On Detecting False Data Injection with Limited Network Information using Transformation based Statistical Techniques

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

***Abstract*—Cyber-attacks poses a serious threat to power system operation. False data injection attack (FDIA) is one such severe threat, if wisely constructed, can cause flawed estimation of power system states, thereby, leading to uneconomical and unsecured operation of power system. In recent years many methods are proposed to secure the smart grid against malicious cyber-events by protecting certain critical measurement sensors. However, making a system completely hack-proof is rather idealistic. In this paper, in addition to the research carried out in this space, we present a new Log transformation based method to detect the FDIA in real time with high probability. The detection probability of the proposed scheme is compared with existing method using IEEE 14 bus system.**

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

NOMENCLATURE

$\boldsymbol{PD^*}, \boldsymbol{QD^*}$	Attacked real and reactive power demand for all the buses in the attacking region N_i.
$\boldsymbol{PD^{true}}$	Real power demand vector before attack.
$\boldsymbol{QD^{true}}$	Reactive power demand vector before attack.
$\boldsymbol{V^*}, \boldsymbol{\delta^*}$	Attacked voltage and angle for all the bues in the attacking region N_i.
ΔP_{di}	Change in real power load at the bus i.
ΔQ_{di}	Change in reactive power load at the bus i.
ϕ	Null set.
N_G^1, N_G^0	Set of generator buses with and without load.
N_i	Set of buses attacking region for load altering attack at i^{th} bus.
N_i^B	Set of boundary buses in the attacking region N_i
N_Z	Set of zero injection buses.
N_{Bi}	Set of buses connecting i^{th} bus directly.
P_i^{spec}	Specified real power injection at bus i post attack.
P_i^{true}	True real power injection at bus i before attack.
P_{mn}, Q_{mn}	Real and reactive power flow in line mn.
Q_i^{spec}	Specified reactive power injection at bus i post attack.
Q_i^{true}	True reactive power injection at bus i before attack.
V^{true}, δ^{true}	True voltage and angle vector.
Y^A	Bus admittance matrix for the attacking region.

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

I. INTRODUCTION

The basic requirement for operating the power system securely and economically is the precise estimate of the operating state based on the available sensor measurements [1]. In the advent of the integration of information and communication technologies into the power grid, the integrity of the sensors can be compromised. The inaccuracy in estimating the power system state causes unreliable operation which can further lead to system failure if not rectified in the nick of time. In the smart grid environment, attacker can intrude the security of the measurement sensors to inject calculated errors in the smart meters deceiving the system operator with manipulated system states [2]–[5].

Protection of critical sensors based defence techniques are proposed in [6]–[9]. In [10], FDI attacks are detected by tracking the dynamics of measurement variations. Although the method detected the attacks on various state variables with high detection probability, but fails to detect for some cases. Moreover, the technique works well when attack causes ample change in the targeted state variable (5-10% of true value). However, for the attacks where the motive of the adversary is to gain momentary economic benefits, the change in the targeted states are considerably small ($\approx \pm 1\%$ of true value) [11], the above method fails to detect the attack. Therefore, in this paper, we present a transformation based technique to detect the false data injection attacks considering limited network information. The effectiveness of the proposed detection scheme is verified for IEEE 14 bus system by considering different attack scenarios.

The rest of the paper is organized as follows, attack model, attacking region and detection methodology are explained in Section II. Section III shows the results considering different attack scenarios and Section IV concludes the paper.

II. PROPOSED WORK

A. Attack Model

Load altering attack aiming to project less load at a particular bus with the motive of financial misconduct is considered in the paper. The attack is modelled considering two attack

scenarios. In scenario 1, load at the ith bus is altered and the nodal power balance equations are satisfied for the attacking region N_i. In scenario 2, the optimised attack is formulated by making sure the change in the load meter readings of all the buses in the attacking region within the limits ($\approx 50\%$ of true value) in order to deceive the system operator without raising suspicions.

To model the attack for the scenario 1, let us consider N_i be the set of buses in the attacking region with the targeted bus for load alteration attack i. It is assumed that the attacker has the access to the meters in the attacking region only. Let N_i^B be set of boundary buses in the attacking region N_i. The bus admittance matrix for the attacking region is Y^A. Let the desired load change by the attacker at the bus i be ΔP_{di} and ΔQ_{di} for real and reactive load respectively. As the attack is confined to the attacking region only, all the boundary buses are treated as slack or reference bus with voltages and angles fixed to their pre-attacked values [12]. This ensures that the power flow in the tie-lines (connecting attacking region to the external region) remains same as the true values (pre-attacked value).

$$\begin{aligned} P_i^{spec} &= P_i^{true} + \Delta P_{di} \\ Q_i^{spec} &= Q_i^{true} + \Delta Q_{di} \end{aligned} \tag{1}$$

$$\begin{aligned} P_m^{spec} &= P_m^{true} \\ Q_m^{spec} &= Q_m^{true} \quad \forall m \in \{N_i - N_i^B\}, m \neq i \end{aligned} \tag{2}$$

Here P^{spec} and Q^{spec} are desired specified real and reactive power injection to launch the attack. As given in (1) and (2), the desired load alteration (ΔP_d and ΔQ_d) is considered for ith bus only.

$$V_m = V_m^{true} \quad \forall m \in N_i^B \tag{3}$$

$$\delta_m = \delta_m^{true} \quad \forall m \in N_i^B \tag{4}$$

Similarly the voltages for all the buses in the non attacking region as well as for boundary buses in the attacking region remains same as true value.

$$P_m^{cal} = Real\{V_m^* \sum_{k=1,k\neq m}^{N_A} V_k Y_{mk}^A\} \quad \forall m \in (N_i - N_i^B) \tag{5}$$

$$Q_m^{cal} = -Imag\{V_m^* \sum_{k=1,k\neq m}^{N_A} V_k Y_{mk}^A\} \quad \forall m \in (N_i - N_i^B) \tag{6}$$

For non-boundary buses in the attacking region, P^{cal} and Q^{cal} can be calculated as given in (5) and (6) which are required for obtaining the mismatch vector ΔP and ΔQ. The changed states corresponding to the load alteration attack can be calculated by solving the Newton-Raphson load flow problem for the attack region N_i given below iteratively.

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} J_1 & J_2 \\ J_3 & J_4 \end{bmatrix} \begin{bmatrix} \Delta \delta \\ \Delta V \end{bmatrix} \tag{7}$$

Here J_1,J_2,J_3 and J_4 are $[\partial P/\partial \delta]$, $[\partial P/\partial V]$, $[\partial Q/\partial \delta]$ and $[\partial Q/\partial V]$ respectively. ΔP and ΔQ are the mismatch vectors for real and reactive power injections respectively.

After obtaining the post attack state variables in the attacking region N_i, the changed flows can be calculated as,

$$\begin{aligned} P_{mn} =& V_m^2(g_{sm} + g_{mn}) - \\ & V_m V_n(g_{mn}\cos\theta_{mn} + b_{mn}\sin\theta_{mn}) \quad \forall m,n \in N_i \end{aligned} \tag{8}$$

$$\begin{aligned} Q_{mn} =& -V_m^2(b_{sm} + b_{mn}) - \\ & V_m V_n(g_{mn}\sin\theta_{mn} - b_{mn}\cos\theta_{mn}) \quad \forall m,n \in N_i \end{aligned} \tag{9}$$

In attack scenario 2, the motive of the attacker remains same as that in scenario 1, i.e. to decrease the load at a particular bus, however, the constraints on the change in loads of the buses in the attacking region is limited to the $\pm 50\%$ of the pre-attack (true) value. The detailed modelling of the attack scenario 2 is now being explained. The objective function is to minimize the load on the bus i for the attacking region N_i as given in (10).

$$\{\boldsymbol{PD^*}, \boldsymbol{QD^*}, \boldsymbol{V^*}, \boldsymbol{\delta^*}\} = arg\{\min_{\substack{\boldsymbol{PD},\boldsymbol{QD},\\ \boldsymbol{\delta},\boldsymbol{V}}} \{PD_i\}\} \tag{10}$$

subjected to (3),(4) and (11)-(14).

$$0.5(PD_m^{true}) \leq PD_m \leq 1.5(PD_m^{true}) \quad \forall m \in N_i \tag{11}$$

$$0.5(QD_m^{true}) \leq QD_m \leq 1.5(QD_m^{true}) \quad \forall m \in N_i \tag{12}$$

Constraints (11) and (12) ensures that all the real and reactive power demands in the attacking region N_i remains within the limits after the attack. Moreover, for the non-boundary buses, the voltage and angles bounded in the limits as given in (13) and (14).

$$0.9 \leq V_m \leq 1.1 \quad \forall m \in N_i - N_i^B \tag{13}$$

$$-\pi/2 \leq \delta_m \leq +\pi/2 \quad \forall m \in N_i - N_i^B \tag{14}$$

After solving (10), the attacked power flow measurements can be obtained by using (8) and (9).

B. Attacking Region

As pointed out in [13], [14], to launch a hidden load altering attack, the attacking region must not have a zero injection bus as a boundary buses. Moreover, the attacking region cannot have generator buses without the load in the attacking region as these meters are physically secured by the plant operator and hacking these require inside help. Furthermore, the attacking region is assumed to have generator buses with loads only as boundary buses, as the voltage of the generator bus is considered to be fixed and is not altered by attack. Based on these assumptions and those given in [11], [15], the attacking region for the scenario 1 can be formulated as,

$$\begin{aligned} N_i = \{N_{Bi} \cup \{i\} :& N_i \cap N_G^0 = \phi; \\ & N_i^B \cap N_Z = \phi; \\ & \{N_i - N_i^B\} \cap N_G^1 = \phi\} \end{aligned} \tag{15}$$

The attacking regions (scenario 1) for IEEE 14 bus system are shown in Fig. 1. For attack scenario 2, the attacking region can have zero injection buses and generator buses, however

the generator buses in the attacking region must not be non-boundary bus. Therefore, for attack scenario 2, the attacking region can be formulated as,

$$N_i = \{N_{Bi} \cup \{i\} : \{N_i - N_i^B\} \cap N_G = \phi\} \quad (16)$$

Apart from the attacking regions shown in Fig. 1, attack

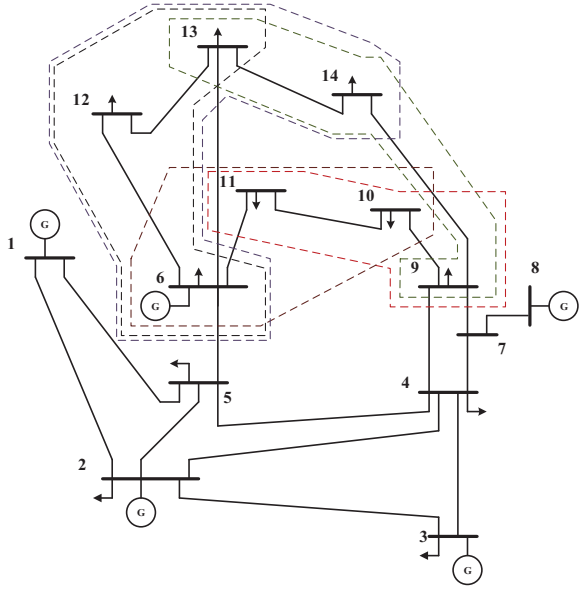


Fig. 1. Attacking regions (scenario 1) for IEEE 14 bus system.

scenario 2 also has N_3 and N_4 with same set of buses $\{2, 3, 4, 5, 7, 9\}$.

C. Detection Methodology

The proposed scheme tracks the dynamics of the measurement data using Kullback-Leibler distance to detect false data injection attacks. Two probability distribution p and q are used to calculate KLD. p is the probability distribution historical measurement variation and q is the distribution of measurement variation between two consecutive time step. Transformation based methods are used to transform one probability distribution into other. In this paper, we use Log transformation to detect false data injection attack.

In the field of image processing, Log transformation is used for transforming the intensity by expanding the value of dark pixels in an image while compressing higher intensity value. As applied here, Log transformation maps narrow range of low measurement values in the input into the wider range of output values. The log transformations can be defined as,

$$s = log(1 + r) \quad (17)$$

Here, r and s are measurement values before and after transformation respectively. To measure the deviation of the measurement variation of the present time sample from the historical measurement variation, Kullback-Leibler distance is used.

The Kullback-Leibler distance is a measure of the information lost when $p(x)$ is used to approximate $q(x)$. The KLD is always non-negative i.e., $D(p\|q) > 0$, and having zero value if and only if $p = q$. It does not obey triangle inequality and is not symmetric, $D(p\|q)$is not equal to $D(q\|p)$. It is also known as information gain, information divergence, and discrimination information. The Kullback- Leibler distance (KLD) between two probability mass functions $p(x)$ and $q(x)$ is represented as,

$$D(p\|q) = \sum p(x) \ln \frac{p(x)}{q(x)} \quad (18)$$

KLD value is compared with predefined threshold value, which is calculated without considering false data injection attack. If the run time KLD is greater than threshold value, adversary has launched FDI attack for that particular time step. Threshold value is an important parameter in proposed scheme and is computed as given in [10]. If we select high threshold value, some of the attacks may not be detected by proposed scheme and if we choose low threshold value, some true measurements may be categorized as compromised measurements. As given in [10], threshold value is selected using histogram plot of historical measurements. For threshold calculation p is derived from histogram plot of historical measurements and q is derived from histogram plot of November month true measurements. In proposed scheme, we use maximum histogram distance with certain confidence level as threshold value. For example, 95% confidence level means that threshold value is larger than 95% of the historical measurements.

III. Results and Discussion

IEEE 14 bus system is used to verify the proposed detection scheme. The load buses in IEEE 14 bus system is linked with each load zone of NYISO as given in [10].

The measurements are obtained by considering the NYISO load data from Jan 1, 2014 to Dec 31, 2014 given in [16]. The eleven load zones are shown in the Fig. 2. Due to the unavailability of 5 min load data, the hourly data is intrapolated as explained in [10].

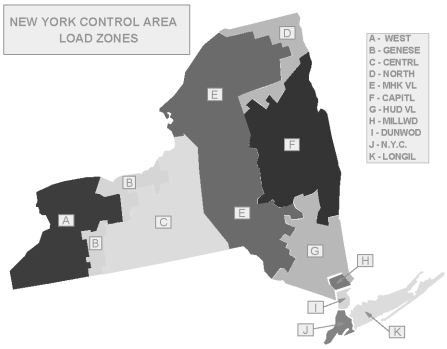
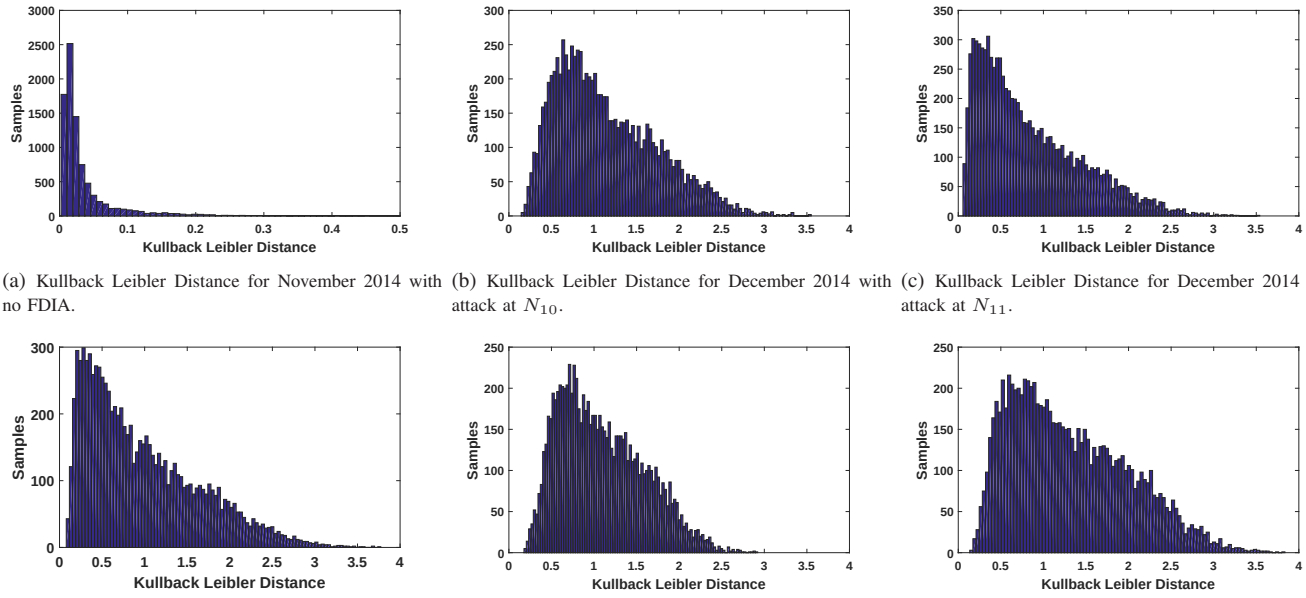


Fig. 2. NYISO map showing 11 load zones.

A fully measured power system is considered, therefore a total of 108 measurements (28 measurements for real and reactive power injection, 80 measurements for real and reactive power flows for all the lines) are obtained for each 5 min time interval. It is further assumed that the measurements for the samples from Jan 1, 2014 to Oct 31, 2014 are without attack and hence considered to be true historical measurements. For the complete month of November, the measurement samples are used to calculate the threshold and the load data for the



(a) Kullback Leibler Distance for November 2014 with no FDIA.

(b) Kullback Leibler Distance for December 2014 with attack at N_{10}.

(c) Kullback Leibler Distance for December 2014 with attack at N_{11}.

(d) Kullback Leibler Distance for December 2014 with attack at N_{12}.

(e) Kullback Leibler Distance for December 2014 with attack at N_{13}.

(f) Kullback Leibler Distance for December 2014 with attack at N_{14}.

Fig. 3. Histogram of Kullback Leibler Distance Using Log transformation for attack scenario 1.

month of December is used to simulate the attack for both attacking scenarios.

The true measurements $z_{true}(t)$ at the time step t are calculated after obtaining V^{true} and δ^{true} by solving the Newton-Raphson load flow problem for the given loading conditions at the time step t. The historical measurement variation $z_{true}(t) - z_{true}(t-1)$ is obtained for all the samples from Jan 1,2014 to Oct 31, 2014. Similarly the measurement variation for the month of November is obtained. Both historical and November measurement samples are then transformed using (17). The threshold is calculated by obtaining the KLD for the transformed measurement variations for 99% confidence. In this study, the threshold is 0.2288 as shown in Fig. 3(a) which is used to detect the attack for both attack scenarios.

A. Attack Scenario 1

The attack is modelled using (1)-(9) for all the load samples for the month of December 2014. The measurement variation $z_a(t) - z_{true}(t-1)$ is calculated from the attacked measurement samples $z_a(t)$ and true measurement $z_{true}(t)$ for complete December load samples.

The histogram of Kullback-Leibler distance considering different attacking regions for attack scenario 1 are shown in Fig. 3. Table I compares the detection probability of the proposed method with the simple KLD technique proposed in [10]. The results reveals that the proposed scheme successfully detect the FDIA for in higher test samples as compared with other method.

B. Attack Scenario 2

The attack is modelled by minimizing (10) subjected to (3),(4) and (11)-(14) for complete month of December. As mentioned for attack scenario 1, the measurement variation for the attack scenario 2 is calculated similarly. The histogram of Kullback-Leibler distance for attack scenario 2 is shown in Fig. 4 and Fig. 5. Table II presents the comparison of detection scheme with and without transformation. Although the method proposed in [10] performs relatively better in attack scenario 2, however the log transformation method detects the attack with considerably higher detection probability.

TABLE I
DETECTION PERCENTAGE COMPARISON FOR ATTACK SCENARIO 1

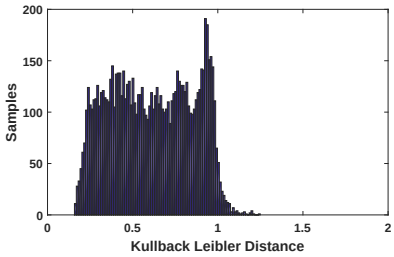
Attacking Region	KLD [10]		Log Tranformation (Proposed Method)	
	Detected Samples	Detection (%)	Detected Samples	Detection (%)
$N_{10}\{9, 10, 11\}$	1192	13.41	8847	99.49
$N_{11}\{6, 10, 11\}$	467	5.25	7755	87.21
$N_{12}\{6, 12, 13\}$	550	6.19	8200	92.21
$N_{13}\{6, 12, 13, 14\}$	6311	70.97	8876	99.82
$N_{14}\{9, 13, 14\}$	1622	18.24	8858	99.62

TABLE II
DETECTION PERCENTAGE COMPARISON FOR ATTACK SCENARIO 2

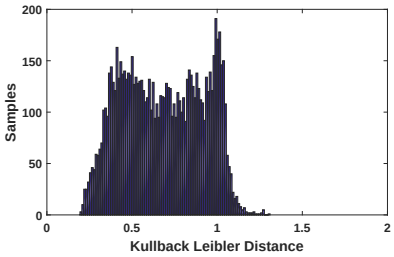
Attacking Region	KLD [10]		Log Tranformation (Proposed Method)	
	Detected Samples	Detection (%)	Detected Samples	Detection (%)
$N_3\{2, 3, 4, 5, 7, 9\}$	1892	21.28	8599	96.71
$N_4\{2, 3, 4, 5, 7, 9\}$	1588	17.86	8853	99.56
$N_{10}\{9, 10, 11\}$	8879	99.85	8888	99.95
$N_{11}\{6, 10, 11\}$	3632	40.85	8847	99.49
$N_{12}\{6, 12, 13\}$	4081	45.90	8871	99.76
$N_{13}\{6, 12, 13, 14\}$	8092	91.00	8889	99.96
$N_{14}\{9, 13, 14\}$	8892	100	8891	99.99

IV. CONCLUSION

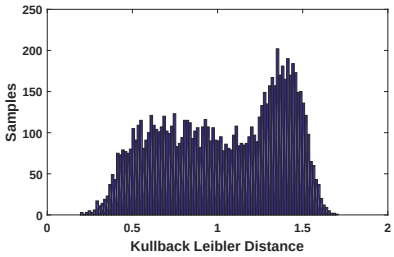
Making power grid resilient to cyber-intrusion is considered as highest priority for the futuristic smart power system. FDIAs are the most serious type of recognized cyber-attacks



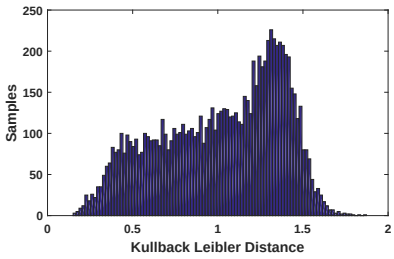
(a) Kullback Leibler Distance for December 2014 with attack at N_3.



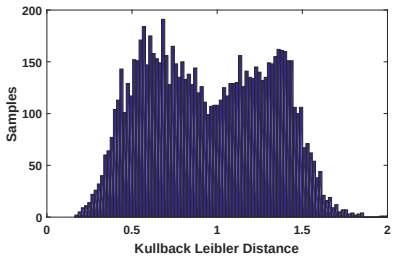
(b) Kullback Leibler Distance for December 2014 with attack at N_4.



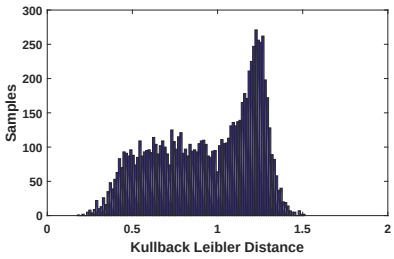
(c) Kullback Leibler Distance for December 2014 with attack at N_{10}.



(d) Kullback Leibler Distance for December 2014 with attack at N_{11}.



(e) Kullback Leibler Distance for December 2014 with attack at N_{12}.



(f) Kullback Leibler Distance for December 2014 with attack at N_{13}.

Fig. 4. Histogram of Kullback Leibler Distance Using Log transformation for attack scenario 2.

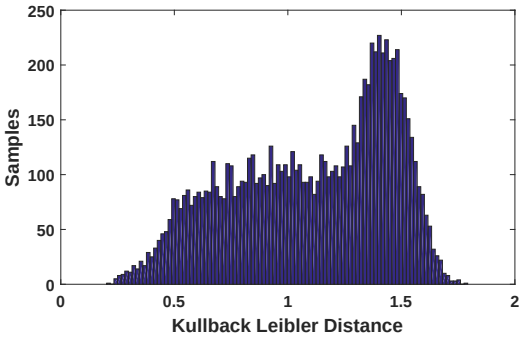


Fig. 5. Kullback Leibler Distance for December 2014 with attack at N_{14}.

which can affect the power system in many adverse forms. In this paper we have presented a new scheme to detect FDIAs by comparing the log transformed measurement variations for historical and real time measurement samples. The method is compared with other similar method proposed in the recent past. The results reveals that the Log transformed based statistical method detects FDIAs with higher efficiency. For this study we have not considered topology changes in the system during attack. However, this can be added by creating a historical scenario considering topology variations without any change in the detection methodology. Our research on analysing the possible impacts of cyber-intrusion and detection is ongoing.

REFERENCES

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC Press, 2004.

[2] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 645–658, 2011.

[4] 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.

[5] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *Selected Areas in Communications, IEEE Journal on*, vol. 32, no. 7, pp. 1460–1470, 2014.

[6] 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," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 3, pp. 717–729, 2014.

[7] 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 *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, vol. 2010, 2010.

[8] M. Talebi, C. Li, and Z. Qu, "Enhanced protection against false data injection by dynamically changing information structure of microgrids," in *Sensor Array and Multichannel Signal Processing Workshop (SAM), 2012 IEEE 7th*. IEEE, 2012, pp. 393–396.

[9] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011, pp. 1162–1167.

[10] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *Smart Grid, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[11] K. Khanna, B. K. Panigrahi, and A. Joshi, "Data integrity attack in smart grid: Optimised attack to gain momentary economic profit," *IET Generation, Transmission & Distribution*, July 2016.

[12] K. Davis, K. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, Nov 2012, pp. 342–347.

[13] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sept 2012.

[14] K. Khanna, B. K. Panigrahi, and A. Joshi, "Feasibility and mitigation of false data injection attacks in smart grid," in *2016 IEEE 6th International Conference on Power Systems (ICPS)*, March 2016, pp. 1–6.

[15] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *Smart Grid, IEEE Transactions on*, vol. 5, no. 4, pp. 1665–1676, 2014.

[16] "Load Data: Market and Operational Data (NYISO)." [Online]. Available: http://www.nyiso.com/public/markets_operations/index.jsp