Data-driven Approach for State Prediction and Detection of False Data Injection Attacks in Smart Grid

Haftu Tasew Reda, Adnan Anwar, Abdun Mahmood, and Naveen Chilamkurti

Abstract—**In a smart grid, state estimation (SE) is a very important component of energy management system. Its main functions include system SE and detection of cyber anomalies. Recently, it has been shown that conventional SE techniques are vulnerable to false data injection (FDI) attack, which is a sophisticated new class of attacks on data integrity in smart grid. The main contribution of this paper is to propose a new FDI attack detection technique using a new data-driven SE model, which is different from the traditional weighted least square based SE model. This SE model has a number of unique advantages compared with traditional SE models. First, the prediction technique can better maintain the inherent temporal correlations among consecutive measurement vectors. Second, the proposed SE model can learn the actual power system states. Finally, this paper shows that this SE model can be effectively used to detect FDI attacks that otherwise remain stealthy to traditional SE-based bad data detectors. The proposed FDI attack detection technique is evaluated on a number of standard bus systems. The performance of state prediction and the accuracy of FDI attack detection are benchmarked against the state-of-the-art techniques. Experimental results show that the proposed FDI attack detection technique has a higher detection rate compared with the existing techniques while reducing the false alarms significantly.**

Index Terms—**Data-driven, false data injection, machine learning, power system security, state estimation, smart grid.**

I. Introduction

THE emergence of cutting-edge information and communication technology with the power grid has transformed the energy ecosystem into the current arena of cyber-physical system known as the smart grid. However, their integration into the power grid has also brought a great number of vulnerabilities that pose breaches of data integrity, confidentiality, availability, and so forth. Threats to the smart grid can take many forms, from compromising meter reading, carrying out remote attacks against communication protocols, to compromising power system state estimation (SE) results.

Weighted least squares (WLS) [1] is the most commonly used SE technique in the industry. As an alternative to WLS, the least absolute value (LAV) [2] is considered better for its robustness. Yet, LAV estimators are typically slow and thus insufficient for real-time system monitoring due to the non-convexity and non-smoothness [3]. Further, the conventional SE methods are facing a growing threat from an emerging data integrity cyber-attack known as false data injection (FDI) [4], [5]. Cyber criminals can launch FDI attacks by injecting malicious data over the measurement reading of intelligent electronic devices (IEDs) [1] and these attacks can be crafted in a way to bypass the bad data detection (BDD) process of the SE. In consequence, the FDI attack can mislead the outcome of the SE and lead to a myriad of security risks, including failure of power system operation. Moreover, the conventional SE methods are inadequate to fully track power system variables and customer load profiles that are changing dynamically.

The main motivation of this paper is the challenge of existing SEs against the incumbent FDI attack. Besides, because of the inherent complexity of power systems, the sheer volume of data and the fact that high-performance computing devices are becoming available, data-driven techniques are increasingly powering various applications of the smart grid. For example, [6] has proposed a data-driven FDI attack design where subspace identification technique is employed for the attack construction, and the authors have investigated the attack detection scheme using coding theory in the cyber-physical system environment. Moreover, in [7], a data-driven method based on partial observable Markov decision process for an FDI attack against automatic voltage controls is evaluated using Q-learning algorithm, where a data-driven FDI attack construction and a data-driven defense strategy are suggested. To address the security issues of the existing SEs, this paper proposes a two-stage power state prediction and attack detection (SPAD) framework for power system security. The first stage aims to predict the power system states, and the second stage is used to detect the FDI attacks. Binary classification based on Kullback-Leibler (KL) distance is used for the detection of FDI attacks. Overall, the proposed SPAD framework aims to improve the detection of incum-

Manuscript received: November 26, 2020; revised: March 23, 2021; accepted: March 22, 2022. Date of CrossCheck: March 22, 2022. Date of online publication: June 1, 2022.

H. T. Reda (corresponding author), A. Mahmood, and N. Chilamkurti are with the Department of Computer Science and IT, La Trobe University, Bundoora, VIC 3086, Australia (e-mail: h.reda@latrobe.edu.au; a.mahmood@latrobe.edu.au; n.chilamkurti@latrobe.edu.au).

A. Anwar is with the School of IT, Deakin University, Waurn Ponds, VIC 3216, Australia (e-mail: adnan.anwar@deakin.edu.au).

DOI: 10.35833/MPCE.2020.000827

bent cyber-attack. Deep neural networks (DNNs) are used for the implementation of the proposed framework.

The main contributions of this paper are summarized as follows. ① A model is developed for the state prediction and a KL distance is derived as an attack detection metric. ② Experiments have been conducted considering attack-free scenario and a wide range of false data attack scenarios. In the proposed model, a false data attack alert is generated when the computed KL value of the predicted states is greater than a decision threshold. One of the main reasons why existing BDD techniques fail to detect FDI attack is that the dissimilarity measure (i.e., residual vectors of the SE) after the attack drops below the threshold of BDD. However, our proposed FDI attack detection technique is capable of adjusting the detection threshold adaptive using the probability distributions between estimated states and previously known attack-free states. ③ In addition, the experiments incorporate medium- to large-scale power system transmission networks (namely 39-, 118-, 300-, and 500-bus systems) to evaluate the scalability of the proposed state prediction model. Besides, the proposed model has been evaluated towards network topology changes and compared with the WLS-based SE models. ④ Moreover, the numerical results show that the proposed model can perform estimations very similar to the results of the WLS estimator. The estimation error in terms of mean square error (MSE) of the predictive SE and the WLS is in the order of 10^{-3}, which is acceptable [1] for the purpose of power system SE. ⑤ Finally, the proposed detection technique for FDI attack detects false data attacks with an accuracy of over 98% compared with the existing false data attack detection with an accuracy of below 85%.

The remainder of this paper is organized as follows. First, the background on measurement models and security of the power system SE is briefly presented. Next, Section II reviews the existing literature where related works of existing SE techniques and FDI attack detection techniques are discussed in Sections II-A and II-B, respectively. Section III discusses the architecture and methodology of the proposed SPAD framework and covers comprehensively each method of state prediction and SPAD. Section IV illustrates the experimental setup and performance evaluation of the proposed state prediction. Moreover, the adversary models used within the proposed SPAD framework are examined in Section V. Further, Section VI presents the numerical results and discussion of the proposed SPAD framework. Finally, this paper is concluded in Section VII.

In a control center, an SE aims to obtain optimum system states based on the received measurements. The m-dimensional measurement vector $\boldsymbol{y}$ can be formulated through a non-linear AC model or a linearised DC model [1], represented by $\boldsymbol{y}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{w}$ and $\boldsymbol{y}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{w}$, respectively, where $\boldsymbol{x}\in\mathbb{R}^{n\times 1}$ is the n-dimensional state vector; $\boldsymbol{h}(\cdot)$ or $\boldsymbol{H}\in\mathbb{R}^{m\times n}$ is a function relating measurements and state vectors (also known as the Jacobian matrix); and $\boldsymbol{w}\in\mathbb{R}^{m\times 1}$ is a noise attributed to the measurement errors. Considering a Gaussian noise distribution approximated by $\mathcal{N}(0,\sigma_i^2)$, the WLS estimator uses minimization of weighted sum of the residual squares [1]. After estimation is performed, the SE conducts detection of malicious data, usually through BDDs [1], [8], e.g., chi-squared distribution (χ^2) and the largest normalized residue (LNR) tests. The BDDs compute the residual vectors in terms of ℓ_2-norm (where ℓ_2-norm of $\boldsymbol{r}$ is defined as $\|\boldsymbol{r}\|_2^2=\sum\boldsymbol{r}^2$) between the original measurements $\boldsymbol{y}$ and the estimated measurements $\hat{\boldsymbol{y}}=\boldsymbol{H}\hat{\boldsymbol{x}}$, given by $\|\boldsymbol{r}\|_2^2=\|\boldsymbol{y}-\boldsymbol{H}\hat{\boldsymbol{x}}\|_2^2$. However, [4] and [5] have indicated that if $\|\boldsymbol{r}\|_2^2<\tau$, it also holds true that $\|\boldsymbol{r}_{false}\|_2^2<\tau$ for detection threshold τ. This implies that the FDI attack vector (which can be represented by $\boldsymbol{a}=\boldsymbol{H}\boldsymbol{b}=[a_1,a_2,...,a_m]^{\mathrm{T}}$, where $\boldsymbol{b}=[b_1,b_2,...,b_n]^{\mathrm{T}}$ is the error vector injected by the adversary) can successfully bypass existing BDD techniques that further calls for the development of new SE and/or new detection schemes.

II. Related Work

A. Review on SE Methods

Various SE methods have been reported in the literature. Reference [9] has summarised that the SE problem formulation can follow optimization-only [1]-[3], hybrid machine learning (ML) optimization [9], [10], or just data-driven methods through ML algorithms [11], [12]. Various existing researches on power system SE deal with optimization schemes including WLS and LAV using convex or non-convex iterative solvers. However, the traditional SE models have a number of limitations. First, they are vulnerable to bad data injection including the FDI attack which has been demonstrated in a number of literatures including [4], [5]. Second, the SE algorithms incur high computational complexity as the estimation process mainly depends on initializations [13]. Third, the estimation procedures take longer time [13] that may leave operators to wait between successive measurement instants. Furthermore, the SEs are challenged by the ever-increasing scale and dynamics of the power system [9], [10]. In contrast, data-driven methods can use states from both current and previous timeslots, and can achieve better performance in accuracy, efficiency, and stability. The application of artificial neural network (ANN) in power system SE is one of the contemporary data-driven researches [11], [12]. Autoencoder-based ANN for power system SE using measurement data has been proposed in [12]. Recent research in [10] has shown that DNN-based SE methods outperform the previously mentioned neural network (NN) techniques. In this paper, we propose a predictive power SE based on deep recurrent NN (DRNN) that utilizes the physical network of the power system.

B. Review on FDI Attack Detection Techniques

1) Detection Categories

χ^2 and LNR are two mostly used attack detectors in the SE. However, it has been shown earlier that they are vulnerable to FDI attack. A considerable amount of research has been done in the mitigation strategy against FDI attack and can be broadly classified into three main categories: protection, detection based on SE, and detection based on ML [8]. The first type, which accounts for the majority of the mitigation strategies against the FDI attack, aims to combat the attack by protecting a set of measurement devices [8], [14] (e.g., graph-theoretic, game-theoretic, and topology perturbation). These strategies, however, have a few drawbacks. First, they could only reach on some minimum number of measurements required to ensure the system observability. In addition, the solutions provided could increase burdens to the operator (for example, the perturbation method). Second, their implementation is not economically feasible while adding the protections over a large number of IEDs or other consumer-side devices. Finally, the protection depends on external elements such as a secure IED; however, if the IED itself is compromised, it will affect the method. Detection methods on the basis of SE include forecasting [8], signal processing [15], and statistical modeling [16].

2) *Detection Based on Statistical Distance*

Statistical-based detection schemes [8], [14] are further divided into cumulative sum test, quickest change detection, and detection based on statistical distance. A statistical distance quantifies the consistency of two probability distributions. Compared with the other categories, the distance-based detection methods achieve significant performance against the incumbent cyber-attacks. KL and Jensen-Shannon (JS) distance are two main statistical distance-based methods which have recently been used for detecting malicious measurements. Reference [16] proposes FDI attack detection for power system measurements using KL distance metric. Similarly, [17] suggests FDI attack detection leveraging KL distance metric and joint power and log transformation, where the latter is used to transform measurement variations to improve detection probability. The JS distance metric has been used for attack detection [18] and electricity theft detection of advanced metering infrastructure networks [19].

Table I summarises a comparison of the proposed SPAD framework in this paper with existing works, where P_D is the detection probability; FPR represents false positive rate; TPR represents the true positive rate, and AUC is the area under the ROC curve.

TABLE I
COMPARISON OF PROPOSED SPAD FRAMEWORK WITH EXISTING WORKS

Type	Comparison attributes	[16]	[17]	[18]	[19]	Proposed
SE	Approach	WLS	WLS	WLS	WLS	Data-driven
	Power flow model	AC	AC	AC	AC	DC and AC
	Estimation performance	Not considered	Not considered	Not considered	Not considered	Considered
	Computational efficiency	Low	Low	Low	Low	Low
Detection	Proposed detection approach	Detection of FDI using KL distance	Detection of FDI using KL distance and joint image processing	Detection of FDI using JS distance	Detection of energy theft using JS distance	Detection of FDI using predictive SE and KL distance
	Probability distribution based on	Estimated measurements	Estimated measurements	Estimated measurements	Estimated measurements	Predicted states
	Adaptive threshold	Not considered	Not considered	Not considered	Not considered	Considered
Detection performance	Detection parameter	P_D	P_D, FPR	P_D	FPR v.s. TPR	FPR v.s. TPR
	Detection accuracy	High	High	Unknown	Unknown	Very high
	AUC	Not considered	Not considered	Not considered	Not considered	Considered
	Recall	Not considered	Not considered	Not considered	Not considered	Considered
	Precision	Not considered	Not considered	Not considered	Not considered	Considered

In summary, this paper is unique in the following aspects. One of the key differences lies on the SE method. We have taken the unique FDI attack detection technique using predictive SE, which is different from the existing WLS-based FDI attack detection techniques. The main idea is to avoid WLS-based SE, which is vulnerable to the majority of stealthy FDI attacks. The other feature of this paper is based on the detection threshold. If the detection threshold is relatively high, existing detectors will incorrectly report a false negative, and existing detectors report a false positive when the threshold is very small. This can be challenging especially when the malicious user can inject sparse attack vectors into the measurements. The proposed binary classification algorithm uses adaptive detection threshold using probability distributions of the normal and attack data. Instead of using a default threshold obtained from the KL distance metric, the detector is evaluated using a number of thresholds, where one that results in the optimal detection performance is selected as the optimal decision threshold. Furthermore, unlike existing works on the KL-based detectors, this paper has evaluated a number of detection performance metrics including receiver operating characteristic (ROC) curve, AUC, recall, and precision.

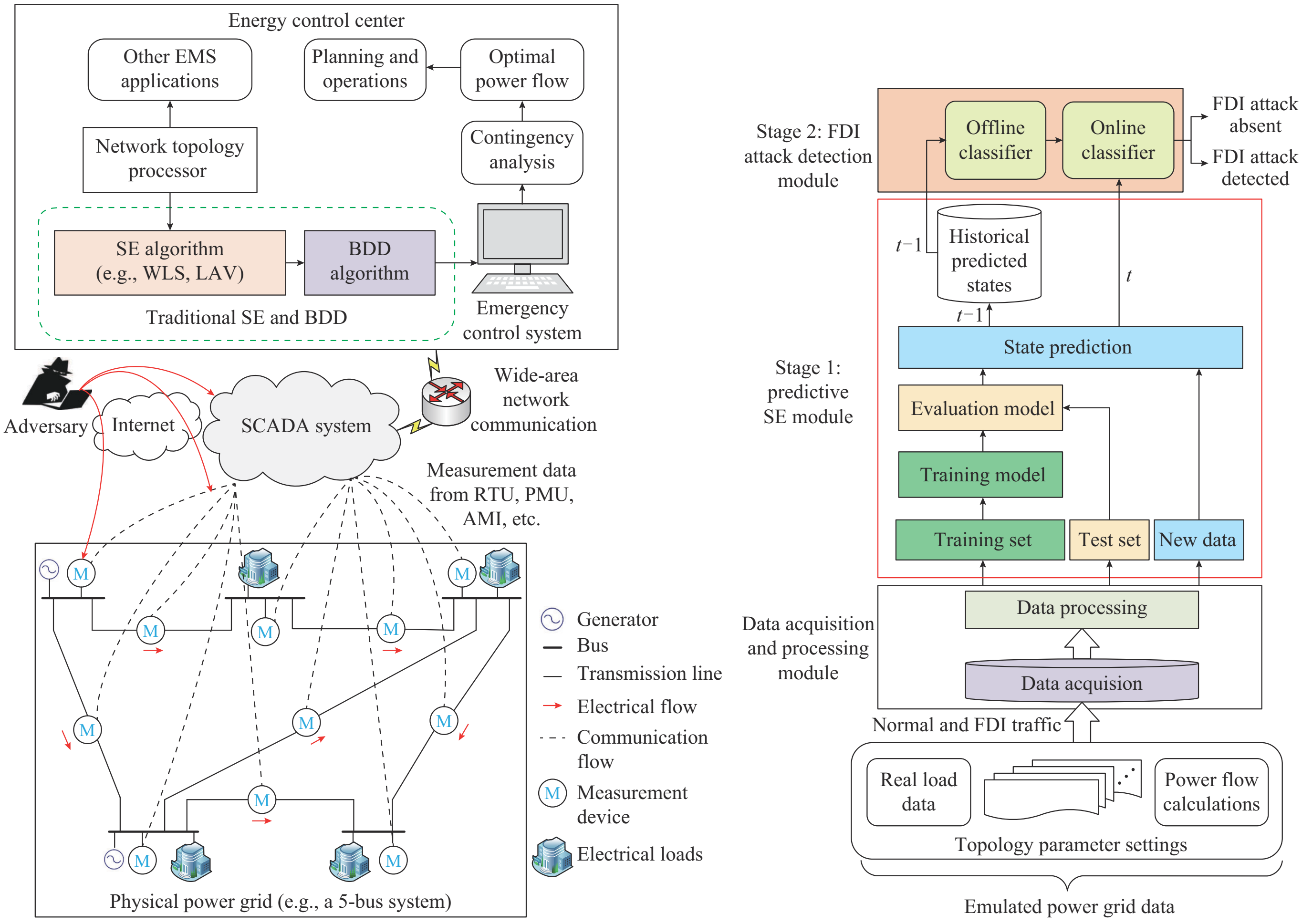
III. ARCHITECTURE AND METHODOLOGY

A. *Proposed SPAD Framework*

Figure 1 shows a block diagram of power system SE and attack detection. Figure 1(a) shows the procedures of SE and attack detection adopted in the conventional energy control center, where SCADA stands for the supervisory control and data acquisition system; and EMS stands for the energy management system. Figure 1(b) is the proposed architecture of the SPAD framework, which augments the SE procedures and cyber-attack detection.

Conventional SE requires network topology processing [1] to be performed prior to the SE procedure. This is specifically indicated by the "network topology processor" in Fig.

1(a), which collects data about circuit breakers and configures real-time system parameters. That is to say, once the network topology is known, the SE assumes that the topology is correct and continues with the estimation and BDD procedures. In our proposed SPAD framework, there is a module called "topology parameter settings" to account for the changes in topology. The following assumption is introduced.



(a)

(b)

Fig. 1. Block diagram of power system SE and attack detection. (a) Considering conventional framework. (b) Considering proposed SPAD framework.

Assumption 1 (topology parameter settings) In one training instance, it is assumed that the topology parameter does not change.

Assumption 1 implies that only one topology parameter is active at any point of time instead of combining the different network topology configurations. In other words, the topology parameter does not change for a configuration considered, and each training procedure is associated with each setup of system configuration. Hence, the datasets are created following the network topology configurations identified by the network topology processor, and are stored in the database of the control center.

For the implementation of the proposed SPAD framework, two DNN concepts namely DRNN and deep feed forward NN (DFFNN) are used. The proposed framework includes three modular elements, namely data acquisition and pre-processing module, predictive SE module (i. e., Stage 1), and the FDI detection attack module (i. e., Stage 2). These are discussed in the following subsections.

B. Data Acquisition and Data Pre-processing

In real-world scenarios, field devices installed over transmission networks measure electrical quantities, and relay their readings to the control centre through IEDs (e. g., Fig. 1(a)). In a typical modern EMS, system operators store plenty of historical measurement data in database systems for a variety of applications such as monitoring and security tools [1]. In this regard, the ML model can be trained using the historical data. In this paper, the proposed data-driven state prediction technique is assessed using data from IEEE standard benchmark systems. The dataset includes measurement sets $\boldsymbol{y}$ as an input and $\boldsymbol{x}$ as an output. Nodal voltage angles/magnitudes, and sensor measurements constituting real power injections at the buses and real/reactive power flows across the branches are generated (as to be demonstrated in Section IV-A).

Further, real-time power load data are used which are obtained from Global Energy Forecasting Competition 2012 [20], hereafter referred to as the GEFCom. The real-time power load data range from the fiscal year 2004 to 2008, altogether 56 months over 20 power utility regions of the USA. More details can be found in Section IV. In DL models, data preprocessing is a critical approach for achieving improved learning efficiency and accuracy. In this step, we deal with inconsistent data, dataset normalization, scaling, and reshaping. In addition, the output variables are scaled to reduce the size of the stochastic gradient descent (SGD), which is used to update weights, resulting in a more stable training model.

C. Proposed Power System State Prediction

The objective of the proposed state prediction model is to infer $\boldsymbol{x}$ based on $\boldsymbol{y}$. The model is trained using a training data sequence given by $S^t=\{(y_{1t},x_{1t}), (y_{2t},x_{2t}), ..., (y_{mt},x_{nt})\}$. As mentioned previously, real-time power load data are used that span a range of time intervals. Hence, the matrix notations $\boldsymbol{Y}$ and $\boldsymbol{X}$ are used for the training and testing, respectively, where $\boldsymbol{Y}=\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1t} \\ y_{21} & y_{22} & \cdots & y_{2t} \\ \vdots & \vdots & & \vdots \\ y_{m1} & y_{m2} & \cdots & y_{mt} \end{bmatrix}$, and $\boldsymbol{X}=\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1t} \\ x_{21} & x_{22} & \cdots & x_{2t} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nt} \end{bmatrix}$.

Algorithm 1 summarises the step-by-step implementation of the power system state prediction. Following Assumption 1 on the topology parameter settings, the following assumption is also considered.

Algorithm 1: power system state prediction

```
procedure ESTIMATE(Y)
  function loadData(·)
    Read network topology configuration
    for $v=1$ to $K$ do
      if $\psi=\Psi_v$ then
        load Dataset{(Y, X)} corresponding to $\psi$
      end if
    end for
  end function
  Initialize weights, epoch, batchSize, learningRate
  trainingSet←80%(Dataset)
  testSet←20%(Dataset)
  Configure model hyperparameters
  Compute non-linear activation functions
  Compute loss function over forward loop
  repeat
  Using ADAM optimiser and learningRate
  Backprop errors, Update weights
  function TRAINMOD(trainingSet)
    for each feature of training set do
      PSEMod←PSEMod.fit(trainingSet, epoch, batchSize)
      return PSEMod
    end for
  end function
  function TESTMOD(testSet)
    for each feature of test set do
      PSEVal←TRAINMOD.evaluate(testSet)
      return PSEVal
    end for
  end function
  end repeat until model improved
  function PREDMOD(y)
    for $m=1$ to $M$ do
      Obtain $y_m$, $\hat{x}$ ← TESTMOD.predict(y)
      return $\hat{x}$
    end for
  end function
end procedure
```

Assumption 2 (network topology configurations) The power grid considered has a finite number of network topology configurations denoted by $K\subseteq\mathbb{N}$. Suppose v is the index of the configurations with $v=\{1,2,...,K\}$.

The *ESTIMATE*($\boldsymbol{Y}$) procedure in Algorithm 1 is used to predict the system states based on the provided input $\boldsymbol{Y}$. The procedure checks which topology configuration is active at any time point and starts loading the dataset, which is given by *Dataset*$\{(\boldsymbol{Y}, \boldsymbol{X})\}$, using the *loadData*(·) function. The corresponding topology configuration is obtained from the topology parameter settings of Fig. 1 which is linked to the network topology processor. Suppose that the set of all finite network configurations is given by $\Psi=\{\Psi_1, \Psi_2, ..., \Psi_v\}|_{\forall v}$. And suppose that the instantaneous network configuration is given by ψ. The procedure is thus expected to load the datasets corresponding to ψ.

Before training the model using the *TRAINMOD*(·) function, hyperparameters such as optimizer, batch size (represented as *batchSize*), and learning rate (represented as *learningRate*), etc. are configured in each layer and weights are initialized using the Xavier normal distribution [21]. A training model *PSEMod* is built after fitting the model on the training set *trainingSet* and the hyperparameters. The function used to train the model is the *TRAINMOD*(·). Then, the trained model is evaluated on the testing set *testSet*. Here, the evaluated model is represented by *PSEVal* where the function is represented by *TESTMOD*(·). Finally, for each measurement reading $m=1$ to M, the state vector corresponding to $\boldsymbol{y}$ is predicted using the improved model. This part is performed by the *PREDMOD*(·) function. Although there are plenty of SGD optimisers including Adagrad, Adadelta, etc. that are suitable for different NN models, ADAM [22] optimizer has been used during the training of the DRNN and DFFNN models. To reduce overfitting, regularization method based on dropout [22] has been used while training the DRNN/DFNN models. Further, Huber loss function is defined while training the DNN models. First, an attack-free dataset is used to train the model, then evaluated with and without the FDI attacks.

1) Motivation for Selection of DNN

RNNs are a class of NNs specialised for predicting a sequence of data involving time. In contrast to FFNNs, RNNs allow cyclical connections that can map to each output from previous inputs. Theoretical and experimental evidences [23] show that DRNNs benefit from the depth of hidden layers and outperform the conventional and shallow RNNs. The depth of RNN is introduced in many ways [23]: input-to-hidden, hidden-to-output, and hidden-to-hidden. Further, for estimating states of correlated power system measurement data, DRNNs outperform the DFFNNs [23]. In this paper, DRNNs are chosen as they are much more robust for prediction and classification tasks than other NNs. Their prediction performance is also compared with the DFFNNs.

2) Model Configuration

For a given observation time t and number of features d, the training sequence for the network model is denoted as $\boldsymbol{s}^t\in\mathbb{R}^d$. The construction of the model is defined through functions between the input, hidden, and output layers. The neuron at the l^{th} hidden layer (represented by $\boldsymbol{h}_l^t\in\mathbb{R}^{d\times n_h}$, where n_h is the number of the hidden neurons) receives the input vector of $\boldsymbol{y}$ and hidden neurons of the previous state. This is represented by (1).

$$\boldsymbol{h}_l^t = \boldsymbol{\psi}_l(\boldsymbol{y}^t, \boldsymbol{h}_l^{t-1}) = \boldsymbol{\psi}_l(\boldsymbol{\omega}_l \boldsymbol{\psi}_{l-1}(\boldsymbol{\omega}_{l-1}\boldsymbol{\psi}_{l-2}, \ldots, (\boldsymbol{\omega}_1 \boldsymbol{h}^{t-1} + \boldsymbol{b}_1 \boldsymbol{y}^t))) \quad (1)$$

where $\boldsymbol{\psi}_l$ is the non-linear activation function of the l^{th} hidden layer; and $\boldsymbol{\omega}_l$ and $\boldsymbol{b}_l$ are the weight vector and bias vector, respectively.

D. Proposed FDI Attack Detection

The KL distance is applied in numerous cases [16]-[19], [24] such as information theory, anomaly detection, data mining, and ML algorithms, and recently, in cyber-attack detection of power system. In this paper, the cyber-attack detection is formulated as a binary classification problem using the KL distance metric. By computing the KL value of the probability distributions between consecutive time steps (i.e., states at the previous time and states at the current time), the detector can effectively monitor the dynamics of the power system states. In the following, we first define the state variations and the corresponding probability distributions, which are important for the detection algorithm.

Definition 1 (state variation) The state variation Δx_i ($\forall x_i \in \boldsymbol{x}$) is the difference between two consecutive states given by $\Delta x_i = x_i(t) - x_i(t-1)$, where t and $t-1$ denote the current and previous time instants, respectively. Let $l_{\Delta x_i}$ and $m_{\Delta \hat{x}_i}$ be the probability distribution of the previous Δx and the predicted current $\Delta \hat{x}_i$, respectively.

Remark 1 After computation of $l_{\Delta x}$ and $m_{\Delta x}$ in Definition 1, the KL distance Λ from $l_{\Delta x}$ to $m_{\Delta \hat{x}}$ can be expressed mathematically as:

$$\Lambda(m_{\Delta \hat{x}} \| l_{\Delta x}) = \sum m_{\Delta \hat{x}} \log_2 \left(\frac{m_{\Delta \hat{x}}}{l_{\Delta x}} \right) \quad (2)$$

Definition 2 (KL distance) $\Lambda(\cdot)$ is a non-negative number, and can be defined as:

$$\Lambda(\cdot) = \begin{cases} \mathbf{R}^+ & m_{\Delta x} \neq l_{\Delta x} \\ 0 & m_{\Delta x} = l_{\Delta x}, \forall x \in \boldsymbol{x} \end{cases} \quad (3)$$

Remark 2 $\Lambda(\cdot)$ of Definition 2 is asymmetrical, meaning that:

$$\begin{cases} \Lambda(m_{\Delta x} \| l_{\Delta x}) = \Lambda(l_{\Delta x} \| m_{\Delta x}) & l_{\Delta x} = m_{\Delta x}, \forall x \in \boldsymbol{x} \\ \Lambda(m_{\Delta x} \| l_{\Delta x}) \neq \Lambda(l_{\Delta x} \| m_{\Delta x}) & \forall x \in \boldsymbol{x} \end{cases} \quad (4)$$

Definition 3 (attack detection) The FDI anomaly detection is formulated as a binary classification problem (defined by (5)) as our aim is to classify measurement samples into normal and FDI attack classes.

$$\delta(\hat{\boldsymbol{x}}) = \begin{cases} 1 & \Lambda(\hat{\boldsymbol{x}}) \geq \tau \\ 0 & \Lambda(\hat{\boldsymbol{x}}) < \tau \end{cases} \quad (5)$$

where τ is obtained from a statistical estimation based on the confidence interval.

The confidence interval is given by:

$$c(\rho) = \bar{\Lambda} \pm z \left(\frac{\sigma_s}{sqrt(S)} \right) \quad (6)$$

where $\bar{\Lambda}$ is the mean of the set of KL values; z is a value obtained corresponding to each detection confidence level ρ as given in Table I; and σ_s is the standard deviation of Λ samples with a sample size of S.

TABLE I
z Values Based on Normal Distribution

ρ (%)	z value
90.0	1.645
95.0	1.960
98.0	2.330
99.0	2.576
99.5	2.807
99.9	3.291

The attack detection algorithm is trained through predicted states of the normal traffic, and evaluated using both normal and bad data injected traffics. Algorithm 2 explains the offline and online FDI attack detection system. *DETECT*(·) is the attack detection procedure. In the offline mode (represented by the *OFFLDETECTION*(·) function), the training model uses adaptive threshold based on the confidence interval of the attack-free traffic. Then, the KL of any incoming traffic is compared against the threshold. Tables II and III illustrate the threshold values obtained for the 1-year and 5-year data corresponding to the z value in Table I, respectively. The two cases are based on the results of the proposed state prediction model. As it can be observed from the two tables, the $\Lambda(\cdot)$ value of those without attack is quite smaller than those of FDI-manipulated data, where the adversary model I is used (threat model is explained in Section IV-C). The performance of the proposed detection system is also compared with the WLS-based KL detection systems in Section V. For a given topological configuration, the detector is trained using the normal traffic to obtain adaptive thresholds for the considered detection confidence level. In addition, the online FDI attack detection is performed for each incoming measurement data and this is illustrated by the *ONLDETECTION*(·) function of Algorithm 2.

IV. Experimental Setup and Performance Evaluation of Proposed State Prediction

In this section, justifications through numerical simulations of the proposed state prediction are presented.

A. Test System Scenario

The data from four power grid standard test systems, i.e., IEEE 39-bus, 118-bus, 300-bus, and ACTIVSg 500-bus systems, are used to assess the performance of the proposed state prediction. The IEEE 118-bus system has 118 buses, 186 branches, with a total of 304 sensor measurements considering the DC power flow. The IEEE 39-bus system has 39 buses, 46 branches, and a total of 85 nodal injections and branch power flows given the DC power flow. For the AC power flow, while the system states include voltage magnitude and phase angle, the measurement data include real and reactive power injections, and real and reactive power flows. Similarly, the IEEE 300-bus and ACTIVSg 500-bus systems have a total of 711 and 1097 measurement data, respectively, considering DC power flow.

Algorithm 2: FDI attack detection

```
Input: $Dataset\{(\boldsymbol{Y}, \boldsymbol{X})\}$
procedure $DETECT(\boldsymbol{Y})$
  function $OFFLDETECTION(\boldsymbol{Y})$
    for each $\boldsymbol{y}$ in $\boldsymbol{Y}$ do
      Evaluate $\hat{\boldsymbol{x}}$ using Algorithm 1
      Evaluate $m_{\Delta\hat{x}}$ as well as $l_{\Delta x}$
      $\Lambda_{hist} \leftarrow \sum m_{\Delta\hat{x}} \log_2\left(\frac{m_{\Delta\hat{x}}}{l_{\Delta x}}\right)$
      Evaluate $\tau$ using (6) and $\Lambda_{hist}$
      return $\tau$
    end for
  end function
  function $ONLDETECTION(\boldsymbol{y})$
    for each smart meter measurement do
      Compute $\hat{\boldsymbol{x}}$ and $m_{\Delta\hat{x}}$
      $\Lambda \leftarrow \sum m_{\Delta\hat{x}} \log_2\left(\frac{m_{\Delta\hat{x}}}{l_{\Delta x}}\right)$
      if $\Lambda(\hat{x}) \geq \tau$ then FDI attack detected
      end if
      if $\Lambda(\hat{x}) < \tau$ then no FDI attack detected
      end if
    end for
  end function
end procedure
```

TABLE II
THRESHOLDS OF Δx FOR 1-YEAR DATA

ρ (%)	z value	KL threshold	
		Without attack	With attack
95.0	2.330	0.0653	2.4637
98.0	2.576	0.0684	2.4891
99.0	2.807	0.0695	2.4975
99.5	3.291	0.0700	2.5017
99.9	3.291	0.0704	2.5051

TABLE III
THRESHOLDS OF Δx FOR 5-YEAR DATA

ρ (%)	z value	KL threshold	
		Without attack	With attack
95.0	1.960	0.2223	2.0764
98.0	2.330	0.2262	2.0992
99.0	2.576	0.2275	2.1068
99.5	2.807	0.2282	2.1106
99.9	3.291	0.2287	2.1136

The experimental dataset is prepared using GEFCom based on an hourly interval. Real-time power load profile of five power zones of two categories are used. The first is for 2004 (a total of 43920 dataset used) and the other is for 2004 to 2008 (a total of 90320 dataset used). The hourly real-time power load data have been sampled to a 5-min interval. This system-level load distribution has further been normalized, distributed to the bus-level load rating of the simulated system. The procedures of dataset preparation of the two test systems and the actual load power data using MATLAB R2019B and MATPOWER [25] are defined as follows. First, the sampled GEFCom power load values are normalized. After setting up the original load case data of the test systems, for each number of samples over the target utility regions, the power loads (including real and reactive) are multiplied by each of the normalized load values. Next, for each of the test systems, the DC and AC optimal power flows are generated. Given the new power load and generation conditions, the system state vectors are then generated. Furthermore, the measurement matrices $\boldsymbol{Y}$ are generated for the AC and DC power flows of the test systems. To be more realistic (i.e., to account for the inherent communication noises against the measurement data), a normally distributed Gaussian noise with mean μ and standard deviation σ is added to the generated measurement. After obtaining the measurement data and system states, the FDI attack is generated using adversarial models I and II shown in Section V. Note that the dataset of the DC and AC power flows are performed independently.

B. Prediction Performance

The proposed state prediction is analysed using the DC and AC power flow models. Implementation results of the DC model for the IEEE 39-bus and 118-bus systems are based on three densely-connected hidden layers. Likewise, the AC model for the IEEE 39-bus and 118-bus systems and the DC model for the IEEE 300-bus and ACTIVSg 500-bus systems are based on six densely-connected hidden layers. Table V is the configuration of the state prediction models with respect to the four test systems for a given observation time. As depicted in Table V and used throughout our numerical simulation, the NN model input refers to the measurement data (e.g., 85 for the IEEE 39-bus system and 304 for the IEEE 118-bus system given the DC power flow), and the NN model output refers to the estimated system states (e.g., 77 for the IEEE 39-bus system and 236 for the IEEE 118-bus system considering the AC power flow) for a given time interval. Similarly, the number of neurons for each densely-connected layer is also described. The following parameters are used while training the NN models for both DC and AC power flows: learning rate is 0.01, epochs are 100, and batch size of training algorithm is 64.

TABLE V
CONFIGURATION OF STATE PREDICTION MODELS

Bus system	Input layer	Hidden layer	Output layer
39-bus (DC)	85	$h_1 = 85 \times 85$, $h_2 = h_1 \times 85$, $h_3 = h_2 \times 85$	38 (for voltage angle)
(DC) 118-bus	304	$h_1 = 304 \times 304$, $h_2 = h_1 \times 304$, $h_3 = h_2 \times 304$	118 (for voltage angle)
39-bus (AC)	117	$h_1 = 117 \times 117$, $h_2 = h_1 \times 117$, ..., $h_6 = h_5 \times 117$	77 (38 for voltage angle and 39 for voltage magnitude)
118-bus (AC)	354	$h_1 = 354 \times 354$, $h_2 = h_1 \times 354$, ..., $h_6 = h_5 \times 354$	236 (118 for voltage angle and 118 for voltage magnitude)
300-bus (DC)	711	$h_1 = 711 \times 711$, $h_2 = h_1 \times 711$, ..., $h_6 = h_5 \times 711$	300 (for voltage angle)
500-bus (DC)	1097	$h_1 = 1097 \times 1097$, $h_2 = h_1 \times 1097$, ..., $h_6 = h_5 \times 1097$	500 (for voltage angle)

Figures 2 and 3 demonstrate the voltage angle and voltage magnitude predictions of the proposed state prediction model and WLS state estimator for IEEE 118-bus and 39-bus systems, respectively. In Fig. 2 and Fig. 3, the predictions are evaluated using unseen test sets.

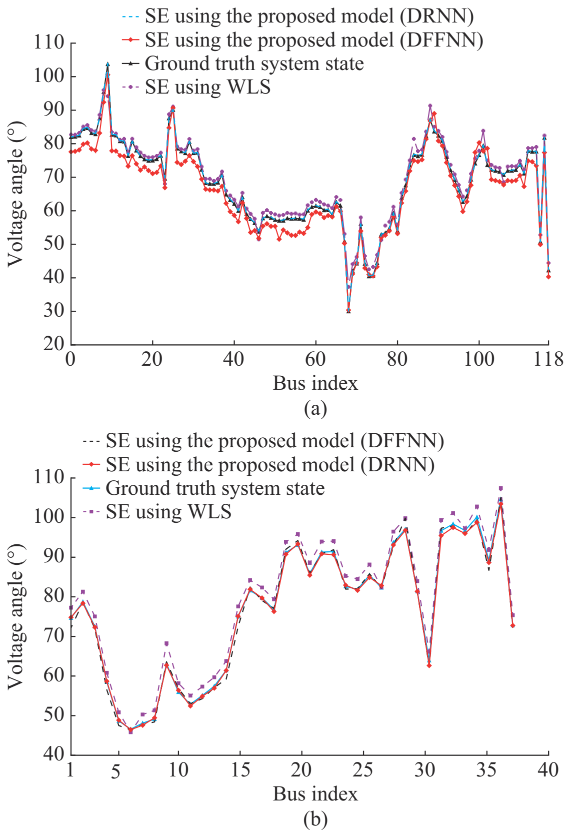


Fig. 2. Voltage angle prediction of proposed state prediction model and WLS state estimator. (a) IEEE 118-bus system. (b) IEEE 39-bus system.

Additionally, to see the efficiency of the proposed model, it has been evaluated using additional unseen data of four different weeks (labeled as week-27, week-28, week-29, and week-52). This is demonstrated in Fig. 4, implemented using DRNN of the proposed model. Additionally, to assess the scalability of the proposed predictive SE method, two larger power system test cases are used: IEEE 300-bus and ACTIVSg 500-bus systems. The plots using the IEEE 300-bus and ACTIVSg 500-bus benchmarks are shown in Fig. 5. In fact, increasing the number of buses of the power grid can also increase the number of measurement points significantly. This, of course, poses a computational complexity towards the learner. However, such challenges can be alleviated by deploying sufficient number of computing devices such as high-bandwidth GPUs or RAMs and/or leveraging feature selection techniques.

The prediction performance of the proposed model is also evaluated against topology changes. This part is assessed in accordance with Assumptions 1 and 2 using the IEEE 300-bus and ACTIVSg 500-bus systems. The aim of this experiment is to evaluate the performance of the predictive SE model if the underlying network topology changes (e. g., such topology updates can be obtained from the network topology processor). In this regard, topology configurations of some selected networks of the IEEE 300-bus and ACTIVSg 500-bus systems have been randomly modified. Only 5 sets of configurations are modified in the IEEE 300-bus system, while 10 sets of configurations are modified in the ACTIVSg 500-bus system.

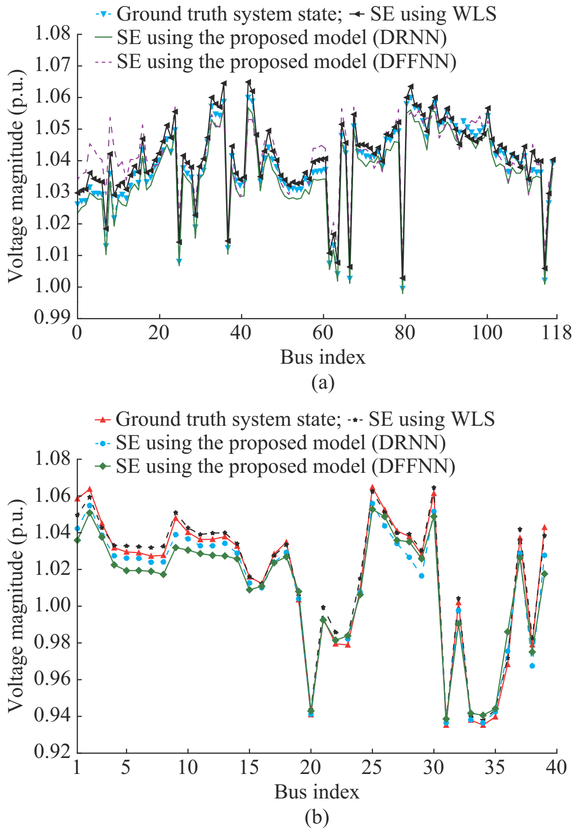


Fig. 3. Voltage magnitude prediction of proposed state prediction model and WLS state estimator. (a) IEEE 118-bus system. (b) IEEE 39-bus system.

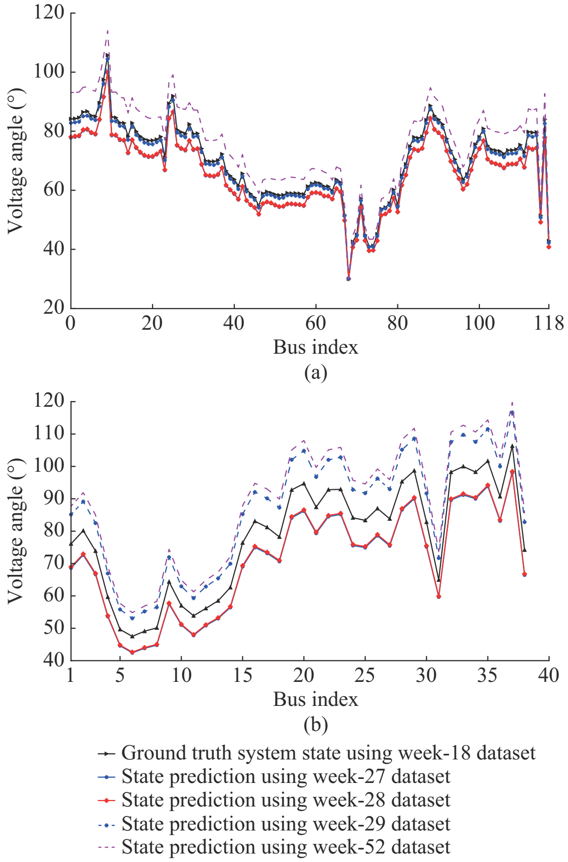
The sets of configurations are parts of the Jacobian matrices $\boldsymbol{H}$ and are generated from MATPOWER [25]. For each configuration, various scaling factors are used to get the topology change. Accordingly, datasets are generated and used for evaluating the prediction performance of the DNN model. The results of SE using the proposed approach and WLS-based SE are shown in Fig. 5 for the IEEE 300-bus and ACTIVSg 500-bus systems.

Numerical results demonstrate that the proposed state prediction is very comparable to the conventional WLS estimator whose estimation error is acceptable for the purposes of power system SE. Except for the AC power flow in Fig. 3, where the DFFNN deteriorates with less prediction results than that of the WLS, the DRNN can perform estimations very close to the result of the WLS estimator.

Furthermore, the performance of the predictive SE is evaluated through the metric MSE. The MSE is defined as (7) for a total number of n states and d observations.

$$MSE(\boldsymbol{x}-\hat{\boldsymbol{x}})=\frac{1}{d}\sum_{t=1}^{d}\left(\frac{1}{n}\sum_{i=1}^{n}(x_i^t-\hat{x}_i^t)^2\right) \tag{7}$$

The performance evaluation in terms of the MSE with the different models for IEEE 39-bus and 118-bus systems is shown in Table VI.



(a)

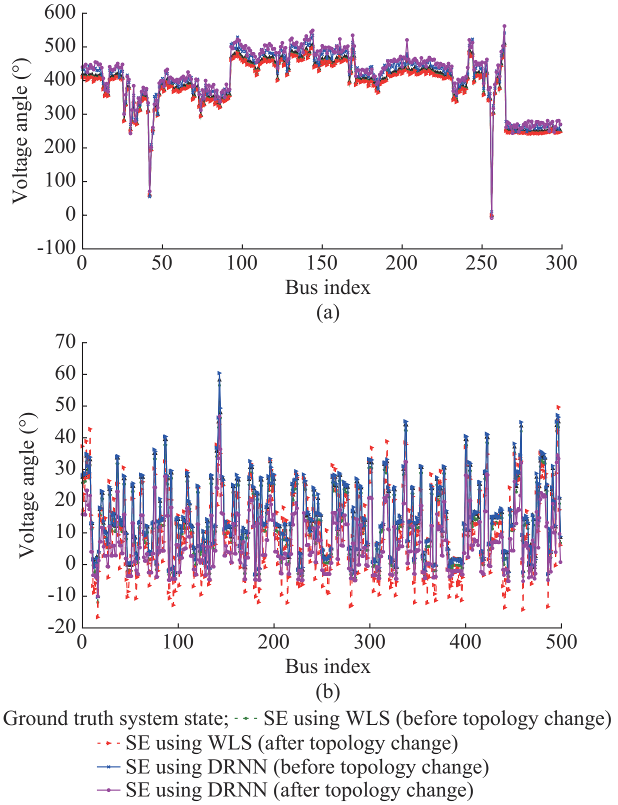
(b)

Fig. 4. Evaluation of proposed state prediction model using various unseen datasets (DC power flow). (a) IEEE 118-bus system. (b) IEEE 39-bus system.

V. Adversary Models

Attackers come up with different adversarial strategies whereby the final effect of the malicious data leads to damage the state variables across the power system domain. Generally, there are two main FDI anomaly strategies for power system measurement models. One requires knowledge of power system topology [4], and the other is based on a data-driven approach also known as the blind FDI attack strategy [26].

The vulnerability of the detection module to adversarial ML is analyzed as follows. Although the main assumption of adversarial model considered in this paper is the false injection attack, coordinated adversarial ML attacks can also be potential challenges against the proposed cyber-attack detection or decision-making module. The adversarial ML may bring inconsistencies against the model during its training and retraining phases and introduce errors into unseen datasets, thereby creating a confusion over a previously trained detection model. Overall, such threat models can cause the ML model to make a wrong decision or misclassifications and affect its detection performance. This current work assumes that the cyber-physical processes involved include data sensing, communication, and decision-making using the ML module. While the false injection attack is against the data integrity of the smart grid, the adversarial ML attack can be like poisoning or evasion attack against the ML module.



(a)

(b)

Fig. 5. Voltage angle prediction before and after topology changes. (a) IEEE 300-bus system. (b) ACTIVSg 500-bus system.

TABLE VI
Performance Evaluation in Terms of MSE with Different Models for IEEE 39-bus and 118-bus Systems

Type	Prediction model	MSE	
		IEEE 39-bus system	IEEE 118-bus system
DC	WLS	6.13×10^{-3}	8.34×10^{-3}
	DFFNN	4.65×10^{-3}	5.96×10^{-3}
	DRNN	2.50×10^{-3}	3.52×10^{-3}
AC	WLS	3.92×10^{-3}	5.34×10^{-3}
	DFFNN	7.57×10^{-3}	8.21×10^{-3}
	DRNN	2.15×10^{-3}	3.18×10^{-3}

Therefore, the whole cyber-physical process is considering the false injection attack during the communication and/or injection across the sensors. As a result, we limit the scope of this paper to just the cyber-attack against the data integrity (i.e., the FDI attack).

The adversary is assumed to have access to the network topology. In particular, two realistic attack models are examined: random FDI attack and targeted FDI attack. While the former aims to inject an attack vector to the measurement quantities that will lead to a falsified estimate of state vectors, the latter aims to find an attack vector that can inject arbitrary errors into some state vectors.

A. Adversary Model I

Here, it is assumed that the adversary can have access only to some κ sensor readings (where $\kappa \geq m-n+1$). This may be due to the fact that some sensors have specific physical defences or may be beyond the reach of the adversary. Let $I_m=\{I_1,I_2,...,I_\kappa\}$ be the set of indices of sensors. According to Theorem II in [4], the adversary can compromise κ sensors under the following conditions:

$$\boldsymbol{a}(i)=\begin{cases}\boldsymbol{Hb} & i\in I_m\\ \boldsymbol{0} & i\notin I_m\end{cases}\tag{6}$$

Algorithm 3 illustrates the implementation of this attack model used in our case scenario. In Algorithm 3, the *ATTACKCONS*(·) procedure (with κ, $\boldsymbol{H}$, and $\boldsymbol{y}$ arguments) generates the attack vector $\boldsymbol{a}(i)$ and adds this attack vector to the measurement vector $\boldsymbol{y}(i)$ of k meters. *randi*(·) and *randn*(·) are random number generator functions where the former is used to generate the set of meters and the latter is used to generate non-zero numbers of the k-sparse attack vector. The *zeros*(·) function returns an array of zeros whose size corresponds to the non-compromised sensor indices.

Algorithm 3: adversary model I

```
Input: $\kappa$, $\boldsymbol{H}$, $\boldsymbol{y}$
Output: $\boldsymbol{y}_{false}$
procedure ATTACKCONS($\kappa$, $\boldsymbol{H}$, $\boldsymbol{y}$)
    $I_\kappa \leftarrow randi([1,m],1,\kappa)$
    if $i\in I_\kappa$ then
        $\boldsymbol{a}(i)\leftarrow \boldsymbol{H}\times randn(\kappa,1)$
        $\boldsymbol{y}_{false}(i)\leftarrow \boldsymbol{y}(i)+\boldsymbol{a}(i)$
    end if
    if $i\notin I_\kappa$ then
        $\boldsymbol{a}(i)\leftarrow zeros(\kappa,1)$
    end if
end procedure
```

B. Adversary Model II

Here we consider a targeted FDI attack where the adversary intends to inject bad data into certain chosen state vectors. Again, for a successful FDI attack, we assume that the adversary has the knowledge of the network topology such as bus and chosen state vectors. Suppose the adversary has chosen $\zeta<n$ set of state variables $x_1,x_2,...,x_{\zeta_i}$, where $\zeta_i=\{1,2,...,\zeta\}$ is the position of the subset of state vectors. In this model of the attack, the adversary aims to construct $\boldsymbol{x}_{false}=\hat{\boldsymbol{x}}+\boldsymbol{b}$. Details of the construction of this attack model are given in [4].

VI. Numerical Results and Discussion of Proposed SPAD Framework

A. Quantifying KL Metric of Detector

Here, we present scenarios to justify the performance of the data-driven KL metric for the detection of bad data injection. The scenarios demonstrated in this subsection are based on the adversary model I. The histogram of state variations of normal and injections of false data are demonstrated in Fig. 6 for the 1-year and 5-year data. The mean differences in the distribution between these two classes of data are also shown in Fig. 6. In addition, the computation results of the KL distance are demonstrated in Fig. 7 and Fig. 8, respectively, for the 1-year and 5-year data. In general, for both data cases, there is a distinction between the histogram of the KL values of the normal and the tampered traffic, and the plots of KL values of these two classes. However, the results also show that the dissimilarity between the normal and the tampered traffic is more noticeable under the 1-year data compared with the 5-year data, mainly due to the difference in the load profile as the latter covers a wide range of 5-year data. Finally, while Fig. 9 illustrates the cumulative distribution function (CDF) between the ground truth and predicted states of the KL distance of the 1-year and the 5-year data. Therefore, the results shown in Figs. 6-9 confirm that power system states at normal operating conditions have almost similar estimations provided that the topology remains the same. However, when FDI attack is injected to some of the measurement data, it results in a different SE in the control center. These results are, in particular, owing to the combined data-driven approach for prediction of power system states and KL distance metric based attack detection.

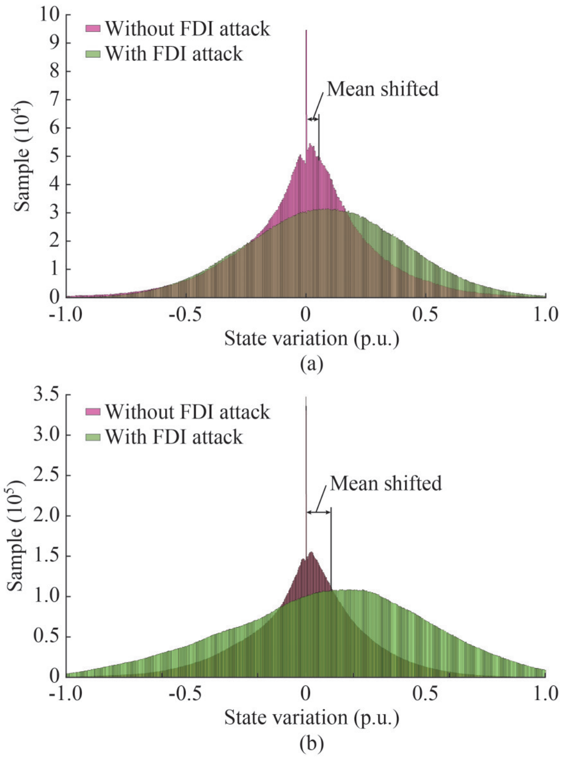
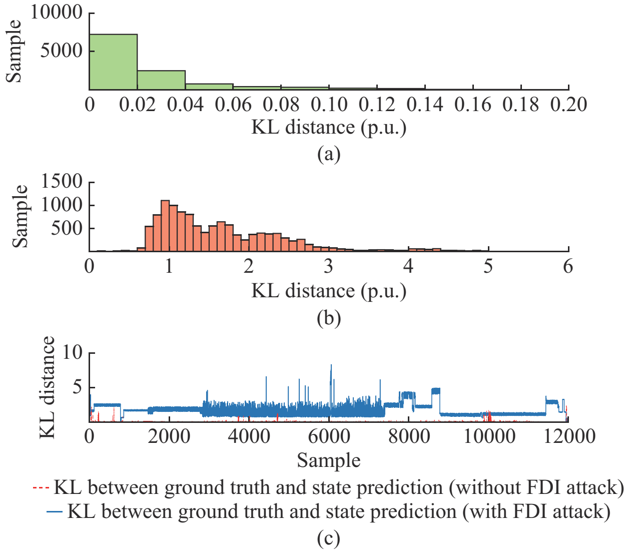


Fig. 6. Histogram of state variations without and with FDI attack. (a) 1-year data. (b) 5-year data.

B. Detection Performance

The detection module is trained through the KL values of the predicted state vectors. ROC curve, AUC, recall and precision are employed for the detection performance. The performance of ROC is evaluated in terms of the probability of correctly classifying the computed KL distance of the predicted states as either attack-free or manipulated data using the decision rule given by (5). The ROC curve, which is a plot of FPR v.s. TPR, is obtained by varying the decision thresholds. FPR and TPR are defined as (9) and (10), respectively. Additionally, the recall and precision are given by (11) and (12), respectively.

$$FPR=\frac{FP}{FP+TN}\tag{9}$$

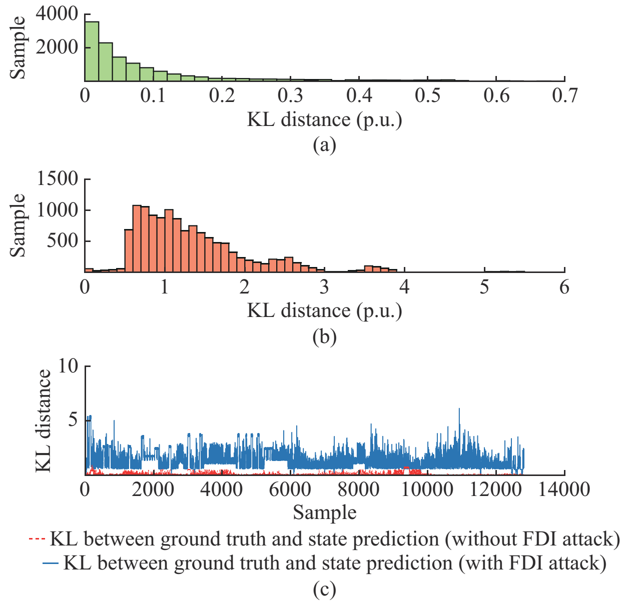


(a)

(b)

(c)

Fig. 7. KL distances of 1-year data (with and without FDI attack). (a) KL of predicted states (without FDI attack). (b) KL of predicted states (with FDI attack). (c) KL distance.



(a)

(b)

(c)

Fig. 8. KL distances of 5-year data (with and without FDI attack). (a) KL of predicted states (without FDI attack). (b) KL of predicted states (with FDI attack). (c) KL distance.

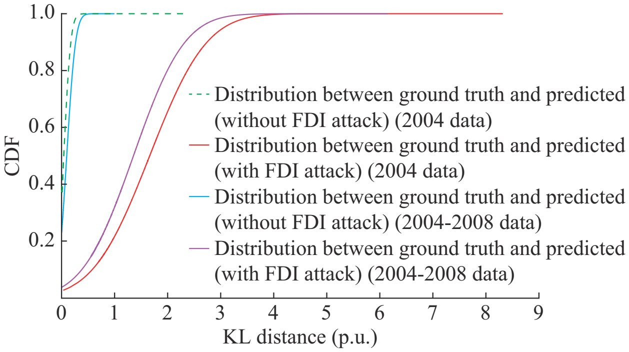


Fig. 9. CDF between ground truth and predicted states of KL distance of 1-year and 5-year data.

$$TPR = \frac{TP}{TP+FN} \tag{10}$$

$$Recall = \frac{TP}{FN+TP} \tag{11}$$

$$Precision = \frac{TP}{FP+TP} \tag{12}$$

where TP represents the successfully identified FDI attacks; FP represents the number of states that are wrongly classified as FDI attacks; and FN represents the number of states that are wrongly classified as normal.

The proposed detection performance is compared against χ^2 distribution test, and with one of recent findings on KL metric based FDI attack detection using WLS estimation [16]. For the χ^2 distribution test, the ℓ_2-norm is computed based on the residuals between the actual and the WLS predicted values using a degree of freedom given by $m-n$. Similarly, to compare with the other technique, the KL of Δx denoting the difference between WLS-predicted states and the actual states is computed.

C. *Attack Scenarios*

To perform the FDI attack detection, three attack scenarios are considered. For each scenario, 12000 samples are used.

1) *Attack Scenario I*

For attack simulation of the IEEE 118-bus system, we assume that the adversary has access to $k=190$ measurement meters, a condition that satisfies the criteria $k \geq m-n+1$ [4]. The attack vector is generated following implementation Algorithm 3 and (6). Figure 10 shows the attack detection results in this attack scenario. In this case, the proposed system has a much better detection performance than the BDD and existing KL-based FDI attack detection technique. The BDD has very poor performance in detecting the FDI anomalies. The KL-based FDI attack detection technique demonstrates better detection results compared with the BDD. However, as the KL metric is dependent on the WLS estimation result, its detection performance is still less than the proposed SPAD framework.

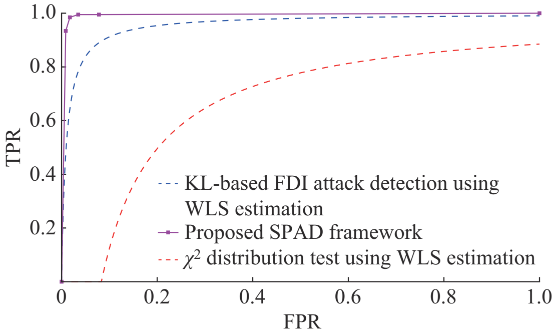


Fig. 10. Attack detection results using 5-year data in attack scenario I.

2) *Attack Scenarios II and III*

These two case scenarios are based on the targeted FDI attack. When the adversary manipulates the state variables, the measurements associated with these elements will be tempered. To inject the bad data, we simulate the bias vector $\boldsymbol{b}$

to be added on each of the 118 state variables of the power network using different settings. First, we use a 10% increase from the initial state value (here referred to as attack scenario II). Then, we increase the bad data by 40%, which means $x_{flase} = x + 0.4x$ (attack scenario III). In both attack scenarios, although the proposed SPAD framework outperforms existing techniques, its classification accuracy deteriorates when the magnitude of the attacks are too small. However, as the magnitude of the attacks increases, so does the KL distance, which leads to a much higher probability of attack detection by the SPAD framework. Figures 11 and 12 are the attack detection results for these two attack scenarios. Table VII demonstrates the detection performance of the proposed SPAD framework in terms of AUC, precision and recall considering both the DC and AC optimal power flows. From the detection numerical results we can conclude that the BDDs are vulnerable to the FDI attack models. In contrast, our proposed scheme has much better detection rate compared with the existing KL-based FDI attack detection and the BDD.

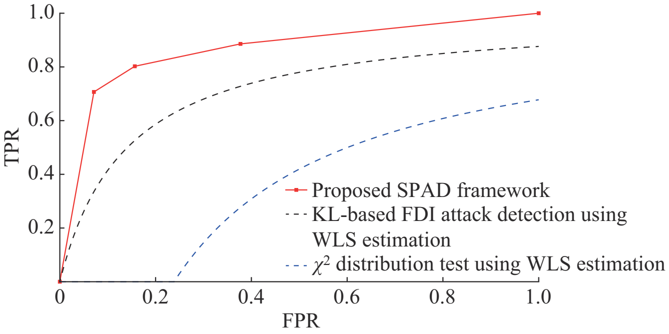


Fig. 11. Attack detection results using 5-year data in attack scenario II.

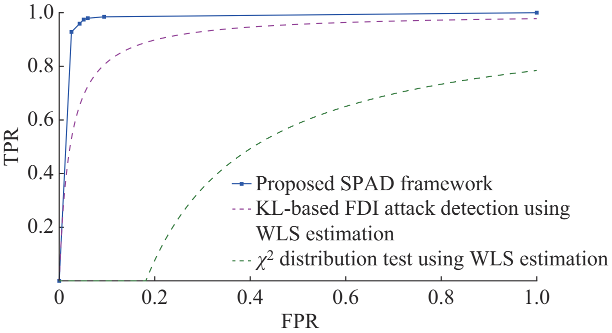


Fig. 12. Attack detection results using 5-year data in attack scenario III.

TABLE VII
DETECTION PERFORMANCE OF SPAD FRAMEWORK IN TERMS OF AUC, PRECISION, AND RECALL

Power flow model	Attack scenario I (%)			Attack scenario II (%)			Attack scenario III (%)		
	AUC	Recall	Precision	AUC	Recall	Precision	AUC	Recall	Precision
DC	99.41	98.59	99.25	86.47	84.77	85.63	98.15	97.54	97.76
AC	97.41	95.54	96.36	84.90	82.48	82.67	96.43	94.89	95.03

VII. CONCLUSION

This research work identifies vulnerabilities of existing power system SEs against the FDI attack and proposes data-driven state prediction and defence strategies to ensure the data integrity of power systems. In particular, the proposed SPAD framework is formulated using DL, where a predictive SE is deployed for estimating the system states, and a KL metric-based detection leverages the predicted states. Accordingly, an attack alert is generated when the computed KL value of the predicted states is greater than the decision threshold. Numerical simulations show that under normal operating conditions of the power system, there occurs only a minimal dissimilarity between consecutive state vectors; however, the KL score rises when falsified measurement data is injected into the meter readings. The proposed SPAD framework detects FDI attacks with a higher accuracy compared with the existing FDI attack detection algorithms. In the future, given low-dimensional properties of power system measurement data and sparsity properties of the FDI attack, attack localization can be explored using data-driven techniques. Furthermore, to deter the growing challenges of data integrity cyber-attacks, a comprehensive data-driven approach of FDI attack construction and cyber defence strategy can be proposed leveraging state-of-the-art DL, reinforcement learning, or deep reinforcement learning models along with optimization approaches. Finally, ML adversarial attacks can exploit the ML-based cyber-attack detection of the smart grid SE and can inject bad data to the decision-making module. Hence, cyber-attack detection against the ML adversarial attacks is recommended as an open research issue.

REFERENCES

[1] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*, 1st ed., Boca Raton: CRC Press, 2004, pp. 1-327.

[2] M. Gol and A. Abur, "LAV based robust state estimation for systems measured by PMUs," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1808-1814, Jul. 2014.

[3] G. Wang, G. B. Giannakis, and J. Chen, "Robust and scalable power system state estimation via composite optimization," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6137-6147, Nov. 2019.

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

[5] H. T. Reda, A. Anwar, and A. Mahmood. (2021, Jul.). Comprehensive survey and taxonomies of false injection attacks in smart grid: attack models, targets, and impacts. [Online]. Available: https://arxiv.org/abs/2103.10594

[6] Z. Zhao, Y. Huang, Z. Zhen *et al.*, "Data-driven false data-injection attack design and detection in cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 51, no. 12, pp. 6179-6187, Dec. 2021.

[7] Y. Chen, S. Huang, F. Liu *et al.*, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158-2169, Mar. 2019.

[8] H. T. Reda, A. Anwar, A. N. Mahmood *et al.* (2021, Mar.). A taxonomy of cyber defence strategies against false data attacks in smart grid. [Online]. Available: https://arxiv.org/abs/2103.16085

[9] A. S. Zamzam, X. Fu, and N. D. Sidiropoulos, "Data-driven learning-based optimization for distribution system state estimation," *IEEE Transactions on Power Systems*, vol. 34, no. 6, pp. 4796-4805, Nov. 2019.

[10] 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*, vol. 67, no. 15, pp. 4069-4077, Aug. 2019.

[11] H. Mosbah and M. El-Hawary, "Multilayer artificial neural networks

for real time power system state estimation," in *Proceedings of IEEE Electrical Power and Energy Conference*, London, Canada, Oct. 2015, pp. 344-351.

[12] P. N. P. Barbeiro, J. Krstulovic, H. Teixeira *et al.*, "State estimation in distribution smart grids using autoencoders," in *Proceedings of IEEE 8th International Power Engineering and Optimization Conference*, Langkawi, Malaysia, Mar. 2014, pp. 358-363.

[13] G. Wang, G. B. Giannakis, Y. Saad *et al*., "Retrieval via reweighted amplitude flow," *IEEE Transactions on Signal Processing*, vol. 66, no. 11, pp. 2818-2833, Jun. 2018.

[14] M. H. Ansari, V. T. Vakili, B. Bahrak *et al.*, "Graph theoretical defense mechanisms against false data injection attacks in smart grids," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 860-871, Sept. 2018.

[15] N. Zivkovi and A. T. Sari, "Detection of false data injection attacks using unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, Sept. 2018.

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

[17] S. K. Singh, K. Khanna, R. Bose *et al*., "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 1, pp. 89-97, Jan. 2018.

[18] H. Manyun, N. Ming, L. Manli *et al*., "Detecting false data injection attacks on modern power systems based on Jensen-Shannon distance," in *Proceedings of IEEE 8th Annual International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*, Tianjin, China, Jul. 2018, pp. 1154-1159.

[19] S. K. Singh, R. Bose, and A. Joshi, "Minimizing energy theft by statistical distance based theft detector in AMI," in *Proceedings of 24th National Conference on Communications*, Hyderabad, India, Feb. 2018, pp. 1-5.

[20] T. Hong, P. Pinson, and S. Fan, "Global energy forecasting competition 2012," *International Journal of Forecasting*, vol. 30, no. 2, pp. 357-363.

[21] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*, Sardinia, Italy, May 2010, pp. 249-256.

[22] D. P. Kingma and J. L. Ba, "Adam: a method for stochastic optimization," in *Proceedings of International Conference on Learning Representations (ICLR)*, San Diego, USA, May 2015, pp. 1-41.

[23] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436-444, May 2015.

[24] S. Kullback and R. A. Leibler, "On information and sufficiency," *The Annals of Mathematical Statistics*, vol. 22, no. 1, pp. 79-86, Mar. 1951.

[25] R. D. Zimmerman and C. Murillo-Sanchez. (2016, Dec.). Matpower 6.0 user's manual. [Online]. Available: https://matpower. org/docs/MATPOWER-manual-6.0.pdf

[26] A. Sayghe, Y. Hu, I. Zografopoulos *et al*., "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581-595, Nov. 2020.

Haftu Tasew Reda received the B.Sc. degree in electrical engineering from Bahir Dar University, Bahir Dar, Ethiopia, in 2007 and the M.Eng. degree (Research) from the Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea, in 2017. Previously, from September 2007 to September 2014, he worked in Ethio Telecom, Addis Ababa, Ethiopia, mainly on radio access engineering. Moreover, from October 2018 to February 2019, he was an R&D RF Hardware Engineer at VOIXATCH, Cheonan, South Korea. He is currently a Ph.D. graduate researcher at the Department of Computer Science and IT, La Trobe University, Bundoora, Australia. His research interests include smart grid cybersecurity, industrial Internet of Things (IoT), wireless sensor networks, and artificial intelligence (AI).

Adnan Anwar is a Cyber Security Academic at Deakin University, Burwood, Australia, and a member of the Centre for Cyber Security Research and Innovation (CSRI). Previously, he worked as a Data Scientist and Analytics Team Leader at Flow Power. He has over 10 years of industrial, research, and teaching experience in universities and research laboratories including NICTA (now, Data61 of CSIRO), University of New South Wales (UNSW), La Trobe University, and Deakin University. He received his Master by Research degree and Ph.D. from UNSW at the Australian Defence Force Academy. He has authored over 70 articles in prestigious venues. He has attracted research income from Government, Defence, Industries and received numerous awards at Deakin for excellence in research and teaching. His research interests include security for critical infrastructures including smart grid, supervisory control and data acquisition (SCADA) system, and application of machine learning and optimization techniques.

Abdun Mahmood received the B.Sc. degree in applied physics and electronics and the M.Sc. (Research) degree in computer science from the University of Dhaka, Dhaka, Bangladesh, in 1997 and 1998, respectively, and the Ph.D. from the University of Melbourne, Melbourne, Australia, in 2008. He had an academic career in university since 2000, working at University of Dhaka, RMIT University, UNSW Canberra, and currently in La Trobe University as an Associate Professor (Reader). He leads a group of researchers. His research interests include machine learning and cybersecurity including anomaly detection in smart grid, supervisory control and data acquisition (SCADA) security, memory forensics, and false data injection.

Naveen Chilamkurti received the Ph.D. degree from La Trobe University, Bundoora, Australia. He is currently the Cybersecurity Program Coordinator of computer science and information technology with La Trobe University. His current research interests include intelligent transport systems (ITS), smart grid computing, vehicular communications, vehicular cloud, cybersecurity, wireless multimedia, wireless sensor networks, and mobile security.