Central Power Research Institute

Vol. 20(1)/01-06, June 2024
ISSN (Print) : 0973-0338
DOI : 10.33686/pwj.v20i1.1161

Power Research

Data Integrity Attacks and their Impact on Cyber-Physical Power System Control Applications

A. Lavanya[1], R. Akshaya[1], D. Sneha Latha[1], V. Bhuvanaa[1], K. Rajkumar[2] and S. Revathi[1]*

[1]Department of EEE, National Institute of Technology, Karaikal - 609609, Puducherry, India

[2]Department of ICE, National Institute of Technology, Tiruchirappalli, Trichy - 620015, Tamil Nadu, India; revathi.s@nitpy.ac.in

Abstract

This paper explores the vulnerability of two-area Automatic Generation Control (AGC) systems in smart grids to False Data Injection (FDI) attacks. The AGC system is modelled using state space equations, and its stability and performance are scrutinized under typical load variations. Utilizing MATLAB Simulink, various FDI attacks are introduced to assess their characteristics and potential consequences. The study emphasizes the critical significance of understanding diverse FDI attacks within the context of two-area AGC networks, underscoring their potential to induce malfunctions and blackouts. The findings highlight the need for heightened awareness of cybersecurity risks in AGC systems and emphasize the importance of fortifying these systems against potential threats to ensure the continued resilience and reliability of smart grids.

Keywords: Automatic Generation Control, False Data Injection Attack, Pulse, Ramp, Scale, Smart Grid, State Space Model, State Estimation Two-Area Power System, Step

1. Introduction

In the context of the evolving energy landscape, modern power grids have transitioned into complex and interconnected systems, facilitated by the implementation of smart grids. Utilizing advanced digital infrastructure, smart grids play a crucial role in meeting the escalating demand for electricity, merging physical components like generators and transmission systems with cyber layers. However, the increased reliance on communication networks in smart grids makes them prone to cyber-attacks, particularly on the Automatic Generation Control (AGC) systems responsible for balancing supply and demand.

This study delves into the vulnerability of AGC systems to False Data Injection (FDI) attacks, with a focus on two area networks. Employing a state-of-the-art modelling approach[1], we intricately characterize the AGC system through state space equations[2-4]. The literature extensively investigates power system vulnerabilities, emphasizing the cyber-physical interaction with SCADA.

This paper enhances current understanding by examining vulnerabilities in the AGC cyber-physical link, utilizing feasibility analysis and optimal control theory. Notably, our study, consistent with the referenced work, by Vrakopoulou *et al.*[5], deliberately excludes emphasis on cryptographic measures for AGC systems. Instead, we concentrate on understanding False Data Injection (FDI) attacks and fortifying AGC systems without relying on cryptographic functions, thereby contributing to the broader discourse on cybersecurity in power systems. This approach allows us to isolate vulnerabilities, assess potential attacks, and focus on understanding security measures in contemporary systems. This paper investigates the impact of targeted frequency-based attacks on system load variations through a simulation-based approach. By specifically manipulating simulated frequency parameters, we emulate real-world disturbances, enabling a comprehensive analysis of the system's resilience and dynamic response under varying loads while mitigating risks to the physical infrastructure in Various FDI attack scenarios[5-7] are meticulously designed and analyzed, encompassing both individual attacks and coordinated strategies[8].

The objective is to comprehensively understand the impact of FDI attacks on the AGC system, emphasizing

*Author for correspondence

the importance of detecting and mitigating these threats for the resilience and security of smart grids. Our findings illuminate diverse possibilities associated with FDI attacks, contributing valuable insights to safeguarding the integrity of modern power grid systems.

2. System Description

2.1 Two-Area AGC System Model

A two-area AGC power system model is a simplified representation of a real power system that consists of two interconnected areas. Each area has its generators and loads, and the two areas are connected by a high-voltage tie-line. The AGC system is responsible for maintaining the frequency of the system and the power flow on the tie-line within predefined limits[9-10].

This helps to ensure the reliable and efficient operation of the power system. Figure 1 shows a diagram of a two-area AGC power system model.

The AGC system monitors the frequency and power flow on the tie-line and sends signals to the generators in each area to adjust their output as needed.

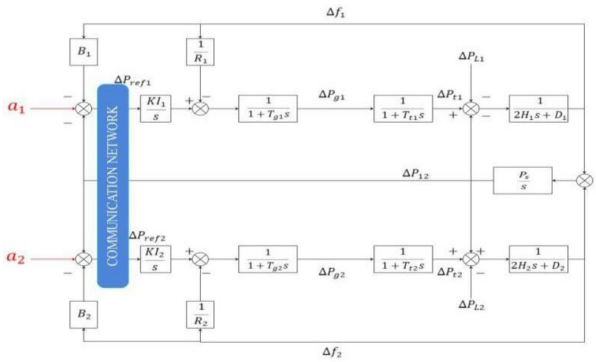

Figure 1. Two area AGC system.

This helps to maintain the frequency and power flow within the predefined limits. And a1 and a2 are considered as the attacking points in area 1 and area 2 respectively. Figure 1 shows the Two-area AGC system.

2.2 State Space Modelling

The state space model can be used to predict the behaviour of the system under different operating conditions and to design and implement control systems for the system. In other words, a state space model for a two-area AGC system is a powerful tool that can be used to understand and control the system. It is used by power system engineers to design and operate power systems safely and efficiently. A state space model is a mathematical representation of a dynamic system in which nine states are obtained:

x1=Δf1= Frequency deviation of area 1 in per units
x2=ΔPg1=Change in mechanical power of governor 1
x3=ΔPt1=Change in valve setting of Turbine 1
x4=ΔPref1= Change in Pref of area 1
x5=ΔP12= Tie-line power deviation
x6=Δf2=Frequency deviation of area 2
x7= ΔPg2=Change in mechanical power of governor 2
x8=ΔPt2=Change in valve setting of Turbine 2
x9=ΔPref2= Change in Pref of area 2

The attacker can manipulate the false data injections in such a way that the ACEs in each area appear to be within normal limits, even though the system is actually under attack. This makes it difficult to detect coordinated FDI attacks using traditional methods. To address this limitation, researchers have proposed several new methods for detecting coordinated FDI attacks. These methods typically involve using more sophisticated data analysis techniques, such as machine learning and statistical methods.

To illustrate this, consider the following coordinated FDI attack on the 2-area system illustrated in this paper:

$$\dot{x} = A_0 x + B_0 u + w$$

$$y = Cx + v$$

where,

$$X=\Delta f_1 \quad \Delta P_{g1} \quad \Delta P_{t1} \quad \Delta P_{ref1} \quad \Delta P_{l2} \quad \Delta Pf_2 \quad \Delta P_{g2} \quad \Delta P_{t2} \quad \Delta P_{ref2}]^T$$

$$u= [u1\ u2]^T$$

where, u is input, u_1, and u_2 are load disturbance of area 1 and area 2, respectively.

$$y= [\Delta f_1\ \Delta f_1]$$

where, y is output, $\Delta \boldsymbol{f}_1$ and $\Delta \boldsymbol{f}_2$ are frequency deviation of area 1 and area 2, respectively The derived State Space equations:

$$\dot{x}_1 = \Delta \dot{f}_1(t) = \frac{-D}{2H_1}\Delta f_1(t) + \frac{1}{2H_1}\Delta P_{g1}(t) - \frac{1}{2H_1}\Delta P_{t1}(t) - \frac{1}{2H_1}\Delta P_{12}(t) \quad (1)$$

$$\dot{x}_2 = \Delta \dot{P}_{g1}(t) = \frac{-1}{T_{t1}}\Delta P_{g1}(t) + \frac{1}{T_{t1}}\Delta P_{g1}(t) \quad (2)$$

$$\dot{x}_3 = \Delta\dot{P}_{t1}(t) = \frac{-1}{T_{g1}}\Delta P_{t1}(t) + \frac{1}{T_{g1}}\Delta P_{ref1}(t) - \frac{1}{R_1 T_{g1}}\Delta f_1(t) \quad (3)$$

$$\dot{x}_4 = \Delta\dot{P}_{ref1}(t) = -K_{I1}B_1\Delta f_1(t) - K_{I1}\Delta P_{12}(t) \quad (4)$$

$$\dot{x}_5 = \Delta\dot{P}_{12}(t) = -P_S\Delta f_1(t) - P_S\Delta F_2(t) \quad (5)$$

$$P_S = \frac{E_1 E_2}{X_{12}}\cos(\delta_{10} - \delta_{20})$$

$$\dot{x}_6 = \Delta\dot{f}_2(t) = \frac{-D}{2H_2}\Delta f_2(t) - \frac{1}{2H_1}\Delta P_{t2}(t) + \frac{1}{2H_2}\Delta P_{12}(t) \quad (6)$$

$$\dot{x}_7 = \Delta\dot{P}_{g2}(t) = \frac{-1}{T_{t2}}\Delta P_{g2}(t) + \frac{1}{T_{t2}}\Delta P_{t2}(t) \quad (7)$$

$$\dot{x}_8 = \Delta\dot{P}_{t2}(t) = \frac{-1}{T_{g2}}\Delta P_{t2}(t) + \frac{1}{T_{g2}}\Delta P_{ref2}(t) - f_2\frac{1}{R_2 T_{g2}}\Delta(t) \quad (8)$$

$$\dot{x}_9 = \Delta\dot{P}_{ref2}(t) = -K_{I2}B_2\Delta f_2(t) - K_{I2}\Delta P_{12}(t) \quad (9)$$

The resulting A, B, C, D matrices are formed and given below:

$$A = \begin{bmatrix} \frac{-D}{2H_1} & \frac{1}{2H_1} & 0 & 0 & \frac{-1}{2H_1} & 0 & 0 & 0 & 0 \\ 0 & \frac{-1}{T_{t1}} & \frac{1}{T_{t1}} & 0 & 0 & 0 & 0 & 0 & 0 \\ -\frac{-1}{R_1 T_{g1}} & 0 & \frac{-1}{T_{g1}} & \frac{1}{T_{g1}} & 0 & 0 & 0 & 0 & 0 \\ -K_{I1}B_1 & 0 & 0 & 0 & -K_{I1} & 0 & 0 & 0 & 0 \\ P_s & 0 & 0 & 0 & 0 & -P_s & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2H_2} & \frac{-D}{2H_2} & \frac{1}{2H_2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{-1}{T_{t2}} & \frac{1}{T_{t2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{R_2 T_{g2}} & 0 & \frac{-1}{T_{g2}} & \frac{1}{T_{g2}} \\ 0 & 0 & 0 & 0 & K_{I2} & -K_{I2}B_2 & 0 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} \frac{-1}{2H_1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{-1}{2H_2} & 0 & 0 & 0 \end{bmatrix}^T$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$D = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

3. Modelling of FDI Attack

False Data Injection attack (FDI) is carried out by flooding the communication signal with random illegitimate data signals.

The following areas are vulnerable to cyber-attacks:

1. The frequency measurement in area 1
2. The frequency measurement in area 2
3. The tie line power measurement

The modelling of the FDI attack is given as:

$$\dot{x} = A\dot{x} + Bu + Baa + w$$

$$y = C\dot{x} + Du + v$$

Attack matrix Ba=

$$\begin{bmatrix} \frac{-1}{2H_1} & 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{-1}{2H_2} & 0 & 0 & \lambda_2 \end{bmatrix}^T$$

where, the attack vector, a = $[a_1\ a_2]^T$ and a1 and a2 are the biases in frequency measurement in area 1 and area 2, respectively; w is the process noise, v is the measurement noise, and the values of $\lambda_1 = \lambda_2 =$ 0.05. The A, B and C matrices are the same as given in the previous section.

D = zeros(size(C,1), size(B,2))

4. Results and Discussion

The parameters of the two-area AGC system considered for this work are specified in Table 1.

Table 1. Parameters of the two area AGC system

Para meters	*Description*	*Area 1*	*Area 2*
R	Speed droop, pu	R1 = 0.05	R2 = 0.0625
D	Freq. sensitive load coefficient, pu	D1 = 0.6	D2 = 0.9
H	Inertia constant, s	H1 = 5	H2 = 4
Tg	Time constant of governor, s	Tg1 = 0.2	Tg2 = 0.3
Tt	Time constant of turbine, s	Tt1 = 0.5	Tt2 = 0.6
B	Bias factor	B1 = 20.6	B2 = 16.9
Ps	Synchronizing power co- efficient	Ps = 2.0	

The simulation of FDI attacks with ramp, scale, pulse, step, and coordinated signals was carried out, and the response of the two-area AGC system was analyzed. The analysis is described in this section.

Scenario 1: **Ramp attack** - The term "ramp" indicates a smooth and continuous change in the measured data, unlike sudden spikes or erratic variations. Figure 2 illustrates a ramp attack, showing changes in tie line power and frequency deviations (Δf) in both area 1 and area 2.

A load change of 0–0.2 at 25s was in area 1, and a ramp signal of slope 0.0025 at 27s was injected in area 1.

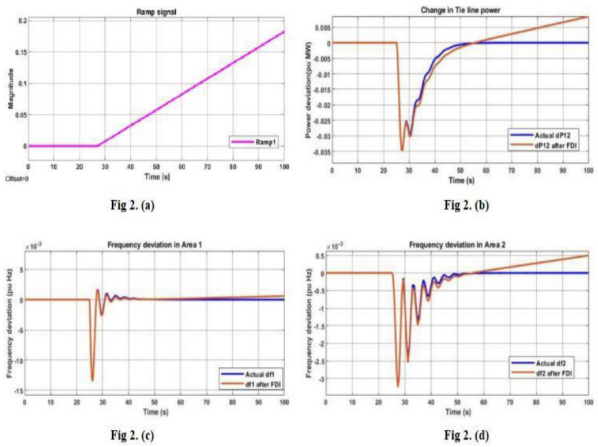

Figure 2. **(a)** Ramp signal, **(b)** Change in tie line power, **(c)** Δf in area 1, **(d)** Δf in area 2.

Scenario 2: **Scale attack** - The term "scale" means either to amplify or reduce the real signal. A load change of 0–0.35 at 5s was given in area 2, followed by a scale attack, which is a quadratic signal with a consistent alteration reaching 0.25 at 5s. The following Figure 3 illustrates a scale attack, showing changes in tie line power and frequency deviations (Δf) in both area 1 and area 2.

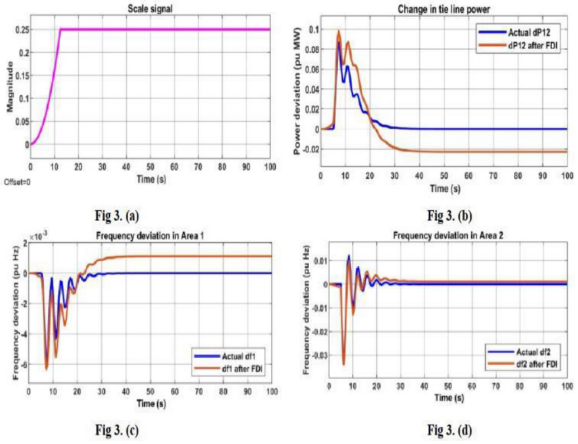

Figure 3. **(a)** Scale signal, **(b)** Change in tie line power, **(c)** Δf in area 1, **(d)** Δf in area 2.

Scenario 3: **Pulse attack** - This attack involves adding a very short pulse to the real measurement.

This attack is considered to be a special type of random attack. The given load change in system area 1 is 0 to 0.3 at 3s. The Figure 4 shows the pulse attack is injected at 5s and is of 0.25 magnitude in area 1. The time duration of the attack was 5s to 25s.

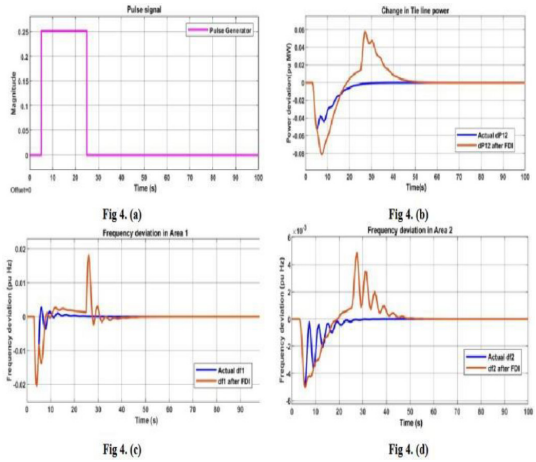

Figure 4. **(a)** Pulse signal, **(b)** Change in tie line power, **(c)** Δf in area 1, **(d)** Δf in area 2.

Scenario 4: **Step attack** - This attack involves either stepping up or increasing the value or stepping down or decreasing the value. The following Figure 5 and 6 shows step up and step

down attack, showing changes in tie line power and frequency deviations (Δf) in both area 1 and area 2.

Case 1: A load change of 0.2 is given at 25 s in area 1. The step attack of magnitude 0.2 is injected at 27s.

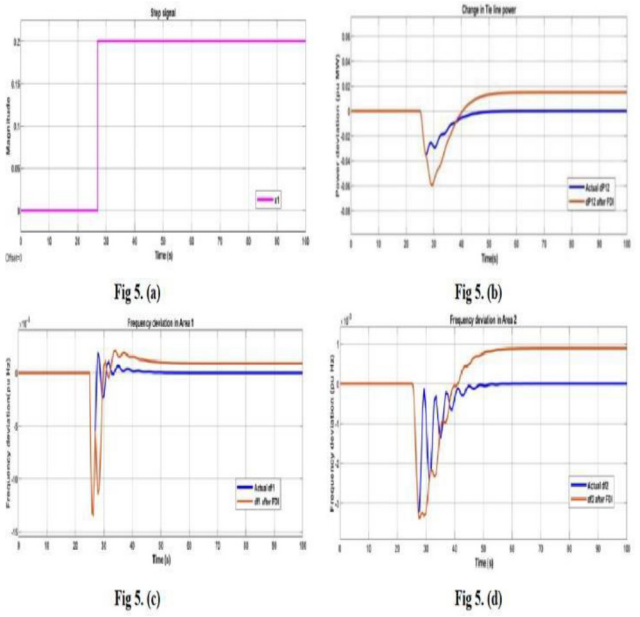

Figure 5. **(a)** Step up signal, **(b)** Change in tie line power, **(c)** Δf in area 1, **(d)** Δf in area 2.

Case 2: The load change is 0.25 given at 25s in area 2. The step attack of magnitude -0.3 is injected at 27 s in area 2.

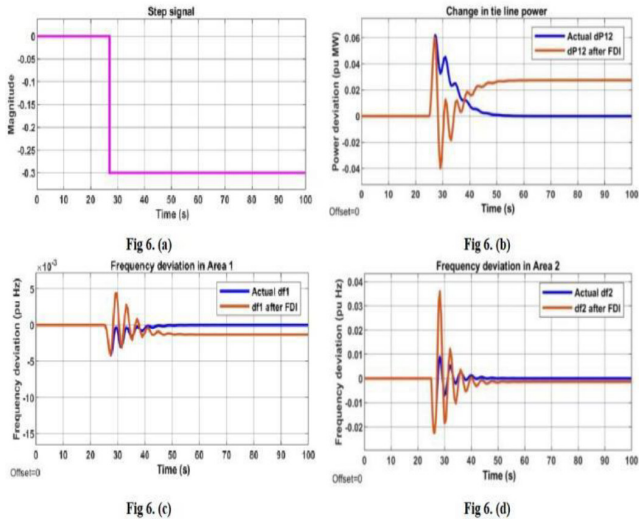

Figure 6. **(a)** Step down signal, **(b)** Change in tie line power, **(c)** Δf in area 1, **(d)** Δf in area 2.

Scenario 5: **Coordinated ramp and pulse attack** - At 0 seconds, a load change of 0.2 occurs in area 1, while area 2 experiences a load change of 0.18. An attack is introduced in area 2 with a ramp slope of 0.005 and an upper signal limit of 0.25 at 5 seconds. Additionally, a pulse signal with a magnitude of 0.25 is applied between 100 seconds and 110 seconds. Figure 7 depicts the coordinated ramp and pulse attack, showing changes in tie line power and frequency deviations (Δf) in both area 1 and area 2.

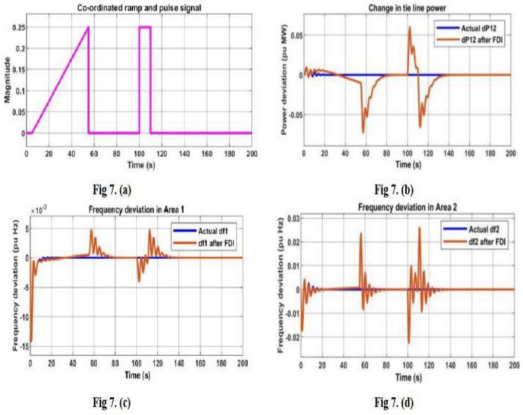

Figure 7. **(a)** Coordinated ramp and pulse signal, **(b)** Change in tie line power, **(c)** Δf in area 1, **(d)** Δf in area 2.

Scenario 6: **Co-ordinated scale and step attack** - A load change of 0.2 at 0s is given in area 1. The attack is injected into Area 1. A scale signal of magnitude 0.8 is given at 5s, followed by a step-up signal of magnitude 0.08 at 100s. Figure 8 depicts the Co-ordinated scale and step attack, showing changes in tie line power and frequency deviations (Δf) in both area 1 and area 2.

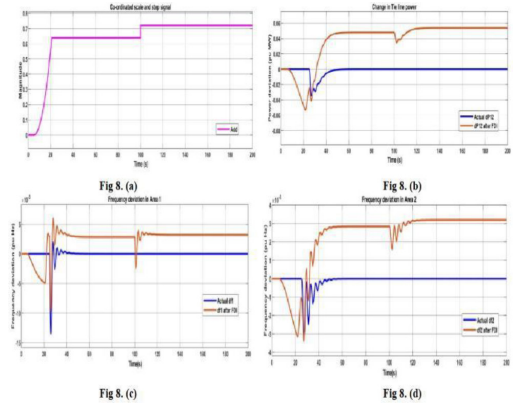

Figure 8. **(a)** Coordinated scale and step signal, **(b)** Change in tie line power, **(c)** Δf in area 1, **(d)** Δf in area 2.

5. Conclusion

In this paper, the two-area AGC system has been modelled and the state space equations are derived. The modelling of FDI attack has been done in MATLAB and has been interfaced with the two-area AGC system. Then the changes in the system are analyzed when a small load change is applied under normal conditions. A small external disturbance was created in the original data, and the basic FDI attack characteristics were observed. This paper emphasizes the need to clearly understand all possible FDI attacks to detect them. In conclusion, the proposed analysis should help to develop better FDI attack detection and mitigation strategies for two area AGC systems.

The proposed analysis aims to contribute to the advancement of FDI attack detection and mitigation strategies for AGC systems. By scrutinizing the characteristics of different attack types, including sophisticated coordinated attacks, the research provides valuable insights for enhancing the cybersecurity resilience of power system control applications. The conclusion underscores the importance of proactive measures and adaptive strategies to bolster AGC systems against potential cyber threats in the context of smart grids.

6. References

1. Pillai AG, Samuel ER, Unnikrishnan A. Optimal load frequency control through combined state and control gain estimation for noisy measurements. Protect Cont Modern Pow Syst. 2020; 5(1). https://doi.org/10.1186/s41601-020-00169-5
2. Magzoub MA, Alquthami T. Optimal design of automatic generation control based on simulated annealing in interconnected two-area power system using hybrid PID-fuzzy control. Energies. 2022; 15(4):1540. https://doi.org/10.3390/en15041540
3. Talukdar BK, Debnath R, Dutta S, Kumar B, Das M. Design of state space model and optimal controller for automatic generation control of two area thermal power system. Int J Adv Res Innov Ideas Edu. 2018; 4(3):1552-8650.
4. Vidya SP, Rayalu MSK. State-space approach of automatic generation control of two-area multi- source power systems. Proc Int Conf Comput Intell Sustain Technol; 2022. p. 453-63. https://doi.org/10.1007/978-981-16-6893-7_41
5. Vrakopoulou M, Esfahani PM, Margellos K, Lygeros J, Andersson G. Cyber-attacks in the automatic generation control. Pow Syst. 2015;303-28. https://doi.org/10.1007/978-3-662-45928-7_11
6. Bi W, Zhang K, Chen CY. Cyber-attack detection scheme for a load frequency control system based on dual-source data of compromised variables. Appl Sci. 2021; 11(4):1584-4. https://doi.org/10.3390/app11041584
7. Patel A, Purwar S. Event-triggered detection of cyberattacks on load frequency control. IET Cyber- Physical Systems: Theory and Applications. 2020; 5(3):263-73. https://doi.org/10.1049/iet- cps.2019.0067
8. He X, Liu X, Li P. Coordinated false data injection attacks in AGC system and its countermeasure. IEEE Access. 2020; 8:191167-76.
9. Ayad A, Khalaf M, El-Saadany EF. Detection of false data injection attacks in automatic generation control systems considering system nonlinearities. IEEE Elect Pow Energ Conf (EPEC), Canada: Toronto, 2018 Oct 10-11; 2018. https://doi.org/10.1109/EPEC.2018.8598328 PMid:30241179
10. 10. An A, Lin J, Cheng C, Zhu W. Distributed model predictive control for two-area interconnected power system. IOP Conf Series Earth Environ Sci. 2018; 186:012008-8. https://doi.org/10.1088/1755- 1315/186/4/012008