False Data Injection Attack Clearance in Microgrid Load Frequency Control

Vikas Pandey[1] and Lini Mathew[2]

[1,2]Department of Electrical Engineering, NITTTR Chandigarh India-160019

Abstract

Microgrids are composed of renewable energy sources (RESs) such as wind and solar energy, along with inverters. This device reduces total system inertia due to the lack of rotational mass.In the face of uncertainty, the low system inertia issue may have an impact on microgrid stability and resiliency. The use of Information and Communication Technology (ICT) infrastructure in a power system raises concerns about cyber security.Discrete False Data Injection Attacks (DFDIA) againstAutomatic Generation Control(AGC) systems are studied to see the robustness of proposed controller.In this study, fuzzy logic, Proportional Integral Derivative (PID), Adaptive Neuro Fuzzy Inference System(ANFIS) controller method is applied in power system connected with Virtual Inertia to remove the fluctuations of electric energy and effect of DFDIA.

Keywords

Load frequency control, Virtual inertia, Cyber-attack, ANFIS.

1. Introduction

A reliable Load Frequency Control (LFC) is a significant capacityin today's power framework, which is scatteredtopographically across a vast area and intricately interconnected with diverse ages [1]. Especially when the off framework microgrids LFC need more intensive care for distantly working provincial areas microgrid activity in the dissemination structure. Since the microgrid uses converter-based, low inertial, and unpredictable limitless Distribution Generations (DGs), it contains more critical discussion and requires progressed control strategies to guarantee persistent stock to loads and to fix repeating change in the system [2].A few of these strategies are used to investigate various aspects of auxiliary LFC in microgrid [3]. In a genuine situation, regular regulators, for example, PI, PID, can provide control activity for one working condition in a boundary change every now and then. As a result, it is difficult to plan the necessary increases to achieve zero recurrence deviation in a wide range of parametric variations. As a result, programmed and adaptable regulators are required. In any case, research is ongoing, and a few techniques are being developed to combat this issue [4].In terms of peak overshoot, settling time, and consistent satiate blunder, ANFIS-based LFC performs better than classical regulators [5]. To distinguish the heap modifications and resolve the recurrence deviation, a versatile control framework is required. In [6,] a powerful control configuration works together to produce a multi–Distributed Energy Resource (DER) microgrid for power sharing in both interconnected and islanded modes.

In power system,components are responsible for the system frequency regulation. Cyber-attacks have become a serious threat to system security. AGC plays a crucial role in cyber-attack detection [7].As far as an assault plot plan, four assault procedures are painstakingly analysed as far as their component and effect on LFC execution, with the best one picked as the embraced assault conspire according to the programmers' point of view. In AGC, particular assault layouts are planned [8]. To drive the recurrence of these assaults, alter the recurrence and tie-line power stream estimations to out

International Conference on Emerging Technologies: AI, IoT, and CPS for Science & Technology Applications, September 06–07, 2021, NITTTR Chandigarh, India

EMAIL: vikas.elect2019@nitttrchd.ac.in (A. 1);lini@nitttrchd.ac.in(A. 2)
ORCID: Not Available (A. 1); Not Available(A. 2)

of the permissible reach. As far as to assault discovery, a clever assault location approach dependent on disparities between powerful properties of factors has been created [9]. A multi-facet perceptron classifier-based strategy is utilized to remove the varieties in region control blunder under attack and in an ordinary condition, and accordingly compromised signals are isolated from typical signs [10]. The AGC utilizes correspondence to send/get estimations/control activities about recurrence and force deviation in the power framework. Little AGC flaws can make the recurrence surpass the allowed range, bringing about the power outage, as displayed in fig.1. Digital aggressors target correspondence directs in more established brilliant lattices, while contemporary keen matrices contain an AGC framework that can recognize sham information infusion assaults [11]. Cyber-assaults on LFC have been tended to considering assault techniques [12]-[16] and countermeasures [17]-[9]. Assault systems contain Denial Of administration (DOS) and postponed input assaults which are mimicked on LFC to break down their effect [12], [13]. A solitary region power framework with a microgrid is demonstrated in this paper utilizing MATLAB/Simulink.ANFIS control strategy is utilized to eliminate the impact of different discrete bogus information infusion assaults against AGC systems. This paper is containing the following areas. Segment 2 System Description. Cyber Attack Strategies on the Load recurrence control Systems depicted in section3. The area is 4focused on Cyber Attack Detection and Clearance utilizing ANFIS Controller. Reenactment and Result Analysisare talked about in area 5.

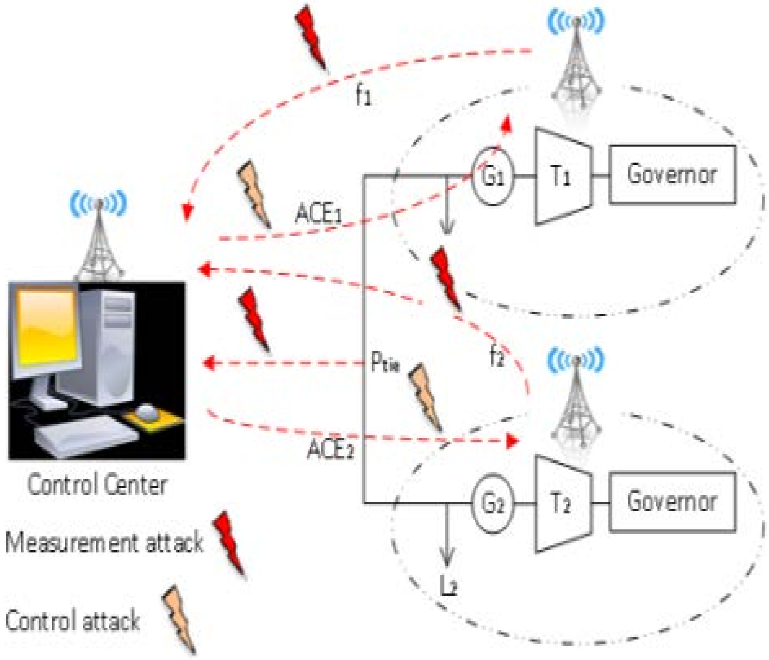

Figure 1: Data communication in Power system

2. SYSTEM DESCRIPTION

In this work, a micro grid with a solitary region power framework is utilized as an experiment. Every region is indicated utilizing the boundaries that relate to it (Table.1).The AGC model square outline for the depicted framework is displayed in Fig 2. Region Control Error (ACE), which is a direct blend of recurrence △f and tie-line power deviation △Ptieis being gathered at LFC focus in Eq. (1). Then, at that point, LFC order is created by LFC focus and sends it to base level parts, which relieve lop-sidedness of dynamic force, in this manner accomplishing recurrence/tie-line power soundness.

$$ACE = \Delta P_{tie} + \beta\Delta f(1)$$

In steady state, frequency deviation of each interconnected system is equal to zero i.e.,Δf=0.

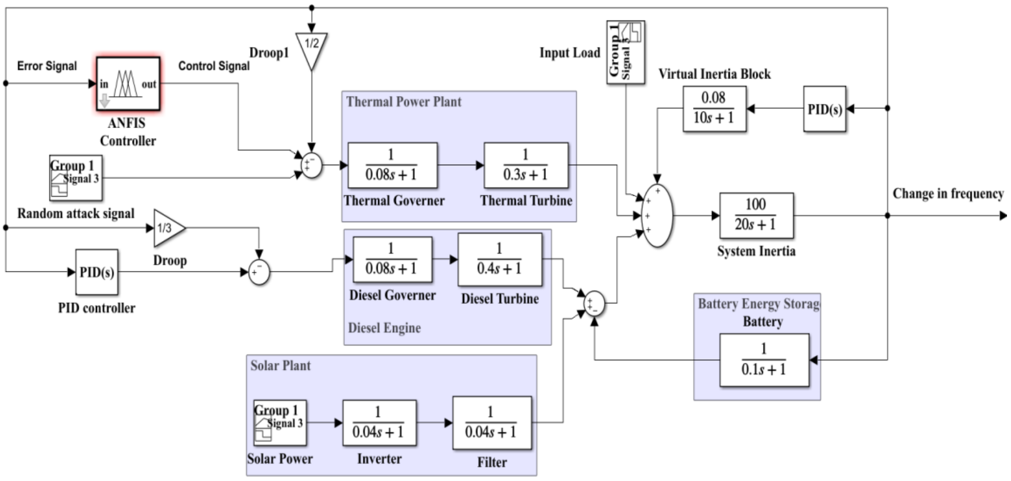

Figure 2: MATLAB SimulinkAutomatic Generation Control model

Table 1
Parameter values of the power system

Parameter	Value
Damper(D)	0.015
2H	0.1667
T_{inv}(S)	0.26
T_{filt}(S)	0.04
T_{dg} (S)	0.004
T_{dt} (S)	0.08
T_{tt} (S)	0.03
T_{tg}(S)	0.008

3.Cyber Attack Strategies on the Load frequency control System

As shown in Fig. 3, the LFC system consists of the plant, measurement system, and LFC controller. The attacker can insert false data before and after the controller, plant, and measurement system at this point. The false data is injected before the controller block in this paper.

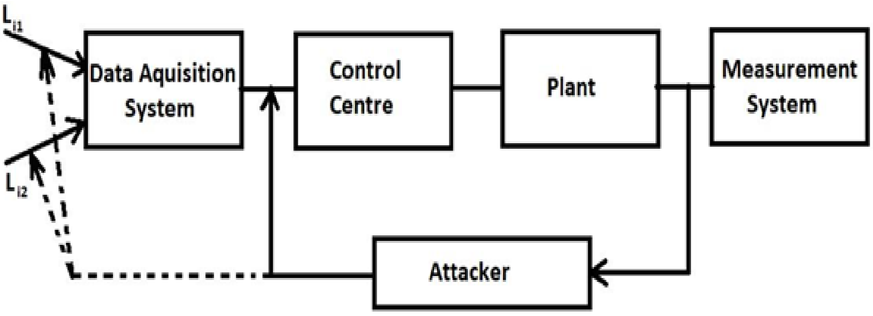

Figure 3: A simplified power system architecture with cyber-attack issue.

The Two main variablesof LFC(frequency and tie-line interchange power) are the potential attack targets. FDI attacks are emphasized in the model, which are usually studied in cyber-attacks.

The mathematical representation of FDIAis shown below:

$$\text{False Data,}F_d= D+ F_{ij} \tag{2}$$

where D is the orginal data and Fi,j is the injected data.

There are two types of data injections.

1. Scaling attack

$$x_{mea} = k_{xtru} \tag{3}$$

   where k is the scaling attack parameter

2. Exogenous attack

$$x_{mea} = x_{tru} + d \tag{4}$$

where x_{mea}, x_{tru}, d represents the falsified measurement, true measurement, and disturbance signal respectively. The disturbing signal can be ramp, pulse, and random signals [20].

4. False data Clearance using Adaptive Neuro Fuzzy Inference System Controller

The ANFIS Toolbox is used to detect the FDI assaults. It maps the contributions by utilizing input enrolment work (going before boundaries) into the yield by utilizing yield participation work (ensuing boundaries) as displayed in Fig.6. To recognize counterfeit information, back spread and a crossbreed of back engendering and least square assessment is utilized. Moreover, in light of the info includes, the Neuro-Fuzzy Controller (NFC) creates one of the six sorts of assaults. The learning system changes both the former and ensuing boundaries. The NFC alters the boundaries of the info and yield enrolment capacities dependent on the blunder basis (amount of squared distinction among real and wanted yields). Fig. 4 shows the stages engaged with ANFIS boundary change [21] [22].

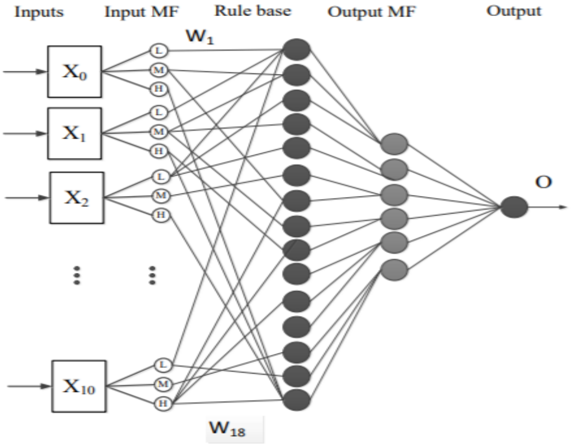

Figure 4: Steps involved for parameter adjustment of ANFIS.

ANFIS employs a three-layer neural network to imitate the fuzzy inference system used in our research. The input and output language variables are represented by the linguistic nodes in layers one and four, respectively. Nodes in layer two are term nodes that act as membership functions for input variables. The fuzzy rule is represented by each neuron in the third layer, which has input connections. Because the chi-square test is used to discover ten features, the input layer has ten nodes

[23]. The membership function is a generalized bell curve, and the second layer is a fuzzification layer with the same membership function. The third layer normalizes the strength of all rules, and the fourth layer uses a generalized bell curve membership function before delivering the aggregated results to the output layer, as illustrated in Fig.5.

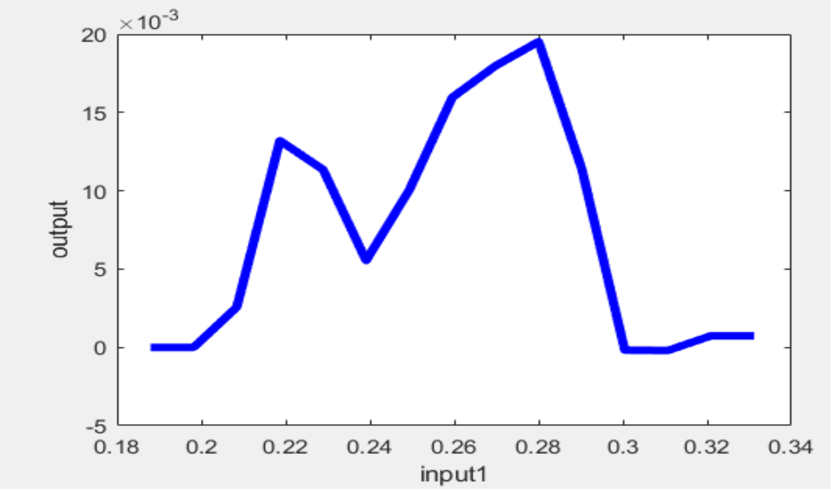

Figure 5: Input and output graph of ANFIS controller

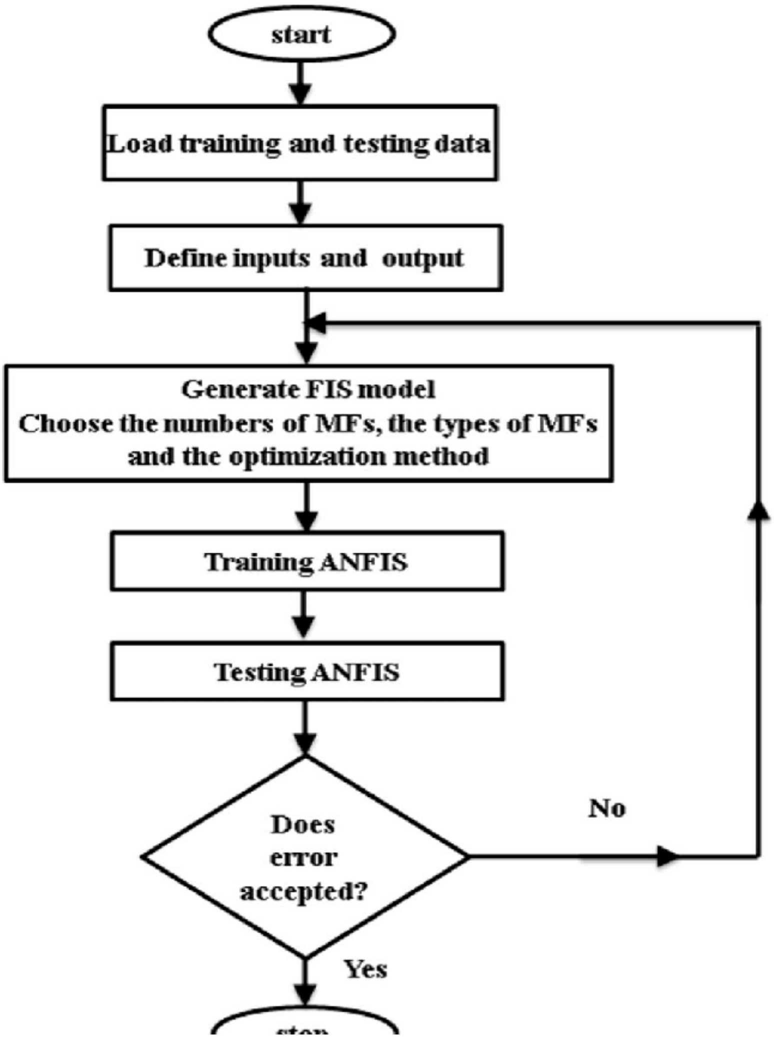

Figure 6: The steps involved in adjusting ANFIS parameters.

5. SIMULATIONS AND ANALYSIS

This study investigates the FDI attack diagnosis of System (as shown in Fig.2) using the MATLAB/SIMULINK software. A microgrid's load frequency control is simulated utilising all available sources, such as PV, wind, fuel cell, diesel, and battery storage. The system response is evaluated to two different scenarios: load and generation variation and discrete FDIA after controller.In this different type of false data is injected after the controller block.

The frequency deviation response of the system is depicted in this scenario with a 0.2p.u step load change and a solar power change, i.e., FDIA injection after controller with 0.5 scaling factor and random scaling factor. Figures (7, 9, 10) show a frequency deviation comparison of system response. The response to changes in thermal, system, and microgrid power is also depicted in Figure 8. The simulation and sampling times are set to 10s and 0.01s, respectively. In comparison to the PID controller and the Fuzzy controller, the proposed controller provides a better and faster response.

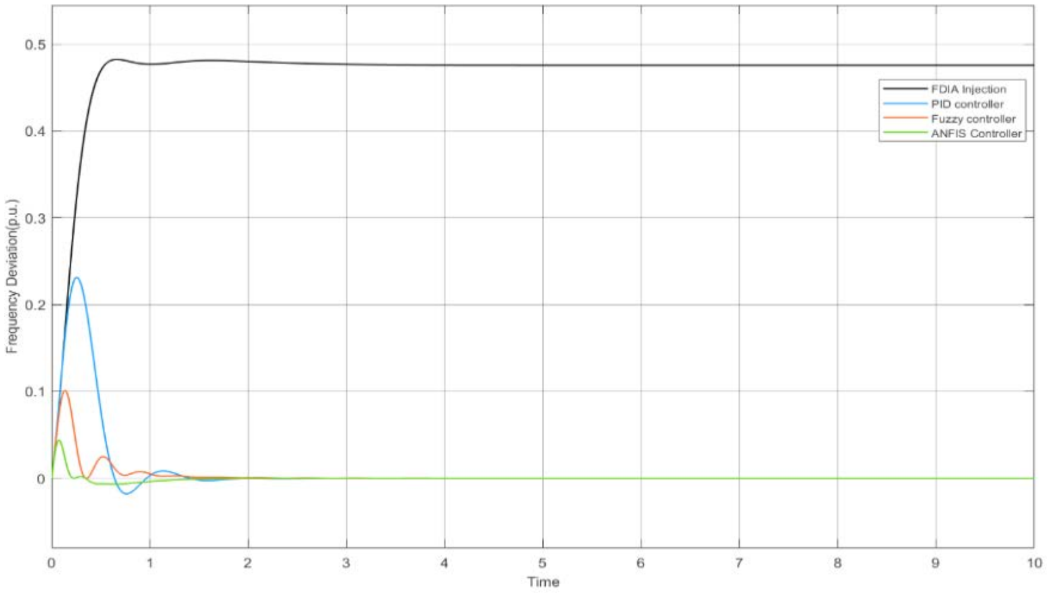

Figure 7: Comparison of system response in frequency deviation with Virtual InertiaSolar cell perturbation 0.2pu, Load disturbance 0.2pu, FDIA injection 0.5.

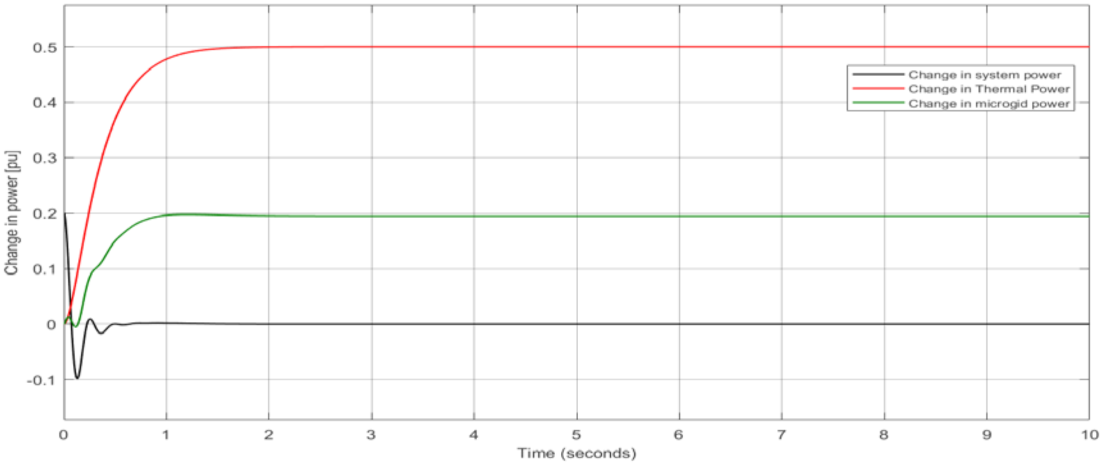

Figure 8: Response of change in thermal, system, and microgrid power

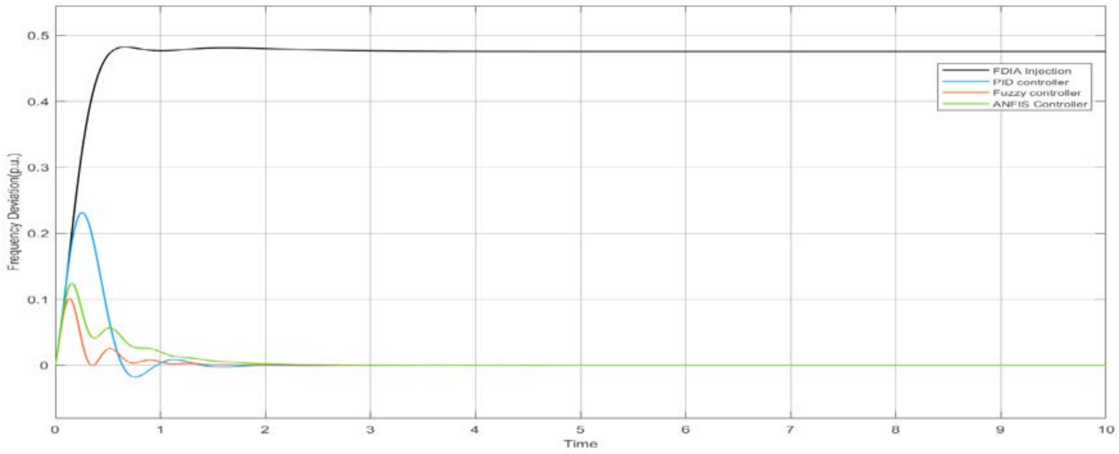

Figure 9: Comparison of system response in frequency deviation without Virtual InertiaSolar cell perturbation 0.2pu, Load disturbance 0.2pu, FDIA injection 0.5.

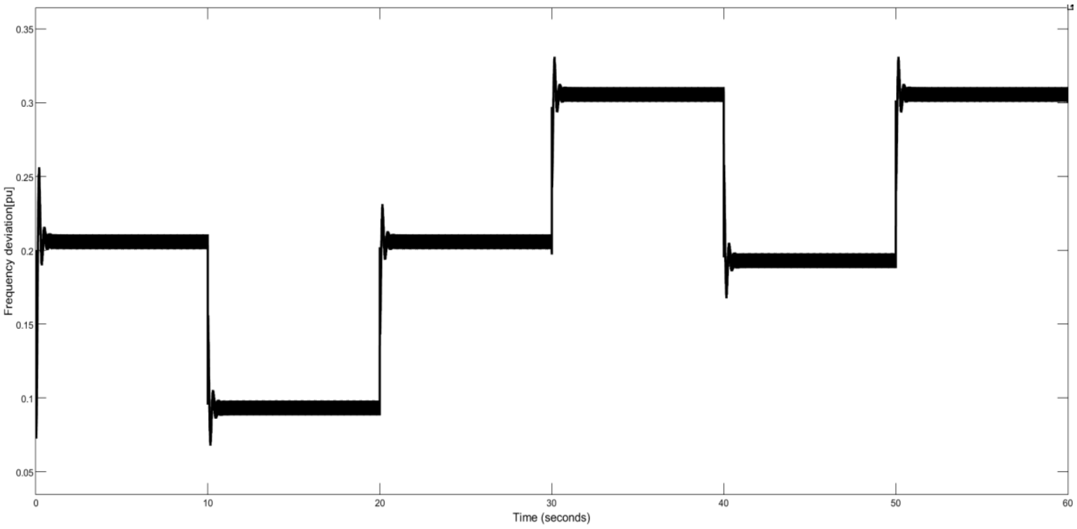

Figure 10: Random False data injection.

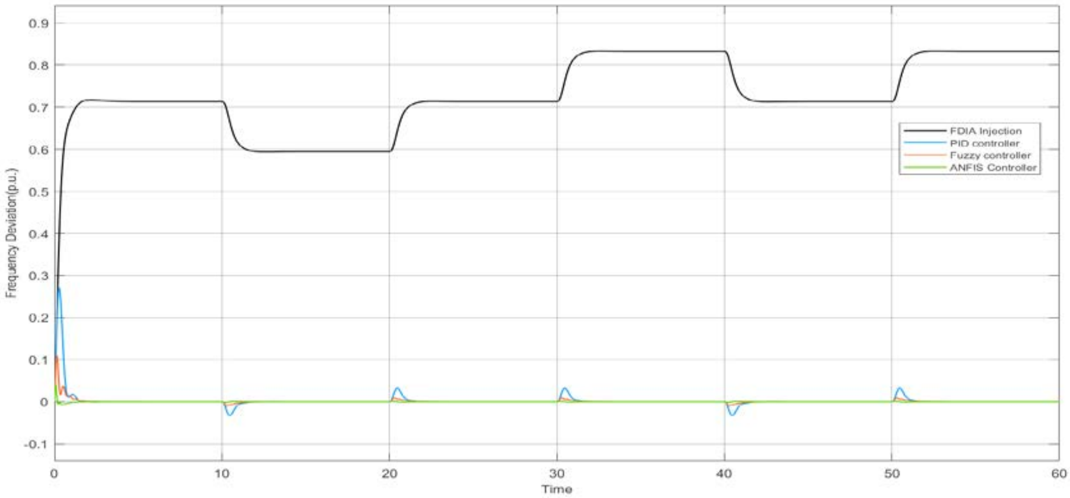

Figure 11: Comparison of system response in frequency deviation with Virtual Inertia in random disturbance

6. Discussion

ANFIS-based Virtual Inertia Load Frequency Control for a Single Area Power System with Microgrid is proposed in this study. The results of the suggested controller are compared to those of the regular PID controller and the fuzzy controller. In terms of peak overshoot, settling time, and steady-state error, the results show that the ANFIS-based LFC outperforms the conventional controller. False data on LFC are investigated using a unified attack strategy following the controller block to assure system security before hackers further degrade LFC performance.The Integral Square Error (ISE) value without controller is 10.76 when solar cell perturbation is 0.2pu, load disturbance is 0.2pu, and FDIA is 0.5, whereas with proposed controller ISE value is 0.0001885, with random FDIA disturbance. The ISE value is 32.9 without the controller and 0.0001604 with the suggested controller. The results show that the suggested ANFIS controller can handle FDIA injection while keeping the LFC constant.

7. References

[1] S. Pandey, S. Mohanty and N. Kishor, "A literature survey on load–frequency control for conventional and distribution generation power systems", *Renewable and Sustainable Energy Reviews*, vol. 25, pp. 318-334, 2013.

[2] S. Kayalvizhi and D. Vinod Kumar, "Load Frequency Control of an Isolated Micro Grid Using Fuzzy Adaptive Model Predictive Control", *IEEE Access*, vol. 5, pp. 16241-16251, 2017.

[3] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuña, and M. Castilla, “Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization,” IEEE Trans. Ind.Electron.vol. 58, no. 1, pp. 158–172, Jan. 2011

[4] D. Kumar, "Load Frequency Control for Two Area Power System Using Different Controllers", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, no. 3, pp. 1109-1115, 2013.

[5] Surya Prakash, and Sunil Kumar Sinha. LFC of Multi-area Power Systems Using Neuro-Fuzzy Hybrid Intelligent Controllers. IETE Journal of Research Apr 2015: 61(5): 526-532.

[6] Hossain M. J, Pota H. R, Mahmud M. A, and Aldeen M. Robust control for power sharing in MGs with low-inertia wind and PV generators. IEEE Trans. Sustain. Comput. July 2015; 6(3): 1067-1077.

[7] Saikia L.C, Nanda J, and Mishra S. Performance Comparison of Several Classical Controllers in AGC for Multi-area Interconnected Thermal System. International Journal of Electrical Power & Energy Systems 2011; 33(3):394-401.

[8] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control", *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580-591, 2014.

[9] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, “Cyber security analysis of state estimators in electric power systems,” in Proc. 49th IEEE Conf. Decision Control, Dec. 2010, pp. 5991–5998.

[10] C. Chen, K. Zhang, K. Yuan, L. Zhu and M. Qian, "Novel Detection Scheme Design Considering Cyber Attacks on Load Frequency Control", *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932-1941, 2018.

[11] N. ŽIVKOVIĆ and A. SARIĆ, "Detection of false data injection attacks using unscented Kalman filter", *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, 2018.

[12] S. Liu, X. P. Liu, and A. El Saddik, “Denial-of-service (DOS) attacks on load frequency control in smart grids,” in Proc. IEEE PES Innovative Smart Grid Technol. Conf., Feb. 2013, pp. 1–6.

[13] A. Sargolzaei, K. Yen, and M. Abdelghani, “Delayed inputs attack on load frequency control in smart grid,” in Proc. IEEE PES Innovative Smart Grid Technol. Conf., Feb. 2014, pp. 1–5.

[14] P. MohajerinEsfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, “Cyber attack in a two-area power system: Impact identification using reachability,” in Proc. 2010 Amer. Control Conf., Jun. 2010, pp. 962–967.

[15] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, “A robust policy for automatic generation control cyber attack in two area power network,” in Proc. 49th IEEE Conf. Decision Control, Dec. 2010, pp. 5973–5978.

[16] R. Tan et al., “Optimal false data injection attack against automatic generation control in power grids,” in Proc. 7th Int. Conf. Cyber-Phys. Syst., Apr. 2016, pp. 1–10

[17] S. Siddharth and G. Manimaran, “Model-based attack detection and mitigation for automatic generation control,” IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[18] P. Srikantha and D. Kundur, “Denial of service attacks and mitigation for stability in cyber-enabled power grid,” in Proc. IEEE PES Innovative Smart Grid Technol. Conf., Feb. 2015, pp. 1–5.

[19] Y. W. Law, T. Alpcan, and M. Palaniswami, “Security games for risk minimization in automatic generation control,” IEEE Trans. Power Syst., vol. 30, no. 1, pp. 223–232, Jan. 2015.

[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] A. Sargolzaei, K. Yen, and M. Abdelghani, “Delayed inputs attack on load frequency control in smart grid,” in Proc. IEEE PES Innovative Smart Grid Technol. Conf., Feb. 2014, pp. 1–5.

[22] C Sun, . Liu, and J. Xie, “Cyber-physical system security of a power grid: State-of-the-art,” Electronics, vol. 5, no. 3, p. 40, 2016.

[23] A. Afzalian, D.A. Linkens. “Training of neuro fuzzy power system stabilizers using genetic algorithms”. Int. J. Electr. Power Energy Syst., 22 (2) (2000), pp. 93-102.