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

*PD*, *QD* Attacked real and reactive power demand for all the buses in the attacking region \(N_i\).

*PDtrue* Real power demand vector before attack.

*QDtrue* Reactive power demand vector before attack.

*V*, *δ* Attacked voltage and angle for all the buses in the attacking region \(N_i\).

\(ΔP_{Bi}\) Change in real power load at the bus \(i\).

\(ΔQ_{Di}\) Change in reactive power load at the bus \(i\).

\(φ\) Null set.

\(N^0_G, N^1_G\) 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 \(N_i\).

\(N_i^Z\) Set of zero injection buses.

\(P^{spec}_{i}\) Specified real power injection at bus \(i\) before attack.

\(P^{true}_{i}\) True real power injection at bus \(i\) before attack.

\(P_{mn}, Q_{mn}\) Real and reactive power flow in line \(mn\).

\(Q^{true}_{i}\) True reactive power injection at bus \(i\) before attack.

\(V^{true}_{i}, δ^{true}_{i}\) True voltage and angle vector.

\(Y_A\) Bus admittance matrix for the attacking region.

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 (≈ ±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 \( i \)th 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 are with in the limits (\( \approx 50\% \) of true value) in order to deceive the system operator without raising suspicions.

To model the attack for 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 \( \Delta P_{di} \) and \( \Delta Q_{di} \) 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).

\[
P^{spec}_{i} = P^{true}_{i} + \Delta P_{di} \\
Q^{spec}_{i} = Q^{true}_{i} + \Delta Q_{di} 
\]

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

\[
P_{mn} = y_m^2(g_{sm} + g_{mn}) - V_mV_n(g_{mn}\cos \theta_{mn} + b_{mn}\sin \theta_{mn}) \quad \forall m, n \in N_i \tag{8}
\]

\[
Q_{mn} = -y_m^2(b_{sm} + b_{mn}) - V_mV_n(g_{mn}\sin \theta_{mn} - b_{mn}\cos \theta_{mn}) \quad \forall m, n \in N_i \tag{9}
\]

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).

\[
\{ PD^*, QD^*, V^*, \delta^* \} = \arg \min_{P_D,Q_D, \delta,V} \{PD_i \} \tag{10}
\]

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

\[
0.5(PD^*_{true}) \leq PD_m \leq 1.5(PD^*_{true}) \quad \forall m \in N_i \tag{11}
\]

\[
0.5(QD^*_{true}) \leq QD_m \leq 1.5(QD^*_{true}) \quad \forall m \in N_i \tag{12}
\]

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,

\[
N_i = \{N_{Bi} \cup \{i\} : N_i \cap N_i^0 = \phi; \quad N_i^B \cap N_G = \phi; \quad \{N_i - N_i^B\} \cap N_i^0 = \phi \} \tag{15}
\]

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 nonboundary bus. Therefore, for attack scenario 2, the attacking region can be formulated as,

\[ N_i = \{ N_{B_i} \cup \{i\} : \{ N_i - N_i^B \} \cap N_G = \phi \} \]  

(16)

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

\[ s = log(1 + r) \]  

(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,

\[ D(p||q) = \sum p(x) \log \frac{p(x)}{q(x)} \]  

(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 selected using histogram plot of historical 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].

![NYISO map showing 11 load zones.](image)

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
The true measurements \( z_{true}(t) \) at the time step \( t \) are calculated after obtaining \( V_{true} \) and \( d_{true} \) 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.

### IV. Conclusion

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