Distributed Attack-Resilient Grid State Estimation Algorithm Using Optimal Filter and Graph Theory

Md Masud Rana[1], Ahmed Abdelhadi[1], and Rui Bo[2]
[1]Department of Engineering Technology, University of Houston, USA
[2] Dept. of ECE, Missouri University of Science and Technology, USA
Email: mrana928@yahoo.com

***Abstract*—Smart grid is built by the combination of electric and information technologies and achieves the two-way interaction between power utilization and power generation. Unfortunately, new security threats appears together with the cyber-physical communication systems. In order to properly monitoring the power network, the cyber attack detection and state estimation is required to identify attack and states. This paper considers the problem of robust state estimation in smart grid and suggests a technique for the distributed state estimation in power networks. Firstly, the distribution power system incorporating multiple synchronous generators are modelled as a state-space framework where attack occurs in measurements. Basically, the false data injection attacks can interfere with state estimation by tampering with sensor measurements. Using mean squared error principle, the distributed dynamic state estimation algorithm is designed where local and neighbouring gains are obtained using optimal filter and graph theory. Extensive simulation results show that the proposed approach can able to estimate the system state within a short period of time.**

***Index Terms*—Cyber attacks, distributed dynamic state estimation, false data injection attack, graph theory, optimal filter.**

I. Introduction

The conventional electric grid is undergoing a significant transformation in its power generation, transmission and distribution units [1], [2]. Interestingly, the use of advanced information and communication technology, sensors, and actuators are able to achieve these imperative milestones [3], [4], [5]. Basically, the smart grid enables two-way communications between the utility operator and consumer, so it is more vulnerable to cyber attacks. Therefore, significant technical challenges arise for wide area monitoring, planning, and controlling the smart grid network [6], [7]. To fulfil these challenges and meet customer satisfaction, the utility operator is monitoring the operational characteristics of power networks through a process called state estimation, which performs the task by filtering and fusing various sensor measurements. The attacks cause losses measurements between the grid and the energy management system (EMS) and can provide misleading information to the EMS. Generally speaking, the transmission of massive measurements to the centralised control center is expensive and infeasible, so the distributed estimation is gaining more popular. In distributed estimation, each agent in the power network is locally process and exchange information to recover system states [8], [9]. Therefore, the distributed state estimation considering cyber attack is an important area of research, and this paper deals with this emerging security issue.

From filtering point of view, the Kalman filter (KF) extended KF (EKF), H-infinity EKF, unscented KF and cubature KF algorithms are used for power system state estimations [10], [11], [12]. Moreover, the forecasted-aided KF algorithm considering cyber attacks is explored in [13] where Euclidean distance metric is used to detect cyber attack. The observer based anomaly detection scheme is presented in [14]. In addition, the wavelet transform-based mixed Kalman particle filter based dynamic state estimation algorithm under FDIA is presented in [15], [16]. The scenario based unsupervised learning algorithm for cyber physical power system is developed in [17]. All the aforementioned algorithms are designed for centralised state estimation which requires all measurements and prone to vulnerable and single point failure. Due to deregulation of power systems, the distributed state estimation is gaining more attention in industrial and research communities.

In order to estimate the discrete time-varying cyber physical system states, an iterative finite impulse response filter is designed [18]. It can effectively estimate the hidden system states without using any specific initialization scheme. For improvement of estimation accuracy, the robust type chandrasekhar-based maximum correntropy KF algorithm for cyber physical system is proposed in [19]. The idea is extended in [20], where attack-resilient remote state estimation scheme is proposed and verified. The attackers are manipulated the sensor measurements and fusion center combines them for state estimations. Using residual prewhitening method, the cyber attack detection method is proposed in [21]. Technically, when the covariance matrix of the residual error is not full-rank, this method is used to solve the cyber attack detection and estimation problem.

Furthermore, the resource constraint based optimal state estimation algorithm for cyber physical system is presented in [22]. Besides, the mixed mixed integer linear programming based cyber attack protection scheme for power system is developed in [23]. The computational complexity is very high and requires significant amount of time as it is a bilevel optimization problem. In order to guarantee cyber and operational security, a command authentication approach is proposed to detect intrusion [24], [25]. Distributed state estimations face real environments where cyber attacks, and noisy measurements are present [26]. Differentiated from prior

978-1-7281-8602-3/20/$31.00 ©2020 IEEE

literature, this study is the first of its kind to solve distributed state estimation problem for smart grid under cyber attacks using the optimal filter theory and Bayesian learning process.

II. Distribution Power Systems State-Space Representation

Fig. 1 shows the typical synchronous generators and loads which are connected to the 8-bus distribution lines [27], [28], [29]. Basically, the nth-synchronous generators can be

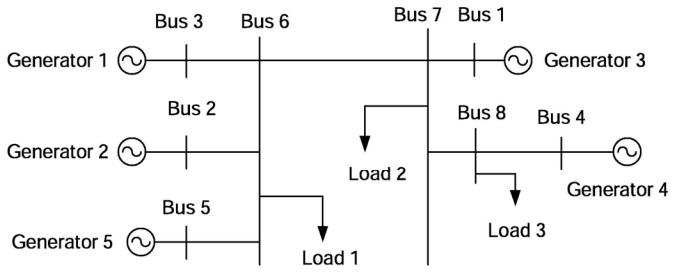

Fig. 1: Distributed power network incorporating synchronous generators.

represented by the following third order differential equations as follows [28], [29], [30]:

$$\Delta\dot{\delta_n} = \Delta\omega_n. \tag{1}$$

$$\Delta\dot{\omega}_n = -\frac{D_n}{H_n}\Delta\omega_n - \frac{\Delta P_{en}}{H_n}. \tag{2}$$

$$\Delta\dot{E'_{qn}} = -\frac{\Delta E'_{qn}}{T'_{don}} + \frac{\Delta E_{fn}}{T'_{don}} + \frac{X_{dn}}{T'_{don}}\Delta I_{dn} - \frac{X'_{dn}}{T'_{don}}\Delta I_{dn}. \tag{3}$$

Here, δ_n is the rotor angle, ω_n is the rotor speed, H_n is the inertia constant, D_n is the damping constant, P_e is the active power delivered at the terminal, E'_{qn} is the quadrature-axis transient voltage, E_{fn} is the exciter output voltage, T'_{don} is the direct-axis open-circuit transient time constant, X_{dn} is the direct-axis synchronous reactance, X'_{dn} is the direct-axis transient reactance, and I_{dn} is the direct-axis current [27].

Generally, an automatic voltage regulator (AVR) is used to control the excitation current which leads to control the terminal voltage [28], [31]. A second-order transfer function is used to represent the AVR as follows [28]:

$$\Delta E_{fn} = b_{0n}z_{1n} + b_{1n}z_{2n}. \tag{4}$$

$$\dot{z_{1n}} = z_{2n}. \tag{5}$$

$$\dot{z_{2n}} = -c_{1n}z_{2n} - c_{0n}z_{1n} + \Delta v_n. \tag{6}$$

Here, z_{1n} and z_{2n} are the AVR internal states, b_{0n} and b_{1n} are transfer function coefficients of the AVR, c_{0n} and c_{1n} are the transfer function coefficients of the excitation system and Δv_n is the control input signal.

Considering N generators in the power network, the d-axis current I_{di} and electrical power P_{ei} are represented as [31]:

$$I_{dn} = \sum_{m=1}^{N} \Delta E'_{qn}[B_{nm}\ cos(\delta_n - \delta_m) - G_{nm}\ sin(\delta_n - \delta_m)]. \tag{7}$$

$$P_{en} = \Delta E'_{qn}\sum_{m=1}^{N}[B_{nm}\ sin(\delta_n - \delta_m) + G_{nm}\ cos(\delta_n - \delta_m)]\Delta E'_{qm}. \tag{8}$$

Here, $n, m \in \{1, \cdots, N\}$, G_{nm} and B_{nm} are the real and imaginary part of the admittance $\mathbf{Y} \in \mathbb{R}^{N\times N}$, which is described in the Appendix A.

After linearizing (7) and (8), ΔP_{en} and ΔI_{dn} are written as follows [28], [32], [33]:

$$\Delta P_{en} = \begin{bmatrix} \frac{\partial P_{en}}{\partial \delta} & \frac{\partial P_{en}}{\partial E'_q} \end{bmatrix} [\Delta\delta\ \Delta E'_q]'. \tag{9}$$

$$\Delta I_{dn} = \begin{bmatrix} \frac{\partial I_{dn}}{\partial \delta} & \frac{\partial I_{dn}}{\partial E'_q} \end{bmatrix} [\Delta\delta\ \Delta E'_q]'. \tag{10}$$

Here, $\Delta E'_q$ and $\Delta\delta$ are the transient voltage deviations and rotor angle deviations. By combining (1)-(6) and (9)-(10), it can be written as follows:

$$\dot{\mathbf{s}}_n = \mathbf{A}_n\mathbf{s}_n + \mathbf{B}_n u_n + \sum_{m\in N_n} \mathbf{A}_{nm}\mathbf{s}_m. \tag{11}$$

Here, the generator state $\mathbf{s}_n = [\Delta\delta_n\ \Delta\omega_n\ \Delta E'_{qn}\ z_{2n}\ z_{1n}]'$, the control input signal $u_n = \Delta v_n$, N_n indicates a set of connected generators, the system matrices $\mathbf{A}_n \in \mathbb{R}^{5\times5}$, $\mathbf{B}_n \in \mathbb{R}^{5\times1}$ and $\mathbf{A}_{nm} \in \mathbb{R}^{5\times5}$ are: $\mathbf{A}_n = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ -\frac{1}{H_n}\frac{\partial P_{en}}{\partial \delta n} & -\frac{D_n}{H_n} & -\frac{1}{H_n}\frac{\partial P_{en}}{\partial E'_{qn}} & 0 & 0 \\ X_n\frac{\partial I_{dn}}{\partial \delta_n} & 0 & -\frac{1}{T'_{don}} + X_n\frac{\partial I_{dn}}{\partial E'_{qn}} & \frac{b_{1n}}{T'_{don}} & \frac{b_{on}}{T'_{don}} \\ 0 & 0 & 0 & -c_{1n} & -c_{0n} \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$,

$\mathbf{A}_{nm} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ -\frac{1}{H_n}\frac{\partial P_{en}}{\partial \delta m} & 0 & -\frac{1}{H_n}\frac{\partial P_{en}}{\partial E'_{qm}} & 0 & 0 \\ X_n\frac{\partial I_{dn}}{\partial \delta_m} & 0 & -\frac{1}{T'_{don}} + X_n\frac{\partial I_{dn}}{\partial E'_{qm}} & \frac{b_{1n}}{T'_{dom}} & \frac{b_{on}}{T'_{dom}} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$,

$\mathbf{B}_n = [0\ 0\ 0\ 1\ 0]'$ [28] and $X_n = \frac{X_{dn} - X'_{dn}}{T'_{don}}$.

The aforementioned system can be written in continuous-time form:

$$\dot{\mathbf{s}} = \mathbf{A}^c\mathbf{s} + \mathbf{B}^c\mathbf{u} + \mathbf{w}. \tag{12}$$

Here, $\mathbf{s} \in \mathbb{R}^{5N\times1}$, $\mathbf{u} \in \mathbb{R}^{N\times1}$, $\mathbf{w} \in \mathbb{R}^{5N\times1}$ is the process noise which can follow the Gaussian distribution incorporating zero mean and $\mathbf{Q}$ covariance, i.e., N($\mathbf{0}$, $\mathbf{Q}$), $\mathbf{A}^c \in \mathbb{R}^{5N\times5N}$ and $\mathbf{B}^c \in \mathbb{R}^{5N\times N}$ are given by: $\mathbf{A}^c = \begin{bmatrix} \mathbf{A}_1 & \mathbf{A}_{12} & \cdots \mathbf{A}_{1N} \\ \mathbf{A}_{21} & \mathbf{A}_2 & \cdots \mathbf{A}_{2N} \\ \vdots & \vdots & \vdots \\ \mathbf{A}_{N1} & \mathbf{A}_{N2} & \cdots \mathbf{A}_N \end{bmatrix}$

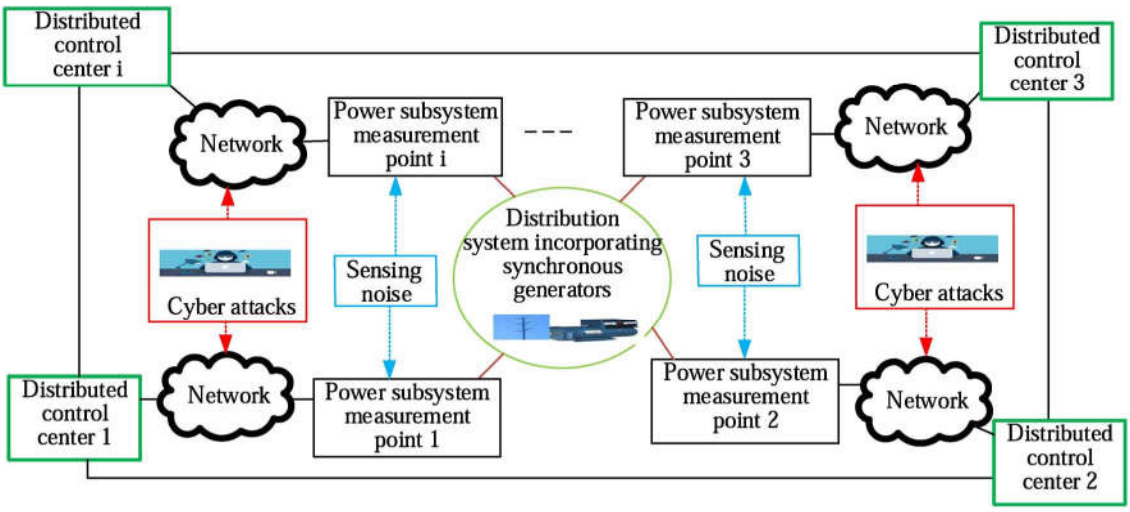

Fig. 2: Interconnected distribution power subsystems incorporating synchronous generators.

and $\mathbf{B}^c = diag(\mathbf{B}_1 \cdots \mathbf{B}_N)$. Now, it can be written as a discrete-time form as follows:

$$\mathbf{s}(t+1) = \mathbf{A}\mathbf{s}(t) + \mathbf{B}\mathbf{u}(t) + \mathbf{w}(t), \tag{13}$$

where $\mathbf{A} = \mathbf{I} + \mathbf{A}^c\Delta t$, Δt is the sampling time, and $\mathbf{B}_d = \mathbf{B}^c\Delta t$.

III. Measurement and Cyber Attack Frameworks

The distributed control centers are interconnected through communication links as shown in Fig. 2. In this figure, there are i-th distribution subsystems which are connected to the neighbours units [33]. These control centers can share information with their neighbours in a distributed way. The sensors are installed into subsystem units to obtain distributed measurements. These sensing information is telemetered to the control centres to estimate system states such as rotor angle. The measurements are obtained as follows:

$$\mathbf{z}_i(t) = \mathbf{C}_i\mathbf{s}(t) + \mathbf{v}_i(t). \tag{14}$$

Here, $\mathbf{z}_i(t) \in \mathbb{R}_i^p$ is the measurement, and $\mathbf{v}_i \backsim N(\mathbf{0}, \mathbf{R}_i)$ is the measurement noise, and $\mathbf{C}_i$ is the sensing matrix.

When the sensing information is transmitted to the control center, the attacker hack the communication network and manipulated measurements. There are different kind of attacks such as false data injection attack (FDIA) and replay attack [34]. For FDIA, the attacker is added intended information to the actual measurement over time, then report it to the control center for misleading. In later case, the adversary records the normal measurements over time [35]. During attack, the actual measurements are replaced to recoded one and thereby moving the system into an incorrect state [36]. Mathematically, when there is attack then the system measurement can be written:

$$\mathbf{z}_i^a(t) = \mathbf{C}_i\mathbf{s}(t) + \mathbf{v}_i(t) + \mathbf{a}_i(t). \tag{15}$$

Here, $\mathbf{a}_i(t)$ is the cyber attack. We consider that the attach vector $\mathbf{a}_i$ is a Gaussian distribution with mean $\mu_\mathbf{i}$ and covariance $\bar{\mathbf{R}}_i^a$, i.e., $\mathbf{a}_i \backsim N(\mu_\mathbf{i}, \bar{\mathbf{R}}_i^a)$ [37], [38]. It is assumed that the attack sequence is uncorrelated to each measurement. Let define the system model parameters $\phi_i = (\mu_\mathbf{i}, \hat{\mathbf{R}}_i)$, where $\hat{\mathbf{R}}_i = \mathbf{R}_i + \mathbf{R}_i^a$ is the combined covariance of noise and cyber attack. Based on this noisy and corrupted version of measurements, the proposed state estimation algorithm is developed in the following section.

IV. Proposed Distributed Smart Grid State Estimation Algorithm

The proposed distributed state estimation algorithm is obtained using the optimal filter and Bayesian learning approaches. Based on the interconnected structure in Fig. 2, the designed scheme is mathematically written as follows:

$$\hat{\mathbf{s}}_i(t+1) = \mathbf{A}\hat{\mathbf{s}}_i(t) + \mathbf{B}\mathbf{u}(t) + \mathbf{G}_i(t)[\mathbf{z}_i^a(t) - \mathbf{C}_i\hat{\mathbf{s}}(t)] + \mathbf{L}_i(t)\sum_{j\in N_i}[\hat{\mathbf{s}}^j(t) - \hat{\mathbf{s}}_i(t)]. \tag{16}$$

Here, $\hat{\mathbf{s}}_i(t+1)$ is the posterior estimated system state, $\hat{\mathbf{s}}_i(t)$ is the previous estimated state, $\mathbf{G}_i(t)$ and $\mathbf{L}_i(t)$ are the local and consensus gains which can minimise the residual error dynamic $\mathbf{z}_i^a(t) - \mathbf{C}_i\hat{\mathbf{s}}(t)$ and neighbouring estimation mismatch $\hat{\mathbf{s}}^j(t) - \hat{\mathbf{s}}_i(t)$ over time. Basically, the last term of the distributed scheme (16) is used for neighboring connections in Fig. 2, while the third term is included for self estimation unit. The following theorem is used to compute these gains for distributed smart grid state estimation.

Theorem 1: After defining the error $\boldsymbol{\eta}_i(t) = \mathbf{s}(t) - \hat{\mathbf{s}}_i(t)$ between the true and estimated system states and using the optimal filter as well as graph theory, the designed gains are obtained as follows:

$$\mathbf{G}_i(t) = [\mathbf{A}\mathbf{P}_i(t)\mathbf{C}_i' + \mathbf{L}_i(t)\sum_{r\in N_i}\{\mathbf{P}^{ri}(t) - \mathbf{P}_i(t)\}\mathbf{C}_i'][\mathbf{C}^i\mathbf{P}^i(k)\mathbf{C}^{'i} + \hat{\mathbf{R}}_i]^{-1}. \tag{17}$$

Using mean squared error principle, the estimation error covariance $\mathbf{P}_i(t+1) = E[\boldsymbol{\eta}_i(t+1)\boldsymbol{\eta}_i'(t+1)]$ is determined by:

$$\mathbf{P}_i(t+1) = \mathbf{A}\mathbf{P}_i(t)\mathbf{A}' - \mathbf{A}\mathbf{P}_i(t)\mathbf{C}_i'[\mathbf{C}_i\mathbf{P}_i(t)\mathbf{C}_i' + \hat{\mathbf{R}}_i]^{-1}\mathbf{C}_i\mathbf{P}_i(t)\mathbf{A}' + \mathbf{Q}. \quad (18)$$

Here, $\mathbf{P}_i(t)$ is the prior estimation error covariance [39]. Using the Bayesian learning formula, the covariance $\hat{\mathbf{R}}_i$ is computed as follows:

$$\hat{\mathbf{R}}_i = (\alpha_i\bar{\mathbf{R}}_i + \rho_i[diag(\hat{\mu}_i)]^2 - (\rho_i+1)[diag(\hat{\mu}_i)]^2 + [diag(\mathbf{z}_i^a - \mathbf{C}_i\hat{\mathbf{s}}_i)]^2)/(\alpha_i+1). \quad (19)$$

$$\hat{\mu}_i = (\rho_i\bar{\mu}_i + \mathbf{z}_i^a - \mathbf{C}_i\hat{\mathbf{s}}_i)/(\rho_i+1). \quad (20)$$

Here, $\bar{\mathbf{R}}_i$ and $\bar{\mu}_i^a$ are the initial values, α_i and ρ_i are the hyper-parameters.

For mathematical simplicity, we assume that neighbouring gain $\mathbf{L}_i(t) = \upsilon\mathbf{I}$, where υ is the designed gain coefficient. Under a steady state condition, it can be computed through the following convex optimization process:

$$\upsilon = \underset{\upsilon}{\text{argmax}} \begin{bmatrix} -\mathbf{I} & \boldsymbol{\Gamma} \\ \boldsymbol{\Gamma}' & -\mathbf{I} \end{bmatrix} < \mathbf{0}. \quad (21)$$

Here, $\boldsymbol{\Gamma} = \mathbf{I}_n \otimes \mathbf{A} - bdiag\{\mathbf{L}\mathbf{C}_i\} - \upsilon(\mathbf{L}_p \otimes \mathbf{I})$, and $\mathbf{L}_p$ is the the Laplacian operator which is obtained through the graph theory after combining all error dynamics in a compact form. The Proof is derived in [33], [40]. The symbol $\otimes$ indicates the Kronecker product. After computing gains and covariance, the estimation process (16) is run in an iterative way. The step by step procedure of the whole system is described in the simulation section.

V. Numerical Simulation Results and Analysis

To estimate the system state, the proposed algorithm is applied to the distribution power network as shown in Fig. 2. For simplicity, we assume that there are $i = 4$ interconnected distributed controllers as shown in Fig. 2. The simulation is conducted through MATLAB and YALMIP environments. The simulation parameters are described in [29]. Basically, the process and measurement noise covariances are followed by Gaussian distributions with covariances are $10^{-4}\mathbf{I}$ and $2{*}10^{-4}\mathbf{I}$, respectively. In addition, the sampling period is 0.02 seconds, and there are five synchronous generators connected to the 8-bus distribution network as shown in Fig. 1. The simulation is conducted considering FDIA.

First of all, it assumes that the attacker is added the FDIA into measurement during 0.1 to 0.5 seconds. In this case, the simulation results are illustrated in Figs. 3-4. Basically, Fig. 3 shows the generator 1 true rotor angle and it estimation result. This state is increasing order, and the proposed algorithm can properly estimate this state within 10 seconds. From 4, the actual rotor speed can estimate within 6 seconds. This is due to the fact that the proposed algorithm can find the suitable gains so the estimated states converge to the actual states within a short period of time. Note that

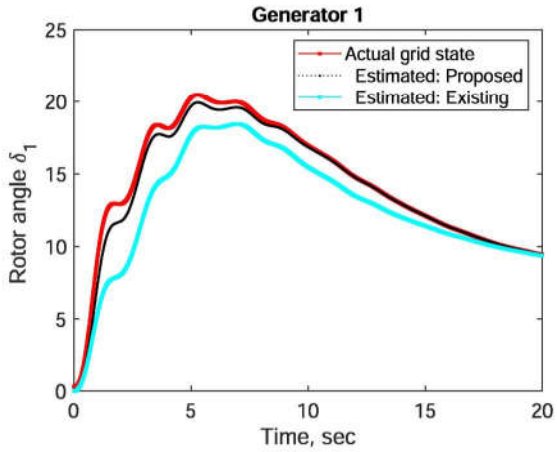

Fig. 3: Generator 1: Actual rotor angle and it estimation with FDIA.

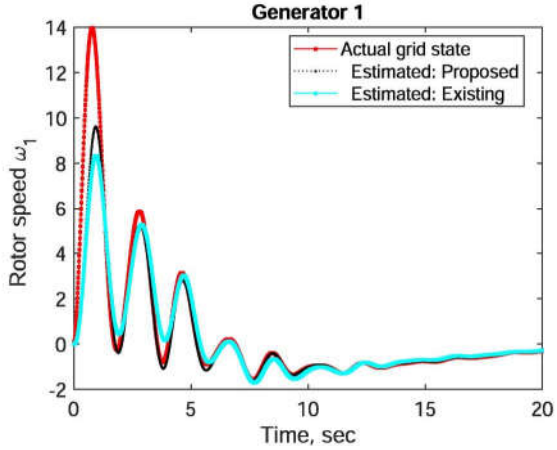

Fig. 4: Generator 1: Actual rotor speed and it estimation with FDIA.

VI. Conclusion and Future Work

State estimation is the key task for power system operation and maintain stability as well as observability. However, the smart grid infrastructure is prone to cyber threats. In order to protect the power network from cyber attacks, this paper proposes a distributed state estimation algorithm. Specifically, we have made three main contributions to enhance the cybersecurity and resiliency of smart grids. First, the 8-bus distribution grid incorporating synchronous generators are modelled as a state-space framework where measurement are obtained by a set of sensors. The measurement data is manipulated by cyber attacks such as FDIA. Second, we proposed an attack-resilient distributed state estimation algorithm based on the optimal filter and graph theory. Finally, simulation results show that the proposed algorithm can able to estimate system state within a short time. We will try to develop a data-drive distributed state estimation algorithm considering cyber attacks.

REFERENCES

[1] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. of the IEEE*, vol. 105, no. 7, pp. 1389–1407, 2017.

[2] M. M. Rana and L. Li, "An overview of distributed microgrid state estimation and control for smart grids," *Sensors*, vol. 15, no. 2, pp. 4302–4325, 2015.

[3] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, "Internet of things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions," *IEEE Access*, vol. 7, pp. 62 962–63 003, 2019.

[4] M. P. Coutinho, G. Lambert-Torres, L. B. da Silva, H. Martins, H. Lazarek, and J. C. Neto, "Anomaly detection in power system control center critical infrastructures using rough classification algorithm," in *Proc. Int. Con. Dig. Eco. Tech.*, 2009, pp. 733–738.

[5] M. Rana, "Architecture of the internet of energy network: An application to smart grid communications," *IEEE Access*, vol. 5, pp. 4704–4710, 2017.

[6] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proc. of the IEEE*, vol. 104, no. 5, pp. 1058–1070, 2016.

[7] M. Rana and L. Li, "Microgrid state estimation and control for smart grid and Internet of Things communication network," *Electronics Letters*, vol. 51, no. 2, pp. 149–151, 2015.

[8] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. Int. Conf. Smart Grid Comm.*, 2011, pp. 202–207.

[9] M. Rana, L. Li, and S. Su, "Distributed microgrid state estimation using smart grid communications," in *2015 IEEE PES Asia-Pacific Power and Energy Engineering Conference*, 2015, pp. 1–5.

[10] J. Zhao, L. Mili, and A. Abdelhadi, "Robust dynamic state estimator to outliers and cyber attacks," in *Power Ene. Soc. Gen. Meet.*, 2017, pp. 1–5.

[11] M. M. Rana, R. Bo, and H. Chen, "Estimating and controlling the renewable microgrid states using iot infrastructure," *Asian Journal of Control*, vol. 21, no. 4, pp. 2105–2113, 2019.

[12] Y. Wang, Y. Sun, and V. Dinavahi, "Robust forecasting-aided state estimation for power system against uncertainties," *IEEE Trans. Pow. Sys. to appera in 2020*.

[13] H. Karimipour and V. Dinavahi, "Robust massively parallel dynamic state estimation of power systems against cyber-attack," *IEEE Access*, vol. 6, pp. 2984–2995, 2017.

[14] G. Anagnostou, F. Boem, S. Kuenzel, B. C. Pal, and T. Parisini, "Observer-based anomaly detection of synchronous generators for power systems monitoring," *IEEE Trans. Pow. Sys.*, vol. 33, no. 4, pp. 4228–4237, 2018.

[15] B. Chen, H. Li, and B. Zhou, "Real-time identification of false data injection attacks: A novel dynamic-static parallel state estimation based mechanism," *IEEE Access*, vol. 7, pp. 95 812–95 824, 2019.

[16] M. M. Rana, L. Li, and S. W. Su, "Cyber attack protection and control of microgrids," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 2, pp. 602–609, 2017.

[17] S. Ahmed, Y. Lee, H. Seung-Ho, and I. Koo, "Unsupervised machine learningbased detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Trans. Inf. For. Sec.*, 2019.

[18] S. Zhao, Y. S. Shmaliy, C. K. Ahn, and L. Luo, "An improved iterative FIR state estimator and its applications," *IEEE Trans. Ind. Inf., to appear in 2020*.

[19] M. V. Kulikova, "Chandrasekhar-based maximum correntropy Kalman filtering with the adaptive kernel size selection," *IEEE Trans. Aut. Cont., to appear in 2020*.

[20] A. Chattopadhyay and U. Mitra, "Security against false data injection attack in cyber-physical systems," *IEEE Trans. Cont. Net. Syst., to appear in 2020*.

[21] Q. Jiang, H. Chen, L. Xie, and K. Wang, "Real-time detection of false data injection attack using residual prewhitening in smart grid network," in *Proc. Int. Conf. Smart Grid Comm.*, 2017, pp. 83–88.

[22] F. Li and Y. Tang, "False data injection attack for cyber-physical systems with resource constraint," *IEEE Trans. Cyb.*, vol. 50, no. 2, pp. 729–738, 2018.

[23] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, 2016.

[24] S. Meliopoulos, G. Cokkinides, R. Fan, L. Sun, and B. Cui, "Command authentication via faster than real time simulation," in *Pow. Energy Soc. Gen. Meet.*, 2016, pp. 1–5.

[25] U. A. Khan and A. M. Stanković, "Secure distributed estimation in cyber-physical systems," in *Proc. Int. Conf. Acou. Spe. Sig. Procs.*, 2013, pp. 5209–5213.

[26] M. M. Rana, L. Li, and S. W. Su, "An adaptive-then-combine dynamic state estimation considering renewable generations in smart grids," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3954–3961, 2016.

[27] E. Ghahremani and I. Kamwa, "Online state estimation of a synchronous generator using unscented Kalman filter from phasor measurements units," *IEEE Trans. Ene. Conv.*, vol. 26, no. 4, pp. 1099–1108, 2011.

[28] J. Liu, A. Gusrialdi, S. Hirche, and A. Monti, "Joint controller-communication topology design for distributed wide-area damping control of power systems," *IFAC Proc. Vol.*, vol. 44, no. 1, pp. 519–525, 2011.

[29] M. M. Rana, L. Li, S. W. Su, and B. J. Choi, "Modelling the interconnected synchronous generators and its state estimations," *IEEE Access*, vol. 6, pp. 36 198–36 207, 2018.

[30] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994, vol. 7.

[31] J. Machowski, J. Bialek, and J. Bumby, *Power system dynamics: stability and control*. John Wiley & Sons, 2011.

[32] A. Farraj, E. Hammad, and D. Kundur, "A distributed control paradigm for smart grid to address attacks on data integrity and availability," *IEEE Trans. Sig. Inf. Proc. Over Net.*, vol. 4, no. 1, pp. 70–81, 2017.

[33] M. M. Rana, B. Rui, and A. Ahmed, "Distributed grid state estimation under cyber attacks using optimal filter and Bayesian approach," *IEEE Systems Journal to Appear in 2020*.

[34] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[35] T. Huang, B. Satchidanandan, P. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Pow. Syst.*, vol. 33, no. 6, pp. 6816–6827, 2018.

[36] C. M. Ahmed, S. Adepu, and A. Mathur, "Limitations of state estimation based cyber attack detection schemes in industrial control systems," in *Proc. Smart City Secu. Priv. Workshop*, 2016, pp. 1–5.

[37] A. Minot, H. Sun, D. Nikovski, and J. Zhang, "Distributed estimation and detection of cyber-physical attacks in power systems," in *Proc. Int. Conf. Comm. Wor.*, 2019, pp. 1–6.

[38] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Trans. Inf. Foren. Sec.*, vol. 13, no. 8, pp. 2015–2030, 2018.

[39] M. M. Rana, "Least mean square fourth based microgrid state estimation algorithm using the internet of things technology," *PloS one*, vol. 12, no. 5, 2017.

[40] M. M. Rana, L. Li, S. W. Su, and W. Xiang, "Consensus-based smart grid state estimation algorithm," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3368–3375, 2017.