energies

MDPI

Review

A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems

Athira M. Mohan, Nader Meskin * and Hasan Mehrjerdi

The Department of Electrical Engineering, Qatar University, Doha 2713, Qatar; amohan@qu.edu.qa (A.M.M.); hasan.mehrjerdi@qu.edu.qa (H.M.)

* Correspondence: nader.meskin@qu.edu.qa

Received: 7 June 2020; Accepted: 4 July 2020; Published: 28 July 2020

Abstract: 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. The power system controllers should have the ability to maintain power system stability. Three important quantities that should be effectively controlled to maintain the stability of power systems are frequency, rotor angle, and voltage. The voltage control in power systems maintains the voltage and reactive power within the required limits and the power factor control enhances the efficiency of power distribution systems by improving load power factors. Among various controls, the frequency control 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, load frequency control (LFC) systems cannot handle complicated data validation algorithms, making them more vulnerable to disturbances and cyber-attacks. In addition, the LFC system has extended digital layers with open communication networks and is designed to operate with less human intervention. Moreover, the frequency fluctuation due to load change or cyber-attack in one area affects all other interconnected areas, and thus threatens the stability of the entire network. Due to these circumstances, research activities are still carried out in the field of frequency control and cyber-security. In this paper, a comprehensive review of the cyber-security of the LFC mechanism in the power system is presented. The highlights of the paper include the identification of attack points of different configurations of the LFC system, discussion of the attack strategies, formulation of various attack models, and a brief review of the existing detection and defense mechanisms against cyber-attacks on LFC.

Keywords: load frequency control system; cyber-security; cyber-attacks; area control error (ACE); tie-line power

1. Introduction

The field of power systems is continuously enhancing through the integration of modern generation schemes, the latest control techniques, advancement in data transmission through open communication networks, and development of security measures of communication network through smart systems. However, it is observed that the integration of new technologies also presents new challenges to power systems. For instance, the incorporation of renewable energy sources (RES) in electricity generation acts as a good choice of solution for pollution and environmental issues, but the operation of power systems with RES produce unsatisfactory frequency stability performance due to their intermittent output power [1]. However, RES have been accepted as a major energy source in some countries due to the expansion of RES technologies, usage of smart inverters [2], and smart

controllable loads [3] that support distributed generation and RES. Smart inverters are greatly used in power grids with distributed energy resources (DER) as they not only act as an interface between DER and grid, but also help to regulate power flow and detect faults. However, smart technologies are prone to cyber-attack as they support wired and wireless communication technologies and can affect the power system stability [2,3]. In addition, Internet of Things (IoT)-based wide-area control and monitoring techniques have been developed for smart power grids with intermittent DER, which can also contribute to attack vulnerability [4–7]. Therefore, from the power system operation point of view, stability enhancement and attack-resilient power system control are highly significant fields that require continuous research. Towards this, this paper is mainly concerned with the frequency stability and cyber-security of the load frequency control (LFC) system.

The frequency performance of a power system has to be monitored and regulated as the frequency deviation from the nominal value can directly affect its operation, security, and reliability. The imbalance between the power consumption by load and power generation causes the frequency of the generator to deviate from its nominal value. 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 [8]. Various frequency regulation methods are adopted to improve the frequency performance and it happens at three levels. The first two levels are performed through the control of generation units and the third level is implemented through loads, for instance, load shedding in adverse situations. These three levels of frequency control are called governor control or primary control, secondary or supplementary control, and tertiary control [9]. The primary control unit detects the frequency/speed changes of the generator unit using a sensor and, according to the detected changes, the governor and turbine settings are altered to control the generator power output [10]. The manner in which participating generation units act in frequency control is called automatic generation control (AGC) [11]. AGC is a secondary control loop that fine-tunes the system frequency to the nominal value [10]. The AGC of power systems allows controlling the permanent frequency deviation that can affect the power system operation and stability. It also shares the power regulation burden among the interconnected power system or multi-area power system via tie-lines. This helps to retain the net interchange of power among the neighboring areas within scheduled values while regulating the area frequencies [11]. Tertiary control is provided in succession to secondary control to guarantee sufficient secondary control reserve through manual or automatic change of generator or participating load working points. The changes are implemented through load control or load shedding, redistribution of generator outputs of secondary control under economic considerations, power interchange program changes, and by connecting or tripping power [12,13]. This survey is concerned with primary and secondary control schemes and a tertiary control is not investigated in this literature.

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 [14]. 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 power system, etc. [14]. 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 [15]. 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 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 [10]. The defense mechanisms of the LFC system generally include resilient control algorithms.

The smart grid (the power transmission system with bidirectional information flow) technology is another class of power systems that implements LFC scheme. The security properties of smart grid or microgrid or any other power system are combination of three basic attributes, namely, "Availability", "Integrity", and "Confidentiality" [16]. The power system cyber-attacks can be classified on the basis of these three high level security requirements [15].

Availability ensures the timely and reliable availability of the information in the transmission network of the power system. From the control point of view, it is the property of the control system or the system components like sensors, actuators, and controllers, to be accessible and operational by an authorized entity upon demand [16]. The attacks like denial of service (DoS), affect the information availability in communication channels and is a threat to such security requirement. The integrity of a system refers to the capability to achieve operational goals through the prevention and detection of attacks on communication channels among actuators, sensors, and controllers [16]. The power system attacks that threaten integrity generally modify the data transferred through the communication channels of the power system. The telemetered data from the RTU of power systems such as line flows or power signals are mainly vulnerable to integrity attacks. Data integrity attacks are serious threats that can endanger the stable operation of grids or power systems [15]. Confidentiality refers to the ability of the system to keep information inaccessible to unauthorized users. This prevents the inferring of state of physical systems by eavesdropping communication of sensors, actuators, and controllers [16]. Therefore, to ensure the three security attributes, highly effective detection and defense mechanisms against cyber-attacks are required.

The literature surveys conducted in the field of LFC systems mainly concentrate on the LFC techniques of conventional and distribution power systems [17], assessment of the impact of cyber-attacks using unit commitment (UC) models [18], risk assessment, and risk mitigation methodologies for the protection of physical power applications and associated cyber infrastructure [10]; LFC models and existing control strategies for diverse configurations of power systems [19]; and cyber-attacks on operations of power systems [15]. Apart from these, some reviews also focus on the attack impact analysis, modeling of networked control systems or cyber physical systems (CPS) under cyber-attacks, and existing attack mitigation techniques in general [16,20,21]. However, a literature survey of the LFC system considering the mathematical models of different LFC configurations, various types of attacks and attack strategies in the LFC system, identification of attack points of different LFC configurations, and existing countermeasures available against various attacks still remain as a gap. Therefore, this review aims to provide a complete discussion regarding the aforementioned areas of LFC system.

The section arrangements of this paper are as follows. Section 2 aims to identify the attack points of different configurations of the LFC system in which cyber-attacks are studied and analyzed. Section 3 provides a brief description of the various types of attacks that can happen in the LFC scheme and attack modeling. Section 4 introduces existing countermeasures against various types of cyber-attacks of LFC system. Future research areas and conclusions are presented in Sections 5 and 6, respectively.

2. LFC System Configurations

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 [10]. 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) [22]. The decisions from the control center are then transmitted to actuators for the implementation of required changes through field

devices or actuators [10]. Primary control or governor control, secondary control scheme with the help of traditional supervisory control and data acquisition (SCADA), 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 [10].

The governor control (local control) system does not rely on the SCADA telemetry system, as the rotor speed measurements of the single generator are locally sensed [10]. 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. However, the control module/controller of this scheme do 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 [10].

Different from governor control, the secondary control of LFC scheme allows the frequency control of multiple generators that are operated in parallel, sharing large electrical loads. 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. In modern electric grid and smart grid, PMU is used for real-time monitoring and control.

The typical LFC loop is given in Figure 1. In conventional power systems, hydro, thermal, and nuclear power plants are the integral power generation components. However, due to the alarming environmental issues, RES started being a vital component in power systems [17]. Therefore, the LFC system with RES is also briefly addressed in this section.

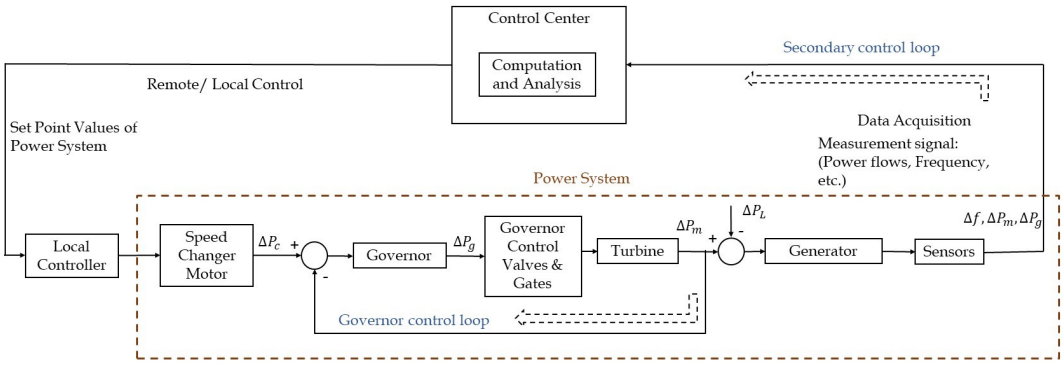

Figure 1. A typical load frequency control (LFC) loop.

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 [17]. An increase in the load demand (ΔP_L in Figure 1) creates a decrease in the generator unit frequency (f) from the nominal value, and the frequency stabilization is implemented through the speed control of generation unit turbines. If the load demand is more than the nominal one, the demand–generation imbalance takes place and the kinetic energy (KE) stored in the rotating mass delivers energy to minimize frequency deviation for a very short time [9]. The inertial response contributed by the rotor KE cannot fix the frequency deviation completely. Therefore, subsequently, the governor and secondary control techniques are activated.

The LFC scheme primarily starts with governor control, which is the control of the generation unit using speed regulation or droop characteristics (R). Droop characteristics represent the slope of the governor steady-speed characteristics curve [8]. From the control point of view, it can be viewed as

a proportional controller that ends up with a steady-state frequency deviation. The AGC provides a reset action and adjusts the generation automatically to re-establish the system frequency to the nominal value for the continuous load changes [23]. The secondary control system resets the frequency deviation at steady state to zero value [8]. The AGC scheme is generally applied to the wide area or interconnected power systems.

2.1. Single-Area LFC Scheme

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 [24]. In single-area LFC system, the increase in the load demand (ΔP_L) creates a decrease in the generator frequency (f) and vice versa. The inertial response contributed by the rotating mass cannot bring the generator frequency to the nominal value, and therefore the governor and the secondary controls are implemented as in Figure 2. The block diagram of a single-area LFC system with the specification of cyber-attack points is shown in Figure 2. The cyber and physical layers of LFC are appealing target points for adversaries and the attack points include transmission channels of communication network, computational algorithms at the control center, and physical sensors/actuators [25–28]. Generally, it is assumed that all the generation units in the single-area produce coherent responses to the system load changes. Thus, all the generating units of the single-area is equivalently represented by a single generating unit [8].

The general dynamics equation for a linear single-area power system is given as below and Table 1 lists the parameters of the LFC system model. The generator–load dynamic relation between the mismatch power deviation ($\Delta P_m(t) - \Delta P_L(t)$) and frequency deviation [14] is expressed as

$$\Delta \dot{f}(t) = \frac{1}{M}\Delta P_m(t) - \frac{1}{M}\Delta P_L(t) - \frac{1}{M}D\Delta f(t), \tag{1}$$

and the turbine dynamics is expressed as:

$$\Delta \dot{P}_m(t) = \frac{1}{T_t}\Delta P_g(t) - \frac{1}{T_t}\Delta P_m(t). \tag{2}$$

Table 1. General model parameters of LFC system.

Parameter	Parameter Description	Unit
$\Delta P_m(t)$	Mechanical power change	p.u.
$\Delta P_g(t)$	Governor output change	p.u.
$\Delta P_L(t)$	Load change	p.u.
$\Delta P_c(t)$	Control signal	p.u.
$\Delta P_{tie}(t)$	Tie-line active power deviation	p.u.
$\Delta P_{wind}(t)$	Wind turbine input power change	p.u.
$\Delta P_{solar}(t)$	Solar input power change	p.u.
$\Delta P_w(t)$	Wind turbine output power change	p.u.
$\Delta P_{pv}(t)$	Photovoltaic (PV) output power change	p.u.
$\Delta P_h(t)$	Hydro turbine output power change	p.u.
$\Delta f(t)$	Frequency deviation of the power system	Hz
R	Speed droop characteristic	Hz/p.u.
D	Equivalent damping coefficient	p.u./Hz
M	Equivalent inertia constant	p.u.-s
T_g	Governor time constant	s
T_t	Turbine time constant	s
T_{wt}	Wind turbine time constant	s
T_{pv}	PV time constant	s
T_w	Water starting time constant	s
β	Frequency bias factor	p.u./Hz
N	Number of control areas	-

The governor dynamics can be expressed as

$$\Delta \dot{P}_g(t) = \frac{1}{T_g}\Delta P_c(t) - \frac{1}{RT_g}\Delta f(t) - \frac{1}{T_g}\Delta P_g(t). \quad (3)$$

The state space model can be derived from these basic differential equations for the design of suitable controllers and analysis of cyber-attacks over the LFC scheme. A state space model of LFC system with state variables such as frequency deviation, voltage angle, generator mechanical output, and governor output is given in [14], where the voltage angle is represented as $\Delta\dot{\theta}(t) = \Delta\omega(t)$ and $\Delta\omega(t)$ is the angular frequency deviation in (rad/s). Some models also incorporate time delays that occur in the communication channels during the transmission of sensor measurements and control signals [14]. For the study of cyber-attacks over the LFC scheme, the basic model is altered to incorporate the attack features. The sensor and actuator channels are the main target channels for the adversaries of the LFC system. In the case of single-area LFC system, the adversarial activities are implemented either through the manipulation of system frequency, the actual output power of generators, and governor control signal or the authorized sources are denied access to these signals.

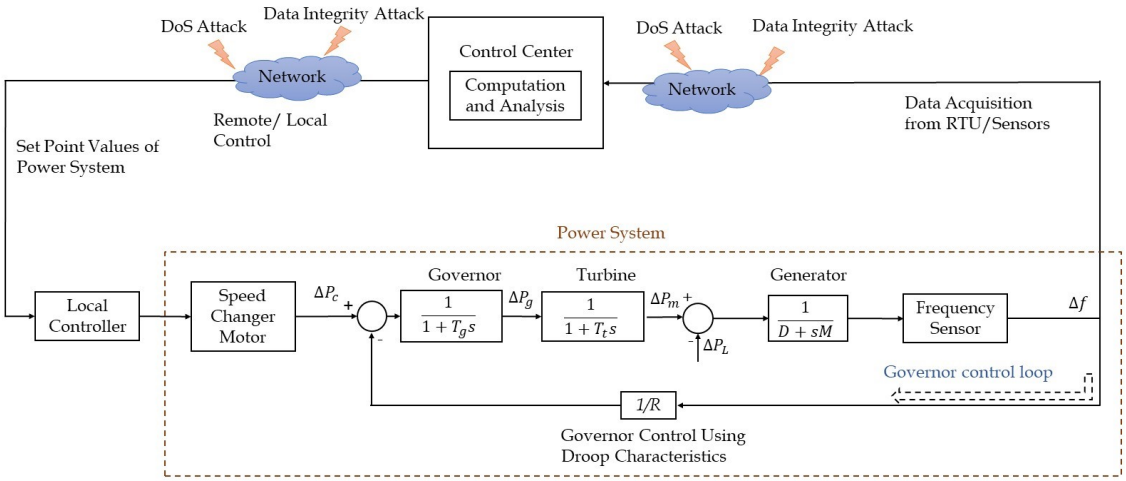

Figure 2. General block diagram of single-area LFC system with attack points.

2.2. Multi-Area LFC Scheme

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 [11]. Here, the frequency control is achieved through the addition of the ACE signal to the feedback loop, which not only accounts for the changes in frequency and exchange of power, but also considers the energy and time error due to the fluctuations in schedule and device [24]. In the interconnected power system, the PMU of electric power grid/RTU of traditional SCADA system sends the sensor measurements such as power system frequency, tie-line power flows, system time deviation, and generator power signals to the control center [24]. AGC relies on the frequency and tie-line power measurements and any manipulation of these measurements due to attacks or load disturbance can have a direct impact on the stability and economic operation [10,29]. Therefore, during the AGC operation, the control center allocates ACEs to respective local controllers and controls frequency deviation and net interchange power of generator sets of each area based on the collected data [23,24].

The general block diagram of the multi-area LFC system (having same area ratings or power capacities) with attack points is given in Figure 3. In the multi-area LFC system, any load change (ΔP_{Li}) in one of the control areas can create frequency deviations in the generator units of the corresponding control area (Δf_i) and in the interconnected area (Δf_j). The increase in load change (ΔP_{Li}) results in the

reduction of generator frequencies (f_i and f_j) and vice versa. Consequently, these frequency variations can result in the deviation of tie-line power value (ΔP^i_{tie}) from the scheduled interchange power value.

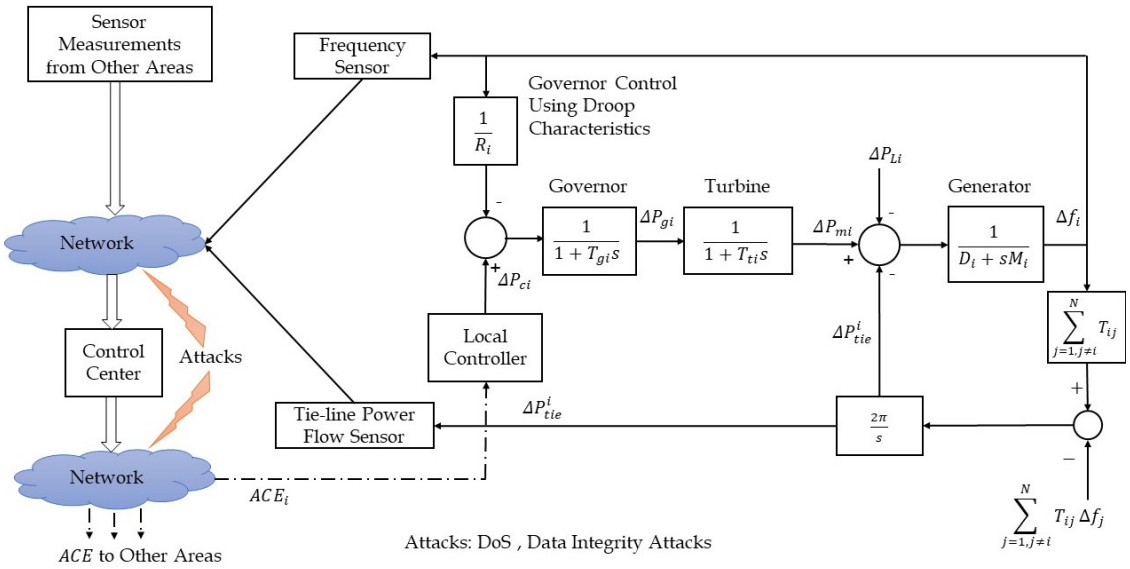

Figure 3. General block diagram of multi-area LFC system with attack points.

The general dynamics equation for a linear multi-area power system is given below [30]. The generator–load dynamic relation between the mismatch power deviation $(\Delta P_{mi}(t) - \Delta P_{Li}(t))$ and frequency deviation of the ith area are expressed as [14]

$$\Delta \dot{f}_i(t) = \frac{1}{M_i}\Delta P_{mi}(t) - \frac{1}{M_i}\Delta P_{Li}(t) - \frac{1}{M_i}D_i\Delta f_i(t) - \Delta P^i_{tie}(t). \tag{4}$$

The turbine dynamics is expressed as

$$\Delta \dot{P}_{mi}(t) = \frac{1}{T_{ti}}\Delta P_{gi}(t) - \frac{1}{T_{ti}}\Delta P_{mi}(t), \tag{5}$$

and the governor dynamics can be expressed as

$$\Delta \dot{P}_{gi}(t) = \frac{1}{T_{gi}}\Delta P_{\mathrm{ci}}(t) - \frac{1}{R_i T_{gi}}\Delta f_i(t) - \frac{1}{T_{gi}}\Delta P_{gi}(t). \tag{6}$$

The tie-line power flow exchange between area i and other areas [31] is given as

$$\Delta P^i_{\mathrm{tie}}(t) = \sum_{j=1, j\neq i}^{N} \Delta P^{ij}_{tie}(t) = \sum_{j=1, j\neq i}^{N} 2\pi T_{ij}\left(\int \Delta f_i(t) - \int \Delta f_j(t)\right), \tag{7}$$

where T_{ij} is the synchronization coefficient. The ACE for area i is expressed as the summation of tie-line power flow and frequency deviation multiplied by the bias factor as follows.

$$ACE_i(t) = \beta_i \Delta f_i(t) + \Delta P^i_{\mathrm{tie}}(t). \tag{8}$$

The $ACE_i(t)$ represents the measured deviations of system frequency and tie-line power export from the nominal values. Here, the area ratings are assumed to be the same and thus the area capacity factor is considered to be one [32,33]. If the area ratings are different, then ACE is given as [32,33]:

$$ACE_i(t) = \beta_i \Delta f_i(t) + \sum_{j=1, j\neq i}^{N} a_{ij} \Delta P_{tie}^{ij}(t), \tag{9}$$

and

$$a_{ij} = \frac{P_{r_i}}{P_{r_j}}, \tag{10}$$

where a_{ij} represents the area capacity factor and P_{r_i}, P_{r_j} represent the power capacities of areas i and j, respectively. Using the frequency and tie-line power flow measurements [25] received from PMU, ACE values for each area is calculated at the control center and transmitted as input control signal to the local controller. ACEs act as the input mechanical power setpoints to the generators of each area and the local controller adjusts power values to keep ACE to the zero value [24,25,34].

The state space models for the analysis and study of cyber-attacks are derived for multi-area systems from the above dynamic equations. A multi-area power system model with uncertainty, generator rate constraint (GRC), and the time delay is provided in [30]. The multi-area power system state space model with proportional integral (PI) controller is provided in [35]. More details regarding the extraction of discrete-time models of control areas, tie-line model, and network model are provided in [36]. The physical and cyber-level modeling of the LFC system is described in [37].

Even though the interconnected structure improves the system performance, it increases the cyber-attack vulnerability through the tie-line input point. For the multi-area systems, the attacker mainly concentrates on the falsification of ACE values through the manipulation of frequency or tie-line power [38]. The attack in one LFC area can be powerful enough to create blackout of the entire power grid [11]. The attack over actuator or sensor channel of the multi-area LFC system can result in the inaccessibility or manipulation of signals like system frequency $(f_i(t))$, tie-line power $(P_{tie}^i(t))$, actuator generator output power $(P_{mi}(t))$, and ACE values $(ACE_i(t))$ of each control area.

Two-Area LFC Scheme

The two-area LFC system is widely used to study the effect of cyber-attacks in multi-area LFC systems due to simplicity and it illustrates the increase of attack points. The mathematical model of the two-area LFC system is formed from the fundamental equations mentioned earlier. The influence of load changes in the generator frequencies and power flows can be analyzed from Figure 4 and it is described as follows [39].

- An increase in the load demand (ΔP_{Lj}) in area j can result in the reduction of generator frequencies (f_i and f_j) and an increase in the power flow to area j.
- If the load demand (ΔP_{Li}) has increased in area i, then it would result in the reduction of generator frequencies (f_i and f_j) and power flow to area j.
- A reduction of load demand (ΔP_{Lj}) in area j would result in the increase of generator frequencies and reduction in power flow to area j.
- A reduction of load demand (ΔP_{Li}) in the area i would result in the increase of generator frequencies and power flow to area j.

The attack points of the two-area LFC system with different area ratings are given in Figure 4 and it is observed that the number of transmission channels is higher compared to the single-area LFC system. Therefore, the impact of attack and deterioration of system performance intensifies in the two-area LFC system as the number of interconnected areas increases. Similar is the case with three-area and four-area power systems. The modeling, controlling, and impact analysis of cyber-attacks of three-area and four-area LFC systems are investigated in [11,19,30,40–48].

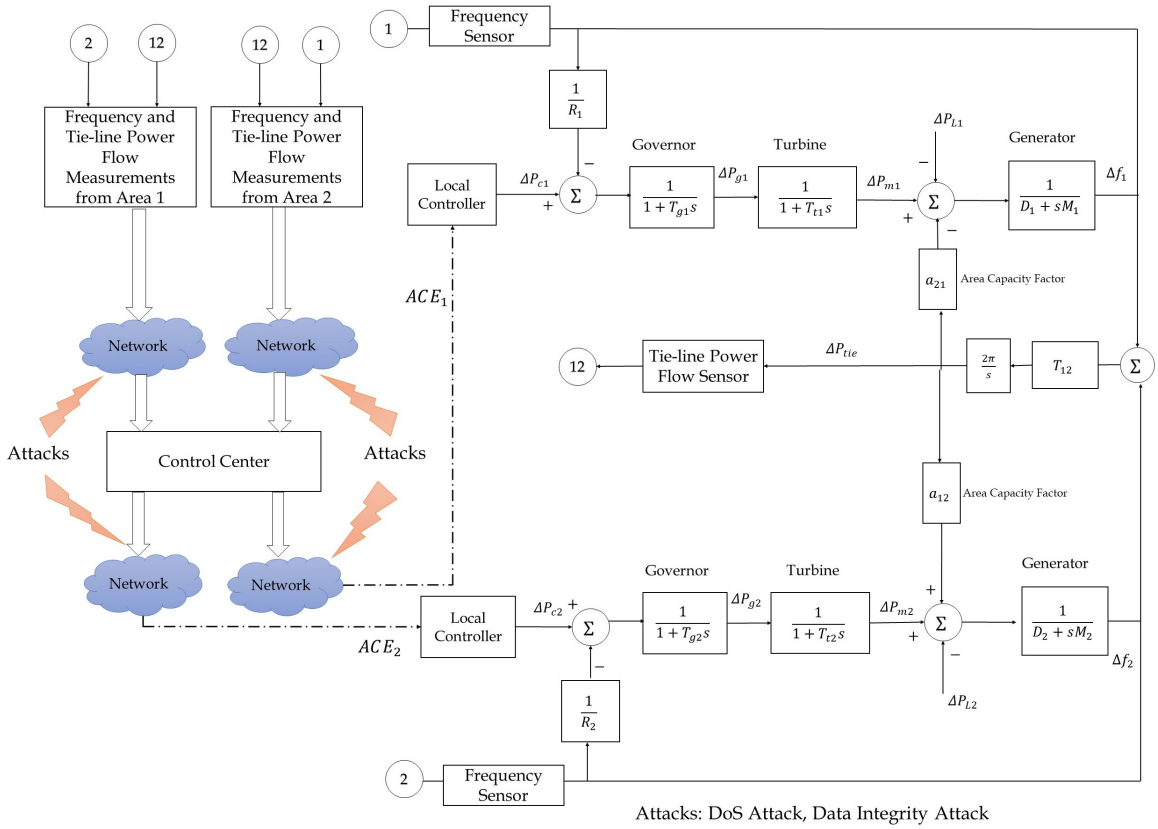

Figure 4. Schematic of two-area LFC system with attack points.

2.3. LFC Scheme with RES

RES-based power generation mechanisms create an eco-friendly and sustainable source of electrical energy [49,50]. The intermittent nature of RES and its high penetration not only affect the power quality and system reliability [51], but also make the frequency deviations faster due to decrease in system inertia [52]. The reduction in the rotational inertia of the power system is due to the inverter/converter connected resources [52–54], which results in a faster rate of change of frequency (RoCoF) and less stable frequency dynamics [53]. Moreover, in the case of interconnected LFC systems, large RES penetration causes tie-line overloading, and consequently the ACE determination and frequency stabilization deteriorate [31]. Due to faster RoCoF, the effect of cyber-attack in LFC systems will be intense for RES integrated power systems [55].

The schematic diagram of the RES integrated single-area LFC system with attack points is given in Figure 5. Here, all the generating units of the RES integrated single-area LFC system are equivalently represented by a single generating unit under the assumption that the generating units of same area swing together and produce coherent responses to the system load changes [8]. Further, the LFC system considered in Figure 5 is as an islanded microgrid (MG) where the load, wind power, and solar power variations are considered as disturbance variations and the primary and secondary controls are achieved through the speed control of governor-turbine units that produce output mechanical powers ΔP_m and ΔP_h. Therefore, in this case, the power system frequency control is established through governor-turbine units for variations in load disturbances and intermittent wind and solar powers. In addition, the influence of load changes in the generator frequency remains similar to single-area LFC system as explained in Section 2.1; however, the fluctuation in the generator frequency would be higher in this case compared to the LFC system without RES integration, due to the additional fluctuation induced by RES penetration.

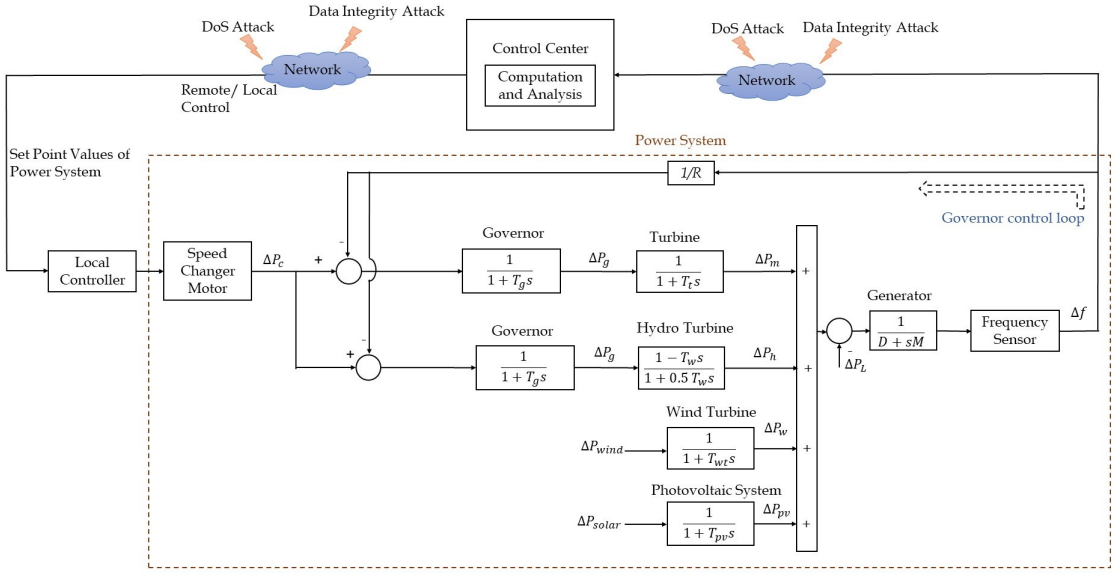

Figure 5. Schematic of RES-integrated single-area LFC system with attack points.

The general dynamic model of an isolated RES (wind turbine, PV [54], and hydropower plant) integrated LFC system [54,56–61] is described as follows.

The generator-load dynamic relation between the mismatch power deviation $(\Delta P_m(t) - \Delta P_L(t))$ and frequency deviation [54] is expressed as

$$\Delta \dot{f}(t) = \frac{1}{M}\Delta P_m(t) + \frac{1}{M}\Delta P_{pv}(t) + \frac{1}{M}\Delta P_w(t) + \frac{1}{M}\Delta P_h(t) - \frac{1}{M}\Delta P_L(t) - \frac{D}{M}\Delta f(t). \tag{11}$$

The turbine and governor dynamics can be expressed as in Equations (2) and (3), respectively. The wind turbine and PV dynamics can be described as

$$\Delta \dot{P}_w(t) = \frac{1}{T_{wt}}\Delta P_{\text{wind}}(t) - \frac{1}{T_{wt}}\Delta P_w(t), \tag{12}$$

$$\Delta \dot{P}_{pv}(t) = \frac{1}{T_{pv}}\Delta P_{\text{solar}}(t) - \frac{1}{T_{pv}}\Delta P_{pv}(t). \tag{13}$$

The hydro turbine-hydraulic governor dynamics according to the transfer function provided in [62] can be given as

$$\Delta \dot{P}_h(t) = \frac{1}{0.5T_w}\Delta P_g(t) - \frac{1}{0.5T_w}\Delta P_h(t) - \frac{1}{0.5}\Delta \dot{P}_g(t), \tag{14}$$

where the governor-dynamics $\Delta \dot{P}_g(t)$ is derived similar to Equation (3). However, in the case of multi-area LFC systems, the RES power dynamics fluctuation and tie-line power deviation can contribute to power imbalance and frequency deviation [31]. Therefore, for interconnected LFC systems, the control error calculation is performed in addition to the general dynamics mentioned above. In the control center, the ACE signal is generated for respective control areas by considering the RES power fluctuation and it can be provided as [31]

$$ACE_i(t) = \beta_i \Delta f_i(t) + \Delta P^i_{\text{tie}}(t) + \Delta P_{RES}(t), \tag{15}$$

where $\Delta P_{RES}(t)$ is the total power fluctuation due to the renewable sources of the LFC system. The integration of renewable power plants adds an additional fluctuation source [31].

Therefore, the intensity of frequency stability deterioration can be more in the case of RES integrated LFC systems compared to the conventional LFC systems when any sort of attack is introduced in its cyber or physical layer. As in the case of conventional LFC systems, the attack over communication channels can cause inaccessibility or manipulation of signals like frequency, tie-line power, the actual generator output, and ACE values of each area.

3. Types of Attacks in LFC System

The main types of attacks on the LFC system are DoS attacks (affecting the data availability) and Data integrity attacks (affecting the system integrity through the manipulation of transmission data). In this review, we try to model the cyber-attacks of LFC system based on the three dimensional attack space proposed in [20]. The axis dimensions of the attack space include "Model knowledge", "Disruption resources", and "Disclosure resources".

The prior knowledge about the system model aids the attacker in the construction of complex and "hard to detect" attacks that can cause severe consequences. In the attack space, the resources that enable the attacker to gather sensitive information (data sequence of calculated control signals from the control center and measurement signals of sensors from RTU/PMU in the case of LFC system) are called disclosure resources and it results in disclosure attacks. The physical dynamics of the control system are not affected by these attacks. Instead, it can gather information for more complex attacks like replay attacks. Further, the resources which disrupt the system operation through violation of data integrity and availability properties are called disruption resources [20]. In the LFC system, communication channels are the main disclosure and disruption resources. The cyber-attacks on the LFC system can happen through threats at the cyber layer and physical layer. The generic sensor and actuator attack models of the LFC system are discussed in the coming subsection.

3.1. Sensor and Actuator Attack Model of LFC System

In order to comprehensively describe the attack in an LFC system, two elements are needed: a mathematical model of the LFC system and the description of the attack policy [16,63,64]. The adversary model or attack model is formulated using the attack policy, which describes the prior knowledge of the system model acquired by the adversary and information set accessed through the disclosure of resources. The prior knowledge resource can include information regarding the plant model, the algorithm used in the controller, and anomaly detectors [64].

A general continuous time-domain model for LFC system under sensor attack can be described as follows,

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + w(t) \\ \tilde{y}(t) &= Cx(t) + v(t) + a_y(t), \end{aligned} \tag{16}$$

where $x(t) \in \mathbb{R}^n, u(t) \in \mathbb{R}^q$, and $\tilde{y}(t) \in \mathbb{R}^m$ are the state variable, control input, and output signal, respectively. Further, $w(t) \in \mathbb{R}^n$ and $v(t) \in \mathbb{R}^m$ represent the process and measurement noise vectors. Let the adversarial input applied at the sensor channels under attack be denoted as $a_y(t) \in \mathbb{R}^m$ and the adversarial input vector can be modeled as

$$a_y(t) = \Gamma^y y_a(t) = \begin{bmatrix} \gamma_1 & & 0 \\ & \ddots & \\ 0 & & \gamma_m \end{bmatrix} \begin{bmatrix} y_{a_1}(t) \\ \vdots \\ y_{a_m}(t) \end{bmatrix}, \tag{17}$$

where Γ^y represents the binary incidence matrix mapping the data corruption to respective signal transmission channels and $y_a(t)$ denotes the data corruption applied to each sensor channel. The measurement data of the LFC system include grid frequency, tie-line power, and the actual output power of the generator.

A general continuous time-domain model for LFC system under actuator attack can be described as follows,

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B\left(u(t) + a_u(t)\right) + w(t) \\ y(t) &= Cx(t) + v(t). \end{aligned} \tag{18}$$

The attack input vector corrupting the actuator channel can be modeled as

$$a_u(t) = \Gamma^u u_a(t) = \begin{bmatrix} \gamma_1 & & 0 \\ & \ddots & \\ 0 & & \gamma_n \end{bmatrix} \begin{bmatrix} u_{a_1}(t) \\ \vdots \\ u_{a_n}(t) \end{bmatrix}, \tag{19}$$

where Γ^u represents the binary incidence matrix, which maps the data corruption applied to the respective actuator channels, and $u_a(t)$ represents the data corruption. The actuator channels of the LFC system carries ACE values issued by the control center. The main attacks affecting LFC systems along with the attack procedure are provided in Figure 6. Various types of attacks, attack scenarios and modeling of attack types (based on sensor and actuator attack categories) of LFC system are discussed below.

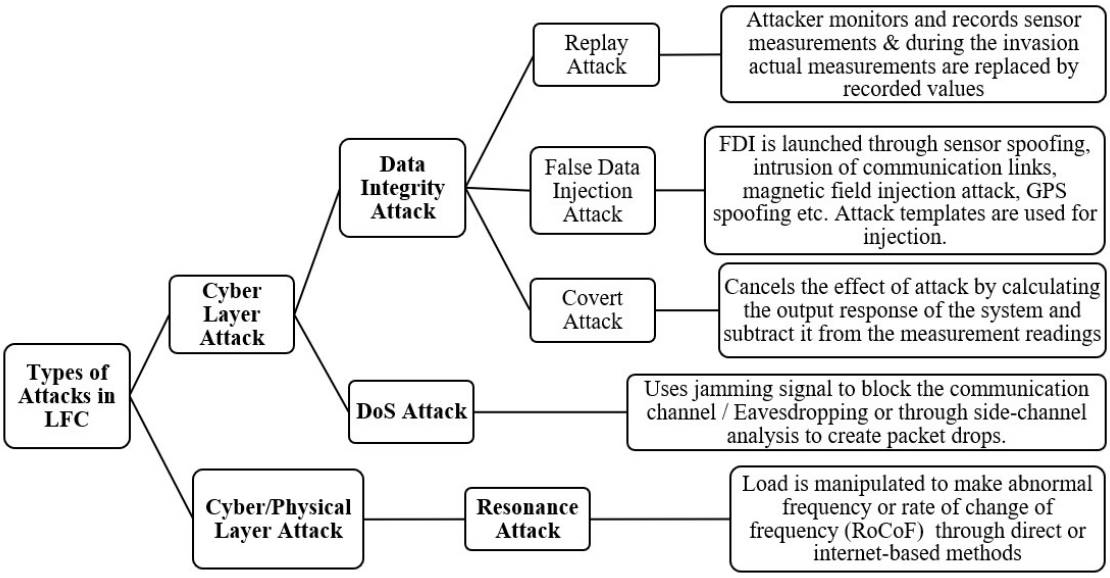

Figure 6. Various attacks of LFC system.

3.2. DoS Attack

DoS is one of the most malicious attacks, which can jam the communication channel by sending huge quantities of inauthentic packets. This is a cyber layer attack that causes heavy transmission burden and consumes excessive amounts of network bandwidth causing interruptions in the network [14,65]. In networked control systems, DoS attacks are injected by tampering transmission channels, thus preventing the control and measurement data from reaching their destination [66]. DoS attacks do not require disclosure capabilities. Moreover, there are attack scenarios (using Bernoulli attack policy) in which the prior system knowledge is not used for the attack [20]. DoS attack policy is generally opted by the attackers with limited information about the control system [67] and usually DoS attacks are easily detectable; however, poor network conditions can affect the easiness of detection [20].

For the LFC system, the communication channels ((1) connecting RTU/PMU and the control center and (2) connecting control center and governor) are the main disruption resources of the DoS attack. DoS attacks can block the measurement data to be transferred to the control center and affect the updating of the control command from the control center/delay the control signals sent to the

actuator deteriorating the power system performance [24]. DoS attacks are also powerful enough to adversely affect the dynamic performance of the LFC system, if the attack happens early before the system convergence [24,68]. Among the various types of DoS attacks (periodic, trivial, random, and protocol aware jamming attack), energy-constrained PWM jamming signal is mainly investigated in LFC systems due to the simplicity of implementation and detection avoidance [69].

Generally, these attacks utilize network defects to consume system resources for disabling the normal operation [70]. Servers with low processing speed and inadequate memory are the main target points of independent DoS attacks. However, for the communication networks with high performance and parallel processing capability, coordinated DoS attack using distributed puppet clients are carried out by attackers. These attacks with higher communication network blocking capability are known as distributed denial of service (DDoS) attack. LFC systems are wide area network control systems with process layer (comprising the data acquisition units that collect measurement data), bay layer (includes communication channels of data transmission), and station layer (comprising control center for computational analysis). Due to this distributed network and a large number of control computations, LFC systems are also prone to DDoS attacks and the communication delay caused by DDoS can adversely affect frequency stability [70]. DDoS attacks, generally executed at application or DNS servers, do not require much model knowledge and it is easy to realize; however, the detection is difficult because the attacker itself is hidden using puppets [70,71]. In other words, the request packets sent by an adversary imitate or appear similar to legal requests with the motive of using system resources [71]. The study of DDoS attack and coordinated defense requires knowledge regarding the interactive characteristics of control devices, communication network, and the physical environment [70].

3.2.1. Attacking Strategies of DoS and DDoS Attacks in LFC System

The DoS attackers use different attacking strategies like "flooding of network" [70] and "implementation of PMU measurement data packet loss" [72] to perform a DoS attack in the LFC system. DoS attackers exploit the side-channel vulnerability of virtual private network (VPN) tunnels of PMU traffic and selectively drop the measurement packets from target PMU through side-channel analysis. The attacker first identifies the IP pair of interested security gateways and uses timing side-channels for the identification and blocking of packets from targeted PMU. The phasor data concentrator (PDC) collects measurements (grid frequency, tie-line power flow, etc.) from PMU and sends the aligned data to the system control center. The measurement packets that are received outside a certain time window are considered as missing data positions and they are filled using fillers (usually zeros) to keep a constant format for the data packets. The zero value is harmful for the operation of AGC, and the absence of data packets can result in increased delivery of energy on tie-line or forced oscillation of power generation and eventually leads to instability [72].

In the case of DDoS attacks, the adversaries affect the availability of services of host servers, like application server, DNS server, etc., with the help of compromised systems in the network [73]. For instance, in the case of synchronize sequence number (SYN) flood attack, the loopholes in the transmission control protocol (TCP) is utilized to systematize the DDoS attack. The delays induced due to the DDoS attack launched in the information layer can affect the control action of the LFC system [70]. The DDoS adversaries can cause the unavailability of either measurement data or control data. The attacker initially attacks the master controllers and utilizes a large number of clients of the network as agents for blocking servers. During the SYN flood attack, flooding of the server is done by taking advantage of defects of the three-way handshakes of the TCP protocol. DDoS is implemented through manipulating the agents to send SYN packets (the packets used to initialize connection in TCP-based communication) to servers. However, the invaded agents will not respond to the acknowledgment packets sent by servers and create numerous waiting TCP connections in the attacked servers. As a result, the network will be congested with useless packets and as a direct

consequence network congestion happens. Consequently, data transmission delays occur in control and measurement channels of the LFC system and affect the stability of power systems [70].

3.2.2. DoS Attack Model

Among the two main DoS attack models (Queueing Model and Stochastic Model [21]) of CPS, the LFC system generally uses the queuing model for the analysis and study of the DoS attack. The queuing model considers a sequence of DoS off/on transitions and the time interval of the DoS attack during which no communication is available [21]. The sleep and attack intervals distribution diagram of the queuing model DoS attack is given in Figure 7 and during the attack interval no data transmission takes place through the attacked sensor or actuator channels. In the absence of attack (represented by DoS off-periods), the LFC control center receives the sensor measurements of respective control cycles and corresponding control signals are generated. In the presence of DoS attack (represented by DoS on-periods) in the sensor channel of LFC system, the controller generates control signal based on the most recently available sensor measurements for maintaining frequency stability. In other words, the control signal generated during the previous control cycle will be used [20,24].

Queuing Model [21]: Let $\{h_n\}_{n\in\mathbb{N}_0}$ with $h_0 \geq 0$ be considered as the DoS off/on transition sequence. The time instants at which the DoS pulses undergo a shift from zero to one are the instants at which the communication of the measurement/control channel start getting interrupted. Then, the attack time interval of the n^{th} DoS attack with an interval length of $\tau_n \in \mathbb{R}_{\geq 0}$ can be given as follows,

$$H_n := \{h_n\} \cup [h_n, h_n + \tau_n[\ , \tag{20}$$

and no communication takes place during this time interval due to the presence of DoS attack.

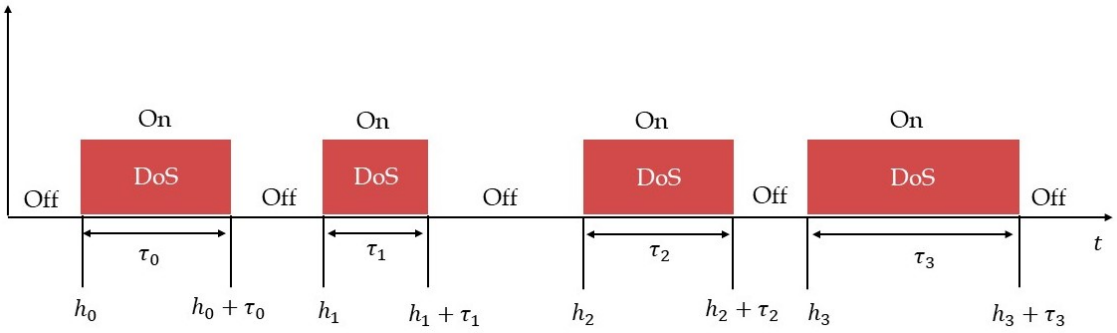

Figure 7. Sleep and attack intervals distribution diagram of DoS attack.

Let $\Xi(\tau, t)$ (DoS on-period set) and $\Theta(\tau, t)$ (DoS off-period set) represent the sets of time instants in the interval $[\tau, t]$ during which the communication is banned and permitted [21], where $\tau, t \in \mathbb{R}_{\geq 0}$, and $t \geq \tau$,

$$\Xi(\tau, t) := \bigcup_{n\in\mathbb{N}_0} H_n \bigcap [\tau, t] \tag{21}$$

$$\Theta(\tau, t) := [\tau, t] \backslash \Xi(\tau, t). \tag{22}$$

Here, $\Xi(\tau, t)$ represents the union of all attack time intervals for a time period (τ, t) and $\Theta(\tau, t)$ represents the set of all sleep intervals for the time period (τ, t). Then, the DoS attack model should be formulated in such a way that, the absence of DoS attack allows the transmission of data to the authorized system units and the presence of DoS attack is represented by the absence of data. Accordingly, DoS attack at the sensor and actuator channels [64] can be modeled as

$$a_y(t) = -S^y \Gamma^y y(t) \tag{23}$$

$$a_u(t) = -S^u \Gamma^u u(t), \tag{24}$$

where S^y and S^u represents the boolean diagonal matrices with the diagonal entry representing the presence ($[S^{(.)}]_{ii} = 1$, during $\Xi(\tau, t)$) and absence ($[S^{(.)}]_{ii} = 0$, during $\Theta(\tau, t)$) of attack. Therefore, when $[S^{(.)}]_{ii} = 1$, the attacked actuator and sensor channels will be unavailable during the attack time interval and no data transfer occurs. When $[S^{(.)}]_{ii} = 0$, the adversary unblocks the attacked channel or the data transfer is permitted.

3.3. Data Integrity Attack/Deception Attack

Data Integrity attacks are implemented through the manipulation of measurement and control signals transmitted among the cyber parts of the power system [21]. The attackers implement data manipulation or malicious data injection in actuator and sensor channels, in such a way that, the transmitted data lies within its own allowable limits. If this condition is violated, the bad data detection schemes easily detect these attacks and it results in an attack without intelligence. In short, for the attack to be successful, it should obey the power system principles [39]. Various types of data integrity/deception attacks on LFC system are discussed below.

3.3.1. False Data Injection (FDI) Attack

It is a general class of integrity attack that is capable of corrupting the real-time data, like frequency and ACE, in LFC systems [74]. FDI attacks generally follow predefined attack templates for signal injection [39]. However, real-world resourceful attackers use strategies that adapt during the attack. The preliminary phase may be designed to uncover system configuration using disclosure resources and obtain real-time data. Then, the subsequent phase will cause the disruption of resources affecting the normal system operation [34]. FDI attacks are applied to the measurement and control channels of the LFC system in the form of input attack vectors ($a_{y_i}(t)$ or $a_{u_i}(t)$) formulated using data corruption strategies or attack templates.

The data corruption $y_{a_i}(t)$ or $u_{a_j}(t)$ applied for executing FDI attack at sensor and actuator channels can be modeled as

$$y_{a_i}(t) \quad or \quad u_{a_j}(t) = \begin{cases} 0 & \text{for } t \notin \tau_a \\ \lambda \cdot \mathcal{F}(.) & \text{for } t \in \tau_a \end{cases} \tag{25}$$

where $i = 1, 2, ..., m$ and $j = 1, 2, ..., n$, λ is the attack parameter, τ_a is the attack time period, and $\mathcal{F}(.)$ is a function that can be independent or dependent on time, actuator signals, and sensor signals. Various kinds of FDI attack templates are provided as follows [20,39,64,74].

- Ramp attack: Ramp attack involves the modification of output measurements $y(t)$ or control signals $u(t)$ using a gradually increasing or decreasing ramp function for an attack period τ_a. During the attack period, $y_{a_i}(t)$ or $u_{a_j}(t)$ will be equal to $\lambda_r \cdot t$, where $\lambda = \lambda_r$ is the ramp parameter and $\mathcal{F}(.) = t$.
- Pulse attack: Pulse attack involves the modification of output measurements or control signals using temporally spaced short pulses with some attack parameter λ_p. Further, $\mathcal{F}(.)$ can describe the pulse shape characteristics.
- Random attack: Random attack involves the modification of output measurements or control signals, over the attack time period, through the addition of values returned from a uniform random function $rand(a, b)$. In this case, $\lambda = 1$ and $\mathcal{F}(.) = rand(a, b)$, where (a, b) represents the lower and upper bounds of $y(t)$ or $u(t)$ [75].
- Scaling attack: Scaling attack involves the modification of output measurements or control signals to higher or lower values based on the scaling parameter λ_s. In this case, the attack at the sensor and actuator channels can be represented as $y_{a_i}(t) = \lambda\mathcal{F}(.) = \lambda_s y_i(t)$ and $u_{a_j}(t) = \lambda\mathcal{F}(.) = \lambda_s u_j(t)$, respectively. When the parameter λ_s is adjusted in such a way that

$\lambda_s y_i(t) = y_{min}$ or $\lambda_s u_j(t) = u_{min}$, then such kind of attack is called min attack, where y_{min} and u_{min} represents the minimum values of the output and control signals, respectively. When the parameter λ_s is adjusted in such a way that $\lambda_s y_i(t) = y_{max}$ or $\lambda_s u_j(t) = u_{max}$, then it is called max attack, where y_{max} and u_{max} represent the maximum values of the output and control signals, respectively.

- Bias injection attack [20,64]: Bias injection attack is the simplest attack, in which the sensor or control signals of the intended channel are injected with a constant bias signal and the attack vectors can be modeled as $a_{y_i}(t) = b_i$ and $a_{u_j}(t) = b_j$ for sensor and actuator channels, respectively.

AGC is an appealing target of FDI adversaries as it controls grid frequency, the critical global parameter of the power system. The FDI attacks are launched in the LFC system through the following ways [25–28].

- Attacking physical sensors by sensor spoofing
- Utilizing communication channels of sensor and actuator data
- Compromising the computational algorithms of the control center
- Compromising the logically isolated VPN channels from the distributed sensors
- Global positioning system (GPS) spoofing: GPS spoofing allows penetration to PMU and affects clock synchronization of substations leading to wrong phase angle measurements

However, the measurement communication channel is the primarily focused disruption resource of FDI attackers, due to the strong protection of computer programs at the control center and due to the less coordination of distributed physical sensors [25,33]. FDI attacks need a good knowledge of system configuration and attack impact models for computation of optimal attack sequence [25,28]. When the attacker has full knowledge of system configuration, but limited access to measurement meters due to their physical protection, the attackers solve the optimization problem for the identification of the minimum number of meters/sensors with maximum vulnerability. However, during an incomplete information scenario, FDI attackers gather topology information for launching valid FDI attack through the following means [76].

- Through the collection of offline and online data using manual techniques or by deploying meters for accessing the grid
- Using the market data related to the economic dispatch problem
- Utilizing power flow measurements: The correlation among the power flow measurements provides topology information, when the system parameters like active and passive loads are varied.

In AGC, the influence of FDI attack over tie-line power and frequency measurements can be illustrated as follows [33],

$$ACE_{i,FDI-Tie}(t) = \sum_{j=1}^{N} a_{ij}\Delta P_{\text{tie}}^{ij}(t) + \beta_i \Delta f_i(t) + A_{tie}(t) = ACE_i(t) + A_{tie}(t) \quad (26)$$

$$ACE_{i,FDI-Freq}(t) = \sum_{j=1}^{N} a_{ij}\Delta P_{\text{tie}}^{ij}(t) + \beta_i (\Delta f_i(t) + A_{freq}(t)) + = ACE_i(t) + \beta_i A_{freq}(t), \quad (27)$$

where $\Delta P_{\text{tie}}^{ij}(t)$ represents the difference between the actual and scheduled tie-line power balancing the areas i and j, a_{ij} is the area capacity factor, $ACE_{i,FDI-Tie}(t)$ and $ACE_{i,FDI-Freq}(t)$ are the false generation correction values due to tie-line power FDI attack and frequency FDI attack, and $A_{tie}(t)$ and $A_{freq}(t)$ are the FDI signals injected to the tie-line power and frequency measurements. When $A_{tie}(t) > 0$ and $A_{freq}(t) > 0$, then $ACE_i(t) < 0$, due to the secondary control action that forces $ACE_{i,FDI-Tie}(t)$ and $ACE_{i,FDI-Freq}(t)$ to be less than zero. This leads to a condition of $\Delta f_i(t) < 0$

and $\Delta P_{\text{tie}}^{ij}(t)) < 0$ as the generator shortfall in that control area. The reverse situation happens when $A_{tie}(t) < 0$ and $A_{freq}(t) < 0$ and can result in load shedding or generator tripping [33].

The FDI attack at the system frequency can be also implemented by injecting a bias signal at the frequency measurements of LFC to drive the steady state frequency deviation to a non-zero value without being detected by employed detection mechanisms [77]. In the absence of bias injection signals, the system frequency asymptotically converges to a nominal value. The computation of the amount of bias injection is performed with an aim of maximizing the impact at the steady state. Its attack policy follows an open-loop approach and does not require disclosure capabilities. However, the adversary needs knowledge about the closed-loop system. The disruption resources include the communication channels of actuator and sensor data [20].

The LFC system model generally considered for the analysis of bias injection attack in [36,77,78] does not account for the speed governor dynamics for brevity. Further, another assumption followed is that the mechanical power supplied to the rotor shaft is equal to the electric power generation [77]. The bias injection attack on frequency measurements of a single-area LFC system is given in Figure 8.

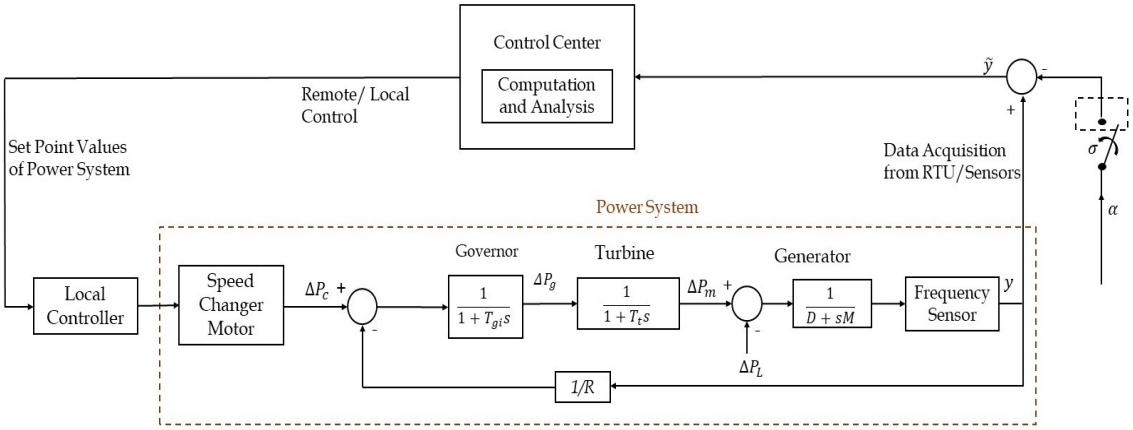

Figure 8. Schematic of single-area LFC system under bias injection attack on frequency measurement.

Here, the scalar $\alpha \in \mathbb{R}$ denotes the bias or false data injected into the measurement channel and $\sigma : \mathbb{R}_+ \to \{0, 1\}$ determines whether the system is under attack or not [77]. The bias injection attack input applied at the frequency measurement signal of the LFC system is given as

$$a_y(t) = -\alpha\sigma(t). \tag{28}$$

In the absence of attack, the system frequency converges asymptotically to the nominal value. The discrete time state space model of the LFC system with an integral controller under bias injection attack is given in [77].

In addition to the above scenario, the FDI attack is also modeled as a nonlinear function with an upper-bound on the non-linearity and it can be used to corrupt the entire transmission data of measurement channel [69].

3.3.2. Replay Attack

Replay attack is another kind of data integrity attack, implemented by first performing a disclosure attack to gather data sequences from the compromised resources and then replaying the recorded data until the end of the attack [63,64]. Replay attacks basically follow the strategy of fraudulently repeating or delaying the valid data transmitted [65]. Attacks of this kind do not require any prior knowledge about the system model, including the information of designed controllers and estimators [21,64]. However, in the attack scenario of predefined physical attack along with the replay attack, scenario dependent knowledge is required for the implementation of physical attack [20]. Replay attacks

require disclosure potentials to acquire data from the communication channels of the control system. In addition, it is capable of disrupting the data channels that are disclosed [20]. These attacks can be modeled as time-varying delays, with unknown information about their upper bound and rate of change [65].

In the case of Byzantine replay attacks, attackers iterate the recorded data from the attacked sensors or actuators for a definite time [65]. The attacks on sensors can be conducted by either cracking the cryptography algorithm or by inducing false sensor readings through manipulating local conditions around it [79,80].

The replay attack at the sensor channel can be modeled as [81,82]

$$a_y(t) = -Cx(t) + y(t-\tau), \tag{29}$$

where $0 < \tau < t$. $y(t-\tau)$ is the sensor data gathered through monitoring. The two stages of replay attack (monitoring and replay phase) are modeled as follows.

- Monitoring Phase $(0 \leq t < t_0)$: During the monitoring phase, the gathered sensor measurements are stored in $J(t)$,

$$\begin{aligned} y_a(t) &= 0 \\ J(t) &= \Gamma^y \cdot y(t). \end{aligned} \tag{30}$$

- Replay Phase $(t_0 \leq t < 2t_0)$: During replay phase, the collected sensor data is sent to the controller until the end of the attack,

$$\begin{aligned} y_a(t) &= J\left(t - t_0\right) \\ J(t) &= J(t-1). \end{aligned} \tag{31}$$

The replay attack at the actuator channel can be modeled in the same manner as in the sensor channel.

In the case of replay attacks over AGC, the adversary monitors and records the sensor measurements (frequency and power measurements) during the normal operation of the power system for some duration. The actual measurements of the compromised sensors/adversarial sensors are replaced by the recorded measurements during the attack and transferred to the control center [48]. The disclosure resources of the replay attack include the communication channels eavesdropped by the attacker (sensor-controller loop in LFC) [48]. The disruption resources generally include the communication channel the attacker can tamper. In the case of a replay attack, it can tamper only the channel from which the data is recorded [64]. One of the peculiarities of the replay attack is that if the invasion happens near the steady state operation of the system, recorded data will be also close to steady state response value. Thus, the anomaly detected at this stage can be easily accounted as a false positive or error during the steady state. This makes the replay attack difficult to be detected during the steady state [79,83].

3.3.3. Covert Attack

Covert attacks create a stealthy and powerful attack strategy from the complete knowledge of the system and using its accessibility to control and measurement signals transmitted over the communication channels [80,84,85]. The covert agent is assumed to have resources to access and inject data to both measurement and actuation channels.

Covert attacks work by the cancellation of the effect of attack signals by calculating the output response of the system and subtracting it from the measurement readings [63,86]. Consequently, the diagnosis system at the controller side receives the measurement data with no information about the attack. This makes the attack stealthy. In addition, it also exploits the threshold maintained in the decision logic of detection systems to reduce false alarms due to the existence of model uncertainties and unknown disturbances. Therefore, the attack would remain covert in spite of the model discrepancies occurring between the plant model of the attacker and the real process [84].

The covertness of attack has been defined in two different domains (physical domain and cyber domain) [87]. Cybernetically covert attacks have a low probability of detection by the diagnostic algorithms that monitor the system dynamics and communication. While the covert attacks in the physical domain (physically covert attacks) can modify the behavior of the system to induce physical effects without being identified by the human observer [87]. The covert attack requires disclosure capabilities, disruption capabilities, and complete knowledge of plant dynamics or system model [20, 88]. The covert attacks on LFC system are not investigated in this literature.

3.4. Zero Dynamics Attack

Zero dynamics attacks also exploit the information of the complete system model to produce attack signals that do not create any change in the output measurement [20]. These attacks utilize the properties of linearity and zeros in transfer function to create an attack strategy that decouples itself from the closed-loop system output [84]. It does not require any disclosure capabilities as it follows an open-loop attack policy. Disruption capabilities on the actuator communication channels are needed for zero-dynamics attacks, and the perfect knowledge about zero-dynamics of the system is required and it can be computed from state and output equation matrices [20]. The LFC systems are generally not prone to zero-dynamics attacks due to the absence of zero and it is a minimum phase system.

3.5. Resonance Attack

Safe and secured operation of the power system is also ensured by admissible intervals of the frequency and RoCoF in power systems. Resonance attack is a type of attack which can lead to an abnormal frequency or RoCoF in the power system by altering the power load or tie-line signals according to a resonance source. Usually, the resonance source is either the output of the system or the function of output. The modified loads or power signals are kept within an admissible interval such that it is too small to be recognized by the detection methods [11]. As the divergence of RoCoF results in the divergence of frequency, the power systems are provided with typical RoCoF protection delays based on the power system inertia. These protection relays may trip as a consequence of adversarial attacks that are capable of moving the RoCoF value beyond its predefined boundary. Consequently, it results in the blackout of power systems.

In the LFC system, the resonance attack can be implemented by deceitfully manipulating power system load demands [11]. Usually, the generation in power plants happens according to the customer's load demand in real-time. The control center sends instructions to the power plant for generating the demanded power, after receiving the power load request of customers via communication networks. By adversely manipulating the aggregated or individual customer load, through the communication channels of demand aggregation system (DAS) in the control center, the power system can be driven to undesirable states. DAS is the system, used in the control center to aggregate customer's inputs or load demands [11]. The abrupt load changes of the accessible grid are performed through various internet-based load manipulation attacks that can cause circuit overflow and disturbance in the balance between the power supply and power demand [89]. The direct and indirect load modification attack strategies are implemented using Electronic Load Controller (ELC) and by compromising grid-wise friendly devices using malicious codes. Once the friendly devices are manipulated using codes, then the load devices can be directly switched on or off [11].

The alternate resonant sources of the LFC system include [11] the following.

- Internal state of the plant: If the attacker is aware of the internal states of the plant (like governor output, turbine output, etc.), then a powerful attack can be launched through load modification according to the estimated state.
- Frequency Derivation: Frequency derivation is another resonance reference that allows the attacker to produce fake input for resonance attack. For instance, the attack input $a_y(t)$ can be taken as $a_y(t) = -0.3 * sign(\hat{f}(t))$ as in [11], where $\hat{f}(t)$ is the frequency derivation.

In single-area LFC system, the load is manipulated in accordance with the resonance source. In multi-area interconnected LFC systems, in addition to local load changes of individual areas, interconnected frequency signals can also be manipulated to implement the attack. The intensity of attack is higher in the case of multi-area systems as the attack in one area causes instability in the non-attacked area too. Resonance attacks become more powerful with the increase in areas [11]. In another version of resonance attack, called resonance switching attack, the adversary switches a small part of the load located near the inter-area link and over-imposes a low switching frequency with one of the inter-area oscillation modes of the system. The identification of inter-area oscillation mode frequency is usually carried out through offline analysis of line measurements [90].

3.6. Time-Delay Switch (TDS) Attack

The adversaries induce TDS attacks in control systems by strategically embedding time delays into the sensor and control loops in order to degrade the stability of the system [91]. LFC systems would either break down or will be driven to an unstable state if significant time delays are injected into the telemetered measurement states or control signals. An LFC system with a TDS attack is modeled as a hybrid system with switch action, "Off/Delay-by-τ", where τ is the random delay time introduced in the measurement state or control signals. The introduction of time delays in the dynamic states of the system can switch the system into an unstable state [91].

To summarize, the identification of attack space of LFC system and the practical implementation strategies of different attacks are provided in Table 2.

Table 2. Identification of attack space and attack implementation strategies of LFC system.

Attack	Disclosure Resources	Disruption Resources	Model Knowledge	Practical Implementation Strategies
DoS Attack	Not needed	Sensor channel Actuator channel	Not needed	PMU packet losses
DDoS Attack	Not needed	Application and DNS sever	Not needed	SYN flood attack method
Bias Injection Attack (FDI variant)	Not needed	Frequency channel	Knowledge of closed-loop system, anomaly detector gains	Sensor or GPS spoofing
Replay Attack	Frequency and tie-line power flow channels	Frequency and tie-line power flow channels	Not needed	Cracking cryptographic algorithms, transmission data manipulations
Resonance Attack	Not needed	DAS channel, tie-line power flows	Complete system knowledge	Load manipulation through ELC or manual switching
Covert Attack	Sensor and actuator channels	Sensor and actuator channels	Complete system knowledge	Sensor and actuator data modification
TDS Attack	Not needed	Sensor and actuator channels	Complete system knowledge	Delaying data packets
Zero-dynamics Attack	Not needed	Actuator communication channels	Perfect knowledge of the zero-dynamics of the system	-

4. Attack Detection and Defense Mechanisms

In this section, previous works on the defense and detection mechanisms of power systems and LFC systems are discussed in general.

4.1. DoS Attack

As mentioned in Section 3.2, DoS adversaries can launch attacks in the transmission channels of CPS through network protocol attacks, network traffic flooding, and communication channel jamming [68]. The general defense and detection approaches followed against DoS attacks in state estimation problem include modified Kalman filtering approach, hypothesis testing problem detection approach [92,93], and game theory approach [94]. The secure control approaches of DoS attacks in CPS include stochastic time-delay system approach, impulsive system approach, small gain system approach, triggering system approach, and game theory approach [21].

In the case of the LFC systems, the launch of DoS attack can deteriorate the system performance and destabilize system severely if the attack is launched before the convergence of the system dynamics [68]. A single-area LFC system with time delay in the communication channel is considered for the study of DoS attack in [14], and for the proper utilization of limited communication bandwidth, an event-triggered control strategy is used. The LFC system under DoS attack is formulated as a time-varying delay switched system and utilizes an average dwell time approach to establish exponential stability criteria [14]. It is proven that if there exists an appropriate ratio of time intervals in the presence and absence of DoS attacks, the convergence of power systems can still be guaranteed. A similar kind of approach is applied for the multi-area LFC system in [95], where exponential stability and $L_2 - gain$ are obtained. The ground of the analysis techniques is to understand the maximum degree of tolerance of the LFC system against the DoS attack and to find the total length of time of DoS attacks for which the stability of the LFC system is maintained [14].

A resilient control strategy against aperiodic DoS attack in interconnected-area power systems with communication delay is proposed in [40]. It is also synchronized with a detection mechanism for differentiating DoS attacks from delays induced in the network. The criteria for the tolerable DoS attacks are derived by employing the Lyapunov–Krasovkii method and switched system method [40]. A resilient event-triggered communication scheme of interconnected power systems that tolerates data losses due to an energy-bound DoS attack is introduced in [96]. The work concentrates on the development of resilient control without the prior knowledge of additional probability distributions of DoS attacks. A new switched system model of the multi-area power system under the simultaneous presence of DoS and stochastic deception attack is developed in [69]. By the virtue of Lyapunov stability theory, exponentially mean-square stability of the system is obtained. In this work, a periodic power-constraint jamming signal is used to model the DoS attack and the signal of deception attack is modeled as a nonlinear function related to measurable outputs.

Apart from the resilient control concepts, there are works concentrated on developing the defense mechanisms against DoS attacks using cellular computational network (CCN) prediction and learning-based techniques. The mitigation of DoS attack in a PV source integrated two-area power system through the implementation of a virtual synchrophasor network (VSN) is presented in [72]. It uses a CCN for the prediction of dropped data from the PMU. The predicted data from CCN are used to implement a VSN. In [24], a defense method using ''Deep auto-encoder Extreme Learning Machine" (DAELM) is proposed. The algorithm supplies lost data through prediction and maintains normal system operations. The prediction of dropped frequency due to attack is implemented with the help of a historical database and data prediction algorithm. Then, the control center sends the actuator command corresponding to the forecast frequency to retain the normal operation of the system [24].

As mentioned earlier, DoS attacks usually penetrate to the servers with less memory and low processing speed and the individual DoS attacks are often inefficient to attack systems with improved processing capability [70]. In such situations, the adversaries carry out DDoS attacks through distributed puppet clients. Moreover, this attack is easily realizable and difficult to locate, as the attackers hide themselves through puppets. The impact of communication delay due to DDoS on the multi-area power system is discussed in [70]. For DDoS attacks, defense mechanisms have to be employed in both information and power layers. The access control line (ACL)-based fireworks are installed in routers to detect DDoS attacks in the information layer. In addition, the hysteresis and large

delays induced in the power layer are eliminated by using compensation controllers [70]. Some of the defense mechanisms of DoS and DDoS attacks are summarized in Table 3.

Table 3. Some defense mechanisms for DoS and DDoS attacks in LFC system.

Defense Mechanism	Advantages	Disadvantages	LFC System for Analysis	Attack Point
DAELM algorithm-based data prediction [24]	Fast and accurate prediction, less prediction time and computational complexity, enhance real-time performance,	No RES integration	Single-area, two-area, three-area	Sensor channels
CNN prediction with VSN [72]	PV integrated, real-time VSN countermeasures	Real-time PMU data delivery is expensive	Single-area, two-area	Sensor channels
Resilient control strategy [14,30,40]	Event-triggered strategy [14], guaranteed exponential $H\infty$ stability [30]	No RES integration	Single-area [14], two-area, three-area [30]	Sensor channel [14], additional control loop [30], both actuator and sensor channels [40]
Coordinated defense of DDoS attack using ACL-based fireworks and compensator controllers [70]	Improves overall control effect, complete attack defense cycle	ACL detection is weak for real-time performance, compensated control can be negative during little delay situations	Single-area	Application and DNS servers

4.2. FDI Attack

FDI attacks are the cyber-attacks that work through the injection of malicious data and data manipulation. Therefore, for the detection of FDI attacks and to ensure the operational reliability of power systems, system monitoring through meter measurements and state estimation techniques are generally employed [97]. Detection schemes employed in LFC systems involve algorithms to check whether the obtained measurements of power system parameters lie within the acceptable ranges [64]. A good detection algorithm should be capable of providing information regarding the location, size and time of the attack in real-time [27]. The detection mechanisms in the networked control system are generally called as anomaly detectors, and they are collocated with the controllers [64].

In legacy power systems with AGC, the state estimation algorithms are executed at relatively high time intervals, therefore it cannot contribute to improving the reliability of sensor data sent to AGC [25,34]. In fact, modern power systems are equipped with high performance computing and data acquisition units that run state estimation algorithms with reduced execution time. Therefore, this can enhance the reliability of measurement data send to AGC algorithms, after passing them through state estimation algorithms [25]. However, the FDI attacks on these power systems have the capability of disturbing the state estimation process, resulting in the transmission of manipulated estimates of sensor measurements to the control center. It basically exploits the tolerance of state estimation algorithms against small measurement errors [76]. Usually, when a power system is attacked, the compromised data is compared with the measurement data of a healthy system, by the monitoring systems to detect those attacks. However, if the attacker has good knowledge about the system, small feasible attack signals would be nearly undetectable and result in a stealthy deception attack [98]. The investigation of the stealthiness properties of FDI attacks in LTI control systems is conducted in [99].

The countermeasures of FDI attacks can be classified into protection-based approaches and detection-based approaches [100]. Protection-based defense methods help in the identification and

protection of critical sensors and detection-based methods concentrate on the detection of FDI attacks using estimation techniques [101].

The vulnerability of the terminal units makes the power systems more prone to integrity attacks. Therefore, protecting the set of basic measurements is one of the defense mechanisms against FDI attacks. In [97], the author demonstrates the existence of successful FDI vectors if the number of compromised meter measurements (k) follows a condition. If $k \geq m - n + 1$, there exists a successful attack vector that can manipulate measurements without being detected where m is the number of meters of measurement and n is the number of state variables. If the number of meters that are attacked is less than $m - n + 1$, then the attack will be detected. Based on this condition, in [102] it is proven that the protection of a set of basic measurements is necessary and sufficient to detect FDI attacks. The problem of finding the location of the basic set of compromised meters using graphical meters is proposed in [103]. Apart from these, few works of literature that investigates various detection mechanisms used in FDI attacks are also discussed below.

Reachability methods are used in [104,105] to identify the existence of FDI attacks, which can cause the violation of safety conditions. In [97], the unknown vulnerability of existing bad data detection algorithms for two class of attacks (FDI attacks and generalized FDI attacks) with the attack goals of finding a random attack vector and targeted attack vector is investigated. Based on the attacking mechanisms, this type of attack is basically classified into "FDI attack" and "Generalized FDI attack" [76,97]. In FDI attacks, the attacker can inject bad data into meter measurements whilst keeping the measurement residual unchanged. In generalized FDI attacks, the attacker utilizes the typical measurement error tolerance of state estimation algorithms and it remains stealthy without being detected [76,97]. Various state estimation methods that use algorithms, like 'Weighted least squares-WLS', "Maximum likelihood criterion", "Least absolute value estimator", etc., are provided in [106]. In addition, different bad data detection schemes like "largest normalized residual", "performance index", and "Chi-square test" are also discussed.

The state estimation techniques (for example, the one which uses Bayesian network) also have disadvantages like the inefficacy in the detection of attack that injects measurement data identical to historical data. Therefore, a new detection scheme based on the tracking of measurement variation dynamics is proposed in [101]. The distance between the probability distributions of measurement variations is derived using Kullback–Leibler distance (KLD) under the AC estimation model. The larger KLD indicates the larger deviation of measurement from the historical data, indicating the presence of false data [101]. Noticing the sparse nature of FDI attacks, a detection technique based on sparse optimization is demonstrated in [107]. The methods of low rank matrix factorization and nuclear norm minimization are proposed to separate the anomalies and nominal states of the power grid [107]. A defense strategy for the attack against smart grid state estimation at the control center is provided in [108]. The method uses an "adaptive cumulative sum algorithm" (CUSUM) for the detection of the adversary as quickly as possible without violating the level of detection accuracy [108]. The defense mechanism for a power system which is typically partitioned into micro-grid groups is proposed in [109]. In this work, the boundaries and information sharing structures of microgrids are dynamically reconfigured such that it would be impossible to create a synchronized FDI attack. More details of FDI attacks detection mechanisms in power grids are provided in [110–116]. In addition to the aforementioned techniques, some of the works that concentrate on the detection in AGC systems using machine learning techniques are discussed below.

A multi-layer perceptron (MLP) classifier-based detection scheme for cyber-attacks in the LFC system is proposed in [117]. In this work, the MLP classifier will be provided with training samples of ACE values collected under normal and compromised conditions. The relevant features of ACE signals are then extracted to clearly identify the difference between normal and compromised signals. The performance of the classifier is then evaluated using an optimal subset and objective function [117]. A neural network-based detection approach for FDI attacks in the sensing loop of two-area distribution system is demonstrated in [26]. The control inputs and output measurement

states are sent to the Luenberger observer for the state estimation. The neural network detection unit receives these estimates for the detection and tracking of FDI attacks. The ability of the neural network to estimate the nonlinear behavior of the system also add advantages to this method [26]. AGC system with non-linearities like time-delay and governor dead-band is equipped with a detection scheme using a particle filter-based approach and sequential importance sampling (SIS) algorithm in [118]. Particle filters are tools used to track the dynamic states of the nonlinear system, modeled using a Bayesian network [118]. A recurring neural network (RNN)-based method is proposed for the detection of FDI attack in the AGC system with non-linearities like transportation time delay and governor dead band in [119]. Another detection technique that relies on physics-based method and deep learning is proposed in [75]. The deep learning method uses historical data of frequency and tie-line power flow measurements for the learning of data patterns and prediction of ACE values through the learned patterns [75]. As a countermeasure for an optimal coordinated attack (FDI attack and load manipulation), a threshold-based detection method is proposed in [38].

A concurrent detection and mitigation mechanism for AGC against FDI attack, through the simultaneous estimation of input and state, is proposed in [29]. It uses a recursive three-step filter for the execution of three steps, namely, time updation, measurement updation, and unknown input estimation [29].

Bias injection attack is one of the variants of FDI attack and the analysis of the impact of bias injection attack over LFC is discussed in [77]. The study is based on finding the maximal impact of the attack on the system when the attacker invades the system frequency and keep it within safe steady-state value without triggering the alarm [77]. The state estimation problem of stochastic dynamical linear systems under bias injection attacks is considered in [120]. The work proposes criteria for the selection of sensors, to be secured in order to compensate for the impact of the attack. The estimator used is the Kalman filter and the attack detection is implemented using the chi-squared test [120]. A set-theoretic method-based detection for bias injection attack is proposed in [36]. Set-induced anomaly detector is developed through the extraction of a convex and compact polyhedral invariant set from the discrete-time network dynamics. Detection happens when the state vector exists from this invariant set [36]. The set-theoretic detection approaches also help to identify attacks during the transient response of the system, even in the presence of disturbances [36]. The distributed detection and isolation of bias injection attack of the smart energy grid using an internal observer is proposed in [121]. It provides local and global steps for the distributed detection of sensor attack sets based on a judgment matrix. It also examines the practical aspects, like detection delay, the accuracy of bias injection attack detection, precomputed threshold limitation, etc., while deploying the detection scheme [121].

4.3. Replay Attack

An online detection mechanism for replay attack, noise-injection attack, and destabilization attack on AGC is proposed in [48]. The proposed algorithm basically employs the dynamic watermarking technique to detect tampered measurements. The generation unit superimposes the control command with a random signal of small magnitude which has certain probability distribution [48]. As a result, the honest sensors display statistical properties similar to the superimposed signal, while the compromised sensors with excessive distortion will not exhibit these relevant statistical properties. Therefore, malicious activities can be detected through certain tests of these statistical properties [48]. It is claimed that the algorithm can be employed even when the adversaries are completely aware of the statistical and physical system models.

A strategy for the detection of the replay attack for system controller of the smart grid is proposed in [83]. The control law is changed from static to random to improve the detection rate of replay attacks. However, this technique compromises the performance to some level [83]. The feasibility conditions of replay attack in a Gaussian LTI control system with infinite Linear Quadratic Gaussian (LQG) controller and χ^2 anomaly detector are provided in [79]. The proposed method also guarantees

the desired detection probability by trading off either LQG performance or detection delay, either by the increase of control effort or decrease of control accuracy [79]. The resilient control strategy against replay attacks in networked control systems using receding horizon control law is given in [122]. The computed control sequence is stored in the plant to use in the near future as a response to replay attacks. The list of the detection techniques of various attacks of LFC system are summarized in Table 4.

Table 4. Detection techniques of data integrity attacks in LFC system.

Detection Technique	Advantages	Disadvantages	LFC System	Attack Point
Particle filter-based detection approach using SIS algorithm [118]	Considers non-linearities like time-delay and governor deadband	Resampling technique is needed	Two-area	Frequency and tie-line measurements
Luenberger observer with artificial neural network [27]	Fast, accurate, resilient to abrupt FDI and GPS spoofing, considers non-linearities	Needs system mathematical model	Two-area	PMU measurements
Cyber-attack detection and mitigation platform [33] using forecasted data	Scans real-time ACE data	Needs frequency correction multiplier	Three-area	ACE channel
Deep learning-based approach using long short term memory [75] (LSTM) networks	Trained LSTM network detects abnormal ACE patterns, not model-based	Needs accurate training data	Two-area	ACE channel
Dynamic water marking technique using control signal [48]	Detects complex attackers having complete system knowledge, hardware update of generation units are not needed	Applied to small-scale power systems	Four-area	Sensor and actuator channels
Set-theoretic approach [36]	Reveals adversaries in the presence of external disturbances and during transient system response	Small persistent signals can pass undetected	Two-area	Frequency measurements

4.4. Covert Attack

The detection technique of covert attack involves the analysis of weak points of an attack and changing the plant behavior after the attacker has discovered the system model. The main weak point of this attack is that it relies strongly on complete system knowledge. A modulation matrix is inserted in the path of control variables to alter the input behavior of the process in [84], for developing a remedial measure. This makes the adversary lose the complete knowledge about the system and the attacks are detected. The preventive measures against covert attack include increasing the difficulty in accessing the control loops. According to the work in [123], the undesirable access can be reduced by using firewall policies, by applying network segmentation and by using specific architecture for network. In addition, the accessibility to data flows can be reduced by using encryption algorithms and time stamping strategies. Another countermeasure is to use control functions like switching controllers that are hard to be identified [87].

4.5. Resonance Attack

Resonance attack is a type of deception attack with two prerequisites: the first is the ability to access the resonance source, and the second is the ability to inject or modify the power plant input according to the resonance reference. Therefore, protection of the input data is the most important countermeasure [11]. In [11], the proposed countermeasure includes the reshaping of the tampered

input for the weakening of the resonance effect. In order to ensure the data authenticity, cryptographic techniques along with timestamps or sequence numbers can be used.

4.6. Time-Delay Switch Attack

Time-delay switch attack implemented in LFC system can affect the system stability and deteriorate performance [91]. The delay injection can be performed by either delaying the telemetered communication packets or at the scale of sampled data points of the sensor [124]. Another way is that the adversary can get access to communication channel and switch off/on the channel. The stability analysis of the LFC system under TDS attack is provided in [91,124]. The delay margin of LFC system under constant and time-varying delays are determined using linear matrix inequality (LMI) techniques and delay-dependent stability criterion in [125]. A prevention strategy using a time delay estimator is proposed in [91]. Here, the controller is augmented with the delay estimator for tracking the injected time delays.

Rapid evolution of PMU and wide area measurement systems (WAMS) helped in the enhancement of coordinated stability control strategies without neglecting time-delays of power system measurements. Therefore, it is necessary to analyze the impact of time-delays in power systems and it is investigated in [126–128].

5. Future Research

The implication from the current review of LFC systems is that most of the research is confined to linear and time-invariant dynamics of the system. The defense mechanisms are not equipped to handle nonlinear system dynamics or time-varying node topology [65]. Only very few works incorporate the non-linearities like GRC and dead zone for the study of attack resilience of the LFC system [30]. Different fields in the cyber-security of LFC system that have not received adequate attention are mentioned below.

- 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 [21].
- Analysis of individual or coordinated attacks in LFC systems under noisy communication networks [20].
- Adequate attention and profound discussion is needed in the area of multiple attack strategies for the development of adaptive defense strategies against different types of attacks [21].
- The vulnerability to distributed attack strategies like DDoS is higher for geographically distributed control systems like LFC. Therefore, more effective coordinated defense strategies for cyber and physical layer has to be developed. ACL-based firework defense strategies of cyber layer applied in [70] have poor real-time performance.
- Extension of estimation and detection schemes to the stochastic model of the LFC system [120].
- 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 RES has to be performed further, as the impact of cyber-attacks can be worse in such kind of systems.
- Apart from analyzing various FDI attacks using the predefined attack templates, multi-step attack strategies adopted by attackers can be also considered for the impact analysis.
- Many of the resilient control techniques developed for defending data integrity techniques do not consider time-delays of the communication channel. The stability of the LFC system may not be affected by small time-delays [27]. However, it can affect the controller efficiency and attack estimation accuracy. Therefore, the defense techniques considering transmission time-delays have to be included in future research.

- 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 LFC system and look for the development of countermeasures.

6. Conclusions

In this work, a state-of-the-art on the cyber-security of load frequency systems is presented. Some of the inferences obtained from the review is 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 AGC 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. This review can help give a background about the different LFC configurations, attack points of LFC systems, and existing cyber-attack resilient measures followed for the LFC systems. However, as mentioned in Section 5, there are many research areas like "stochastic LFC systems", "non-linearities of LFC systems", "cyber-security against stealthy attacks in LFC systems", etc. still remain unexplored. This review work may assist to follow up research in those areas which have received less attention since the core details like modeling of attacks of LFC systems and most of the attack scenarios are comprehensively provided through this discourse.

Author Contributions: N.M. and H.M. conceptualized the review work and A.M.M. performed formal analysis, resource collection, writing (original draft preparation), and visualization. The work is reviewed, supervised, and edited by N.M. and H.M. All authors have read and agreed to the published version of the manuscript.

Funding: This publication was made possible through the NPRP grant (10-105-170107) from the Qatar National Research Fund (a member of the Qatar Foundation). The statements made herein are solely the responsibility of the authors.

Acknowledgments: This work is supported by Qatar University through graduate assistantship (GTRA-CENG-2019-13).

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

References

1. Ali, R.; Mohamed, T.H.; Qudaih, Y.S.; Mitani, Y. A new load frequency control approach in an isolated small power systems using coefficient diagram method. *Int. J. Electr. Power Energy Syst.* **2014**, *56*, 110–116. [CrossRef]
2. Arbab Zavar, B.; Palacios-Garcia, E.J.; Vasquez, J.C.; Guerrero, J.M. Smart inverters for microgrid applications: A review. *Energies* **2019**, *12*, 840. [CrossRef]
3. Shen, J.; Jiang, C.; Li, B. Controllable load management approaches in smart grids. *Energies* **2015**, *8*, 11187–11202. [CrossRef]
4. Xiang, Y.; Lu, X.; Yu, Z.; Shi, D.; Li, H.; Wang, Z. IoT and edge computing based direct load control for fast adaptive frequency regulation. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019; pp. 1–5.
5. Wang, Q.; Wang, H.; Zhu, L.; Wu, X.; Tang, Y. A Multi-Communication-Based Demand Response Implementation Structure and Control Strategy. *Appl. Sci.* **2019**, *9*, 3218. [CrossRef]
6. Mateev, V.; Marinova, I. Distributed Internet of Things System for Wireless Monitoring of Electrical Grids. In Proceedings of the 2018 20th International Symposium on Electrical Apparatus and Technologies (SIELA), Bourgas, Bulgaria, 3–6 June 2018; pp. 1–3.
7. Keyhani, A.; Chatterjee, A. Automatic generation control structure for smart power grids. *IEEE Trans. Smart Grid* **2012**, *3*, 1310–1316. [CrossRef]
8. Saadat, H. *Power System Analysis*; McGraw-Hill: New York, NY, USA, 1999.
9. Oshnoei, A.; Khezri, R.; Muyeen, S.M.; Blaabjerg, F. On the contribution of wind farms in automatic generation control: review and new control approach. *Appl. Sci.* **2018**, *8*, 1848. [CrossRef]
10. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. *Proc. IEEE* **2011**, *100*, 210–224. [CrossRef]

11. Wu, Y.; Wei, Z.; Weng, J.; Li, X.; Deng, R.H. Resonance attacks on load frequency control of smart grids. *IEEE Trans. Smart Grid* **2017**, *9*, 4490–4502. [CrossRef]
12. UCTE. Appendix 1: Load-Frequency Control and Performance. Available online: https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/pre2015/publications/ce/oh/appendix1_v19.pdf (accessed on 4 June 2020).
13. Kirby, B.; Ela, E.; Milligan, M. Analyzing the impact of variable energy resources on power system reserves. In *Renewable Energy Integration*; Elsevier: Amsterdam, The Netherlands, 2017; pp. 85–101.
14. 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]
15. Chatterjee, K.; Padmini, V.; Khaparde, S.A. Review of cyber attacks on power system operations. In Proceedings of the 2017 IEEE Region 10 Symposium (TENSYMP), Cochin, India, 14–16 July 2017; pp. 1–6.
16. 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]
17. Pandey, S.K.; Mohanty, S.R.; Kishor, N. A literature survey on load–frequency control for conventional and distribution generation power systems. *Renew. Sust. Energy Rev.* **2013**, *25*, 318–334. [CrossRef]
18. Dagoumas, A. Assessing the impact of cybersecurity attacks on power systems. *Energies* **2019**, *12*, 725. [CrossRef]
19. Alhelou, H.H.; Hamedani-Golshan, M.E.; Zamani, R.; Heydarian-Forushani, E.; Siano, P. Challenges and opportunities of load frequency control in conventional, modern and future smart power systems: A comprehensive review. *Energies* **2018**, *11*, 2497. [CrossRef]
20. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. A secure control framework for resource-limited adversaries. *Automatica* **2015**, *51*, 135–148. [CrossRef]
21. Mahmoud, M.S.; Hamdan, M.M.; Baroudi, U.A. Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges. *Neurocomputing* **2019**, *338*, 101–115. [CrossRef]
22. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Mitigating the impacts of covert cyber attacks in smart grids via reconstruction of measurement data utilizing deep denoising autoencoders. *Energies* **2019**, *12*, 3091. [CrossRef]
23. Vrakopoulou, M.; Esfahani, P.M.; Margellos, K.; Lygeros, J.; Andersson, G. Cyber-attacks in the automatic generation control. In *Cyber Physical Systems Approach to Smart Electric Power Grid*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 303–328.
24. 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]
25. Tan, R.; Nguyen, H.H.; Foo, E.Y.S.; Dong, X.; Yau, D.K.Y.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Optimal false data injection attack against automatic generation control in power grids. In Proceedings of the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 11–14 April 2016; pp. 1–10.
26. Abbaspour, A.; Sargolzaei, A.; Yen, K. Detection of false data injection attack on load frequency control in distributed power systems. In Proceedings of the 2017 North American Power Symposium (NAPS), Morgantown, WV, USA, 17–19 september 2017; pp. 1–6.
27. 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]
28. Liu, X.; Li, Z. False data attack models, impact analyses and defense strategies in the electricity grid. *Electr. J.* **2017**, *30*, 35–42. [CrossRef]
29. Khalaf, M.; Youssef, A.; El-Saadany, E. Joint detection and mitigation of false data injection attacks in AGC systems. *IEEE Trans. Smart Grid* **2018**, *10*, 4985–4995. [CrossRef]
30. Cheng, Z.; Yue, D.; Hu, S.; Huang, C.; Dou, C.; Chen, L. Resilient load frequency control design: DoS attacks against additional control loop. *Int. J. Electr. Power Energy Syst.* **2020**, *115*, 105496. [CrossRef]
31. Bevrani, H. *Robust Power System Frequency Control*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 85.
32. Murty, P.S.R. Load Frequency Control. In *Electrical Power Systems*; Elsevier: Amsterdam, The Netherlands, 2017; pp. 651–700.
33. Roy, S.D.; Debbarma, S. Detection and Mitigation of Cyber-Attacks on AGC Systems of Low Inertia Power Grid. *IEEE Syst. J.* **2019**, *14*, 2023–2031. [CrossRef]

34. Tan, R.; Nguyen, H.H.; Foo, E.Y.S.; Yau, D.K.Y.; 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]
35. 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]
36. 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]
37. Franzè, G.; Tedesco, F.; Casavola, A.; Garone, E. A leader-follower architecture for Load Frequency Control purposes against cyber attacks in power grids-Part I and II. In Proceedings of the 2016 IEEE 55th Conference on Decision and Control (CDC), Las Vegas, NV, USA, 12–14 December 2016; pp. 5128–5139.
38. Chen, C.; Cui, M.; Wang, X.; Zhang, K.; Yin, S. An investigation of coordinated attack on load frequency control. *IEEE Access* **2018**, *6*, 30414–30423. [CrossRef]
39. Sridhar, S.; Manimaran, G. Data integrity attacks and their impacts on SCADA control system. In Proceedings of the IEEE PES General Meeting, Providence, RI, USA, 25–29 July 2010; pp. 1–6.
40. 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]
41. Alrifai, M.T.; Hassan, M.F.; Zribi, M. Decentralized load frequency controller for a multi-area interconnected power system. *Int. J. Electr. Power Energy Syst.* **2011**, *33*, 198–209. [CrossRef]
42. Daneshfar, F.; Bevrani, H. Multiobjective design of load frequency control using genetic algorithms. *Int. J. Electr. Power Energy Syst.* **2012**, *42*, 257–263. [CrossRef]
43. Dong, L.; Zhang, Y.; Gao, Z. A robust decentralized load frequency controller for interconnected power systems. *ISA Trans.* **2012**, *51*, 410–419. [CrossRef]
44. Bevrani, H.; Daneshfar, F.; Daneshmand, P.R. Intelligent automatic generation control: Multi-agent Bayesian networks approach. In Proceedings of the 2010 IEEE International Symposium on Intelligent Control, Yokohama, Japan, 8–10 September 2010; pp. 773–778.
45. Adaryani, M.R.; Afrakhte, H. NARMA-L2 controller for three-area load frequency control. In Proceedings of the 2011 19th Iranian Conference on Electrical Engineering, Tehran, Iran, 17–19 May 2011; pp. 1–6.
46. Vrdoljak, K.; Perić, N.; Petrović, I. Sliding mode based load-frequency control in power systems. *Electr. Power Syst. Res.* **2010**, *80*, 514–527. [CrossRef]
47. Prakash, S.; Sinha, S.K. Four area Load Frequency Control of interconnected hydro-thermal power system by Intelligent PID control technique. In Proceedings of the 2012 Students Conference on Engineering and Systems, Allahabad, India, 16–18 March 2012; pp. 1–6.
48. Huang, T.; Satchidanandan, B.; Kumar, P.R.; Xie, L. An Online Detection Framework for Cyber Attacks on Automatic Generation Control. *IEEE Trans. Power Syst.* **2018**, *33*, 6816–6827. [CrossRef]
49. Yammani, C.; Maheswarapu, S. Load Frequency Control of Multi-microgrid System considering Renewable Energy Sources Using Grey Wolf Optimization. *Smart Sci.* **2019**, *7*, 198—-217.
50. Doolla, S.; Bhatti, T.S. Load frequency control of an isolated small-hydro power plant with reduced dump load. *IEEE Trans. Power Syst.* **2006**, *21*, 1912–1919. [CrossRef]
51. Semshchikov, E.; Hamilton, J.; Wu, L.; Negnevitsky, M.; Wang, X.; Lyden, S. Frequency control within high renewable penetration hybrid systems adopting low load diesel methodologies. *Energy Procedia* **2019**, *160*, 483–490. [CrossRef]
52. Kumar, G.V.; Sarojini, R.K.; Palanisamy, K.; Padmanaban, S.; Holm-Nielsen, J.B. Large Scale Renewable Energy Integration: Issues and Solutions. *Energies* **2019**, *12*, 1996. [CrossRef]
53. Rezkalla, M.; Pertl, M.; Marinelli, M. Electric power system inertia: Requirements, challenges and solutions. *Electr. Eng.* **2018**, *100*, 2677–2693. [CrossRef]
54. Magdy, G.; Mohamed, E.A.; Shabib, G.; Elbaset, A.A.; Mitani, Y. Microgrid dynamic security considering high penetration of renewable energy. *Prot. Control Mod. Power Syst.* **2018**, *3*, 23. [CrossRef]
55. 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.
56. Datta, A.; Bhattacharjee, K.; Debbarma, S.; Kar, B. Load frequency control of a renewable energy sources based hybrid system. In Proceedings of the 2015 IEEE Conference on Systems, Process and Control (ICSPC), Bandar Sunway, Malaysia, 18–20 December 2015; pp. 34–38.

57. Datta, A.; Konar, S.; Singha, L.J.; Singh, K.M.; Lalfakzuala, A. A study on load frequency control for a hybrid power plant. In Proceedings of the 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 22–24 February 2017; pp. 1–5.
58. Xu, Y.; Li, C.; Wang, Z.; Zhang, N.; Peng, B. Load frequency control of a novel renewable energy integrated micro-grid containing pumped hydropower energy storage. *IEEE Access* **2018**, *6*, 29067–29077. [CrossRef]
59. Hakimuddin, N.; Khosla, A.; Garg, J.K. Centralized and decentralized AGC schemes in 2-area interconnected power system considering multi source power plants in each area. *J. King Saud Univ. Eng. Sci.* **2020**, *32*, 123–132.
60. Arya, Y. AGC of restructured multi-area multi-source hydrothermal power systems incorporating energy storage units via optimal fractional-order fuzzy PID controller. *Neural. Comput. Appl.* **2019**, *31*, 851–872. [CrossRef]
61. Arya, Y.; Kumar, N. Design and analysis of BFOA-optimized fuzzy PI/PID controller for AGC of multi-area traditional/restructured electrical power systems. *Soft Comput.* **2017**, *21*, 6435–6452. [CrossRef]
62. Yousef, H.A. *Power System Load Frequency Control: Classical and Adaptive Fuzzy Approaches*; CRC Press: Boca Raton, FL, USA, 2017.
63. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
64. Teixeira, A.; Pérez, D.; Sandberg, H.; Johansson, K.H. Attack models and scenarios for networked control systems. In Proceedings of the 1st International Conference on High Confidence Networked Systems; ACM: New York, NY, USA, 2012; pp. 55–64.
65. 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]
66. Amin, S.; Cárdenas, A.A.; Sastry, S.S. Safe and secure networked control systems under denial-of-service attacks. In *Proceedings of the International Workshop on Hybrid Systems: Computation and Control*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 31–45.
67. Cetinkaya, A.; Ishii, H.; Hayakawa, T. An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy* **2019**, *21*, 210. [CrossRef]
68. 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 February 2013; pp. 1–6.
69. 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]
70. Wang, Q.; Tai, W.; Tang, Y.; Zhu, H.; Zhang, M.; Zhou, D. Coordinated Defense of Distributed Denial of Service Attacks against the Multi-Area Load Frequency Control Services. *Energies* **2019**, *12*, 2493. [CrossRef]
71. Jaafar, G.A.; Abdullah, S.M.; Ismail, S. Review of recent detection methods for HTTP DDoS attack. *J. Comput. Netw. Commun.* **2019**, *2019*, 1283472.
72. Zhong, X.; Jayawardene, I.; Venayagamoorthy, G.K.; Brooks, R. Denial of service attack on tie-line bias control in a power system with pv plant. *IEEE Trans. Emerg. Top. Comput. Intell.* **2017**, *1*, 375–390. [CrossRef]
73. Girma, A.; Garuba, M.; Li, J.; Liu, C. Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment. In Proceedings of the 2015 12th International Conference on Information Technology-New Generations, Las Vegas, NV, USA, 13–15 April 2015; pp. 212–217.
74. Sridhar, S.; Govindarasu, M. Model-based attack detection and mitigation for automatic generation control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591. [CrossRef]
75. Jevtic, A.; Zhang, F.; Li, Q.; Ilic, M. Physics-and Learning-based Detection and Localization of False Data Injections in Automatic Generation Control. *IFAC-PapersOnLine* **2018**, *51*, 702–707. [CrossRef]
76. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. [CrossRef]
77. 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]
78. Kontouras, E.; Tzes, A.; Dritsas, L. Cyber-attack on a power plant using bias injected measurements. In Proceedings of the 2017 American Control Conference (ACC), Seattle, WA, USA, 24–26 May 2017; pp. 5507–5512.

79. Mo, Y.; Sinopoli, B. Secure control against replay attacks. In Proceedings of the 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 30 September–2 October 2009; pp. 911–918.
80. Fritz, R.; Zhang, P. Modeling and detection of cyber attacks on discrete event systems. *IFAC-PapersOnLine* **2018**, *51*, 285–290. [CrossRef]
81. Mo, Y.; Weerakkody, S.; Sinopoli, B. Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Syst. Mag.* **2015**, *35*, 93–109.
82. Hoehn, A.; Zhang, P. Detection of replay attacks in cyber-physical systems. In Proceedings of the 2016 American Control Conference (ACC), Boston, MA, USA, 6–8 July 2016; pp. 290–295.
83. Zhao, J.; Wang, J.; Yin, L. Detection and control against replay attacks in smart grid. In Proceedings of the 2016 12th International Conference on Computational Intelligence and Security (CIS), Wuxi, China, 16–19 December 2016; pp. 624–627.
84. Hoehn, A.; Zhang, P. Detection of covert attacks and zero dynamics attacks in cyber-physical systems. In Proceedings of the 2016 American Control Conference (ACC), Boston, MA, USA, 6–8 July 2016; pp. 302–307.
85. Li, W.; Xie, L.; Wang, Z. A novel covert agent for stealthy attacks on industrial control systems using least squares support vector regression. *J. Electr. Comput. Eng.* **2018**, *2018*, 1–14. [CrossRef]
86. Smith, R.S. Covert misappropriation of networked control systems: Presenting a feedback structure. *IEEE Control Syst. Mag.* **2015**, *35*, 82–92.
87. De Sá, A.O.; da Costa Carmo, L.F.R.; Machado, R.C.S. Covert attacks in cyber-physical control systems. *IEEE Trans. Ind. Informat.* **2017**, *13*, 1641–1651. [CrossRef]
88. De Sá, A.O.; da Costa Carmo, L.F.R.; Machado, R.C.S. A controller design for mitigation of passive system identification attacks in networked control systems. *J. Internet Serv. Appl.* **2018**, *9*, 1–19. [CrossRef]
89. Mohsenian-Rad, A.H.; Leon-Garcia, A. Distributed internet-based load altering attacks against smart power grids. *IEEE Trans. Smart Grid* **2011**, *2*, 667–674. [CrossRef]
90. Hammad, E.; Khalil, A.M.; Farraj, A.; Kundur, D.; Iravani, R. Tuning out of phase: Resonance attacks. In Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA, 2–5 November 2015; pp. 491–496.
91. 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]
92. Zhang, H.; Qi, Y.; Zhou, H.; Zhang, J.; Sun, J. Testing and defending methods against DoS attack in state estimation. *Asian J. Control* **2017**, *19*, 1295–1305. [CrossRef]
93. Sinopoli, B.; Schenato, L.; Franceschetti, M.; Poolla, K.; Jordan, M.I.; Sastry, S.S. Kalman filtering with intermittent observations. *IEEE Trans. Automat. Contr.* **2004**, *49*, 1453–1464. [CrossRef]
94. Wu, Y.; Li, Y.; Shi, L. A game-theoretic approach to remote state estimation in presence of a dos attacker. *IFAC-PapersOnLine* **2017**, *50*, 2595–2600. [CrossRef]
95. Shen, Y.; Fei, M.; Du, D.; Zhang, W.; Stanković, S.; Rakić, A. Cyber Security Against Denial of Service of Attacks on Load Frequency Control of Multi-area Power Systems. In *Advanced Computational Methods in Energy, Power, Electric Vehicles, and Their Integration*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 439–449.
96. Peng, C.; Li, J.; Fei, M. Resilient Event-Triggering H∞ Load Frequency Control for Multi-Area Power Systems With Energy-Limited DoS Attacks. *IEEE Trans. Power Syst.* **2016**, *32*, 4110–4118. [CrossRef]
97. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2011**, *14*, 13. [CrossRef]
98. Kwon, C.; Liu, W.; Hwang, I. Security analysis for cyber-physical systems against stealthy deception attacks. In Proceedings of the 2013 American Control Conference, Washington, DC, USA, 17–19 June 2013; pp. 3344–3349.
99. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. Revealing stealthy attacks in control systems. In Proceedings of the 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 1–5 October 2012; pp. 1806–1813.
100. Yang, Q.; Yang, J.; Yu, W.; An, D.; Zhang, N.; Zhao, W. On false data-injection attacks against power system state estimation: Modeling and countermeasures. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *25*, 717–729. [CrossRef]

101. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting false data injection attacks in ac state estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [CrossRef]
102. Bobba, R.B.; Rogers, K.M.; Wang, Q.; Khurana, H.; Nahrstedt, K.; Overbye, T.J. Detecting false data injection attacks on dc state estimation. In Proceedings of the Preprints of the First Workshop on Secure Control Systems, CPSWEEK, Stockholm, Switzerland, 12 April 2010; pp. 1–9.
103. Bi, S.; Zhang, Y.J. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Trans. Smart Grid* **2014**, *5*, 1216–1227. [CrossRef]
104. 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.
105. 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.
106. Giannini, M. Improving Cyber-Security of Power System State Estimators. 2014. Available online: https://www.diva-portal.org/smash/get/diva2:704601/FULLTEXT01.pdf (accessed on 7 June 2020).
107. Liu, L.; Esmalifalak, M.; Ding, Q.; Emesih, V.A.; Han, Z. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Trans. Smart Grid* **2014**, *5*, 612–621. [CrossRef]
108. Huang, Y.; Li, H.; Campbell, K.A.; Han, Z. Defending false data injection attack on smart grid network using adaptive CUSUM test. In Proceedings of the 2011 45th Annual Conference on Information Sciences and Systems, Baltimore, MD, USA, 23–25 March 2011; pp. 1–6.
109. Talebi, M.; Li, C.; Qu, Z. Enhanced protection against false data injection by dynamically changing information structure of microgrids. In Proceedings of the 2012 IEEE 7th Sensor Array and Multichannel Signal Processing Workshop (SAM), Hoboken, NJ, USA, 17–20 June 2012; pp. 393–396.
110. Li, X.; Hedman, K.W. Enhancing Power System Cyber-Security with Systematic Two-Stage Detection Strategy. *IEEE Trans. Power Syst.* **2019**, *35*, 1549–1561. [CrossRef]
111. Yang, L.; Li, Y.; Li, Z. Improved-ELM method for detecting false data attack in smart grid. *Int. J. Electr. Power Energy Syst.* **2017**, *91*, 183–191. [CrossRef]
112. Wang, X.; Luo, X.; Zhang, Y.; Guan, X. Detection and Isolation of False Data Injection Attacks in Smart Grids via Nonlinear Interval Observer. *IEEE Internet Things J.* **2019**, *6*, 6498–6512. [CrossRef]
113. Wang, X.; Luo, X.; Zhang, M.; Guan, X. Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers. *Int. J. Electr. Power Energy Syst.* **2019**, *110*, 208–222. [CrossRef]
114. Rahman, M.A.; Mohsenian-Rad, H. False data injection attacks against nonlinear state estimation in smart power grids. In Proceedings of the 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, Canada, 21–25 July 2013; pp. 1–5.
115. Rahman, M.A.; Mohsenian Rad, H. False data injection attacks with incomplete information against smart power grids. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 3153–3158.
116. Li, S.; Yılmaz, Y.; Wang, X. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Trans. Smart Grid* **2014**, *6*, 2725–2735. [CrossRef]
117. Chen, C.; Zhang, K.; Yuan, K.; Zhu, L.; Qian, M. Novel detection scheme design considering cyber attacks on load frequency control. *IEEE Trans. Ind. Informat.* **2017**, *14*, 1932–1941. [CrossRef]
118. Khalaf, M.; Youssef, A.; El-Saadany, E. A Particle Filter-Based Approach for the Detection of False Data Injection Attacks on Automatic Generation Control Systems. In Proceedings of the 2018 IEEE Electrical Power and Energy Conference (EPEC), Toronto, ON, Canada, 10–11 October 2018; pp. 1–6.
119. Ayad, A.; Khalaf, M.; El-Saadany, E. Detection of false data injection attacks in automatic generation control systems considering system nonlinearities. In Proceedings of the 2018 IEEE Electrical Power and Energy Conference (EPEC), Toronto, ON, Canada, 10–11 October 2018; pp. 1–6.
120. Miloševič, J.; Tanaka, T.; Sandberg, H.; Johansson, K.H. Analysis and mitigation of bias injection attacks against a Kalman filter. *IFAC-PapersOnLine* **2017**, *50*, 8393–8398. [CrossRef]
121. Luo, X.; Wang, X.; Zhang, M.; Guan, X. Distributed detection and isolation of bias injection attack in smart energy grid via interval observer. *Appl. Energy* **2019**, *256*, 113703. [CrossRef]

122. Zhu, M.; Martinez, S. On the performance analysis of resilient networked control systems under replay attacks. *IEEE Trans. Autom. Control* **2013**, *59*, 804–808. [CrossRef]
123. Stouffer, K.; Falco, J.; Scarfone, K. Guide to industrial control systems (ICS) security. *NIST Spec. Publ.* **2011**, *800*, 16.
124. Sargolzaei, A.; Yen, K.; Abdelghani, M.N. Delayed inputs attack on load frequency control in smart grid. In Proceedings of the ISGT 2014, Washington, DC, USA, 19–22 February 2014; pp. 1–5.
125. Jiang, L.; Yao, W.; Wu, Q.H.; Wen, J.Y.; Cheng, S.J. Delay-dependent stability for load frequency control with constant and time-varying delays. *IEEE Trans. Power Syst.* **2011**, *27*, 932–941. [CrossRef]
126. Jia, H.; Yu, X.; Yu, Y.; Wang, C. Power system small signal stability region with time delay. *Int. J. Electr. Power Energy Syst.* **2008**, *30*, 16–22. [CrossRef]
127. Wu, H.; Tsakalis, K.S.; Heydt, G.T. Evaluation of time delay effects to wide-area power system stabilizer design. *IEEE Trans. Power Syst.* **2004**, *19*, 1935–1941. [CrossRef]
128. Milano, F.; Anghel, M. Impact of time delays on power system stability. *IEEE Trans. Circuits Syst. I* **2011**, *59*, 889–900. [CrossRef]