JOURNALS | Journal of Visual Artificial Intelligence

Volume 2 Issue 1 (June 2026)
J. Vis. Artif. Intell., 2026, 1(1), 26104
DOI : https://doi.org/10.64189/vai.26104

Review Article

OPEN ACCESS

Cyber-Resilient Load Frequency Control in Modern Interconnected Power Systems: A Systematic Literature Review of Intelligent and Secure Control Strategies

Satheeshkumar R,[1,*] Jagatheesan K,[2] Lenin V R,[3] Kanendra Naidu[4] and Anand B[5]

[1] *Paavai Engineering College, Namakkal, Tamilnadu, 637018, India*
[2] *Vivekanandha College of Engineering for Women, Tiruchengode, Tamilnadu, 637205, India*
[3] *Anil Neerukonda Institute of Technology and Sciences, Andhra Pradesh, 531162, India*
[4] *Universiti Teknologi MARA, Shah Alam, Selangor, 40450 Malaysia*
[5] *Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, 641032, India*

*Corresponding Author
Satheeshkumar R
satheesh2811@gmail.com

Received: 04 May 2026
Revised: 15 June 2026
Accepted: 25 June 2026
Published Online: 29 June 2026

Citation

Satheeshkumar R, Jagatheesan K, Lenin V R, K. Naidu, Anand B, Cyber-resilient load frequency control in modern interconnected power systems: A systematic literature review of intelligent and secure control strategies, *Journal of Visual Artificial Intelligence*, 2026, 1(1), 26104, https://doi.org/10.64189/vai.26104.

Abstract

Load Frequency Control (LFC) is very significant in the present situation. With that, one can be certain to maintain and manage power stability in relation to frequency changes while continuing reliable power traded over different tie-lines, which are all actually occurring in modern power systems. In addition, deregulated operation regimes are also implicated, holding stability with LFC systems by email threats like cyber security which occurred mostly during the process. This paper provides an excellent review from the literature on LFC methodologies not only of classical, robust, and optimization but intelligent and cyber-resilient control strategies as well. Further development focused on more modern approaches like model predictive control, sliding mode control, fractional-order control, and the development of observer-based techniques for increased robustness and rejection of disturbances in a complex multi-area system. Concomitantly, since then, conventional metaheuristic algorithms become most popular and are amongst the best for controllers optimized to be very transiently responsive and stable in the steady state. Recent research trends are towards such cyber-secure and resilient LFC designs which enable event-triggered or self-triggered control, distributed/decentralized framework, resilient observers, and new age methods like neural networks, fuzzy logic, or reinforcement learning based real-time attack detection and defense. This review provides a comprehensive analysis of 124 peer-reviewed studies published between 2015 and 2026 on cyber-resilient LFC for interconnected power systems. The analysis shows that around 38% of the studies concentrate on resilient control strategies, while 29% focus on cyber-attack detection and mitigation techniques. Approximately 18% investigate intelligent optimization and artificial intelligence (AI)-based solutions, whereas the remaining 15% explore secure communication frameworks, blockchain technologies, and distributed control architectures. The review also highlights a clear shift in recent research toward AI-enabled adaptive control, observer-based estimation, event-triggered communication, distributed control methods, and blockchain-supported secure LFC frameworks designed for renewable-rich smart grids.

Keywords: Artificial intelligence; Frequency stability; Load frequency control; Renewable energy integration; Resilient control.

1. Introduction

In the recent years the frequency and power regulation has changed significantly, as the electro mechanical traditional power grid has moved towards the modern actively smart power grid operation. In regards to the frequency regulation, it is a regulating circuit that maintains the power balance between connected control areas in a network, i.e., the import and export of power across regulating gates in integrated areas under changing power demand conditions. Large-scale employment of renewable energy requirement and energy storage, the control information structure on the basis of communication systems and energy power points with the present-day system is one of the notable features, allowing the system to shift its focus from the high inertia, low uncertainty and low operational complexity. In contrast with the gradual changes in the components included in systems, the level of complexity of the changes in the frequency regulation has exceeded all expectations, especially since it was made a must to come up with such measures given the present day control expectations.[1]

There are many physical and technological disruptions in the practice of depending on digital communication networks, leading to creating huge cyber security stakes in cyber-physical systems. One of the most targeted entry points concerns the LFC loop, which lies between sensors, communication channels, and control centers. This means that it can easily be bamboozled by numerous cyber attacks among them false specious data injection, denial-of-service, replay-type, and time delay attack.[2] Actuation of these malicious touch points can lead to lack of faith in the accuracy of signals for measurement or retardation in control actions that provokes overall frequency response instability in interconnected power systems. Hence, indeed, there is certainly a very high level of research priority sought on cyber-resilient frequency design for the modern operation like smart grid.

In the past decade, a variety of secure and smart LFC approaches have been suggested by researchers to build the system resilience against uncertainties and threats. In this manner, the conventional PI/PID controllers have started to be replaced, or rather supplemented with newer advanced methods like model predictive control, H∞ control, observer-based techniques, event-triggered control, and distributed control framework. Intelligence-based approaches have proven to effectively deal with these and many other severe problems by incorporating such noteworthy modern methods as neural network, reinforcement learning, and adaptive optimization algorithms. Studies on cyber-attack and resilient control showed that there is a gap to be amended with detailed developmental measures featuring vast Literature on Intelligent and Secure LFC Strategies for modern interconnected power systems has been displayed on Fig. 1. It is, therefore, the aim of this research to systematically investigate existing research by conducting feedback to produce details into computer intrusion resilient how to control frequency. This study, therefore, by classifying the detection technique, attack simulation, and control design that are impactful to secure designs, provides a comprehensive understanding of existing phenomena patterns.

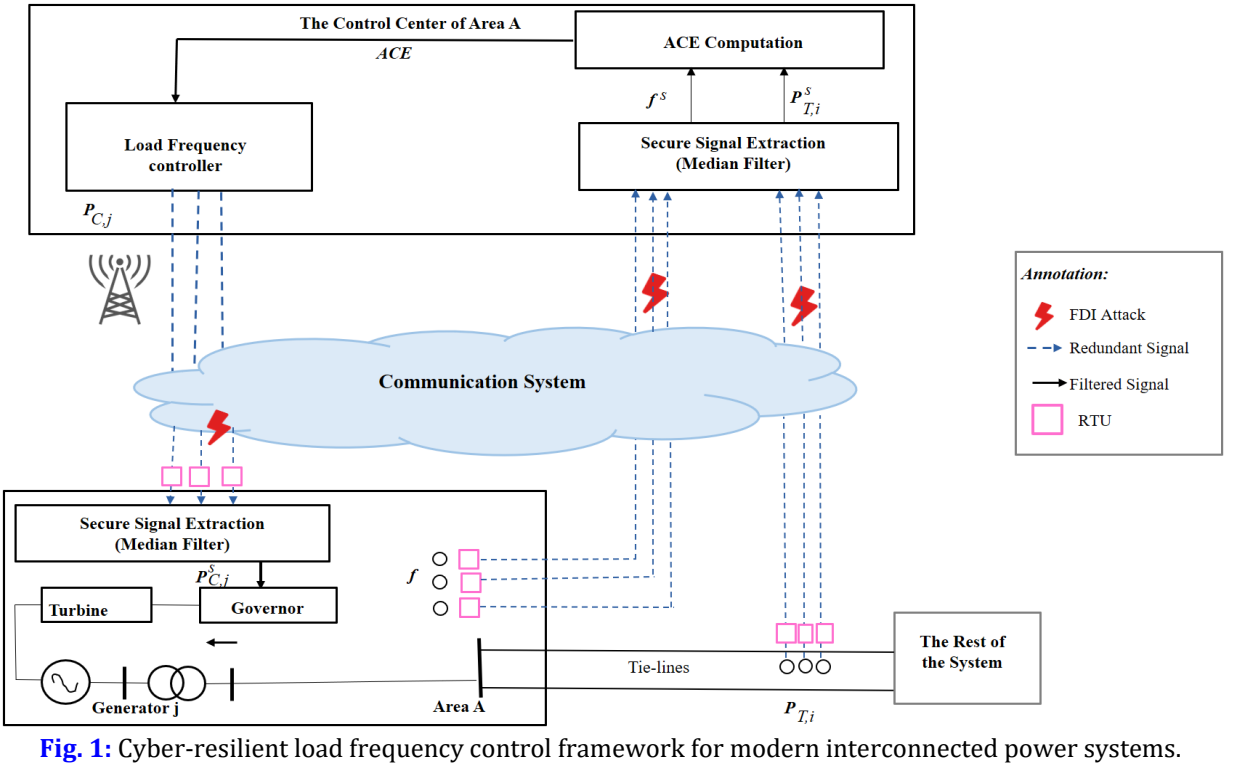

Fig. 1: Cyber-resilient load frequency control framework for modern interconnected power systems.

2. Literature review

The acceleration in both systems' digitization and the integration of renewable energies, cyber - physical interconnections in smart grids, attention devoted to research in cyber-attack-resilient LFC has increased substantially. Notably, various research groups have made efforts to implement detection of attacks, mitigation, or resilient control methodologies in order to protect the frequency regulation method from malevolent stages of cyber intrusions. Unequivocally more studies in this area could be categorized into seven broad thematic groups according to the type of cyber threat anticipated and its corresponding control or security strategy. These categories consist: Time-Delay and Communication Delay Attacks, False Data Injection (FDI) Attacks, Denial-of-Service (DoS) Attacks, Deception and Bias Injection Attacks, Hybrid and Coordinated Cyber Attacks, Renewable Integrated and Microgrid Cybersecurity Studies, Intelligence and Data-Driven Cyber-Resilient Control Methods as shown in Table 1, and the flowchart was displayed in Fig. 2.

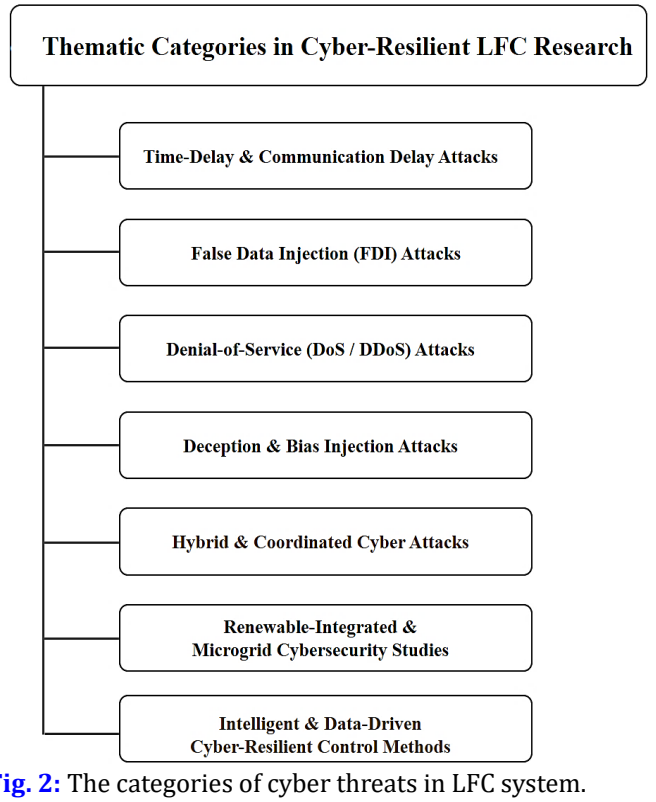

Fig. 2: The categories of cyber threats in LFC system.

Robust control strategies were developed to enhance the resilience of LFC systems against delayed input cyber attacks, thereby improving frequency regulation under compromised communication conditions. Preventive and detection mechanisms were introduced to address time-delay switch attacks in distributed power systems, ensuring the secure operation of the Automatic Generation Control (AGC) loop.[3] The adverse impact of communication time-delay attacks on AGC performance and overall system stability was also demonstrated.[4] To support the evaluation of cyber-resilient control strategies, an experimental cyber security testbed for critical power infrastructure was established.[5] Furthermore, comprehensive studies reviewed the major cyber security threats affecting smart grid frequency control and summarized effective countermeasures for cyber-enabled power systems.[6] Research also examined the consequences of DoS attacks and proposed appropriate mitigation and preventive control strategies.[7] Secure state estimation based on distributed compressive sensing was introduced to improve system resilience under cyber uncertainties, showing that cyber attacks can significantly reduce grid observability.[8] The authors of [9,10] discussed the cyber security challenges associated with smart meter data intelligence and future energy systems.

A leader–follower architecture was proposed to enhance the resilience of LFC systems against cyber attacks by improving coordination in frequency regulation.[11] A comprehensive survey of cyber-physical attacks and defense mechanisms in smart grids highlighted major resilience challenges and security requirements.[12] A hierarchical Stackelberg game-based resilient control strategy was introduced to mitigate intelligent cyber attacks in Cyber-Physical Systems (CPS).[13] A cyber-physical control framework was also developed to preserve power system stability under malicious cyber disturbances.[14] The author[15] was designed the hierarchical cyber attack detection scheme for smart home environments by considering power overloading and frequency disturbances. Simulation-based approaches were presented to analyze cyber security threats in smart grids and evaluate the effectiveness of mitigation algorithms.[16] Planning and operational challenges in smart grids, including cyber security concerns, were also comprehensively discussed.[17] An Industrial Control System (ICS) security testbed was developed in [18] to investigate timing attacks and evaluate their impact on control system performance. Adaptive neural network-based techniques were proposed to improve the detection of malicious data injection attacks in CPS.[19] A decision-support framework was introduced to enhance the resilience and operational reliability of cooperative cyber-physical control systems under cyber threats.[20]

A novel cyber-attack detection scheme was developed for LFC systems, enabling the identification of a wide range of cyber attacks with improved detection accuracy.[21] Defensive strategies were proposed to mitigate the impact of DoS attacks on multi-area LFC systems, thereby enhancing system security and operational reliability.[22] The impact of resonance attacks on smart grid frequency regulation was investigated in [23] demonstrating their potential to destabilize power

system operation. A FDI attack detection method was introduced for distributed LFC systems using shared measurement data to improve attack identification.[24] A real-time cyber-physical testbed was developed to evaluate the security, protection, and control performance of power system operations under cyber attacks.[25] Cybersecurity protection strategies for power grid control infrastructures and communication networks were also investigated to improve the resilience of distributed power systems.[26] The effects of bias injection attacks on power plant operation and system performance were analyzed, highlighting their influence on control stability.[27] In [28], author modelled the cascading failure attacks in power systems using a stochastic game framework to evaluate their impact on grid reliability.[28] A resilient networked control system was designed to withstand time-delay switch attacks, ensuring secure communication between controllers and power system components.[29] The cyber attacks targeting data integrity in storage-based transient stability control were investigated, and suitable mitigation strategies were proposed to enhance grid resilience.[30]

Significant progress was made in 2018 toward improving the cyber resilience of LFC systems. A sliding mode observer-based control strategy was developed for multi-area power systems.[31] to enhance robustness against bounded delayed-input cyber attacks, resulting in improved frequency regulation under adverse operating conditions. Comprehensive reviews also examined the cyber-physical resilience of modern power systems by identifying major vulnerabilities and summarizing defense mechanisms against malicious cyber threats.[32] Another extensive survey highlighted the evolution of LFC in conventional and smart power systems, emphasizing the increasing importance of cybersecurity in future frequency control applications [33]. Advanced techniques for attack detection and identification were introduced for AGC systems, enabling faster and more reliable recognition of cyber intrusions.[34] A set-theoretic approach was proposed in [35] to detect data corruption attacks in cyber-physical power systems, thereby improving the reliability of monitoring and control functions. The author was employed a stochastic unknown-input estimator to strengthen attack detection capabilities in LFC systems operating under uncertain conditions. [36] Neural network-based resilient control methods were also developed to maintain stable operation of distributed power systems during both component faults and cyber attacks.[37] Fault-tolerant control strategies for electronically coupled distributed energy resources further enhanced the resilience and reliability of microgrid operation.[38] The security challenges associated with networked control systems in smart grids were comprehensively reviewed, identifying existing vulnerabilities and potential protection mechanisms.[39] In [40], author was proposed the distributed Model Predictive Control (MPC) framework for wide-area power systems to ensure secure and scalable operation under malicious cyber attacks.

A decentralized functional observer-based optimal LFC framework was developed to improve frequency regulation in the presence of unknown inputs, system uncertainties, and cyber attacks.[41] The effects of DoS attacks on power system stability were thoroughly investigated and resilient control strategies were proposed to mitigate their impact.[42] An event-triggered H∞ control approach was introduced by the author[43] for multi-area LFC systems operating under hybrid cyber attacks, improving both communication efficiency and system robustness. Resilient event-triggered output feedback control techniques were also developed to maintain stable frequency regulation despite malicious cyber intrusions.[44] Dynamic characteristic analysis was employed to detect cyber-physical attacks on LFC systems, enabling timely identification of abnormal operating conditions.[45] Observer-based attack detection and mitigation methods were further proposed to improve the resilience of frequency control against coordinated cyber attacks.[46] Deterministic dynamic state estimation using unknown input observers was introduced to enhance the accuracy and security of interconnected power system LFC.[47] The author [48] was proposed effective defense mechanisms against DoS attacks to strengthen the reliability and stability of frequency control systems operating in cyber-enabled power grids. Coordinated defense strategies against distributed DoS attacks were also investigated to ensure secure operation of multi-area LFC services.[49] The attack–defense interaction models considering incomplete information were developed to optimize cybersecurity strategies and improve the resilience of LFC systems against evolving cyber threats.[50]

A dynamic event-based MPC framework was developed to maintain stable frequency regulation in power systems operating under cyber-attacks.[51] The impact of cyber attacks on AC–HVDC interconnected power systems with emulated inertia was comprehensively analyzed, highlighting their influence on system stability and dynamic performance.[52] Renewable energy-based LFC schemes were further investigated by incorporating stochastic generation, communication delays, and packet losses to improve operational reliability under uncertain conditions.[53] Cyber-attack-tolerant frequency control strategies were introduced to ensure secure and reliable operation of interconnected power systems despite malicious intrusions.[54] Robust defense mechanisms were also developed to mitigate load-altering attacks, thereby enhancing the resilience of LFC systems against

coordinated cyber threats.[55] Counteractive control techniques were proposed to address cyber-attack uncertainties affecting frequency regulation and to maintain system stability under adverse operating conditions.[56] A memory-based event-triggered H∞ LFC strategy was designed to improve resilience against deception attacks while reducing communication overhead.[57] Secure frequency control methods for microgrids were also developed to maintain stable operation under FDI attacks targeting measurement sensors.[58] Robust LFC schemes capable of withstanding random time-delay attacks were further proposed to enhance the reliability of communication-based control systems.[59] A credibility-based secure distributed LFC framework was introduced to defend interconnected power systems against FDI attacks while ensuring reliable frequency regulation.[60]

A comprehensive survey summarized the cybersecurity challenges, vulnerabilities, and defense mechanisms associated with LFC systems in modern power networks.[61] Memory-event-triggered H∞ control schemes were proposed to improve frequency regulation under communication delays and cyber attacks while reducing unnecessary data transmission.[62] Active fault-tolerant control strategies were introduced to maintain stable LFC performance in the presence of both physical faults and cyber-attacks.[63] FDI attack detection methods based on Kalman filtering and controller design were also developed to enhance the security of LFC systems.[64] Dual-source data-driven detection techniques further improved the identification of compromised variables and cyber attacks in frequency control applications.[65] An intrusion mitigation framework was proposed to strengthen cybersecurity and enhance the resilience of interconnected power systems during frequency regulation.[66] Switching system-based LFC strategies capable of withstanding DoS attacks were developed to ensure reliable operation of multi-area power systems.[67] Event-triggered control methods for Markovian jump interconnected power systems were also introduced to improve resilience against DoS attacks while reducing communication overhead.[68] Furthermore, intrusion detector-dependent distributed economic MPC was proposed for secure load frequency regulation in systems integrated with plug-in electric vehicles under cyber attack scenarios.[69] Decentralized robust disturbance observer-based LFC techniques were also developed to enhance disturbance rejection and improve the reliability of interconnected power systems under uncertain operating conditions.[70]

An H-infinity (H∞) based LFC scheme was developed for multi-area power systems to maintain stable frequency regulation under cyber attacks and time-varying communication delays.[71] Distributed observer-based event-triggered control methods were introduced to improve the resilience of multi-area LFC systems against malicious cyber intrusions while reducing communication overhead.[72] Event-triggered resilient LFC strategies were also proposed for cyber-physical power systems to effectively mitigate the impact of DoS attacks.[73] Dynamic event-triggered output feedback control approaches were designed to ensure secure frequency regulation under multiple coordinated cyber attacks.[74] A comprehensive review summarized recent advances in cybersecurity analysis, attack detection, and defense mechanisms for cyber-physical power systems, highlighting the growing importance of resilient control architectures.[75] Robust LFC methods for wind-integrated power systems were further developed to address communication delays and packet losses while maintaining system stability.[76] Dynamic event-triggered H∞ control schemes were introduced to enhance the resilience of multi-area power systems against hybrid cyber-attacks.[77] The resilient LFC strategies capable of withstanding DoS attacks were proposed to improve the security and reliability of interconnected power systems.[78] Sliding mode event-triggered control techniques were also developed to strengthen the robustness of multi-area LFC systems operating under hybrid cyber attacks.[79] The resilient control-based frequency regulation schemes were proposed for isolated microgrids by considering both cyber attacks and parameter uncertainties, thereby ensuring secure and reliable system operation.[80]

A cybersecurity-oriented LFC framework in [81] was proposed by the author for hybrid interconnected renewable power systems to enhance resilience against a wide range of cyber attacks. Sliding Mode Observer (SMO)-based attack estimation techniques were introduced to improve the resilience of frequency control in interconnected power systems under cyber attacks.[82] Robust networked LFC architectures were also developed to withstand hybrid cyber attacks while maintaining reliable system performance.[83] Online recursive attack detection combined with adaptive fuzzy mitigation was proposed to protect islanded microgrids from cyber-physical attacks targeting LFC operation.[84] The vulnerability of Linear Quadratic Gaussian (LQG)-based virtual inertia frequency control to DoS attacks was investigated, and its impact on isolated microgrid stability was thoroughly analyzed.[85] Distributed coordination-based LFC schemes incorporating attack detection and compensation mechanisms were further developed to mitigate the effects of DoS attacks in interconnected power systems.[86] Quantum-inspired cybersecurity techniques were also explored to strengthen the protection of electrical infrastructure against emerging cyber threats.[87] A Dragonfly Algorithm-optimized PID controller was proposed to improve automatic frequency control in interconnected

DSTS power grids, resulting in enhanced dynamic performance and reduced frequency deviations [88]. An Ant Colony Optimization (ACO)-based PI controller was also developed to improve frequency regulation in interconnected power systems by achieving faster and more stable dynamic responses [89]. Comprehensive reviews highlighted the evolving cybersecurity challenges and defense strategies for cyber-physical power systems.[90]

The contribution of energy storage technologies to frequency management in nuclear power systems was comprehensively investigated, highlighting their role in improving system stability and reliability.[91] A cyber-resilient frequency control framework that accounts for system nonlinearities and practical operating constraints was proposed to improve the reliability and security of interconnected power systems.[92] The author [93] was applied ACO-optimized secondary control strategies to microgrids, leading to improved frequency regulation during system disturbances. A fuel cell-based non-integer controller was introduced to strengthen both LFC and cybersecurity in renewable energy microgrids operating under cyber attacks [94]. Cyberattack defense strategies for smart grid LFC integrated with electric vehicles were also proposed to enhance system resilience and operational security.[95] Preventive LFC schemes were developed to improve the reliability of aging multi-area power systems subjected to cyber attacks.[96] Resilient frequency regulation methods capable of mitigating hybrid cyber attacks were further introduced to enhance power system security.[97] Decentralized secure LFC strategies were proposed for multi-area power systems operating under complex cyber threats, ensuring reliable frequency regulation.[98] A data-driven attack recovery (DAR-LFC) mechanism was also developed to restore normal operation following cyber attacks on frequency control systems.[99] Power system stability was comprehensively analyzed from a cyber-attack perspective to identify potential vulnerabilities and improve system resilience.[100] Data-driven switching-based LFC approaches were proposed for multi-area power systems to maintain secure frequency regulation under cyber attack conditions.[101] Smart frequency control techniques were further developed to withstand FDI attacks in cyber-physical power systems.[102] Cyberattack-aware LFC frameworks were introduced to improve the security and reliability of interconnected power systems operating in hostile cyber environments.[103] The attack-parameter-dependent DoS-resilient LFC strategies and blockchain-enabled defense mechanisms were proposed to strengthen cybersecurity and ensure reliable frequency regulation under DoS attacks.[104,105]

A reinforcement learning-based LFC framework was developed for microgrids to maintain stable frequency regulation under FDI attacks.[106] Secure LFC methods were further proposed for cyber-physical power systems by considering cyber attacks, communication delays, and varying risk levels to improve operational reliability.[107] An estimation-based Linear Quadratic Regulator (LQR) approach was introduced to mitigate data integrity attacks in hybrid power systems, thereby enhancing control performance under compromised communication environments.[108] Advanced LFC schemes were also developed for renewable energy- and electric vehicle-integrated power systems to effectively suppress frequency deviations triggered by cyber attacks.[109] The impact of DoS attacks on LFC performance in deregulated power markets was comprehensively analysed, highlighting the associated operational challenges and mitigation requirements.[110] A modified hybrid fractional PID control strategy optimized using the mZOA algorithm was proposed to improve frequency regulation under multiple cyber attack scenarios.[111] Observer-based fuzzy event-triggered LFC incorporating neural network approximation was introduced to enhance resilience against multiple cyber attacks while reducing communication burden.[112] A resilient tri-parametric fractional frequency control strategy was also developed by considering communication latency, demonstrating improved robustness under delayed cyber environments.[113] A comprehensive defense framework was proposed to simultaneously mitigate FDI, DoS, and latency attacks, thereby strengthening secure frequency regulation in cyber-physical power systems.[114] The robust LFC strategies for renewable-integrated smart grids were presented to maintain reliable frequency regulation despite cyber interruptions and communication uncertainties.[115]

Neural network-based adaptive LFC strategies were developed for multi-area power systems to improve resilience against hybrid cyber attacks while maintaining reliable frequency regulation.[116] Comprehensive studies also analyzed the vulnerabilities, threat models, and security architectures of cyber-physical power systems, providing valuable insights into the design of resilient control frameworks.[117] The impact of optimization algorithms and energy storage systems on frequency management in both standalone and interconnected power systems was systematically investigated, demonstrating the effectiveness of coordinated energy storage in enhancing frequency stability.[118] Controlled energy storage-based cyber-resilient LFC frameworks were further proposed for renewable-integrated power systems to improve operational security under cyber attack scenarios.[119] Secure LFC strategies employing quantized MPC under round-robin communication protocols were introduced to ensure reliable frequency regulation in networked power systems.[120] Dynamic

self-triggered LFC approaches were also developed to address the challenges of non-ideal communication environments while reducing communication overhead.[121] An integral re-averaging control strategy was proposed for T–S fuzzy reaction–diffusion power systems to enhance resilience against cyber attacks and maintain system stability.[122] Robust PI-type LFC schemes were further designed for renewable energy-integrated power systems by considering communication delays associated with electric vehicle aggregators.[123] In addition, cascaded optimized fractional-order controllers were introduced to strengthen the cyber resilience of green hydrogen-based microgrids against FDI attacks.[124] From the literature, it is clear that an evolution was noticed from conventional resilient control and attack detection methods to the intelligent, distributed, data-driven, and blockchain-supported secure control framework for LFC. The latest studies are focusing on hybrid cyber-attack resilience, AI-based adaptive control, event-triggered communication, observer-based estimation, and secure decentralized architectures, and highlight the necessity of cyber-secured frequency regulation in renewable-rich, low-inertia, and highly connected modern power systems.

To make the scope of the reviewed literature easier to navigate, the 124 studies summarized above have been reorganized into four focused tables rather than a single extended one. Table 1 groups the studies by the type of cyber-attack they address, spanning ten broad categories from DoS and FDI to time-delay and hybrid multi-vector attacks, along with the number of studies, the years they span, and their reference numbers.

Table 1: Attack types addressed in cyber-resilient LFC research (2015-2026, n = 124 studies).

Attack type	No. of studies	Year range	Ref.
General / Unspecified Cyber Attack	42	2016-2026	11, 13, 14, 15, 21, 32, 34, 36, 37, 40, 41, 44, 46, 50, 51, 52, 54, 56, 62, 63, 65, 69, 71, 72, 80, 81, 82, 87, 92, 94, 95, 96, 99, 100, 101, 103, 107, 109, 111, 113, 119, 122
DoS/DDoS	14	2015-2025	7, 22, 42, 48, 49, 67, 68, 73, 78, 85, 86, 104, 105, 110
Time-Delay / Latency Attacks	9	2015-2020	1, 2, 3, 4, 18, 29, 31, 53, 59
FDI	9	2016-2026	19, 24, 58, 60, 64, 102, 106, 114, 124
Hybrid / Multi-Vector Attacks	9	2019-2026	43, 74, 77, 79, 83, 97, 98, 112, 116
Data Integrity / Deception Attacks	6	2017-2025	27, 30, 35, 55, 57, 108
Cyber-Physical Attacks (General)	3	2016-2023	12, 45, 84
Cascading / Resonance Attacks	2	2017	23, 28
Data / Measurement Attacks	1	2015	9
Cyber Intrusion	1	2021	66
Not specified in source study	28	2015-2026	5, 6, 8, 10, 16, 17, 20, 25, 26, 33, 38, 39, 47, 61, 70, 75, 76, 88, 89, 90, 91, 93, 115, 117, 118, 120, 121, 123

Table 2: Control strategies proposed for cyber-resilient LFC (2015-2026).

Control strategy	No. of studies	Year range	Ref.
General Resilient Control	21	2015-2026	1, 11, 14, 29, 53, 58, 60, 67, 78, 80, 81, 94, 97, 98, 102, 103, 104, 107, 109, 111, 121
Event-Triggered Control	11	2019-2025	43, 44, 57, 62, 68, 72, 73, 74, 77, 79, 112
Defense / Mitigation Strategy	8	2015-2025	2, 48, 49, 55, 56, 66, 95, 114
AI / Data-Driven Control	7	2018-2026	37, 84, 99, 101, 106, 116, 122
H∞ / Robust Control	7	2020-2026	54, 59, 71, 76, 83, 115, 123
Optimization-Tuned / Fractional Control	6	2023-2026	88, 89, 93, 113, 118, 124
Observer-Based Control	5	2018-2023	31, 41, 47, 70, 82
MPC	4	2018-2026	40, 51, 69, 120
Game-Theoretic Control/Defense	3	2016-2019	13, 28, 50
Fault-Tolerant Control	2	2018-2021	38, 63
LQR/LQG Control	2	2023-2025	85, 108
Energy-Storage-Based Control	2	2023-2026	91, 119
Blockchain-Based Control	1	2024	105

Table 3: Cyber-attack detection methods reported in lfc research (2015-2026).

Detection method	No. of studies	Year range	Ref.
Attack Detection Technique (General)	4	2015-2023	3, 34, 84, 86
State/Input Estimation-Based Detection	3	2018-2023	36, 47, 82
Detection Algorithm (General)	2	2016-2017	15, 24
Detection Scheme (General)	2	2017-2021	21, 65
Intrusion Detection	2	2021	66, 69
Set-Theoretic Detection	1	2018	35
Observer-Based Detection	1	2019	46
Kalman-Filter-Based Detection	1	2021	64

Table 2 turns to how these attacks are countered, sorting the work into thirteen families of control strategy, including event-triggered schemes, observer-based designs, model predictive control, H∞/robust formulations, and more recent AI- and data-driven approaches.

In Table 3 narrows in on detection specifically, since not every study that proposes a control strategy also proposes a way to detect the attack in the first place; here the studies fall into eight detection-technique families, among them Kalman-filter-based, set-theoretic, observer-based, and intrusion-detection methods.

Finally, Table 4 steps back from cataloguing individual studies and instead distils seven open research gaps that emerge once the field is viewed as a whole, covering coordinated multi-vector attacks, the growing complexity of renewable and EV-integrated grids, the disconnect between detection and control design, scalability to large distributed systems, the generalizability of AI-based methods, the still-nascent use of blockchain and quantum-based security, and the lack of standardized testbeds for comparing approaches; each of these gaps is linked back to the specific studies that motivate it.

2. Critical analysis, research gaps, limitations, and future research directions

2.1 Critical analysis of the reviewed literature

The literature reviewed in this study demonstrates that considerable progress has been made in developing cyber-resilient LFC strategies for interconnected power systems. Initial research mainly concentrated on maintaining frequency stability under conventional operating conditions using classical controllers such as PI and PID controllers. As power systems evolved into highly interconnected cyber-physical systems, researchers increasingly focused on addressing cyber threats that could compromise the reliability and stability of frequency control. In recent years, significant attention has been given to developing resilient control techniques capable of detecting and mitigating cyber

Table 4: Future challenges and open research directions for Cyber-Resilient LFC.

Challenge / Research gap	Description
Multi-vector and coordinated attacks	Most studies address a single attack type in isolation; robust detection/control under simultaneous FDI, DoS and time-delay attacks remains largely open (only 9 hybrid studies, e.g. refs 43, 74, 79, 112, 116).
Renewable- and EV-integrated grids	Low-inertia, high-penetration renewable and EV-aggregator systems introduce new attack surfaces; only a small, recent subset of studies (e.g. refs 109, 119, 123, 124) addresses this explicitly.
Real-time detection-control co-design	Detection methods (16 studies) and control strategies (79 studies) are largely developed separately; tightly-coupled, real-time detection-and-mitigation frameworks are comparatively rare.
Scalability to large, distributed/multi-area systems	Event-triggered and distributed MPC approaches (e.g. refs 40, 51, 69, 120) show promise but scalability to large multi-area, multi-agent grids needs further validation.
Data-driven / AI-based generalization	AI and data-driven control (7 studies) is emerging but often validated on limited test systems; generalization, explainability and adversarial robustness remain open questions.
Blockchain- and quantum-based security	Only isolated studies (e.g. refs 87, 105) explore blockchain- or quantum-based protection; practical, standardized implementations for LFC remain unexplored.
Standardized cybersecurity testbeds and benchmarks	Testbed/case-study work (e.g. refs 5, 18, 25) is limited; the field lacks common, openly available benchmark platforms for comparing detection and control strategies.

attacks such as FDI, DoS, replay attacks, communication delays, deception attacks, and coordinated hybrid attacks. Advanced control approaches, including model predictive control, adaptive control, observer-based methods, sliding mode control, event-triggered control, distributed control, and artificial intelligence-based techniques, have shown improved performance compared with conventional controllers, particularly under uncertain operating conditions. Similarly, nature-inspired optimization algorithms have been widely adopted to enhance controller tuning and improve dynamic performance.

Although these developments have contributed significantly to the field, the existing literature remains fragmented. Most studies investigate only a specific attack scenario or a particular control strategy without considering the combined influence of multiple cyber-attacks, renewable energy uncertainty, communication network limitations, and practical implementation issues. Consequently, the available research provides only a partial understanding of cyber resilience in modern interconnected power systems.

2.2 Research gaps

The comprehensive review of the literature has revealed several research gaps that require further investigation. The majority of existing studies examine individual cyber attacks independently, whereas real-world power systems are more likely to experience coordinated attacks involving multiple attack vectors. The interaction between hybrid cyber attacks and renewable energy uncertainties has received comparatively little attention. Another important limitation is the lack of experimental validation. Most published works evaluate their proposed methods using simulation platforms, while only a limited number of studies demonstrate their effectiveness through Hardware-in-the-Loop (HIL) testing, Real-Time Digital Simulator (RTDS), OPAL-RT platforms, or industrial-scale implementations. As a result, the practical feasibility of many proposed techniques remains uncertain.

Artificial intelligence has emerged as a promising solution for cyber-attack detection and resilient control. However, many AI-based approaches rely on complex deep learning models whose decision-making process is difficult to interpret. The absence of explainable AI limits their acceptance in safety-critical power system applications. The increasing integration of renewable energy sources introduces additional operational uncertainties, including intermittent generation, reduced system inertia, and rapidly changing operating conditions. Many existing cyber-resilient control strategies do not adequately account for these challenges, particularly when combined with cyber-attacks. Communication issues also remain insufficiently addressed. Factors such as communication delays, packet losses, synchronization errors, bandwidth limitations, and network congestion can significantly influence controller performance but are often simplified or neglected in current studies. Furthermore, many proposed control strategies have been validated only for small-scale two-area or three-area interconnected systems. Their scalability and computational performance in large-scale interconnected smart grids with numerous distributed energy resources require further investigation.

Finally, relatively few studies consider compliance with practical cybersecurity standards and industrial communication protocols. Bridging the gap between academic research and real-world deployment remains an important challenge.

2.3 Limitations of existing approaches

The review indicates that every resilient control strategy possesses certain advantages as well as inherent limitations. Conventional PI and PID controllers are simple to implement but generally provide limited resilience against sophisticated cyber-attacks. Robust and adaptive controllers improve disturbance rejection but often require accurate system models and involve higher design complexity. MPC offers excellent dynamic performance; however, its computational requirements may restrict real-time implementation in large-scale systems. Observer-based techniques depend heavily on estimation accuracy and may become sensitive under severe model uncertainties. AI-based methods achieve high detection accuracy but often require large training datasets and lack transparency in their decision-making process. Likewise, blockchain-based communication frameworks enhance data integrity and security but introduce additional communication overhead and latency that must be carefully managed.

2.4 Novelty statement

Unlike existing review articles that primarily focus on conventional LFC techniques, optimization algorithms, or individual cyber-attack scenarios, this study presents a comprehensive and systematic review of intelligent and cyber-resilient LFC strategies for modern interconnected power systems. The review synthesizes evidence from 124 peer-reviewed publications (2015–2026) and integrates developments in resilient control, cyber-attack detection, secure communication, artificial intelligence, and distributed control into a unified analytical framework. It provides a structured classification of control methodologies according to controller design, cyber threats, defense mechanisms, optimization techniques, communication architectures, and renewable energy integration. This work identifies emerging research trends, highlights unresolved

technical challenges, and establishes future research directions involving AI-enabled adaptive control, event-triggered communication, observer-based estimation, blockchain-supported security, and decentralized frequency regulation. By connecting control theory with cybersecurity and intelligent energy management, this review offers a holistic perspective that is currently lacking in the existing LFC literature.

2.5 Future research directions

The findings of this review suggest several promising directions for future research. Explainable artificial intelligence should be explored to improve the transparency and reliability of AI-assisted cyber-attack detection and resilient control. The integration of digital twin technology with LFC may enable continuous monitoring, predictive analysis, and proactive mitigation of cyber threats. Blockchain and distributed ledger technologies also offer significant potential for secure communication and data authentication, although their scalability and computational efficiency require further improvement.

Future studies should investigate resilient control strategies capable of handling coordinated hybrid cyber attacks under highly uncertain operating conditions associated with renewable energy integration, electric vehicles, energy storage systems, and distributed generation. Greater emphasis should also be placed on developing scalable distributed control architectures suitable for large interconnected power systems. Experimental validation should become an integral part of future research. Hardware-in-the-Loop testing, real-time digital simulation, FPGA implementation, and pilot-scale demonstrations would provide stronger evidence of practical applicability. In addition, the development of standardized benchmark systems, publicly available datasets, and common performance evaluation metrics would facilitate objective comparison among different cyber-resilient control techniques and accelerate progress in this research area.

3. Cyber-attack themes and resilient control strategies

The Fig. 3 presents a thematic classification of modern, interconnected power systems in cyber-resilient LFC research; this is evidenced from [32]. Some cybersecurity risks at the LFC level are also illustrated, with time manipulation attacks, malicious data insertion, denial, deception, and hybrid coordinated threats given germane mention.[61] These threats then spread across various coordinated regions, communication links, control loops, and, in some cases, to frequency. Among the means to counter these challenges include various resilient control strategies like observer-based control, triggers of event-based control, and completion control systems.[75]

Renewable integration and microgrid environments increase the uncertainty of the system considerably-the boiling points of which are cyber vulnerability. Intelligent

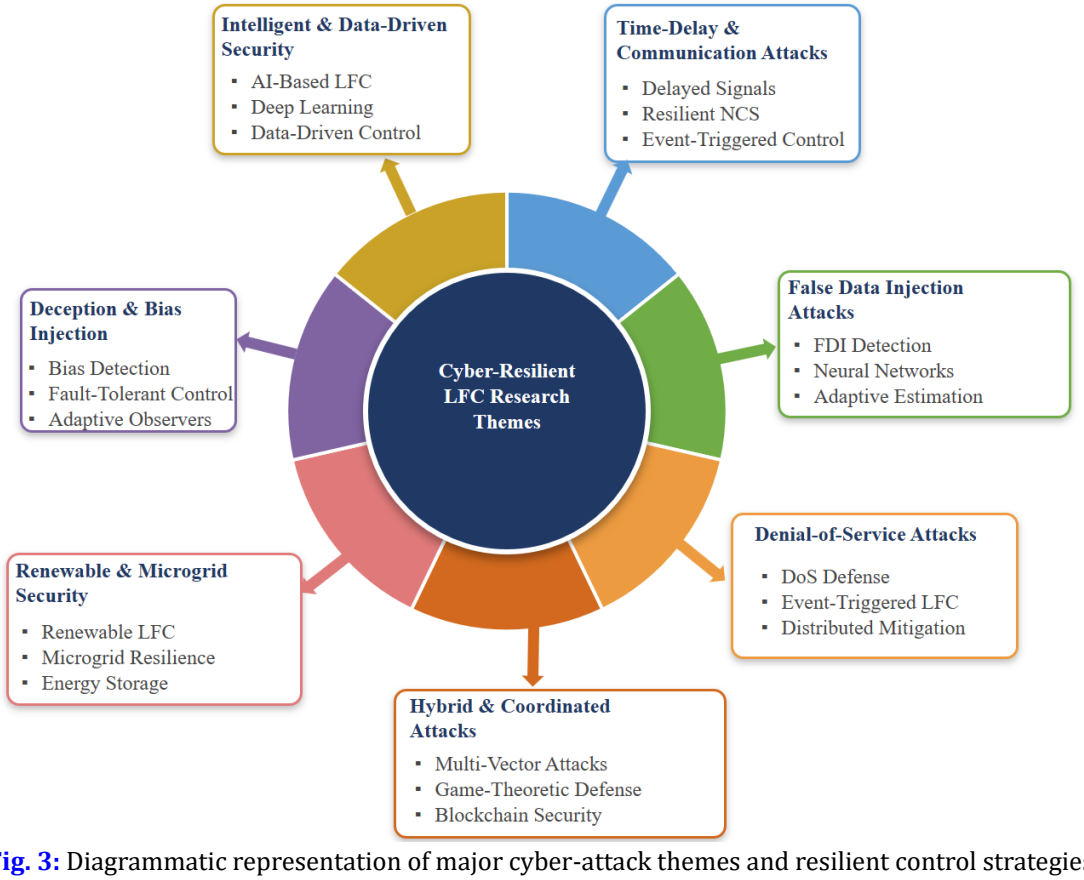

Fig. 3: Diagrammatic representation of major cyber-attack themes and resilient control strategies.

and data-driven methods are portrayed as advanced mitigation tools with artificial intelligence, reinforcement learning, and neural networks. Blockchain-enabled exposure to security features of communication architectures increasingly demands data integrity. This exposition shows how the conventional robust control changes to an adaptive and intelligent system of cyber-resilient LFC. It further goes further inside the basic layers such that it combines detection, estimation, and mitigation into a single organized viewpoint. In general, this figure provides a well-rounded concept of all characteristics nurturing cyber-resilient LFC themes and emerging trends in future smart grids.

3.1. Time-delay and communication delay attacks

Time-delay and communication delay attacks represent one of the earliest and most extensively investigated cyber security threats in LFC systems. These attacks intentionally introduce delays into sensor measurements, control commands, or communication channels linking interconnected control areas, thereby disrupting the timely exchange of frequency and tie-line power information. Since LFC relies on continuous feedback to maintain the balance between power generation and demand, even small communication delays can degrade dynamic performance, increase frequency oscillations, and prolong settling time under disturbed operating conditions.[1,31] Early studies primarily focused on analysing the impact of communication delays on AGC performance and assessing their influence on overall system stability. As research progressed, greater attention was directed towards identifying abnormal communication delays using delay estimation techniques, timestamp verification, residual monitoring, and communication health assessment. These detection mechanisms enable the control system to distinguish malicious delays from normal network latency, allowing appropriate corrective actions to be initiated before system performance deteriorates.

To reduce the adverse effects of delay attacks, several mitigation strategies have been proposed. Delay compensation algorithms, predictive estimation methods, redundant communication paths, and packet recovery techniques help maintain reliable information exchange during network disturbances. In parallel, resilient control approaches have evolved from conventional robust controllers to more advanced techniques, including sliding-mode observer-based control, H∞ control, memory-based control, and event-triggered control. These methods reduce the dependence on continuous communication while maintaining frequency stability despite uncertain network conditions. More recently, distributed and quantized control frameworks have demonstrated improved robustness against random and stochastic communication delays in large-scale interconnected power systems.[59] Overall, research on time-delay attacks has progressed from impact assessment to the development of integrated detection, mitigation, and resilient control strategies, significantly improving the cyber security and operational reliability of modern cyber-physical power systems.

3.2 False data injection attacks

FDI attacks are among the most extensively studied cyber security threats in LFC systems because they directly compromise the integrity of measurement data used for frequency regulation. In these attacks, an adversary deliberately manipulates critical signals, such as frequency deviation, tie-line power, and Area Control Error (ACE), with the objective of misleading the controller while remaining undetected.[58] Unlike conventional disturbances, FDI attacks are particularly dangerous because the manipulated data often appear legitimate, allowing the attack to gradually degrade system performance without triggering immediate alarms.[60] Initial research in this area primarily focused on state estimation and anomaly detection techniques to identify inconsistencies between measured and estimated system states. As the field advanced, observer-based methods, unknown-input observers, and Kalman filter-based algorithms were introduced to improve attack detection accuracy and reconstruct compromised signals. Adaptive estimation techniques further enhanced the ability to detect stealthy attacks under varying operating conditions.

Several mitigation strategies have been developed to minimize the impact of compromised measurements on system performance. Secure state estimation, adaptive filtering, measurement validation, and sensor redundancy are widely adopted to isolate corrupted data and recover reliable system information before control actions are executed. More recently, credibility-based distributed LFC frameworks have been proposed to evaluate the trustworthiness of information exchanged among interconnected control areas, thereby reducing the influence of compromised communication channels.[102] In parallel, resilient control strategies have evolved to include observer-based controllers, adaptive control schemes, fuzzy logic, neural networks, and deep learning techniques capable of maintaining stable frequency regulation even in the presence of manipulated data. These intelligent approaches continuously update system models, improve attack identification, and support real-time corrective actions. Overall, research on FDI attacks has progressed from basic detection methods to integrated frameworks that combine attack detection, data validation, mitigation, and resilient control, thereby enhancing the cyber security and operational reliability

of modern interconnected power systems.

3.3 Denial-of-service attacks

DoS attacks primarily target the communication infrastructure of interconnected power systems by interrupting, delaying, or blocking the transmission of control signals between sensors, controllers, and control centres. As a result, critical information such as frequency deviation, tie-line power, and ACE may not reach the controller within the required time, leading to poor coordination among control areas, increased frequency deviations, and reduced system reliability. Early studies mainly investigated the impact of packet losses, communication interruptions, and signal blocking on AGC, demonstrating that prolonged communication failures can significantly degrade transient performance and even threaten system stability. To detect such attacks, researchers have proposed communication health monitoring, packet-loss analysis, network traffic monitoring, watchdog timers, and anomaly detection techniques that continuously assess the availability and integrity of communication links.

Following attack detection, several mitigation strategies have been introduced to maintain reliable frequency regulation during communication disruptions. These include redundant communication networks, packet retransmission mechanisms, adaptive communication scheduling, and coordinated defense strategies that reduce the impact of large-scale network attacks. At the control level, resilient solutions such as event-triggered control, switching-based control, observer-based control, and predictive control have been developed to maintain acceptable performance even when communication links are temporarily unavailable. Decentralized and distributed LFC architectures further improve system resilience by reducing dependence on a centralized communication network and enabling local controllers to operate independently during communication failures. More recent studies have integrated adaptive secure observers, robust control techniques, and distributed resilient control frameworks to enhance the ability of cyber-physical power systems to withstand DoS attacks while preserving frequency stability. Overall, research on DoS attacks has evolved from analysing communication failures to developing comprehensive frameworks that combine attack detection, mitigation, and resilient control, thereby improving the security and reliability of modern interconnected power systems.

3.4 Deception and bias injection attacks

Deception and bias injection attacks are stealthy cyber threats that manipulate control inputs or measurement signals without interrupting communication between system components. Instead of blocking data transmission, these attacks introduce carefully crafted false information into frequency deviation, ACE, or tie-line power measurements, making the manipulated signals appear similar to normal operating disturbances. As a result, the controller may generate incorrect control actions, leading to gradual deterioration of frequency regulation performance while the attack remains difficult to detect. Early research mainly focused on analysing the impact of deception attacks on interconnected power systems and developing mathematical models to understand their influence on system dynamics. To identify these stealthy attacks, researchers introduced set-theoretic methods, residual-based monitoring, observer-based estimation, and adaptive state estimation techniques capable of detecting subtle deviations between measured and expected system behaviour.[35] These approaches significantly improved the detection of malicious signal manipulation under uncertain operating conditions.

To minimize the impact of compromised measurements such as observer-based signal reconstruction, adaptive bias compensation, secure state estimation, and measurement validation methods are widely used to recover reliable system information before it is utilized by the controller. In addition, active fault-tolerant control strategies have been developed to simultaneously address both physical component faults and cyber intrusions, thereby improving overall system resilience. Memory-based H∞ controllers, intelligent observers, and adaptive estimation algorithms further enhance the capability of LFC systems to compensate for hidden malicious inputs while maintaining stable frequency regulation.[57] Recent research has also incorporated artificial intelligence-based observers and real-time bias compensation techniques to improve detection accuracy and accelerate system recovery. Overall, the development of secure LFC frameworks for deception and bias injection attacks has evolved from impact analysis to integrated detection, mitigation, and resilient control strategies, providing improved protection against stealthy cyber threats in modern interconnected power systems.

3.5 Hybrid and coordinated cyber attacks

Hybrid cyber attacks combine multiple attack strategies, such as FDI, DoS, deception, and communication delay attacks, to simultaneously compromise different components of interconnected power systems. These coordinated attacks are considerably more challenging to identify and mitigate because they exploit multiple vulnerabilities at the same time, resulting in severe degradation of LFC performance and overall grid stability. The initial indication of a hybrid attack is often the simultaneous occurrence of abnormal communication behaviour and inconsistent

measurement data, making conventional single-layer detection methods insufficient. Consequently, recent research has focused on developing integrated detection frameworks that combine anomaly detection, observer-based estimation, machine learning algorithms, and multi-source data fusion techniques to identify complex attack patterns more accurately. Attacker-defender game-theoretic models have also been introduced to analyse the interaction between attackers and system operators, enabling more effective cyber security planning and risk assessment.[80]

Once a hybrid attack is detected, mitigation strategies aim to isolate compromised communication channels, validate measurement data, and maintain reliable information exchange across interconnected control areas. Adaptive communication management, secure data validation, coordinated recovery mechanisms, and redundant network architectures have been widely investigated to reduce the impact of simultaneous attacks. In parallel, resilient control strategies have evolved from conventional robust controllers to adaptive and intelligent control frameworks capable of maintaining frequency stability under multiple cyber threats. Deep learning-based predictive models have recently been employed to anticipate attack behaviour and support proactive mitigation before system performance is significantly affected. Block chain-assisted secure communication has also emerged as a promising solution for preserving data integrity and preventing unauthorized data manipulation. Furthermore, cooperative multi-agent defense frameworks enable distributed controllers to exchange trusted information and coordinate control actions, thereby enhancing the overall resilience of interconnected power systems against sophisticated cyber attacks.[79] Overall, current research on hybrid cyber attacks highlights the growing need for integrated detection, mitigation, and resilient control mechanisms to ensure the secure and reliable operation of future cyber-physical power grids.

3.6 Renewable-integrated and microgrid cyber themes

The increasing penetration of renewable energy resources and microgrids has introduced new cyber security challenges for LFC, particularly in low-inertia power systems. Unlike conventional power networks, renewable-rich systems exhibit higher operational uncertainty and reduced inertia, making them more vulnerable to cyber attacks that target communication networks, distributed controllers, and measurement devices. Such attacks can amplify frequency deviations, disrupt power sharing among distributed energy resources, and degrade the overall stability of interconnected microgrids. Consequently, recent research has focused on identifying abnormal operating conditions through distributed monitoring, phasor measurement unit (PMU)-based state estimation, anomaly detection algorithms, and data-driven analytics capable of distinguishing cyber attacks from normal renewable power fluctuations. These detection techniques provide early warning of malicious activities while reducing false alarms caused by the intermittent nature of renewable generation.

Following attack detection, several mitigation strategies have been developed to improve the resilience of renewable-integrated power systems. Secure communication protocols, distributed state estimation, adaptive energy management, and coordinated control of distributed energy resources help maintain reliable operation even when parts of the communication network are compromised. Energy storage systems, including battery energy storage and hybrid storage technologies, further enhance frequency support by compensating for power imbalances during cyber disturbances. In addition, resilient control strategies based on adaptive control, stochastic control, model predictive control, and distributed secondary frequency control have been widely investigated to maintain frequency stability under uncertain operating conditions. More recently, artificial intelligence and data-driven approaches have been incorporated into LFC frameworks to improve attack detection, predictive decision-making and real-time disturbance rejection.[119] Emerging concepts such as hydrogen-integrated power systems and hybrid energy systems are also being explored to enhance the cyber resilience of future smart grids. Overall, current research demonstrates that combining advanced detection methods, effective mitigation techniques, and intelligent resilient control is essential for ensuring secure and reliable frequency regulation in renewable-rich interconnected power systems.

3.7. Intelligent and data-driven security themes

Intelligent and data-driven cyber security has become one of the most promising research directions for improving the resilience of LFC systems against evolving cyber threats. The rapid advancement of artificial intelligence, machine learning, deep learning, and reinforcement learning has enabled LFC systems to move beyond conventional rule-based security mechanisms towards adaptive and predictive cyber defense. These techniques continuously analyse large volumes of operational data to detect abnormal system behaviour, identify attack patterns, and distinguish cyber attacks from normal operating disturbances with higher accuracy than traditional model-based approaches.[101,106] Deep learning algorithms, intelligent state observers, and data-driven anomaly detection models have demonstrated significant improvements in identifying

stealthy attacks, estimating compromised system states, and providing early warning of potential cyber intrusions, even under highly uncertain operating conditions.

The intelligent mitigation strategies employ adaptive learning, online model updating, and predictive decision-making to minimize the impact of malicious activities before they propagate through the control system. Data validation, secure information fusion, trust evaluation, and block chain-assisted communication further enhance the integrity and reliability of data exchanged among interconnected control areas. At the resilient control level, AI-assisted adaptive controllers, reinforcement learning-based control, self-triggered control, and intelligent decentralized control frameworks enable rapid recovery from cyber disturbances while maintaining stable frequency regulation. Hybrid AI-observer architectures further improve estimation accuracy and support real-time compensation for compromised measurements, thereby strengthening the overall resilience of interconnected power systems.[116] As future smart grids become increasingly digitalized and renewable-intensive, the integration of intelligent detection, adaptive mitigation, and AI-enabled resilient control is expected to play a key role in achieving autonomous, secure, and reliable frequency regulation under dynamic cyber-physical environments.

4. Conclusion

The summary is a hidden place with cyber-robust LFC built to keep varying weather pumps in an unsafe position at a modern, synchronized electrical power output insertion where it binds substantial portions of inject-into from the side of increasing renewable penetration, communication delays, and cyber-physical vulnerabilities. Having studied research contributions conducted in a wide genre, it is shown that much research progresses through self-assorted and combined recovery southeast productions in cyber-attack modelling, detection, and resilient control designs, gathering together conventional, robust, observer-based, and in-depth event-triggered and AI driven approaches. Cyber attacks will cause serious disturbances in frequency stability, disturb tie-line power regulation, and threaten the secure operation of multi-area power systems if the system is attacked with FDI, denial-of-service, replay, and time delay attacks. The first takes into account traditional PI/PID-based LFC methods from the study. Through all documented articles, it is clear that the traditional LFC with PI/PID control is ineffectual for the contingencies of low-inertia renewable-incorporated grids as well as cyber combined threats. Advanced control strategies show enhancement of robustness in comparison to conventional methods. Advanced control strategies include using edge methods, for example, H∞ control, model-area model-based control, or sliding mode control and distributed observer-based techniques to attack and the approach with adaptive robust control for the design of novel LFC algorithms. Also, the intelligent robot is put into action with the flexibility of the brain network used as reinforcement learning and hybrid optimization algorithms, bolstered by fuzzy logic to help the system shrug off any attack and attempt any real-time recovery in cyber-physical environments. It is clear that the review also demonstrates the growing trend towards integrated frameworks combining intrusion detection systems, secure communication protocols, and data-driven control to enable reliable frequency regulation. Increasing use of event-triggered and decentralized control architectures can lead to reduced communication overhead and prevent system instability even when deprived from network constraints and cyber disruptions. Moreover, inclusion of energy storage systems and renewable deployment force multipliers their dynamic frequency response and operational flexibility. However, advances being made, several research gaps are yet to be fully addressed such as accuracy of real-time implementations, scalability in large interconnected grids, the coordination of defense against hybrid cyber-attacks, and the necessity of standardizing security-aware LFC frameworks. Future research shall tackle AI-based explainable controller developments, security using block chain communication and adaptive and resilient control strategies viable for a highly digitalized smart grid. Potentially, it focuses on cyber-resilient and intelligent LFC design to ensure a secure, stable, and sustainable operational mode of interconnected next-generation power systems.

CRediT Author Contribution Statement

Satheeshkumar R: Conceptualization, Writing - Original draft, Writing-Review & editing. **Jagatheesan K.:** Formal analysis, Writing - Review & editing. **Lenin V R:** Supervision. **Kanendra Naidu:** Investigation, Validation. **Anand B:** Investigation, Validation. All authors have read and agreed to the published version of the manuscript.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data Availability Statement

No data were generated or analyzed during the current study. Therefore, data sharing is not applicable to this article.

Conflict of Interest

There is no conflict of interest.

Artificial Intelligence (AI) Use Disclosure

The authors declare that artificial intelligence (AI)-assisted tools were used only for language refinement, grammar improvement, and manuscript structuring purposes during the preparation of this work. All technical content, experimental implementation, results, and interpretations were independently developed and verified by the authors.

Supporting Information

Not applicable

References

[1] M. Shafique, N. Iqbal, October. Load frequency resilient control of power system against delayed input cyber attack, In 2015 Symposium on Recent Advances in Electrical Engineering (RAEE), IEEE, 2015, 1-6, doi: 10.1109/RAEE.2015.7352757.

[2] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, Preventing time-delay switch attack on load frequency control in distributed power systems, *IEEE Transactions on Smart Grid*, 2015, **7**, 1176-1185, doi: 10.1109/TSG.2015.2503429.

[3] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, A. Mehbodniya, S. Sargolzaei, A novel technique for detection of time delay switch attack on load frequency control, *Intelligent Control and Automation*, 2015, **6**, 205, doi: 10.4236/ica.2015.64020.

[4] K. Rahimi, A. Parchure, V. Centeno, R. Broadwater, Effect of communication time-delay attacks on the performance of automatic generation control, Proceedings of the 2015 North American Power Symposium (NAPS), 2015, 1–6, doi: 10.1109/NAPS.2015.7335168

[5] J. Jarmakiewicz, K. Maślanka, K. Parobczak, Development of cyber security testbed for critical infrastructure, Proceedings of the 2015 International Conference on Military Communications and Information Systems (ICMCIS), 2015, 1–10, doi: 10.1109/ICMCIS.2

[6] C. Lopez, A. Sargolzaei, H. Santana, C. Huerta, Smart grid cyber security: An overview of threats and countermeasures, *Journal of Energy and Power Engineering*, 2015, **9,** doi: 10.17265/1934-8975/2015.07.005.

[7] P. Srikantha, D. Kundur, Denial of service attacks and mitigation for stability in cyber-enabled power grid, Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2015, 1–5, doi: 10.1109/ISGT.2015.7131827.

[8] R. J. Hamidi, H. Khodabandehlou, H. Livani, M. S. Fadali, Application of distributed compressive sensing to power system state estimation, Proceedings of the 2015 North American Power Symposium (NAPS), 2015, 1–6, doi: 10.1109/NAPS.2015.7335114.

[9] D. Deka, R. Baldick, S. Vishwanath, Optimal data attacks on power grids: Leveraging detection & measurement jamming, Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2015, 392–397, doi: 10.1109/SmartGridComm.2015.7436332.

[10] D. Alahakoon, X. Yu, Smart electricity meter data intelligence for future energy systems: A survey, *IEEE Transactions on Industrial Informatics*, 2015, **12**, 425–436, doi: 10.1109/TII.2015.2414355.

[11] G. Franzè, F. Tedesco, A. Casavola, E. Garone, A leader-follower architecture for load frequency control purposes against cyber attacks in power grids-Part II, Proceedings of the 2016 IEEE 55th Conference on Decision and Control (CDC), 2016, 5134–5139, doi: 10.1109/CDC.2016.7799054.

[12] H. He, J. Yan, Cyber-physical attacks and defences in the smart grid: A survey, *IET Cyber-Physical Systems: Theory & Applications*, 2016, **1**, 13–27, doi: 10.1049/iet-cps.2016.0019.

[13] Y. Yuan, F. Sun, H. Liu, Resilient control of cyber-physical systems against intelligent attacker: A hierarchal Stackelberg game approach, *International Journal of Systems Science*, 2016, **47**, 2067–2077, doi: 10.1080/00207721.2014.973467.

[14] A. Farraj, E. Hammad, D. Kundur, A cyber-physical control framework for transient stability in smart grids, *IEEE Transactions on Smart Grid*, 2016, **9**(2), 1205–1215, doi: 10.1109/TSG.2016.2581588.

[15] Y. Liu, S. Hu, A. Y. Zomaya, The hierarchical smart home cyberattack detection considering power overloading and frequency disturbance, *IEEE Transactions on Industrial Informatics*, 2016, **12**(5), 1973–1983, doi: 10.1109/TII.2016.2591911.

[16] A. Razaq, H. Tianfield, B. Pranggono, H. Yue, Simulating smart grid cyber security, *Smart Grid: Networking, Data Management and Business Models*, 2016, **1**, 97–116, doi: 10.1201/b19664-5.

[17] Z. A. Khan, D. Jayaweera, Planning and operational challenges in a smart grid, *Smart Power Systems and Renewable Energy System Integration*, 2016, 153–177, doi: 10.1007/978-3-319-30427-4_9.

[18] E. Korkmaz, A. Dolgikh, M. Davis, V. Skormin, ICS security testbed with delay attack case study, Proceedings of the MILCOM 2016 IEEE Military Communications Conference, 2016, 283–288, doi: 10.1109/MILCOM.2016.7795340.

[19] A. Abbaspour, K. K. Yen, S. Noei, A. Sargolzaei, Detection of fault data injection attack on UAV using adaptive neural network, *Procedia Computer Science*, 2016, **95**, 193–200, doi: 10.1016/j.procs.2016.09.312.

[20] S. Noei, A. Sargolzaei, A. Abbaspour, K. Yen, A

decision support system for improving resiliency of cooperative adaptive cruise control systems, *Procedia Computer Science*, 2016, **95**, 489–496, doi: 10.1016/j.procs.2016.09.326.

[21] C. Chen, K. Zhang, K. Yuan, L. Zhu, M. Qian, Novel detection scheme design considering cyber attacks on load frequency control, *IEEE Transactions on Industrial Informatics*, 2017, **14**(5), 1932–1941, doi: 10.1109/TII.2017.2765313.

[22] Y. Shen, M. Fei, D. Du, W. Zhang, S. Stanković, A. Rakić, Cyber security against denial-of-service attacks on load frequency control of multi-area power systems, *Proceedings of the International Conference on Intelligent Computing for Sustainable Energy and Environment*, 2017, 439–449, doi: 10.1007/978-981-10-6364-0_44.

[23] Y. Wu, Z. Wei, J. Weng, X. Li, R. H. Deng, Resonance attacks on load frequency control of smart grids, *IEEE Transactions on Smart Grid*, 2017, **9**, 4490–4502, doi: 10.1109/TSG.2017.2661307.

[24] A. Abbaspour, A. Sargolzaei, K. Yen, Detection of false data injection attack on load frequency control in distributed power systems, Proceedings of the 2017 North American Power Symposium (NAPS), 2017, 1–6, doi: 10.1109/NAPS.2017.8107333.

[25] S. Poudel, Z. Ni, N. Malla, Real-time cyber physical system testbed for power system security and control, *International Journal of Electrical Power & Energy Systems*, 2017, **90**, 124–133, doi: 10.1016/j.ijepes.2017.01.016.

[26] J. Jarmakiewicz, K. Parobczak, K. Maślanka, Cybersecurity protection for power grid control infrastructures, *International Journal of Critical Infrastructure Protection*, 2017, **18**, 20–33, doi: 10.1016/j.ijcip.2017.07.002.

[27] E. Kontouras, A. Tzes, L. Dritsas, Impact analysis of a bias injection cyber-attack on a power plant, *IFAC-PapersOnLine*, 2017, **50**, 11094–11099, doi: 10.1016/j.ifacol.2017.08.2493.

[28] W. Liao, S. Salinas, M. Li, P. Li, K. A. Loparo, Cascading failure attacks in the power system: A stochastic game perspective, *IEEE Internet of Things Journal*, 2017, **4**, 2247–2259, doi: 10.1109/JIOT.2017.2761353.

[29] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, B. Carbunar, Resilient design of networked control systems under time delay switch attacks, application in smart grid, *IEEE Access*, 2017, **5**, 15901–15912, doi: 10.1109/ACCESS.2017.2731780.

[30] A. Farraj, E. Hammad, D. Kundur, On the impact of cyber attacks on data integrity in storage-based transient stability control, *IEEE Transactions on Industrial Informatics*, 2017, **13**, 3322–3333, doi: 10.1109/TII.2017.2720679.

[31] J. Li, X. Liu, X. Su, Sliding mode observer-based load frequency control of multi-area power systems under delayed inputs attack, Proceedings of the 2018 Chinese Control and Decision Conference, 2018, 3716–3720, doi: 10.1109/CCDC.2018.8407768.

[32] S. Mehrdad, S. Mousavian, G. Madraki, Y. Dvorkin, Cyber-physical resilience of electrical power systems against malicious attacks: A review, *Current Sustainable/Renewable Energy Reports*, 2018, **5**, 14–22, doi: 10.1007/s40518-018-0094-8.

33] H. H. Alhelou, M. E. Hamedani-Golshan, R. Zamani, E. Heydarian-Forushani, P. Siano, Challenges and opportunities of load frequency control in conventional, modern and future smart power systems: A comprehensive review, *Energies*, 2018, **11**(10), 2497, doi: 10.3390/en11102497.

[34] A. Ameli, A. Hooshyar, E. F. El-Saadany, A. M. Youssef, Attack detection and identification for automatic generation control systems, *IEEE Transactions on Power Systems*, 2018, **33**, 4760–4774, doi: 10.1109/TPWRS.2018.2810161.

[35] E. Kontouras, A. Tzes, L. Dritsas, Set-theoretic detection of data corruption attacks on cyber physical power systems, *Journal of Modern Power Systems and Clean Energy*, 2018, **6**, 872–886, doi: 10.1007/s40565-018-0452-y.

[36] A. Ameli, A. Hooshyar, A. H. Yazdavar, E. F. El-Saadany, A. Youssef, Attack detection for load frequency control systems using stochastic unknown input estimators, *IEEE Transactions on Information Forensics and Security*, 2018, **13**, 2575–2590, doi: 10.1109/TIFS.2018.2824253.

[37] A. Abbaspour, A. Sargolzaei, K. K. Yen, A neural network based resilient control design for distributed power systems under faults and attacks, Proceedings of the 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), 2018, 1–6, doi: 10.1109/EEEIC.2018.8494626.

[38] S. Gholami, S. Saha, M. Aldeen, Fault tolerant control of electronically coupled distributed energy resources in microgrid systems, *International Journal of Electrical Power & Energy Systems*, 2018, **95**, 327–340, doi: 10.1016/j.ijepes.2017.08.024.

[39] A. Sargolzaei, A. Abbaspour, M. A. Al Faruque, A. Salah Eddin, K. Yen, Security challenges of networked control systems, *Sustainable Interdependent Networks: From Theory to Application*, 2018, 77–95, doi: 10.1007/978-3-319-74412-4_6.

[40] A. Liu, L. Bai, Distributed model predictive control for wide area measurement power systems under

malicious attacks, *IET Cyber-Physical Systems: Theory & Applications*, 2018, **3**, 111–118, doi: 10.1049/iet-cps.2017.0056.

[41] H. H. Alhelou, M. E. H. Golshan, N. D. Hatziargyriou, A decentralized functional observer based optimal LFC considering unknown inputs, uncertainties, and cyber-attacks, *IEEE Transactions on Power Systems*, 2019, **34**, 4408–4417, doi: 10.1109/TPWRS.2019.2916558.

[42] Y. Shen, M. Fei, D. Du, Cyber security study for power systems under denial-of-service attacks, *Transactions of the Institute of Measurement and Control*, 2019, **41**, 1600–1614, doi: 10.1177/0142331217709528.

[43] J. Liu, Y. Gu, L. Zha, Y. Liu, J. Cao, Event-triggered H∞ load frequency control for multiarea power systems under hybrid cyber attacks, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019, **49**(8), 1665–1678, doi: 10.1109/TSMC.2019.2895060.

[44] X. Zhou, Z. Gu, F. Yang, Resilient event-triggered output feedback control for load frequency control systems subject to cyber attacks, *IEEE Access*, 2019, **7**, 58951–58958, doi: 10.1109/ACCESS.2019.2914492.

[45] W. Bi, K. Zhang, Y. Li, K. Yuan, Y. Wang, Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis, *IEEE Systems Journal*, 2019, **13**, 2859–2868, doi: 10.1109/JSYST.2019.2911869.

[46] W. Bi, K. Zhang, K. Yuan, Y. Wang, C. Chen, K. Wang, Observer-based attack detection and mitigation for load frequency control system, Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), 2019, 1–5, doi: 10.1109/PESGM40551.2019.8973575.

[47] H. H. Alhelou, M. E. H. Golshan, N. D. Hatziargyriou, Deterministic dynamic state estimation-based optimal LFC for interconnected power systems using unknown input observer, *IEEE Transactions on Smart Grid*, 2019, **11**, 1582–1592, doi: 10.1109/TSG.2019.2940199.

[48] Y. Li, P. Zhang, L. Ma, Denial of service attack and defense method on load frequency control system, *Journal of the Franklin Institute*, 2019, **356**, 8625–8645, doi: 10.1016/j.jfranklin.2019.08.036.

[49] Q. Wang, W. Tai, Y. Tang, H. Zhu, M. Zhang, D. Zhou, Coordinated defense of distributed denial of service attacks against the multi-area load frequency control services, *Energies*, 2019, **12**, 2493, doi: 10.3390/en12132493.

[50] W. Bi, C. Chen, K. Zhang, Optimal strategy of attack-defense interaction over load frequency control considering incomplete information, *IEEE Access*, 2019, **7**, 75342–75349, doi: 10.1109/ACCESS.2019.2921603.

[51] Y. Liu, Y. Chen, M. Li, Dynamic event-based model predictive load frequency control for power systems under cyber attacks, *IEEE Transactions on Smart Grid*, 2020, **12**, 715–725, doi: 10.1109/TSG.2020.3022094.

[52] K. Pan, J. Dong, E. Rakhshani, P. Palensky, Effects of cyber attacks on AC and high-voltage DC interconnected power systems with emulated inertia, *Energies*, 2020, **13**(21), 5583, doi: 10.3390/en13215583.

[53] D. K. Panda, S. Das, S. Townley, Toward a more renewable energy-based LFC under random packet transmissions and delays with stochastic generation and demand, *IEEE Transactions on Automation Science and Engineering*, 2020, **19**, 1217–1232, doi: 10.1109/TASE.2020.3042570.

[54] C. Chen, K. Zhang, M. Ni, Y. Wang, Cyber-attack-tolerant frequency control of power systems, *Journal of Modern Power Systems and Clean Energy*, 2020, **9**, 307–315, doi: 10.35833/MPCE.2019.000185.

[55] C. Chen, M. Cui, X. Fang, B. Ren, Y. Chen, Load altering attack-tolerant defense strategy for load frequency control system, *Applied Energy*, 2020, **280**, 116015, doi: 10.1016/j.apenergy.2020.116015.

[56] S. Prasad, Counteractive control against cyber-attack uncertainties on frequency regulation in the power system, *IET Cyber-Physical Systems: Theory & Applications*, 2020, **5**, 394–408, doi: 10.1049/iet-cps.2019.0097.

[57] E. Tian, C. Peng, Memory-based event-triggering H∞ load frequency control for power systems under deception attacks, *IEEE Transactions on Cybernetics*, 2020, **50**, 4610–4618, doi: 10.1109/TCYB.2020.2972384.

[58] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, A. Sargolzaei, Resilient frequency control design for microgrids under false data injection, *IEEE Transactions on Industrial Electronics*, 2020, **68**(3), 2151–2162, doi: 10.1109/TIE.2020.2975494.

[59] K. S. Xiahou, Y. Liu, Q. H. Wu, Robust load frequency control of power systems against random time-delay attacks, *IEEE Transactions on Smart Grid*, 2020, **12**(1), 909–911, doi: 10.1109/TSG.2020.3018635.

[60] Z. Hu, S. Liu, W. Luo, L. Wu, Credibility-based secure distributed load frequency control for power systems under false data injection attacks, *IET Generation, Transmission & Distribution*, 2020, **14**(17), 3498–3507, doi: 10.1049/iet-gtd.2020.0389.

[61] S. Saxena, S. Bhatia, R. Gupta, Cybersecurity analysis of load frequency control in power systems: A survey, *Designs*, 2021, **5**, 52, doi: 10.3390/designs5030052.

[62] S. Yan, Z. Gu, J. H. Park, Memory-event-triggered H∞ load frequency control of multi-area power systems with cyber-attacks and communication delays, *IEEE Transactions on Network Science and Engineering*, 2021, **8**, 1571–1583, doi: 10.1109/TNSE.2021.3064933.

[63] Y. Zhang, T. Yang, Z. Tang, Active fault-tolerant control for load frequency control in multi-area power systems with physical faults and cyber attacks, *International Transactions on Electrical Energy Systems*, 2021, **31**, e12906, doi: 10.1002/2050-7038.12906.

[64] R. Zhu, C. Huang, S. Deng, Y. Li, Detection of false data injection attacks based on Kalman filter and controller design in power system LFC, *Journal of Physics: Conference Series*, 2021, **1861**, 012120, doi: 10.1088/1742-6596/1861/1/012120.

[65] W. Bi, K. Zhang, C. Chen, Cyber attack detection scheme for a load frequency control system based on dual-source data of compromised variables, *Applied Sciences*, 2021, **11**, 1584, doi: 10.3390/app11041584.

[66] F. R. Badal, Z. Nayem, S. K. Sarker, D. Datta, S. Rahman Fahim, S. M. Muyeen, M. R. Islam Sheikh, S. K. Das, A novel intrusion mitigation unit for interconnected power systems in frequency regulation to enhance cybersecurity, *Energies*, 2021, **14**, 1401, doi: 10.3390/en14051401.

[67] X. C. ShangGuan, Y. He, C. K. Zhang, L. Jin, L. Jiang, M. Wu, J. W. Spencer, Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks, *Control Engineering Practice*, 2021, **107**, 104678, doi: 10.1016/j.conengprac.2020.104678.

[68] A. Kazemy, M. Hajatipour, Event-triggered load frequency control of Markovian jump interconnected power systems under denial-of-service attacks, *International Journal of Electrical Power & Energy Systems*, 2021, **133**, 107250, doi: 10.1016/j.ijepes.2021.107250.

[69] Z. Hu, S. Liu, W. Luo, L. Wu, Intrusion-detector-dependent distributed economic model predictive control for load frequency regulation with PEVs under cyber attacks, *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2021, **68**, 3857–3868, doi: 10.1109/TCSI.2021.3089770.

[70] N. Vafamand, M. M. Arefi, M. H. Asemani, T. Dragičević, Decentralized robust disturbance-observer based LFC of interconnected systems, *IEEE Transactions on Industrial Electronics*, 2021, **69**, 4814–4823, doi: 10.1109/TIE.2021.3078352.

[71] G. Zhang, J. Li, O. Bamisile, Y. Xing, D. Cai, Q. Huang, An H∞ load frequency control scheme for multi-area power system under cyber-attacks and time-varying delays, *IEEE Transactions on Power Systems*, 2022, **38**(2), 1336–1349, doi: 10.1109/TPWRS.2022.3171101.

[72] M. Zhang, S. Dong, P. Shi, G. Chen, X. Guan, Distributed observer-based event-triggered load frequency control of multiarea power systems under cyber attacks, *IEEE Transactions on Automation Science and Engineering*, 2022, **20**, 2435–2444, doi: 10.1109/TASE.2022.3208016.

[73] K. D. Lu, Z. G. Wu, Resilient event-triggered load frequency control for cyber-physical power systems under DoS attacks, *IEEE Transactions on Power Systems*, 2022, **38**, 5302–5313, doi: 10.1109/TPWRS.2022.3229667.

[74] P. Chen, D. Zhang, L. Yu, H. Yan, Dynamic event-triggered output feedback control for load frequency control in power systems with multiple cyber attacks, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, **52**, 6246–6258, doi: 10.1109/TSMC.2022.3143903.

[75] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, K. Li, A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems, *Journal of Modern Power Systems and Clean Energy*, 2022, **11**, 727–743, doi: 10.35833/MPCE.2021.000604.

[76] X. Zhao, Z. Ma, S. Li, S. Zou, Robust LFC of power systems with wind power under packet losses and communication delays, *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2022, **12**, 135–148, doi: 10.1109/JETCAS.2022.3141108.

[77] J. Wang, D. Wang, L. Su, J. H. Park, H. Shen, Dynamic event-triggered H∞ load frequency control for multi-area power systems subject to hybrid cyber attacks, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, **52**, 7787–7798, doi: 10.1109/TSMC.2022.3163261.

[78] S. Hu, X. Ge, Y. Li, X. Chen, X. Xie, D. Yue, Resilient load frequency control of multi-area power systems under DoS attacks, *IEEE Transactions on Information Forensics and Security*, 2022, **18**, 936–947, doi: 10.1109/TIFS.2022.3232961.

[79] X. Liu, D. Bai, S. Qiao, G. Xiao, S. S. Ge, Resilient and event-triggered sliding mode load frequency control for multi-area power systems under hybrid cyber attacks, *IET Control Theory & Applications*, 2022, **16**(17), 1739–1750, doi: 10.1049/cth2.12340.

[80] D. K. Mishra, P. K. Ray, L. Li, J. Zhang, M. J. Hossain, A. Mohanty, Resilient control-based frequency regulation scheme of isolated microgrids considering cyber attack and parameter uncertainties, *Applied Energy*, 2022, **306**, 118054, doi: 10.1016/j.apenergy.2021.118054.

[81] M. Bakeer, A. Bakeer, G. Magdy, M. M. Aly, A new cyber-security approach for load frequency control of hybrid interconnected renewable power systems, *Journal of Cleaner Production*, 2023, **425**, 138866, doi: 10.1016/j.jclepro.2023.138866.

[82] A. D. Syrmakesis, H. H. Alhelou, N. D. Hatziargyriou, A novel cyberattack-resilient frequency control method for interconnected power systems using SMO-based attack estimation, *IEEE Transactions on Power Systems*, 2023, **39**, 5672–5686, doi: 10.1109/TPWRS.2023.3340744.

[83] X. Lv, Y. Sun, V. Dinavahi, X. Zhao, F. Qiao, Robust networked power system load frequency control against hybrid cyber attack, *IET Smart Grid*, 2023, **6**, 391–402, doi: 10.1049/stg2.12107.

[84] A. Abazari, M. M. Soleymani, M. Zadsar, M. Ghafouri, C. Assi, M. Shafie-Khah, Online recursive detection and adaptive fuzzy mitigation of cyber-physical attacks targeting topology of IMG: An LFC case study, *IEEE Transactions on Smart Grid*, 2023, **15**, 2129–2145, doi: 10.1109/TSG.2023.3304537.

[85] A. M. Mohan, N. Meskin, H. Mehrjerdi, LQG-based virtual inertial control of islanded microgrid load frequency control and DoS attack vulnerability analysis, *IEEE Access*, 2023, **11**, 42160–42179, doi: 10.1109/ACCESS.2023.3271012.

[86] J. Yang, Q. Zhong, K. Shi, S. Zhong, Distributed coordination LFC approach for interconnected power systems under detection and compensation mechanism targeting DoS attacks, *IEEE Transactions on Industrial Informatics*, 2023, **19**, 11008–11018, doi: 10.1109/TII.2023.3242587.

[87] D. Lakshmi, N. Nagpal, S. Chandrasekaran, A quantum-based approach for offensive security against cyber attacks in electrical infrastructure, *Applied Soft Computing*, 2023, **136**, 110071, doi: 10.1016/j.asoc.2023.110071.

[88] D. Boopathi, K. Jagatheesan, R. Satheeshkumar, B. Anand, J. Jaya, Automatic frequency control for interlinked DSTS power grid using Dragonfly algorithm tuned PID controller, Proceedings of the 2023 IEEE 20th India Council International Conference (INDICON), 2023, 1161–1167, doi:10.1109/INDICON59947.2023.10440739.

[89] R. Satheeshkumar, K. Jagatheesan, D. Boopathi, K. R. C. Prusty, K. Naidu, Frequency management of an interconnected power system using ant colony optimization technique enhanced PI controller, Proceedings of the International Conference on Data Analytics and Insights, 2023, 505–514, doi: 10.1007/978-981-99-3878-0_43.

[90] L. F. Ribas Monteiro, Y. R. Rodrigues, A. C. Zambroni de Souza, Cybersecurity in cyber–physical power systems, *Energies*, 2023, **16**(12), 4556, doi: 10.3390/en16124556.

[91] D. Boopathi, K. Jagatheesan, S. Samanta, B. Anand, R. Satheeshkumar, Energy storage units for frequency management in nuclear generators-based power system, *Energy Storage Technologies in Grid Modernization*, 2023, 105–134, doi: 10.1002/9781119872146.ch4.

[92] A. D. Syrmakesis, H. H. Alhelou, N. D. Hatziargyriou, A novel cyber resilience method for frequency control in power systems considering nonlinearities and practical challenges, *IEEE Transactions on Industry Applications*, 2023, **60**, 2176–2190, doi: 10.1109/TIA.2023.3332702.

[93] D. Boopathi, K. Jagatheesan, B. Anand, J. Jaya, R. Satheeshkumar, Investigation of a microgrid power system for frequency regulation by implementing ant colony optimization technique optimized secondary controller, *Renewable Energy Optimization, Planning and Control*, 2023, 229–236, doi: 10.1007/978-981-19-8963-6_22.

[94] S. Yıldız, B. Yildirim, M. T. Özdemir, Enhancing load frequency control and cybersecurity in renewable energy microgrids: A fuel cell-based solution with non-integer control under cyber-attack, *International Journal of Hydrogen Energy*, 2024, **75**, 438–449, doi: 10.1016/j.ijhydene.2024.02.145.

[95] M. Ranjan, R. Shankar, U. Raj, S. Kumar, J. Kumar, Cyber-attack and defense method for load frequency control in smart grid systems with electric vehicles, *Optimal Control Applications and Methods*, 2024, **45**(6), 2722–2747, doi: 10.1002/oca.3184.

[96] D. Wu, F. Guo, Z. Yao, D. Zhu, Z. Zhang, L. Li, X. Du, J. Zhang, Enhancing reliability and performance of load frequency control in aging multi-area power systems under cyber-attacks, *Applied Sciences*, 2024, **14**(19), 8631, doi: 10.3390/app14198631.

[97] A. Saxena, R. Shankar, C. Kumar, S. K. Parida, A resilient frequency regulation for enhancing power system security against hybrid cyber-attacks, *IEEE Transactions on Industry Applications*, 2024, **60**, 4583–4597, doi: 10.1109/TIA.2024.3354228.

[98] X. Jia, T. Lv, B. Li, H. Li, B. Liu, Decentralized secure load frequency control for multi-area power systems under complex cyber attacks, *IEEE Transactions on Smart Grid*, 2024, **15**, 5043–5054, doi: 10.1109/TSG.2024.3379411.

[99] A. D. Syrmakesis, C. Alcaraz, N. D. Hatziargyriou, DAR-LFC: A data-driven attack recovery mechanism for load frequency control, *International Journal of Critical Infrastructure Protection*, 2024, **45**, 100678, doi: 10.1016/j.ijcip.2024.100678.

[100] I. Semertzis, A. Ştefanov, A. Presekal, B. Kruimer, J. L. R. Torres, P. Palensky, Power system stability analysis from cyber attacks perspective, *IEEE Access*, 2024, **12**, 113008–113035, doi: 10.1109/ACCESS.2024.3443061.

[101] G. Tian, F. Wang, Data-driven load frequency control for multi-area power system based on switching method under cyber attacks, *Algorithms*, 2024, **17**, 233, doi: 10.3390/a17060233.

[102] S. Oshnoei, M. R. Aghamohammadi, M. H. Khooban,

Smart frequency control of cyber-physical power system under false data injection attacks, *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2024, **71**, 5582–5595, doi: 10.1109/TCSI.2024.3396703.

[103] S. R. Fahim, R. Atat, C. Kececi, A. Takiddin, M. Ismail, K. R. Davis, E. Serpedin, Cyberattack aware load frequency control in power systems, Proceedings of the 2024 58th Asilomar Conference on Signals, Systems, and Computers, 2024, 1058–1062, doi: 10.1109/IEEECONF60004.2024.10942756.

[104] S. Hu, X. Ge, W. Zhang, D. Yue, DoS-resilient load frequency control of multi-area power systems: An attack-parameter-dependent approach, *IEEE Transactions on Information Forensics and Security*, 2024, **19**, 3423–3434, doi: 10.1109/TIFS.2024.3361159.

[105] A. Y. Abdelaziz, F. K. Abo-Elyousr, Blockchain-based approach for load frequency control of smart grids under denial-of-service attacks, *Computers and Electrical Engineering*, 2024, **116**, 109150, doi: 10.1016/j.compeleceng.2024.109150.

[106] S. I. Abouzeid, Y. Chen, M. Zaery, M. A. Abido, A. Raza, E. H. Abdelhameed, Load frequency control based on reinforcement learning for microgrids under false data attacks, *Computers and Electrical Engineering*, 2025, **123**, 110093, doi: 10.1016/j.compeleceng.2025.110093.

[107] H. Zhang, Z. Wang, J. Zhang, Secure load frequency control of cyber-physical power systems under cyber attacks and delays, *IEEE Internet of Things Journal*, 2025, doi: 10.1109/JIOT.2025.3588844.

[108] V. Kapil, S. Prasad, Data integrity cyber-attack mitigation using linear quadratic regulator-based load frequency control in hybrid power system, *International Journal of Emerging Electric Power Systems*, 2025, **26**(4), 669–679, doi: 10.1515/ijeeps-2024-0102.

[109] U. Raj, R. Shankar, S. Rani, M. Ranjan, Enhanced load frequency regulation in cyberattack triggered grids with renewable energy and electric vehicles, *Electrical Engineering*, 2025, **107**, 7363–7381, doi: 10.1007/s00202-024-02925-4.

[110] D. K. Gupta, A. V. Jha, P. Sahu, S. Mohapatra, G. Dei, B. Appasani, A. Srinivasulu, P. Nsengiyumva, Load frequency control analysis of cyber-physical power system with denial-of-service attack in deregulated power markets, *Smart Grids and Sustainable Energy*, 2025, **10**, 22, doi: 10.1007/s40866-025-00250-8.

[111] S. N. Sahu, R. K. Khadanga, D. Das, Y. Arya, S. Panda, S. Padhy, P. R. Sahu, LFC of distributed power generation system under different cyberattacks utilizing a new mZOA-based hFPD-PI+FP control strategy, *Sustainable Computing: Informatics and Systems*, 2025, 101282, doi: 10.1016/j.suscom.2025.101282.

[112] D. Xu, Y. Liu, J. H. Park, Observer-based fuzzy event-triggered LFC for wind power systems under multiple cyberattacks via an NN approximation approach, *IEEE Transactions on Automation Science and Engineering*, 2025, doi: 10.1109/TASE.2025.3584950.

[113] P. Aryan, G. L. Raja, U. Mehta, T. R. Chelliah, U. R. Muduli, A resilient tri-parametric fractional frequency control for cybersecurity threats amid latency, *IEEE Transactions on Industry Applications*, 2025, doi: 10.1109/TIA.2025.3546173.

[114] S. Yang, K. W. Lao, H. Hui, J. Su, S. Wang, Secure frequency regulation in power system: A comprehensive defense strategy against FDI, DoS, and latency cyber-attacks, *Applied Energy*, 2025, **379**, 124772, doi: 10.1016/j.apenergy.2024.124772.

[115] R. Singh, R. Kumar, U. Raj, R. Shankar, Robust load frequency control in cyber-vulnerable smart grids with renewable integration, *Energies*, 2025, **18**, 2899, doi: 10.3390/en18112899.

[116] X. Wang, J. H. Park, J. Wang, D. Zhang, Neural network-based adaptive LFC approach for multi-area power systems vulnerable to hybrid attacks, *IEEE Transactions on Smart Grid*, 2026, doi: 10.1109/TSG.2026.3653032.

[117] D. O. Olasehinde, O. Bamisile, C. J. Ejiyi, G. Zhang, D. Cai, J. Li, L. Wei, Q. Huang, Cybersecurity in cyber-physical power systems: Analyzing vulnerabilities, threats, and control structures, *Cluster Computing*, 2026, **29**, 133, doi: 10.1007/s10586-025-05894-w.

[118] R. Satheeshkumar, K. Jagatheesan, D. Boopathi, K. Naidu, Impact of optimization algorithms with energy storage systems in frequency management of standalone/interconnected power systems, *Nature-Inspired Approaches to Engineering and Healthcare Solutions*, 2026, 21–39, doi: 10.1007/978-3-032-08596-2_2.

[119] M. Naz, K. N. Paracha, M. M. Gulzar, A. R. Bhatti, R. Liaqat, Cyberattack resilient load frequency control in renewable integrated power system considering controlled energy storage, *Journal of Energy Storage*, 2026, **141**, 119157, doi: 10.1016/j.est.2025.119157.

[120] G. Liu, C. Zhang, F. Li, S. Li, X. Liu, Secure load frequency control for power systems under round-robin protocol: A quantized MPC strategy, *ISA Transactions*, 2026, doi: 10.1016/j.isatra.2025.12.054.

[121] Q. Wan, Y. W. Wang, X. K. Liu, A. D. Syrmakesis, N. D. Hatziargyriou, Dynamic self-triggered load frequency control for multi-area power systems under non-ideal communication environments, *IEEE Transactions on Smart Grid*, 2026, doi: 10.1109/TSG.2025.3649018.

[122] X. Wang, K. Shi, M. Zhu, H. Yan, Y. Sun, X. Cai, Integral re-averaging control strategy load frequency control for T-S fuzzy reaction-diffusion power system under cyberattacks, *International Journal of Robust and Nonlinear Control*, 2026, **36**(3), 1245–1257, doi: 10.1002/rnc.70170.

[123] M. Ramesh, A. K. Yadav, P. K. Pathak, Optimal robust PI-type load frequency control of renewable penetrated power system with delayed electric vehicles aggregators, *International Journal of Information Technology*, 2026, **18**, 645-654, doi: 10.1007/s41870-025-02798-1.

[124] N. A. Nagem, M. Aly, E. A. Mohamed, A. F. Fareed, D. M. Alqahtani, W. A. Hafez, Cascaded optimized fractional controller for green hydrogen-based microgrids with mitigating false data injection attacks, *Fractal and Fractional*, 2026, **10**, 55, doi: 10.3390/fractalfract10010055.