Load Frequency Control System

Subjects: Energy & Fuels

Contributor: Athira M. Mohan , Nader Meskin , Hasan Mehrjerdi

Power systems are complex systems that have great importance to socio-economic development due to the fact that the entire world relies on the electric network power supply for day-to-day life. Therefore, for the stable operation of power systems, several protection and control techniques are necessary. Among various power system controls, the load frequency control (LFC) is the most time-consuming control mechanism of power systems due to the involvement of mechanical parts. As the control algorithms of frequency stabilization deliver control signals in the timescale of seconds, LFC systems cannot handle complicated data validation algorithms, making them more vulnerable to disturbances and cyber-attacks. Hence advanced research is highly encouraged in the field of development of attack resilient frequency stabilization techniques and in the area of cyber-security of LFC systems.

load frequency control system cyber-attacks attack points

1. Introduction

Although LFC schemes ensure power system stability with reliable electric power of guaranteed quality and zero frequency deviations, it is prone to cyber-attacks from malicious adversaries. Modern deregulated power system LFC schemes use open communication infrastructure in contrast to conventional LFCs, which used dedicated communication channels for the transmission of signals, among remote terminal units (RTU), control center, and generator unit [1]. The highly decentralized LFC scheme with open communication network is more prone to various malicious attacks like jamming of communication channels, injection of false data, alterations in the load of the power system, etc. [1]. In addition, LFC schemes have to generate control signals in the timescale of seconds. Therefore, the LFC loop cannot afford to use complex data validation algorithms for the validation and estimation of measurement data. The attackers can take advantage of this and manipulate the measurement data with less detailed mathematics [2]. These circumstances indicate the vulnerability of the LFC system to cyber-attack. Therefore, the study and analysis of attack impacts on the LFC system are highly important. The research activities in the area of cyber-security of the LFC system also help developing countermeasures like detection and defense mechanisms which can mitigate cyber-attack impacts. The impact of the attack in the LFC system is measured in terms of breach of operating frequency [3]. The defense mechanisms of the LFC system generally include resilient control algorithms [4].

2. LFC System Configurations and Attack Point Identification

The power system control loops (including LFC systems) consists of control centers, electronic field devices, and communication networks working together, for the reliable and efficient generation, transmission, and distribution of power [3]. Sensors collect measurements of various physical parameters, like the terminal voltage, power flow, rotor speed, etc., from the field devices and the measurements are sent to the control center using dedicated communication protocols. The group of computational algorithms that processes and analyzes the measurements from sensors or terminal units is collectively called as energy management system (EMS) [5]. The decisions from the control center are then transmitted to actuators for the implementation of required changes through field devices or actuators. Primary control or governor control, secondary control scheme with the help of traditional supervisory control and data acquisition (SCADA), the secondary control scheme in smart grid/microgrid control using phasor measurement units (PMU), etc. have been developed for the LFC in the generation side of the power system [3]. The LFC scheme is basically implemented to ensure the balance between load and frequency in the power system and thus eliminating the non-zero frequency deviation [6]. A well-designed power system with LFC adjusts perfectly against the load variations and system disturbances while producing high-quality electric power and maintaining frequency within the tolerance limit [4].

The LFC scheme primarily starts with governor control, which is the control of the generation unit using speed regulation or droop characteristics. Droop characteristics represent the slope of the governor steady-speed characteristics curve [6]. From the control point of view, it can be viewed as a proportional controller that ends up with a steady-state frequency deviation [4].

The governor control (local control) of LFC system does not rely on the SCADA telemetry system, as the rotor speed measurements of the single generator are locally sensed [3]. In this case, the valve position of the prime mover is adjusted according to the sensed speed to reflect the corresponding change in the output power of the generator [4].

Even though this is a local control scheme, the control module/controller of this scheme does have a communication link with the control center of the plant as it defines the governor controller operating setpoint using this link. The attack surface of local control loops is limited due to the local sensing of measurements without using the SCADA network. Therefore, attacks like DoS, replay, integrity, timing, etc. are not applicable to this control loop. However, the malware can still compromise system cyber-security measures and enter substation LAN through entry points like USB keys. The malware then corrupts the control module settings and disrupts normal operation. The Modbus protocol is used by the controllers of modern digital governor control for the communication with control center computers via Ethernet [3][4].

Different from governor control, the secondary control of the LFC scheme allows the frequency control of multiple generators that are operated in parallel, sharing large electrical loads. The secondary control provides a reset action for the steady-state frequency deviation and adjusts the generation automatically to re-establish the system frequency to the nominal value for the continuous load changes [7]. The secondary control system resets the frequency deviation at steady-state to zero value [6].

The LFC system configurations can be divided into single-area and multi-area schemes. In the multi-area or interconnected-area LFC system, the power exchange between the areas happens through connections called tie-lines [6]. The aim of the single-area LFC system is only restricted to the stabilization of operating frequency to the nominal value as the interconnected system adjustment is not needed [8]. In the multi-area LFC system, the generators of each area have to control local load and tie-line power variations from interconnected areas to attain load balances at local and global levels [6].

Traditionally, LFC of an area or interconnected areas involving multiple generators is done with the help of energy control centers that make use of on-line computers and remote data acquisition systems like SCADA [4]. In the modern electric grid and smart grid, PMU is used for real-time monitoring and control. The communication channels from RTUs to the control center and from the control center to governor control are the main attack points of secondary control loops both in single-area and multi-area LFC systems [1][4][9].

The typical LFC loop is given in Figure 1 and the attack points of the single-area LFC system are provided in Figure 2. The schematic diagram of the multi-area LFC system with attack points is provided in Figure 3.

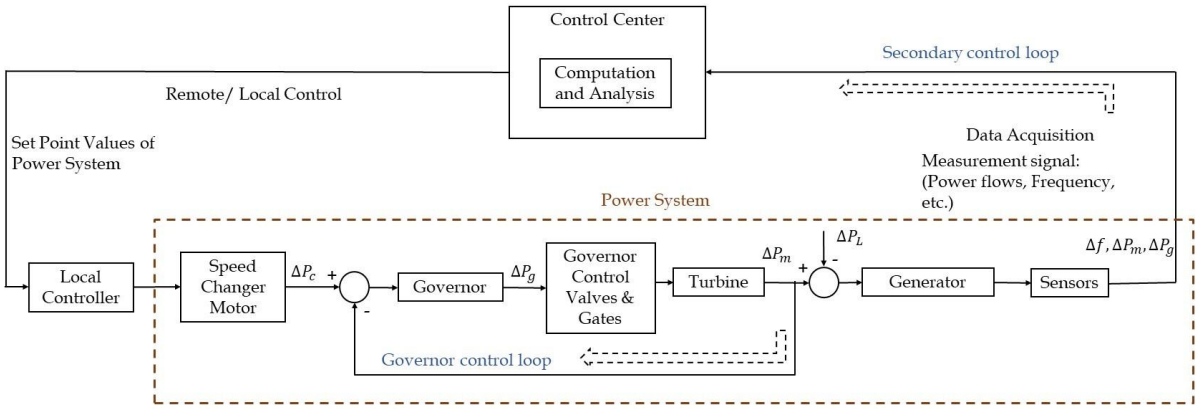

Figure 1. A typical load frequency control (LFC) loop [4].

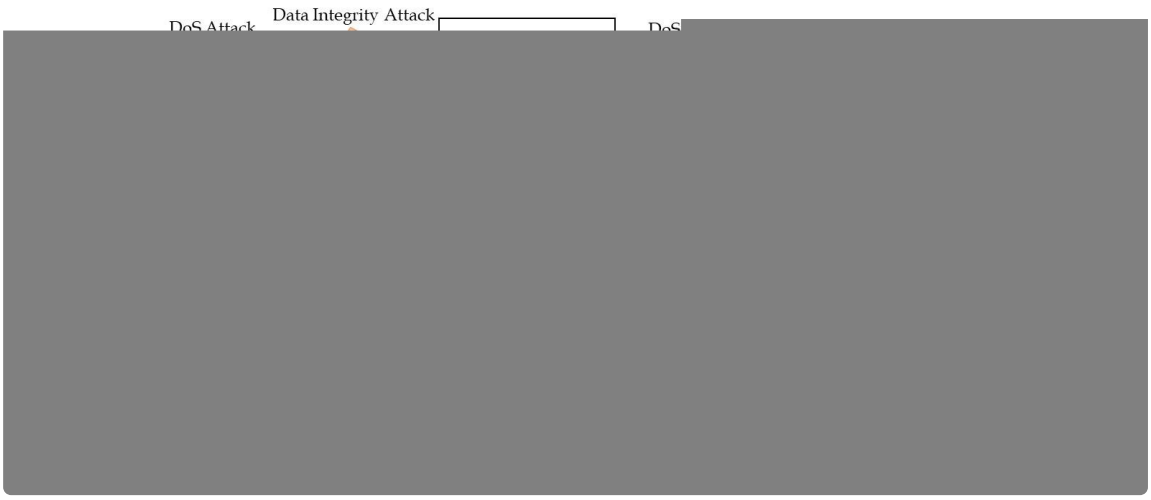

Figure 2. General block diagram of single-area LFC system with attack points [4].

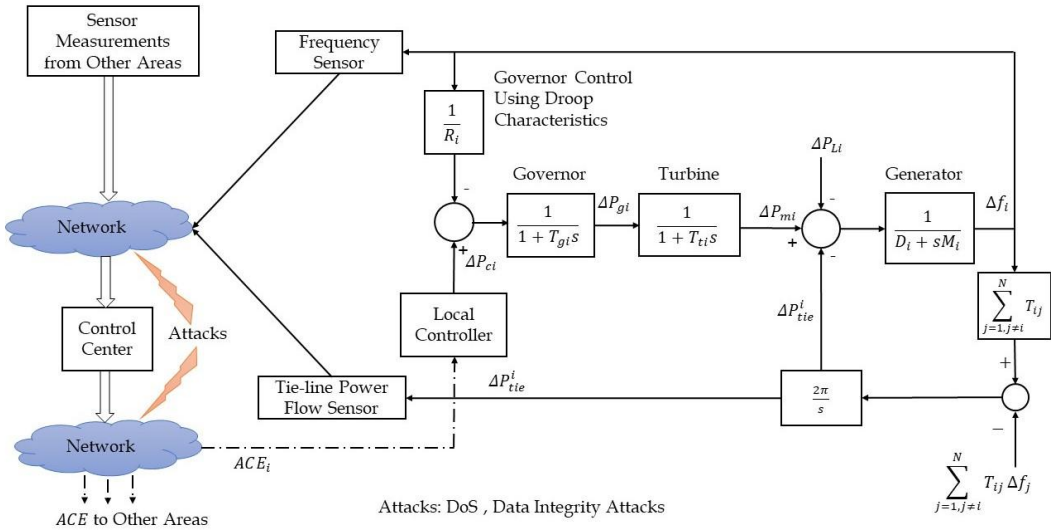

Figure 3. General block diagram of multi-area LFC system with attack points [4].

The main types of cyber-attacks in the LFC system are given in Figure 4.

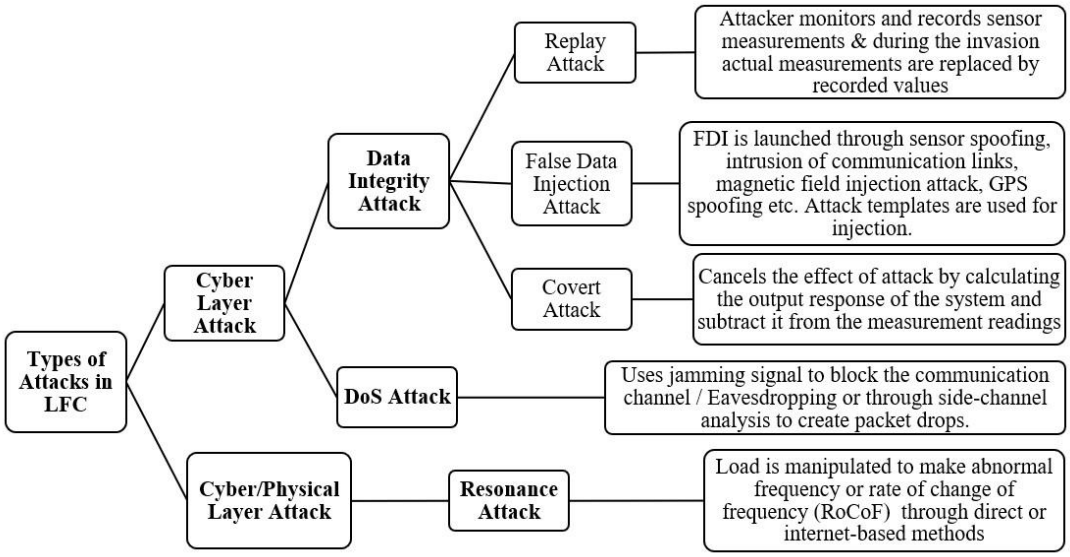

Figure 4. Various attacks of the LFC system [4].

3. Future Research

Different fields in the cyber-security of the LFC system that has not received adequate attention are mentioned below [4].

- Impact analysis of coordinated or hybrid attacks and the development of mitigation techniques for these attacks. Resource constraints, like bandwidth of communication channels, energy limitations, etc., should be also considered simultaneously during the development of attack detection and defense mechanisms, and then the security and service quality can be assured at the same time [9].
- Analysis of individual or coordinated attacks in LFC systems under noisy communication networks [10].
- Adequate attention and profound discussion are needed in the area of multiple attack strategies for the development of adaptive defense strategies against different types of attacks [9].
- Renewable energy sources (RESs) are gathering higher attention in the field of power systems due to their intermittent nature. Research in the field of cyber-security of LFC systems with integrated RESs has to be performed further, as the impact of cyber-attacks can be worse in such kind of systems.
- Research works that analyze the effects of covert attacks in networked control systems like LFC are also highly encouraged as it seems to be an unexplored area. As the covert adversaries implement powerful and stealthy attack strategies it is high time to investigate the impact of such attack in the LFC system and look for the development of countermeasures.

4. Conclusion

Some of the inferences obtained from the research works related to the LFC system are that the vulnerability to cyber-attacks is higher for multi-area LFC systems due to the increased number of attack points. In addition, as the frequency response time of LFC systems is more, the computational

algorithms of these systems are slower compared to other control loops in the power systems. Therefore, more research is essential to develop fast computational algorithms and resilient control strategies. There are many research areas like “stochastic LFC systems”, “non-linearities of LFC systems”, “cyber-security against stealthy attacks in LFC systems”, etc. which still remain unexplored [4].

References

1. Yubin Shen; Minrui Fei; Dajun Du; Cyber security study for power systems under denial of service attacks. *Transactions of the Institute of Measurement and Control* **2017**, *41*, 1600-1614, 10.1177/0142331217709528.
2. Kaustav Chatterjee; V. Padmini; S. A. Khaparde; Review of cyber attacks on power system operations. *2017 IEEE Region 10 Symposium (TENSYMP)* **2017**, *1*, 1-6, 10.1109/tenconspring.2017.8070085.
3. Siddharth Sridhar; Adam Hahn; Manimaran Govindarasu; Cyber–Physical System Security for the Electric Power Grid. *Proceedings of the IEEE* **2012**, *100*, 210-224, 10.1109/JPROC.2011.2165269.
4. Athira Mohan; Nader Meskin; Hasan Mehrjerdi; A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems. *Energies* **2020**, *13*, 3860, 10.3390/en13153860.
5. Saeed Ahmed; Young-Doo Lee; Seung Ho Hyun; Insoo Koo; Mitigating the Impacts of Covert Cyber Attacks in Smart Grids Via Reconstruction of Measurement Data Utilizing Deep Denoising Autoencoders. *Energies* **2019**, *12*, 3091, 10.3390/en12163091.
6. Saadat;Hadi. Power system analysis; McGraw-Hill: New York, USA, 1999; pp. 527-555.
7. Maria Vrakopoulou; Peyman Mohajerin Esfahani; Kostas Margellos; John Lygeros; Goran Andersson; Cyber-Attacks in the Automatic Generation Control. *Solving Problems in Thermal Engineering* **2015**, *1*, 303-328, 10.1007/978-3-662-45928-7_11.
8. André Teixeira; Iman Shames; Henrik Sandberg; Karl Henrik Johansson; A secure control framework for resource-limited adversaries. *Automatica* **2015**, *51*, 135-148, 10.1016/j.automatica.2014.10.067.
9. Yuancheng Li; Pan Zhang; Longqiang Ma; Denial of service attack and defense method on load frequency control system. *Journal of the Franklin Institute* **2019**, *356*, 8625-8645, 10.1016/j.jfranklin.2019.08.036.
10. MagdiSadek Mahmoud; Mutaz M. Hamdan; Uthman Baroudi; Uthman A. Barudi; Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and

challenges. *Neurocomputing* **2019**, *338*, 101-115, 10.1016/j.neucom.2019.01.099.