Protection of Power System during Cyber-Attack using Artificial Neural Network

Md. Shahidul Islam*, **Shafia Sultana, Md. Motakabbir Rahman**

Department of Electrical and Electronic Engineering, Rajshahi University of Engineering & Technology (RUET), Rajshahi, **BANGLADESH**

*Corresponding Contact:
Email: siruet@gmail.com

ABSTRACT

Impacts of frequency and voltage disturbance on an isolated power system caused by cyber-attack have been discussed, and a neural network-based protective approach has been proposed in this research work. Adaptive PID controllers for both load frequency control and automatic voltage regulator have been implemented using an artificial neural network-oriented by genetic algorithm. The parameters of the PID controller have been tuned offline by using a genetic algorithm over a wide range of system parameter variations. These data have been used to train the neural network. Three input switch has been implemented to control governor speed regulation and amplifier gain. For load frequency control neural network tuned PID controller mitigate frequency disturbance 48% faster than manually tuned PID and for the automatic voltage regulator, neural network tuned PID controller mitigate voltage disturbance 70% faster than manually tuned PID during cyber-attack.

Key words:

Load Frequency Control (LFC); Automatic Voltage Regulator (AVR); cyber-attack, cyber-security; Artificial Neural Network (ANN); Genetic Algorithm (GA); Proportional-Integral-Derivative (PID); supervisory control and data acquisition (SCADA)

8/22/2019 **Source of Support:** None, **NoConflict of Interest:** Declared

INTRODUCTION

In the power system, supervisory control and data acquisition (SCADA) systems have been incorporated for increasing its reliability and efficiency by introducing automatic control. SCADA is performing remote data acquisition and processing, which is equipped with online computers. Recently, in this system smart grid concept has been introduced to encompass the automation from generation to transmission, to distribution, and finally to the consumer for attaining optimized use of facilities along with improving services of the system (Thomas and McDonald 2015; Locke and Gallagher 2010). A smart grid introduces two-way communication where the electricity and information can be exchanged between the utility and consumers (Rawat and Bajracharya 2015). The utilization of information technology in physical infrastructure has opened up new possibilities of cyber-attack in the smart grid (Ericsson 2010; Ten et al. 2010; Sridhar et al. 2012; Yan et al. 2012). The hacker may access the confidential data of the system, which has an enormous impact on the economy, operation, and control of the system. Cyber-attack causes data falsification; as a result, an excessive delay occurs between sensors and controllers, finally decreases in energy efficiency (Farraj et al. 2016, Deng et al. 2017; Liu et al. 2017). The authors in Sridhar and Manimaran (2010) have discussed the effect of intelligent data integrity attacks on a power network voltage control loop. The consequence of data reliability and denial of service attacks have been discussed in Huang et al. (2009). The authors Teixeira et al. (2014), Isozaki et al. (2016), and Cameron et al. (2018) have discussed the impacts of injecting false data and causing a denial of service attack on voltage control scheme for voltage violation. The impacts of attackers with online learning ability to find an optimal strategy for attacking automatic voltage control have been analyzed in Chen et al. (2018).

During cyber-attack, automatic generation control (AGC) unit and load frequency control (LFC) loop are liable to maintain stable frequency with the variation of load (Tan et al. 2017; Sahabuddin et al. 2016; Biswas and Sarwat 2016; Sridhar and Govindarasu 2014). The authors in Sridhar and Govindarasu (2014) have discussed the impact of false data injection on AGC and an anomaly detection algorithm as countermeasure has been proposed.

Rahman et al. (2017) have investigated the impact of cyber-attack on PID based AGC. Mosaad and Salem 2014 has been proposed a design methodology based on artificial neural networks (ANN) for an adaptive PID load frequency control. The impact of cyber-attack (positive biased or negative biased attack) on LFC has been discussed in Hassan et al. (2016). A feedback LFC with three input switch has been proposed, but it requires significant time to reach stability, and the frequency does not get to its normal value after a variation in the real power of the system (Hassan et al. 2016). So, it should be analyzed the impact of cyber-attack properly, to reduce frequency and voltage deviation, and to settle system stability.

System Modeling of LFC

For quality service, nominal frequency is ensuring during generation, transmission, and distribution of electric energy. The elementary model for this purpose is LFC. The author Saadat in 1999, has investigated that LFC maintains uniform frequency, although the frequency deviation doesn't become zero. A simple LFC is made up of a turbine, a generator, and a governor, figure 1 shows the block diagram of LFC.

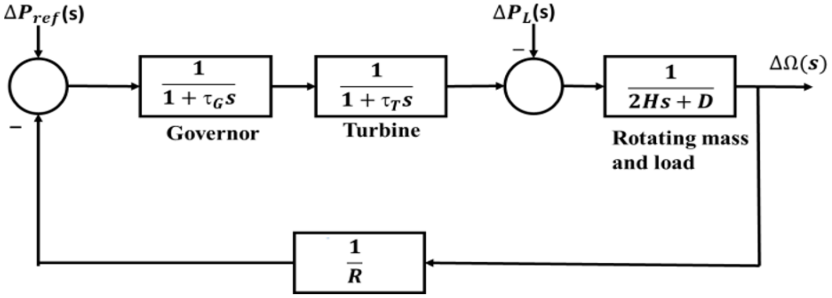

Figure 1: Block diagram of LFC for an isolated power system (Saadat, 1999)

Depending on speed regulation (R), the governor adjusts generation with varying load demand, which maintains a stable frequency.

The close loop transfer function of LFC is as follows (Saadat, 1999):

$$\frac{\Delta\Omega\,(s)}{-\Delta P_L(s)} = \frac{(1+\tau_g s)(1+\tau_T s)}{(2Hs+D)(1+\tau_g s)(1+\tau_T s)+\frac{1}{R}} \qquad (1)$$

The system parameters for LFC are shown in table 1. If we evaluate equation (1) using the specifications of table 1, then according to Routh-Hurwitz array, the governor speed regulation must be greater than 0.0135 (Saadat, 1999).

Table 1: System parameters for LFC

Parameter	**Value**
Turbine time constant, τ_T	0.5 s
Governor time constant, τ_G	0.2 s
Generator inertia constant, *H*	5 s
Change in load, ΔP_L	0.2 pu
Frequency	50 Hz
Integral controller, K_i	7
Governor speed regulation	R

System Modeling of AVR

Figure 2 represents the block diagram of AVR. Here the sensor senses the terminal voltage, and the excitation of the generator change accordingly to keep the voltage at a tolerable state.

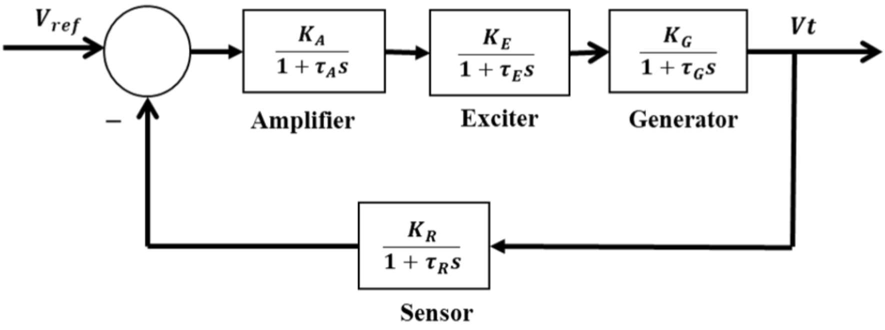

Figure 2: Block diagram of AVR

The closed-loop transfer function of AVR by relating the generator terminal voltage (V_t) to the reference voltage (V_{ref}) is (Saadat, 1999):

$$\frac{V_t}{V_{ref}} = \frac{K_A K_E K_G(1+\tau_R s)}{(1+\tau_A s)(1+\tau_E s)(1+\tau_G s)(1+\tau_R s)+K_A K_E K_G K_R} \qquad (2)$$

The system parameters for AVR are shown in table 2. If we evaluate equation (2) using the parameters given in table 2, then according to Routh-Hurwitz array, the amplifier gain K_A must be less than 12.16 (Saadat, 1999).

Table 2: System parameters for AVR

Parameters	**Value**
Amplifier gain	K_A
Exciter gain, K_E	1
Generator gain, K_G	1
Sensor gain, K_R	1
Amplifier time constant,τ_T	0.1
Exciter time constant,τ_E	0.4
Generator time constant,τ_G	1
Sensor time constant,τ_T	0.05

CONTROL METHODOLOGY

The aim of this research work is to operate the system at a steady-state irrespective of any frequency and voltage disturbance. Two methodologies have been discussed and compared here, which are:

1. Genetic algorithm tuned PID controller:

Genetic algorithm (GA) is a heuristic or higher-level procedure that is inspired by natural selection and provides a sufficiently good solution to an optimization problem. Like other optimization techniques, the GA starts by defining optimization variables and fitness functions. Here GA has been used for off-line tuning of PID controller parameters minimizing the integral square error.

2. Artificial Neural Network (ANN) tuned adaptive PID controller:

The Adaptive control technique is a technique to redesign the PID controller by tuning its parameters automatically on-line while ensuring its preceding performance. In this paper, ANN (Artificial Neural Network) has been utilized to tune the parameters of the PID controller on-line.

Artificial Neural Networks, which are considered as a relatively new information processing technique, are inspired by the neural networks of animal brains. A neural network consists of a variety of terribly easy and extremely inter-connected processors called neurons within the animal brain (Mosaad and Salem, 2014; Donepudi, 2017). The neurons are connected by an oversized variety of weighted links over that signals will pass.

In this research work, while designing LFC, a multilayer feed-forward neural network has been trained with six input (a wide range of system parameters such as table 1) and three outputs (values of Kp, Ki, Kd for corresponding system parameters). The network has been trained using the Levenberg Marquardt algorithm.

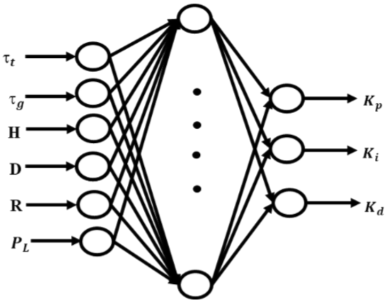

Figure 3: Structure of ANN for LFC

While designing AVR, a multilayer feed-forward neural network has been trained with eight inputs (a wide range of system parameters such as table 2) and three outputs (Values of K_p, K_i, K_d for corresponding system parameters). The training dataset has been created using GA. In both cases, the numbers of neurons in the hidden layer are 20.

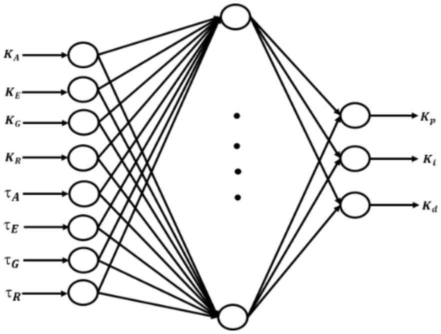

Figure 4: Structure of ANN for AVR

Proposed Model for LFC using ANN-based on-line tuned PID:

The system stability may fall due to frequency disturbance. Figure 5 shows the proposed solution to diminish the oscillating frequency deviation by connecting a three-input switches in the feedback path of the LFC block.

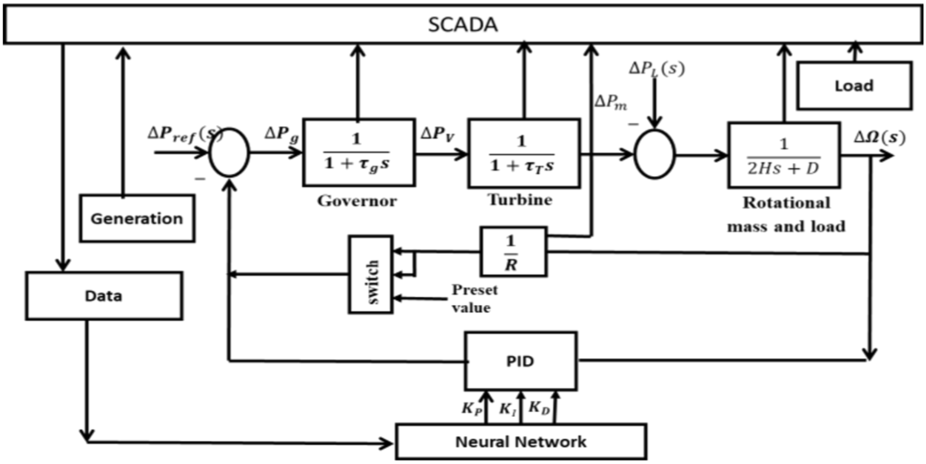

Figure 5: Proposed model for LFC.

Proposed Model for AVR:

Voltage stability may unsettle due to cyber-attack on the AVR system. Figure 6 presents the proposed protective model for AVR in an isolated power system.

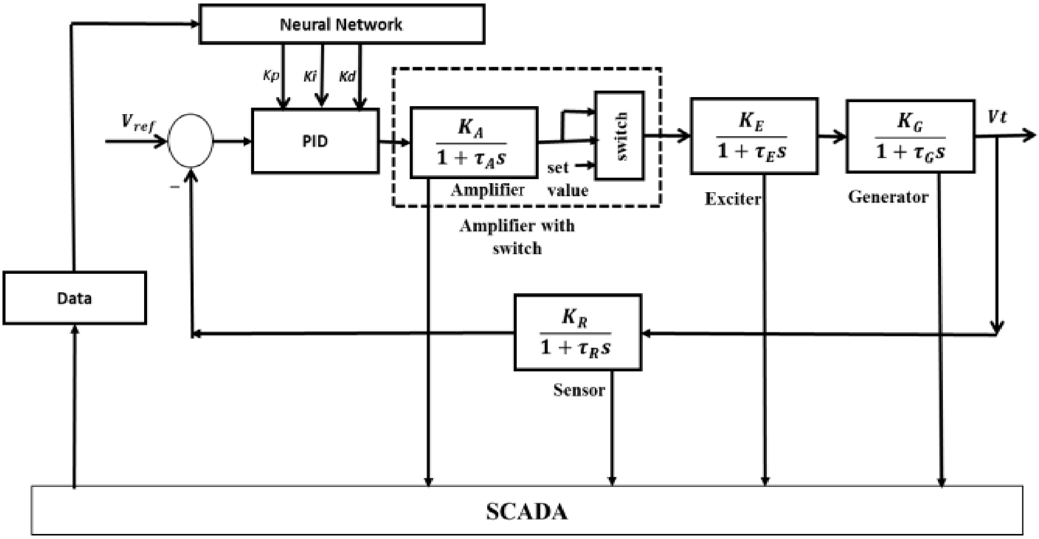

Figure 6: Proposed model for AVR.

Here the neural network will take all the input from SCADA and tune the PID controller automatically. Then the neural tuned PID controller will control the system (LFC or AVR). In figure 5, a three-input switch has been used to control the speed regulation of the governor so that the speed regulation can't be less than 0.0135. In figure 6, a three-input switch has been used to control the amplifier gain so that the amplifier gain can't be larger than 12.16 for ensuring stability criterion (Saadat, 1999).

CYBER ATTACK ON LFC

During a cyber-attack, the governor fails to set the value of governor speed regulation. Figure 7 represents the effect of speed regulation.

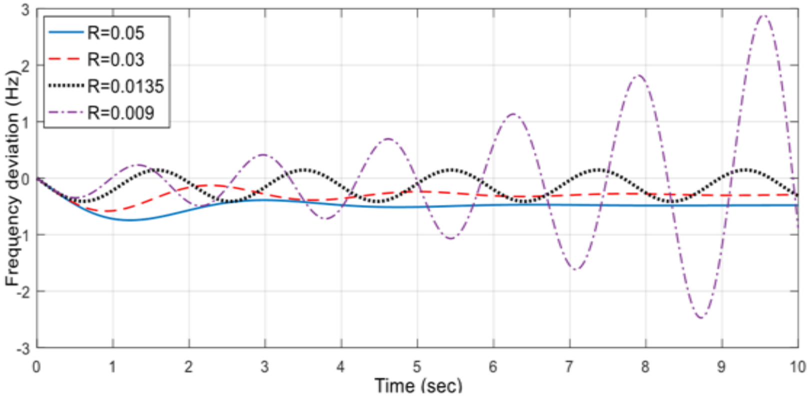

Figure 7: Effect of Speed regulation on LFC

If the value of speed regulation increases due to the cyber-attack, then the cyber-attack is defined as a positively biased cyber-attack. And if the value of the speed regulation decreases, then the cyber-attack is defined as a negatively biased cyber-attack. Figure 8 and figure 9 shows the frequency deviation in the case of positively biased and negatively biased, respectively.

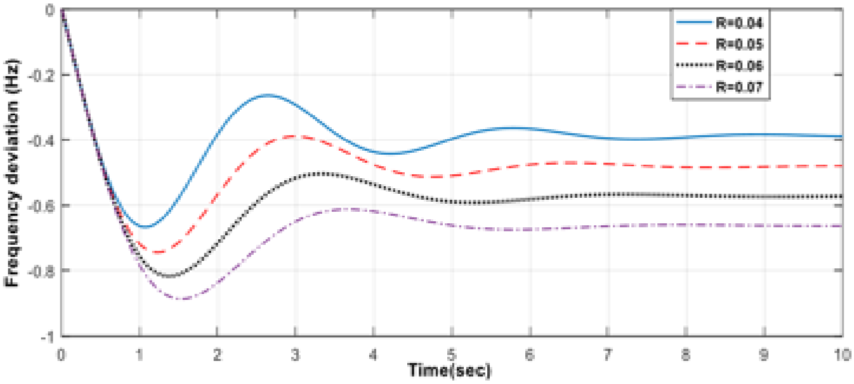

Figure 8: Frequency deviation in case of positively biased attack

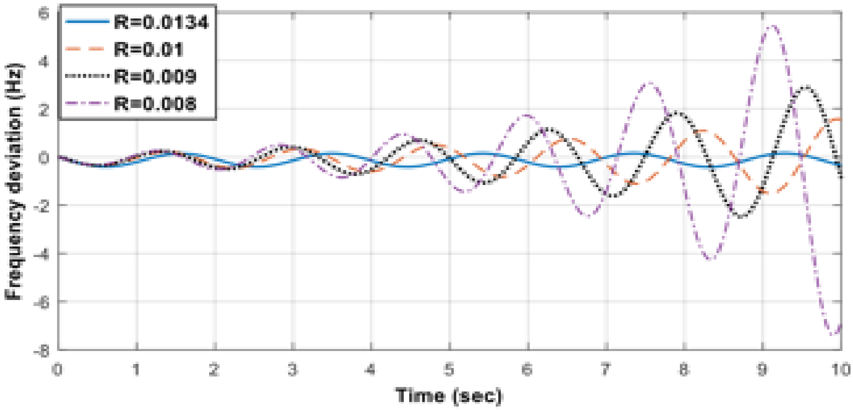

Figure 9: Frequency deviation in case of negatively biased attack

SOLUTION FOR LFC

The proposed ANN-based adaptive PID based LFC with three input switch has two steps of protection. Firstly, the adaptive PID controller can be tuned automatically at any system parameter; secondly, the three input switch monitors the speed regulation of the governor (R). When the value of R becomes less than 0.0135, the three input switch sends the preset value to keep the system stable. This protection scheme not only protects the system during cyber-attack but also is much faster than manually tuned PID controller (Donepudi, 2015). For LFC neural network tuned PID controller, mitigate frequency disturbance 48% faster than manually tuned PID controller.

A comparison between manually tuned PID, GA tuned PID, and neural network tuned PID has been shown in figure 10, and their numerical comparison for settling time has been shown in table 3. Controlling the positive and negative biased attack has been shown in figure 11 and figure 12, respectively.

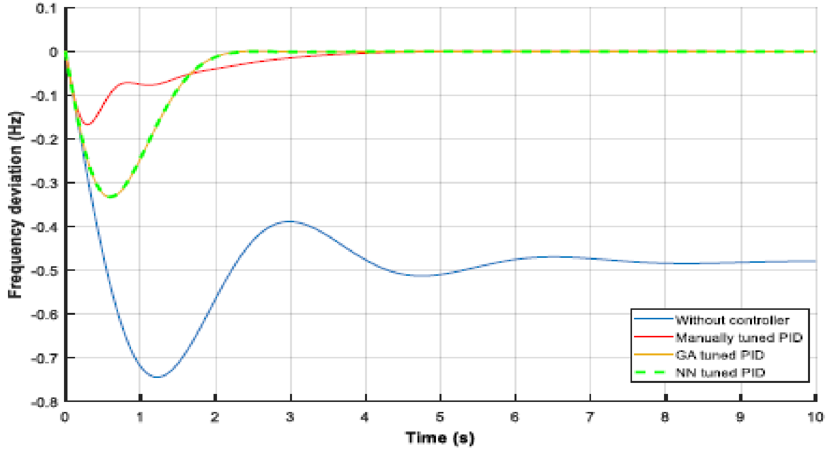

Figure 10: Step response of LFC

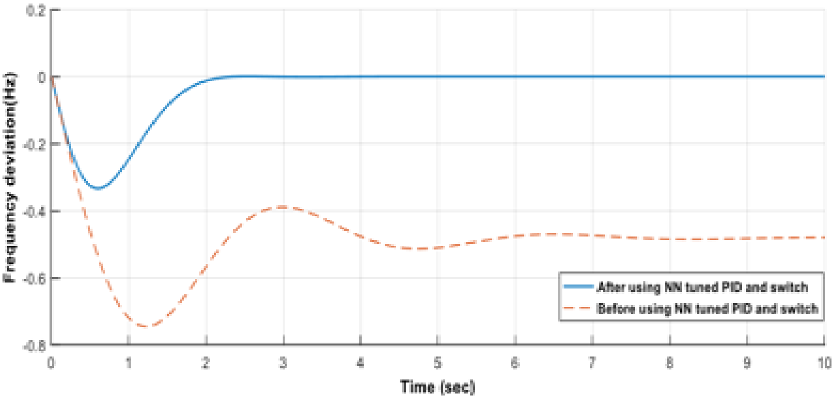

Figure 11: Controlling Positively biased attack

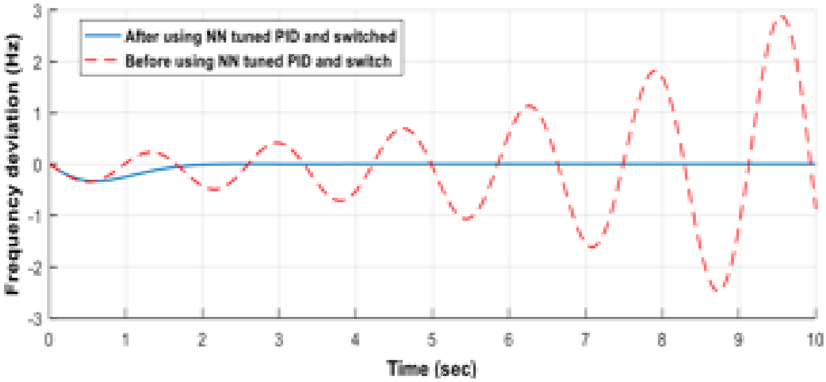

Figure 12: Controlling Negative biased attack.

Table 3: Comparison table of Manually Tuned PID, GA Tuned PID, and NN tuned PID

Manually Tuned PID	GA Tuned PID	NN tuned PID
4.07 s	2.11 s	2.115 s

SOLUTION FOR AVR

The proposed ANN-based adaptive PID based AVR with three input switch also has two steps of protection like LFC. Firstly, the adaptive PID controller can be tuned automatically at any system parameter; secondly, the three input switch monitors the amplifier gain of AVR. When the value of amplifier gain becomes greater than 12.16, the three input switch injects the preset value to achieve system stability. This protection scheme not only protects the system during cyber-attack but also is more-faster than manually tuned PID controller. For AVR neural network tuned PID controller mitigate voltage disturbance 70% faster than manually tuned PID during cyber-attack.

Characteristics of step response of AVR with manually tuned PID, GA tuned PID, and neural network tuned PID has been shown in figure 13, and their numerical comparison for settling time is shown in table 4.

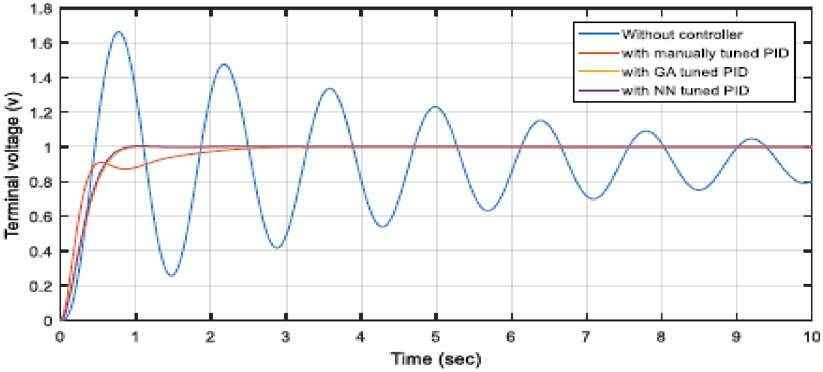

Figure 13: Step response of AVR

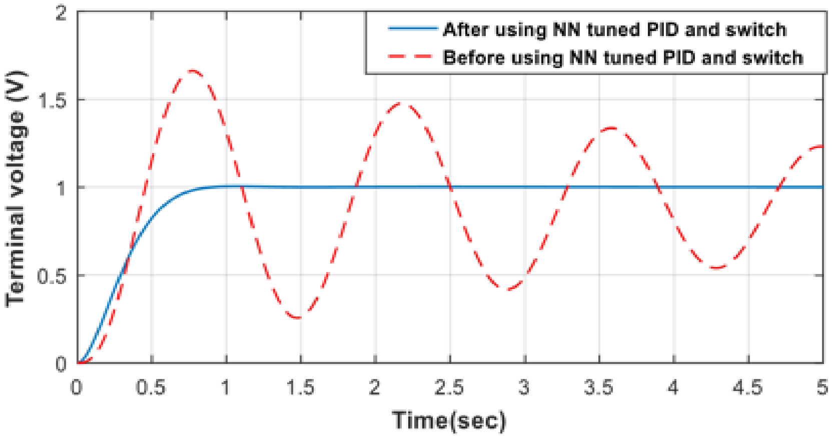

Figure 14: Voltage control during cyber-attack

Table 4: Comparison table of Manually Tuned PID, GA Tuned PID, and NN tuned PID

Manually Tuned PID	GA Tuned PID	NN tuned PID
2.6 s	0.81 s	0.761 s

CONCLUSION

In this paper, to ensure frequency and voltage stability, the impact of cyber-attack on LFC and AVR has been investigated successfully. For defending these types of attacks, a countermeasure has been proposed. Adaptive PID controller along with a three-input switches for both LFC and AVR has been implemented using ANN, which is oriented by GA. The result shows that for LFC neural network tuned PID controller mitigate frequency disturbance 48% faster than manually tuned PID and for AVR neural network tuned PID controller eliminates voltage disturbance 70% faster than manually tuned PID during cyber-attack**.** Future research will involve cyber-security for the interconnected systems.

REFERENCES

Biswas, S., & Sarwat, A. (2016). Vulnerabilities in two-area Automatic Generation Control systems under cyber-attack. In *Resilience week, 2016, IEEE* (pp. 40–45).

Cameron, C., Patsios, C., Taylor, P., & Pourmirza, Z. (2018). Using self-organizing architectures to mitigate the impacts of denial-ofservice attacks on voltage control schemes. *IEEE Transactions on Smart Grid*, *10*(3), 3010–3019.

Chen, Y., Huang, S., Liu, F., Wang, Z., & Sun, X. (2018). Evaluation of reinforcement learning based false data injection attack to automatic voltage control. *IEEE Transactions on Smart Grid*, *10*(2), 2158–2169.

Deng, R., Xiao, G., Lu, R., Liang, H., & Vasilakos, A. V. (2017). False data injection on state estimation in power systems-Attacks, impacts and defense: A survey. *IEEE Transactions on Industrial Informatics*, *13*(2), 411–423.

Donepudi, P. K. (2015). Crossing Point of Artificial Intelligence in Cybersecurity. *American Journal of Trade and Policy*, *2*(3), 121-128. https://doi.org/10.18034/ajtp.v2i3.493

Donepudi, P. K. (2017). Machine Learning and Artificial Intelligence in Banking. *Engineering International*, *5*(2), 83-86. https://doi.org/10.18034/ei.v5i2.490

Ericsson, G. N. (2010). Cyber security and power system communication-essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, *25*(3), 1501–1507.

Farraj, A., Hammad, E., & Kundur, D. (2016). A cyber-physical control framework for transient stability in smart grids. *IEEE Transactions on Smart Grid*, *9*(2), 1205–1215.

Hassan, M., Roy, N. K., & Sahabuddin, M. (2016). Mitigation of frequency disturbance in power systems during cyber-attack. In *Proceedings of IEEE International Conference on Electrical, Computer, Telecommunications Engineering*. https://doi.org/10. 1109/ICECTE.2016.7879601.

Huang, Y.L., Cardenas, A. A., Amin, S., Lin, Z.S., Tsai, H.Y. and Sastry, S. (2009). "Understanding the physical and economic consequences of attacks on control systems," Int. J. Critical Infrastructure Protection, vol. 2, no. 3, pp. 73–83.

Isozaki, Y., Yoshizawa, S., Fujimoto, Y., Ishii, H., Ono, I., Onoda, T., et al. (2016). Detection of cyber-attacks against voltage control in distribution power grids with PVs. *IEEE Transactions on Smart Grid*, *7*(4), 1824–1835.

Liu, X., Shahidehpour, M., Li, Z., Liu, X., Cao, Y., & Li, Z. (2017). Power system risk assessment in cyber-attacks considering the role of protection systems. *IEEE Transactions on SmartGrid*, *8*(2), 572–580.

Locke, G., & Gallagher, P. D. (2010). NIST framework and roadmap for smart grid interoperability standards, release 1.0. In *National Institute of Standards and Technology* (Vol. 33).

Mosaad, M.I, and Salem, F. (2014). LFC Based Adaptive PID Controller using ANN and ANFIS Techniques. *Journal of Electrical Systems and Information Technology 1 (2014) 212–222*

Rahman, M. A., Rana, M. S., and Anower, M. A. (2017). ″Indemnity for Frequency Disruption in a Smart Grid during Cyber–Attack. *2nd International Conference on Electrical & Electronic Engineering (ICEEE)*, 27–29. 2017, RUET, Rajshahi, Bangladesh.

Rawat, D. B., and Bajracharya C. (2015). Detection of false data injection attacks in smart grid communication systems. *IEEE Signal Process.Lett.*, 22 (10), 1652-1656.

Saadat, H. (1999). *Power system analysis*. New York: McGraw-Hill.

Sahabuddin, M., Dutta, B., & Hassan, M. (2016). Impact of cyber-attack on isolated power system. In *Proceedings of IEEE 3rd International Conference on Electrical Engineering and Information Communication Technology*. https://doi.org/10.1109/CEEOCT. 2016.7873088.

Sridhar, S., & Govindarasu, M. (2014). Model-based attack detection and mitigation for automatic generation control. *IEEE Transactions on Smart Grid*, *5*(2), 580–591.

Sridhar, S., & Manimaran, G. (2010). *Data integrity attacks and their impacts on SCADA control system* (pp. 1–6). IEEE: Power and Energy Society General Meeting.

Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210–224.

Tan, R., Nguyen, H. H., Foo, E. Y., Yau, D. K., Kalbarczyk, Z., Iyer, R. K., et al. (2017). Modeling and mitigating impact of false data injection attacks on automatic generation control. *IEEE Transactions on Information Forensics and Security*, *12*(7), 1609–1624.

Teixeira, A., Dan, G., Sandberg, H., Berthier, R., Bobba, R.B., & Valdes, A. (2014). Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures. In *Proceedings of IEEE American control conference* (pp. 4372–4378).

Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cyber security for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *40*(4), 853–865.

Thomas, M. S., & McDonald, J. D. (2015). *Power system SCADA and smart grids*. Boca Raton: CRC Press.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, *14*(4), 998–1010.

--0--

How to Cite:

Islam, M. S., Sultana, S., & Rahman, M. M. (2019). Protection of Power System during Cyber-Attack using Artificial Neural Network. *Engineering International*, *7*(2), 73-84. https://doi.org/10.18034/ei.v7i2.478