ \ t\ \ is\ compromised. \\ 0, & otherwise \end{cases} \tag{6}$$

CNN $\hat{m}_n^t$'s performance is consistent in the range of 0 and 1. The classifier then characterizes a range limit for comparing values to 0 or 1. In compliance with the rise or decrease in the specification parameters, the separation edge may be modified. The discrimination limit in this paper is set at 0:25 according to the usual procedure unless otherwise specified.

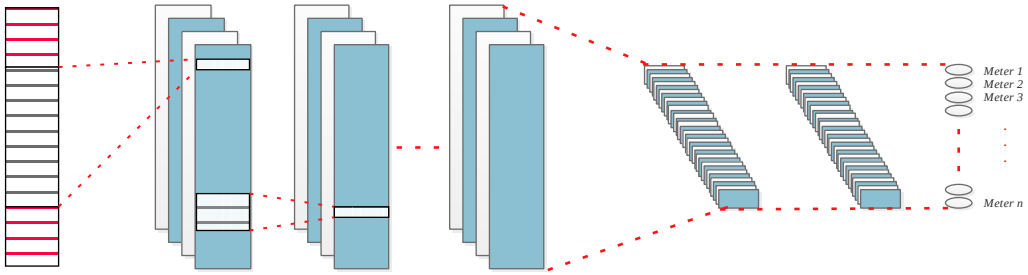


Fig. 2. Proposed 1D Deep Learning CNN Architecture

New CNN architectures also include much of the original CNN's design concepts, such as convolution and pooling. Conventional CNN's use only 2D data; such as images and videos Their name is "2D CNNs". A variation of the 2D CNNs has recently been produced named 1D Convolutional [37]. The experiments have shown that these one-dimensional CNNs have the following advantages when applied to one-dimensional signals:

- For 1D CNNs, instead of matrix operations, FP and BP do Computational difficulty of 1D CNNs is smaller than 2D CNNs.
- The recent work suggests that 1D CNNs with a limited number of hidden layers (i.e. 1D data) are capable of performing challenging functions For instance, in 2D CNNs, certain tasks involve deeper architectures. Networks with shallow interfaces are much simpler to design and Implement.
- Many GPUs and hyperparameter optimization (e.g. Cloud computing or GPU farms). In contrast, traditional machine architectures are feasible and fast for CNNs with a single secret layer (e.g. 2 or less) and fewer neurons (e.g. 50-100).
- Due to their lower computational demands, 1D CNNs are well-suited for real-time and handheld platforms
- Compact 1D CNNs have been demonstrated to have excelled on applications with little labeled data and dynamic signal variations (i.e., patient ECG, civil, mechanical, or aerospace structures, high-power circuitry, power engines or motors, etc.).

In **Fig. 2**, there are two groups of CNNs, distinguished by their techniques for pooling: 1) “CNN-layers” that include 1D convolutions and 2) Fully connected layers (MLP).

As stated above, the primary parameters of the proposed neural network are: we use two convolutional layers to extract the convolutional features To achieve the balance between the accuracy and computational time, the two convolutional layers are chosen. In particular, the rise in convolution layers would improve the precision, but the computing load often increases. For the experiments reported in this paper, we used two convolution layers to balance both the accuracy and the efficiency. Increasing the number of layers adds a larger number of parameters increases the chance of overfitting [38]. The proposed CNN network hyperparameter settings are shown in **Table 1**.
Each convolution layer has many filters. The length of the kernels is the same as the number of data points and the lengths of kernels are 2, 3, 5, and 7 respectively. A set of kernels that has a length of 5 will extract information for an hour or a day (or several days) about each data item. Also, kernels with lengths of 5 and 7 will identify features from the weekly/annual periodicity. To - the risk of neural network overfitting, the network dropout percentage is set to 0.25.

Table 1. Hyperparameter settings

Stage	Type	Kernal	Function	Output Size
1	Input	-	-	19
2	Conv	5 x 1	Feature Extraction	128
3	BatchNormalization	-	Standardized (Mean = 0 & SD =1)	128
4	Leaky RELU	-	Activation	128
5	Conv	3 x 1	Feature Extraction	256
6	BatchNormalization	-	Standardized (Mean = 0 & SD =1)	256
7	Leaky RELU	-	Activation	256
8	Conv	3 x 1	Balanced Accuracy	128
9	BatchNormalization	-	Standardized (Mean = 0 & SD =1)	128
10	Leaky RELU	-	Activation	128
11	Conv	3 x 1	Balanced Accuracy	64
12	BatchNormalization	-	Standardized (Mean = 0 & SD =1)	64
13	Leaky RELU	-	Activation	64
14	Pooling Layer (Flatten)	-	Reduce learned features	1216
15	Fully Con. Layer (MLP)	-	Buffer	19
16	Sigmoid		Activation	19

The design includes an input layer, some convolutional layers, a smoothing layer, an associated shrouding layer, and an output layer. The input layer contains *n* input numbers which through time refer to the *n* estimates. Filter in the first convolutional layer is used to generate highlights through means of convolution operation, non-linear transformation then batch-normalization with the changed linear unit activation (ReLU)[30] window. The deep CNN architecture for FDIA locational detection is seen in the **Fig. 2**.The entity maps $c_{1,}$ such as the first convolutional layer, which can be transmitted from input N is expressed as equation 7

$$x_{1,j} = \mathrm{Re}\,LU\,(N * h_{1,j} + k_{1,j}) \tag{7}$$

Here, $h_{1,j}$ was its j^{th} convolution bit, which is essentially a 1D filter, and $k_{1,j}$ would be the scalar predetermination that compares. In equation. (5), the entire convolution yield of a generally used deep learning portrait is complemented with a scalar predisposition $k_{1,j}$ [31]. The operation of convolution is defined * in (8) and the performance is described as location *i*.

$$\sum_{n=1}^{k_{1,j}} (h_{1,j})[i] * (N)[i - l + \frac{k_{1,j}}{2}] \tag{8}$$

$k_{1,j}$ and *here indicate separately the duration of the $h_{1,j}$ filter and the operation of the inner product portion. The masked highlights of the (p-1)th convolutional layer generated by the filter are most often used as a contribution to the pth convolutional layer and are then treated. The output may be measured as equation 9

$$x_{p,j} = \mathrm{Re}\,LU\,(x_{q-1} * h_{p,j} + k_{q,j}) \tag{9}$$

Where $x_{p,j}$ has been the p[th] convolutional layer j[th] feature map. There are hyperparameters in the sum of filters on each layer and in the depth of convolutional layers, which can be stated in the reconstruction field. The highlights obtained from the last convolutional layer, i.e. $p_{\max}$[th] convolutional layer, are transformed to a single vector in a smooth layer and cared for in a completely connected hidden layer with the ReLU activation function. That is

$$x_{P,j} = \mathrm{Re}\,LU\,(u_P * x_{p\max} + k_P) \tag{10}$$

Where $x_{P,j}$, u_P, and k_P indicate individual level layer element guidelines, weights, and biases. The nodes are also fully associated with n nodes there in the output layer. The sigmoid activation function is used to order every estimation for the nodes in the output layer. The final multi-label outcome $\hat{m}_j^t$ for meter j at period t is obtained in equation 11.

$$\hat{m}_j^t = sigmoid\,(u_F * x_P + k_F) \tag{11}$$

where u_F and k_F mean the weights and biases of the dense layer, separately. We need to initially update the learning boundaries, i.e., filters h, u weights, and k biases, in each layer before using the suggested locational detection strategy for FDIA 's estimates. This process of parameter tuning is known as training, which indents to determine the appropriate parameters for organizing the input and output as in training data.

a) Cross-validation and mini-batch: We are taking the mini-batch to eliminate blood openings to render it appropriate for Understanding and reject over-fitting concentrate. The mini-batch also includes 200 statistics in our simulations. A fixed number of training samples are selected irregularly from each iteration, for example, a mini-batch, to calculate the direction. By normal machine learning practices, 7/10 is separated in a prepared set and 3/10 is included in each cluster's approvals. The fitting process is completed by the Adam optimizer through a learning speed of 0.001 and a tolerance of 5 underlying.

b) Loss function: We are aware of the difficulty of a loss function in measuring the true outcome from ground truth for any set that is more than normal to locate an optimal learning parameter. The failure potential of the new CNN is selected for cross-entropy function, to expand the enterprise to multi-label arrangements. The crossing is a loss function to a mini-batch $\theta = \{t_1, t_2, t_3, \cdots, t_{200}\}$ is achieved by equation 12.

$$cross\ entropy\ (\theta) = \sum_{n\in\theta} -\frac{1}{N} \sum_{i=1}^{N} (\hat{m}_i^t \log (m_i^t) + (1 - \hat{m}_i^t \log (1 - \hat{m}_i^t))) \tag{12}$$

We will obtain the Adam [30] analyzer to define the total limits of a mini-batch θ with an unmistakably marked loss function.

5. IEEE BUS Test System

Throughout this portion, we are reviewing the demonstration in the IEEE 14, 30, 57, and 118 transportation power frames of the proposed FDIA locational detection tool. System topologies may be obtained from MATPOWER [34] and described in **Table 2**. Measurements

in meters become often interlinked along with parallel buses or sections. Moreover, by splitting the meter figures of the adjacent lists CNN earns highlights. We list the meter calculations dependent on the topology of the network. We mention the stream meters of q = 1 in this document as first:

i) the unindexed meters of bus q and set q = q + 1 are listed;

ii) They finish the listing process if q > 14(30,57 and 118);

iii) the strategy should transform to *i* in every case.

At this stage, the index is carried out from line meters and the injection meters are labeled in compliance with the through transport order. For purposes of representation, the IEEE 14-bus structure is defined in **Fig. 3** as a reported detection location. For the convenience of the posts, the location and lists for the 30, 57, and 118-transport systems are ignored.

Table 2. Statistics of IEEE Bus Test Systems

Buses	14 - bus	30 - bus	57 - bus	118-bus
Power Lines	20	39	75	186
Measurements	19	37	71	180
Inject measurements	8	13	24	70
flow measurements	11	21	47	110
Unmeasured lines	2	3	5	9

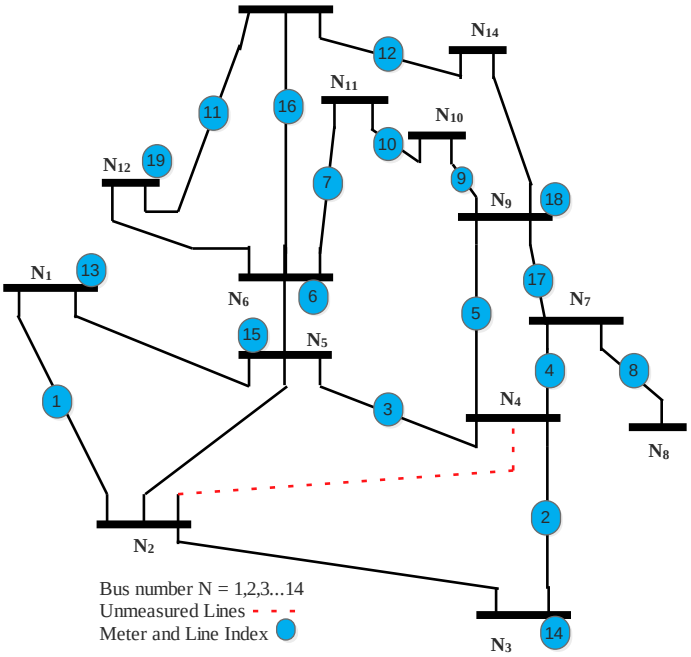


Fig. 3. The 14-bus IEEE Test System

a) Base Load

Firstly, by extending this current knowledge by deliberately producing heaps on each bus, we create optimistic results. The loads generated follow an ordinary flow whose average equivalence is 1/6 of the approximation of the basis load[34] and the normal distribution. We

also produce negotiated information. The two FDIAs are unique to the ordered FDIA and unstructured FDIA. With the usual FDD mechanism in the CNN-LD system, unstructured FDIAs may be stopped. The system must treat us faulty measurements then properly dispose of them. But we establish coordinated FDIA all over.

b) Attack Implementation:

They build knowledge compromised by a min-cut FDIA model of partial network details[10], owing to the restricted financial intentions of the attackers. Most specifically, the individual needing the basic cost of acquiring the information on a certain transmission line impedance is the perfect partial information attack. The system limits are created as follows without missing a detailed statement:

i)A discreet uniform distribution (2; 5) inside the 14- and the 30-bus system as well as a discrete uniform (2; 10), in the specific distribution in the 57- and 118-bus structure follows the quantity of target state variables.
ii) Knowledge regarding the actual transmission line impedance is calculated at the cost of collecting it in the same manner. In each other case, the injection data differ from 1 to 5 and are set to 1.

c) Measurement Noise:

Eventually, since the modes of estimate and communication are unavoidably efficient, we are appreciating periodic Gaussian noise. The standard deviation assumption in specific increases in a figure from 0.1 to 0.5. 5 and in all other cases it is set to 0.2.

d) Metrics of performance assessment:

In our analysis, we use precision and recall including its findings obtained to assess efficiency. Precision and recall are described by

$$\text{Precision} = \frac{TPR}{TPR + FPR} \tag{13}$$

furthermore,

$$\text{Recall} = \frac{TPR}{TPR + FNR} \tag{14}$$

Apart from that. In this paper the probability of a compromised location is assigned to True Positive Rate (TPR), False Positive Rate (FPR), or False negative (FDR), an uncompromised location is separated from the undermined and an uncompromised location is separately wide. We often strike the F1-Score to achieve a form of balance among precision and recall. F1-Score is a consistency and analysis geometrical standard that is informed as

$$\text{F}_1\text{-Score} = 2.\frac{\text{Precision} + \text{Recall}}{\text{Precision} * \text{Recall}} \tag{15}$$

Find three different forms of a quantifiable norm that have long called observable measurement. Root Mean Square Error (RMSE), R-squared accuracy (R2) is a crucial true metric that is a recurrence model presenting the degree of the discrepancy or empirical discrepancies in terms of a relevant variable that can be clarified by a free component, Mean Absolute Error (MAE). The four types of success evaluation used in this study can be overcome using the following conditions,

$$R-Squared=\frac{n\left(\sum ab\right)-\left(\sum a\right)\left(\sum b\right)}{\sqrt{\left[n\sum a^{2}-\left(\sum a\right)^{2}\right]\left[n\sum b^{2}-\left(\sum b\right)^{2}\right]}}, \tag{16}$$

$$RMSE=\frac{\sqrt{\sum_{t=1}^{n}\left(x_{ft}-x_{rt}\right)^{2}}}{\sqrt{n}}, \tag{17}$$

and $$MAE=\frac{\sum_{t=1}^{n}\left|x_{ft}-x_{rt}\right|}{\sqrt{n}} \tag{18}$$

6. Results and Discussions

Initially, we are focusing on the six metrics between SVM-RBF, an ANN-MLP, and a specific IEEE bus system with different numbers and a proposed CNN-LD with a specific IEEE bus system shown in **Table 3**. The 1D CNN-LD proposed system defines three baseline algorithms, which justify the efficacy of the method suggested both in accuracy and recall, F1-Score, precision, R-squared, and RMSE.

Table 3. Comparison of results of specific IEEE bus test method

Technique	No. of Buses	Precise (%)	Recall (%)	F1 Source	Accuracy (%)	R-Squared	RMSE	MAE	Training Time (S)
Proposed CNN-LD									
	14 - bus	99.48	99.17	99.29	98.31	0.7974	0.1074	0.0115	304.9
	30 - bus	99.34	99.21	99.53	98.08	0.8048	0.1057	0.0111	376.6
	57 - bus	99.27	99.39	99.46	98	0.7614	0.1165	0.0135	453.3
	118-bus	99.21	99.44	99.18	97.89	0.9104	0.1783	0.0164	936.7
SVM-RBF									
	14 - bus	83.69	88.51	84.68	89.71	0.7138	0.1036	0.0137	267.4
	30 - bus	83.72	88.13	84.71	89.48	0.7189	0.1047	0.0133	352.1
	57 - bus	83.41	88.27	84.58	89.79	0.7819	0.1041	0.0136	473.7
	118-bus	83.56	88.22	84.64	90.41	0.7352	0.1033	0.0134	986.4
ANN-MLP									
	14 - bus	94.35	97.52	97.93	84.68	0.5714	0.1006	0.0152	327.2
	30 - bus	94.69	97.71	98.16	84.36	0.5891	0.1012	0.0126	417.8
	57 - bus	94.52	97.89	98.19	84.61	0.5793	0.1009	0.0137	583.7
	118-bus	94.17	97.73	98.06	84.49	0.6218	0.1011	0.0132	1073.2

From **Table 3**, we look at the measurements when the number of hidden layers keeps steady on 4. The proposed architecture accomplishes high F1-Score, precision, and recall, accuracy, R-squared, and RMSE. The accuracy obtained by SVM-RBF is higher, although the precision and analysis are lower than those obtained by ANN-MLP. We would like to emphasize that

the CNN's extremely high accuracy is due to the co-occurrence and consistency within the CNN-LD structure we have designed.

In [0;1], the outputs from the CNN $\hat{m}_i^t$'s are fixed, and the separation limit is quantized at 0 or 1. In **Fig. 4**, the segregation limit has been set at 0.5. The estimation of the limit essentially defines the compromise between TPR and FPR. A higher TPR and lower FPR are created in particular by the lower limit. The solution in **Fig. 4** is tested, where FPR versus TPR plots while the limit is 0 to 1. The area under the ROC (AU-ROC) is generally regarded as a performance index of the partial limit to represent relative tradeoffs between TPR and FPR. The area between FPR, TPR, *x*, and *y*-axis is characterized here as AU-ROC. An outstanding AU-ROC model is around 1, which means it is strongly detachable. The algorithm assumes that 1 is 1 and 0 is 0. By the moment a prediction is similar to 0 for AU-ROC, 0 is expected and 0 is estimated. The figure shows that the proposed instrument is close to AU-ROC 1, which response here to the delightful discriminatory limit of the component proposed.

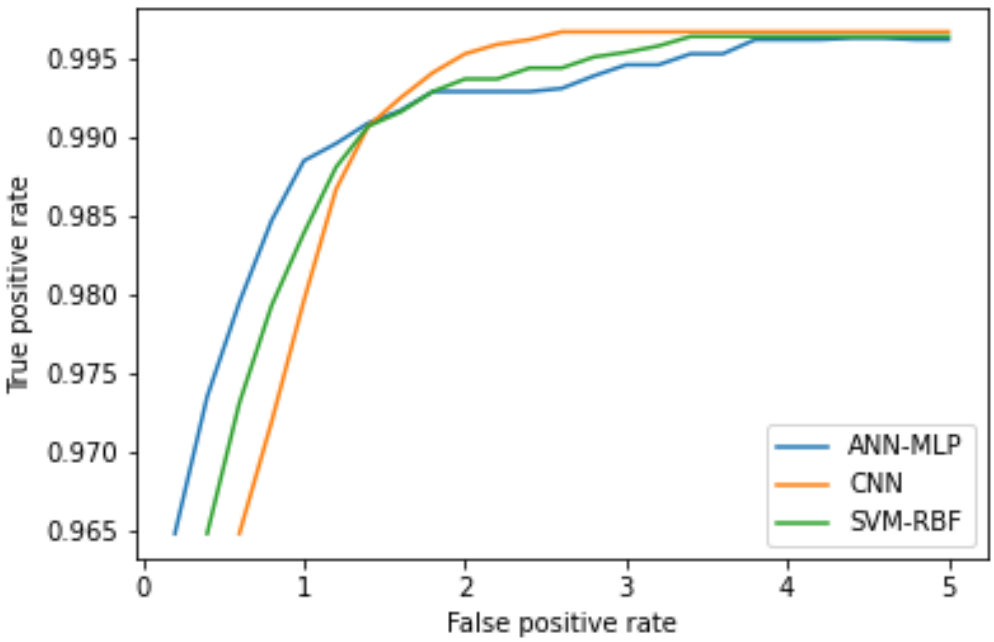
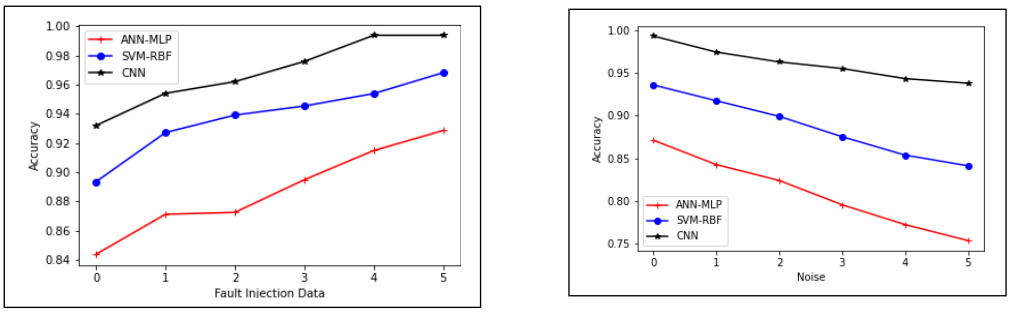


Fig. 4. The proposed mechanism's ROC curve. If FPR decreases from 0 to 0.0002 and then can simply track TPR and FPR from 0 to 0.002. TPR rises to 0.99 very rapidly.

We are drifting away and evaluating how effectively the program works to detect attacks. We consider the power system as optimistic so there is no attack if $\hat{m}_i^t = 0$, in each $i = 0,1,2,\cdots,n$. Everything others are considered as compromised by the power system, or attacks are possible. **Fig. 5** discusses the application of the new instrument for FDIA close detection identification. In specific, the detection performance and the two metrics are compared: SVM-RBF and CNN. We have considered the IEEE 118 bus transport framework for comparing the stealthy FDIA detection through fault-injection accuracy and noise measurement deviation.



(a) (b)

Fig. 5. The accuracy of the IEEE 118- bus system stealthy FDIA detection. (a) Fault-injection accuracy data. (b) Accuracy compared with normal noise measurement deviation.

Fig. 5a demonstrates the detection accuracy of ANN-MLP, SVM-RBF, and proposed CNN-LD identification. The suggested acknowledgment typically accomplishes the most significant exploration quality in comparing proposed 1D CNN-LD and SVM-RBF techniques. We also analyze the accuracy of the similarity detection against the standard deviation of estimates of **Fig. 5b**. Similar to its structure, it fulfills the most remarkable accuracy of the exploration. Until leaving this section we should highlight that given the fact that the plan is based on recognizing FDIA regions, the multi-label classification methodology will enhance the accuracy of the location detection process. That is since the multi-label ensemble imprisons the abnormality of meter predictions and their co-occurrence dependency.

Table 4. Performance Analysis

Model	Year	Accuracy	Precision	Recall	F1_score	MAE	Time
Proposed CNN	-	98.31	99.48	99.17	99.29	0.0115	304.9
FADN-W-2048 [39]	2020	-	-	-	-	0.01894	113.47
DNN [39]	2020	0.843	0.596	0.429	0.487	-	-
1D-CNN [38]	2020	0.871	0.689	0.439	0.536	-	-
TextCNN [38]	2020	0.83	0.956	0.601	0.738	-	-
ANN [9]	2020	80.69	81	81	80	-	6.8
KNN [9]	2020	99.7	99.8	98	99.7	-	25.6
ELM [8]	2019	94.71	-	-	-	-	304.7
CNN-RNN-BiLSTM [36]	2019	0.9712	0.9929	0.999	-	-	-

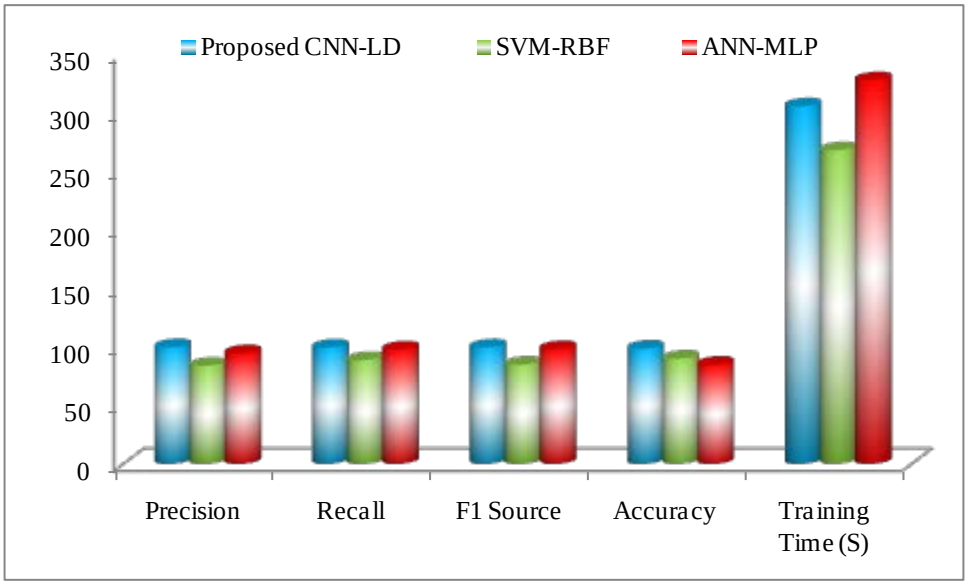


Fig. 6. Performance Comparison

Table 4, gives the comparison of our proposed approach with the existing models in terms of metrics such as Accuracy, Precision, Recall, F1-score, Mean Absolute Error and Training Time. Because of the ability of the proposed CNN model as a classifier to extract power flow correlation functionality and increase location detection, the proposed approach out performs when compared with the existing models. Even though the run time is high in our proposed approach, as overall the performance metrics and quality of the detection process is improved in terms of the quantitative values obtained during the validation. Moreover, Xue, D et.al.,[8] contrasted and proposed CNN to demonstrate the error accuracy parameters during his study. The findings often discuss and compare the general performance metrics and computation time for any model, as the IEEE 14-transport test system is seen in **Fig. 6**. This has helped us to test the FDIA utilizing our results of specific machines. 98.31% of us met performance of 84.68%, and 89.71% respectively.

7. Conclusion

In this paper, we have formulated the locational detection problem of FDIA as a multi-label classification system. The FDD standard is for estimating the quality of measurement data in real-time and for extracting data of poor quality. The CNN is intended to capture FDIA's anomalies and co-occurrences. The mechanism is model-free in that the architecture does not depend on the supposed attack model and it's cost-effective in that the architecture is based on the existing FDD which does not involve the alternation of the existing FDD system and the time of detection on household computers in hundreds of microseconds. Furthermore, in IEEE 14, 30, 57, and 118- bus power systems, we have conducted extensive simulations that demonstrate practicality. We have shown in particular that CNN-LD can detect the entire bus system locally under different noise and attack conditions. In addition, we have also demonstrated that state-of-of-the-the-the-art benchmarks can be better.

References

[1] Z. Chen, W. Hu, J. Wang, S. Zhao, B. Amos, G. Wu, and D. Siewiorek, "An empirical study of latency in an emerging class of edge computing applications for wearable cognitive assistance," in *Proc. of the Second ACM/IEEE Symposium on Edge Computing*, pp. 1-14, 2017. Article (CrossRef Link)

[2] D.W. Roop, "Power system SCADA and smart grids [book reviews]," *IEEE Power and Energy Magazine*, 14(1), pp. 115-116, ISBN 9780367658847, 2015.

[3] V. Kekatos, G.B. Giannakis, "Distributed robust power system state estimation," *IEEE Transaction on Power Systems*, 28(2), pp. 1617-1626, 2012. Article (CrossRef Link)

[4] S. Gao, L. Xie, "Solar-Lezama, A., Serpanos, D., &Shrobe, H. "Automated vulnerability analysis of AC state estimation under constrained false data injection in electric power systems," in *Proc. of 2015 54th IEEE conference on decision and control (CDC)*, pp. 2613-2620, 2015. Article (CrossRef Link)

[5] 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 Transactions on Smart Grid*, 8(4), pp.1630-1638, 2016. Article (CrossRef Link)

[6] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, 5, pp.13787-13798, 2017. Article (CrossRef Link)

[7] J. Fan, Y. Khazbak, J. Tian, T. Liu, and G. Cao, "Mitigating stealthy false data injection attacks against state estimation in smart grid," in *Proc. of 2018 IEEE Conference on Communications and Network Security (CNS)*, pp. 1-9, 2018. Article (CrossRef Link)

[8] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework," *IEEE Access*, 7, pp. 31762-31773, 2019. Article (CrossRef Link)

[9] Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S., "Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques," *International Journal of Environmental Research and Public Health*, 17(24), 9347, 2020. Article (CrossRef Link)

[10] Q. Yang, D. Li, W. Yu, Y. Liu, D. An, X. Yang, and J. Lin, "Toward data integrity attacks against optimal power flow in smart grid," *IEEE Internet of Things Magazine*, 4(5), pp. 1726-1738, 2017. Article (CrossRef Link)

[11] S. Tripathi, and S. De, "Data-driven optimizations in IoT: A new frontier of challenges and opportunities," *CSI Transactions on ICT*, 7(1), pp. 35-43, 2019. Article (CrossRef Link)

[12] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topicsin Power Electronics*, 2019. Article (CrossRef Link)

[13] S.A. Foroutan, and F.R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber-Physical Systems: Theory & Applications*, 2(4), pp. 161-171, 2017. Article (CrossRef Link)

[14] D. Ding, Q.L. Han, Y. Xiang, X. Ge, X.M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, 275, pp. 1674-1683, 2018. Article (CrossRef Link)

[15] T.L. Lin, T.L. Ding, C.Y. Fan, and W.C. Chen, "Error concealment algorithm based on sparse optimization," *Multimedia Tools and Applications*, 76(1), pp. 397-413, 2017. Article (CrossRef Link)

[16] K. Gopalakrishnan, S.K. Khaitan, A. Choudhary, A. Agrawal, "Deep convolutional neural networks with transfer learning for computer vision-based data-driven pavement distress detection," *Construction and Building Materials*, 157, pp. 322-330, 2017. Article (CrossRef Link)

[17] G. Gui, H. Pan, Z. Lin, Y. Li, and Z. Yuan, "Data-driven support vector machine with optimization techniques for structural health monitoring and damage detection," *KSCE Journal of Civil Engineering*, 21(2), pp.523-534, 2017. Article (CrossRef Link)
[18] P. Liu, P. Yang, W.Z. Song, Y. Yan, and X.Y. Li, "Real-time identification of rogue WiFi connections using environment-independent physical features," in *Proc. of IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pp. 190-198, 2019. Article (CrossRef Link)
[19] G. Xu, M. Liu, Z. Jiang, W. Shen, and C. Huang, "Online fault diagnosis method based on transfer convolutional neural networks," *IEEE Transactions on Instrumentation Measurement*, 69(2),pp. 509-520, 2019. Article (CrossRef Link)
[20] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel Distributed Systems*, 25(3), pp. 717-729, 2013. Article (CrossRef Link)
[21] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, "Detecting False Data Injection Attacks Against Power System State Estimation with Fast Go-Decomposition Approach," *IEEE Transactions on Industrial Information*, 15(5), pp. 2892-2904, 2018. Article (CrossRef Link)
[22] 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 Transactions on Smart Grid*, 8(4), pp. 1630-1638, 2016. Article (CrossRef Link)
[23] G. Liang, S.R. Weller, J. Zhao, F. Luo, and Z.Y. Dong, "The 2015 Ukraine Blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, 32(4), pp. 3317-3318, 2016. Article (CrossRef Link)
[24] Guevara, L., & Auat Cheein, F., "The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems," *Sustainability*, 12(16), 6469, 2020. Article (CrossRef Link)
[25] T. Zhou, D. Peng, C. Xu, W. Zhang, and J. Shen, "Adaptive particle filter based on Kullback–Leibler distance for underwater terrain aided navigation with multi-beam sonar," *IET Radar Sonar Navigation*, 12(4), pp. 433-441, 2018. Article (CrossRef Link)
[26] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber-attacks detection using supervised learning and heuristic feature selection," in *Proc. of 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 108-112, 2019. Article (CrossRef Link)
[27] X. Wang, X. Luo, Y. Zhang, and X. Guan, "Detection and isolation of false data injection attacks in smart grids via nonlinear interval observer," *IEEE Internet of Things Magazine*, 6(4), pp. 6498-6512, 2019. Article (CrossRef Link)
[28] G. Folino, and P. Sabatino, "Ensemble based collaborative and distributed intrusion detection systems: A survey," *Journal of Network and Computer Applications*, 66, pp. 1-16, 2016. Article (CrossRef Link)
[29] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, 9(3), pp. 1636-1646, 2016. Article (CrossRef Link)
[30] L. Zhang, G. Wang, and G.B. Giannakis, "Real-time power system state estimation and forecasting via deep unrolled neural networks," *IEEE Transactions on Signal Processing*, 67(15), pp. 4069-4077, 2019. Article (CrossRef Link)
[31] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, 5, pp. 13787-13798, 2017. Article (CrossRef Link)
[32] X. Cheng, Y. Zhang, Y. Chen, Y. Wu, and Y. Yue, "Pest identification via deep residual learning in complex background," *Computers and Electronics in Agriculture*, 141, pp. 351-356, 2017. Article (CrossRef Link)

[33] M. Ganjkhani, S.N. Fallah, S. Badakhshan, S. Shamshirband, and K.W. Chau, "A novel detection algorithm to identify false data injection attacks on power system state estimation," *Energies*, 12(11), pp. 2209, 2019. Article (CrossRef Link)

[34] G. Liang, S.R. Weller, F. Luo, J. Zhao, and Z.Y. Dong, "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism," *IEEE Transactions on Smart Grid*, 9(4), pp. 3820-3829, 2017. Article (CrossRef Link)

[35] Chandel, P., & Thakur, T., "Smart Meter Data Analysis for Electricity Theft Detection using Neural Networks," *Advances in Science, Technology and Engineering Systems Journal*, 4(4), 161-168, 2019. Article (CrossRef Link)

[36] R. Deng, G. Xiao, R. Lu, H. Liang, and A.V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Transaction on Industrial Information*, 13(2), pp. 411-423, 2016. Article (CrossRef Link)

[37] Feng, X., Hui, H., Liang, Z., Guo, W., Que, H., Feng, H. & Ding, Y., "A Novel Electricity Theft Detection Scheme Based on Text Convolutional Neural Networks," *Energies*, 13(21), 5758, 2020. Article (CrossRef Link)

[38] Yang, J., Xi, M., Jiang, B., Man, J., Meng, Q., & Li, B., "FADN: Fully connected attitude detection network based on industrial video," *IEEE Transactions on Industrial Informatics*, 17(3), 2011-2020, 2020. Article (CrossRef Link)

Dr.V.Prasanna Srinivasan, B.E, M.E, Ph.D., is an Associate Professor in the Department of Information Technology, since December 2006. He obtained his B.E (CSE) from Madras University and M.E (Embedded Systems) from Anna University, Chennai. He received his PhD from Anna University, Chennai. He has been in the teaching profession for the past 18 years and has handled UG programs. His areas of interest include Embedded System Design, Design Space Exploration, and Fault Tolerant Systems. He is currently guiding 2 research scholars. He has published 6 papers in refereed International Journals.

Dr. K.Balasubadra, received her B.E. Degree in Electronics and Communication Engineering in 1988 and M.E Degree in Applied Electronics in 1997. She received her Doctorate Degree in Information and Communication Engineering from Anna University, Chennai, in 2009. She has 34 years of teaching experience and has guided many B.E. and M.E projects. Five research scholars guided by her have been awarded Ph.D degree from Anna University, Chennai. Her research interests are Analog VLSI, Optical Communication and Wireless networks. She has published 30 papers in International Journals and 20 papers in conferences in National and International levels. She is a Life member of Indian Society for Technical Education, Member Institution of Engineers (India) and was a member in IEEE for more than 10 years.

Dr.K.Saravanan B.E., M.E, Ph.D., is an Assistant Professor in the Department of Information Technology at R.M.D. Engineering College since 2010. He completed his Diploma in Electrical and Electronics Engineering in the year 2000 from Panimalar Polytechnic, Chennai. He completed his B.E degree in Computer Science and Engineering in the year 2003 from G.K.M. College of Engineering and Technology (Madras University), Chennai and M.E degree in Embedded System Technologies in the year 2007 from Veltech Engineering College (Anna University), Chennai and He completed Ph.D in the 2020 from Anna University. He has 16 years of teaching experience and he has published 5 Papers in International Journals. He is a life member of ISTE.

Mr.Arjun Vaithilingam Sudhakar is a Graduate student in Machine Learning Specialization at the University of Montreal and part of the Montreal Institute of Learning Algorithm(Mila) research lab. He is a recipient of the Microsoft Diversity Award and Université de Montréal / Mila's graduate fellowship that includes tuition fee waivers (Bource C Scholarship). His field of research includes NLP, Computer Vision, and Reinforcement Learning.

Ms.S.Malarkodi is a dynamic certified cybersecurity researcher contributing to a wide range of cybersecurity projects and author and co-creator of the cyber school Blog. Presently she is a technical member in the National Cyber Defence Research Centre (NCDRC) and contributor for OWASP SAMM Tool development. Currently working in a private organisations Photon Infotech as a Senior Security Analyst.