designs

MDPI

Article

Cybersecurity Analysis of Load Frequency Control in Power Systems: A Survey

Sahaj Saxena [1], Sajal Bhatia [2,*] and Rahul Gupta [1]

[1] Electrical and Instrumentation Engineering Department, Thapar Institute of Engineering and Technology, Punjab 147004, India; sahaj.saxena@thapar.edu (S.S.); rgupta5_be18@thapar.edu (R.G.)
[2] School of Computer Science and Engineering, Sacred Heart University, 3135 Easton Turnpike, Fairfield, CT 06825, USA
* Correspondence: bhatias@sacredheart.edu

Abstract: Today, power systems have transformed considerably and taken a new shape of geographically distributed systems from the locally centralized systems thereby leading to a new infrastructure in the framework of networked control cyber-physical system (CPS). Among the different important operations to be performed for smooth generation, transmission, and distribution of power, maintaining the scheduled frequency, against any perturbations, is an important one. The load frequency control (LFC) operation actually governs this frequency regulation activity after the primary control. Due to CPS nature, the LFC operation is vulnerable to attacks, both from physical and cyber standpoints. The cyber-attack strategies ranges from a variety of attacks such as jamming the network communication, time-delay attack, and false data injection. Motivated by these perspectives, this paper studies the cybersecurity issues of the power systems during the LFC operation, and a survey is conducted on the security analysis of LFC. Various cyber-attack strategies, their mathematical models, and vulnerability assessments are performed to understand the possible threats and sources causing failure of frequency regulation. The LFC operation of two-area power systems is considered as a tutorial example to quantify the vulnerabilities. Mitigation strategies through control theoretic approaches are then reviewed and highlighted for LFC operation under cyber-attack.

Keywords: area control error; cybersecurity; control theory; load frequency control; two-area power system

Citation: Saxena, S.; Bhatia, S.; Gupta, R. Security Analysis of Load Frequency Control (LFC) in Power Systems: A Survey. *Designs* **2021**, *5*, 52. https://doi.org/10.3390/designs5030052

Received: 28 June 2021
Accepted: 30 July 2021
Published: 4 August 2021

1. Introduction

Today, the power sector is one of the critical infrastructures in the industrial control system because generation, transmission, and distribution of power are governed by automation. Moreover, the penetration of renewable energy resources, incorporation of demand side to provide ancillary services, and power systems restructuring is increasing daily. Due to large interconnections and remotely located generation, load, and control terminals, the power systems can be categorized as a cyber-physical systems where sensing, communication, and computing technologies are applied to physical spaces [1,2]. Note that the concept of cyber-physical power systems was initially depicted in [3] as a dedicated case of a cyber-physical system in a power system. It includes a large number of computing devices (servers, embedded systems, etc.), data acquisition devices (sensors and phasor measurement unit, etc.), and physical devices (large-scale generator set, distributed power supply, load, etc.). All these devices are interconnected through communication and transmission networks [4–7].

It is well known that the dependency on the communication media makes power systems vulnerable to cyber-attack as there are many openings in the network to disrupt the signal flow [8–11]. The cyber-attack known as the "Stuxnet malware incident" brought substantial damage to the Iranian nuclear program [12], which clearly indicated that the security is inefficient [13]. Such an incident raised alarm to avoid serious issues in the

advanced power technology. In a smart grid, the frequency regulation, optimal power flow analysis, and contingency analysis operations are based on the network communication technology, such as LAN, 3G, 4G, or 5G [14–16]. It is nearly impossible to remove the openings in the network for attack, however we can propose the framework focusing on (i) attack detection, (ii) effect of attack, and (iii) resilient system development. Note that the attackers target the power grid to (i) obtain economic benefits in terms of electricity bill reduction by tampering the smart meters, (ii) make profit in terms of contingency in electricity market, and (iii) promote terrorism. In principle, cyber-resilient power systems are required which can execute smooth generation of power despite an hostile cyber-threat environment. Thus, targeting the smart grid is actually a critical societal-threatening resource.

Among the different functionalities of power system, LFC is a crucial one [17]. LFC is always considered a benchmark problem in control theory as electrical grids are monitored by SCADA and controlled by industrial control systems [18–21]. This secondary frequency control operation (after the primary control by droop of the generator) is responsible for maintaining the frequency within scheduled range around (50/60 Hz depending upon the geographical region) and power flow on tie lines to agreed value. This operation can be affected by adversary to perturb the schedule frequency. In fact, the attacks could prevent the appropriate measurement signal being transferred to the control center, and affect the control center to make true commands. This creates large fluctuation of the frequency and deteriorate the power quality; in extreme cases, could lead the power system to collapse. In view of this, the objective of cybersecurity of LFC operation deals mainly with (1) the problem of finding the malicious measurements and prevent the controller from performing incorrect area control error (ACE) computations, and (2) maintaining the balance between generation and demand in the presence of untrusted measurements. With these security objectives of LFC operation, this article presents a control theoretic tutorial/survey and makes the following key contributions:

1. it provides an overview of the vulnerability assessment of LFC operation from a network-based attack standpoint;
2. it presents the implementation of network-based attacks on LFC operation in a simulated environment;
3. it provides a brief review of attack detection, identification and mitigation strategies on normal LFC operation along with existing techniques for hardware validation;
4. it discusses the role of data-driven and learning-based algorithms as trending tools for the attack modeling and defense strategy in the LFC operation.

We have omitted the comprehensive analysis of detection and mitigation schemes from this article and an instead attempted is made to produce a quick, clear, and concise summary with motivation towards the problem handling approach as a control engineering.

The remainder of the paper is structured as follows. Section 2 describes the motivation of this study towards cybersecurity in the power system and cyber-physical control-oriented mathematical description of LFC operation. As a whole, the attack on LFC operation ranges from a wiretapping attack (i.e., spoofing attack) to integrity attack (i.e., parameter or variable falsification attack). Section 3 presents different techniques to generate the adverse effects caused by the attackers in the LFC operation. The simulation studies for vulnerability assessment in LFC operation with the nominal controller (who is unaware of the unknown situations) are presented in Section 4 to showcase the effect of the cyber-attack. The next step is the requirement of resilient framework to detect and withstand the cyber-attack. Therefore, the summary of mitigation schemes on the basis of the different concepts in control theory is provided in Section 5 followed by literature survey on hardware testing of LFC operation in Section 6. Finally, Section 7 summarizes the paper and provides directions for future work in this critical area of research.

2. Motivation and the LFC System

2.1. Cyber-Attack Cases

In the power sector, around 800 cyber-attacks have been observed since the 1980s. Around 250 cyber cases were observed in US that are unintentional such as the *Arizona Public Service Outage* (2007) and *Florida Power and Light Outage* (2008), to name a few [22]. However, probably the first intentional major attack on power sector was observed on 23 December 2015 in Ukraine where the blackout lasted for several hours [23,24]. The attack was performed by malware through a phishing email. The workstation was hacked and the power supply got interrupted, and the communication network between customer and provider were blocked. This incident opened the eyes of the control researchers to look for some resilient control mechanism incorporating the cyber-physical approach to secure the power operation.

2.2. Mathematical Description of LFC Operation

The cyber-attacks on power generation operation can be introduced in different modes and strategies. The LFC operation of power system can be viewed as a networked control operation on a cyber-physical system. Note that a cyber-attack can change the structure of the LFC control system thereby deteriorating the performance. To explain the attacks and its effects in the LFC operation, we consider a standard simplified power generator network comprising of two control areas where each area consists of governor, non-reheated turbine, and load and machine (refer Figure 1) [25,26]. The notations used are also standard. In LFC operation, the area control error (ACE) is used to maintain zero steady-state error for frequency deviation Δf. Note that in multi-area power system, for the i-th control area

$$ACE_i = \beta \Delta f_i + \Delta P_{tie,ij},$$

where β is bias factor, and $\Delta P_{tie,ij}$ is a tie-line power between i-th and j-th control area. The different entities in each control area can be expressed through an input–output relationship in terms of transfer function; the governor is represented by

$$\frac{1}{T_G s + 1}, \tag{1}$$

the turbine by

$$\frac{1}{T_T s + 1}, \tag{2}$$

and the load and machine by

$$\frac{K_P}{T_P s + 1}. \tag{3}$$

The parameters T_G, T_T, T_P are the time constants of governor, turbine, and machine, respectively, and K_P is the gain of the machine. The speed regulator takes a constant gain $(1/R)$ and delay acquires a form $\exp(-\theta s)$ where θ is the amount of time as a delay.

Throughout this paper, the discussion is limited to the attack on the communication channel propagating the ACE command and its prevention. Now, the cyber-attacks on LFC operation can be introduced in different modes and strategies.

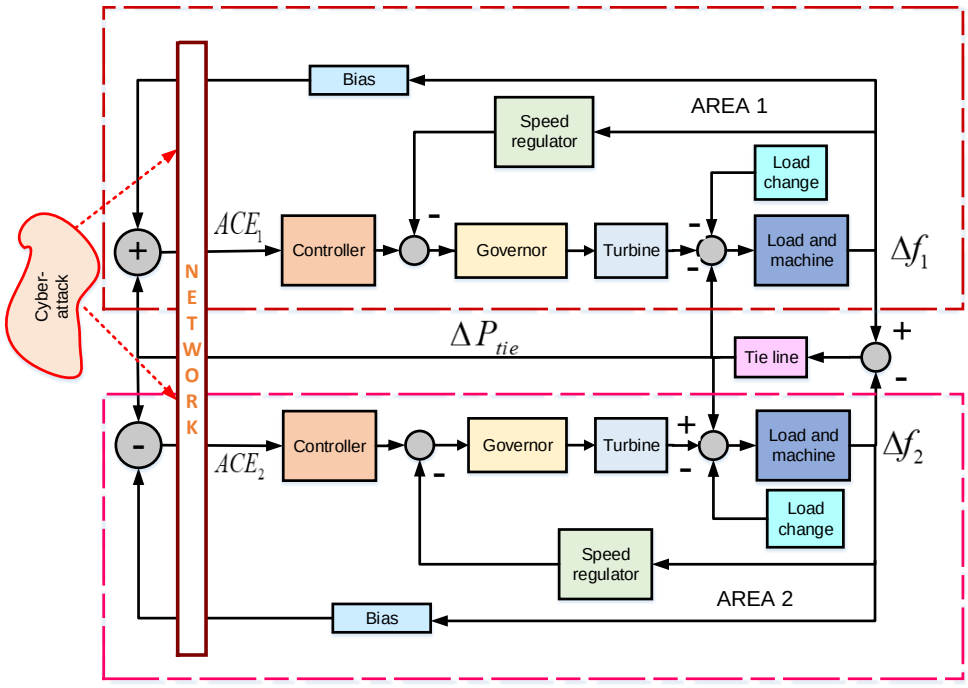

Figure 1. A typical two-area power system with LFC loops. All the paths for signal transmission passing through a rectangle "NETWORK" are the possible points from where the attacker can gain access to the signal.

3. Classification of Attacks on LFC

3.1. Strategic Attack

The classification based on method is enlisted below [27].

1. Replay attack: Replay attack is a kind of data manipulation attack. The attacker records the data coming from the sensor and replays the recorded data with the actual data in order to hide the theft or attack. Replay attacks can be executed in two phases which are as follows:
   (a) Monitoring Phase: In this phase, the attacker records the data or information coming from the sensor/actuator and stores it in a different variable.
   (b) Replaying Phase: At this stage, the data collected in the monitoring phase are replayed again and again until the attack has been successfully executed by the attacker.
2. Denial of Service (DoS): The transmission channel is blocked by flooding the excessive message (measurements) coming from the sensor.
3. Data integrity attack: The transmissions are modified to a create false signal. For example, the modified area control error takes the form

$$ACE_u = ACE + x,$$

   where x is attacker's input.
4. Timing attack: Delay is created to prevent the transmissions to reach in time. For example,

$$ACE_u = ACE(t - \tau),$$

   where τ is delay term. This delay term may be constant or time-varying function. Obviously, the time-varying function create potential risk.
5. Covert Attack: This attack basically works on the principle of canceling the effect of attack signal by calculating the response of the output and subtracting the readings

which are being measured. Covert attack becomes more stealthy as it can access the data as well as inject the false data into the channels of sensors and actuators of a CPS.

6. Zero dynamics attack: For successful execution of zero dynamics attack the attacker should have perfect knowledge of plant dynamics which are computed from state and output equations matrices. In this attack, the output of linear system are decoupled and uses the zeroes in transfer function to develop a particular attack strategy.

3.2. Template Attack

The attack, namely, template attack, can be introduced by modifying the amplitude of message signal. Such an attack can be broadly divided into following types.

1. Scaling attack: The magnitude or value of messages are scaled. For example,

$$ACE_u = aACE,$$

where constant a is a real number.

2. Ramp attack: The message of constant magnitude is continuously transmitted. For example,

$$ACE_u = b,$$

where b is fixed.

3. Pulse attack: The transmissions acquires a pulse shape with fixed time.
4. Random attack: The messages of random values are propagated.
5. Resonance attack: The message is modified according to a resonance source (e.g., rate of change of frequency).
6. Bias injection attack: In this attack, a constant bias signal is injected into the channels of sensors or control signal.

3.3. Location Attack

Based on the location of attack, the attack in CPS structure (from networked control theory perspective) of LFC system can be of three types.

1. Attack on sensor: The transmitted measurements are altered under this attack.
2. Attack on control: The control signal is varied.
3. Attack on actuator: The actuator signal is distorted in this type of attack.
4. Attack through Load: In LFC operation, the attacker can also penetrate through the load disturbance ΔP_d. The attack format may be

$$\Delta P_d^* = \Delta P_d + \delta$$

where δ is constant.

Thus, from the discussion made above, the overall pictorial representation of the various cyber-attacks on the LFC operation can be summarized in Figure 2.

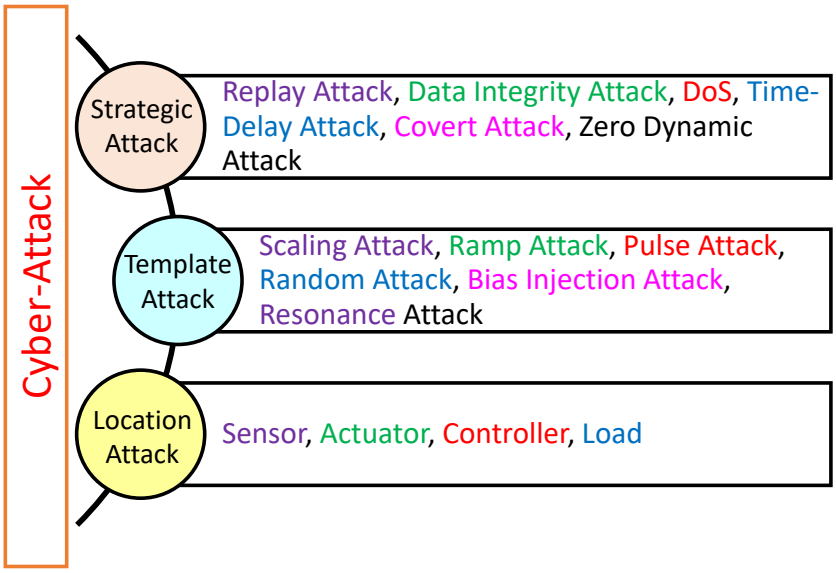

Figure 2. Classification of cyber-attacks on LFC.

4. Simulation Study

Based on the discussions in the previous Section 3, this section studies how the different attacks templates affect the performance in the frequency regulation. Using an Intel CORE^{TM} i7 processor, all the simulations have been carried out through MATLAB and Simulink. The block diagram depicted in Figure 1 is replicated with transfer functions expressed in (1)–(3). The parameters of both the control area are [25] identical: $R = 2.4$, $\beta = 0.425$, $T_G = 0.08$, $T_T = 0.3$, $T_P = 20$, and $K_P = 120$. The delay is considered as $\theta = 1$ s. For LFC approach, we consider a PI controller

$$C(s) = k_P + \frac{k_I}{s},$$

where $k_P = -0.1$ and $k_I = -0.671$. The system is subjected to load disturbance $\Delta P_L = 0.01$ p.u.

The different cyber-attacks are induced to the LFC system. The system under a data integrity attack with input $x = 0.2$ is exhibited in Figure 3, which states that Δf_i, $i = 1, 2$ do not reach zero. Similarly, the timing attack with induced delay $\tau = 10$ s destabilizes the system response, see Figure 4.

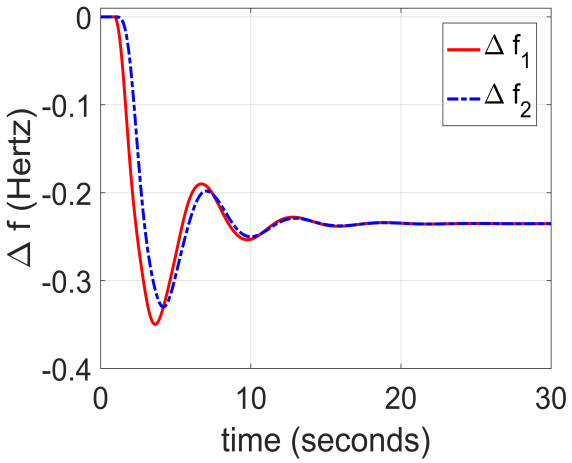

Figure 3. Frequency measurement under data integrity attack.

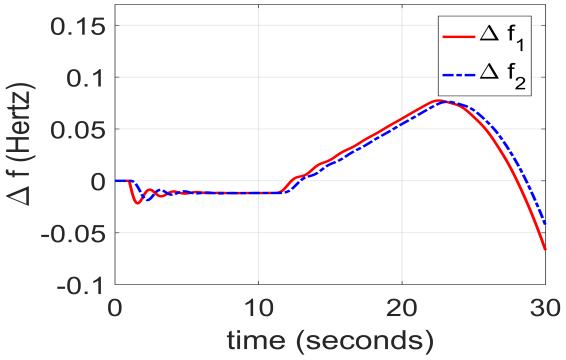

Figure 4. Frequency measurement under timing attack.

Under template attack, for instance, the ACE is scaled five times, i.e., $a = 5$, the response becomes oscillatory as depicted in Figure 5.

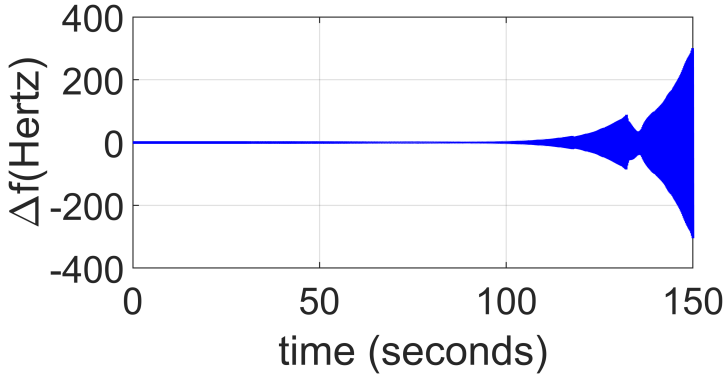

Figure 5. Frequency measurement under scaling attack.

In a random attack, the ACE value for some instance is blocked and provided with some random values, say from -1 to 1. The ACE picks up some random value from this range instead of the original value. As shown in Figure 6, the frequency excursions occur in an abrupt manner around the ideal 0 baseline, making the response unstable.

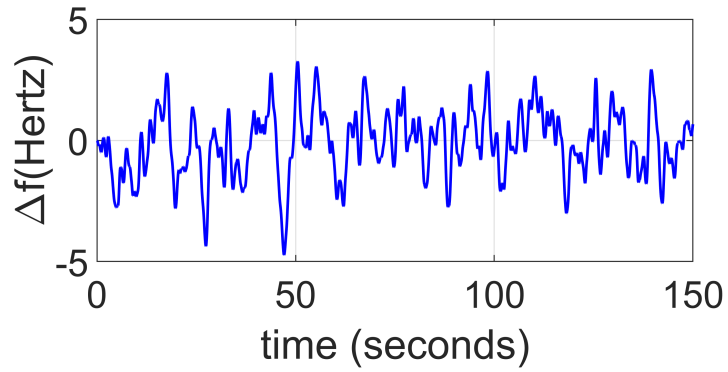

Figure 6. Frequency measurement under random attack.

A ramp attack is executed when we replace the continuously changing ACE with a constant. Under this attack, the frequency response increases by $+b$ or decreases by $-b$ with that constant slope and never comes to zero thereby making system unstable as shown in Figure 7 for $b = 2$.

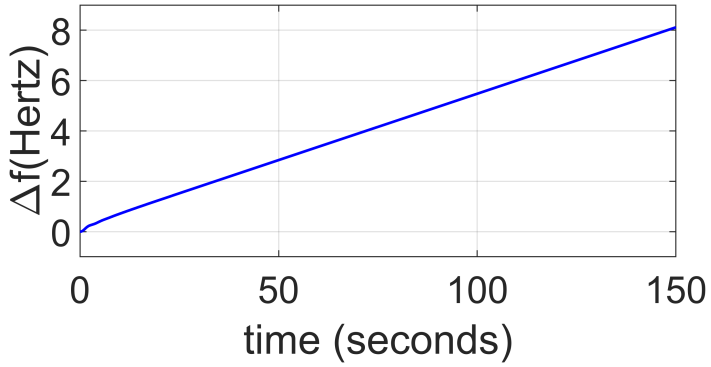

Figure 7. Frequency measurement under ramp attack.

In a pulse attack, a continuous pulsating input is given in channel of *ACE* which completely disturbs the response as shown in Figure 8. Here, the amplitude of pulsating input is 5. The intensity of fluctuation from the baseline depends on the amplitude of the pulse given; the higher the amplitude, the higher the oscillations and the more unstable system the becomes.

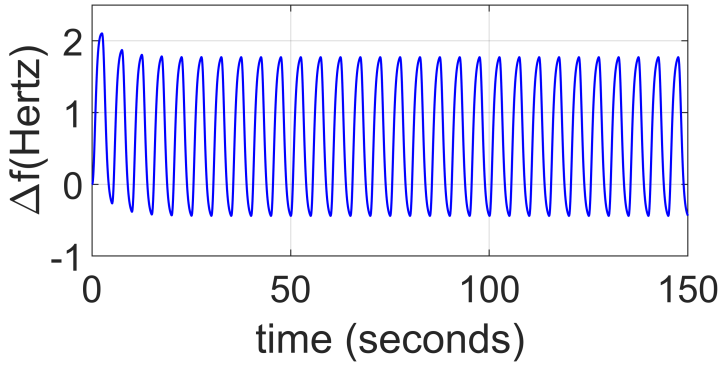

Figure 8. Frequency measurement under pulse attack.

In a time-delay attack, an attacker makes sure that the incoming *ACE* values do not reach to the controller on time and a delay is inculcated into the system, then due to the delayed *ACE* values, the response becomes quite unstable after some time as shown in Figure 9. Here, a delay of 5 s was given to the system and approximately after 105 s system starts oscillating.

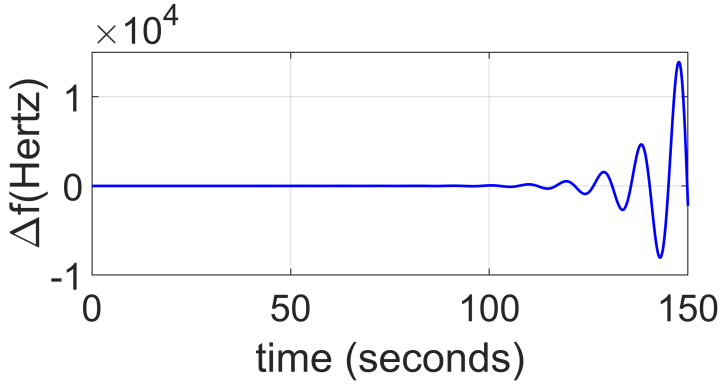

Figure 9. Frequency measurement under time delay attack.

Under bias injection attack, as described in Figure 1 the block named as "bias" is hindered or manipulated by the attacker under this kind of attack as shown in Figure 10. It is evident that the response instantly drops from the base line and remains constant

thereby creating the fixed variation in the frequency reading. Similarly, Figure 11, shows the non-zero fluctuation when bias is negative.

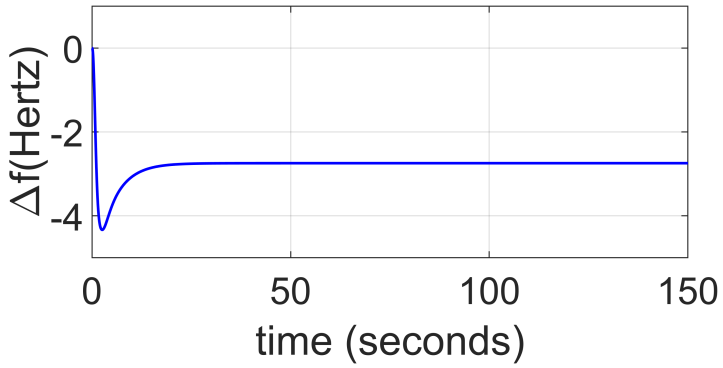

Figure 10. Frequency measurement under positive bias injection attack.

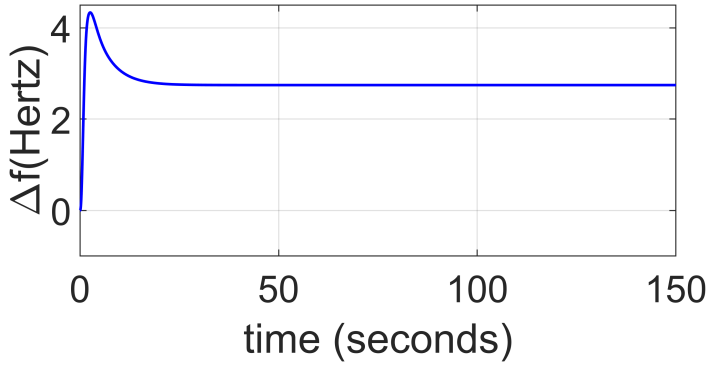

Figure 11. Frequency measurement under negative bias injection attack.

The location based attack is also a serious type of attack. The most common type in this category is load attack. The simulation studies for such type of attack with $\Delta P_L = 0.01 + \delta$ where δ is Gaussian random signal with mean zero and variation 0.1 is shown in Figure 12. It is clear that the frequency measurements are fluctuating around the zero base line.

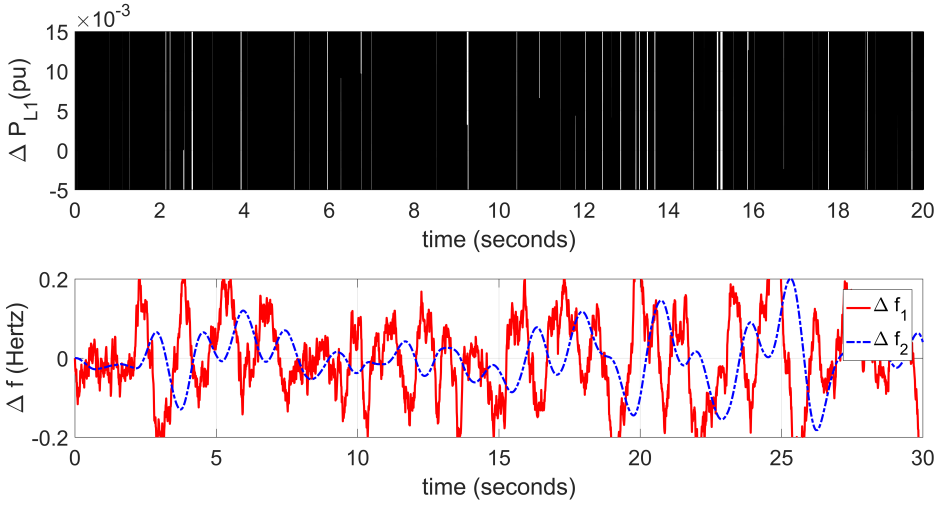

Figure 12. Frequency measurement under load attack ΔP_L.

Based on the simulation studies and considering the control theory aspect, the following observations can be made:

1. The integrity attack actually produces a constant bias in the scheduled frequency and such an attack can be eliminated easily.
2. In a timing attack, if the delay identification is possible or the upper bound on the delay is predicted then delay compensation schemes could be applied as mitigation tools.
3. The template attack simulated in this paper is the amplification of the error signal, and such an attack is among the most dangerous attacks as it immediately amplifies the signal and even the noise present in the network.
4. The random attacks are often probabilistic in nature and such attacks can be modeled with the stochastic control theory.
5. The nature of ramp attack presented in simulation studies seems to be a jamming type as the measurements received are fixed and error is not exactly diagnosed.
6. Pulse attack is also one of the dangerous type of cyber-attack as it has fluctuating nature, that is, the magnitude increases or decreases frequently which results into the wear and tear of the electrical grid.
7. Location-based attack as already mentioned are risky and easy to implement as there is a requirement of load perturbations that could be easily injected into the generation system.

Thus, based on the these observations for the attack implementation, the next section will throw light upon the defense strategies.

5. Attack Detection and Prevention

In this section, we present a brief survey of the existing control approaches to limit the adversary attempts which thwart the LFC operation. The main idea behind the detection and prevention is the observation and prediction. In the control center where LFC operation is carried out, a real-time database is available from the the various kinds of measurement data, when the LFC suffers attacks and unable to receive the measurement data (for example, in case of time-delay attack), the control center immediately performs the data prediction algorithm to predict the delayed or lost data in order to estimate and pass the lost data to the control center thereby making LFC operation to restore smoothly and frequency regulation performs stably.

5.1. Limited Access in the Control Center

The basic prevention is the limited access to the supervisory control and data acquisition or computer systems in the control center. Avoiding external peripheral devices such as USB sticks, hard disk to plug in the computer is one of the physical prevention. The other option is the usage of security standards such as IEC 62351 to safeguard smart grids by specifying cipher suites (authentication, integrity protection and encryption algorithms) [28]. The other option is to simply suspend the LFC operation in case of attack.

5.2. DoS Prevention

Different methods based on DoS attack have been studied on the LFC system of interconnected power system in power grid. From control theory viewpoint, DoS activity in system is incorporated by modeling the system into a switched system (on/off in sensing loop of power system) and then switched system control theory is applied to strengthen the resilience in LFC operation, for example, state feedback controller [29], sliding mode control [30], etc.

The authors of [31] proposed a method that uses data prediction based on deep autoencoder extreme learning machine to defend against DoS attacks. A weighted H_1-based resilient control technique [32] is proposed to detect and mitigate the DoS attack. Game theoretic topology [33,34] for mitigation is also beneficial here. The event-triggered resilient control is now gaining attraction to deal DoS attack [35–38]. A novel filter structure has been proposed and a sub-optimal distributed resilient filtering scheme has been developed to prevent micro-grid against malicious cyber threat [39].

5.3. False Data Injection Prevention

Watermarking-based defense techniques [40,41] are highly popular schemes which actually conceptualize the identification of attack by matching the artificially injected probability-based sensor noise to measurement with the corrupted one. An algorithm based on a state estimator serves a suitable remedy to prevent false data injection also called stealth attack in the power network [42–45]. Characterizing the vulnerabilities based on power flow analysis is also a strong solution [46]. Unknown input observer based schemes reported in [47] are used to determine and mitigate false data injection attack. Functional observer based methodologies for optimal LFC operation under cyber-attack are also introduced in [48,49]. False data injection detection can be analyzed under reachability framework where the attacker acquires access to the states of the power system [50]. The scaling and unknown disturbance attack can also be detected using support vector machine concepts [51] and multi-layer perceptron classifier-based approach [52].

The cyber-attack can also be avoided by maintaining the LFC operation in a safe domain by finding the appropriate state constraints and raising alarm if the state is out of this domain [53]. A set-theoretic approach for false data detection is employed to observe the adversary [54]. A model (real-time load forecast) [55], linear inequality matrix [56], and feedback linearization control-based [57] detection and mitigation serves a useful algorithm in LFC operation. Recently, an optimal two-stage Kalman filtering approach has been proposed to handle the template attacks and has been validated on benchmark mulit-area power systems [58]. In [59], the authors suggested installing an automatic intrusion mitigation unit supported with PID controller that can not only protect the LFC operation against the cyber-attack, but also against power system model uncertainties and external noises.

5.4. Time Delay Mitigation

Time delays are evident and unavoidable in cyber-physical systems, however the intentional delay intrusion can cause catastrophe to system. A two-tiered mitigation policy based on machine learning [60] is successfully implemented to counter the delay in LFC operation. A time-delay estimator to estimate any time delays to avoid delay based attack is introduced in [61] and disturbance rejection is performed using the traditional PID controller.

Few more detection and mitigation strategies for the resilient LFC framework can be found in the comprehensive survey performed in [62].

6. Hardware Validation

Apart from theoretical analysis, the hardware implementation and real-time testing is necessary to ensure the proper safety of LFC operation. In view of this, experimental validation on IEEE 16-bus system [63] and CPS security test bed [64] are performed. Testing of consensus-based LFC operation on renewable energy micro-grid is conducted in [65]. OPAL RT [66] is also a suitable platform to test the proposed cybersecurity solutions to LFC operation, for example, the authors of [67] proposed an observer-based resilient control scheme and utilizes OPAL-RT for validation. In fact, OPAL-RT provides integration of emulated network with equipment and power grid dynamics simulation to assess the network behavior under different types of cyber-attack. The advanced laboratory testing methods have been elaborated in [68] to carry out the electric grid simulations. The other evaluation methods, for example, the distributed DOS and man-in-the-middle attack using real-time simulations and hardware-in-loop techniques have been studied in [69].

7. Conclusions and Future Work

Safe and reliable operation of the LFC is the prime concern in power generation. LFC operation in power systems is actually a CPS which requires researchers from system, control, and information engineering. In the present study, vulnerabilities of LFC operation in the smart grid, different kinds of attacks in the system, and their defense measures to

increase the security of the future power systems have been discussed. The article also provides a preliminary review that allows students, researchers, and practitioners to gain a fundamental understanding of the nature of cyber-attack and defense in LFC operation of power systems.

There are many research gaps for control engineering where they can contribute to CPS security in LFC operation of power systems, such as identification of critical resources, prediction and detection of attacks schemes, and robust and optimal attack resilient techniques. In addition, digital protection, sampling strategies, reachability analysis, and machine learning tools can be effective tools in the near future for designing a strong defense framework in the power sector.

These days, data-driven and learning-based control schemes are gaining increasing popularity in the LFC operation. For instance, machine learning tools such as batch and online learning algorithms (supervised and semisupervised) can be utilized with decision- and feature-level fusion attack modeling, detection, and defense techniques [70]. The reinforcement learning methods [71] for the adaptive control law in LFC operation could possibly be the next extension for the cybersecurity of electric grid. Artificial neural network-based observer and state estimation via Kalman filtering methods (for example, the work in [72,73] and references therein) contribute toward identifying false data detection. The key idea behind all these techniques is that the LFC problem is formulated in a way that the measurements are augmented with the additional signal. This signal may be the noise term, and based on the nature of the noise, it is predicted if the attack occurred or not. These strategies are still at its nascent stage and a full-fledged analysis is still required.

Author Contributions: Conceptualization, S.S. and S.B.; Formal analysis, S.S., S.B. and R.G.; Funding acquisition, S.B.; Investigation, S.S., S.B. and R.G.; Methodology, S.S. and S.B.; Project administration, S.S. and S.B.; Supervision, S.S.; Visualization, R.G.; Writing—original draft, S.S., S.B. and R.G.; Writing—review and editing, S.S., S.B. and R.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the School of Computer Science and Engineering, Sacred Heart University, Fairfield, CT 06825, USA.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Song, H.; Fink, G.; Jeschke, S. *Security and Privacy in Cyber-Physical Systems*; Wiley Online Library: Vienna, Austria, 2017.
2. Weerakkody, S.; Ozel, O.; Mo, Y.; Sinopoli, B. Resilient control in cyber-physical systems: Countering uncertainty, constraints, and adversarial behavior. *Found. Trends Syst. Control* **2019**, *7*, 1–252.
3. Xie, L.; Ilic, M.D. Module-based modeling of cyber-physical power systems. In Proceedings of the 2008 the 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 513–518.
4. Liu, Y.; Peng, Y.; Wang, B.; Yao, S.; Liu, Z. Review on cyber-physical systems. *IEEE/CAA J. Autom. Sin.* **2017**, *4*, 27–40. [CrossRef]
5. Pasqualetti, F.; Dörfler, F.; Bullo, F. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In Proceedings of the 2011 50th IEEE Conference on Decision and Control and European Control Conference, Orlando, FL, USA, 12–15 December 2011; pp. 2195–2201.
6. Ding, D.; Han, Q.L.; Xiang, Y.; Ge, X.; Zhang, X.M. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* **2018**, *275*, 1674–1683. [CrossRef]
7. Dibaji, S.M.; Pirani, M.; Flamholz, D.B.; Annaswamy, A.M.; Johansson, K.H.; Chakrabortty, A. A systems and control perspective of CPS security. *Annu. Rev. Control* **2019**, *47*, 394–411. [CrossRef]
8. Bhatia, S.; Kush, N.S.; Djamaludin, C.; Akande, A.J.; Foo, E. Practical modbus flooding attack and detection. In *Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014) [Conferences in Research and Practice in Information Technology, Volume 149]*; Australian Computer Society, Inc.: Darlinghurst, Australia, 2014; pp. 57–65.
9. Pour, M.M.; Anzalchi, A.; Sarwat, A. A review on cyber security issues and mitigation methods in smart grid systems. In Proceedings of the SoutheastCon 2017, Charlotte, NC, USA, 31 March–2 April 2017; pp. 1–4.

10. Koutsoukos, X.; Neema, H.; Martins, G.; Bhatia, S.; Sztipanovits, J.; Stouffer, K.; Tang, C.Y.; Candell, R. Performance evaluation of secure industrial control system design: A railway control system case study. In Proceedings of the 2016 Resilience Week (RWS), Chicago, IL, USA, 16–18 August 2016; pp. 101–108.
11. Parian, C.; Guldimann, T.; Bhatia, S. Fooling the Master: Exploiting Weaknesses in the Modbus Protocol. *Procedia Comput. Sci.* **2020**, *171*, 2453–2458. [CrossRef]
12. Farwell, J.P.; Rohozinski, R. Stuxnet and the future of cyber war. *Survival* **2011**, *53*, 23–40. [CrossRef]
13. Sánchez, H.S.; Rotondo, D.; Escobet, T.; Puig, V.; Quevedo, J. Bibliographical review on cyber attacks from a control oriented perspective. *Annu. Rev. Control* **2019**, *48*, 103–128. [CrossRef]
14. Gheisarnejad, M.; Khooban, M.H.; Dragicevic, T. The future 5G network based secondary load frequency control in maritime microgrids. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**. [CrossRef]
15. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 13–27. [CrossRef]
16. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 645–658. [CrossRef]
17. Pappachen, A.; Fathima, A.P. Critical research areas on load frequency control issues in a deregulated power system: A state-of-the-art-of-review. *Renew. Sustain. Energy Rev.* **2017**, *72*, 163–177. [CrossRef]
18. Saxena, S.; Fridman, E. Event-triggered load frequency control via switching approach. *IEEE Trans. Power Syst.* **2020**, *35*, 4484–4494. [CrossRef]
19. Saxena, S. Load frequency control strategy via fractional-order controller and reduced-order modeling. *Int. J. Electr. Power Energy Syst.* **2019**, *104*, 603–614. [CrossRef]
20. Saxena, S.; Hote, Y.V. Stabilization of perturbed system via IMC: An application to load frequency control. *Control Eng. Pract.* **2017**, *64*, 61–73. [CrossRef]
21. Hanwate, S.; Hote, Y.V.; Saxena, S. Adaptive policy for load frequency control. *IEEE Trans. Power Syst.* **2017**, *33*, 1142–1144. [CrossRef]
22. Smith, E.; Corzine, S.; Racey, D.; Dunne, P.; Hassett, C.; Weiss, J. Going beyond cybersecurity compliance: What power and utility companies really need to consider. *IEEE Power Energy Mag.* **2016**, *14*, 48–56. [CrossRef]
23. Case, D.U. Analysis of the cyber attack on the Ukrainian power grid. *Electr. Inf. Shar. Anal. Cent. (E-ISAC)* **2016**, *21*, 388.
24. Weerakkody, S.; Sinopoli, B. Challenges and opportunities: Cyber-physical security in the smart grid. In *Smart Grid Control*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 257–273.
25. Kundur, P.; Balu, N.J.; Lauby, M.G. *Power System Stability and Control*; McGraw-Hill New York: New York, NY, USA, 1994; Volume 7.
26. Saxena, S.; Hote, Y.V. Load frequency control in power systems via internal model control scheme and model-order reduction. *IEEE Trans. Power Syst.* **2013**, *28*, 2749–2757. [CrossRef]
27. Sarangan, S.; Singh, V.K.; Govindarasu, M. Cyber attack-defense analysis for automatic generation control with renewable energy sources. In Proceedings of the 2018 North American Power Symposium (NAPS), Fargo, ND, USA, 9–11 September 2018; pp. 1–6.
28. Fries, S.; Hof, H.J.; Seewald, M. Enhancing IEC 62351 to improve security for energy automation in smart grid environments. In Proceedings of the 2010 Fifth International Conference on Internet and Web Applications and Services, Barcelona, Spain, 9–15 May 2010; pp. 135–142.
29. Liu, S.; Liu, X.P.; El Saddik, A. Denial-of-service (DoS) attacks on load frequency control in smart grids. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 Feburary 2013; pp. 1–6.
30. Wu, C.; Wu, L.; Liu, J.; Jiang, Z.P. Active defense-based resilient sliding mode control under denial-of-service attacks. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 237–249. [CrossRef]
31. Li, Y.; Zhang, P.; Ma, L. Denial of service attack and defense method on load frequency control system. *J. Frankl. Inst.* **2019**, *356*, 8625–8645. [CrossRef]
32. Cheng, Z.; Yue, D.; Hu, S.; Xie, X.; Huang, C. Detection-based weighted H_∞ LFC for multi-area power systems under DoS attacks. *IET Control Theory Appl.* **2019**, *13*, 1909–1919. [CrossRef]
33. Srikantha, P.; Kundur, D. Denial of service attacks and mitigation for stability in cyber-enabled power grid. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–20 Feburary 2015; pp. 1–5.
34. Yuan, Y.; Sun, F.; Liu, H. Resilient control of cyber-physical systems against intelligent attacker: A hierarchal stackelberg game approach. *Int. J. Syst. Sci.* **2016**, *47*, 2067–2077. [CrossRef]
35. Sun, H.; Peng, C.; Wang, Y.; Tian, Y.C. Output-based resilient event-triggered control for networked control systems under denial of service attacks. *IET Control Theory Appl.* **2019**, *13*, 2521–2528. [CrossRef]
36. Shen, Y.; Fei, M.; Du, D. Cyber security study for power systems under denial of service attacks. *Trans. Inst. Meas. Control* **2019**, *41*, 1600–1614. [CrossRef]
37. Liu, J.; Gu, Y.; Zha, L.; Liu, Y.; Cao, J. Event-Triggered H_∞ Load Frequency Control for Multiarea Power Systems Under Hybrid Cyber Attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1665–1678. [CrossRef]
38. Chen, X.; Wang, Y.; Hu, S. Event-triggered quantized H_∞ control for networked control systems in the presence of denial-of-service jamming attacks. *Nonlinear Anal. Hybrid Syst.* **2019**, *33*, 265–281. [CrossRef]

39. Chen, W.; Ding, D.; Dong, H.; Wei, G. Distributed resilient filtering for power systems subject to denial-of-service attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1688–1697. [CrossRef]
40. Huang, T.; Satchidanandan, B.; Kumar, P.; Xie, L. An online detection framework for cyber attacks on automatic generation control. *IEEE Trans. Power Syst.* **2018**, *33*, 6816–6827. [CrossRef]
41. Mo, Y.; Chabukswar, R.; Sinopoli, B. Detecting integrity attacks on SCADA systems. *IEEE Trans. Control. Syst. Technol.* **2013**, *22*, 1396–1407.
42. Dan, G.; Sandberg, H. Stealth attacks and protection schemes for state estimators in power systems. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 214–219.
43. Teixeira, A.; Amin, S.; Sandberg, H.; Johansson, K.H.; Sastry, S.S. Cyber security analysis of state estimators in electric power systems. In Proceedings of the 49th IEEE conference on decision and control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 5991–5998.
44. Zhong, H.; Du, D.; Li, C.; Li, X. A novel sparse false data injection attack method in smart grids with incomplete power network information. *Complexity* **2018**, *2018*, 8503825. [CrossRef]
45. Alhalali, S.; Nielsen, C.; El-Shatshat, R. Mitigation of cyber-physical attacks in multi-area automatic generation control. *Int. J. Electr. Power Energy Syst.* **2019**, *112*, 362–369. [CrossRef]
46. Tuttle, M.; Wicker, B.; Poshtan, M.; Callenes, J. Algorithmic approaches to characterizing power flow cyber-attack vulnerabilities. In Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 Feburary 2019; pp. 1–5.
47. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
48. Alhelou, H.H.; Golshan, M.E.H.; Hatziargyriou, N.D. A decentralized functional observer based optimal LFC considering unknown inputs, uncertainties, and cyber-attacks. *IEEE Trans. Power Syst.* **2019**, *34*, 4408–4417. [CrossRef]
49. Lygeros, J. On reachability and minimum cost optimal control. *Automatica* **2004**, *40*, 917–927. [CrossRef]
50. Esfahani, P.M.; Vrakopoulou, M.; Margellos, K.; Lygeros, J.; Andersson, G. Cyber attack in a two-area power system: Impact identification using reachability. In Proceedings of the 2010 American Control Conference, Baltimore, MD, USA, 30 June–2 July 2010; pp. 962–967.
51. Bi, W.; Zhang, K.; Li, Y.; Yuan, K.; Wang, Y. Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis. *IEEE Syst. J.* **2019**, *13*, 2859–2868. [CrossRef]
52. Chen, C.; Zhang, K.; Yuan, K.; Zhu, L.; Qian, M. Novel detection scheme design considering cyber attacks on load frequency control. *IEEE Trans. Ind. Inform.* **2017**, *14*, 1932–1941. [CrossRef]
53. Kontouras, E.; Tzes, A.; Dritsas, L. Impact analysis of a bias injection cyber-attack on a power plant. *IFAC-PapersOnLine* **2017**, *50*, 11094–11099. [CrossRef]
54. Kontouras, E.; Anthony, T.; Dritsas, L. Set-theoretic detection of data corruption attacks on cyber physical power systems. *J. Mod. Power Syst. Clean Energy* **2018**, *6*, 872–886. [CrossRef]
55. Sridhar, S.; Govindarasu, M. Model-based attack detection and mitigation for automatic generation control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591. [CrossRef]
56. Zhao, F.; Yuan, J.; Wang, N.; Zhang, Z.; Wen, H. Secure Load Frequency Control of Smart Grids under Deception Attack: A Piecewise Delay Approach. *Energies* **2019**, *12*, 2266. [CrossRef]
57. Esfahani, P.M.; Vrakopoulou, M.; Margellos, K.; Lygeros, J.; Andersson, G. A robust policy for automatic generation control cyber attack in two area power network. In Proceedings of the 49th IEEE Conference on Decision and Control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 5973–5978.
58. Ayyarao, T.S.; Kiran, I.R. A Two-Stage Kalman Filter for Cyber-Attack Detection in Automatic Generation Control System. *J. Mod. Power Syst. Clean Energy* **2021**. [CrossRef]
59. Badal, F.R.; Nayem, Z.; Sarker, S.K.; Datta, D.; Rahman Fahim, S.; Muyeen, S.; Islam Sheikh, M.; Das, S.K. A Novel Intrusion Mitigation Unit for Interconnected Power Systems in Frequency Regulation to Enhance Cybersecurity. *Energies* **2021**, *14*, 1401. [CrossRef]
60. Lou, X.; Tran, C.; Tan, R.; Yau, D.K.; Kalbarczyk, Z.T. Assessing and mitigating impact of time delay attack: A case study for power grid frequency control. In Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems, Montreal, QC, Canada, 16–18 April 2019; pp. 207–216.
61. Sargolzaei, A.; Yen, K.K.; Abdelghani, M.N. Preventing time-delay switch attack on load frequency control in distributed power systems. *IEEE Trans. Smart Grid* **2015**, *7*, 1176–1185. [CrossRef]
62. Mohan, A.M.; Meskin, N.; Mehrjerdi, H. A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems. *Energies* **2020**, *13*, 3860. [CrossRef]
63. Tan, R.; Nguyen, H.H.; Foo, E.Y.; Yau, D.K.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Modeling and mitigating impact of false data injection attacks on automatic generation control. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1609–1624. [CrossRef]
64. Ashok, A.; Wang, P.; Brown, M.; Govindarasu, M. Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed. In Proceedings of the 2015 IEEE Power & Energy Society General Meeting, Denver, CO, USA, 26–30 July 2015; pp. 1–5.

65. Wang, B.; Sun, Q.; Han, R.; Ma, D. Consensus-based secondary frequency control under denial-of-service attacks of distributed generations for microgrids. *J. Frankl. Inst.* **2019**, *358*, 114–130. [CrossRef]
66. Cybersecurity. Available online: https://www.opal-rt.com/cybersecurity-overview/ (accessed on 10 December 2019).
67. Khalghani, M.R.; Solanki, J.; Solanki, S.K.; Khooban, M.H.; Sargolzaei, A. Resilient Frequency Control Design for Microgrids Under False Data Injection. *IEEE Trans. Ind. Electron.* **2020**, *68*, 2151–2162. [CrossRef]
68. Montoya, J.; Brandl, R.; Vishwanath, K.; Johnson, J.; Darbali-Zamora, R.; Summers, A.; Hashimoto, J.; Kikusato, H.; Ustun, T.S.; Ninad, N.; et al. Advanced laboratory testing methods using real-time simulation and hardware-in-the-loop techniques: A survey of smart grid international research facility network activities. *Energies* **2020**, *13*, 3267. [CrossRef]
69. Liu, Z.; Wang, Q.; Tang, Y. Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems. *IEEE Access* **2020**, *8*, 95997–96005. [CrossRef]
70. Ozay, M.; Esnaola, I.; Vural, F.T.Y.; Kulkarni, S.R.; Poor, H.V. Machine learning methods for attack detection in the smart grid. *IEEE Trans. Neural Netw. Learn. Syst.* **2015**, *27*, 1773–1786. [CrossRef] [PubMed]
71. Yan, Z.; Xu, Y. A multi-agent deep reinforcement learning method for cooperative load frequency control of a multi-area power system. *IEEE Trans. Power Syst.* **2020**, *35*, 4599–4608. [CrossRef]
72. Abbaspour, A.; Sargolzaei, A.; Forouzannezhad, P.; Yen, K.K.; Sarwat, A.I. Resilient control design for load frequency control system under false data injection attacks. *IEEE Trans. Ind. Electron.* **2019**, *67*, 7951–7962. [CrossRef]
73. Foroutan, S.A.; Salmasi, F.R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 161–171. [CrossRef]