Design of a FDIA Resilient Protection Scheme for Power Networks by Securing Minimal Sensor Set

Tanmoy Kanti Das[1], Subhojit Ghosh[2], Ebha Koley[2], and Jianying Zhou[3]

[1] Department of Computer Applications,
[2] Department of Electrical Engineering,
National Institute of Technology Raipur,
G.E.Road, Raipur, Chhattisgarh, India-492010
{tkdas.mca,sghosh.ele,ekoley.ele}@nitrr.ac.in
[3] Singapore University of Technology and Design,
Singapore 487372
jianying_zhou@sutd.edu.sg

Abstract. Recent times have witnessed increasing utilization of wide area measurements to design the transmission line protection schemes as wide area measurements improve the reliability of protection methods. Usage of ICT tools for communicating sensor measurement in power networks demands immunity and resiliency of the associated protection scheme against false data injection attack (FDIA). Immunity against malicious manipulation of sensor information is attainable by securing the communication channels connecting the sensors through cryptographic protocols, and encryption. However, securing all the sensors and communication channels is economically unviable. A practical solution involves securing a reduced set of sensors without compromising fault detection accuracy. With the aim of developing a simple, economically viable and FDIA resilient scheme under the assumption that the adversary has complete knowledge of the system dynamics, the present work proposes a logical analysis of data (LAD) based fault detection scheme. The proposed scheme identifies the minimal set of sensors for FDIA resiliency and detects the state (faulty or healthy) of the power network relying on the measurements received from the 'minimal sensor set' only. Validation of the proposed protection scheme on IEEE 9-bus system reveals that in addition to being FDIA resilient, it is reliable and computationally efficient.

Keywords : *Smart Grid, Transmission Line Protection, False Data Injection Attack (FDIA), Fault Detection, Partially Defined Boolean Function (pdBf), Logical Analysis of Data.*

1 Introduction

The reliable operation of any power system is heavily dependent on the development of a suitable protection scheme against line faults and contingencies.

A reliable protection scheme allows for faster fault detection and hence early restoration of power supply post-fault. In recent times, with the soaring assimilation of the physical power transmission system with the cyber information and communication tools in smart grids, the possibility of cyber-attacks poses a serious challenge towards the development and implementation of a reliable protection mechanism against faults. The protection component plays a significant role in the overall operation and control of a power system. The increased stress on rapid detection of faults and reduction in fault levels is arising because of the penetration of renewable energy sources has led to a paradigm shift from classical protection scheme using local measurements to protection scheme relying on 'wide area measurements' [1]. The effective performance of a protection scheme, which rely on wide area measurements, is highly dependent on the sensor information transmitted to the control centers through the cyber network. Over-dependence of power systems on the public communication networks for reliable monitoring and operation, makes it vulnerable to cyber attacks [2].

False data injection attack (FDIA) is considered as the most potent cyber attack in which the overall power grid can be made to collapse by the hacker with minimal effort. During FDIA, the attacker corrupts the integrity of a set of measurements that are used in the protection algorithm by tampering the meter/sensor measurements [3, 4]. The protection algorithms are part of the backup protection strategy, which is operated from the control center(s). Transmission of false data to the control center may lead to unnecessary control action that might result in contingencies or even blackout. Consequently, the present scenario demands a protection scheme that is either immune to data falsification or/and includes a component for preemptive detection of false data injection. The state-of-the-art for protection of transmission lines [5–8] has not addressed the deployment of a security mechanism against vulnerabilities caused by FDIA.

Conventional power networks address the need for system monitoring through state estimation [9], which is carried out using the power system model, and sensor informatics. Conventional bad data detection methods that are part of state estimators are supposed to detect any malicious manipulation of sensor information. However, Liu et al. [10] have demonstrated that a hacker, having enough knowledge about the system dynamics, can bypass the bad data detection techniques and inject any arbitrary errors into state variables by suitably injecting malicious sensor information using FDIA. Thus, the manipulation of sensor information during an attack can provide a deceptive picture regarding the system dynamics and operation, leading to either non-operation of the relay during fault or tripping of the relay followed by isolation during a non-faulty/healthy case. Inappropriate actions of the protective relays, and a delay in the detection of such attacks can result in a huge economic loss, asset damage, and collapse of the related sub-systems and control mechanisms. With the explosive growth in the use of sensors (CT, PT, PMU) and communication network for continuous online real-time monitoring using the information of the current and/or voltage signals at different buses or locations, the scope of mounting a false data injection attack has increased significantly in recent times.

Recent works on FDIA in power grid have mainly concentrated on the modeling of FDIA, detection of an attack and defensive measures [11–25]. The probable implications arising out of FDIA on power system have been addressed in [3, 11, 12]. The notable schemes reported for FDIA detection in power networks are based on transmission line susceptance measurements [13], reactance perturbation [14], joint-transformation [15], extreme learning machine [16], sparse optimization [17] and cumulative sum approach [18]. Yang et al. [19] proposed a countermeasure to FDIA using the premise that the *sensors*, which measure injective power flow in the buses and are connected to several other buses require security. Since inaccessibility of those *sensors* will make it difficult for an attacker to mount an FDIA. A defense mechanism to protect a set of state variables has been proposed in [20, 21].

An adaptive Markov based defense strategy for the protection of smart grid has been reported in [22]. A two-layer attack-defense mechanism to protect PMUs against FDIA is presented in [23]. In [24], a greedy search algorithm is presented to obtain the subset of measurements required to be protected to defend against FDIA. In [25], a scheme based on bilevel mixed integer linear programming has been presented to prevent the falsification of load data. A defensive method against data integrity attacks based on the optimal PMU placement strategy is proposed in [23]. An algorithm for appropriate placement of PMU in electric transmission network for reliable state estimation against FDIA has been presented in [26]. In [27], a generalized scheme for detecting data integrity attacks in cyber-physical systems based on sensor characteristics and noise dynamics has been proposed.

Most of the existing works on FDIA mentioned above have only concentrated on detection of FDIA without analyzing its effect on the operation of the transmission line protection module. To the best of our knowledge, no work has been reported on analyzing the implications of FDIA on fault detection and developing an FDIA immune protection scheme. A simple solution to this problem is to replace the set of all the existing sensors τ with 'secure sensors'. Secure sensors communicate using cryptographic protocols and methods, which prevent any chances of FDIA unless the keys of cryptographic protocols are compromised. Moreover, secure sensors are protected from physical tampering using tamper-resistant hardware. However, the sheer number of installed meters/sensors in electric grids makes it impractical to replace all the sensors with secured sensors [28]. At best, we can secure a small set of sensors τ_{s}, where $\tau_{\mathrm{s}} \subset \tau$.

Moreover, the selection of the reduced sensor set should ensure no degradation in the performance of the protection algorithm, in terms of accurately detecting various fault scenarios, even in the presence of FDIA. This demands optimally locating those sensors whose information either do not contribute to the system monitoring or can be correlated with other sensor information. With τ_{s}, the protection algorithm is expected to carry out the intended task of detecting the faults by suitable mapping of secured sensor information with the fault scenarios. Considering a moderate-size network having a few hundred installed

sensors, a brute force search to locate τ_s over all possible small-size subsets are prohibitively costly.

In the present work, the twin problems of identifying τ_s and correlating the protection scheme output (faulty/healthy) with the sensor information are solved using a classifier, which utilizes a partially defined Boolean function based data analysis technique known as Logical Analysis of Data (LAD) [29–31]. For a two-class classification problem, LAD aims at optimally generating a set of rules/patterns, which can collectively classify all the known observations (power system scenarios). Features/sensor-measurements, which contribute insignificantly to the classification task, are ignored and further not included in the rules. In addition of providing immunity against FDIA, a significant contribution of the LAD based protection scheme is the reduction in complexity of the detection algorithm since the overall sensor information is substantially reduced without employing any dimension reduction technique.

Popular classifiers, like KNN, ANN, SVM, etc., which are generally preceded by some feature extraction method, are difficult to implement on the digital relays that work on threshold settings. On the contrary, in the LAD-based scheme, the raw data (i.e., sensor information) are directly fed into the classifier without any pre-processing and the classification rules provide a threshold for each input feature (i.e., sensor information in the present problem). Further, the generalization of LAD to datasets of varying dimensions makes the proposed scheme independent of the power system network topology. It is to be noted that, unlike the existing works on 'optimal sensor placement' [23] based on maintaining *'system state observability'*, the present work aims at the identification of optimal sensor set for imparting immunity to protection scheme against FDIA. Securing sensors identified using 'system state observability' do not guarantee immunity to power line protection schemes against FDIA.

The effectiveness of the proposed scheme has been evaluated by performing extensive simulations under normal operation and FDIA for IEEE 9 bus system. While simulating the false data injection attack, it is assumed that the attacker has complete knowledge regarding the power system model. For varying scenarios, the proposed scheme is able to correctly detect the state of transmission line, i.e., faulty or healthy under FDIA of varying degrees with significantly reduced execution time (maximum 45 microseconds). The highlights/novelty of the proposed work can be summarized as:

1. Development of an FDIA immune protection scheme with the assumption that the *attacker has complete knowledge of the power system.*
2. Development of a data analysis based approach for identifying the limited set of sensors that would be secured using tamper-resistant hardware, cryptographic protocol, and encryption.
3. Design of a rule-based fault detection scheme by mapping the secured sensor information with the state of the power system using LAD-based classifier.

The remainder of the paper is organized as follows. Section 2 discusses the development of the proposed LAD based protection scheme. Section 3 demonstrates the test results on the IEEE 9-bus system to exemplify the proposed scheme.

Finally, Section 4 summarizes the contributions of the paper and provides conclusions and future research direction.

2 Design of a LAD based Classifier for Fault Detection

As mentioned earlier, a hacker may try to mislead the control center to take some unnecessary action by presenting an unrealistic picture of the grid to the control center using FDIA. For example, consider the attack on a healthy system by falsification of the current signal carried out by FDIA as depicted in the Figure 3(a). Any corrective measure based on that falsified information will critically affect the normal operation of the grid and may lead to power-cut or blackout. A natural solution to avoid the damage caused by FDIA involves securing all the sensors of the grid and that will thwart falsification of sensor information. However, the large number of sensors deployed over wide geographical span makes the task of providing security to all the individual sensors impractical because of the related financial implications [28]. A financially viable option is to secure a small set of the existing sensors. For an n bus system, assuming current and voltage monitoring at each bus, the overall sensor set τ is given as

$$\tau = [S_{I_1}, S_{V_1}, S_{I_2}, S_{V_2}, \ldots, S_{I_n}, S_{V_n}] \tag{1}$$

In the analysis of power system protection schemes, two widely used measures are referred to as *security* and *dependability*. Security refers to the ratio of the predicted no-fault cases to the actual number of no-fault cases while the dependability relates to the ratio of the detected fault cases to the actual number of faults. Now, the goal of identifying the minimal set of sensors τ_s involves finding $|\tau_s| << |\tau|$, such that the security and dependability of the overall power system protection mechanism are maintained using only the sensors from τ_s. In other words, with the information provided by τ_s, the detection of faults can be carried out. Also any sensor, which is a member of τ_s, will be protected using tamper-resistant hardware, cryptographic protocols, and encryption algorithms. Consequently, falsification of measurements transmitted from those sensors would be impossible during any FDIA.

It should be noted that the classical dimension reduction technique like PCA, which aims at reducing redundant information based on the interrelationship among different attributes is not suitable for identifying τ_s since the physical significance of individual sensor information is not maintained. The dual issues of optimally reducing the sensor information while preserving the physical significance of the data (i.e., bus voltage and current) and classification of network state (healthy/faulty) have been addressed in the present work by adopting a logical analysis of data (LAD) based classification scheme [29, 30]. LAD is a data analysis technique, which uses partially defined Boolean function (pdBf) and its extensions to find patterns or rules for classification. These patterns (a.k.a. rules) can be linked to a causal-effect relationship(s) among observations and its class labels.

For the present work, observations correspond to the sensor information for a particular fault/scenario, while the class label refers to the occurrence/non-occurrence of a fault. The patterns (or rules) correlate the magnitude of current and voltage at different buses with the fault detector output i.e. 0 or 1 respectively for no fault and fault conditions. The patterns or rules generated by LAD with τ_s can be used to classify future observations, i.e., to predict the occurrence of a fault. A typical dataset comprising of different observations (power system scenarios) consists of two sets X^+ and X^- respectively comprising of sensor information during fault X^+ and no fault X^- cases.

$$X^+ = \begin{bmatrix} I_{1,1} & V_{1,1} & I_{2,1} & V_{2,1} & \dots & \dots & I_{n,1} & V_{n,1} \\ I_{1,2} & V_{1,2} & I_{2,2} & V_{2,2} & \dots & \dots & I_{n,2} & V_{n,2} \\ I_{1,3} & V_{1,3} & I_{2,3} & V_{2,3} & \dots & \dots & I_{n,3} & V_{n,3} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ I_{1,u} & V_{1,u} & I_{2,u} & V_{2,u} & \dots & \dots & I_{n,u} & V_{n,u} \end{bmatrix} \quad (2) \qquad \theta(X^+) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ . \\ . \\ . \\ 1 \end{bmatrix} \quad (3)$$

$$X^- = \begin{bmatrix} I_{1,u+1} & V_{1,u+1} & I_{2,u+1} & V_{2,u+1} & \dots & \dots & I_{n,u+1} & V_{n,u+1} \\ I_{1,u+2} & V_{1,u+2} & I_{2,u+2} & V_{2,u+2} & \dots & \dots & I_{n,u+2} & V_{n,u+2} \\ I_{1,u+3} & V_{1,u+3} & I_{2,u+3} & V_{2,u+3} & \dots & \dots & I_{n,u+3} & V_{n,u+3} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ I_{1,m} & V_{1,m} & I_{2,m} & V_{2,m} & \dots & \dots & I_{n,m} & V_{n,m} \end{bmatrix} \quad (4) \quad \theta(X^-) = \begin{bmatrix} 0 \\ 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix} \quad (5)$$

With $X^+ \cap X^- = \emptyset$.

The LAD generates positive and negative patterns corresponding to faulty and healthy scenarios from observations X^+ and X^-. The patterns are generated optimally with minimum sensor information for classifying all the cases. We refer to subsection 2.3 for the formal definition of a pattern.

Initially, LAD was designed to work with binary data only, in which the set of binary observations $X(= X^+ \cup X^-)$ is expressed as a pdBf ρ representing a mapping between $X \rightarrow \theta(.)\{1, 0\}$. The algorithm aims at finding an approximate extension γ of ρ, such that γ can classify all the unknown observations in the sample space. In a nutshell, logical analysis of data involves the following five steps [31].

1. Binarization of Observations: For conversion of non-binary observations to binary while preserving the inherent characteristics of observations.
2. Elimination of Redundancy (or Support Sets Generation).
3. Pattern Generation.
4. Theory Formation: For Identification of a minimal set of patterns.
5. Classifier Design and Validation.

The above steps are dealt with in the subsequent sub-sections.

2.1 Binarization of Observations

For observations represented by numerical data, a threshold (a.k.a. cut-point) based method is adapted to convert the numerical data to binary. A numerical attribute β is represented in binary using two types of Boolean variables, i.e., level and interval variables. For a given cut-point c_p, we introduce a level variable $b(\beta, c_p)$ such that

$$b(\beta, c_p) = \begin{cases} 1, & \text{if } \beta \geq c_p. \\ 0, & \text{otherwise.} \end{cases} \tag{6}$$

Similarly, interval variables $b(\beta, c_p^i, c_p^j)$ are created for each pair of cut-points c_p^i and c_p^j and given by

$$b(\beta, c_p^i, c_p^j) = \begin{cases} 1, & \text{if } c_p^i \leq \beta < c_p^j. \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

The cut-point computation process is explained using an example dataset presented in the Table 1. The dataset consists of five observations with three features A, B, C. Afterward, a class label is attached to each record (Table 2). To convert the feature A to binary, a dataset is created as in the Table 3. Further, we apply

Attributes	A	B	C
X^+:positive examples	3.5	3.8	2.8
	2.6	1.6	5.2
	1.0	2.1	3.8
X^-:negative examples	3.5	1.6	3.8
	2.3	2.1	1.0

Table 1.

A	B	C	Class Labels (Truth Values)
3.5	3.8	2.8	1
2.6	1.6	5.2	1
1.0	2.1	3.8	1
3.5	1.6	3.8	0
2.3	2.1	1.0	0

Table 2.

A	Class Labels (Truth Values)
3.5	1
2.6	1
1.0	1
3.5	0
2.3	0

Table 3.

A	Class Labels (Truth Values)
3.5	1
3.5	0
2.6	1
2.3	0
1.0	1

Table 4.

A	Class Labels
3.5	2
2.6	1
2.3	0
1.0	1

Table 5.

the following steps to estimate the cut-points.

1. Sort the dataset of Table 3 over A and we obtain the dataset of Table 4.
2. If two or more successive observations have identical attribute value v^i but different class labels, discard all those observations except one. Now, replace the class label of v^i by a new and unique class label. Refer to Table 5.
3. Repeat the step 2 until only unique values of the attribute are left.
4. Introduce a new cut-point $c_p^j = \frac{(A^i + A^{i+1})}{2}$, if class labels of A^i, A^{i+1} are different.

We found following cut-points using above mentioned steps.

$$c_p^1 = 3.05,\ c_p^2 = 2.45,\ c_p^3 = 1.65\ .$$

Consequently, six Boolean variables comprising of three level and three interval variables are created. After conversion of all the attributes, the binary dataset

obtained is presented in the Table 6. A “categorical" attribute β can be converted into binary by associating each possible value v_i of β with a Boolean variable

$$b(\beta, v_i) = \begin{cases} 1, & \text{if } \beta = v_i. \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

$A \geq 3.05$	$A \geq 2.45$	$A \geq 1.65$	$1.65 \leq A < 3.05$	$2.45 \leq A < 3.05$	$1.65 \leq A < 2.45$	$B \geq 2.95$	$B \geq 1.85$	$1.85 \leq B < 2.95$	$C \geq 4.5$	$C \geq 3.3$	$C \geq 1.9$	$1.9 \leq C < 4.5$	$1.9 \leq C < 3.3$	$3.3 \leq C < 4.5$	Class
b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}	$\mathcal{L}$
1	1	1	0	0	0	1	1	0	0	0	1	1	1	0	1
0	1	1	1	1	0	0	0	0	1	1	1	0	0	0	1
0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	1
1	1	1	0	0	0	0	0	0	0	1	1	1	0	1	0
0	0	1	1	0	1	0	1	1	0	0	0	0	0	0	0

Table 6. Binary dataset generated from the Table 2 having 15 binary variables from b_1 to b_{15}.

2.2 Support set generation

Redundant attributes may be present in the binary dataset generated through binarization or any other means and removal of redundant attributes is achieved through the computation of *minimal support set*. If the projections X_M^+, X_M^- of the binary attribute set M are such that $X_M^+ \cap X_M^- = \emptyset$, then M is known as the support set of X. If removal of any constituent of M leads to $X_M^+ \cap X_M^- \neq \emptyset$, then M is known as minimal support set. For finding the minimal support set, “Mutual-Information-Greedy” algorithm from [32] has been adapted, using which the following binary features are selected.

$$M = \{b_2, b_{15}, b_8, b_1\}.$$

2.3 Modified pattern generation method

In Boolean algebra, a Boolean variable or its negation is known as *literals* and conjunction of such literals is known as *term*. In LAD, if a term only covers some positive (negative) observations, then it is termed as positive (negative) *pattern*.

Moreover, if a pattern is minimal, i.e., removal of any literal from the pattern leads to a pattern, which is covering both positive and negative observations, then it is called 'prime pattern'. In this paper, we have used an optimized version of the prime pattern generation technique as proposed by Boros et al. [30]. The pattern generation algorithm involves a major modification over the algorithm proposed in [30]. The modification increases the probability that the coverage of a point or observation by a single pattern only. Consequently, the 'theory formation' step used to select the most suitable pattern to cover an observation is no longer required.

After the execution of the algorithm on the projection $M = \{b_2, b_{15}, b_8, b_1\}$ of the binary dataset, following positive prime patters are produced:(i) $\bar{b}_2 b_{15}$, (ii)$b_2\bar{b}_{15}$. Negative prime patterns generated by following an identical procedure and the corresponding negative patterns are (i) $\bar{b}_2\bar{b}_{15}$, (ii)$b_2 b_{15}$. It can be observed, that the binary variables appearing in the generated patterns are not dependent on the attribute B. Thus, the set of reduced attribute (or the *set of secured sensor* in the present problem) τ_s is given by $\tau_{\mathbf{s}} = \{\mathbf{A}, \mathbf{C}\}$.

2.4 Design of Classifier

In this step, generated patterns are transformed into rules. Let us now consider the first positive pattern $\bar{b}_2 b_{15}$. The rule generated using the meaning of $\bar{b}_2 b_{15}$ (see Table 6) is $\neg(A \geq 2.45) \wedge (3.3 \leq C < 4.5) \implies$ 'Class label'= 1. One or more positive rules can be combined into 'if else-if else' structure to design a classifier (fault detector for the present problem). A simple classifier designed using the positive patterns is presented below.

Simple Classifier.

Input: Observation consisting of attribute A, B, C.
Output: Class label $\mathcal{L}$.

if $(\neg(A \geq 2.45) \wedge (3.3 \leq C < 4.5))$ **then**
    Class label $\mathcal{L} = 1$.
else if $((A \geq 2.45) \wedge \neg(3.3 \leq C < 4.5))$ **then**
    Class label $\mathcal{L} = 1$.
else
    Class label $\mathcal{L} = 0$.
end if

It can be observed from the 'Simple Classifier' also that the feature B of the original dataset is redundant and omitted by the classifier. Hence, for the present problem, the reduced sensor τ_s is given by $\tau_s = \{A, C\}$. The removal of redundant data and reduction in the number of sensors is achieved without any degradation in the classification accuracy.

3 Performance Evaluation

In this section, the efficacy of the proposed scheme in terms of optimality of τ_s, appropriateness of rules framed by LAD for fault detection and resilience against FDIA has been evaluated through comprehensive simulation studies. In this regard, the performance evaluation has been conducted on IEEE 9-bus benchmark test power system. The system has been simulated using Simulink and Simpower system toolboxes of MATLAB and executed on a 64-bit, 4 core workstation with an Intel Xeon processor and 16 GB RAM. The IEEE 9-bus system includes 9 buses, 6 lines and 3 loads as shown in Fig 1. In the system, 54 meters (3 for current and 3 for voltage measurement at each bus of the line) are deployed, which gather information at the corresponding bus.

For generating the training dataset to derive the minimal sensor set τ_s and to frame the classification rules for fault detection based on the information from τ_s only, normal operation without attack by any adversary is considered. Normal operation incorporates scenarios associated with the healthy operation, contingencies, and faults in the power network. Observations related to healthy system state are having a class label 0. On the other hand, observations associated with a faulty system state are marked by 1 as their class label. Note that, the observations related to contingencies also have the class label as 1. The details of power system scenarios considered for training dataset preparation are presented in the Table 7.

During fault or power system contingencies (load variation and power swing) the current and voltage magnitude vary widely, and protection mechanisms present in the control center may require to take corrective measures to restore the optimal operating condition of the power system. However, if a healthy system is subjected to measures related to fault or contingencies, the consequences could be devastating. Any attacker with prior knowledge regarding the power system operation can manipulate the magnitude of voltage and current signals in order to mislead the control center to take unnecessary action whose consequence could be catastrophic.

To analyze the performance of the proposed protection scheme in terms of robustness against injection of fake data that may cause unintended operation, *test dataset* for validation has been generated by simulating several *false data injection attack* (FDIA) carried out against unsecured sensors. Two such attacks are presented in the Figure 2(a) and 3(a). Along with FDIAs, several fault and no-fault cases have also been simulating under varying fault parameters (fault location, fault inception angle and fault resistance). Some no-fault cases involving system frequency and voltage variation, switching of transmission line and sudden load encroachments have also been considered in the testing data for security analysis during healthy condition. The inclusion of FDIA, fault and no-fault cases in the test dataset allows validating the immunity of the proposed scheme against FDIA.

With the generated training dataset consisting of normal operation only, the LAD based approach discussed in section 2 is employed for the design of a clas-

Fault Parameters	Fault Type	LG, 2LG, 3LG, 2L and 3L
	Fault Location	1% to 100% of the line length at an interval of 5 km
	Fault inception angle	0^o to 90^o
	Fault resistance	0Ω, 50Ω and 100Ω
Power Syst. Contingency	Load variation	±20%,±40%
	Frequency variation	±2%,±5%
	Voltage variation	±5%,±10%
No Fault		

Table 7. Power Syst. Scenarios Considered.

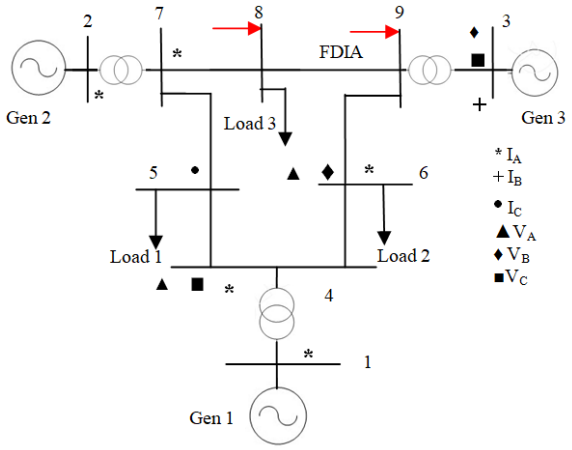

Fig. 1. IEEE 9-bus system with 13 protected sensors on different buses.

sifier to differentiate the healthy system state from the faulty state. The training dataset consists of 4648 observations. Among those, 4500 observations are from different faulty scenarios and rest are observations from healthy scenarios. Let us now summarize the results related to individual steps of LAD over the training set.

1. *Binarization of Observations*: In this step, 12048 binary feature variables are created from 54 current and voltage information collected from 9 different buses following the steps described in subsection 2.1.
2. *Support Set Generation*: Here 21 binary variables are selected from 12048 available binary variables using the method described in the subsection 2.2.
3. *Pattern Generation*: In this step, 28 rules are generated. The secure sensor set τ_s is also generated at this point. The details of secure sensors are available in the Figure 1. Form the possible 54 sensors, by using only 13 secured sensors (7 currents and 6 voltages), it is possible to detect the faults. Note that, it is clear from Figure 1 that two buses, i.e., bus-8 and bus-9 (marked by arrow) do not have any secure sensor.

4. *Classifier Design and Validation*: A classifier is built using the rules generated in the last step. The details of which are available in the Alogorithm 3.

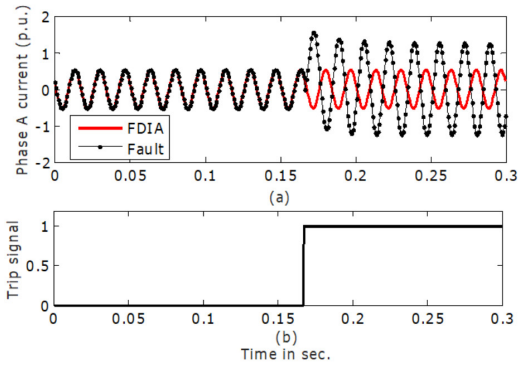

Fig. 2. (a) Suppression of current waveform of Phase "A" by FDIA during actual fault at bus-9 (b) Corresponding Trip signal by resilient protection scheme.

Let us now illustrate the results using an example. A single line to ground fault at 50 km from the bus-7 in the line between bus-7 and bus-8 has been simulated and the corresponding voltage and current waveform acquired by the unsecured sensors at bus-9 during the fault in the absence and presence of FDIA has been illustrated in Fig. 2(a). It can be observed that the current waveform in phase "A" during "AG" fault is manipulated at bus-9 by the attacker. Thus, replicating the healthy scenario post-fault, and in an attempt to mislead any fault detection process, the control center is presented with the falsified information only. The corresponding test result of the proposed FDI resilience protection scheme is shown in Fig. 2(b). It can be observed that the proposed scheme is able to detect the fault correctly even in the presence of FDIA and issued the 'Trip signal' for proper operation of the relay at the appropriate time. Further, a healthy (no fault) case has also been analyzed in which the attacker launches an FDIA at bus-8 by replicating a single line to ground fault. The corresponding test results depicted in Fig.3(a, b) confirm the immunity of the proposed scheme against FDIA.

Further, the performance assessment of the proposed scheme has been carried out using two statistical indices commonly used in the performance analysis of transmission line protection schemes, i.e., *dependability* and *security*. Dependability relates to the ratio of the detected fault cases to the actual number of faults while security refers to the ratio of the predicted no-fault cases to the actual number of no-fault cases. We could achieve 100% dependability and security in all the scenarios. Furthermore, the detection of fault is achieved in less than 45 microseconds. We have also carried out similar exercise using IEEE 39-bus

Algorithm 2 Resilient Protection Scheme for IEEE 9-bus system.

if $\neg(I_{3,B} \geq 1.105100) \wedge \neg(V_{4,A} \geq 0.795880)$ **then**
  Fault.
else if $\neg(I_{3,B} \geq 1.105100) \wedge \neg(V_{3,C} \geq 0.722580)$ **then**
  Fault.
else if $(V_{4,A} \geq 0.795880) \wedge \neg(V_{3,C} \geq 0.722580)$ **then**
  Fault.
else if $(V_{4,A} \geq 0.795880) \wedge \neg(V_{3,B} \geq 0.744375)$ **then**
  Fault.
else if $(V_{4,A} \geq 0.795880) \wedge \neg(V_{4,C} \geq 0.721830)$ **then**
  Fault.
else if $(V_{4,A} \geq 0.795880) \wedge (I_{7,A} \geq 2.697800)$ **then**
  Fault.
else if $\neg(I_{5,C} \geq 0.949195) \wedge (I_{7,A} \geq 2.697800)$ **then**
  Fault.
else if $\neg(V_{3,C} \geq 0.722580) \wedge (V_{3,B} \geq 0.744375)$ **then**
  Fault.
else if $(V_{3,C} \geq 0.722580) \wedge \neg(V_{6,B} \geq 0.553810)$ **then**
  Fault.
else if $(V_{3,C} \geq 0.722580) \wedge (I_{7,A} \geq 2.697800)$ **then**
  Fault.
else if $(V_{3,C} \geq 0.722580) \wedge \neg(V_{6,A} \geq 0.567410)$ **then**
  Fault.
else if $(V_{3,B} \geq 0.744375) \wedge \neg(V_{4,C} \geq 0.721830)$ **then**
  Fault.
else if $\neg(I_{6,A} \geq 1.196150) \wedge \neg(V_{6,A} \geq 0.567410)$ **then**
  Fault.
else if $\neg(V_{4,C} \geq 0.721830 \wedge \neg(V_{6,A} \geq 0.567410)$ **then**
  Fault.
else if $\neg(I_{2,A} \geq 2.528100) \wedge \neg(V_{6,B} \geq 0.553810)$ **then**
  Fault.
else if $(V_{6,B} \geq 0.553810) \wedge (I_{7,A} \geq 2.697800)$ **then**
  Fault.
else if $(I_{3,B} \geq 1.105100) \wedge (V_{4,A} \geq 0.795880) \wedge (I_{2,A} \geq 2.528100)$ **then**
  Fault.
else if $(I_{3,B} \geq 1.105100) \wedge (V_{4,A} \geq 0.795880) \wedge \neg(V_{6,A} \geq 0.858385)$ **then**
  Fault.
else if $(I_{3,B} \geq 1.105100) \wedge (I_{6,A} \geq 0.594455) \wedge \neg(I_{6,A} \geq 0.776730)$ **then**
  Fault.
else if $\neg(V_{4,A} \geq 0.795880) \wedge \neg(I_{5,C} \geq 0.949195) \wedge (V_{3,C} \geq 0.722580)$ **then**
  Fault.
else if $\neg(V_{4,A} \geq 0.795880) \wedge \neg(I_{5,C} \geq 0.949195) \wedge \neg(I_{2,A} \geq 2.528100)$ **then**
  Fault.
else if $\neg(V_{4,A} \geq 0.795880) \wedge (V_{3,C} \geq 0.722580) \wedge \neg(I_{4,A} \geq 0.843595)$ **then**
  Fault.
else if $\neg(V_{4,A} \geq 0.795880) \wedge (V_{3,B} \geq 0.744375 \wedge \neg(I_{7,A} \geq 0.780975)$ **then**
  Fault.
else if $\neg(V_{4,A} \geq 0.795880) \wedge (V_{3,B} \geq 0.744375) \wedge \neg(I_{6,A} \geq 1.196150)$ **then**
  Fault.
else if $(I_{5,C} \geq 0.949195) \wedge \neg(I7, A \geq 0.780975) \wedge \neg(I_{4,A} \geq 0.843595)$ **then**
  Fault.
else if $\neg(V3, C \geq 0.722580) \wedge \neg(V4, C \geq 0.721830) \wedge (V6, B \geq 0.553810)$ **then**
  Fault.
else if $(V_{3,C} \geq 0.722580) \wedge (I_{7,A} \geq 0.780975) \wedge \neg(V_{4,C} \geq 0.721830)$ **then**
  Fault.
else if $\neg(V_{4,A} \geq 0.795880) \wedge \neg(I5, C \geq 0.949195) \wedge (V_{4,C} \geq 0.721830) \wedge \neg(I_{1,A} \geq 2.874700)$ **then**
  Fault.
else
  No Fault.
end if

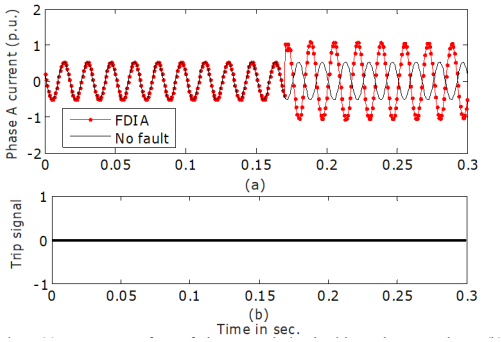

Fig. 3. (a) Suppression of current waveform of Phase "A" by FDIA during healthy operation at bus-9 (b) Corresponding Trip signal by resilient protection scheme.

bench-marked system having 234 installed voltage and current sensors, and we have achieve 100% security and dependability in this case also.

4 Conclusion

Dependence of protection algorithms on the information from the sensors spreading across wide geographical locations has increased the risk of FDIAs in power networks. In this paper, an FDIA resilient protection scheme has been proposed, in which immunity against FDIA has been achieved by securing a minimal set of sensors. The identification of sensor set contributing maximum to the system monitoring while avoiding redundancy has been carried out by employing a Boolean function based approach known as LAD. In addition of locating the strategic sensors, and thus, reducing the dimension of measured data, the LAD based approach provides a rule-based mapping between the secured sensor information, and the state (i.e., healthy or faulty) of the power system both under normal condition and FDIA. This avoids providing security to all the sensors, thereby reducing the financial cost for necessary immunity against FDIA. The proposed computationally efficient protection scheme has been well validated for different types of faults under varying fault and power system operating parameters for IEEE three machine 9-bus system. The validation confirms the robustness of the proposed scheme against FDIA, by performing the intended relaying action. Future work in this direction is planned on extending the proposed protection scheme for fault classification, section identification, and location estimation during FDIA.

Acknowledgment

Jianying Zhou's work was supported by SUTD start-up research grant SRG-ISTD-2017-124.

References

1. A. G. Phadke, H. Volskis, R. Menezes de Moraes, T. Bi, R. N. Nayak, Y. K. Sehgal, S. Sen, W. Sattinger, E. Martinez, O. Samuelsson, D. Novosel, V. Madani, and Y. A. Kulikov. The wide world of wide-area measurement. *IEEE Power and Energy Magazine*, 6(5):52–65, Sep. 2008.
2. S. Sridhar, A. Hahn, and M. Govindarasu. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, Jan 2012.
3. 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):1630–1638, July 2017.
4. Xuan Liu and Zuyi Li. False data attack models, impact analyses and defense strategies in the electricity grid. *The Electricity Journal*, 30(4):35 – 42, 2017. Special Issue: Contemporary Strategies for Microgrid Operation & Control.
5. K. Chen, J. Hu, and J. He. Detection and classification of transmission line faults based on unsupervised feature learning and convolutional sparse autoencoder. *IEEE Transactions on Smart Grid*, 9(3):1748–1758, May 2018.
6. S. R. Mohanty, A. K. Pradhan, and A. Routray. A cumulative sum-based fault detector for power system relaying application. *IEEE Transactions on Power Delivery*, 23(1):79–86, Jan 2008.
7. S. R. Samantaray. Phase-space-based fault detection in distance relaying. *IEEE Transactions on Power Delivery*, 26(1):33–41, Jan 2011.
8. Ch.D. Prasad and Paresh Kumar Nayak. Performance assessment of swarm-assisted mean error estimation-based fault detection technique for transmission line protection. *Computers & Electrical Engineering*, 71:115 – 128, 2018.
9. A. Monticelli. Electric power system state estimation. *Proceedings of the IEEE*, 88(2):262–282, Feb 2000.
10. Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 21–32, New York, NY, USA, 2009. ACM.
11. Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.*, 14(1):13:1–13:33, June 2011.
12. 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 Transactions on Industrial Informatics*, 13(2):411–423, April 2017.
13. R. Deng and H. Liang. False data injection attacks with limited susceptance information and new countermeasures in smart grid. *IEEE Transactions on Industrial Informatics*, 15(3):1619–1628, March 2019.
14. C. Liu, J. Wu, C. Long, and D. Kundur. Reactance perturbation for detecting and identifying fdi attacks in power system state estimation. *IEEE Journal of Selected Topics in Signal Processing*, 12(4):763–776, Aug 2018.
15. S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi. Joint-transformation-based detection of false data injection attacks in smart grid. *IEEE Transactions on Industrial Informatics*, 14(1):89–97, Jan 2018.
16. Liqun Yang, Yuancheng Li, and Zhoujun Li. Improved-elm method for detecting false data attack in smart grid. *International Journal of Electrical Power & Energy Systems*, 91:183 – 191, 2017.

17. L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Transactions on Smart Grid*, 5(2):612–621, March 2014.
18. S. Li, Y. Yılmaz, and X. Wang. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Transactions on Smart Grid*, 6(6):2725–2735, Nov 2015.
19. 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 and Distributed Systems*, 25(3):717–729, March 2014.
20. S. Bi and Y. J. Zhang. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Transactions on Smart Grid*, 5(3):1216–1227, May 2014.
21. R. Deng, G. Xiao, and R. Lu. Defending against false data injection attacks on power system state estimation. *IEEE Transactions on Industrial Informatics*, 13(1):198–207, Feb 2017.
22. Qi Wang, Wei Tai, Yi Tang, Ming Ni, and Shi You. A two-layer game theoretical attack-defense model for a false data injection attack against power systems. *International Journal of Electrical Power & Energy Systems*, 104:169 – 177, 2019.
23. Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao. On optimal pmu placement-based defense against data integrity attacks in smart grid. *IEEE Transactions on Information Forensics and Security*, 12(7):1735–1750, July 2017.
24. J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan. Sparse malicious false data injection attacks and defense mechanisms in smart grids. *IEEE Transactions on Industrial Informatics*, 11(5):1–12, Oct 2015.
25. X. Liu, Z. Li, and Z. Li. Optimal protection strategy against false data injection attacks in power systems. *IEEE Transactions on Smart Grid*, 8(4):1802–1810, July 2017.
26. Q. Yang, L. Jiang, W. Hao, B. Zhou, P. Yang, and Z. Lv. Pmu placement in electric transmission networks for reliable state estimation against false data injection attacks. *IEEE Internet of Things Journal*, 4(6):1978–1986, Dec 2017.
27. Chuadhry Mujeeb Ahmed, Jianying Zhou, and Aditya P. Mathur. Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in cps. In *Proceedings of the 34th Annual Computer Security Applications Conference*, ACSAC '18, pages 566–581, New York, NY, USA, 2018. ACM.
28. T. T. Kim and H. V. Poor. Strategic protection against data injection attacks on power grids. *IEEE Transactions on Smart Grid*, 2(2):326–333, June 2011.
29. Y. Crama, P. L. Hammer, and T. Ibaraki. Cause-effect relationships and partially defined boolean functions. *Ann. Oper. Res.*, 16(1-4):299–325, January 1988.
30. E. Boros, P. L. Hammer, T. Ibaraki, A. Kogan, E. Mayoraz, and I. Muchnik. An implementation of logical analysis of data. *IEEE Transactions on Knowledge and Data Engineering*, 12(2):292–306, March 2000.
31. Gabriela Alexe, Sorin Alexe, Tibérius O. Bonates, and Alexander Kogan. Logical analysis of data – the vision of peter l. hammer. *Annals of Mathematics and Artificial Intelligence*, 49(1):265–312, Apr 2007.
32. Hussein Almuallim and Thomas G. Dietterich. Learning boolean concepts in the presence of many irrelevant features. *Artificial Intelligence*, 69(1):279 – 305, 1994.