2017 the 5th IEEE International Conference on Smart Energy Grid Engineering

On False Data Injection Attack against Dynamic State Estimation on Smart Power Grids

Hadis Karimipour
School of Engineering
University of Guelph
Guelph, Ontario, Canada
e-mail: hkarimi@uoguelph.ca

Venkata Dinavahi
Dep. of Elec. & Com. Eng.
University of Alberta
Edmonton, Alberta, Canada
e-mail: dinavahi@ualberta.ca

Abstract—**Although the advancement of cyber technologies in sensing, communication and smart measurement devices significantly enhanced power system security and reliability, its dependency on data communications makes it vulnerable to cyber-attacks. Coordinated false data injection (FDI) attacks manipulate power system measurements in a way that emulate the real behaviour of the system and remain unobservable, which misleads the state estimation process, and may result in power outages and even system blackouts. In this paper a robust dynamic state estimation (DSE) algorithm is proposed and implemented on the massively parallel architecture of graphic processing unit (GPU). Numerical simulation on IEEE-118 bus system demonstrate the efficiency and accuracy of the proposed mechanism.**

Keywords-bad data detection; cyber-attack; false data injection; dynamic state estimation; graphic processing units; large-scale systems; Markov chain; parallel programming; SCADA; PMUs

I. INTRODUCTION

A smart power grid is a typical cyber-physical system (CPS) which integrates a physical power transmission system with the cyber computation and communication infrastructure [1].

Although the advancement of cyber technologies in sensing, communication and smart measurement devices significantly enhanced power system operation and reliability, its dependency on data communication makes it vulnerable to cyberattacks [2]. Coordinated false data injection (FDI) attacks [3] manipulate power system measurements in a way that emulate the real behaviour of the system and remain unobservable, which misleads the state estimation process, and may result in power outages and even system blackouts [4], [5].

The increasing demand for reliable and economical electricity services raises critical challenges in online monitoring and control of future power grids which rely on dynamic state estimation (DSE) [6], [7]; therefore, security of DSE and its vulnerability to cyber-attack is a major concern.

Detecting and identifying bad data in state estimation is traditionally or conventionally done by comparing the telemetered measurements from supervisory control and data acquisition system (SCADA) with the estimated values of the states. Traditionally, bad data are assumed to be caused by random errors resulting from a fault in a meter and/or its attendant communication system [8], [9]. These errors were modeled by a change of variance in the Gaussian noise, which is detectable using Chi-squares and largest normalized residuals (LNR) test. Many researchers have considered the problem of bad data detection (BDD) in power systems [10], [11], however conventional BDD approaches usually fail when the network malfunction is intentionally caused by an attacker [12], [13].

In order to identify the vulnerability of a power grid, necessary and sufficient conditions were defined to quantify the minimum number of measurements required for a stealth attack [14]. Also, efforts have been made to develop a security-oriented cyber-physical state estimation framework using off-line information in [15], [16] which could identify the compromised set of measurements. Using computational intelligence technique [17] proposed a detection method to identify compromised data belonging to critical infrastructures.

This problem is also formulated as identification of a subset of the measurements which are more vulnerable and easier to be attacked [18]–[21]. The results show that false data injection attacks are easier to detect using the dc model of the system compared to the ac model. However, considering the large size of electric grids, selecting such subsets is a highly complex and computational intensive problem.

One important fact which is neglected in the above works is that the cyber-security analysis should be performed in a timely manner, in order to solve the data attack construction problem efficiently. Otherwise it will slow down the process of state estimation, online monitoring and control of the system behaviour. In such cases even if the attack is detected, there is no time to take an action and prevent further casualties.

Another main concern related to most of the above approaches is that they are not tested on large-scale power systems so the complexity and efficiency of the proposed approaches in practical systems is unclear. Overall, the computational complexity of the proposed approaches grows exponentially with the size of the power network which may make them unpractical for realistic systems.

To overcome the effect of cyber-attacks, in this paper considering the stochastic nature of the system disturbances a cyber-physical model of the power system utilizing the Markov chain theory [22] is proposed. A Markov chain

978-1-5386-1776-2/17/$31.00 ©2017 IEEE

based on these states is then defined. After each estimation process all states are checked on the Markov chain. If the estimated states are close to a value with low probability or out of the Markov chain, the possibility of the cyber-attack is deemed high. In order to speed up the whole process, the proposed robust DSE is implemented on GPU which are specially designed to deal with large amount of data. GPUs have already found applications for accelerating different power system applications [23], [24].

The organization of this paper is as follows. Section II provides formulation and the state estimation model used in this work. Section III explains the proposed robust parallel DSE against FDI and its implementation. The simulation results are provided in Section IV followed by conclusion in Section V.

II. EKF-Based Dynamic State Estimation

The state-space model of the power system DSE can be described as:

$$x_{t+1} = F_t x_t + b_t + \omega_t, \qquad (1)$$
$$E[\omega_t \omega_t^T] = O_t,$$

$$m_{t+1} = h(x_{t+1}) + \varepsilon_{t+1},$$
$$E[\varepsilon_t \varepsilon_t^T] = R_t, \qquad (2)$$

where $\boldsymbol{x}$ is the vector of system states comprised of voltage magnitudes and phase angles at all buses except the slack bus. $\boldsymbol{F}$ represents the state transition matrix, $\boldsymbol{b}$ is state trajectory vector, and $\boldsymbol{\omega}$ is the Gaussian noise vector with zero mean, and covariance matrix $\boldsymbol{O}$. $\boldsymbol{h(x)}$ and $\boldsymbol{m}$, are vectors of nonlinear measurement functions and measurement data, respectively. $\boldsymbol{\varepsilon}$ is the measurement noise assuming normal distribution with zero mean, and $\boldsymbol{R}$ is the measurement error covariance matrix.

In order to predict the estimation value, model of the system should be identified. In this work $\boldsymbol{F}$ and $\boldsymbol{b}$ are described as follows based on the exponential smoothing technique. Utilizing extended Kalman filter (EKF) the predicted values can be updated using the next set of measurements at the time instant *t + 1*. The updated state through EKF can be written as:

$$\begin{aligned} \hat{x}_{t+1} &= \tilde{x}_{t+1} + K_{t+1}(m_{t+1} - h(\tilde{x}_{t+1})), \\ K_{t+1} &= \tilde{\rho}_{t+1} H_{t+1}^T [H_{t+1} \tilde{\rho}_{t+1} H_{t+1}^T + R]^{-1} \\ \rho_{t+1} &= \tilde{\rho}_{t+1} - K_{t+1} H_{t+1} \tilde{\rho}_{t+1} \end{aligned} \qquad (3)$$

where $\hat{\mathbf{x}}$, $\tilde{\boldsymbol{x}}$, $\boldsymbol{K}$, and $\boldsymbol{H}$ are estimated state, predicted state, Kalman gain and jacobian matrix, respectively. $\boldsymbol{\rho}$ and $\tilde{\boldsymbol{\rho}}$ are error covariance matrices for estimated and predicted values, respectively. For simplicity $\boldsymbol{O}$ is assumed to be constant.

A. Bad Data Detection

Even under normal operating conditions the measurements may be corrupted by random errors. The process of detecting exceptional errors is called BDD. Traditionally BDD tries to detect measurements errors using the statistical properties of the weighted measurement residual. Generally, the presence of bad data is determined if

$$r_i^N = \frac{|r_i|}{\sigma_{ii}} \qquad (4)$$

where $\boldsymbol{r_i^N}$ is the largest normalized residual (LNR), $\boldsymbol{\sigma_{ii}}$ is the standard deviation of the i^{th} component of the residual vector and $\boldsymbol{\chi}$ is the threshold [25].

It should be noted that measurement redundancy is a key issue in the performance of BDD which means it is necessary to have more measurements than the minimum number required for system observability. However, existing measurement configurations may not always yield such desired level of redundancy which makes the BDD impractical.

B. False Data Injection Attack

In false data injection (FDI) attacks, the adversary who has the knowledge of the network configuration can inject some of the meter readings from SCADA and manipulate the state variables arbitrarily. This type of malicious attacks can effectively bypass the existing BDD technique.

The general rule for a hidden attack is that the attacker must alter the data so that the measurements can plausibly correspond to the physical properties of the system. The main idea of FDI attack is to add a nonzero attack vector a to the original measurements vector m which results in a false estimation ^*x* + *c*, where c is the error added to the original estimation. Considering the measurement residual, a necessary condition to hide an attack can be derived as follows:

$$\begin{aligned} r_a &= \|m_a - H\hat{x}_a\| = \|m + a - H(\hat{x} + c)\| \\ &= \|m - H\hat{x} + (a - Hc)\| = \|m - H\hat{x}\| \end{aligned} \qquad (5)$$

The above equality constraint results in $\boldsymbol{a - Hc.}$ A structured sparse attack like $\boldsymbol{a = Hc}$ will result in the same residual and will not be detected by BDD. In this case, the system operator would mistake $\boldsymbol{\hat{x} + c}$ for a valid estimate. Fig. 1 shows a possible cyber-attack on an energy control center.

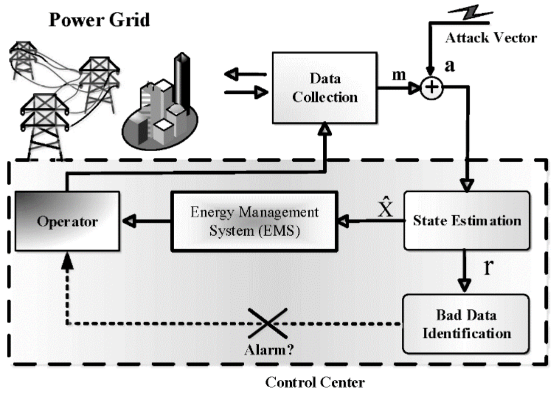

Figure 1. Energy Management System under cyber-attack, a: attack vector, m: measurement, r: measurement residual, x^: estimated state.

<u>*Definition*</u>: The sparse attack vector $\boldsymbol{a} = [a_1,\ldots, a_m]^T$ is called false data injection attack if and only if it satisfies the relation $\boldsymbol{a} = \boldsymbol{Hc}$, where $\boldsymbol{c} = [c_1,\ldots, c_n]^T$ is an arbitrary nonzero vector [3].

Imagine that the attacker wants to adjust the estimated value for $\mathbf{v}_j$ to $\mathbf{v}_j^a$, the following equation must be solved in order to find the voltage magnitude which will yield the desired power flow:

$$P_{ij} = V_i^2 g_{ij} - V_i V_j^a \left(g_{ij} \cos\theta_{ij} - b_{ij} \sin\theta_{ij}\right) \qquad (6)$$

where $\boldsymbol{g_{ij}}$ and $\boldsymbol{b_{ij}}$ represent line admittance parameters, and $\boldsymbol{\theta_{ij} = \theta_i - \theta_j}$. Since power flow and power injection are functions of voltage magnitudes and phase angles, the value of other measurements can be calculated considering the relationship between power flow and power injection. Also, the attacker must change all the measurements which are functions of $\boldsymbol{v_j}$.

C. Markov-Chain Formulation

Consider a physical system that has k possible states and at any given time, the system is in one of its k states. Defining a set of states as $\boldsymbol{C_i}$, a stochastic process which fulfils the following properties is called an l^{th} order Markov-chain:

$$\begin{aligned} &\Pr(C_{t+1} = s_i | C_t = s_1, \ldots, C_0 = s_k) = \\ &\Pr(C_{t+1} = s_i | C_t = s_1, \ldots, C_{t-l} = s_l) \end{aligned} \qquad (7)$$

where $\boldsymbol{Pr}$ refers to probability function and $\boldsymbol{t}$ represent the time. In this process the probability of getting into the next state depends upon the $\boldsymbol{l}$ previous states. To define a Markov model, the following probabilities have to be specified: the transition probability matrix $\boldsymbol{TP} = [\boldsymbol{tp_{ij}}]_{\boldsymbol{k\times k}}$ and initial probabilities $\boldsymbol{\pi_i} = \boldsymbol{Pr}(\boldsymbol{C_0} = \boldsymbol{s_i})$ where

$$\mathrm{tp_{ij}} = \Pr(C_{t+1} = s_i | C_t = s_i), \qquad i, j \in 1,2, \ldots k \qquad (8)$$

With $\sum_{j=1}^{k} \mathrm{tp_{ij}} = 1$. The following represents the Markov chain model:

$$\Pr(C_{t+1} = s_i | C_t = s_1, \ldots, C_{t-l} = s_l) = \sum_{j=1}^{k} \pi_\mathrm{i}\, \mathrm{tp_{ij}} \qquad (9)$$

1) Detection of potential attack

The proposed parallel DSE using EKF calculates the state of the system using the equations described in Section II. The Euclidean distance of the historical data and estimation of the trusted buses are calculated. The Euclidean method compares the difference between the two sets of data (x_1; x_2) based on the distance metric as given in (10):

$$ED(x_1, x_2) = \sqrt{(x_{1,1} - x_{2,1})^2 + \cdots + (x_{1,n} - x_{2,n})^2} \qquad (10)$$

If the difference is larger than a pre-computed threshold, the detector triggers an alarm. However, to avoid false alarms due to measurement or system errors, the threshold was set to filter 99.9% of noise. Also, in case of the load change, the change in voltage magnitude or phase angle can be predicted, so that the model parameters can be adjusted to reflect the change in the voltage due to the load change.

III. GPU Architecture and Programming Interface

The application of parallel processing in power system analysis is motivated by the desire for faster computation and the structure of the problems. The GPU is specially designed to address mathematically expensive data-parallel problems using CUDA which was the first general-purpose programming model for the GPU hardware [26]. The programmer divides work into threads, threads into thread blocks, and thread blocks into grids. The actual execution of a thread is performed by the abstracted CUDA cores which are a number of single precision floating point units. There is a two-level hierarchy in each thread named, *blockId* and *threadId*. The top level is a two dimensional array of blocks which is organized as a grid. All blocks in a grid have the same dimensions and share the same *blockId* values.

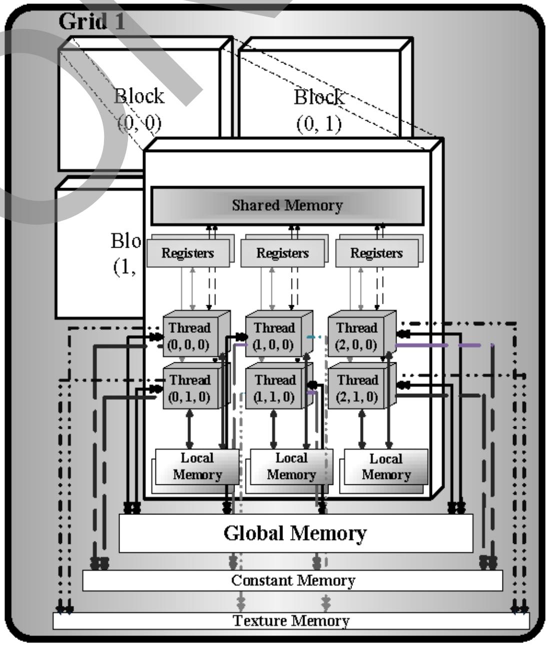

Figure 2. CUDA memory hierarchy and thread organization for data-parallell processing.

At the fundamental level, each group of the threads have their own set of local memory and a set of registers. Threads in a block have collective access to shared memory which is local to that block. All the threads also have access to a global memory which is the main memory of the GPU with the largest size and slowest access speed. Constant memory is a fast but read-only memory and texture memory is usually used for graphics rendering applications. Finally, the GPU also has access to the host computer's main memory, but not direct access [26]. Fig. 2 shows the memory hierarchy in a grid of four blocks described above. In this work, the C-run-time library and the Win32 API was used to have a full control on the synchronization of GPU data-transfer. CUDA version 5.0 with compute capability 2.0 is used for programming. Fig. 3 shows the inside architecture of Tesla$_{TM}$ S2050 computing system. This device contains 16 streaming multiprocessors (SMs), each with 32 streaming processors (SPs), an instruction unit, and on-chip memory.

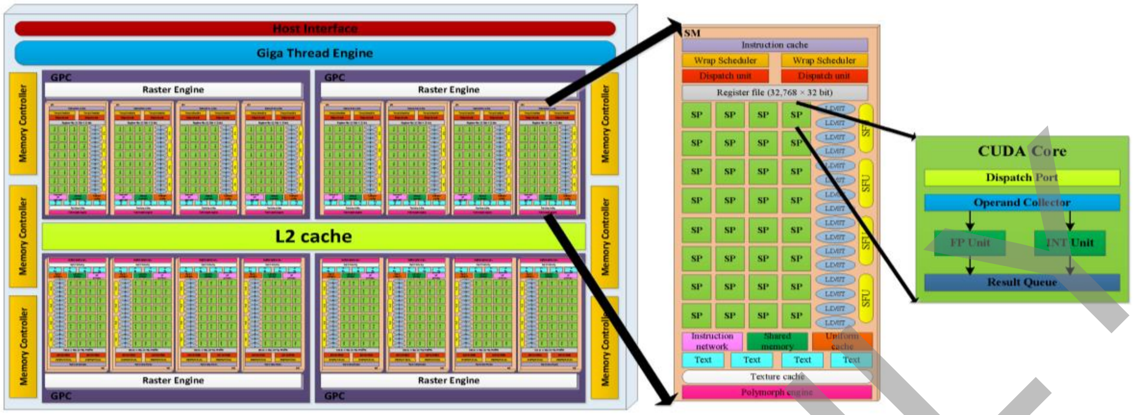

Figure 3. Tesla^{TM} S2050 computing system architecture.

A. *Implementation of Robust DSE against FDI on GPU*

The proposed robust DSE combines several aspects of parallelism to utilize the full capability of the GPUs as efficiently as possible. Initializations are done on the CPU. After that all of the data are transferred to the GPU for executing the robust DSE algorithm. In the first step, the traditional serial algorithm is converted into smaller independent tasks which results in task parallelism to be solved in parallel. All of the independent tasks in the three main steps of EKF are calculated in parallel to accelerate the algorithm. $\tilde{\boldsymbol{x}}$, $\boldsymbol{\rho}$ and $\tilde{\boldsymbol{\rho}}$ can be calculated simultaneously.

In order to take advantage of the single instruction multiple data (SIMD) based architecture of the GPUs for basic computations data parallelism is used for matrix-vector and matrix-matrix products. By assigning each independent *for* loop to individual threads, the tasks can be executed in parallel by converting into a kernel. In the robust DSE algorithm, several tasks are composed of matrix-matrix and matrix-vector product or summations which can be assigned to an individual kernel to run in parallel. Each kernel is responsible for the calculation of that specific task. As the number of independent threads is a lot more than the CPU cores, this type of parallelization is not possible on the CPU. Sparse matrix-vector multiplication and sparse triangular solve is used for GPU implementation using cuSPARSE library [27].

IV. SIMULATION ANALYSIS

To explore the efficiency of the GPU based robust DSE against FDI, IEEE 118-bus system were implemented on the GPU for simulation studies. To demonstrate the performance of the proposed method in terms of speed-up, the above test system were used to perform simulations on Tesla^{TM}S2050 GPU server from NVIDIA$^{®}$ with 4 Fermi GPUs, and 448 cores in each GPU. The CPU is the quad-core Intelr Xeon^{TM} E5-2620 with 2.0 GHz core clock and 32 GB memory, running 64-bit Windows 7$^{®}$ operating system. For accuracy analysis estimated states are verified using power flow analysis by PSS/E$^{®}$.

A. *Performance Evaluation*

In order to evaluate the accuracy of the proposed method, the results of the state estimation under normal operating conditions are plotted in Fig. 4 and Fig. 5. As there is no attack in the system, the results of state estimation are close enough to PSS/E$^{®}$ (real states).

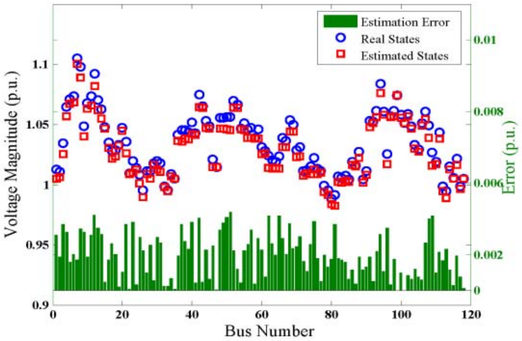

Figure 4. Voltage magnitude under normal operating condition.

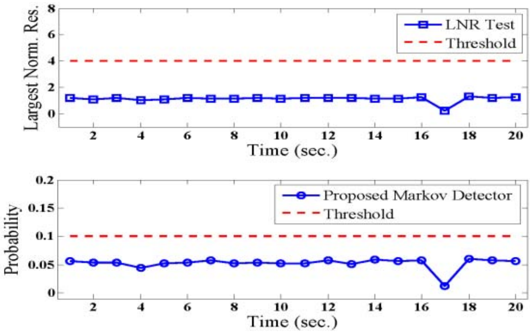

Figure 5. Detector output along with threshold under normal operating condition.

It is also shown in Fig. 5 that both LNR and proposed Markov detector test were result in lower values than the threshold indicating that there was no attack in the system. The small differences compared to PSS/E® results are justifiable considering the fact that the order of block execution in each GPU grid is undefined in kernel definition. Therefore, it leads to slightly different results if different CUDA blocks perform calculations on overlapping portions of data. The same experiment is performed for all case studies, however only results of IEEE-118 bus system, are plotted for brevity.

B. Attack Detection Analysis

In the second scenario, the proposed approach was evaluated for FDI attack. The goal of the attack was to change the power injection at bus 22 by influencing the estimated values for the state variables at this bus in the IEEE 118-bus system shown in Fig. 6. For this attack to remain hidden other measurements have to be changed as well. In order to satisfy (5) and (6), power injections at buses 20 and 23 need to be changed. Also, the power flows on the 21-22 and 22-23 connecting lines need to be adjusted as well which will change the power flow on line 20-21. As a result the estimated value for bus 21 should also change to keep the attack hidden.

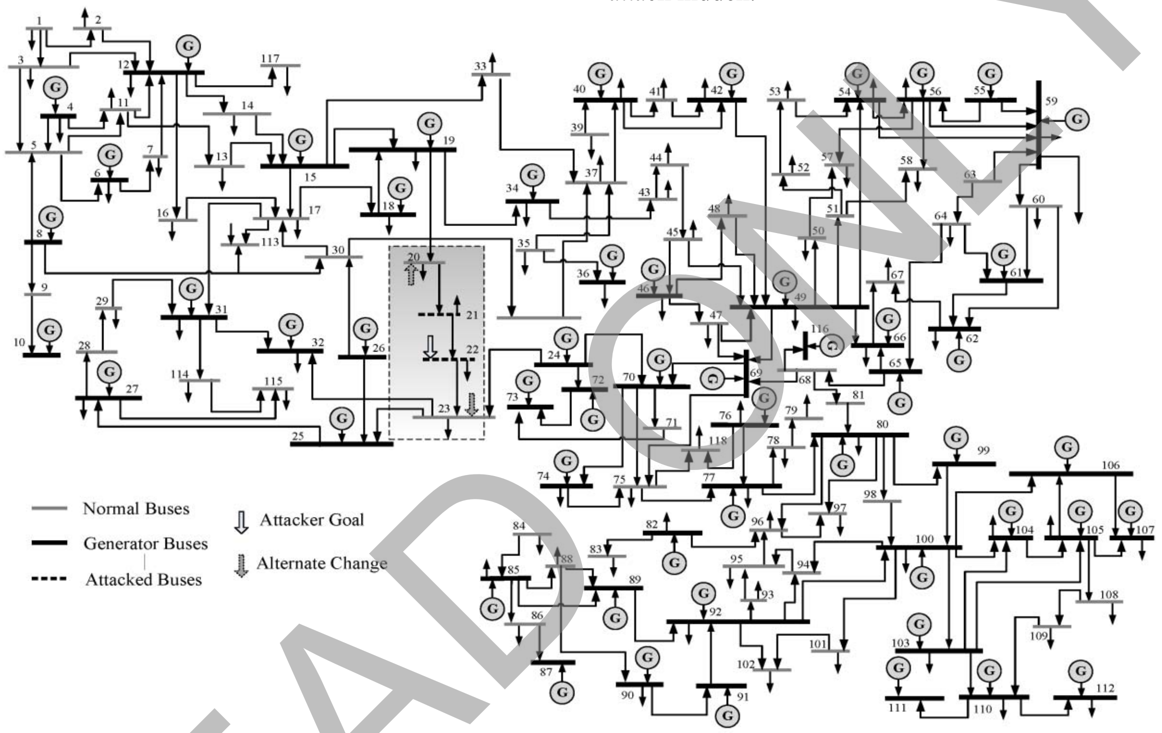

Figure 6. IEEE 118-bus test power system.

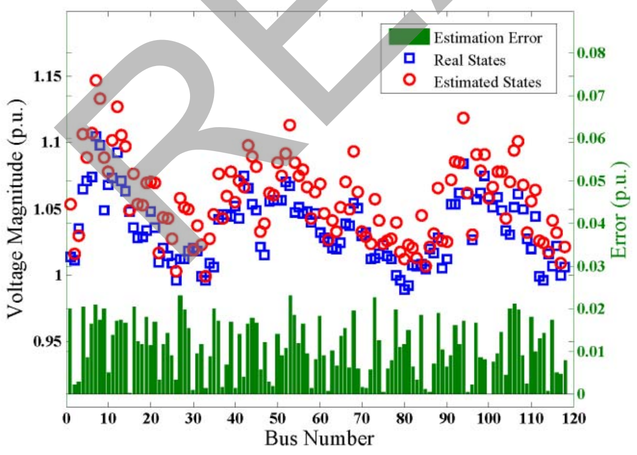

Figure 7. Voltage magnitude under FDI attack.

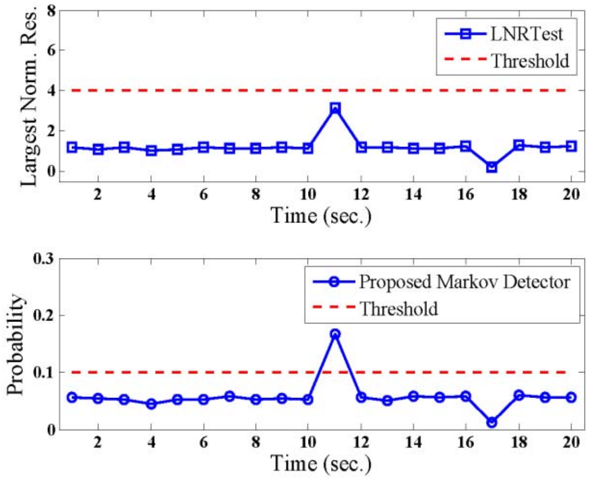

Figure 8. Detector output along with threshold under FDI attack.

Fig. 7 shows the behavior of the LNR and proposed FDI test under the cyber-attack. It is clear from these results that the estimation does not match with the measured values. During this attack, the LNR detector resulted in values below threshold and thus it was not able to detect the attack in the system as shown in Fig. 8. However, in the same setup, the proposed Markov detector exceeds the threshold; hence, the FDI attack can be detected. The same experiment is performed for all case studies resulted in similar results, providing the effectiveness of the proposed approach.

V. Conclusion

In this paper, a robust parallel dynamic state estimation approach utilizing graphic processing units and extended Kalman filter was presented. The proposed approach can detect false data injection attack using trusted set of measurements which were secured using optimized PMU installation. Considering the stochastic nature of the power system, using Markov chain theory and history of the system's dynamic behaviour a Markov model was proposed to check the accuracy of the estimation results using the Euclidean distance metric. Other type of cyber-attack which falls under FDI attack category can be identified using proposed methods. Simulation results on IEEE-118 bust system verify the accuracy of the proposed method both under normal operating condition and under false data injection attack. Increasing or decreasing the system size will not affect the efficiency and accuracy of the proposed method. Moreover, using large case study along with parallel implementation on GPUs shows the speed and applicability of the proposed approach for real-time large-scale power systems.

References

[1] T. Vollmer, M. Manic, "Cyber-physical system security with deceptive virtual hosts for industrial control networks", IEEE Trans. in Industrial Informatics, vol. 10, no. 2, pp. 1337-1347, May 2014.

[2] A. R. Metke and R. L. Ekl, "Security techn ology for smart grid networks", IEEE Trans. on Smart Grid, vol. 1, no. 1, pp. 99-107, Jun. 2010.

[3] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids", Proc. of ACM Conf. on Comp. and Comm. Sec., pp. 21-32, Nov. 2009.

[4] H. Xiao, W. Zidong, L. Yang , D.H. Zhou, "Least-squares fault detection and diagnosis for networked sensing systems using a direct state estimation approach", IEEE Trans. in Industrial Informatics, vol. 9, no. 3, pp. 1670-1679, Aug. 2013.

[5] O. Vukovi´c, G. D´an, "Security of fully distributed power system state estimation: detection and mitigation of data integrity attacks", IEEE Trans. on Sel. Are. in Comm., vol. 32, no. 7, pp. 1500-1508, Jul. 2014.

[6] E. Ghahremani, I. Kamwa, "Dynamic state estimation in power system by applying the extended kalman filter with unknown inputs to phasor measurements", Proc. of Environmental Sci., vol. 11, pp. 655-661, 2011.

[7] H. Karimipour, V. Dinavahi, "Parallel relaxation-based joint dynamic state estimation of large-scale power systems", IET Gen., Tran. & Dist., vol. 10, no. 2, pp. 452-459, 2 4 2016.

[8] A. Abur, "A bad data identification method for linear programming state estimation", IEEE Trans. on Power Syst., vo1. 5, no. 3, pp. 894-900, Aug. 1990.

[9] A. Abur and A. G. Expoosito, "Bad data identification when using ampere measurements", IEEE Trans. on Power Syst., vol. 12, no. 2, May 1997.

[10] L. Milli, T. V. Cutsem, and M. R. Pavella, "Bad data identification methods in power system state estimation", IEEE Trans. on Power App. and Syst., vol. 103, no. 11, pp. 3037-3049, Nov. 1985.

[11] A. Monticelli, F. F. Wu, and M. Y. Multiple, "Bad data identification for state estimation by combinatorial optimization", IEEE Trans. on Power Del., vol. 1, no. 3, pp. 361-369, July 1986.

[12] E. N. Asada, A. V. Garcia, and R. Romero, "Identifying multiple interacting bad data in power system state estimation", Proc. of IEEE PES, pp. 571-577, Jun. 2005.

[13] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems", Proc. of ACM Conf. on Dec. and Cont., pp. 5991-5998, Dec. 2010.

[14] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, P. Shengyi, U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information", IEEE Trans. on Smart Grid, vol. 4, no. 1, pp. 235-244, March 2013.

[15] S. Zonouz, K. M. Rogers, R. Berthier and T.J. Overbye, "SCPSE: security-oriented cyber-physical state estimation for power grid critical infrastructures", IEEE Trans. on Smart Grid, vol. 3, no. 4, pp. 1790- 1799, Dec. 2012.

[16] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, A. Tajer, "Coordinated data-injection attack and detection in the smart grid: a detailed look at enriching detection solutions", IEEE Signal Process. Mag., vol. 29, no. 5, pp. 106115, Sep. 2012.

[17] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling", IEEE Trans. on Industrial Informatics, vol. 11, no. 1, pp. 104-111, Feb. 2015.

[18] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids", IEEE Trans. on Smart Grid, vol. 2, pp. 326-333, Jun. 2011.

[19] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid", IEEE Trans. on Smart Grid, vol. 2, pp. 645-658, 2011.

[20] O. Vukovi´c, K. Cheong Sou, G. D´an, H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation", IEEE Trans. on Sel. Are. in Comm., vol. 30, no. 6, pp. 1108-1118, July 2012.

[21] S. Bi, Y. J. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation", IEEE Trans. on Sel. Are. in Comm., vol. 32, no. 7, pp. 14711485, Jul. 2014.

[22] S. P. Meyn, R. L. Tweedie, "Markov chain and stochastic stability", Springer-verlag., 2005.

[23] Z. Liu, X. Li, L. Wu, S. Zhou, K. Liu, "GPU-accelerated parallel co-evolutionary algorithm for parameters identification and temperature monitoring in permanent magnet synchronous machines", IEEE Trans. in Industrial Informatics, Apr. 2015.

[24] H. Karimipour, V. Dinavahi, "Parallel Domain-Decomposition-Based Distributed State Estimation for Large-Scale Power Systems", IEEE Tran. on Ind.App., vol. 52, no. 2, pp. 1265-1269, April 2016.

[25] A. Abur, A. G´omez-Exp´osito, "Power system state estimation theory and implementation", Marcel Dekker, Inc., 2004.

[26] NVIDIA, "NVIDIA Tesla: a unified graphics and computing architecture", NVIDIA CUDA C Programming Guide 4.0., 2013.

[27] NVIDIA, "cuSPARSE library", NVIDIA Developer, Feb. 2013.