2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe) | 978-1-6654-3613-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/EEEIC/ICPSEurope51590.2021.9584690

Direct Search-based Delay Attack Mitigation in Electric Vehicle Aggregators

Khashayar Torabi Farsani, Maryam Dehghani, Roozbeh Abolpour, Navid Vafamand
Shiraz University
Shiraz, Iran
{kh.torabi, mdehghani, a.abolpour, n.vafamand}@shirazu.ac.ir

Mohammad S. Javadi
INESC TEC
Porto, Portugal
msjavadi@gmail.com

Fei Wang
North China Electric Power University
Baoding, China
feiwang@ncepu.edu.cn

João P. S. Catalão
FEUP and INESC TEC
Porto, Portugal
catalao@fe.up.pt

***Abstract*—Nowadays, recent advances in information technology and communication facilitates using networked controlled systems in different industrial plants. Whereas data is transferred among different components of the networked systems, they are vulnerable to various types of attacks. This important issue in nowadays industrial plants should be treated logically and reasonable protection mechanisms to mitigate such attacks should be provided. This paper considers delay attack impacts on frequency regulation of an electric vehicle aggregator (EVA) system. The command control action is received by the EVA through an imperfect channel containing uncertainties subject to the time-delay attack. A systematic approach based on a direct search algorithm (DSA) is developed to design a resilient proportional-integral (PI) controller for mitigating such attacks. The proposed DSA provides low-conservative results, explores the design space to find a feasible solution, and computes the PI controller gains to assure the stability of the EVA system in the presence of the delay attack. Stability analysis and numerical simulations for a typical attacked EVA frequency regulation are given to show the effectiveness of the developed controller.**

***Keywords*—Delay attack, Electric vehicle aggregator system, Model uncertainty, Direct search algorithm.**

I. INTRODUCTION

In recent years, due to environmental concerns and pollution, as well as the gradual depletion of fossil resources, researchers have a lot of attention to electric vehicles (EVs). On the other hand, the emergence of these vehicles has caused them to deal with the negative effects of renewable energy sources [1], the most salient of which is fluctuations in the generations. The EV aggregator (EVA) is connected to and controlled by a load frequency control (LFC) center to regulate the charging and discharging operations of the batteries involved in it [2]. The EVAs and the LFC center establish a networked control system, which transfer data through a communication network vulnerable to attacks that lead to data delay, loss, or alteration [3]. These issues negatively affect the performance and stability of the EVA LFC system [4].

These days, information technology (IT) made the transfer of data through networks so easy and implementable. However, the IT structure is vulnerable to cyber-attacks [5],[6]. In other words, an attacker causes an error and manipulates control signals, and changes the data by performing an attack on the IT infrastructure and may destroy the system.

For instance, an attacker could sabotage and turn off a large grid and increase or decrease a load of a power transformer. Various types of attacks have been studied in research papers, including a false data injection attack (FDIA) [3], and a GPS spoofing attack (GSA) [7], a denial-of-service (DoS) attack [8], and a time-delay attack (TDA) [9]. According to salient aspects of the delay attack in reducing the system's relative stability, this paper is devoted to analyzing it on a sample practical EVA LFC system [10].

Many works have been done on the subject of the attack detection and mitigation, such as [11], which shows a series of FDIAs against state estimation in power distributions systems, and also, in [12], a method is provided to examine the vulnerability of PMUs in counterfeit attacks and attack reconstruction. Ref. [8] concerns designing resilient state feedback controllers for a class of networked control systems under DoS attacks. In [13], a method is presented to detect dissonances based on FDIA using an observer consisting of two parts, Luenberger, and a neural network. Recently, the issue of the LFC system under attack has received much attention [3]. The authors of [14] develop an adaptive resilient LFC scheme for sub-systems of smart grids under DoS attacks with energy constraints. The TDA has been discussed in [9], [15], which produces a time-varying delay in the dynamics of power systems. Such an attack will have devastating consequences if no prevention measures are considered in the design of these systems.

Some research is devoted to the stability analysis and controller design of the EVA LFC system in presence of time delays [2]. However, the way of calculating the controller gains in these papers is conservative. Also, the effect of system uncertainties on the closed-loop time delayed LFC has not been studied, yet. Reminding the necessity of considering the effects of TDA and parameter uncertainties, and the drawbacks of the existing results, this paper uses a novel and systematic approach, called direct search algorithm (DSA), to design a robust controller for an EVA LFC system. The designed controller ensures the stability of the closed-loop system based on its characteristic equation. Initially, the characteristic equation with TDA is approximated by a quasi-polynomial representation. The DSA is then applied to the polynomial representation to search for a feasible solution in the pre-specified proportional-integral (PI) controller gains space and numerically find the controller gains. To show the merits of the suggested method, numerical simulations are conducted and the effects of system parameters and TDA value on the closed-loop stability margin and controller gains are studied.

J.P.S. Catalão acknowledges the support by FEDER funds through COMPETE 2020 and by Portuguese funds through FCT, under POCI-01-0145-FEDER-029803 (02/SAICT/2017).

This paper is continued as follows: In Section II, the EVA LFC system in presence of uncertain parameters and TDA is introduced. In Section III, the proposed method for delay attack compensation and frequency controller design are discussed. In Section IV, simulations are conducted. Section V ends this paper by evoking some concluding remarks and future perspectives.

II. EVA LFC SYSTEM

One key role of EVA units is to manipulate the charging and discharging of EVs in parking lots to help regulate the frequency of the connected AC microgrid. The EVAs get the controller commands from a control center to inject or absorb electric power and distribute it among the available EVs. To maintain the efficiency of the EVA operation, the communication link should be established between the EVA and control centers in a reliable manner. Whereas the communication links are perfect in practice, they are vulnerable to different issues including attacks. They highly affect the stability of the power system.

In this paper, to investigate the stability of the power system in the presence of attacks, a single-area LFC system is connected to an EVA through an imperfect communication network. The schematic of a typical single-area LFC system including a generator, an EVA, TDS attack, and the droop and PI controllers is drawn in Fig. 1. As can be seen in Fig. 1, the Δf is the deviation of AC power system frequency. ΔP_g, ΔP_{EV}, and ΔP_d are electrical power output, EVA power output, and load disturbance, respectively, ΔX_g and ΔP_m are the valve position and mechanical power output, respectively. The other parameter definitions and values are given in Table I. The characteristic equation of EVA LFC system of Fig. 1 can be written as follows:

$$L(s,K,\alpha,f) = P(.) + Q(.)F(s) \tag{1}$$

where $K = [K_p, K_i]$ is the vector of the PI controller gain, f is the TDA value and $F(s)$ is its corresponding representation in the frequency domain. The details of system parameters and the polynomials in $P(.)$ and $Q(.)$ are given in (2)-(3). As can be seen in the characteristic polynomial of the EVA system, α_0, α_1 are uncertain parameters which are assumed to be in a pre-specified range. Also, $= [K_p, K_i]$ are the controller unknown parameters which should be designed to overcome the TDA and parameter uncertainties and should guarantee the overall system stability and frequency regulation under the delay attack and uncertain parameters.

III. APPROACH TO COMPENSATE DELAY ATTACK

In this paper, a control procedure is presented that is resistant to delay attack. This control method is a robust PI controller that is designed using the direct search method. In the following, the required steps for designing the controller are elaborated.

$$\begin{aligned} P(.) &= \sum_{i=0}^{6} P_i S^i = 0.0576S^6 + 1.0673S^5 \\ &+ 5.9685S^4 + (10.9445 + 0.3818\alpha_0 K_P)S^3 \\ &+ (4.0455 + 4.0091\alpha_0 K_P + 0.3818\alpha_0 K_I)S^2 \\ &+ (1.0909 + 1.9091\alpha_0 K_P + 4.0091\alpha_0 K_I)S^1 \\ &+ 1.9091\alpha_0 K_I \end{aligned} \tag{2}$$

TABLE I: SYSTEM PARAMETERS' VALUES AND DEFINITIONS

Par.	Value	Definition	Par.	Value	Definition
T_g	0.2 s	governor time constant	R	1/11 Hz /$p.u.MW$	speed droop regulation
T_c	0.3 s	turbine time constant	K_{EV}	1 s	battery coefficient
T_r	12 s	reheat time constant	M	8.8	generator inertia constant
T_{EV}	0.1 s	battery time constant	D	1	load-damping coefficient
F_P	1.6	fraction of total turbine power	α_0	$\in$ [0.9 1]	participation factors uncertainties
β	21	frequency bias factor	α_1	$\in$ [0 0.1]	

$$\begin{aligned} Q(.) &= \sum_{i=0}^{4} Q_i S^i = (1.3745\alpha_1 K_P)S^4 \\ &+ (11.5691\alpha_1 K_P + 1.3746\alpha_1 K_I)S^3 \\ &+ (23.8637\alpha_1 K_P + 11.5691\alpha_1 K_I)S^2 \\ &+ (1.9091\alpha_1 K_P + 23.8637\alpha_1 K_I)S^1 \\ &+ 1.9091\alpha_1 K_I \end{aligned} \tag{3}$$

A. System modeling in presence of TDA

The EVA system introduced in Section II in presence of a time delay attack and parameter uncertainties are considered, according to Fig. 1. It is assumed that the delay attack is applied to the system as follows:

$$0 < f < F \tag{4}$$

Therefore, the characteristic equation of the system despite the delay attack is as follows:

$$L(s,K,\alpha,f) = \sum_{i=0}^{6} P_i S^i + \sum_{i=0}^{4} Q_i S^i e^{-Fs} \tag{5}$$

It should be noted that the characteristic function $L(s,K,\alpha,f)$ is a function of some known and unknown variables. Obviously, s is the Laplace variable. K entails controller parameters which are unknown and they should be determined via the DSA. α denotes the parameter uncertainties in the model. It is assumed that the uncertainties are in a predefined range. f is the value of attack which imposes delay in the communication channel and influences the performance of overall system. The goal of this section is to present a methodology for PI controller design such that the frequency is regulated in presence of the delay attack and uncertainties.

The TDA imposes an exponential function in the characteristic equation. Therefore, it is necessary to change the display of the system to obtain a polynomial form. Accordingly, the Rekasius approach is applied to the nonlinear term e^{-Fs}, it is replaced by $\frac{1-TS}{1+TS}$. Therefore, the characteristic equation can be mentioned in terms of the new variable in T as follows [16]:

$$\hat{L}(s,K,\alpha,T) = 0 \tag{6}$$

The objective is to choose the PI controller gains $K = [K_p, K_I]^T$ for regulating the frequency Δf in the presence of the uncertain participation factor vector $\alpha = [\alpha_0, \alpha_1]^T$.

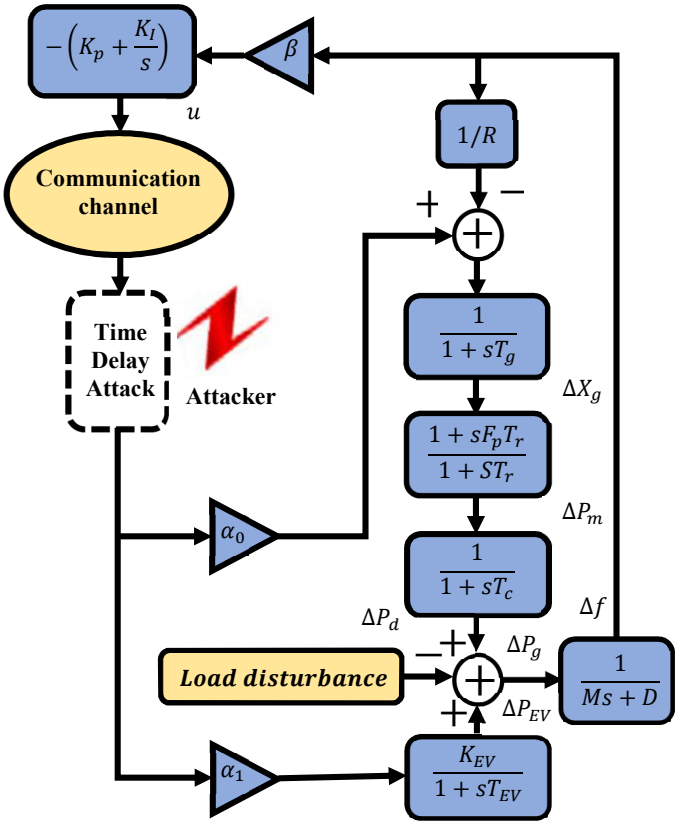


Fig. 1.The EVA system attacked by a TDA.

B. Controller design using DSA

If the system (6) is considered, then various methods can be used to analyze the stability of such a system, including the Lyapunov-Krasovskii functional (LKF) method [17]. However, assessing the LKF stability through LMIs imposes conservativeness on the problem. In this paper, the DSA [18] is used, because it is a low conservative method. The main idea of the direct search algorithm is to presume a design space for the unknown controller parameters. Then, a systematic approach is utilized to search in the design space and find a feasible solution which assures the system stability and the required performance.

Since two gains K_p and K_I should be found, the design space can be determined in two-dimensional space. Assume that a triangular shape as shown in Fig. 2 is the design space of the parameters. This means that the feasible solution is only allowed inside this triangle (blue part). In general, the number of unknown variables is more than two and we call this shape a simplex.

Obviously, checking all points inside such a simplex to check whether it's a feasible point or not is completely time-consuming and due to the infinite number of points, it's illogical. The idea is based on the direct searching concept in [18], which firstly assesses the stability status of the three vertices of the simplex, i.e., K_1, K_2, K_3 in Fig. 2. If one of them is feasible, the algorithm returns it and stops. Otherwise, it should check whether there is a feasible point inside the simplex or not (second step). This can be checked through exposed edges lemma.

Lemma 1 [16]: All the points inside a simplex are totally infeasible if the characteristic polynomials generated at all vertices are unstable and the characteristic polynomials on the convex combination of each two vertices do not include any imaginary roots.

Lemma 1 presents an approach which guides us if we should search inside a simplex or we can simply eliminate it in the design space. The conditions in the lemma consist of two different constraints.

The first, needs to check the feasibility of the vertices which needs $\hat{L}(s, K_i, \alpha, T), i = 1,2,3$. If it is satisfied, we should constitute the convex combination of the above three characteristic functions and check for possible imaginary roots [18]. If this constraint is also satisfied, this simplex will surely contain no feasible point and it should be eliminated.

Assume that for a considered simplex, the conditions of Lemma 1 are not satisfied completely. This means that the first and the second steps are not satisfied and we should turn to the third step. In other words, none of the vertices are feasible and the conditions of Lemma 1 are not satisfied. In this situation, we should divide the simplex to two smaller parts and continue the first and second steps for those simplexes (Fig. 3).

Continuing the above-mentioned method, we gradually check the simplexes constituted in the design space to find a solution. Obviously, this algorithm does not need searching all the points inside the design space and it just checks the vertices and the polynomials on the convex combination of the vertices.

Therefore, it is practical and applicable. On the other hand, the algorithm only omits the totally infeasible simplexes according to Lemma 1, so it is evidently non-conservative. Fig. 4 summarizes the steps of direct search algorithm.

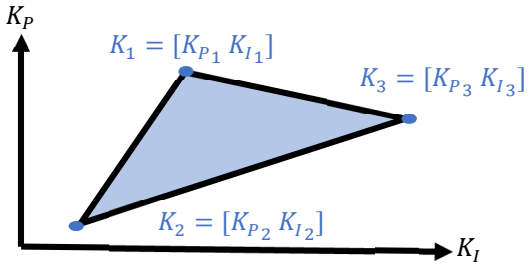


Fig. 2. Assumed design space for the controller parameters.

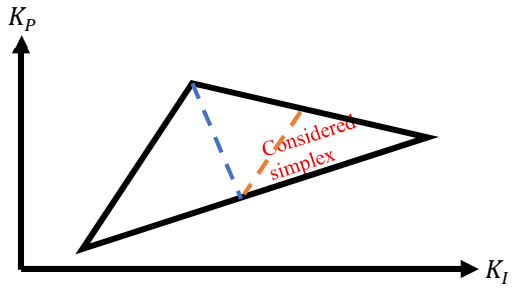


Fig. 3. Dividing the simplex to smaller ones.

IV. Simulation Results

In this section, the stability of the EVA system is analyzed using the direct search method, and the effect of parameter uncertainty and time delay attack on stability and frequency variations in the (K_p, K_I) -plane is investigated. Also, PI controller gain regions will be obtained for the stability of the closed loop system. Finally, the results and time-domain simulations will be presented in two scenarios.

A. Effect of time delay attack on the stability region

To show the effects of time delay attack on the stability of the closed loop system, the stability regions with uncertainties $\alpha_0 = [0.9,1]$ and $\alpha_1 = [0,0.1]$ for several attack delays is given in 2D and 3D spaces in Fig. 5.

According to the results of Fig 5, which is obtained from the direct search algorithm introduced in Section III for various time delay attacks, it is concluded that the more sever attack has a more negative effect on the stability region of the uncertain system. In other words, with a higher attack delay, the stability region becomes smaller.

As shown in Fig. 5, the larger delay attack, the smaller stability region is resulted. In Fig. 5a the stability region shown by a lighter color is due to a smaller TDA, while in Fig. 5b, the stability region of a larger TDA is shown by a lighter color. For a better understanding of the results, both 2D and 3D shapes of the stability regions are included in Fig 5. The transparent colors are selected to reach a better graph.

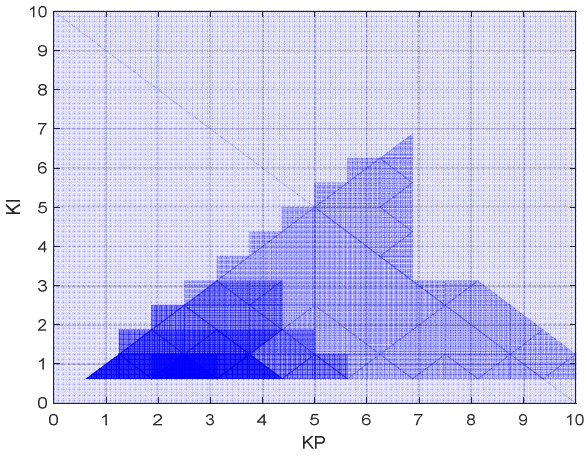
B. Simulation of TDA on the closed-loop system

Considering the specific controller $K = [K_p, K_i]$ based on the results obtained in Fig 5, the effects of TDA on the EVA are evaluated and the results are shown in Fig. 6.

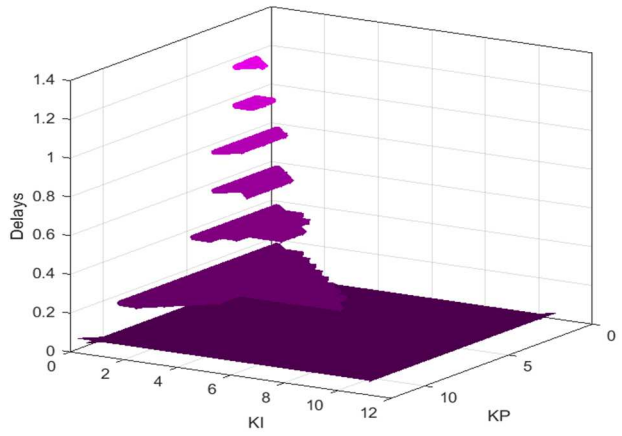
Fig 6(a) demonstrates the variation of TDA. Fig. 6(b) shows that the system is robust against TDA and the frequency can soon be regulated and the TDA effects are mitigated.

Fig. 6(c) illustrates the control signal which is implementable.

This simulation proves the effectiveness of the direct search method for TDA mitigation and the approach is successful as a defense mechanism against this type of attack.



(a)



(b)

Fig. 5. Stability regions for EV aggregator participation factors $\alpha_0 = [0.9,1]$, $\alpha_1 = [0,0.1]$, (a). 2D stability regions for various delays, (a). 3D stability regions.

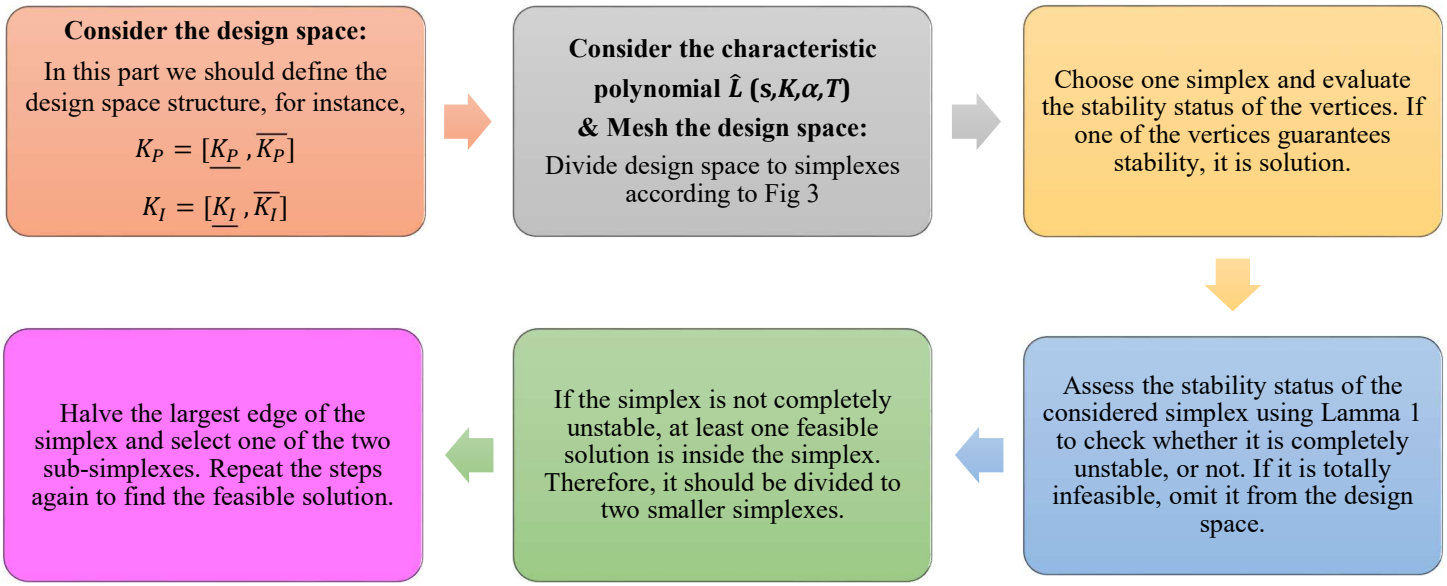
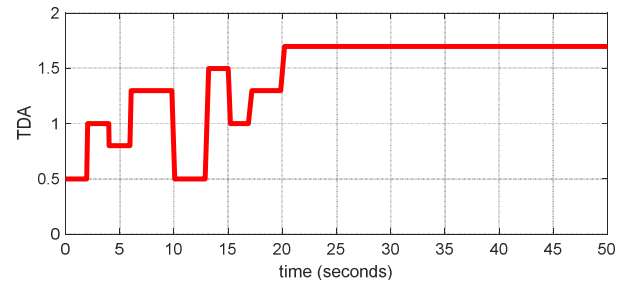
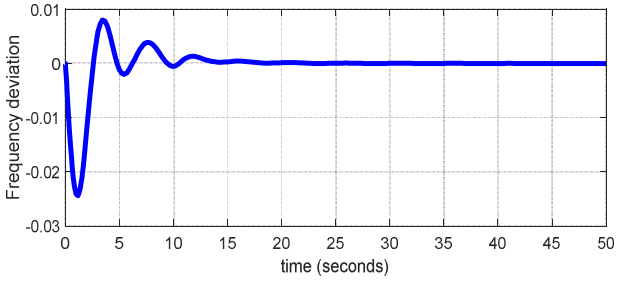


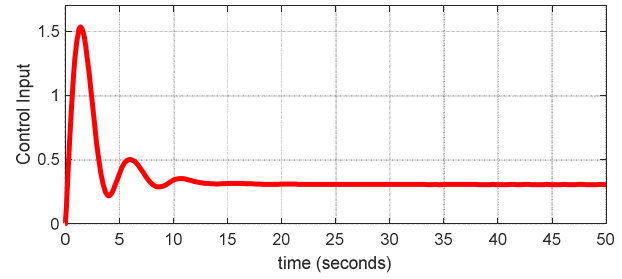
Fig. 4. The direct searching approach



(a)



(b)



(c)

Fig. 6. Time domain simulation (a) TDA, (b) Frequency deviation, (c) Control input.

V. Conclusion

In this paper, the challenges of connecting an EVA to a LFC system with a TDA were investigated. The characteristic equation of the closed-loop system controlled by a PI controller was derived. Then, a numerical iterative DSA was introduced to find a feasible solution for the controller gains that assure the robust closed-loop stability against system uncertainties and TDA. Several scenarios were presented to show the impact of TDA value on the LFC stability and frequency response. It was shown that by increasing the value of the TDA, the area of the stability region was reduced. For future work, considering other kinds of attacks on the system and proposing related defense mechanisms are suggested.

References

[1] Ko, K.S. and Sung, D.K., 2017. The effect of EV aggregators with time-varying delays on the stability of a load frequency control system. *IEEE Transactions on Power Systems,* vol. 33, no. 1, pp.669-680.

[2] A. Naveed, S. Sonmez, and S. Ayasun, "Impact of Electric Vehicle Aggregator with Communication Time Delay on Stability Regions and Stability Delay Margins in Load Frequency Control System," *J. Mod. Power Syst. Clean Energy,* pp. 1–7, Jul. 2020, doi: 10.35833/MPCE.2019.000244.

[3] H. Javanmardi, M. Dehghani, M. Mohammadi, S. Siamak, and M. R. Hesamzadeh, "BMI-Based Load Frequency Control in Microgrids Under False Data Injection Attacks," *IEEE Syst. J.*, pp. 1–11, 2021, doi: 10.1109/JSYST.2021.3054947.

[4] K. Torabi-Farsani, M. H. Asemani, F. Badfar, N. Vafamand, and M. H. Khooban, "Robust Mixed μ-synthesis Frequency Regulation in AC Mobile Power Grids," *IEEE Trans. Transp. Electrification,* vol. 5, no. 4, pp.1182-1189, 2019.

[5] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019, doi: 10.1109/TSMC.2018.2884952.

[6] E. Tian and C. Peng, "Memory-Based Event-Triggering H∞ Load Frequency Control for Power Systems Under Deception Attacks," *IEEE Trans. Cybern.,* vol. 50, no. 11, pp. 4610–4618, Nov. 2020, doi: 10.1109/TCYB.2020.2972384.

[7] S. Siamak, M. Dehghani, and M. Mohammadi, "Dynamic GPS Spoofing Attack Detection, Localization, and Measurement Correction Exploiting PMU and SCADA," *IEEE Syst. J.*, pp. 1–10, 2020, doi: 10.1109/JSYST.2020.3001016.

[8] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, "Resilient Control Design Based on a Sampled-Data Model for a Class of Networked Control Systems Under Denial-of-Service Attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020, doi: 10.1109/TCYB.2019.2956137.

[9] A. Sargolzaei, K. Yen, and M. N. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2014, pp. 1–5.

[10] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic Stability Analysis and Control of Secondary Frequency Regulation for Islanded Microgrids Under Random Denial of Service Attacks," *IEEE Trans. Ind. Inform.*, vol. 15, no. 7, pp. 4066–4075, Jul. 2019, doi: 10.1109/TII.2018.2885170.

[11] R. Deng, P. Zhuang, and H. Liang, "False Data Injection Attacks Against State Estimation in Power Distribution Systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019, doi: 10.1109/TSG.2018.2813280.

[12] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability Analysis of Smart Grids to GPS Spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3535–3548, Jul. 2019, doi: 10.1109/TSG.2018.2830118.

[13] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient Control Design for Load Frequency Control System Under False Data Injection Attacks," *IEEE Trans. Ind. Electron.,* vol. 67, no. 9, pp. 7951–7962, Sep. 2020, doi: 10.1109/TIE.2019.2944091.

[14] K.-D. Lu, G.-Q. Zeng, X. Luo, J. Weng, Y. Zhang, and M. Li, "An Adaptive Resilient Load Frequency Controller for Smart Grids with DoS Attacks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 4689–4699, May 2020, doi: 10.1109/TVT.2020.2983565.

[15] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei and B. Carbunar, "Resilient Design of Networked Control Systems Under Time Delay Switch Attacks, Application in Smart Grid," in *IEEE Access*, vol. 5, pp. 15901-15912, 2017, doi: 10.1109/ACCESS.2017.2731780.

[16] R. Abolpour, M. Dehghani, and H. A. Talebi, "A non-conservative state feedback control methodology for linear systems with state delay," *Int. J. Syst. Sci.,* pp. 1–15, Mar. 2021, doi: 10.1080/00207721.2021.1892235.

[17] W. I. Lee, S. Y. Lee, and P. Park, "Affine Bessel–Legendre inequality: Application to stability analysis for systems with time-varying delays," *Automatica*, vol. 93, pp. 535–539, Jul. 2018, doi: 10.1016/j.automatica.2018.03.073.

[18] R. Abolpour, M. Dehghani, and H. A. Talebi, "Output feedback controller for polytopic systems exploiting the direct searching of the design space," *Int. J. Robust Nonlinear Control,* vol. 29, no. 15, pp. 5164–5177, Oct. 2019, doi: 10.1002/rnc.4673.