State Estimation in the Presence of Cyber Attacks Using Distributed Partition Technique

Muhammad Rashed, Iqbal Gondal,
Joarder Kamruzzuman, Syed Islam
ICSL,School of Engineering IT and
Physical Sciences

Federation University
Mt Helen, VIC 3350 Australia
muhammadrashed@students.federation
.edu.au

***Abstract*—The security of smart grid (SG) is an open problem. False data injection attacks (FDIAs) could pose serious risks to automated smart grid and can cause power system outages which eventually could lead to huge economical losses. Cyber-attacks on critical infrastructure are big concerns to the nation's energy reliability; and attackers come up with new attack strategies that couldn't be detected by the traditional bad data detection methods. Although bad data detection (BDD) schemes based on traditional state estimation and chi-square tests within power systems have been used and considered very reliable in detecting false measurements, these BDD schemes and state estimators have been found vulnerable and failed to combat engineered cyber-attacks. In this paper, a novel chi-square detector has been used with a combination of two state estimators in Distributed Partitioning State Estimation (DPSE), results show it is very effective to combat FDIAs when compared with traditional state estimation techniques. The main idea of DPSE is to increase the sensitivity of the chi-square tests by partitioning the large grids into small blocks and applying the tests on each partition individually. State estimator modelled on a novel chi-square detector which is based on particle swarm optimization (PSO) algorithm significantly improved the results. Numerical simulations conducted in MATPOWER confirm the feasibility and effectiveness of the proposed method.**

Keywords—smart grid, falsified data injection, DSE, DPSE, APSE State Estimation, WLS, Chi-square test.

I. INTRODUCTION

The SG uses two-way communication in order to create a widely distributed automated energy delivery network [1]. State Estimation is an algorithm used within power systems in order to determine the system current state based on the system model and measurements collected from different bus using metering systems [2]. The concept of power system state estimation was introduced originally by Schweppe and as a result measurements of power system state estimation are being used by many methods to detect bad data [4]. These measurements help in maintaining the operation & stability of the network. In state estimation real-time measurements for active and reactive power and current are collected at various busbars and are fed to the SCADA or control centres through communication channel or medium such as wireless and wired. Busbars serve joining points of power lines and SG infrastructure. State Estimation provides an effective online monitoring of the SG that helps main control centres in different decision-making processes such as generation and consumption planning and helps in building real time models of electricity networks in energy management systems (EMSs) [26]. The three mostly used state estimation techniques are maximum likelihood, Weighted Least Square (WLS) & minimum variance.

A traditional state estimation such as WLS is considered a reliable technique in terms of collecting state variables and measurements such as voltage magnitude, phase angle and power at different nodes for a typical network topology with the help of Phasor Measurement Units (PMUs) [10]. A PMU is an advanced digital meter used at different buses within SG for monitoring of SG operations [7]. It can measure not only the phasor of the bus voltage but also the current phasors of incident power branches with high accuracy.

WLS has been one of the most trustworthy techniques when it comes to segregating measurements from bad data in order to estimate system states. Its main objective is to minimize the sum of the squares of the difference between the estimated and the actual value of the state variable, which is also known as the error. The bad data detection schemes combined with additional techniques can aid in identifying and segregating the bad data samples within state estimation results [27]. The bad data samples can be identified and detected using distributed state estimation at each node when combined with residual norm test [8,24]. These identification techniques were investigated and tested using realistic examples and these proved to be effective to identify, detect and recover from measurement manipulation within the SG.

An attack adversary can strike and inject malicious data into state estimation measurements if well equipped with knowledge of certain parts of network configuration [28]. Such an adversary can accomplish undetected malicious data attacks on state estimation measurements [12]. The Distributed State Estimation (DSE) have been considered very effective in detecting false data injection attacks that cannot be detected by traditional state estimation detection methods such as WLS alone. DSE is a technique that is based on partitioning the SG system into smaller subsystems in order to locate a faulty node [5].

It is possible that bad measurements could be present due to issues such as meter failure, faulty cable and reasons that are outside of the scope of FDIAs. There are certain techniques developed that can detect bad data in this case and remove them. Research works demonstrate that FDIAs that have prior knowledge of the network configuration within power systems can bypass traditional BDD schemes and are hard to detect [30]. Cyber-attack such FDIAs can purposely craft sparse measurements to perturb the results of state estimators and not detectable through BDD schemes such as chi-square tests [31]. FDIAs pose a threat to SG critical

infrastructure and are big concerns to the nation's energy operational reliability; as attackers keep coming up with new strategies that couldn't be detected by the traditional bad data detection methods.

For FDIAs, there are three assumptions:
1) attackers have complete knowledge about operations of the power systems.
2) attackers possess information about network topology, power system parameters and BDD mechanism.
3) attackers can manipulate the measurements of customers meters.
The most common technique used to detect these three kinds of FDIAs is to pass the state measurements through a normalised residual test which is based on an objective function for a certain probability of error determined from a residual test [32]. This technique is very useful and is used in combination with most of the bad data detection schemes. However, FDIAs that are based on complete network configuration can pose a challenge and stay within the threshold limit and stay undetected when residual norm test is applied to a whole system. DSE is useful in detecting these kinds of FDIAs where system is subdivided into smaller subsystems based on certain clustering algorithm and network topology and chi-square tests is applied to smaller subsystems [35].

There are several BDD schemes available that can be used in combination with traditional state estimation such as WLS for filtering the false information from clean data; well-known methods include Chi-squares tests and normalized residuals method [33]. Chi-squares test is used for detecting false data injection attack within this paper. It has been claimed in the literature that chi-square test is a reliable technique when combined with traditional state estimation methods in order to identify FDIAs within SG [31]. Chi-squares test takes the square of the difference of the actual and estimated measurements, based on the assumption that the error caused by the state estimation process is subjected to normal distribution with zero mean and unity variance [26]. We use traditional chi-square test because it can implement a real-time detection mechanism for random anomalies and failures within the SG. We also implemented a novel online detection method based on chi-square tests proposed in [8]. This novel method is developed by solving an optimal problem based on particle swarm optimization (PSO) algorithm. This method considers the characters of traditional chi-square detection methods associated with two kinds of state estimates.

Adaptive Partitioning State Estimation (APSE) was used in which graph of IEEE39-bus system was generated and divided into three subsystems using the L-bounded Graph Partition Algorithm with bad data detection methods and results prove to be accurate than traditional state estimation by Liu et. al [12]. The Chi-square test results are in direct proportion to the number of measurements taken hence more measurements will provide results close to actual values on the cost of processing time required for conducting tests. Subsystem-Extension is used to update the graph in order to narrow the suspicious region of bad data.

DSE is based on partitioning the large system into smaller subsystems and apply chi-square tests in each subsystem [5]. Since the threshold of the smaller subsystem is expected to be lower than the entire system, it is more sensitive to detect bad data in each system. However, large number of subsystems will require more time for processing chi-square tests.

In this paper, FDIAs cases were implemented within IEEE 14-bus and IEEE-30 bus systems considering the chi-square detection state estimator 1 fails in identifying this attack. A novel chi-square detection method associated with two kinds of state estimators mentioned in [8] are implemented. The tests are solved using MATPOWER. The methodology DPSE is a mix of DSE [5] and APSE [12] with an additional state estimator 2 modelled with an online chi-square detector based on PSO and prior history statistical information of state variables.

II. DISTRIBUTED PARTITIONING STATE ESTIMATION USING CHI-SQUARE TEST

Power system state estimation uses real-time redundant measurements to improve data accuracy, meaning not all measurements are considered.

State estimation is widely used to ensure the safety and economy of operation of any power system. The state variables [1,7] are related to the measurements as shown in (1).

$$z = h(x) + e \tag{1}$$

where **x** is the state variables and **z** is the meter measurements.

h(x)= $[h_1 (x_1, x_2 \ldots, x_n) , \ldots, h_m (x_1, x_2, \ldots, x_n)]^T$ where $h_1(x_1, x_2, \ldots, x_n)$ is a function of $x_1, x_2, \ldots, x_n$. e = $[e_1, e_2, \ldots, e_m]^T$ is the measurement noise which is assumed to follow gaussian distribution of zero mean in power system state estimation formulation [5].

Power system state estimation is a measurement of state vectors at different points and busbars that collects real-time measurements in order to find an estimate $\hat{x}$ of x that is the best fit of the measurement z according to eq (1) and solved by the WLS Algorithm [7].

The state estimation formulation can be written as :

$$J(x) = [z - h(x)]^T R^{-1} [z - h(x)] \tag{2}$$

where R^{-1} is referred as the measurement inverse covariance matrix.

In Chi-squares test, the normalized-sum square residual $J(\hat{x})$ follows $x^2_{(m-n)}$ distribution, where m is the number of measurements and n is the number of state variables [5,6].

A hypothesis test would be performed on the Chi-Square distribution to determine if the residual lies within the "acceptable region".The test will use the following conditions based on the results of the chi-square test [6]:

$$\begin{cases} H_0: J(\hat{x}) \geq x^2_{(m-n),p} & bad\ data \\ H_0: J(\hat{x}) \leq x^2_{(m-n),p} & no\ bad\ data \end{cases} \tag{3}$$

where $x^2_{(m-n),p}$ is the detection threshold corresponding to p, where p is the detection confidence which is taken as 95% in this paper [6]. The measurements are bus voltage magnitudes.

WLS estimation problem $\sum_{i=1}^{m} \frac{(z_i - h_i(x))^2}{\sigma_i^2}$ follows a $x^2_{(m-n)}$ distribution, where m-n is the degree of freedom[7].

Algorithm 1 *Weighted Least Square Algorithm*

1: procedure WLS estimate
WLS computes the maximum likelihood of actual state variable
2: Pick initial value for $x=x^0$
3: Solve $(z_i - f_i(x))$ *for* $i = 1 \ldots N_m$
4: Calculate Matrix H as function of x
5: Calculate $H^T T^{-1} H$
6: Calculate $H^T R^{-1} H$
7: Solve for $\Delta X \Delta X = [H^T R^{-1} H]^{-1} H^T R^{-1} [z_i - f_i(x)]$
8: Calc Max $(|\Delta x|_i)$ $i = 1 \ldots N_s$
9: Max $(|\Delta x|_i) < \mathcal{E}$
10: Yes: end procedure
11: No: update x: $x = x + \Delta x$ *go to 3*
12: end procedure

The following steps are used for conducting Chi-squares tests [5]:

a) Compute the objective function below in order to solve WLS estimation problem:

$$J(\hat{x}) = \sum_{i=1}^{m} \frac{(z_i - h_i(x))^2}{\sigma_i^2} \quad (4)$$

b) Chi-squares distribution table corresponds to a value of $x^2_{(m-n),p}$ giving a detection confidence with probability p of 95% and *(m-n)* degrees of freedom.

c) Test the objective function $J(\hat{x}) \geq x^2_{(m-n),p}$ against the value in distribution table. If the resulting value is greater, then bad data is detected. If the value is below the threshold, then it's assumed to be free of false data.

The Jacobian matric, H_1 is given by

$$H_1(x) = \frac{\partial H_1(x)}{\partial x} \quad (5)$$

The Gain matrix $_1(x^k)$ is given by

$$G_1(x^k) = [H_{1i}^T(x_k) R_1^{-1} H_1(x_k)]^{-1} \quad (6)$$

The error covariance matrix of the estimate x is given by

$$Cov([x]) = [H_1^T R_1^{-1} H_1] \quad (7)$$

In order to develop a second estimator 2 based on a novel chi-square detector for dynamic power system, the corresponding state *x(k)* and measurement equations *z(k)* can be expressed as

$$x(k+1) = f(x(k)) + w(k) \quad (8)$$

$$z(k+1) = h(x(k+1)) + v(k+1) \quad (9)$$

The forecasted state vector $\widehat{x_1}\left(k + \frac{1}{k}\right)$ with the corresponding forecasted error covariance matrix $P_1\left(k + \frac{1}{k}\right)$ can be expressed as

$$\widehat{x_1}\left(k + \frac{1}{k}\right) = F(k)\widehat{x_1}(k) + G(k) \quad (10)$$

$$P_1\left(k + \frac{1}{k}\right) = F(k) P_1(k) F^T(k) + Q \quad (11)$$

The traditional chi-square test is not able to detect the injection attack. In order to detect this new injection attack, another state estimator 2 is used based on prior history statistical information of state variables without being attacked leading to a novel chi-square detection based on two state estimators proposed in [8] and as shown in Fig.1. The state estimate and its estimated covariance matrix based on this novel chi-square detection are derived as

$$\widehat{x_2}(k+1) = F(k)E\{x(k)\} + G(k) \quad (12)$$

$$P_2(k+1) = F(k)Cov\{x(k)\}F^T(k) + Q \quad (13)$$

We Tested and analysed this novel chi-square technique using distributed state estimation for both IEEE14 and IEEE30 Bus systems using MATPOWER. The PMUs at each bus or node were used to collect the actual Voltage magnitude and fed to communication channels. This process was repeated after FDIAs. The measured estimates were passed through traditional as well as new chi-square tests. This process was repeated using different subdivisions.

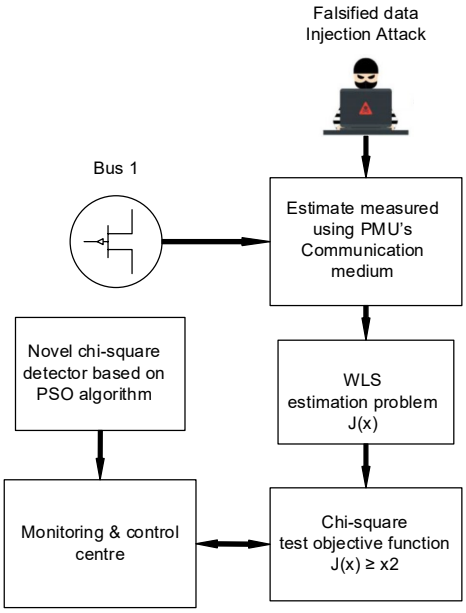

Fig. 1. FDIA into SG and chi-square test

A. *Falsified Data Injection Scenarios*

In this section, the sequence of steps to evaluate DPSE are introduced. The first step is the implementation of state estimation using IEEE14 and IEEE30 bus system using MATPOWER. The measured values undergo the standard Chi-squares test. Figure 1. illustrates a model about FDIA on estimate values collected through PMU's in IEEE14 and IEEE30 Bus system.

The power flow on bus 1 was injected with bad data and changed by 1.06MW. The chi-square test was solved by MATPOWER with the help of a novel chi-square detector. The weighted sum-squared residual in (3) *J(x)=46.93* was calculated more than the threshold $x^2_{(m-n),p} = 46.19$ of the local partitioned bus system revealing the presence of bad data within the estimate measurements. Without the use of this novel chi-square detector & state estimator 2, the residual *J(x)=46.12* was estimated to be lower than the local subsystem

threshold limit hence presence of bad data could not be detected.

FDIAs were injected for every bus system unless all the measurement estimates were falsified. We measured these values after every FDIAs. These values were stored in a tabular format for results to be plotted. We performed a similar analysis for different DPSE techniques such as partitioning of the SG into 7 and 3 subsystems and without the use of any subdivision with the help of a novel chi-square detector. We also repeated this test at the output of each bus.

B. *Experimental Strategy*

The main procedure for DPSE consists of following steps:

a. Record actual SE measurements using PMUs

b. Inject FDIAs

c. Divide the SG into smaller distributed subsystems according to the system's physical topology

d. State estimation in each subsystem

e. Apply DPSE Detection in each subsystem unless you locate the faulty node

f. Use novel chi-square detector

g. Estimate the difference/error in actual and falsified values

h. Repeat the above steps for SG using subdivision in 7 parts, 3 parts and at every bus

C. *Results and Discussion*

Our method DPSE, unlike DSE and APSE, makes an emphasis that the size of the subsystem is crucial in detecting the FDIAs using chi-square tests. In order to prove it, we conducted several tests and picked up samples that were not detected by applying standard chi-square tests on a whole system. The results show that FDIAs were detected relatively easily when the size of the subsystem was smaller. We also used the Novel chi-square detector alongside with standard chi-square detector based on prior statistical information as shown in Fig.2. With the help of a novel chi-square detector, the residual $J(x)$ was found to be higher than the threshold limit of the local subsystem which means there is a presence of bad data. We plotted the actual and falsified values such as voltage magnitude against bus bars. The graphs show that estimate values measured with the help of novel-chi-square detector are closer to non-falsified values as compared to using only one state estimator 1.

Figures 3 & 4 illustrate the plot of values measured at each bus, using different subdivisions that is to partition the overall system into smaller subsystems and apply chi-square tests to each subsystem independently for both IEEE14 and IEEE30. The estimates that are closest to actual values were those using novel chi-square detector based on prior known information. The second results that came closer were those measured through DPSE at distributed subsystem 7 using standard chi-square detector; we subdivided the SG into 7 subsystems and then applied the chi-square tests to each subsystem. This also means we divide the IEEE14 into a group of 2 nodes each and IEEE 30 into 4 nodes each, last two nodes can be done separably.

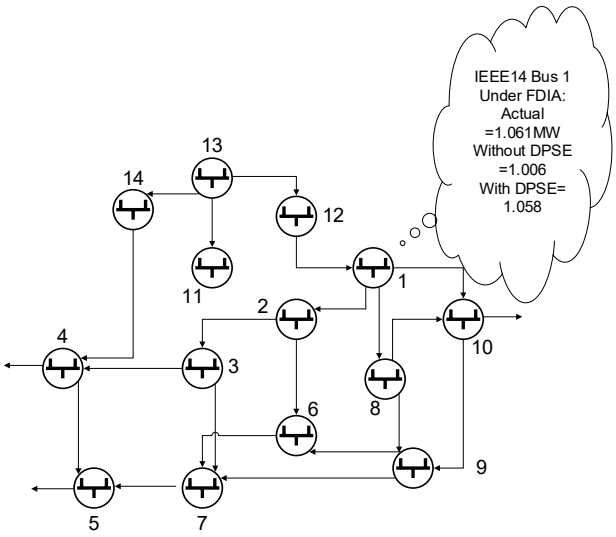

Fig. 2. Bus 1 under FDIA in IEEE Bus 14

Table I. STATE ESTIMATES USING DPSE

Bus	Actual values at PMUs without FDIAs (MW)	Values without DPSE (MW)	Values with DPSE (MW)
1	1.06	1.00	1.05
2	1.04	0.98	1.04
3	1.01	0.95	1.00
4	1.01	0.95	1.00
5	1.01	0.96	1.01
6	1.07	1.01	1.06
7	1.04	0.99	1.04
8	1.08	1.02	1.07
9	1.03	0.97	1.03
10	1.02	0.97	1.02
11	1.04	0.99	1.04
12	1.05	1.00	1.05
13	1.04	0.99	1.04
14	1.01	0.96	1.01

Table II. RMSE FOR DPSE

Time	RMSE
0.28	0.053964622
8.40E-01	0.027339712
1.96E+00	0.01289377
3.92E+00	0.001422997

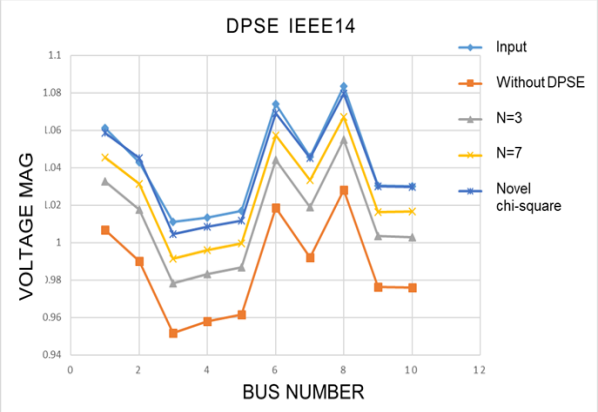

Fig.3. State estimate plot IEEE14

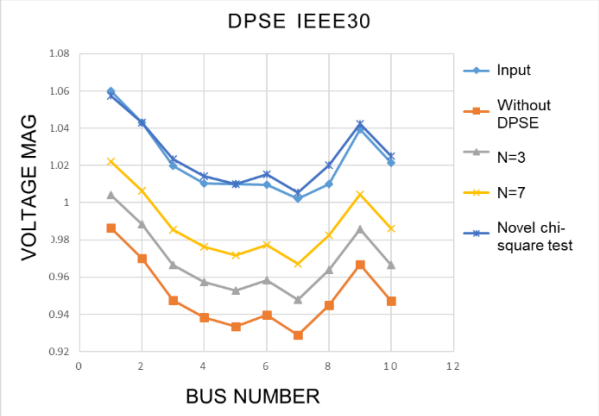

Fig.4. State estimate plot IEEE30

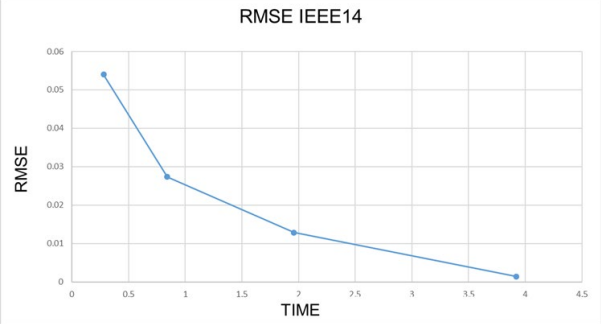

Fig. 5. RMSE for all DPSE schemes IEEE14

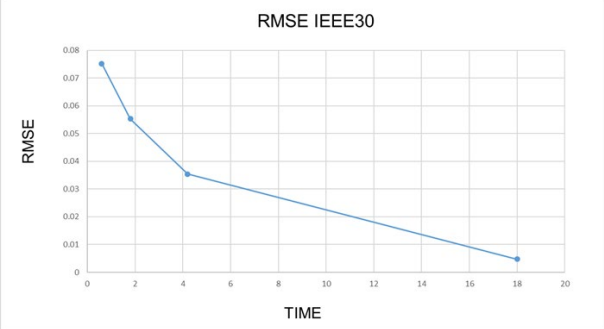

Fig. 6. RMSE for all DPSE schemes IEEE30

The next results that came closer to actual values after subsystem 7 were those using subsystem 3 subdivision. The least realistic estimates were the ones where no DPSE was used and chi-square tests were applied to overall system. These results demonstrate that the smallest subsystem size is also crucial for conducting effective chi-square-tests with state estimator 2.

Table I. represents the voltage at each bus in IEEE14 bus system. The first column represents the actual input without FDIA. The 3rd and 4th columns refer to state estimate values at each bus after FDIA, without and with DPSE, respectively. In our tests, results confirmed that traditional chi-squares test applied on whole system was not be able to detect the FDIAs in some cases. In order to make this more effective, we partitioned the whole system into smaller subsystems and treated each partition as a separate independent system.

D. RMSE Calculation & Discussion

Root Mean Square Error (RMSE) represent error between two data sets [19]. In other words, it compares a predicted value P_i and an observed O_i or known value. The smaller RMSE value illustrates less error and hence predicted and observed values are closer. It's also known as Root Mean Square Deviation and is one of the most widely used statistics in GIS.

We used the following equation to calculate the root mean square error RMSE [19], based on measured and actual value.

$$RMSE = \sqrt{\sum_{i=1}^{n} \frac{(P_i - O_i)^2}{n}} \quad (12)$$

We estimated the root mean squared error between these distribution techniques in reference to actual values and the results for IEEE14 & IEEE30, are shown in Figures 5 & 6. The lowest error was found using novel detector. However, cost for this approach is high in terms of processing time. The processing time increases especially when there are over 10,000 nodes. There must be a tradeoff in order to choose the right operational point and it depends on priorities of SCADA.You can swap the order of subtraction because the next step is to take the square of the difference. This is because the square of a negative value will always be a positive value.

III. CONCLUSION

This paper has proposed a novel detection method of false data injection attacks (FDIAs) against dynamic and distributed state estimation. The values of the state variables and their estimates are determined by solving an optimal model based on PSO algorithm. The new state estimator 2 is modelled on a chi-square detector that was formed based on prior history statistical information of state variables collected at each bus. This state estimator 2 was used in parallel with traditional chi-square detection state estimator 1 and BDD was found to be more effectively working when combined with distributed portioning state estimation (DPSE) in detecting FDIAs.

The novelty of this approach is that 2 state estimators in combination with different partitioning state estimation techniques such as DSE and APSE were not used together in earlier research work. FDIAs were injected within SG systems in such a fashion that these were not detectable when detection technique such as chi-square test was applied to a whole system and without the use of partitioning. The results appear accurate especially when the subsystem is smaller. However,

the use of a parallel state estimator will lead to much more complex residual model in distributed state estimation for a larger network, with increased cost of online detection and processing time.

ACKNOWLEDGEMENT

Research was done in Internet Commerce Security Lab (ICSL) at the school of Engineering IT and Physical Sciences, Federation University. ICSL has been established in collaboration of Westpac, IBM and Victorian Government.

REFERENCES

[1] M. Zhang *et al.*, "False data injection attacks against smart gird state estimation: Construction, detection and defense," *Science China Technological Sciences,* vol. 62, no. 12, 2019, doi: 10.1007/s11431-019-9544-7.

[2] V. Lamba, N. Šimková, and B. Rossi, "Recommendations for smart grid security risk management," *Cyber-Physical Systems,* vol. 5, no. 2, pp. 92-118, 2019, doi: 10.1080/23335777.2019.1600035.

[3] R. K. Kaur, L. K. Singh, and B. Pandey, "Security Analysis of Smart Grids: Successes and Challenges," *IEEE Consumer Electronics Magazine,* vol. 8, no. 2, pp. 10-15, 2019, doi: 10.1109/MCE.2018.2880852.

[4] F. C. Schweppe, "Power System Static-State Estimation, Part III: Implementation," *IEEE Transactions on Power Apparatus and Systems,* vol. PAS-89, no. 1, pp. 130-135, 1970, doi: 10.1109/TPAS.1970.292680.

[5] Y. Gu, T. Liu, D. Wang, X. Guan, and Z. Xu, "Bad data detection method for smart grids based on distributed state estimation," ed, 2013, pp. 4483-4487.

[6] Y. Al-Eryani and U. Baroudi, "An Investigation on Detecting Bad Data Injection Attack in Smart Grid," ed, 2019, pp. 1-4.

[7] B. Matthiss, J. Erb, and J. Binder, "Using Smart Meters for Distribution Grid State Estimation," ed, 2019, pp. 1-5.

[8] R. Chen, X. Li, H. Zhong, and M. Fei, "A novel online detection method of data injection attack against dynamic state estimation in smart grid," *Neurocomputing,* vol. 344, pp. 73-81, 2019, doi: 10.1016/j.neucom.2018.09.094.

[9] X. Nian-de, W. Shi-Ying, and Y. Er-Keng, "A New Approach for Detection and Identification of Multiple Bad Data in Power System State Estimation," *IEEE Transactions on Power Apparatus and Systems,* vol. PAS-101, no. 2, pp. 454-462, 1982, doi: 10.1109/TPAS.1982.317128.

[10] Y. Shi, H. D. Tuan, T. Q. Duong, H. V. Poor, and A. V. Savkin, "PMU Placement Optimization for Efficient State Estimation in Smart Grid," *IEEE Journal on Selected Areas in Communications,* vol. 38, no. 1, pp. 71-83, 2020, doi: 10.1109/JSAC.2019.2951969.

[11] A. G. Phadke, "Synchronized phasor measurements in power systems," *IEEE Computer Applications in Power,* vol. 6, no. 2, pp. 10-15, 1993, doi: 10.1109/67.207465.

[12] L. Ting, G. Yun, W. Dai, G. Yuhong, and G. Xiaohong, "A novel method to detect bad data injection attack in smart grid," ed, 2013, pp. 3423-3428.

[13] T. V. Cutsem, M. Ribbens-Pavella, and L. Mili, "Hypothesis Testing Identification: A New Method For Bad Data Analysis In Power System State Estimation," *IEEE Transactions on Power Apparatus and Systems,* vol. PAS-103, no. 11, pp. 3239-3252, 1984, doi: 10.1109/TPAS.1984.318561.

[14] G. N. Korres, "A Distributed Multiarea State Estimation," *IEEE Transactions on Power Systems,* vol. 26, no. 1, pp. 73-84, 2011, doi: 10.1109/TPWRS.2010.2047030.

[15] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," vol. 14, no. 1, pp. 21-32, 2009, doi: 10.1145/1952982.1952995.

[16] X. Le, C. Dae-Hyun, and S. Kar, "Cooperative distributed state estimation: Local observability relaxed," ed, 2011, pp. 1-11.

[17] V. Kekatos and G. B. Giannakis, "Distributed Robust Power System State Estimation," *IEEE Transactions on Power Systems,* vol. 28, no. 2, 2012, doi: 10.1109/TPWRS.2012.2219629.

[18] O. Kosut, J. Liyan, R. J. Thomas, and T. Lang, "Malicious Data Attacks on the Smart Grid," *IEEE Transactions on Smart Grid,* vol. 2, no. 4, pp. 645-658, 2011, doi: 10.1109/TSG.2011.2163807.

[19] M. Ćalasan, S. H. E. Abdel Aleem, and A. F. Zobaa, "On the root mean square error (RMSE) calculation for parameter estimation of photovoltaic models: A novel exact analytical solution based on Lambert W function," *Energy conversion and management,* vol. 210, 2020, doi: 10.1016/j.enconman.2020.112716.

[20] X. Le, M. Yilin, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," ed, 2010, pp. 226-231.

[21] http://www.pserc.cornell.edu/matpower/.

[22] G. Valverde and V. Terzija, "Unscented Kalman filter for power system dynamic state estimation," *IET Generation, Transmission and Distribution,* vol. 5, no. 1, pp. 29-37, 2011, doi: 10.1049/iet-gtd.2010.0210.

[23] A. Gomez-Exposito, A. Abur, A. de La Villa Jaen, and C. Gomez-Quiles, "A Multilevel State Estimation Paradigm for Smart Grids," *Proceedings of the IEEE,* vol. 99, no. 6, pp. 952-976, 2011, doi: 10.1109/JPROC.2011.2107490.

[24] M. R. Camana Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely Randomized Trees-Based Scheme for Stealthy Cyber-Attack Detection in Smart Grid Networks," IEEE access, vol. 8, pp. 19921-19933, 2020, doi: 10.1109/ACCESS.2020.2968934.

[25] Y. Chakhchoukh, H. Lei, and B. K. Johnson, "Diagnosis of Outliers and Cyber Attacks in Dynamic PMU-Based Power State Estimation," IEEE transactions on power systems, vol. 35, no. 2, pp. 1188-1197, 2020, doi: 10.1109/TPWRS.2019.2939192.

[26] A. Jovicic and G. Hug, "Linear State Estimation and Bad Data Detection for Power Systems with RTU and PMU Measurements," 2020.

[27] Y. Li and Y. Wang, "Developing graphical detection techniques for maintaining state estimation integrity against false data injection attack in integrated electric cyber-physical system," Journal of systems architecture, vol. 105, 2020, doi: 10.1016/j.sysarc.2019.101705.

[28] B. Matthiss, J. Erb, and J. Binder, "Using Smart Meters for Distribution Grid State Estimation," ed, 2019, pp. 1-5.

[29] L. Nandakumar, G. Tillem, Z. Erkin, and T. Keviczky, "Protecting the grid topology and user consumption patterns during state estimation in smart grids based on data obfuscation," Energy Informatics, vol. 2, no. S1, pp. 1-23, 2019, doi: 10.1186/s42162-019-0078-y.

[30] C. Pei, Y. Xiao, W. Liang, and X. Han, "PMU Placement Protection Against Coordinated False Data Injection Attacks in Smart Grid," IEEE transactions on industry applications, vol. 56, no. 4, pp. 4381-4393, 2020, doi: 10.1109/TIA.2020.2979793.

[31] M. A. Rahman, A. Datta, and E. Al-Shaer, "Security design against stealthy attacks on power system state estimation: A formal approach," Computers & security, vol. 84, pp. 301-317, 2019, doi: 10.1016/j.cose.2019.03.022.

[32] J. Shi, S. Liu, B. Chen, and L. Yu, "Distributed Data-Driven Intrusion Detection for Sparse Stealthy FDI Attacks in Smart Grids," IEEE transactions on circuits and systems. II, Express briefs, pp. 1-1, 2020, doi: 10.1109/TCSII.2020.3020139.

[33] Y. Shi, H. D. Tuan, T. Q. Duong, H. V. Poor, and A. V. Savkin, "PMU Placement Optimization for Efficient State Estimation in Smart Grid," IEEE Journal on Selected Areas in Communications, vol. 38, no. 1, pp. 71-83, 2020, doi: 10.1109/JSAC.2019.2951969.

[34] J. K. Watitwa and K. O. Awodele, "Active Distribution System State Estimation: Comparison Between Weighted Least Squares and Extended Kalman Filter Algorithms," ed, 2020, pp. 1-5.

[35] T. Zou, A. S. Bretas, C. Ruben, S. C. Dhulipala, and N. Bretas, "Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks," Electric power systems research, vol. 187, 2020, doi: 10.1016/j.epsr.2020.106490.