JOURNAL OF NANO- AND ELECTRONIC PHYSICS
Vol. **13** No 3, 03030(4pp) (2021)

ЖУРНАЛ НАНО- ТА ЕЛЕКТРОННОЇ ФІЗИКИ
Том **13** № 3, 03030(4cc) (2021)

A Novel Security Unit with Mitigating Frequency Deviation for Interconnected Power System Considering Cyberattack

J. Mondal[1], F.R. Badal[2], Z. Nayem[2], D. Chakraborty[3], T. Hossain[3], M.D. Arifuzzaman[4], N. Mondol[5], S.K. Das[2]

[1] *Bangabandhu Sheikh Mujibur Rahman Science & Technology University, Gopalganj-8100, Bangladesh*
[2] *Rajshahi University of Engineering & Technology, Rajshahi-6204, Bangladesh*
[3] *American International University Bangladesh, Bangladesh*
[4] *Varendra University, Rajshahi, Bangladesh*
[5] *Khulna University of Engineering & Technology, Khulna, Bangladesh*

(Received 10 January 2021; revised manuscript received 14 June 2021; published online 25 June 2021)

Interconnected power system is a promising source of electric power that fulfils the excess demand of electricity throughout the world whose safe and reliable operation is necessary for decreasing load-shedding and increasing resiliency. The development of information and communication technology (ICT) not only blessing for us but also hampers our technology by promoting cyber-crime. Cyber-attack (CA) on power system is now becoming a common problem that produces unauthorized access to the control unit of power system and hampers the whole system partially or completely by changing the sensitive data of power system and control unit. The performance of the power system is regulated by employing a fractional-order-proportional-integral-derivative (FPID) controller and is compared with conventional PID controller in this paper. The reliable performance of the power system completely depends on the efficient design of controller, but the parameters of the controller are largely affected by the CA and damage the whole system. Any change of the control unit or the system parameters may decrease the resiliency and the stability of the power system. An automatic cyber-attack mitigation technique (ACAMU) has been proposed in this article to completely mitigate the CA and its impact on the system and controller to enhance the security and resiliency of power system by maintaining a fixed data for both system and controller.

Keywords: Interconnected power system, FPID controller, Cyber-attack, Security unit.

DOI: 10.21272/jnep.13(3).03030 PACS numbers: 07.05.Tp, 07.07.Tw

1. INTRODUCTION

The growing rate of electricity demand due to modernization of the world is becoming a big challenge throughout the world. Interconnected power system (INPS) is a promising solution that produces power by using fossil fuel as well as renewable energies to meet this excess demand of electricity. Several subsystems are connected through transmission line, called tie line to construct the INPS. Each area has its own production capacity to meet its load demand and also deliver power to another area while power shortage [1-4].

The proper and efficient control of frequency of each area and tie line delivered power is the main concern of power system to enhance the reliability and resiliency. Any change in supply to demand ratio or in the equipment parameters, the nominal frequency and tie line power of INPS may be deviated from its nominal value that are responsible to load-shedding, damage the connected load, unstable the operation of power system. Load frequency control (LFC) technique with proper controller is employed in the power system to mitigate the load and parameter changing problem and return the frequency and power deviation to the zero level [5].

Cyber-security is the major concern of power system that need to be controlled properly. The CA on U.S. gas pipeline and smart grid as well as the attack on Ukraine power system indicate the frequent and regular attack on the power system to breakdown the overall system [6-8]. Unauthorized access to the control unit, collecting and changing the sensitive data on which the overall system depends are the main interest of the cyber attacker to decrease the production level and resiliency and increase the overall cost. As well as, the uncontrolled changing of the system parameters increases the frequency and power deviation [9].

To mitigate the problems of CA in single area power system, a controlled switching unit has been proposed in [10] that investigates the impact of positive and negative biased CA on LFC. Ref. [11] investigated a review of the performance against CA for smart grid and identifies the areas where CA may occur. False data injection in the power system during CA has been investigated in [12]. By understanding the behavior of the circuit breaker, protection devices and logics, the CA on the parameters and settings of the system can be mitigated [13]. A transformation-based algorithm has been proposed based on Kull back Leibler distance measurement to find the modification or injection of false data into the smart grid [14].

All of these aforementioned papers have investigated the CA impacts on single area power system. This paper analyses the performance of INPS by changing the system parameters in case of CA. The objective of this article is to investigate the system's performance with the aid of fractional-order proportional integral derivative (FPID) controller and compare its results with PID controller initially. Since, the system and the controller parameters are the main target of the cyber attacker to change their data and damage the system, the proposing of an automatic cyber-attack mitigation unit (ACAMU) is the main contribution of this paper to

The results were presented at the International Conference on Innovative Research in Renewable Energy Technologies (IRRET-2021) mitigate the change of the system and controller parameters by maintaining a fixed data for ensuring reliable and secure operation of INPS.

The remaining article is arranged as follows: system modeling and problem issues are discussed in Section 2 while Section 3 proposes the control technique of CA. Section 4 investigates the performance of the proposed system and conclusion is carried out in Section 5.

2. SYSTEM MODELING AND PROBLEM STATEMENT

The modeling and related problems of INPS has been studied in this section. The minimizing of frequency and power deviation is done by incorporating two control-loop. Primary control loop mitigates the change of load and secondary control loop returns these deviations to zero level. The dynamic modeling of INPS, as shown in Fig. 1, can be represented by power system,

$$\Delta \dot{f}_1 = \frac{d_1}{m_1}\left\{\frac{1}{d_1}\Delta m_1 - \frac{1}{d_1}\Delta l_1 - \Delta f_1 - \frac{1}{d_1}\Delta p_{12}\right\}, \tag{2.1}$$

$$\Delta \dot{g}_1 = \frac{1}{X_{g1}}\left\{\Delta c_1 - \Delta g_1 - \frac{1}{R_1}\Delta f_1\right\}, \tag{2.2}$$

$$\Delta \dot{m}_1 = \frac{1}{X_{t1}}\{\Delta g_1 - \Delta m_1\}, \tag{2.3}$$

$$\Delta \dot{p}_{12} = S_p\{\Delta f_1 - \Delta f_1\}, \tag{2.4}$$

$$\Delta \dot{m}_2 = \frac{1}{X_{t2}}\{\Delta g_2 - \Delta m_2\}, \tag{2.5}$$

$$\Delta \dot{g}_2 = \frac{1}{X_{g2}}\left\{\Delta c_2 - \Delta g_2 - \frac{1}{R_2}\Delta f_2\right\}, \tag{2.6}$$

$$\Delta \dot{f}_2 = \frac{d_2}{m_2}\left\{\frac{1}{d_2}\Delta m_2 - \frac{1}{d_2}\Delta l_2 - \Delta f_2 + \frac{1}{d_2}\Delta p_{12}\right\}. \tag{2.7}$$

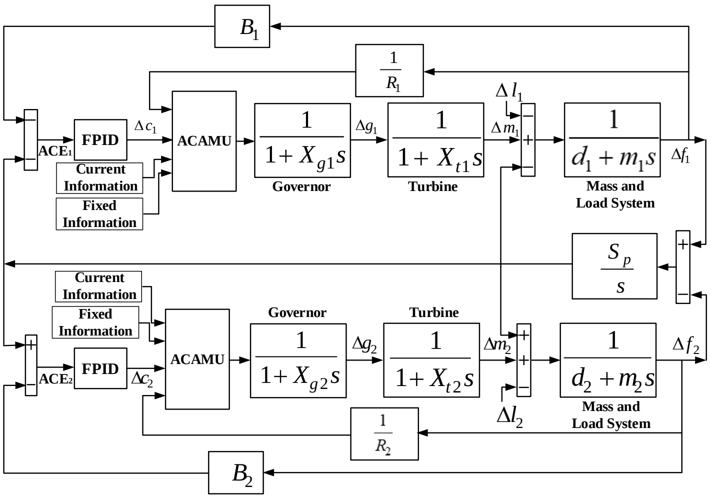

Fig. 1 – Control structure of interconnected power system

The parameters value is listed in Table 1. The open-loop system performance has been investigated in Fig. 2 that exhibits unstable operation of power system. To stabilize and make the frequency and power deviation to zero, FPID controller has been employed whose transfer function can be given as,

$$C(s) = K_p + K_i S^{-u} + K_d S^{-v}, \tag{2.8}$$

where, K_p, K_i and K_d are proportional, integral and derivative gain as well as u and v are integrator and differentiator order that improves the system performance as compared to conventional PID controller. In this modeling, the speed regulator R and the variables of FPID controller are the sensitive parameters on which whole system performance depends. Any change of these parameters increases the performance deviation and unstable the system operation. Thus, these parameters attract the attention of cyber attacker.

3. CYBER-ATTACK MITIGATION TECHNIQUE

To eliminate the unauthorized change of the sensitive parameters of R and controller, an automatic cyber-attack mitigation unit has been proposed here. This control approach consists of hardware and network unit where all sensitive data are fixed in a hardware. The ACAMU only can read the data from this hardware but cannot write or update any hardware information. This hardware is not connected to the power system through on-line. The ACAMU always monitors the present value of the sensitive network data and finds the difference between present and fixed value. If it finds no change between them, then the control action of ACAMU is turned off and permits normal operation of the system. If there is any difference between the present monitored data and hardware fixed data, the control action of ACAMU is turned on and produced an error signal that is minimized to zero by control action of ACAMU and fed data to the system equal to the hardware fixed data. Thus, the changes of sensitive data can be overcome and ensure a reliable and stable performance power system.

4. PERFORMANCE EVALUATION

The open-loop system response exhibits unstable operation of power system which is controlled by implementing FPID controller is shown in Fig. 2 whose parameters value is listed in Table 2. Though, the FPID controller minimizes the deviations of frequency and power, but any change of speed regulator R, biasing factor or control parameters is responsible to increase these deviations. The change of R or biasing factor is responsible to change the governor speed. Again, the cyber attacker may also change the controller parameters which changes the area control error (ACE).

Fig. 3 investigates the performance of system with varying system parameters. Though the controller minimizes the frequency and power deviations, but the change of R may unstable the system during CA. It indicates the essentiality of ACAMU. A case is investigated by choosing the affected and fixed data for both R and controller that is listed in Table 2 which ensures that the ACAMU eliminates the change of parameters value and makes the system secure and gives a fixed performance as before CA, as shown in Fig. 4. The comparison of FPID with PID controller is investigated in Fig. 4 that exhibits smallest overshoot, rise time, settling time and steady-state error for FPID controller. From Fig. 4, it can be investigated that the FPID controller takes the system to the transient response within minimum time and minimizes the system's deviation to zero as compared to conventional PID controller that ensures better and reliable performance of FPID controller.

Table 1 – Fixed parameter value of interconnected power system for nominal operation

Area	R	m	d	X_g	X_t	S_p	Δl
Area-1	0.05	10	0.6	0.2	0.5	0	0.2
Area-2	0.0625	8	0.9	0.3	0.6	2	0

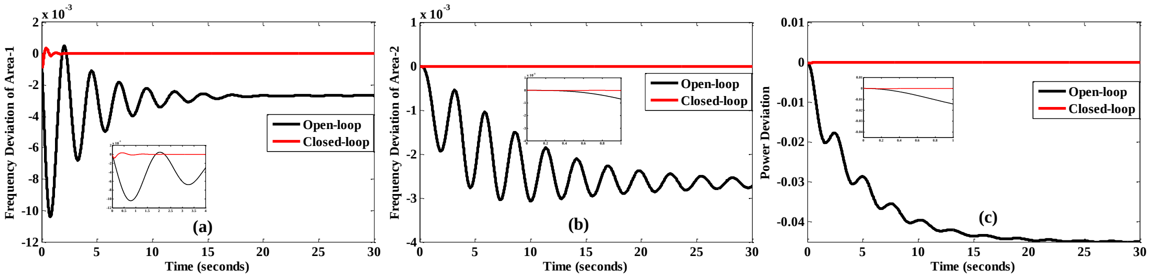

Fig. 2 – Frequency deviation: area-1 (a), area-2 (b), and tie line power deviation (c)

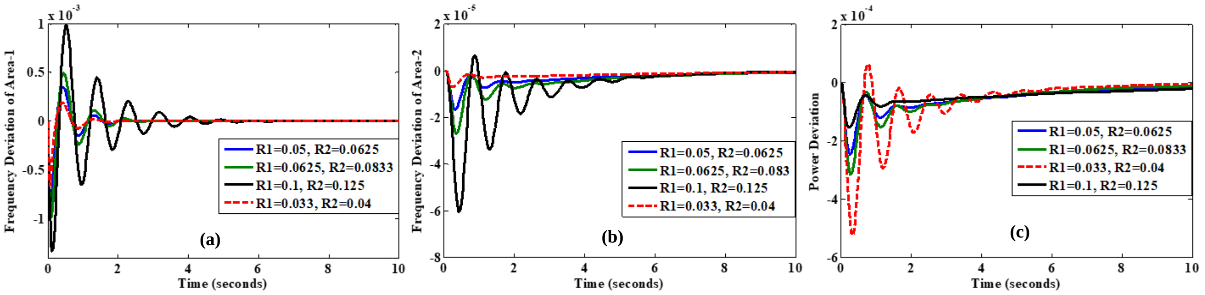

Fig. 3 – Frequency deviation: area-1 (a), area-2 (b), and tie line power deviation (c) due to the change of R during cyber-attack with FPID controller

Table 2 – Fixed and choosing affected data of the sensitive parameters

Data Type	R_1	R_2	K_{p1}	K_{p2}	K_{i1}	K_{i2}	K_{d1}	K_{d2}	u_1	u_2	v_1	v_2
Affected Data	0.0625	0.083	50	20	70	0.01	50	1	0.7	1	1.5	1.9
Fixed FPID	0.05	0.0625	100	15	150	0.01	5	5	0.995	2	1.5	1.5
Fixed PID	0.05	0.0625	3.5	4	6	2	2	2	–	–	–	–

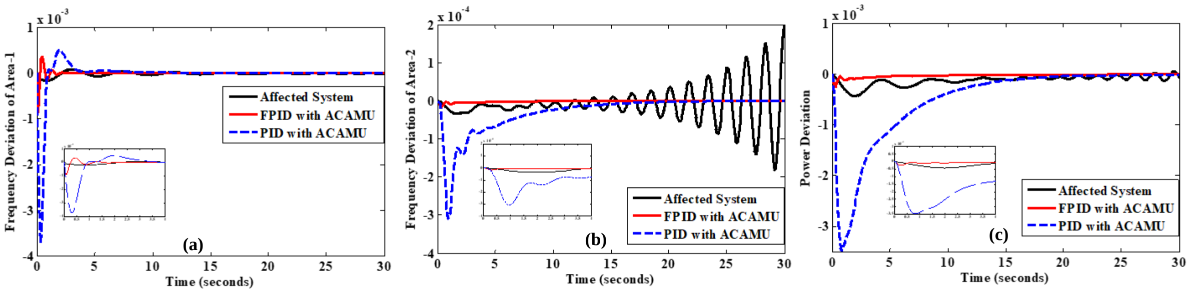

Fig. 4 – Frequency deviation: area-1 (a), area-2 (b), and tie line power deviation (c) with ACAMU, FPID and PID controller during cyber-attack

5. CONCLUSIONS

The cyber security issue in the power system is an important factor that needs to be continuously and efficiently controlled. The cyber attacker may damage the whole power system by changing the system parameters by using communication network. This paper presents a cyber-attack mitigation approach for interconnected power system with FPID and PID controller that efficiently overcome the problems generated by cyber-attack and increases system reliability, resiliency, and stability. The comparison between FPID and PID ensures better flexibility, stability of FPID controller.

REFERENCES

1. P.K. Mohanty, B.K. Sahu, T.K. Pati, S. Panda, S.K. Kar, *IET Generation Transmission & Distribution* **10**, 3764 (2016).
2. F.R. Badal, P. Das, S.K. Sarker, S.K. Das*, Protection and Control of Modern Power Systems* **4**, 1 (2019).
3. S.K. Sarker, F.R. Badal, S.K. Das, M. Yuan, *3rd International Conference on Electrical Information and Communication Technology (EICT),* 1 (2017).
4. S.K. Sarker, F.R. Badal, S.K. Das, *International Journal of Dynamics and Control* **6**, 1207 (2018).
5. N. Chuang, *IET Control Theory & Applications* **10**, 67 (2016).
6. *Stuxnet Style Attack on US Smart Grid* (2018).
7. *Ukraine's Power Outage Was a Cyber Attack: Ukrenergo* (2017).
8. *US Gas Pipeline Hit by Cyber Attack* (2018).
9. A.K. Thirukkovulur, H. Nandagopal, V. Parivallal, *IEEE International Conference on Computational Intelligence and Computing Research,* 1 (IEEE: 2012).
10. M. Hassan, N. Roy, M. Sahabuddin, *2nd International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE),* 1 (IEEE: 2016).
11. Y. Wadhawan, A. AlMajali, C. Neuman, *Electronics* **7**, 249 (2018).
12. R. Deng, G. Xiao, R. Lu, H. Liang, A.V. Vasilakos, *IEEE Trans. Ind. Inform.* **13**, 411 (2016).
13. X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, Z. Li*, IEEE Trans. Smart Grid* **8**, 572 (2016).
14. S.K. Singh, K. Khanna, R. Bose, B.K. Panigrahi, A. Joshi, *IEEE Trans. Ind. Inform.* **14** (1), 89 (2018).

Новий блок системи безпеки зі зменшенням відхилення частоти для об'єднаної енергосистеми з урахуванням кібератак

J. Mondal[1], F.R. Badal[2], Z. Nayem[2], D. Chakraborty[3], T. Hossain[3], M.D. Arifuzzaman[4], N. Mondol[5], S.K. Das[2]

[1] *Bangabandhu Sheikh Mujibur Rahman Science & Technology University, Gopalganj-8100, Bangladesh*
[2] *Rajshahi University of Engineering & Technology, Rajshahi-6204, Bangladesh*
[3] *American International University Bangladesh, Bangladesh*
[4] *Varendra University, Rajshahi, Bangladesh*
[5] *Khulna University of Engineering & Technology, Khulna, Bangladesh*

Об'єднана енергосистема є перспективним джерелом електричної енергії, яке задовольняє надлишкові потреби в електроенергії у всьому світі, безпечна та надійна робота якого необхідна для зменшення навантаження та підвищення стійкості. Розвиток інформаційно-комунікаційних технологій (ICT) не лише стимулює, а й гальмує технології, сприяючи кіберзлочинності. Кібератака (CA) на енергосистему в теперішній час стає поширеною проблемою, яка призводить до несанкціонованого доступу до блоку управління енергосистемою і частково або повністю перешкоджає роботі всієї системи, змінюючи конфіденційні дані енергосистеми та блоку управління. Продуктивність енергосистеми регулюється використанням FPID (fractional-order-proportional-integral-derivative) контролера і порівнюється з продуктивністю звичайного PID контролера. Надійна робота енергосистеми повністю залежить від ефективної конструкції контролера, але на параметри контролера значною мірою впливає CA, ушкоджуючи всю систему. Будь-яка зміна блоку управління або параметрів системи може знизити стійкість та стабільність енергосистеми. У статті запропоновано автоматичний метод захисту від CA (ACAMU), щоб повністю уникнути CA та її впливу на систему та контролер, для підвищення безпеки і стійкості енергосистеми, підтримуючи фіксовані дані як для системи, так і для контролера.

Ключові слова: Об'єднана енергосистема, FPID контролер, Кібератака, Блок системи безпеки.