

Joint Transformation based Detection of False Data Injection Attacks in Smart Grid

Sandeep Kumar Singh, *Student Member, IEEE*, Kush Khanna, *Student Member, IEEE*, Ranjan Bose, *Senior Member, IEEE*, Bijaya Ketan Panigrahi, *Senior Member, IEEE*, and Anupam Joshi, *Fellow, IEEE*

Abstract—For reliable operation and control of smart grid, estimating the correct states is of utmost importance to the system operator. With recent incorporation of information technology and Advanced Metering Infrastructure (AMI), the futuristic grid is more prone to cyber-threats. The False Data Injection (FDI) attack is one of the most thoroughly researched cyber-attacks. Intelligently crafted, it can cause false estimation of states, which further seriously affects the entire power system operation. In this paper, we propose Joint Transformation based scheme to detect FDI attacks in real time. The proposed method is built on the dynamics of measurement variations. Kullback-Leibler Distance (KLD) is used to find out the difference between probability distributions obtained from measurement variations. The proposed method is tested using IEEE 14 bus system considering attack on different state variables. The results shows that the proposed scheme detects FDI attacks with high detection probability.

Index Terms—Cyber security, false data injection, Kullback-Leibler distance, smart grid.

NOMENCLATURE

a	Attack vector.
c	Error caused in the state vector due to attack vector a .
e	Gaussian meter error vector.
H	Measurement Jacobian.
V	$V \angle \theta$.
x_{bad}	State vector after attack.
x	System state vector.
z_{bad}	Perturbed measurements after attack.
\hat{x}	Estimated state vector.
σ_i	Standard deviation of measurement z_i .
c, γ	Positive constants.
D	Degree of damage.
g_{ij}, b_{ij}	Conductance and susceptance of line $i - j$.
g_{si}, b_{si}	Shunt conductance and shunt susceptance at bus i .
$h(x)$	Measurement function.
m	Number of measurements available.
N_{bus}	Set of all the buses in the network.
p	Probability distribution of measurement variation from current and previous time step.
P_i	Real power injection at bus i .

P_{ij}	Real power flow in the line $i - j$.
q	Probability distribution of measurement variation for historical data.
Q_i	Reactive power injection at bus i .
Q_{ij}	Reactive power flow in the line $i - j$.
r	Set of measurement data before the transformation T .
s	Set of measurement data after the transformation T .
V, θ	System states (Voltage magnitude and Angle).
Y	Bus admittance matrix.
z	Set of measurement vector.

I. INTRODUCTION

THE smart grid facilitates control of electricity demand and supply in reliable, sustainable and economic manner by incorporating information technology and communication infrastructure. Advanced Metering Infrastructure (AMI) and Demand Side Management (DSM) enables two-way communication between the utilities and end customers. This integration enables customers to monitor their load pattern in real time and often earn incentives from the utilities for controlling their usage in peak hours. However, the cyber-physical security of the grid is now prone to cyber-attacks [1]–[3]. A malicious actor can now hack into the communication network, accessing and modifying the confidential grid and user information.

Data integrity attacks can be launched by the attacker by intruding the physical security of the smart meters/sensors. By judiciously forming the attack vector, adversary injects false/malicious data into the smart meters and misleads the system operator with incorrect yet feasible system state. Depending on the motive of adversary, these fraudulent measurements may lead power system to an uneconomical yet stable or to a completely unstable state of operation. The possible impacts of false data injection (FDI) attack on power system have been reported in [4]–[6]. A co-ordinated attack forcing system to an insecure or uneconomic state of operation can further lead to a collapse if not detected in time as presented in [7]. Many methods have been reported in the literature to alleviate FDI attacks in the smart grid.

The defence techniques can be broadly classified into two categories: 1) Protection-based defence, and 2) Detection-based defence. As power grid covers a vast geographical area with hundreds and thousands of smart meters/sensors, the cost of protecting all smart meters can be very high. It is, therefore, realistic for the system operator to only protect a set of critical sensors and corresponding measurements [8]. In [9], Bobba et al. proposed the detection of FDI attacks by protecting

Sandeep K. Singh, K. Khanna, Ranjan Bose and B. K. Panigrahi are with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India e-mail: (sandeepsingh012@gmail.com, kushkhanna06@gmail.com, rbose@ee.iitd.ac.in, bkpanigrahi@ee.iitd.ac.in).

Anupam Joshi is with the Computer Science and Electrical Engineering Department, University of Maryland Baltimore County, Baltimore MD 21250, USA (email: joshi@umbc.edu).

a strategically selected set of sensor measurements. A light-weight watermarking technique is proposed to defend against false data injection attacks [10]. Talebi et al. [11] presented a strategy for detection of FDI attacks by reconfiguring the micro-grids dynamically and makes it impossible to organize a synchronized injection. Necessary and sufficient conditions to select the protection measurements and find the optimal solution which protects the state estimates with least number of measurements were proposed in [12]. The smart meters can be protected by continuously monitoring the measurement data or by encrypting the measurement data. Shortcomings of the protection based defence are twofold; firstly, securing the critical set of measurements leads to decrease in redundant trustworthy measurements; secondly, the assumption of making a completely hack-proof smart sensor is unrealistic.

The detection based methods on the other hand are based on analysis of meter data. Kosut et al. [13] introduced a Bayesian formulation of the bad data problem, which captures the prior information that a control center has about the likely state of the power system. Similarly in [14], a Bayesian framework for the characterization of fundamental tradeoffs at the control center and for the adversary is presented. Bayesian framework is used to detect any unusual data which does not have the same measurement distribution as historical measurement distribution. However, in the case of malicious data having same distribution pattern as historical data or if an adversary replaces the current meter readings with previous readings having same distribution, the Bayesian approach fails to detect the attack. Liu et al. [15] proposed a novel false data detection mechanism based on the separation of nominal power grid states and anomalies. In [16], a sequential detector based on the generalized likelihood ratio is proposed for quickest detection of FDI attack in smart grid. The authors also proposed a distributed sequential detector using level-triggered sampling for wide-area monitoring in smart grid. Rawat et al. [17] proposed Chi-square detector and cosine similarity matching scheme for detecting malicious data injection. A real-time detection scheme against FDI attack in smart grid is proposed in [18] using Markov chain based analytical model. Liu et al. [19] proposed a collaborative intrusion detection mechanism against FDI attack.

Gu et al. [20] came up with a method to detect FDI attack in smart grid by considering the measurement variations, however, the proposed technique fails to detect the attacks on certain state variables on some of the buses. Due to the quasi-static nature of the power system, the variation in the measurements are minimal. This lowers the detection probability if the attacker injects the small errors in measurements for targeting certain state variables. We propose, an image processing based technique to detect the attacks by transforming the measurement variation which enhances the resolution (scaling) of the probability distribution function, thereby, increasing the detection probability. In image processing, transformation based approach maps input pixel value to output pixel using predefined transformation function. Log transformation and power-law (gamma) transformation [21] are widely used methods for image enhancement. In our proposed work, probability distribution of measurement variations are

obtained from the histogram plot of measurement variations. The chosen transformation techniques are computationally efficient and detects the FDI attacks without burdening the state estimation process. Although, Absolute Distance (AD) and Jensen Shannon Distance (JSD) [22] can also compare the two probability distributions, as applied in this work, we chose Kullback Leibler Distance (KLD) [23] to calculate the difference between historical true measurement variations and false measurement variations due to comparatively higher detection efficiency. If the run time KLD is smaller than the threshold value (pre-defined set-point obtained from historical measurement variation), then there is no FDI attack. If the distance is larger than threshold, the received measurement sample is compromised. The proposed transformation based approach detects the FDI attacks with high probability of detection as compared to previously reported results. Table I summarizes various defence techniques reported in literature.

TABLE I
ADVANTAGES AND LIMITATIONS OF DEFENCE TECHNIQUES AGAINST FDI ATTACKS.

Defence Techniques	Advantages	Limitations
Protection based defence [8]–[12]	Only protect a set of critical meters and corresponding measurements.	Only the protected measurements are trusted, decrease of redundancy, protection may not be secure all of the time.
Detection based defence [13]–[19]	Analyse the raw measurements, able to detect ones that do not fit the distribution of historical measurements. Spatial and Temporal based detection methods are used.	Do not detect false data that fits the distribution of historical measurements. Captures the attacks that leads to extreme abnormal system states.
Kullback Leibler Distance [20], [23]	Track the dynamics of the measurements by calculating distance indices (KLD) between adjacent steps.	Fails to detect FDI attacks on some state variables.
Proposed methodology	Use transformation based schemes [21] to detect FDI, able to detect attacks on most of state variables with high detection efficiency.	Although the proposed scheme detects the attack more efficiently than [20], still attack on θ_8 remains undetected for some samples.

The rest of the paper is organised as follows. In section II, traditional bad data detection scheme, false data injection attack and formulation of attack are presented. Section III presents proposed method for detecting false data injection attacks. Test set-up is explained in section IV. Section V presents the numerical results and performance evaluation. Section VI concludes this paper.

II. BACKGROUND

A. State Estimation

The idea of state estimation in power system was proposed in [24]. State estimation facilitates identification of accurate operating condition of power system by continuously monitoring the bus voltages and transmission line loading in real time. In order to obtain the accurate voltage phasors at all the buses,

state estimation uses set of redundant measurements in order to filter out the errors in the measurements arising due to faulty meters or due to telemetry failure [25]. The measurements used can be a set of real power injection, reactive power injection, real and reactive power flow measurements. For a N_{bus} power system, the number of states defining the power system completely are $2N_{bus} - 1$ when polar co-ordinates are considered. The state vector ' \mathbf{x} ' contains N_{bus} voltage magnitude and $N_{bus} - 1$ phase angles with one angle is given an arbitrary value 0 for a reference. Thus the state vector is given as,

$$\mathbf{x} = [\theta_2, \theta_3, \dots, \theta_{N_{bus}}, V_1, V_2, \dots, V_{N_{bus}}] \quad (1)$$

For a set of measurements ' \mathbf{z} ', the Weighted Least Square (WLS) state estimator minimizes the following objective function,

$$J(\mathbf{x}) = \sum_{i=1}^m (z_i - h_i(\mathbf{x})) / \sigma_i^2 \quad (2)$$

The measurement function $h(x)$ can be formulated as,

$$P_i = \Re\{\mathbf{V}_i^* \sum_{k=1, k \neq i}^{N_{bus}} \mathbf{V}_k Y_{ik}\} \quad \forall i \in N_{bus} \quad (3)$$

$$Q_i = -\Im\{\mathbf{V}_i^* \sum_{k=1, k \neq i}^{N_{bus}} \mathbf{V}_k Y_{ik}\} \quad \forall i \in N_{bus} \quad (4)$$

$$P_{ij} = V_i^2 (g_{si} + g_{ij}) - V_i V_j (g_{ij} \cos \theta_{ij} + b_{ij} \sin \theta_{ij}) \quad \forall i, j \in N_{bus} \quad (5)$$

$$Q_{ij} = -V_i^2 (b_{si} + b_{ij}) - V_i V_j (g_{ij} \sin \theta_{ij} - b_{ij} \cos \theta_{ij}) \quad \forall i, j \in N_{bus} \quad (6)$$

The iterative procedure for estimating the system state vector \mathbf{x} is explained in appendix. To accurately monitor the power system operation, the state estimation must be able to detect, identify and remove the measurement errors if present. Bad data is detected by performing the Chi-Square test [25] as follows,

$$J(\hat{\mathbf{x}}) = \sum_{i=1}^m (z_i - h_i(\hat{\mathbf{x}})) / \sigma_i^2 \leq \tau \quad (7)$$

If $J(\hat{\mathbf{x}})$ is greater than τ then bad data is present. Here τ is defined for given degree of freedom and confidence level. The meters which are the source of bad data are eliminated by performing normalised residue test [25].

B. False Data Injection Attacks

Attacker can inject malicious data to the measurement sensors by forming the attack vector which bypasses the bad data detection of the state estimation as shown in [5]. If $\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| \leq \tau$, an attack vector \mathbf{a} , which is the linear

combination of column vector of \mathbf{H} (i.e. $\mathbf{a} = \mathbf{H}\mathbf{c}$), can bypass the bad data detection test as shown below,

$$\begin{aligned} \|\mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c})\| &= \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + \mathbf{a} - \mathbf{H}\mathbf{c}\| \\ &= \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| \leq \tau \end{aligned} \quad (8)$$

Depending on the type of measurements (P_i , P_{ij} , Q_i and Q_{ij}) available for the estimating the states, for each measurement type of measurement function, H can be expressed as,

$$\begin{bmatrix} \frac{\partial h_1(\mathbf{x})}{\partial \theta_2} & \cdots & \frac{\partial h_1(\mathbf{x})}{\partial \theta_{N_{bus}}} & \frac{\partial h_1(\mathbf{x})}{\partial V_1} & \cdots & \frac{\partial h_1(\mathbf{x})}{\partial V_{N_{bus}}} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial h_m(\mathbf{x})}{\partial \theta_2} & \cdots & \frac{\partial h_m(\mathbf{x})}{\partial \theta_{N_{bus}}} & \frac{\partial h_m(\mathbf{x})}{\partial V_1} & \cdots & \frac{\partial h_m(\mathbf{x})}{\partial V_{N_{bus}}} \end{bmatrix} \quad (9)$$

here, $h_1(\mathbf{x}) \dots h_m(\mathbf{x})$ are measurement functions for m number of measurements, and are defined based on the type of measurements as given in (3)-(6).

False data injection attacks can be modelled for targeting single or multiple state variables. FDI attacks can be classified into two categories: 1) Load change attack, and 2) Load redistribution attack [26]. Furthermore, FDI attacks can also be launched without complete network information as presented in [27]. Attacks to gain momentary economic benefits are also proposed in [28]. The ultimate objective of an attacker is to launch a stealthy attack, which can deceive the system operator and bypasses the bad data detection. In this paper, our focus is on the real time detection of the FDI attacks. The approach is therefore to model the most generalised attack and thereby coming up with the most robust detection technique which can be applied for all possible data injection attacks.

C. Formulation of Attack

Although the attack can be formulated differently depending on the motives of the attacker, but the final impact of these malicious data on power system is always falsified system states. Depending on the attack model, there may be single affected state variable or multiple. If the detection methodology is able to detect the attack which affects only single state, it will also perform accurately for the attacks affecting multiple state variables because as the affected state variables increases, the false measurements increases which in turn results in higher Kullback Leibler Distance (KLD) value which will be explained in detail in the subsequent section. Therefore, the target of the attack considered in the paper is single state variable.

To launch the attack, adversary changes all the measurements for real and reactive power injections; and real and reactive power flows by injecting the error in the meters to project the desired changed state variable to the system operator. For example, if the attacker targets θ_2 state variable by injecting an error of -10% , the attack vector can be formulated by considering,

$$\mathbf{c} = \underbrace{[-0.1\theta_2, 0, \dots, 0]}_{\theta_{[1 \times (N_{bus}-1)]}}; \underbrace{[0, \dots, 0]}_{V_{[1 \times N_{bus}]}} \quad (10)$$

The perturbed measurements are calculated by using state vector, $\mathbf{x}_{bad} = \hat{\mathbf{x}} + \mathbf{c}$ and solving (3)-(6). For successfully

launching the attack, it is assumed that the attacker has knowledge of the network adjoining the bus corresponding to the target state vector. The perturbed measurements are given by,

$$\mathbf{z}_{bad} = \mathbf{h}(\mathbf{x}_{bad}) + \mathbf{e} \quad (11)$$

III. PROPOSED DETECTION METHODOLOGY

A. Transformation Schemes

When any individual meter is compromised by an adversary, it causes erroneous estimation of system states. The proposed method detects FDI attacks using dynamics of measurement data. The probability distribution of historical measurement variation is denoted by q and p is the probability distribution of measurement variation for current and previous time step. One probability distribution is transformed to other probability distribution by transformation based method.

Transformation based schemes are used in image processing to enhance the quality of image. Image enhancement is a process of reshaping an image to make it more suitable for any specific application. Power-law (Gamma) transformation and log transformation are some of the widely used image transformation techniques [21]. We have applied above mentioned transformations to power system measurements for detecting the FDI attacks in real-time.

Distance metrics are calculated using above mentioned transformed probability distributions of measurement variations. Considering the measurement variation, before and after transformation, denoted by ' r ' and ' s ', respectively. r (untransformed measurement variation) is defined as $|z(k) - z(k-1)|$. ' r ' and ' s ' are related by an expression $s = T(r)$, where T is a transformation that maps a measurement variation r into s .

In joint transformation, power and log transformations are jointly used. Power transformation is used in threshold selection and log transformation is used to calculate runtime distance KLD. Power and log transformation are explained below:

- 1) Power-Law (Gamma) Transformation: The basic expression for the transformation is given as,

$$s = cr^\gamma \quad (12)$$

where c and γ are positive constants. A family of transformation is obtained simply by varying γ [21]. This transformation with fractional values of γ map small range of input measurement values into wide range of values, with the opposite being true for higher values of input measurements. Power transformation reduces to identity transformation when $\gamma = c = 1$. Power-law transformation is useful for contrast manipulation.

- 2) Log Transformation: The expression for the log transformation is given as,

$$s = c \log(1 + r) \quad (13)$$

where c is constant. This transformation maps narrow range of measurement values into a wider range of values [21]. The opposite is true of higher values of measurements.

B. Kullback Leibler Distance

In order to detect the attack, transformed measurement variation is obtained. The divergence of measurement variation for the current time sample with the historical measurement variation is given by Kullback Liebler Distance (KLD) [23]. The KLD is also known as relative entropy or information gain. The expression for KLD is as follows:

$$D(p||q) = \sum_s p(s) \ln \frac{p(s)}{q(s)} \quad (14)$$

It is the expectation of logarithmic difference between probability distributions p and q . KLD is always non-negative $D(p||q) \geq 0$ [23]. It is additive for independent distributions and due to unsymmetrical property, $D(p||q)$ is not equal to $D(q||p)$. As KLD is not an absolute distance metric, it does not follow triangle inequality.

Once the KLD is obtained, it is compared with the threshold value, which is obtained without considering FDI attack. If the value of the distance metric is greater than the threshold, FDI attack is detected for the considered time step.

C. Threshold Selection

Selection of proper threshold value is very crucial and it affects the accuracy of detection. The historical measurements are assumed to be accurate throughout the paper. The measurement samples of one month prior to attack are compared with the historical data set to obtain the threshold value [20]. KLD for each sample is calculated as given in (14) and histogram is plotted. The selected threshold is that KLD value in the sample set which is greater than 99% of all the KLDs obtained for complete one month. If higher threshold value is selected (maximum KLD obtained from all the samples for the month), the proposed scheme will not able to detect certain FDI attacks. Furthermore, if a lower threshold value is selected, some true measurements may get labeled as false. The obtained threshold is dependent on network topology. While considering topology changes, the historical measurement data set is updated in accordance with the considered topology change. Hence the threshold value will be different for different network topology.

IV. TEST SETUP

A. System Details

IEEE 14 bus system, as shown in Fig. 1, is used to validate the effectiveness of the proposed detection scheme. The load buses in IEEE 14 bus system is linked with each load zone of NYISO as given in [20].

All the measurement data are calculated by considering NYISO load data from Jan 1, 2012 to Dec 31, 2012 which is obtained from [29]. The hourly load data is converted to 5 min data. Although the steps for obtaining historical measurements are already mentioned in [20], steps with some modifications are briefly explained below;

- 1) Hourly load data (real power demand) obtained from NYISO is mapped with IEEE 14 bus test system and converted to 5 minutes data.

- 2) IEEE 14 bus system test data is used to calculate the reactive power demand for each bus at 5 minutes interval by keeping constant power factor for respective bus in accordance with test system data.
- 3) Real and Reactive generation for each 5 min interval is obtained by proportionally changing the real and reactive power generation of the IEEE 14 bus system based on the net load for the considered time interval.
- 4) Voltages and angles at each bus is obtained by running the load flow program for each time interval. Gaussian noise¹ of 1% standard deviation is added in the measurements obtained using (3)-(6).

We have considered a fully measured power system, therefore we have, 14 real and reactive power injection measurements for each bus and 40 real and reactive to and fro power flow measurements. Therefore, a total of 108 measurements are considered at each 5 minutes time interval.

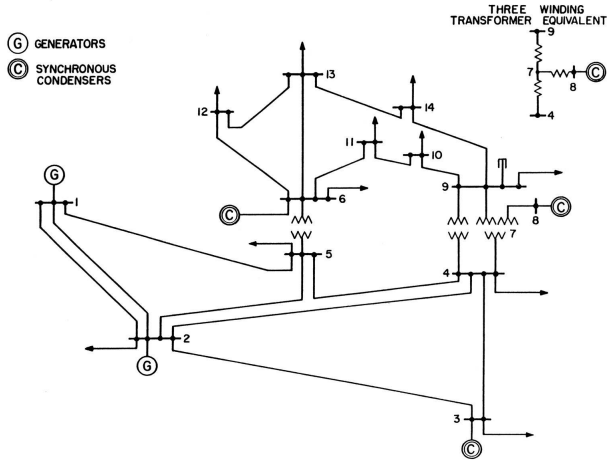


Fig. 1. IEEE 14 bus system.

To obtain the probability distribution p and q , all the measurements coming from 108 measurement sensors are considered for each 5 minutes time interval. q is obtained by transforming the probability distribution of measurement variation $|z(k) - z(k-1)|$ for all the measurement from Jan 1, 2012 to Oct 31, 2012. The measurement data for the month of November is considered to be without attack and therefore it is used to calculate the threshold value. We have considered FDI attack at each time interval for the December month. p is obtained for the month of December by transforming the measurement variation $|z_{bad}(k) - z(k-1)|$.

V. RESULTS AND DISCUSSION

All the simulation have been done on DELL PC with 3.20 GHz Intel Core i7 processor and 8 GB RAM on Windows 8 Enterprise. Programming has been done on MATLAB R2014b. The proposed scheme is tested when adversary targeted single state variable, and that state variable is increased or decreased by some percentage of its true value. Due to this attack, all measurements associated with that state variable are changed

¹Gaussian error is assumed for meters which is in line with [25].

TABLE II
COMPARISON OF PROPOSED TRANSFORMATION BASED SCHEME WITH [20]

State	KLD [20] UD(%) for IAs(%)				Joint Transformation UD(%) for IAs(%)			
	90	95	105	110	90	95	105	110
θ_2	0	1	2	0	0	0	0	0
θ_3	22	55	56	32	0.14	0.16	0.03	.02
θ_4	0	0	0	0	0	0	0	0
θ_5	0	0	0	0	0	0	0	0
θ_6	0	0	0	0	0	0	0	0
θ_7	58	70	70	61	0	0	0	0
θ_8	96	96	95	95	0	46.6	46.6	0
θ_9	0	0	0	0	0	0	0	0
θ_{10}	0	0	0	0	0	0	0	0
θ_{11}	0	0	0	0	0	0	0	0
θ_{12}	0	1	2	0	0	0	0	0
θ_{13}	0	0	0	0	0	0	0	0
θ_{14}	0	5	7	0	0	0	0	0
V_1	0	0	0	0	0	0	0	0
V_2	0	0	0	0	0	0	0	0
V_3	0	2	2	0	0	0	0	0
V_4	0	0	0	0	0	0	0	0
V_5	0	0	0	0	0	0	0	0
V_6	0	0	0	0	0	0	0	0
V_7	0	20	20	0	0	0	0	0
V_8	96	96	96	96	0	0	0	0
V_9	0	0	0	0	0	0	0	0
V_{10}	0	0	0	0	0	0	0	0
V_{11}	0	0	0	0	0	0	0	0
V_{12}	0	0	0	0	0	0	0	0
V_{13}	0	0	0	0	0	0	0	0
V_{14}	0	0	0	0	0	0	0	0

with false data. For simulating this attack, we introduce a concept of degree of damage, denoted as D . It is defined as the difference between true value and false value; and created by different injection amounts (IA). The proposed scheme is simulated for four different injection amounts, which are 90%, 95%, 105% and 110% and observe the effect of D in detection rate. 90% injection amount means that state variable is 10% less than true value. If the difference between true data and false data is more, probability of detection of false data will also be high. Results are shown in the form of UD%. UD% stands for percentage of undetected (UD) samples, which is equal to undetected samples divided by total samples. In the test setup, there are 8892 samples for each attacking case.

To justify the accuracy of the proposed method in detecting the FDI attack, the results are compared with previously reported method [20]. The earlier method used the probability distribution of measurement variations directly, whereas we, by applying transformation schemes on probability distribution of measurement variation, have obtained better detection efficiency. By efficiency here we mean, the undetected samples are less as compared to previously reported results.

Histogram of the KLDs obtained using the transformed measurement variations are plotted for the month of November, where all the measurement values are assumed to be accurate (no FDI attack) and for December, where attack on different state variables is simulated. The overlapping region between the two histogram plot denotes the undetected samples². In the proposed methodology, we have chosen constant c and γ equal to 2 and 1.3 respectively³.

²The exact number of undetected samples can be obtained after setting an appropriate threshold. However, the overlapped region reflects the detection efficiency of the method. Large overlapped region means poor detection efficiency.

³The detailed explanation on selecting parameters is given in Appendix

A. Without considering topology changes

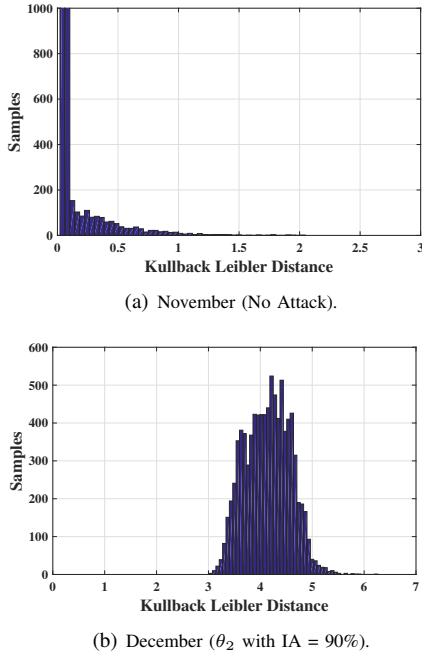


Fig. 2. Histogram of KLD values using Joint Transformation.

The attack is simulated at each time interval for the month of December. The network topology is assumed to be fixed for all measurement samples. Fig. 2(a) and Fig. 2(b) show the histograms for November (no attack) and December (for attack on θ_2 with IA = 90%) respectively. In joint transformation, power transformed KLDs are used to calculate the threshold value, and log transformed KLDs are used to detect the attack for the month of December. The range of KLDs for the month of November (No Attack) is 0.0211 to 2.0474. The threshold considering 99% confidence level is 0.9381. Considering attack on θ_2 with D = 10%, the range of KLD values for the month of December is 3.013 to 6.264. It is clear from the Fig. 2(b) that KLDs for all the samples for the month of December is greater than the threshold 0.9381. The overlapping region is reduced to minimum level after joint transformation which also reflects in higher detection efficiency. Percentage undetected samples are close to 0% for nearly all state variables, however, for θ_8 joint transform also fails to detect the attack for IAs 95% and 105%. The reason is that the bus 8 is only connected to bus 7 and hence few measurements are affected if θ_8 is manipulated. As the state variable increases, number of meters in which the attack is injected increases which results in higher KLD value and hence the attack is detected, which is shown in Table III, therefore the proposed method can be considered as a generalised method to detect false data injection attacks. With the assumption that the historical data is already transformed previously, the time taken for calculating runtime KLD is 0.808 ms for one sample. Similarly if historical data is to be transformed (\approx 87K samples are transformed), then the complete process takes 250 ms, which is still far less as SE is generally performed in every 2 minutes [30]. Furthermore, the proposed method

does not label undetected faults (high impedance faults) as FDI attack, as for such faults the measurement variation is similar to that of slight perturbation of load and hence remain undetected. During our investigation, run-time KLD for the high impedance fault case was always less than the threshold.

TABLE III
VARIATION OF KLD CONSIDERING ATTACK ON MULTIPLE STATE VARIABLES

Attack on states	IA (%)	Kullback Leibler Distance
No-attack	-	0.7830
θ_2	110	3.8760
θ_2, θ_4	110	6.7222

B. Considering network topology changes

Any change in the network topology will cause false detection if the threshold is not appropriately selected for the topology change in consideration. In order to avoid false detection, different thresholds are obtained for different network topology changes in the system. The data set of historical measurements for each line outage is created and the attack is simulated for each topology change. The joint transformation scheme successfully detects the attacks for majority of state variables, however for some cases as tabulated in Table IV, the proposed transformation scheme fails to detect the attack. Undetected system states for the corresponding line outages are shown in first and second column respectively of Table IV. It is noteworthy that the max/min undetected samples shown in third and fourth column are for the cases when the UD(%) is greater than 0%.

TABLE IV
UNDETECTED PERCENTAGE CONSIDERING TOPOLOGY CHANGES⁴.

Undetected States	Line Outage	UD %	
		Max(%) ^{Line} _{IA%}	Min(%) ^{Line} _{IA%}
θ_3	2-13, 15-20	9.16 ⁽³⁾ ₍₉₅₎	0.01 ⁽⁴⁾ ₍₁₀₅₎
θ_7	3-5, 8-13, 15-20	23 ⁽³⁾ ₍₁₀₅₎	0.01 ⁽¹⁶⁾ ₍₁₁₀₎
θ_8	1-20	75.61 ⁽³⁾ _(95,105)	0.02 ⁽¹³⁾ _(90,110)
θ_{10}	3-5, 16, 18	23.50 ⁽¹⁶⁾ ₍₁₁₀₎	7.64 ⁽⁵⁾ ₍₁₀₅₎
θ_{11}	3-5, 9, 10, 11, 12, 16-19	31.69 ⁽¹¹⁾ ₍₉₅₎	0.01 ^(12,16,19) ₍₁₀₅₎
θ_{12}	12, 19	40.76 ⁽¹²⁾ ₍₉₀₎	0.34 ⁽¹⁹⁾ ₍₉₅₎
θ_{13}	13	2.68 ⁽¹³⁾ ₍₉₀₎	2.68 ⁽¹³⁾ ₍₉₀₎
θ_{14}	10, 17, 20	12.39 ⁽¹⁷⁾ _(90,110)	0.01 ⁽¹⁰⁾ ₍₉₅₎
V_3	3	17.90 ⁽³⁾ _(90,110)	17.90 ⁽³⁾ _(90,110)
V_8	1, 3, 4, 5, 8-13, 18, 20	67.74 ⁽⁸⁾ _(90,110)	0.09 ⁽¹³⁾ _(90,110)

⁴UD % shown in the table is only for the cases where undetected samples are greater than zero. Moreover, it is worth mentioning that for certain IA, the proposed method also detects all the samples for line outage given in second column.

From the test results, it is clear that joint transformation based approach can successfully detect false data injection attacks with higher detection efficiency. However, when network topology changes are considered, the results slightly deteriorates as compared to that when topology change is not considered. Moreover, joint transformation fails to detect attack on θ_8 . It is thus advised that the meters connected directly to the bus 8 must be secured by the system operator in order to alleviate all the possibilities of cyber-threats.

VI. CONCLUSION AND FUTURE SCOPE

False data injection attack is an emerging threat to the security and integrity of smart grid operation. From gaining economic profit to line overloading, line tripping to cascaded failure, the impacts of the FDI attacks are manifold. Therefore in order to protect the smart grid from these serious repercussions, the detection of such attacks are of utmost importance. In this paper, we presented a new transformation based detection schemes for detecting FDI attack. As presented in the paper, the proposed joint transformation scheme detects FDI attacks with high detection probability. It is shown with the help of results that the proposed scheme in general, can detect all false data injection attacks. However, if adversary injects false data in small magnitudes, the proposed scheme is able to detect the attacks with high detection efficiency for the cumulative false data injection greater than $\pm 1\%$, but if the attack magnitude is less, the detection efficiency decreases. Moreover, in the quest of the higher detection efficiency, the false positive rate is also slightly increased. Our research on bringing down the false positive rate is ongoing. Furthermore, in future this work can be extended for identifying targeted compromised meters.

APPENDIX

A. Iterative steps for estimating system states.

Errors are assumed to have a Normal distribution with zero mean and known covariance matrix \mathbf{R} .

$$R_{m,m} = \begin{bmatrix} \sigma_1^2 & 0 & \cdots & 0 \\ 0 & \sigma_2^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_m^2 \end{bmatrix} \quad (15)$$

The function to be minimized (2) can be rewritten as,

$$\mathbf{J}(\mathbf{x}) = [\mathbf{z} - \mathbf{h}(\mathbf{x})]^T \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \quad (16)$$

$$\mathbf{g}(\mathbf{x}) = \frac{\partial \mathbf{J}(\mathbf{x})}{\partial \mathbf{x}} = -\mathbf{H}^T(\mathbf{x}) \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \quad (17)$$

here $\mathbf{H}(\mathbf{x})$ is defined as in (9).

Expanding $\mathbf{g}(\mathbf{x})$ using Taylor series we get,

$$\mathbf{g}(\mathbf{x}) = \mathbf{g}(\mathbf{x}^k) + \frac{\partial \mathbf{g}(\mathbf{x}^k)}{\partial \mathbf{x}} (\mathbf{x} - \mathbf{x}^k) + \dots = 0 \quad (18)$$

$$\mathbf{G}(\mathbf{x}^k) = \frac{\partial \mathbf{g}(\mathbf{x}^k)}{\partial \mathbf{x}} = \mathbf{H}^T(\mathbf{x}^k) \mathbf{R}^{-1} \mathbf{H}(\mathbf{x}) \quad (19)$$

From (18) and (19) we get,

$$\mathbf{x}^{k+1} - \mathbf{x}^k = \mathbf{G}(\mathbf{x}^k)^{-1} \mathbf{H}^T(\mathbf{x}^k) \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \quad (20)$$

after rearranging,

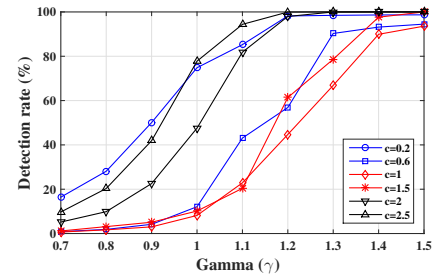
$$[\mathbf{G}(\mathbf{x}^k)] \Delta \mathbf{x}^{k+1} = \mathbf{H}^T(\mathbf{x}^k) \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \quad (21)$$

here $\Delta \mathbf{x}^{k+1} = \mathbf{x}^{k+1} - \mathbf{x}^k$. Considering flat start and setting $k = 0$, \mathbf{x}^{k+1} is calculated iteratively until the maximum $\Delta \mathbf{x}^{k+1} < \epsilon$.

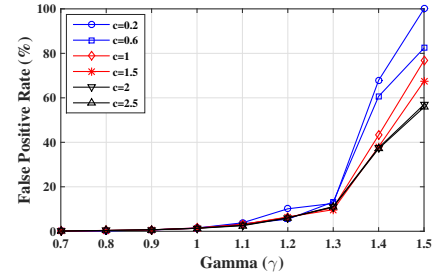
B. Parameter Selection

For power transformation as given in (12), there are two parameters c and γ . As γ tends to increase beyond 1, the measurement variations between adjacent time intervals decreases and vice versa. Similarly, if $c > 1$, measurement variations will increase and if $c < 1$, the same will be decreased. It is also observed that for the values of $\gamma > 1.5$, the measurement variation tends to zero.

As mentioned in (13), the log transformed measurement variation s is directly proportional to constant c . To find the appropriate values of c and γ , we varied γ for set of pre-specified values of c . Detection rate and false positive for variation in γ is calculated.



(a) Detection rate.



(b) False positive rate.

Fig. 3. Detection rate and false positive rate for different values of Gamma (γ).

The study reveals that γ should be more than 1 for high detection rate. Fig. 3(a) shows detection rate for different values of parameter γ when adversary launched an attack on state variable θ_7 with 95% injection amount. As shown in results, detection rate is very less when $\gamma \leq 1$ and a steep rise in the detection rate is achieved for the values of $\gamma > 1$. False positive rate on the other hand increases sharply as γ increases beyond 1.3. As shown in Fig. 3(b), for $c = 2$, false positive rate is increased from 11.09% to 37.55% when parameter γ changed from 1.3 to 1.4.

To analyse the effect of constant c on performance of proposed method, c is varied for set of values of γ . Fig. 4(a) shows detection rate for different values of c when adversary launched an attack on state variable θ_7 with 95% injection amount. Detection rate is high for $c < 0.5$, it is decreasing between 0.5 and 1.2, and after 1.2, it is increasing. Furthermore, as shown in Fig. 4(b), false positive rate is in low range when c has a value greater than 1.

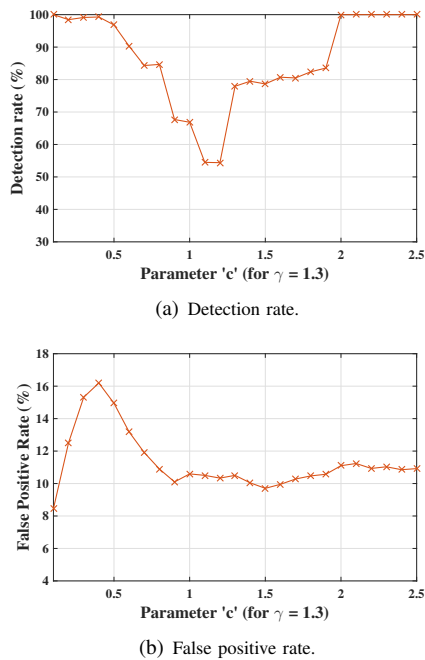


Fig. 4. Detection rate and false positive rate for different values of parameter 'c'.

REFERENCES

- [1] C. W. Ten, C. C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov 2008.
- [2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan 2012.
- [3] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58–66, Jan 2012.
- [4] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. the First Intl Workshop Cyber-Physical Systems*, June 2008, pp. 495–500.
- [5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst.*, vol. 14, no. 1, p. 13, 2011.
- [6] "NISTIR 7628: Guidelines for smart grid cyber security," Tech. Rep., September 2010. [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
- [7] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, Sept 2012.
- [8] 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 Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, 2014.
- [9] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Proc. Preprints 1st Workshop Secure Control Syst. (CPSWEEK)*, vol. 2010, 2010.
- [10] S. Bhattarai, L. Ge, and W. Yu, "A novel architecture against false data injection attacks in smart grid," in *Proc. IEEE Int. Conf. Commun. (ICC)*. IEEE, 2012, pp. 907–911.
- [11] M. Talebi, C. Li, and Z. Qu, "Enhanced protection against false data injection by dynamically changing information structure of microgrids," in *Proc. IEEE 7th Sensor Array Multichannel Signal Process. Workshop (SAM)*. IEEE, 2012, pp. 393–396.
- [12] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *IEEE GLOBECOM Workshops (GC Wkskps)*. IEEE, 2011, pp. 1162–1167.
- [13] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. 44th Annu. Conf. Inf. Sci. Syst. (CISS)*, 2010.
- [14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Proc. 45th Int. Univ. Power Eng. Conf. (UPEC)*. IEEE, 2010, pp. 1–6.
- [15] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.
- [16] S. Li, Y. Yilmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. on Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov 2015.
- [17] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct 2015.
- [18] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive cusum method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, June 2016.
- [19] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Trans. on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, Sept 2015.
- [20] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.
- [21] R. C. Gonzalez and R. E. Woods, *Digital Image Processing, 3rd Edition*. Pearson, 2008.
- [22] D. M. Endres and J. E. Schindelin, "A new metric for probability distributions," *IEEE Trans. Inf. Theory*, 2003.
- [23] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.
- [24] F. Schweppe, "Power system state estimation, parts i, ii and iii," *IEEE Trans. Power Apparatus Syst.*, vol. 89, pp. 120–135, 1970.
- [25] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.
- [26] Z. Qin, Q. Li, and M.-C. Chuah, "Unidentifiable attacks in electric power systems," in *Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*. IEEE Computer Society, 2012, pp. 193–202.
- [27] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.
- [28] K. Khanna, B. K. Panigrahi, and A. Joshi, "Data integrity attack in smart grid: optimised attack to gain momentary economic profit," *IET Gener. Transm. Distrib.*, vol. 10, no. 16, pp. 4032–4039, 2016.
- [29] "Load Data: Market and Operational Data (NYISO)." [Online]. Available: http://www.nyiso.com/public/markets_operations/index.jsp
- [30] R. Berthier, R. Bobba, M. Davis, K. Rogers, and S. Zonouz, "State estimation and contingency analysis of the power grid in a cyber-adversarial environment," in *NIST Workshop on Cybersecurity for Cyber-Physical Systems*, 2012.



networks.

Sandeep Kumar Singh (S'15) received the B.Tech. degree in electronics and communication engineering from Dr. A.P.J. Abdul Kalam Technical University, Lucknow, India, in 2010 and the M.E. degree in electronics and telecommunication engineering from the Shri Govindram Seksaria Institute of Technology and Science, Indore, Indore, India, in 2012. He is currently working towards the Ph.D. degree with the Indian Institute of Technology Delhi, New Delhi, India. His research interests include cyber security of smart grid and advanced metering infrastructure



Kush Khanna (S'15) received the B.Tech. degree in Electrical and Electronics Engineering from Uttar Pradesh Technical University, Lucknow, India in 2008 and M.Tech degree in Power Systems from National Institute of Technology Calicut, Kozhikode, India in 2014. He is currently pursuing his Ph.D. degree from Department of Electrical Engineering at Indian Institute of Technology Delhi, New Delhi, India. His research interests include cyber physical power systems, power system analysis and optimization.



Ranjan Bose (M'10 SM'11) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT) Kanpur, Kanpur, India, in 1992 and the M.S. and Ph.D. degrees in electrical engineering from the University of Pennsylvania, Philadelphia, PA, USA, in 1993 and 1995, respectively. From 1996 to 1997, he was with Alliance Semiconductor Inc., San Jose, CA, USA, as a Senior Design Engineer. Since November 1997, he has been with the Department of Electrical Engineering, IIT Delhi, New Delhi, India, where he is currently the

Microsoft Chair Professor. His current research interests include broadband wireless access, wireless security, and coding theory.



B. K. Panigrahi (SM'06) received the Ph.D. degree in Power Systems from Sambalpur University, Sambalpur, India, in 2004. He is a Professor in Department of Electrical Engineering at Indian Institute of Technology Delhi, New Delhi, India. His research interests include intelligent control of FACTS devices, application of advanced digital signal processing techniques for power quality assessment, and soft computing application to power system planning, operation, and control.



Anupam Joshi (F'14) is a Professor of Computer Science and Electrical Engineering at UMBC. Earlier, he was an Assistant Professor in the CECS department at the University of Missouri, Columbia. He obtained a B. Tech degree in Electrical Engineering from IIT Delhi in 1989, and a Masters and Ph.D. in Computer Science from Purdue University in 1991 and 1993 respectively. His research interests are in the broad area of networked computing and intelligent systems. His primary focus has been on data management and security for mobile, pervasive, and

sensor systems. He has created agent based middleware to support discovery, composition, and secure access of services/data over both infrastructure based and ad-hoc wireless networks, as well as systems that integrate sensors with the grid. He is also interested in Semantic Web, Social Media, and Data/Web Mining, where he has worked on creating personalized and secure web spaces using a combination of agents, policies, and soft computing.