Detection of False Data Injection Attack on Load Frequency Control in Distributed Power Systems

Alireza Abbaspour
Department of Electrical Engineering
Florida International University
Miam, FL, USA
alireza.abaspour@gmail.com

Arman Sargolzaei
Department of Electrical Engineering
Florida Polytechnic University,
Lakeland, FL, USA

Kang Yen
Department of Electrical Engineering
Florida International University
Miam, FL, USA

***Abstract*—The False Data Injection (FDI) attack on Load Frequency Control (LFC) caused by the adversary can destabilize the power system. This could cause potential economic and life damages. Therefore, the real-time detection of FDI attacks is necessary and essential to compensate negative effects of such attacks. This paper presents a neural network-based detection (NND) approach to estimate and detect the FDI attacks injected to sensing loop (SL) of the system. A two-area distributed power system is considered as our case study to demonstrate the effectiveness of NND strategy. The simulation results clearly show that the FDI attack can be detected and estimated in real-time with sufficient accuracy.**

***Index Terms*—Fault detection; False Data Injection; Neural Network; Load Frequency Control**

I. Introduction

False data injection (FDI) attack is one of the major potential treats to the power system that can destabilize the power distribution and may lead serious financial loss and safety issues [1]–[5]. False data whether produced by a faulty component, e.g., sensors and actuators, or FDI in a malicious attempt, may deteriorate the control performance of the system [6]–[8]. Therefore, the resiliency of the power control systems against faults, failures and attacks is an attractive topic among researchers in the field of power distribution [9]–[16].

In a smart grid, the role of the LFC is to maintain the frequency and power interchanges within the desired values at the grid [17]. A resilient LFC system will help to improve the reliability of the power grid system. In order to develop an LFC system resilient to FDI attack, in the first step, a detection algorithm should be designed and implemented on the LFC system. In the next step, by using the information obtained from the detection algorithm, a control system will be devised to compensate for the occurred fault [18], [19]. The detection algorithm should be capable of finding out where the intruder attacked and measuring the amount of the inserted false data [20]. Various approaches have been used to detect FDI in the literature [20]–[24]. A Kalman filter based intrusion detection design is presented on [20]. In their design, Kalman filter was used for the grid state estimation, and a χ^2 is used to detect anomalies between the estimated and the measured data and if an intrusion happens, the χ^2-detector will trigger an alarm. Akhlaghi et al. introduced an extended Kalman filter (EKF) approach to detect anomalies in a two-area four-machine system and a 16-machine and 68-bus system [21]. In their approach, a multi step adaptive interpolation technique was used to make a trade of between the computational load and the accuracy of the estimation. Abbaspour et al. introduced a neural adaptive observer fault detection design for actuator and sensor faults for a general nonlinear system [22]. In their approach, EKF was used for online updating of the neural network (NN) coefficients. Teixeira et al. introduced an anomaly detection system that considers each subsystem as a node in a micro-grid system [25]. In their system, a distributed structure is developed to detect and isolate faults based on local models and measurements. Ten et al. introduced an FDI detection scheme for the power grid system based on a combination of hidden Markov model, transaction model and feature aided tracking [23]. An interval fuzzy type-2 scheme for smart grids was introduced by Linda et al. to improve the performance of a clustering based intrusion detection approach through tuning the sensitivity thresholds [24].

This paper is focused on detection of the FDI attacks on the load frequency control (LFC) systems. In this study, a new NN-based design is developed for detection of the FDI attacks in the LFC system. The ability of NN in estimating the nonlinear behavior of the system motivated us to use this tool for FDI attack detection in the LFC system. The proposed design consists of an NN and a Luenberger observer. The simulation results show that our design is able to detect and measure the inserted FDI attack to the system. The contribution of this work can be summarized as 1) It introduces a new scheme for FDI attack detection in power system; 2) Unlike many other detection approaches this method detects the anomalies in the system online; 3) This method can track abrupt faults with sufficient accuracy.

The rest of this paper is organized as follows: Section II presents the mathematical model of the LFC system, while Section III illustrates the design procedure of the detection system. The numerical simulation results are provided in Section IV. Finally, Section V provides the conclusion and future works of this study.

II. LFC Model

Here, a two-area power system is considered as the case study to show the effectiveness of the presented NND technique. Both power areas are connected to a centralized load frequency controller (LFC) which sends control signals to the plants and receives state signals through sensor measurements. The FDI attacks can be injected to the LFC feedback path by jamming the communication channels [26]. Here the LFC is designed with a state feedback controller which requires power state estimations. In the case, the adversary can make the system unstable by injecting FDI attack to the telemetered state signals.

The LFC multi-area interconnected power system is briefly described in the literature [9], [27], [28]. It should be noted that the NN observer design will cover the nonlinear behavior of the system. The state space model of the LFC for the power system is given in (1). Here a linear approximation of the system is described, however, a nonlinear term ($D\Delta P_l$) is added to cover nonlinear behavior of the LFC system.

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + D\Delta P_l, \quad x(0) = x_0 \\ y(t) = Cx(t) \end{cases} \tag{1}$$

where ΔP is the load deviation, $x(t) = [x_1, x_2]^T$ and $u(t)$ are the states and inputs respectively. The system states $x_i = [\Delta f^i, \Delta P_g^i, \Delta P_{tu}^i, \Delta P_{pf}^i, e^i]^T$ are states for the power areas $i = 1, 2$. where $\Delta f^i, \Delta P_g^i, \Delta P_{tu}^i, \Delta P_{pf}^i, e^i$ are frequency deviation, generator power deviation, turbine value position, power flow of tie-line and control error, respectively. The control error of the power area is $e^i(t) = \int_0^t \beta^i \Delta f^i dt$ where β^i is the frequency bias factor. x_0 is the initial state condition; C is a 10×10 unite matrix; A, B are constant matrices with appropriate dimensions which can be calculated by

$$A = \begin{bmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{bmatrix} \tag{2}$$

$$B = diag\{\begin{bmatrix} B_1 & B_2 \end{bmatrix}^T\} \tag{3}$$

$$D = diag\{\begin{bmatrix} D_1 & D_2 \end{bmatrix}^T\} \tag{4}$$

The control signal $u(t)$ can be found through the state feedback controller design as

$$u(t) = -K\hat{x}(t) \tag{5}$$

where K is a constant matrix and can be designed through pole placement method [29]. The matrices A_{11}, A_{12}, A_{21}, A_{22}, B_1, B_2, D_1 and D_2 can be calculated as follows. Consider $i = 1, 2$ and $j = 1, 2$ are indexes for A, B and D matrices:

$$A_{i,i} = \begin{bmatrix} -\mu_i/J_i & 1/J_i & 0 & -1/J_i & 0 \\ 0 & -1/T_{tu,i} & 1/T_{tu,i} & 0 & 0 \\ -1/\omega_i T_{g,i} & 0 & -1/T_{g,i} & 0 & 0 \\ \sum_{i=j,j=1}^{2} 2\pi T_{i,j} & 0 & 0 & 0 & 0 \\ \beta_i & 0 & 0 & 0 & 1 \end{bmatrix} \tag{6}$$

$$A_{i,j} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{i,j} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{7}$$

$$B_i = \begin{bmatrix} 0 & 0 & 1/T_{g,i} 0 & 0 \end{bmatrix}^T \tag{8}$$

$$D_i = \begin{bmatrix} -1/J_i & 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{9}$$

where ω_i, J_i, $T_{g,i}$, μ_i, and $T_{tu,i}$ are the speed-droop coefficient, the moment of inertia of generator, the governor time constant, damping coefficient, and the time constant of turbine for the i^{th} power area. $T_{i,j}$ is the stiffness constant between the i^{th} and the j^{th} power area.

III. FDI detection design

The presented method is illustrated in Fig.1. The power areas are connected to the centralized LFC. The adversary can inject FDI attacks to the communication channels which transmit the measured state, and control signals. The anomaly observer consists of a Luenberger observer and a feed-forward NN. The control input signals from the controller and output states are sent to the Luenberger observer to estimate the states. Finally the estimated states are transmitted to NND unit for detection and tracking the FDI attack. The NN observer, NN updating laws, and the Luenberger observer are described in the the following subsections.

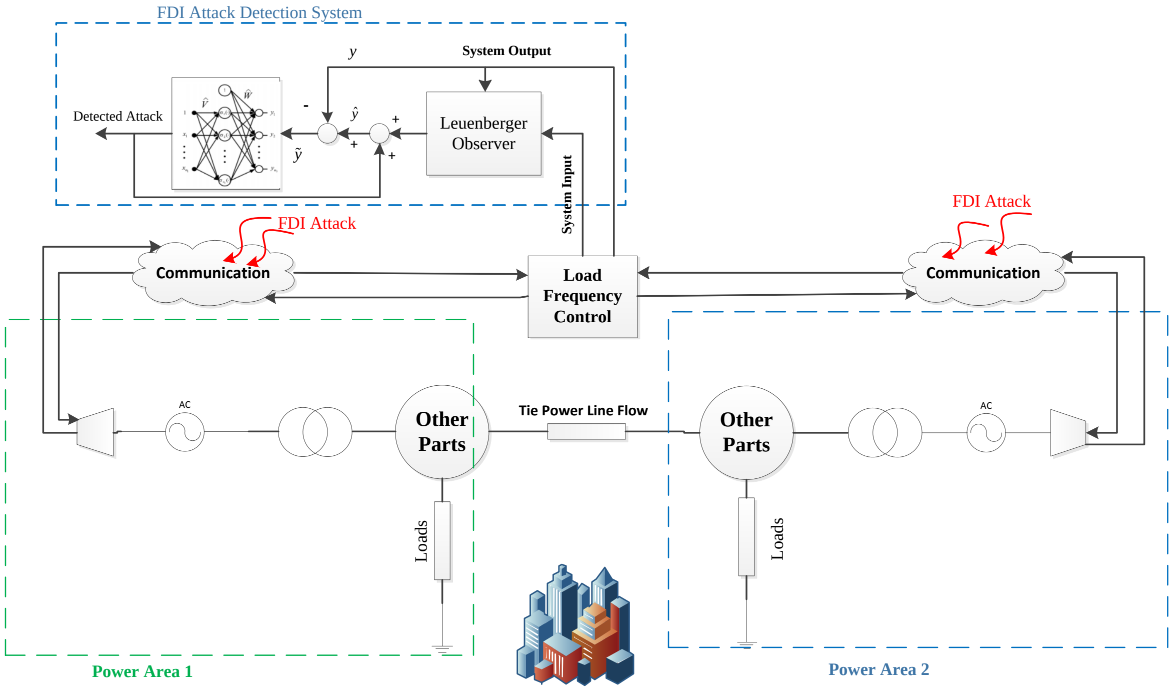

Fig. 1: Block Diagram of the proposed intrusion detection strategy for LFC system

A. *NN observer*

In this subsection, the design procedure of the proposed NN-based anomaly detector is illustrated. In this design, a feed-forward NN structure in conjunction with a luenberger observer are used to construct a recurrent model that is able to detect FDI attack in the LFC system. The proposed recurrent observer can be presented as follows

$$\begin{aligned}\dot{\hat{x}}(t) &= A\hat{x}(t) + Bu(t) + L\left(y(t) - \hat{y}(t)\right), \quad \hat{x}(0) = 0 \\ \hat{y}(t) &= C\hat{x}(t)) + F(\hat{x}, u, W)\end{aligned} \tag{10}$$

where L is the Luenberger observer gain and its design procedure will be explained in the following subsections; $\hat{x}(t)$ and $\hat{y}(t)$ are the estimated of $x(t)$, and $y(t)$; $F(\hat{x}, u, W)$ is the NN fault detector. The stability of this observer is investigated in [30], which demonstrates that for a restricted set of $x \in R^n$ and efficient number of hidden layers of neurons, weights and threshold, the recurrent NN is stable and is able to continuously estimate any nonlinear function as

$$F(x, u, W) = W\sigma(V\bar{x}) + \tilde{x}(t) \tag{11}$$

where W, V are the NN output and hidden weight matrices, respectively. Here, $\bar{x} = [x, u]^T$, $\tilde{x}(t) = x(t) - \hat{x} \leq e_M$ is the estimation error of the NN which is bounded by e_M, σ is a sigmoid activation function which represents the transfer function of the hidden layers [30]

$$\begin{aligned}\sigma_i(V^i\bar{x}) = \tfrac{2}{1+exp^{-2V^i\bar{x}}} - 1 \\ i = 1, 2, ..., N\end{aligned} \tag{12}$$

where N denotes the number of hidden layers, V^i is the i^{th} row of V, and the i^{th} element of $\sigma(V\bar{x})$ is denoted by $\sigma_i(V^i\bar{x})$.

B. *NN Updating Laws*

The updating laws of the NN observer are illustrated in this subsection. These laws are needed to ensure the stability and convergence of the NN in its learning process. The convergence of the NN weight update under these rules is investigated and demonstrated using the Lyapunov indirect method in [30]. Recalling the observer equation in (11), the NN updating laws can be presented as

$$\begin{aligned}\dot{\hat{W}}(t) &= -\gamma_1\left(\frac{\partial C_f}{\partial \hat{W}}\right) - \eta_1\|\tilde{y}\|\hat{W} \\ \dot{\hat{V}}(t) &= -\gamma_2\left(\frac{\partial C_f}{\partial \hat{V}}\right) - \eta_2\|\tilde{y}\|\hat{V}\end{aligned} \tag{13}$$

where γ_1 , $\gamma_2 > 0$ are the NN learning coefficients; $\tilde{y} = y - \hat{y}$; $C_f = 0.5(\tilde{y}^T\tilde{y})$ is the objective function of the NN, and η_1, η_2 are small positive coefficients which can be tuned by designer to get optimum performance in NN. In order to obtain the NN updating laws (13), the derivative of the objective function can be calculated using static gradient approximation and chain rules

[30], thus, we have

$$\begin{aligned}\dot{\hat{W}}(t) &= -\gamma_1 \left(\tilde{y}^T A_c^{-1}\right)^T L_1^T - \eta_1 \|\tilde{y}\| \hat{W} \\ \dot{\hat{V}}(t) &= -\gamma_2 \left(\tilde{y}^T A_c^{-1} \hat{W} L_2\right)^T - \eta_2 \|\tilde{y}\| \hat{V}\end{aligned} \tag{14}$$

where $A_c = k_n \times I_{10}$ and k_n is a small positive constant; L_1 and L_2 are be defined by

$$\begin{aligned}L_1 &= \sigma(\hat{V}\hat{\bar{x}}) \\ L_2 &= I - \Gamma(\hat{V}\hat{\bar{x}})\end{aligned} \tag{15}$$

and

$$\Gamma(\hat{V}\hat{\bar{x}}) = diag\left(L_1(i)^2\right), i = 1, 2, 3 \tag{16}$$

and $L_1(i)$ denotes the ith element of L_1 vector.

C. Luenberger observer

The Luenberger observer is designed to estimate the $\hat{x}(t)$ and send it to the NND unit for FDI attack detection. Let us define the error of the estimation as $\tilde{x}(t) = x(t) - \hat{x}(t)$, and by subtracting (10) from (1), we have

$$\begin{aligned}\dot{\tilde{x}}(t) &= A\tilde{x}(t) + D\Delta P_l - LC\tilde{x}(t) - LF(\hat{x}, u, W) \\ &= (A - LC)\,\tilde{x}(t) + D\Delta P_l - LF(\hat{x}, u, W)\end{aligned} \tag{17}$$

We neglected the nonlinear term $D\Delta P_l$ to simplify the Luenberger design because it will be identified with the NN observer ($F(\hat{x}, u, W)$), thus we have

$$\dot{\tilde{x}}(t) = (A - LC)\,\tilde{x}(t), \quad \tilde{x}(0) = x_0 \tag{18}$$

The L observer should be defined in a way that the eigenvalues of the $A - LC$ are all negative real values, then, the estimation error will converge to zero as $t \to \infty$. L can calculated using pole placement method [29].

IV. Simulation Results

The simulation studies are conducted on a two power area LFC system to evaluate the effectiveness of presented detection technique. The Luenberger observer is designed to feed the NND unit and the controller. More information about the Luenberger observer design can be found in [31]. The proposed NN in this study has 5 hidden layer and its parameters are selected as follows: $A_c = -0.001 \times I_{10}$, $\gamma_1 = \gamma_2 = 0.1$, $\eta_1 = \eta_2 = 0.05$, W_0 is a 10×5 matrix which all of its elements are 0.1, and V_0 is a 5×20 matrix with the same elements.
The parameters values for the power system is described in Table 1 of reference paper [9]. The LFC matrices are described in the APPENDIX. The simulation is conducted for 10 seconds. Two scenarios are considered in this simulation. In the first scenario, the adversary injected FDI attack to the third state of the first power area as follows:

$$FDI = \begin{cases} 0 & t < 5 \\ 1 & t \geq 5 \end{cases} \tag{19}$$

which means, FDI attack starts at $t = 5sec$ for the amount of 1 per unit (pu). Figure 2 shows the FDI attack (dashed line) along with attack estimation (solid line). Results clearly show that the NND method is able to detect and track the FDI attack.

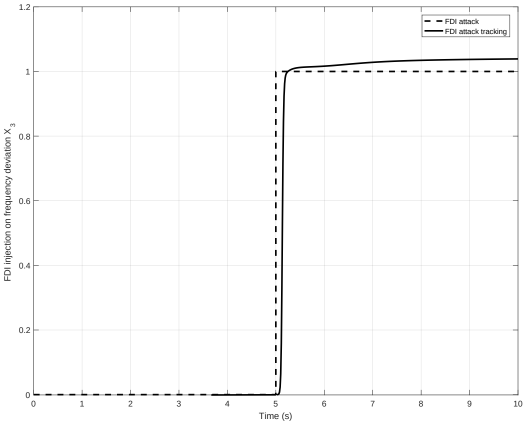

Fig. 2: Scenario 1-FDI attack and its estimation

For the second scenario, it's considered that the adversary injected a sinusoidal signal to the third feedback state of the first power area as described in the following equation:

$$FDI = \begin{cases} 0 & t < 2 \\ 5sin(5t) & t \geq 2 \end{cases} \tag{20}$$

Figure 3 illustrates the FDI attack and its estimation for the second scenario.

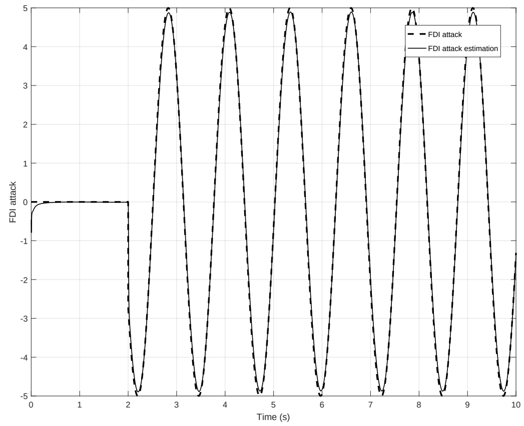

Fig. 3: Scenario 2-FDI attack and its estimation

V. Conclusion

This paper presented a new neural network based detection technique for an interconnected LFC power system to detect and estimate FDI attack which is injected to the state feedback of the system. Due to nonlinear behavior of power system the NN is used to alarm the system about the existence of FDI attacks in the system. The presented detection technique has been evaluated on a LFC model and the simulation results show that the presented method was able to successfully detect and accurately track the FDI attacks injected to the communication channels.

Appendix A
LFC System Matrices

Based on the parameters given in the table 1 of [9], the LFC matrices are given as follows:

$$A_{1,1} = \begin{bmatrix} -0.15 & 0.1 & 0 & -0.1 & 0 \\ 0 & -5 & 5 & 0 & 0 \\ -166.66 & 0 & -8.33 & 0 & 0 \\ 1.24 & 0 & 0 & 0 & 0 \\ 21.5 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{21}$$

$$A_{2,2} = \begin{bmatrix} -0.083 & 0.083 & 0 & -0.083 & 0 \\ 0 & -2.22 & 2.22 & 0 & 0 \\ -11.11 & 0 & -5.55 & 0 & 0 \\ 1.24 & 0 & 0 & 0 & 0 \\ 21.5 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{22}$$

$$A_{1,2} = A_{2,1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1.24 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{23}$$

$$B_1 = \begin{bmatrix} 0 & 0 & 8.33 & 0 & 0 \end{bmatrix}^T \tag{24}$$

$$B_2 = \begin{bmatrix} 0 & 0 & 5.55 & 0 & 0 \end{bmatrix}^T \tag{25}$$

The LFC feedback states are from the third state of the first and the second power areas. In the simulation, the controller gain $K = [K_1 \quad K_2]$ is calculated based on pole placement method:

$$K_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 51.16 & 0.9 & 0.54 & -2.5 & 5.07 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 11.90 & 0.15 & 0.28 & -0.65 & 0.65 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{26}$$

$$K_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 5.52 & 0.04 & 0.08 & -0.17 & 0.34 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 110.75 & 2.65 & 0.97 & -4.69 & 8.82 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{27}$$

References

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

[2] J. Yan, Y. Tang, B. Tang, H. He, and Y. Sun, "Power grid resilience against false data injection attacks," in *Power and Energy Society General Meeting (PESGM), 2016*, pp. 1–5, IEEE, 2016.

[3] M. Motalleb, E. Reihani, and R. Ghorbani, "Optimal placement and sizing of the storage supporting transmission and distribution networks," *Renewable Energy*, vol. 94, pp. 651–659, 2016.

[4] A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei, "Detection of fault data injection attack on uav using adaptive neural network," *Procedia Computer Science*, vol. 95, pp. 193–200, 2016.

[5] K. G. Boroojeni, M. H. Amini, and S. Iyengar, "Smart grids: Security and privacy issues," 2016.

[6] K. G. Boroojeni, M. H. Amini, and S. Iyengar, "Overview of the security and privacy issues in smart grids," in *Smart Grids: Security and Privacy Issues*, pp. 1–16, Springer, 2017.

[7] A. G. Delavar, M. Nejadkheirallah, and M. Motalleb, "A new scheduling algorithm for dynamic task and fault tolerant in heterogeneous grid systems using genetic algorithm," in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, vol. 9, pp. 408–412, IEEE, 2010.

[8] S. Akhlaghi, N. Zhou, and Z. Huang, "Adaptive adjustment of noise covariance in kalman filter for dynamic state estimation," *arXiv preprint arXiv:1702.00884*, 2017.

[9] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 1176–1185, 2016.

[10] M. E. Raoufat, A. Khayatian, and A. Mojallal, "Performance recovery of voltage source converters with application to grid-connected fuel cell dgs," *IEEE Transactions on Smart Grid*, 2016.

[11] M. Motalleb, M. Thornton, E. Reihani, and R. Ghorbani, "Providing frequency regulation reserve services using demand response scheduling," *Energy Conversion and Management*, vol. 124, pp. 439–452, 2016.

[12] M. R. Khalghani, M. A. Shamsi-nejad, and M. H. Khooban, "Dynamic voltage restorer control using bi-objective optimisation to improve power quality's indices," *IET Science, Measurement & Technology*, vol. 8, no. 4, pp. 203–213, 2014.

[13] A. Dehghan Banadaki, F. Doost Mohammadi, and A. Feliachi, "State space modeling of inverter based microgrids considering distributed secondary voltage control," *49th North American Power Symposium (NAPS), Morgantown, WV, USA.*, 2017.

[14] M. R. Khalghani and M. H. Khooban, "A novel self-tuning control method based on regulated bi-objective emotional learning controller's structure with tlbo algorithm to control dvr compensator," *Applied Soft Computing*, vol. 24, pp. 912–922, 2014.

[15] A. Dehghan Banadaki and A. Feliachi, "Voltage control using eigen value decomposition of fast decoupled load flow jacobian," *49th North American Power Symposium (NAPS), Morgantown, WV, USA.*, 2017.

[16] A. I. Sarwat, M. Amini, A. Domijan, A. Damnjanovic, and F. Kaleem, “Weather-based interruption prediction in the smart grid utilizing chronological data,” *Journal of Modern Power Systems and Clean Energy*, vol. 4, no. 2, pp. 308–315, 2016.

[17] C.-K. Zhang, L. Jiang, Q. Wu, Y. He, and M. Wu, “Delay-dependent robust load frequency control for time delay power systems,” *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2192–2201, 2013.

[18] M. E. Raoufat, K. Tomsovic, and S. M. Djouadi, “Dynamic control allocation for damping of inter-area oscillations,” *IEEE Transactions on Power Systems*, 2017.

[19] M. E. Raoufat, K. Tomsovic, and S. M. Djouadi, “Virtual actuators for wide-area damping control of power systems,” *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4703–4711, 2016.

[20] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using kalman filter,” *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.

[21] S. Akhlaghi, N. Zhou, and Z. Huang, “A multi-step adaptive interpolation approach to mitigating the impact of nonlinearity on dynamic state estimation,” *IEEE Transactions on Smart Grid*, 2017.

[22] A. Abbaspour, P. Aboutalebi, K. K. Yen, and A. Sargolzaei, “Neural adaptive observer-based sensor and actuator fault detection in nonlinear systems: Application in uav,” *ISA transactions*, vol. 67, pp. 317–329, 2017.

[23] C.-W. Ten, J. Hong, and C.-C. Liu, “Anomaly detection for cybersecurity of the substations,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 865–873, 2011.

[24] O. Linda, M. Manic, and T. Vollmer, “Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge,” in *Resilient Control Systems (ISRCS), 2012 5th International Symposium on*, pp. 48–54, IEEE, 2012.

[25] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “Distributed fault detection and isolation resilient to network model uncertainties,” *IEEE transactions on cybernetics*, vol. 44, no. 11, pp. 2024–2037, 2014.

[26] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, “Detecting false data injection attacks on dc state estimation,” in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, vol. 2010, 2010.

[27] A. Sargolzaei, M. Abdelghani, *et al.*, “Detection of and responses to time delays in networked control systems,” Sept. 1 2015. US Patent App. 14/842,447.

[28] A. Sargolzaei, K. Yen, and M. Abdelghani, “Delayed inputs attack on load frequency control in smart grid,” in *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, pp. 1–5, IEEE, 2014.

[29] N. S. Nise, *CONTROL SYSTEMS ENGINEERING, (With CD)*. John Wiley & Sons, 2007.

[30] H. A. Talebi, K. Khorasani, and S. Tafazoli, “A recurrent neural-network-based sensor and actuator fault detection and isolation for nonlinear systems with application to the satellite’s attitude control subsystem,” *IEEE Transactions on Neural Networks*, vol. 20, no. 1, pp. 45–60, 2009.

[31] C.-T. Chen, *Linear system theory and design*. Oxford University Press, Inc., 1995.