Resilient Net Zero: An Overview on Secure Control Methods for Networked Microgrids

Jinhui Wu, Fanghong Guo, Fuwen Yang,

Changyun Wen, Mo-Yuen Chow, and Francesca Boem

Developing efficient and reliable Renewable Energy Sources (RESs) to reduce the exploitation of traditional power generation is essential for achieving Net Zero Strategy (NZS) in a sustainable and affordable way. However, due to their nature, many RESs are geographically distributed; for instance, wind power stations are typically built along coastlines to harness sea wind energy, and photovoltaic power panels maybe distributed over residential buildings. This geographical distribution naturally leads to the term: Distributed Energy Resources (DERs). To efficiently utilize and coordinate DERs, the concept of Networked MicroGrids (NMGs) has emerged. Compared to single MicroGrids (MGs), NMGs can make fully use of DERs by enabling energy exchange and coordinated control among interconnected MGs. However, the interconnectedness also increases the complexity, uncertainty and potential vulnerability of NMGs to faults and cyber attacks. This review aims at summarizing the latest effective methodologies to secure the distributed secondary control layer, focusing on the impact of attacks on controllers, sensors, and communication channels. Additionally, this article outlines future research directions that could enhance

This work has been supported in part by the National Natural Science Foundation of China (Grant No. 62373328), in part by Zhejiang Provincial Natural Science Foundation of China (Grant No. LR25F030003), and in part by the Engineering and Physical Sciences Research Council, United Kingdom (Grant Reference: EP/W024411/1). For the purpose of open access, the author has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising. Corresponding author Fanghong Guo (email: fhguo@zjut.edu.cn)

Jinhui Wu and Changyun Wen are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: jinhui.wu@ntu.edu.sg; ecywen@ntu.edu.sg)

Fanghong Guo is with the Department of Automation, Zhejiang University of Technology, and also with Zhejiang Key Laboratory of Intelligent Perception and Control for Complex Systems, Hangzhou 310023, China. (email: fhguo@zjut.edu.cn).

Fuwen Yang is with the School of Engineering and Built Environment, Griffith University (Gold Coast), Southport, QLD 4222, Australia (e-mail: fuwen.yang@griffith.edu.au).

Mo-Yuen Chow is with the Shanghai Jiao Tong University, Shanghai, China (e-mail: moyuen.chow@sjtu.edu.cn).

Francesca Boem are the Department of Electronic and Electrical Engineering, University College London, London WC1E 6BT, UK. (e-mail: f.boem@ucl.ac.uk).

the reliability, resilience and flexibility of NMGs under cyber attacks, thereby guiding efforts to achieve a secure NZS.

I. NZS AND NMGS ON CYBER SECURITY

Due to the global climate change, there is an increasing call for governments, businesses and individuals to take measures to reduce carbon emissions and many countries have formulated relevant policies and targets to limit them. One forward-looking strategy that has obtained consent among many countries, the NZS, was proposed around 2020 by the U.S.A., U.K., Australia, China, etc, aiming at achieving net-zero emissions by approximately 2050, through reducing and offsetting greenhouse gas emissions. NZS is generally defined as achieving a balance between the greenhouse gas emissions produced and those removed from the atmosphere [1]. From the electrical engineering perspective, a key role in achieving Net Zero is played by the generation of green electricity from RESs. To achieve net-zero emissions by 2050, it is fundamental to considerably increase the generation from renewable sources, such as solar farms, wind turbines and hydroelectric plants, in conjunction with efficient battery energy management technologies and smart plugs [2]. Examples of such initiatives include the King Island Renewable Energy Project in Australia [3], the Isle of Eigg project in the U.K. [4], etc.

To efficiently manage RESs and deliver high-quality electricity while minimizing resource utilization in future power systems, MGs have been proposed and developed over the last decades [5]. However, the demand to improve energy efficiency, sustainability, reliability and resilience has accelerated the transformation of individual MGs. Connecting a number of autonomous MGs in a networked framework at the physical layer, the control layer, or both, is a promising strategic effort aimed at providing high-quality, eco-friendly power supply to local customers by leveraging shared DERs. This approach also allows to optimize the economic distribution of electrical energy resources to loads. As a result, the concept of NMGs is proposed in [6] for the first time by Sandia National Lab in the U.S.A. According to the definition, an NMG is composed of clusters of MGs that are geographically close or willing to share their privacy information by linking to distribution feeders with point of common coupling [7]. Compared to individual MGs, this connection allows to coordinate NMGs at a higher level to operate as an integral part of the grid, providing advanced ancillary services and offering multiple operational benefits. By harnessing the advantages of various distributed RESs, NMGs will become one of the most promising and powerful mechanisms to realize the NZS.

NMGs can enhance power system performance and reduce environmental impact primarily through the integration of distributed RESs. The efficient operation of these resources, however, relies on a large number of Internet of Things (IoT)-enabled devices such as smart plugs, smart sensors and communication interfaces. As a result, NMGs can be regarded as a typical Cyber-Physical System (CPS), where both the dynamic characteristics of physical devices and the advantages of networking are jointly considered to strengthen NMGs' monitoring and control capabilities [8], [9]. Nevertheless, this CPS framework significantly increases dependence on reliable communication networks, making NMGs vulnerable to cyber issues such as communication delay, data loss, malicious cyber intrusions, etc [10]. These factors introduce new uncertainties and security risks that challenge the stability and reliability of NMGs. White papers from the energy sector also emphasize that energy infrastructures are prime targets of cyber threats due to their potential for widespread disruption [11]. Addressing these security challenges is therefore essential for the realization of a secure NZS.

Similar to individual MGs, NMGs also adopt a hierarchical control architecture consisting of primary, secondary, and tertiary layers [12]. At the primary level, renewable power generation units are integrated into NMGs or the main grid by power electronics and typically operate in either grid-following or grid-forming modes. Due to the decreasing number of conventional synchronous generators driven by the traditional non-renewable energy resources and the inherent limitations of grid-following units (e.g., low short-circuit ratio), grid-forming inverters have become increasingly dominant for the system stability and reliability. They are usually controlled via droop control or virtual synchronous generator strategies to achieve power sharing while enhancing system reliability by increasing inertia [13]. Nevertheless, due to the communication-free property of the primary control, it inherently involves a trade-off between accurate power sharing and frequency/voltage restoration, which makes secondary control indispensable for the system recovery. Since the communication is inevitable in both the secondary and tertiary layers, the "cyber nature" of CPS in NMGs is most evident in these two layers. The tertiary layer mainly addresses economic dispatch and system-level optimization. One of the typical applications in this layer is the smart demand-side management (DSM) that involves machine learning-based optimization algorithms [14], [15]. They can exploit customer load profiles to generate scheduling strategies to regulate pricing and keep the load profile flat, particularly in NMGs with electric vehicle (EV) penetration, where the integration of grid-to-vehicle (G2V), vehicle-to-vehicle (V2V), and vehicle-to-grid (V2G) further enhances the system flexibility by charging and discharging EVs. Since the operating interval is relatively slow (in 15 minutes

to 1 hour) in the tertiary layer, it renders the impact on instantaneous stability less direct even though tertiary signals may also be exposed to abnormal data or cyber attacks to cause economic or reputation damage [16]. That is why in this paper we focus on the secondary control layer which remains the most vulnerable and reliability-critical part of NMGs as it governs real-time restoration of operational parameters while being highly exposed to cyber vulnerabilities.

The main objectives of secondary control can be divided into two categories: (i) Improving power quality and (ii) Restoring essential operational parameters such as frequency, voltage, and current sharing. On improving power quality, one typical issue is the total harmonic distortion (THD). To overcome this problem, inverters that equipped with harmonic compensation and reactive power support capabilities can contribute to both power quality enhancement and grid support [17]. From a system-level perspective, coordinated control strategies enable distributed compensation for power quality issues, allowing NMGs to share resources such as energy storage and filtering capabilities. These strategies can be integrated with RESs and DSM to ensure cleaner, more stable power delivery while progressing toward net-zero targets. Regarding essential operational parameters such as frequency, voltage, and current sharing, since disrupting them can cause the most direct and destructive form of cyber attacks, thus malicious manipulation at this layer can lead to severe frequency/voltage oscillations and power imbalance.

Based on the above analysis, securing the secondary control of NMGs to recover these critical parameters is a fundamental requirement for building trustworthy and reliable NZS from both electrical and control engineering perspectives. This paper reviews secure control methods for NMGs that ensure power delivery to loads even under cyberattacks. It examines various control strategies for restoring frequency and maintaining effective power distribution during denial-of-service (DoS), false data injection (FDI), and latency attacks at different cyber locations. Furthermore, it summarizes the types of attacks targeting the secondary layer of NMGs and their detrimental impacts on system resilience and reliability. By consolidating recent research and resilient control methodologies developed since the early 2010s [18], [19], this work aims to support scholars and practitioners in advancing the secure integration of RESs-an essential step toward a reliable and sustainable net-zero energy future. Although achieving 100% renewable generation in safety-critical infrastructures such as power grids may not be immediately feasible, the analysis presented here remains valid in scenarios combining renewable and conventional generation.

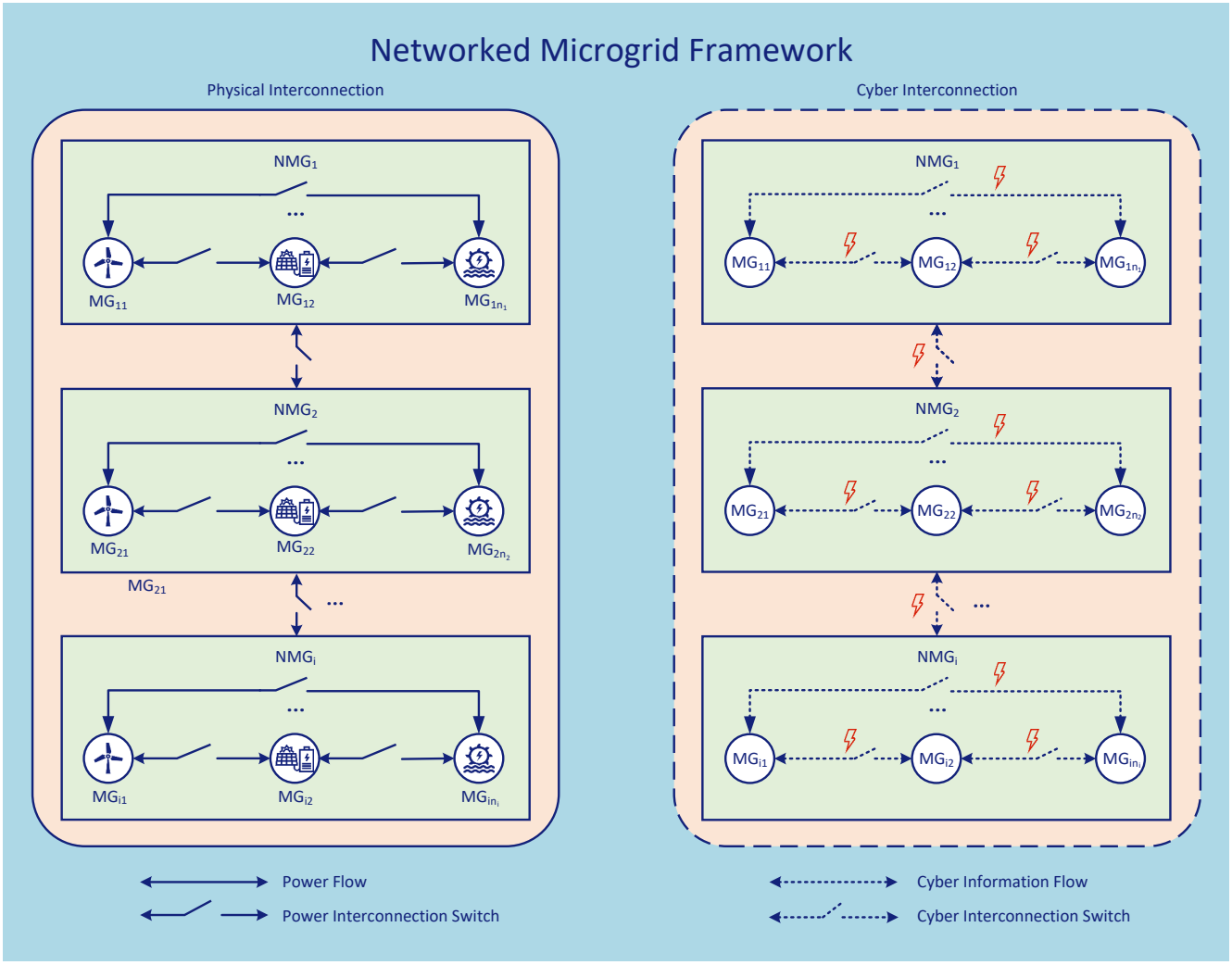


Fig. 1. Physical and cyber framework of NMGs. This figure illustrates the composition of NMGs both in physical and cyber connections. The red lightning symbols indicate possible attacks on interconnected NMGs.

II. Cyber Issues for NMGs

A scheme of NMGs is shown in Fig. 1, where a number of MGs are connected with each other, both in the physical and cyber layers, based on their geographic locations and privacy permissions. It is worth noting that such networked frameworks are vulnerable to cyber attacks both within each NMG and among NMGs. When attacks occur between MGs within an NMG system, they may hinder NMGs' operational abilities in several aspects. For instance, attacks may prevent NMGs from achieving accurate frequency/voltage restoration. Additionally, attacks can also lead to complications in power distribution among the various distributed generators (DGs) [7]. Once attacks take place between one NMG and another, the overall power distribution among the NMGs may not adhere to the most optimal strategy prescribed by tertiary layer objectives. Consequently, NMGs may not be able to operate in the most energy-efficient manner under cyber attacks. Besides, the leaked data may be maliciously exploited by attackers

to infer the information and structure of neighboring NMGs or to gain illegal economic benefits, which may further lead to privacy leakage and abnormal operation of the whole NMG system [20]. Therefore, cybersecurity concerns will significantly impede progress towards the NZS and compromise its security and feasibility.

Data security is a fundamental aspect of NMGs reliability. To realize a secure NZS, data security in NMGs should be discussed and guaranteed as a priority. Based on the different properties of data, data security can be classified according to the timeliness, availability and accuracy [21]. The description of each property is summarized in Table I. Attackers will interfere with the secondary control of NMGs based on these three factors that affect the data reliability. Common attacks in NMGs include DoS attacks, latency attacks and FDI attacks [22]. As shown in Fig. 2, the DoS attacks typically compromise data timeliness and availability by overwhelming the target with a flood of internet traffic or sending malicious information that triggers crashes in NMGs. The main goal of DoS attacks is to deny legitimate and accurate data access to NMGs, thereby disrupting the normal functioning of NMGs. Another attack harmful to the data timeliness and availability of NMGs is the latency attack. Rather than focusing on directly making data unavailable so as to damage or disable NMGs, the latency attacks aim to introduce delays or inconsistencies in the timing of processes, communications, or data flows. This can lead to various adverse effects, including decreased NMG performance, NMG data corruption, and synchronization issues, etc. In addition to apparently undermining the desired NMG performance by the disruption to the timeliness and availability of data, FDI attacks allocate additional resources to disguise their malicious intent and destroy the data accuracy. Therefore, the FDI attacks can possess sophisticated capabilities for evasion, employing various methods of covertness and stealth across different attack prototypes. The features of DoS, FDI and latency attacks are summarized in Table II. All these attacks targeting the secondary layer control, have physical implications, and can create a physical damage to the NMG, or even the environment; that is why they can also be defined as Cyber-Physical attacks.

III. Detection methods for cyber security

Before summarizing different ways of dealing with cyber attacks, Fig. 3 presents the overall cyber-security framework in NMGs. When an attack targets an NMG and its cyber-layer, it encounters a first information defense layer protected by information defense technologies, including pseudo-random algorithms and other traditional cyber-security tools. Recently, several novel effective methods have been proposed at this layer to enhance cyber security for NMGs, such as the Paillier cryptosystem [23] and

TABLE I
RELIABILITY OF DATA

Property	Description	Impact
Data Timeliness	• The required communicated information among NMGs and within NMGs (sensor measurements, control inputs, etc.) is received with some delay	
Data Availability	• The required information is not available • Can be related to a non-efficient use of limited communication bandwidth	• Reduced system performance • Possible controller design failure • Possible NMG instability
Data Accuracy	• Communicated data is compromised, modified, replicated or with missing values	

differential privacy techniques [24]. Hence, one critical way to defend NMGs against cyber attacks is to encrypt and secure authentication. For more strategies on defending against network attacks and improving security at the information defense layer, readers are referred to comprehensive review articles such as [25].

However, the growing presence of smart sensors and smart plugs in modern NMGs expands the system's attack surface, increasing the likelihood that sophisticated adversaries may bypass encryption and other conventional cyber-security measures to compromise the control layer. At the same time, these devices also generate rich streams of measurement data that can be leveraged to enhance situational awareness and defense in the CPS framework. This dual role highlights the critical importance of developing powerful monitoring systems that can both exploit the data from smart devices and identify anomalies or cyber-attacks in the signals exchanged among interconnected NMGs, thereby mitigating potential threats before they escalate. Once abnormal behaviors are detected, the connection between the compromised NMGs and the rest of the network can be isolated based on their operational conditions, allowing the affected NMGs to operate independently and preventing the propagation of attacks to the entire system. The effectiveness

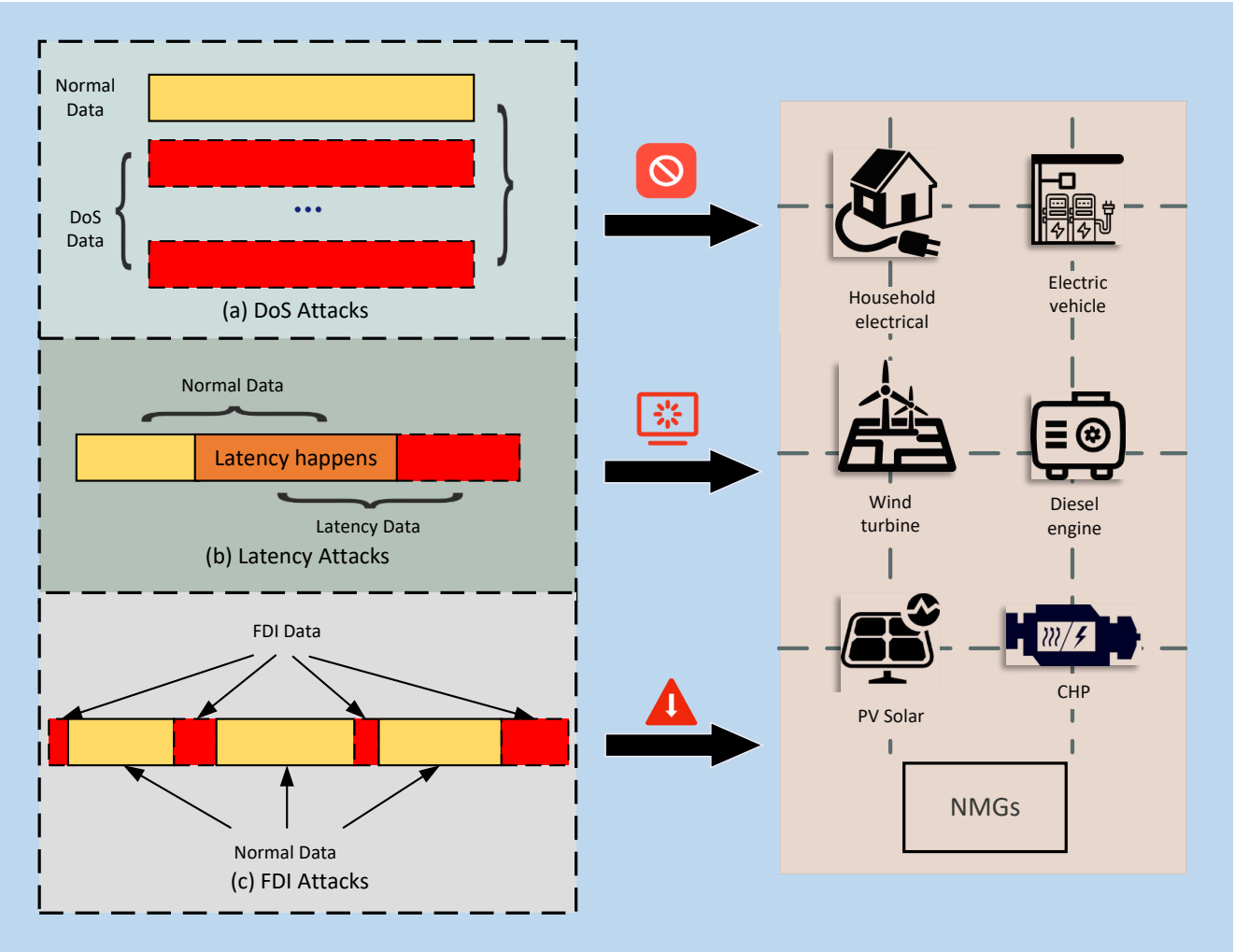


Fig. 2. Descriptions of different attacks. The dashed box on the left illustrates the typical impact of various types of attacks according to the data in NMGs. The normal data are indicated in yellow and the abnormal data are indicated in red. The right side shows that these attacks will affect NMGs containing different DERs.

TABLE II
FEATURES OF ATTACKS

Name	Complexity	Resource Consumption	Covertness	General Formulations
DoS Attacks	Low	High	Low	$\theta x(t)$
FDI Attacks	High	Medium	High	$x(t) + f(x_a(t))$
Latency Attacks	Medium	Medium	Medium	$x(t - t_a)$

*$x(t)$ denotes the item affected by the attacks. θ is related to the conditions of DoS attacks, $f(x_a(t))$ denotes the false data injection part and t_a denotes the delayed time caused by latency attacks.

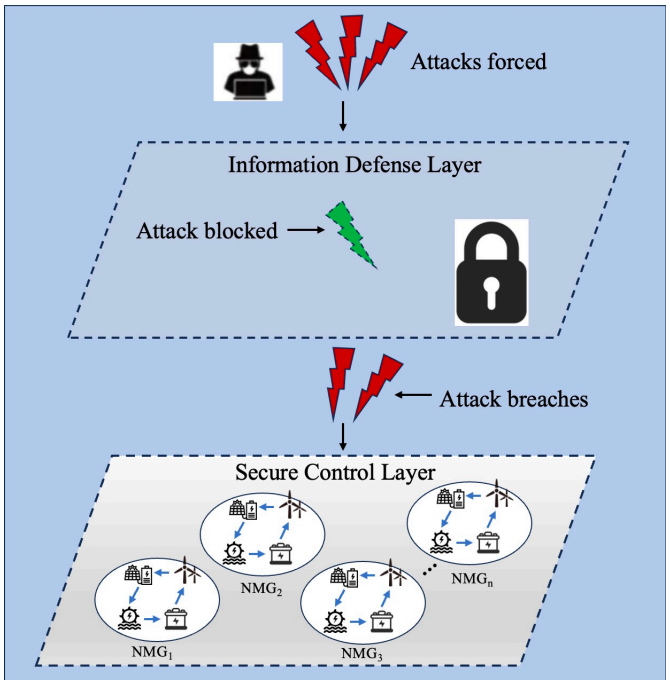


Fig. 3. The overall cybersecurity framework for NMGs

of these monitoring systems relies heavily on efficient detection algorithms aiming at directly identifying abnormal signals at the control layer with approaches in the literature ranging from classical statistical signal processing and control-theoretic methods to advanced machine learning and data-driven techniques.

This section provides an overview of several representative and effective detection methods proposed for NMG applications. In [26], a discordant element detection approach is proposed to detect false data in cooperative NMGs and inconsistent measured data in the NMGs are identified to isolate FDI attacks. This approach is tailored to distributed systems, making it effective in detecting localized anomalies in interconnected components. To deal with unknown constant power loads in NMGs, both detection and mitigation methods based on a distributed high-order sliding-mode nonlinear observer are addressed in [27]. Since both of these works assume some level of prior knowledge of NMGs, they are infeasible in the presence of multiple simultaneous attacks or uncertain noise. To allow for high adaptive and precise detection for more complex attacks and operational environments in NMGs, learning-based detection methods that depend less on NMG models and prior knowledge of NMG systems are designed in [28], [29], [30]. A supervised machine learning method that combines optimal prediction intervals is proposed in [28], which aims to classify normal and attack scenarios based on wireless sensor data. To further leverage the temporal dependencies in NMG data, the recurrent neural network is constructed in [29] to provide more accurate detection of anomalies over time. Nevertheless, this supervised learning approach requires

TABLE III
CYBER ISSUES IN THREE LOCATIONS

Location	Damage
Sensors	The measurement data transmitted in the NMG will be compromised, possibly reducing controllers' and system's performance.
Communication Channels	The data received by each DG in the NMG will become incorrect or not up to date, possibly failing to achieve the purpose of secondary control goals.
Controllers	The controller may still give an incorrect signal if the controller is attacked, compromising control performance.

extensive labeled data for training, which may not always be available for practical NMG systems. As an alternative, in [30], Reinforcement Learning (RL) is introduced into NMGs to identify vulnerabilities and remediate FDI attacks through interactions with the environment. RL is a typical unsupervised learning method that is performed by exploring and exploiting the operational environment. The use of RL allows the system to continuously improve and be scalable to new threats. However, it requires a carefully-designed reward function; otherwise, the performance of RL may dramatically degrade. Considering that the primary focus of this paper is on resilient distributed control, as elaborated in Section IV, this section provides a brief overview of selected representative methods. For a more comprehensive review of state-of-the-art detection techniques, readers are referred to the surveys in [31], [32], together with the references cited therein.

IV. RESILIENT DISTRIBUTED SECONDARY CONTROL ON CYBER ATTACKS

Even in the presence of appropriate monitoring and detection architectures, NMGs could still be affected by more intelligent attackers that could be stealthy to the detection and cause damage to NMGs. Therefore, the study of resilient control remains essential, especially in the face of increasing system uncertainties and cyber threats. The research on resilient control has experienced a clear evolution over time. Initially, the focus was on defending against simple and explicit attacks like DoS [33], gradually extending to more complex and covert threats such as FDI attacks [34]. Early work typically addressed single-attack strategies under the assumption of bounded attack scenarios. As the threat landscape grew more sophisticated with more malicious attackers involved, researchers began to explore hybrid control strategies capable of handling combinations of attack types. Recently, the emphasis has shifted toward dealing with unbounded

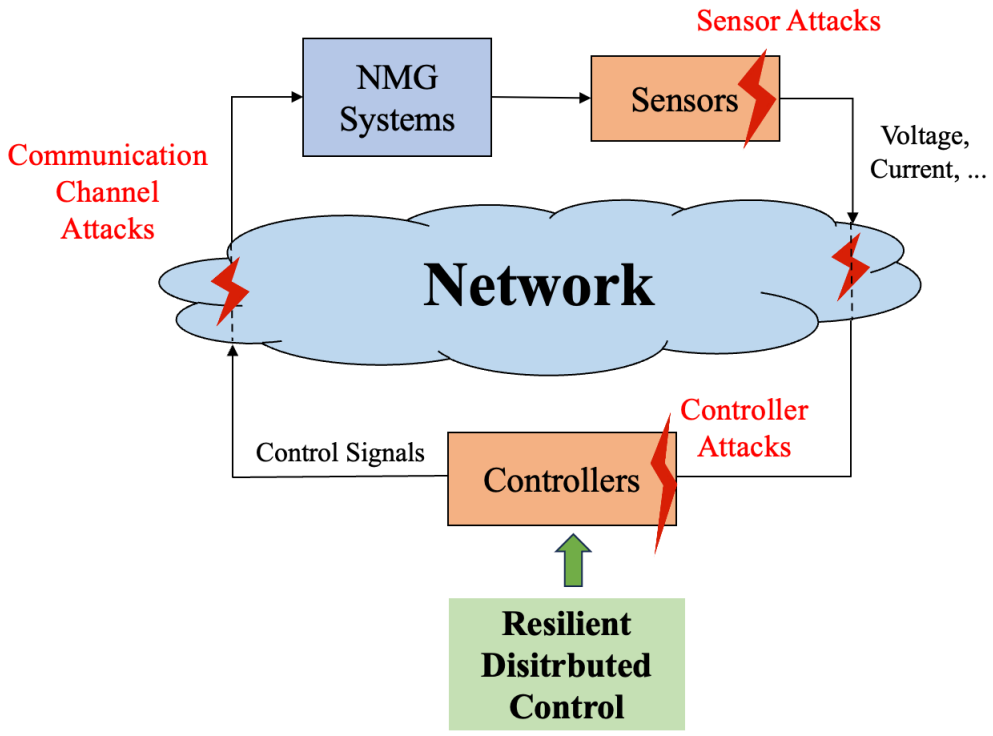


Fig. 4. Attacks occur in sensors, communication channels and controllers.

attack scenarios [35], reflecting a more realistic and challenging set of conditions. Fig. 4 is given to clearly show that the most commonly compromised positions of NMGs are identified as communication channels, sensors, and controllers. Besides, the implications of attacks on these three locations are also analyzed in Table III, where it can be seen that no matter which one or more locations are attacked, the reliability of NMGs will be dramatically reduced and irreversible damage to NMGs will be caused. Hence, to exhaustively review the recent research progress on resilient distributed control and clearly explain the impact of attacks occurring in different locations of NMGs, in the following, different resilient distributed control schemes are summarized. An overall framework of control methodology and their characteristics are summed up in Table IV.

A. Compromised communication channels

When attacks take place targeting the communication channels of NMGs, a general attack model between ith NMG and jth NMG can be formulated as [35]

$$\hat{z}_{ij} = z_{ij} + \alpha_{ij} z_a, \tag{1}$$

where z_{ij} is the normal communicated variable (which can represent frequency signals, voltage signals, current signals, etc.) transferred in the communication channel from the ith NMG to the jth NMG with the corrupted variable $\hat{z}_{ij}$. z_a is the injected malicious vector with the parameter α_{ij}. Attacks in the communication channels may cause the propagation of wrong neighboring information among NMGs and interfere in the operation of the cooperative control. As a consequence, this could potentially [20]

- delay the realization of frequency and voltage restoration

TABLE IV
COMPARISON OF DISTRIBUTED RESILIENT CONTROL METHODS IN NMGS

Classification	Pros	Cons
Model Predictive Control (MPC) [36], [37]	• Optimal control based on the receding-horizon mechanism	• Heavy computational consumption
Adaptive Control [35], [38], [39]	• High adaptability based on adaptive laws	• Complex control laws
Observer-Based Control [32], [40], [41], [42]	• Robust to disturbances	• Need to redesign a specific observer based on different attack properties
Virtual Layer-Based Control [34], [43]	• Isolating attacks based on the virtual layer	• Ambiguous physical meaning of virtual control variables
Sliding Mode Control [44], [45], [46]	• Fast dynamic response to cyber attacks	• Possible chattering problems that degrade the control performance
Learning-Based Control [47], [48]	• Achieving satisfactory control performance without modelling	• Difficulties in providing theoretical guarantees and explainability issue
Event-Triggered Control [49], [50]	• Resource efficiency by designing certain conditions (events)	• Potential Zeno behaviors

- violate power sharing limits causing DGs' overloads
- make DGs to synchronize at wrong references
- affect the transmission of control signals and state information
- prevent remote control operations, making it impossible for operators to remotely regulate and control NMGs.
- lead to information isolation between NMGs, affecting the coordinated operation of the overall system.

B. Compromised controllers

To maximize destructive impact, attackers may directly target secondary control laws by accessing the places where the controllers are running or embedded. When the secondary controller is compromised, the formulation can typically be described as follows:

$$\hat{u}_i = u_i + \alpha_i u_a, \tag{2}$$

where u_i is the normal input designed by the controller and $\hat{u}_i$ is the corrupted input of the ith NMG. u_a is the injected malicious input value with parameter α_i. Once the controller attack (2) is launched, the physical system fails to operate as intended due to its response to the modified attack signal u_a, which deviates from the original signal u_i. The potential consequences of these controller attacks on distributed secondary controllers can be summarized as follows [7]:

- Failure to restore the frequency or voltage of NMGs
- Cause NMGs oscillation and compromise the stability
- Interfere with the demand response strategy, leading to the supply-demand imbalance
- Potentially cause intentional blackouts or other malicious actions.

C. Compromised sensors

For the ith DG in an NMG, the measured states can usually be modeled as

$$\hat{y}_i = y_i + \alpha_i y_{ia}, \tag{3}$$

where y_i is the valid measurement of ith sensor with its corrupted measurement $\hat{y}_i$. y_{ia} is the abnormal attack vector with the parameter α_i. Sensors under attack (3) may negatively affect the behaviour of the NMG as follows [51]:

- Tampering or interfering with sensor data may result in incorrect voltage and frequency readings, leading to unnecessary adjustments and system instability;
- Inaccurate load information can cause errors in load distribution in DGs, resulting in overload or underload in some NMGs, further affecting the stability of the whole NMG system;
- Sensor errors can affect the monitoring and forecasting of RESs such as solar and wind power, leading to a decrease in the integration and utilization efficiency of these energy sources;
- Incorrect sensor measurement can mislead the fault diagnosis process, prolong troubleshooting time, and increase the difficulty of NMG recovery.

D. Representative works

Table V presents a set of recent representative works and highlights the control strategies employed and the types of cyber-physical attacks addressed in NMGs. Based on this Table, several key trends can be identified in the evolving approaches to secure and resilient control in NMGs:

1) Transition Toward Practical and Targeted Attack Mitigation: Earlier research typically treated cyber attacks as a type of system disturbance and applied robust control techniques designed for conventional system uncertainties. However, recent studies have increasingly recognized the fundamental differences between cyber attacks and external disturbances. This has led to more direct and practical defense strategies that explicitly consider attack dynamics, intent, and impact. These strategies are tailored to specific threat models and are designed to respond rapidly and effectively in real time.

2) Emergence of Data-Driven and Hybrid Control Paradigms: Traditional model-based control methods are gradually being complemented, or in some cases, replaced by data-driven, learning-based, and data-model-hybrid approaches. These paradigms aim to reduce the dependency on precise mathematical models as they may fail to capture the evolving system behavior under cyber attack conditions. Instead, intelligent methods can enhance adaptability and give self decision-making ability to NMGs, particularly in dynamic and uncertain NMG operating environments. Techniques such as reinforcement learning, federated learning, are being explored to support resilient control under incomplete or corrupted information.

3) Move Towards Integrated and Multi-Strategy Control Architectures: With the increasing complexity of cyber attacks, single control strategies, such as standalone sliding mode control or adaptive control, have shown to be inadequate. Current trends emphasize the integration of multiple control methods to form hierarchical, coordinated, or cooperative frameworks. For example, event-triggered control and predictive control are combined to maintain efficient and resilient control performance, or multiple types

TABLE V
LITERATURE SUMMARY ON CONTROL METHODS UNDER CYBER ATTACKS IN NMGS

Defense Strategy	Control Scheme and Example	Attack Type	Key Feature
Robustness Enhancement	a) Sliding mode resilient distributed control[29]; b) Observer-based methods[38][43]	FDI attacks	Treats attacks as disturbances
Attack Mitigation	a)Virtual layer[40][49]; b)Compensator consensus control [51]	FDI/DoS attacks	Isolate or mitigate attacks' impact by using auxiliary control inputs
Topology Reconfiguration	a)Event-triggered control [53]; b)Flexible decentralized/distributed control[52], [12]	FDI/DoS attacks	Prevent cyber attacks by designing specific rules to reconstruct the communication
Adaptive Gain	a)Fuzzy inference adaptive control [35]; b)Belief value-based control[52]	FDI attacks	Propose adaptive laws to protect NMGs
Prediction-Based Defense	a)Model-free predictive control[35]; b) Sampled-data predictive control[52]	Latency/DoS attacks	Use forecasting data/model to mitigate attacks
Learning-Integrated Control	a)Machine learning[44]; b) Reinforcement learning [53]	Latency/DoS/FDI attacks	Learning algorithms are tailored to fit the operation environment of NMGs under cyber attacks

of observers are integrated to enhance detection capabilities. These architectures provide better anomaly tolerance and enable more precise control actions under adversarial conditions, ensuring stable operation and performance even during sustained or multi-position attacks.

4) Adaptive Topology and Flexible Control Frameworks: As simultaneous attacks on controllers, sensors and communication links increase, the need to dynamically reconfigure network topology and integrate flexible control strategies has emerged as a critical research direction. This interdisciplinary approach leverages concepts from communication theory, control theory, and power systems engineering to enhance the resilience and attack tolerance of NMGs.

These trends reflect a broader shift from purely defensive strategies toward intelligent, adaptive, and system-aware designs that anticipate and respond to evolving threats. Ongoing work continues to explore how to efficiently balance performance, resilience, and computational feasibility in next-generation NMG control systems.

E. Case Studies

To illustrate the effectiveness of secure control in NMGs, this section analyzes the control performance of several popular resilient controllers under various attack scenarios with the corresponding system configuration shown in Fig. 5. The simulation parameters are given in Table VI and more information on the simulation setup can be found in [42]. The control objective of the first four cases is to restore the AC NMGs' frequency under different types of cyber attacks, while the fifth case focuses on current sharing in DC NMGs. u_i and ω_i represent the input signals and the angular frequency of the ith NMG system, respectively. In the case study, the current sharing ratios among DGs are preset for illustration. However,

TABLE VI
PARAMETERS OF NMG SYSTEMS

	DG1|DG2		DG3|DG4	
Primary Control	$\tau_{P_1}\|\tau_{P_2}$	0.016	$\tau_{P_3}\|\tau_{P_4}$	0.016
	$k_{P_1}\|k_{P_2}$	6e-5|3e-5	$k_{P_3}\|k_{P_4}$	2e-5|1e-5
Load	$R_{L_1}\|R_{L_2}$	50 Ω/phase	$R_{L_3}\|R_{L_4}$	50 Ω/phase
Lines	$R_1 = R_2 = 0.6\Omega,\ L_1 = L_2 = 0.03393$H $R_3 = R_4 = 0.6\Omega,\ L_3 = L_4 = 0.03393$H			

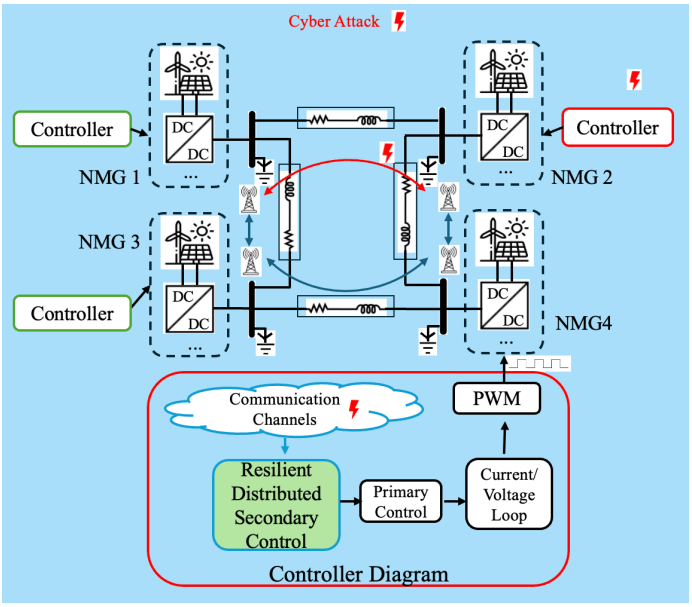


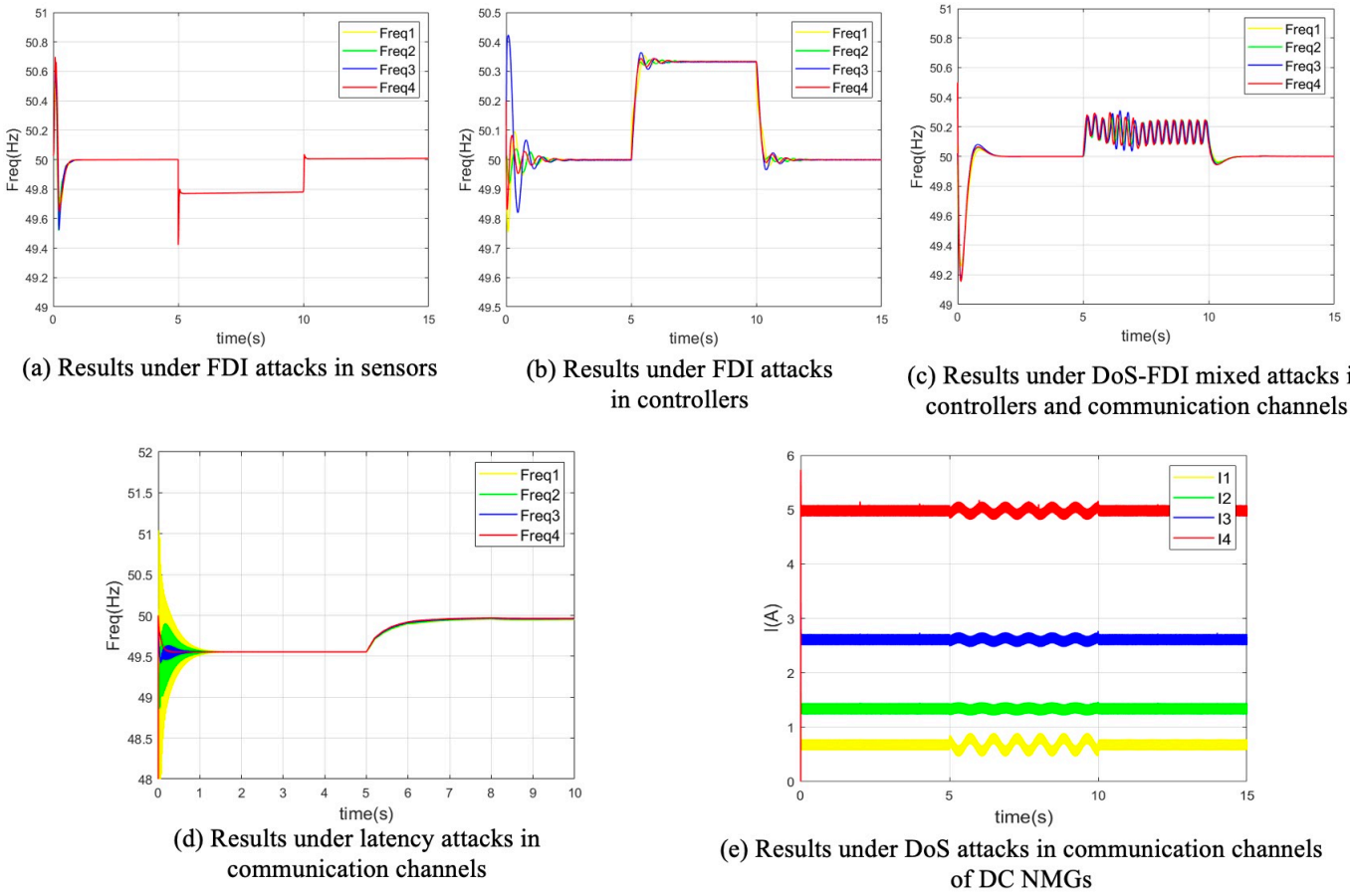
Fig. 5. A representative NMG structure for the case studies

in practical NMGs, these ratios are not fixed but are determined by the tertiary control layer, where the DSM and the energy management system play a critical role in optimizing scheduling decisions based on factors such as economic operation, supply-demand balance, and overall system efficiency.

1) *FDI attacks in sensors*. It can be seen in Fig. 6(a) that the NMGs are initially controlled by a distributed PID secondary controller, and the frequency gradually recovers to $50Hz$. At the $5th$ second, a typical sinusoidal FDI signal $0.1414sin(0.05t)$ is injected into the frequency sensor of DG1 to deviate the frequency from $50Hz$. At the $10th$ second, the intermediate observer-based resilient controller [42] is activated with the following equation in the ith NMG

$$u_i = \alpha_i(\nu_i - \omega_i), \tag{4}$$

with the auxiliary variable $\dot{\nu_i} = \beta_i {e_i}^{\omega} + \gamma_i e_i^P$ where ${e_i}^{\omega}$ is the frequency error and e_i^P is the power sharing error. α_i, β_i and γ_i are the corresponding proportional gains. With this resilient controller,



(a) Results under FDI attacks in sensors

(b) Results under FDI attacks in controllers

(c) Results under DoS-FDI mixed attacks in controllers and communication channels

(d) Results under latency attacks in communication channels

(e) Results under DoS attacks in communication channels of DC NMGs

Fig. 6. Simulation results of different control schemes under cyber attacks

the system frequency successfully recovers to $50Hz$, showing the effectiveness and robustness of the proposed resilient controller.

2) *FDI attacks in controllers*. Fig. 6(b) shows that the distributed secondary control can restore frequency but the deviation of frequency occurs after suffering from FDI attacks signals $20sin(10t) + 20$ in all DGs' controllers after the $5th$ second. After 10 seconds, the following iterative observer-based resilient controller [41] is designed to restore the frequency to $50Hz$

$$u_i = -c_i\omega_i - s_{i,k+1} \tag{5}$$

where the first part with control gain c_i is designed to achieve consensus of the frequency to $50Hz$ and the second part $s_{i,k+1}$ is given to mitigate the impact of FDI attacks by using the estimation of the iterative observer.

3) *Simultaneous attacks with DoS attacks in communication channels and FDI attacks in controllers*.

Fig. 6(c) is depicted to describe how the simultaneous attacks (FDI attacks signal $5sin(20t) + 5$ in DG1, DoS in communication channel between DG1 and DG2) affect the NMGs and how the following resilient controller works [54]

$$u_i = G \sum_{j=1}^{N} a_{ij} \left(\omega_j - \omega_i\right) - s_{i,k+1}, \tag{6}$$

where a_{ij} is related to the knowledge of DoS attacks, G is the controller gain to be designed, and N is the number of neighboring NMGs. In this case, the non-resilient distributed secondary controller fails after encountering DoS and FDI attacks in the $5th$ seconds. This failure persists until the above resilient controller takes effect 10 seconds later, demonstrating the effectiveness and necessity of the resilient controller in NMGs' frequency recovery.

4) *Latency attacks in communication channels*. According to [55], the $t - T$ latency attacks occur in all communication channels to affect the angular frequency, denoted as $\omega_i(T)$. To defend this attack, the following resilient controller is given against the latency attacks in communication channels of NMGs

$$u_i = a_\omega \sum_{j \in \mathbb{N}_i} \left(\omega_i(t-T) - \omega_j(t-T)\right) + b_i a_\omega \left(\omega_i(t-T) - \omega_n\right) \tag{7}$$

where a_ω is the control gain, t and T are related to the sampling time and delays, ω_n is the reference value. The frequency changes are depicted in Fig. 6(d) where it can be observed that the frequency cannot be restored to the reference value $50Hz$ without the proposed resilient controller before 5 seconds. After the proposed resilient controller is performed, the frequency is gradually restored to $50Hz$.

5) *FDI and DoS attacks in the communication channels of DC NMGs*. To show the impact of FDI attack signal $2sin(8t)$ in exchanged information between DG3 and DG4, and DoS attacks in communication channel between DG1 and DG2, this case gives the results of current sharing in DC NMGs after designing the following resilient distributed controller [33]

$$u_i = \int \left[K_i E_i + u_i^o\right] dt \tag{8}$$

where E_i, with control gain K_i, is related to the average voltage value under DoS attacks and u_i^o is an auxiliary item corresponding to the observer gain. By utilizing the above-mentioned controller,

the current allocation results are given in Fig. 6(e) where the system lost communication between $[5s, 5.007s]$ and the output current of each DG fluctuates due to the influence of the DoS attack. At the $10th$ second, the proposed resilient controller is able to re-allocate the output current to a ratio of $6:3:2:1$ again.

Based on the above cases, it is evident that different attacks at different locations will produce different degrees of adverse effects. Notably, compared to distributed resilient control, when distributed non-resilient control is running, the system frequency deviates from its reference value, and the intended proportional current distribution cannot be maintained under cyber attacks. After the proposed resilient controllers are designed, resilient frequency restoration and power sharing can be achieved in NMGs.

It is worth noting that it is important to analyze the frequency of attacks at different locations. However, cyber attackers are often malicious and rarely disclose details of their activities to protect their own privacy [56]. Moreover, the study of attack frequency is also hindered by organizations' reluctance to disclose their experiences with security breaches. Consequently, to the best of our knowledge, while some government websites [57] offer databases that catalog cyber incidents like data theft and hijacking, identifying the specific types of attacks responsible for these incidents and accurately summarizing the frequency of these attacks remains challenging. The report of cyber attacks against the Ukrainian critical infrastructure is one of the few well-documented cases on the electric grid, extensively investigated since 2016 [58]. This report indicates that one of the most frequently employed attacks in this context is a variant of the DoS attack, that is, the Distributed DoS (DDoS) attack. In this study, we focus on three of the most common and impactful attack types encountered in NMGs: DoS, FDI, and latency attacks. While there are many other types of attacks, our aim is to address the most representative threats observed in the research literature.

As controller designers in cyber-physical NMGs, it is our responsibility to develop advanced resilient control strategies capable of mitigating the impact of any type of attack, independently from their likelihood, as the potential consequences of cyber-attacks to safety-critical systems such as the electric grid are tremendous. We hope that future access to more comprehensive incident data will further support the design of targeted, resilient control mechanisms against a broader range of cyber-physical threats.

V. Conclusion and trends of resilient control for NMGs

This article provides a state-of-the-art overview in the area of distributed resilient secondary control methods for NMGs under various attack scenarios. Different types of attacks are summarized depending on data classification and the location of the attacks. To mitigate the impact of such attacks, the article also lists

prevalent detection methods. Moreover, to address the problem of attacks that can bypass detectors, this article then focuses on summarizing various effective resilient distributed secondary control mechanisms positioned at three critical positions within NMGs: communication channels, sensors, and controllers. According to the current research progress on resilient secondary control for NMGs, in the following, we present some trending topics in the literature.

A. Advanced attacks defense

Current research generally assumes the attacks can be modeled as Eq. (1) - Eq. (3) or their mixed models. However, this assumption may be ideal as sophisticated attackers will adapt attack strategies to maximize the impact of their attacks in a model-free manner.

The growing implementation of smart sensors and plugs in NMGs is able to generate a huge amount of data and provide opportunities to address the inherent limitations of physical models. This trend emerges in data-driven and learning-based approaches as a key research direction for future sustainable NMGs. For instance, data-driven control based on Willems' fundamental lemma [59] integrates system identification and control, enabling the direct derivation of control strategies from data. Similarly, neural network-based learning control methods reduce dependence on physical models by training on large datasets from uncertain NMG dynamics. RL-based methods [30], on the other hand, can derive control strategies through environmental exploration and trial-and-error processes.

In summary, data-driven/learning-based detection algorithems should be given more attention and the resilience of NMGs could be enhanced by taking full use of real-time data without model dependencies.

B. Configurable resilient control

As a representative CPS, NMGs inherit one of the intrinsic properties of such systems: to maximize functionality, numerous IoT devices and RESs may be connected to or disconnected from NMGs, resulting in a dynamically changing configuration. Consequently, the configuration of NMGs evolves over time due to system upgrades, internal faults, the connection and disconnection of NMGs, etc. Selecting an appropriate configuration under varying operating conditions significantly affects the stability, economic performance, and resilience of NMGs against cyber attacks. For example, k-means clustering, routing algorithms, optimization-based methods have been proposed to deal with configuration problems of NMGs. However, current methodologies may fail to achieve configurable control and need to re-design the controller if the NMG configurations change. As the scale of NMGs expands and the integration of

DERs and EVs increases, the likelihood of configuration changes within NMGs will rise significantly. Therefore, it is crucial to develop efficient and configurable control frameworks that ensure both resilience and reliability.

A potential approach involves classifying various DERs into different clusters and selecting one or more leaders within each cluster [12]. The leaders are responsible for receiving information from the main grid or buses and are capable of making independent decisions without communicating with other clusters (decentralized structure). The remaining DERs act as followers and respond to the leaders' decisions in a distributed manner. This decentralized-distributed structure allows for a flexible number of clusters, leaders, and followers. It enables any DERs to disconnect from neighboring DERs and operate independently, thus creating a configurable control architecture to respond to varying operating conditions and increase the difficulty for attackers to infer NMGs' structure.

C. Privacy preserving

As NMG networks expand and grow with the integration of EVs, privacy concerns are expected to intensify. It is common that distributed resilient controllers often rely on real-time, accurate information from NMGs. However, sensitive data such as electricity prices, customer energy consumption patterns, and power usage and load profiles associated with V2G may not be readily disclosed due to privacy and market competitiveness considerations. These challenges underscore the need for developing privacy-preserving distributed resilient controllers for future NMGs.

A natural solution to this challenge is to employ encryption techniques to protect sensitive data. Among these, blockchain-based encryption has emerged as a particularly promising method due to its inherent capability for decentralized data storage and integrity verification. By leveraging blockchain technology [60], sensitive information can be securely distributed across the network, minimizing the risk of unauthorized access while maintaining data availability. Additionally, differential privacy has recently garnered attention as an effective means of safeguarding the privacy of NMGs in a distributed manner. This approach encrypts information by introducing noise into the system data, thereby obscuring the true values from attackers while still allowing for meaningful analysis and control for NMG systems.

In conclusion, future distributed control schemes should not only incorporate these privacy-preserving methods but also be designed to effectively recover real data from encrypted information or utilize encrypted information directly for control purposes. This dual capability would enable the realization of resilient and reliable NMGs without compromising privacy.

D. Performance guaranteed control

In NMGs, heterogeneous DERs such as PV units, wind turbines, and emerging EV technologies exhibit diverse response times due to their inherent physical dynamics, communication topologies, and control mechanisms. Such heterogeneity may induce instability, degrade power quality, and reduce overall system reliability. Most existing control strategies are based on asymptotic convergence theory, which increasingly falls short of meeting the high-performance requirements of future NMGs. Consequently, designing distributed predefined-time resilient controllers that ensure system reliability while guaranteeing pre-specified control performance remains a promising yet unresolved challenge.

Moreover, the majority of existing resilient control schemes prioritize guaranteeing resilience and reliability without adequately addressing associated costs. If cost considerations are overlooked, future control strategies may become prohibitively unaffordable, undermining their practicality and scalability. As the scale of NMGs expands, the need for optimal control becomes paramount to ensure both affordability and efficiency [37]. To address these challenges, advanced optimal resilient control strategies can be developed to realize voltage/frequency restoration with minimal control effects.

These advanced methods not only improve the responsiveness of DERs but also optimize resource allocation and operational costs. By integrating cost considerations into the design of predefined-time resilient control strategies, NMGs can achieve a balance between performance, reliability, and economic feasibility, paving the way for secure and efficient NMGs in the future.

REFERENCES

[1] S. Fankhauser, S. M. Smith, M. Allen, K. Axelsson, T. Hale, C. Hepburn, J. M. Kendall, R. Khosla, J. Lezaun, E. Mitchell-Larson *et al.*, "The meaning of net zero and how to get it right," *Nature Climate Change*, vol. 12, no. 1, pp. 15–21, 2022.

[2] Z. Deng, Y. Zhou, A. Kamal, R. Na, I. P. Brown, and Z. J. Shen, "Smart plug 2.0: A solid-state smart plug device preventing fire and shock hazards," *IEEE Transactions on Power Electronics*, vol. 38, no. 3, pp. 3140–3151, 2022.

[3] "King island renewable energy integration project," 2016. [Online]. Available: https://arena.gov.au/projects/king-island-renewable-energy-integration-project/

[4] "The isle of eigg project," 2025. [Online]. Available: http://isleofeigg.org

[5] F. Guo, Q. Xu, C. Wen, L. Wang, and P. Wang, "Distributed secondary control for power allocation and voltage restoration in islanded dc microgrids," *IEEE Transactions on Sustainable Energy*, vol. 9, no. 4, pp. 1857–1869, 2018.

[6] E. Trinklei, G. Parker, W. Weaver, R. Robinett, L. B. Gauchia, C.-W. Ten, W. Bower, S. F. Glover, and S. Bukowski, "Scoping study: networked microgrids," Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2014.

[7] B. Chen, J. Wang, X. Lu, C. Chen, and S. Zhao, "Networked microgrids for grid resilience, robustness, and efficiency: A review," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 18–32, 2021.

[8] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of cps security," *Annual Reviews in Control*, vol. 47, pp. 394–411, 2019.

[9] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A survey on cyber–physical systems security," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21 670–21 686, 2023.

[10] L. Sheng, G. Lou, W. Gu, S. Lu, S. Ding, and Z. Ye, "Optimal communication network design of microgrids considering cyber-attacks and time-delays," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3774–3785, 2022.

[11] "Threat landscape for the ics engineering and integration sector," 2021. [Online]. Available: https://ics-cert.kaspersky.com/publications/reports/2021/03/17/threat-landscape-for-the-ics-engineering-and-integration-sector-2020/

[12] F. Guo, Z. Li, J. Wu, Z. Huang, and H. Ni, "A decentralized-distributed control framework for configurable networked microgrids," *IEEE Transactions on Industrial Electronics*, vol. 72, no. 1, pp. 959–968, 2024.

[13] S. E. Sati, M. B. Abdelghany, B. Hamad, A. Al-Durra, H. H. Zeineldin, T. H. EL-Fouly, and E. F. El-Saadany, "Economic power-sharing and stability enhancement for virtual synchronous generators in islanded mg," *IEEE Transactions on Power Systems*, vol. 40, no. 1, pp. 188–203, 2024.

[14] G. S. Thirunavukkarasu, M. Seyedmahmoudian, E. Jamei, B. Horan, S. Mekhilef, and A. Stojcevski, "Role of optimization techniques in microgrid energy management systems-a review," *Energy Strategy Reviews*, vol. 43, p. 100899, 2022.

[15] M. F. Zia, E. Elbouchikhi, and M. Benbouzid, "Microgrids energy management systems: A critical review on methods, solutions, and prospects," *Applied Energy*, vol. 222, pp. 1033–1055, 2018.

[16] Z. Cheng, J. Duan, and M.-Y. Chow, "To centralize or to distribute: That is the question: A comparison of advanced microgrid management systems," *IEEE Industrial Electronics Magazine*, vol. 12, no. 1, pp. 6–24, 2018.

[17] B. Adineh, M. R. Habibi, A. N. Akpolat, and F. Blaabjerg, "Sensorless voltage estimation for total harmonic distortion calculation using artificial neural networks in microgrids," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 7, pp. 2583–2587, 2021.

[18] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 20–23, 2015.

[19] Z. Chen, F. Pasqualetti, J. He, P. Cheng, H. L. Trentelman, and F. Bullo, "Guest editorial: Special issue on security and privacy of distributed algorithms and network systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3725–3727, 2020.

[20] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020.

[21] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2586–2633, 2020.

[22] M. Liu, F. Teng, Z. Zhang, P. Ge, M. Sun, R. Deng, P. Cheng, and J. Chen, "Enhancing cyber-resiliency of DER-based smart grid: A survey," *IEEE Transactions on Smart Grid*, vol. 15, no. 5, pp. 4998–5030, 2024.

[23] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 4035–4049, 2019.

[24] L. Wang, W. Liu, F. Guo, Z. Qiao, and Z. Wu, "Differentially private average consensus with improved accuracy-privacy trade-off," *Automatica*, vol. 167, p. 111769, 2024.

[25] Y. Lu and M. Zhu, "A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems," *Annual Reviews in Control*, vol. 47, pp. 423–440, 2019.

[26] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative DC microgrids-A discordant element approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2019.

[27] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "Detection and mitigation of false data in cooperative DC microgrids with unknown constant power loads," *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9565–9577, 2021.

[28] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 650–658, 2021.

[29] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5294–5310, 2021.

[30] A. J. Abianeh, Y. Wan, F. Ferdowsi, N. Mijatovic, and T. Dragičević, "Vulnerability identification and remediation of FDI attacks in islanded DC microgrids using multiagent reinforcement learning," *IEEE Transactions on Power Electronics*, vol. 37, no. 6, pp. 6359–6370, 2022.

[31] M. Uzair, L. Li, M. Eskandari, J. Hossain, and J. G. Zhu, "Challenges, advances and future trends in AC microgrid protection: With a focus on intelligent learning methods," *Renewable and Sustainable Energy Reviews*, vol. 178, p. 113228, 2023.

[32] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.

[33] Z. Lian, Y. Zhu, F. Guo, C. Peng, and Q. Zhou, "Distributed cyber resilient control strategy for remote DC microgrids under integrated satellite terrestrial networks," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 3, pp. 2363–2372, 2025.

[34] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A FDI attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929–1938, 2020.

[35] J. Xiao, L. Wang, Z. Qin, and P. Bauer, "A resilience enhanced secondary control for AC micro-grids," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 810–820, 2024.

[36] T. Li, X. Wen, B. Chen, and Z. Wang, "Distributed MPC-based constant voltage control for DC microgrids under DoS attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 71, no. 9, pp. 4266–4270, 2024.

[37] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragičević, "Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1487–1498, 2021.

[38] A. Abazari, M. Zadsar, M. Ghafouri, R. Atallah, and C. Assi, "A data mining/anfis and adaptive control for detection and mitigation of attacks on DC MGs," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 2406–2422, 2023.

[39] X.-K. Liu, C. Wen, Q. Xu, and Y.-W. Wang, "Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3742–3754, 2021.

[40] J. Lu, X. Zhang, X. Hou, and P. Wang, "Generalized extended state observer-based distributed attack-resilient control for DC microgrids," *IEEE Transactions on Sustainable Energy*, vol. 13, no. 3, pp. 1469–1480, 2022.

[41] Q. Tang, C. Deng, Y. Wang, F. Guo, and S. Fan, "Iterative observer-based resilient control for energy storage systems in microgrids under FDI attacks," *IEEE Transactions on Smart Grid*, vol. 15, no. 5, pp. 4744–4753, 2024.

[42] F. Guo, Z. Huang, J. Wu, Z. Li, S. Liu, and L. Xing, "Distributed secondary resilient controller design for islanded ac microgrids under stealthy frequency sensor attack," *IEEE Transaction on Circuits and Systems-I: Regular Papers*, vol. 71, no. 12, pp. 6203–6214, 2024.

[43] M. Jamali, M. S. Sadabadi, M. Davari, S. Sahoo, and F. Blaabjerg, "Resilient cooperative secondary control of islanded AC microgrids utilizing inverter-based resources against state-dependent false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 71, no. 5, pp. 4719–4730, 2024.

[44] Y. Jiang, Y. Yang, S.-C. Tan, and S. Y. Hui, "Distributed sliding mode observer-based secondary control for DC microgrids under cyber-attacks," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 1, pp. 144–154, 2021.

[45] A. J. Abianeh, M. M. Mardani, F. Ferdowsi, R. Gottumukkala, and T. Dragičević, "Cyber-resilient sliding-mode consensus secondary control scheme for islanded ac microgrids," *IEEE Transactions on Power Electronics*, vol. 37, no. 5, pp. 6074–6089, 2022.

[46] J. Hu, Q. Sun, M. Zhai, and B. Wang, "Privacy-preserving consensus strategy for secondary control in microgrids against multilink false data injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 10, pp. 10 334–10 343, 2023.

[47] Y. Xia, Y. Xu, S. Mondal, and A. K. Gupta, "A transfer learning-based method for cyber-attack tolerance in distributed control of microgrids," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 1258–1270, 2024.

[48] A. Afshari, M. Karrari, H. R. Baghaee, and G. Gharehpetian, "Resilient synchronization of voltage/frequency in AC microgrids under deception attacks," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2125–2136, 2021.

[49] Z. Huang, Y. Li, M. Ke, and J. Deng, "Distributed secondary control with an event-triggered consensus-based observer for energy storage systems in islanded Dc microgrids," *IEEE Transactions on Sustainable Energy*, vol. 15, no. 2, pp. 1167–1179, 2024.

[50] H. Yang, T. Li, Y. Long, and Y. Xiao, "Event-triggered distributed secondary control with model-free predictive compensation in AC/DC networked microgrids under DoS attacks," *IEEE Transactions on Cybernetics*, vol. 54, no. 1, pp. 298–307, 2024.

[51] Y. Liu, Y. Li, Y. Wang, X. Zhang, H. B. Gooi, and H. Xin, "Robust and resilient distributed optimal frequency control for microgrids against cyber attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 375–386, 2022.

[52] J. Wu, F. Guo, and F. Boem, "Decentralised-distributed secondary frequency restoration and power sharing control for microgrid clusters," in *2024 European Control Conference (ECC)*, pp. 279–284. IEEE, 2024.

[53] Y. Wang and B. C. Pal, "Destabilizing attack and robust defense for inverter-based microgrids by adversarial deep reinforcement learning," *IEEE Transactions on Smart Grid*, vol. 14, no. 6, pp. 4839–4850, 2023.

[54] Q. Tang, C. Deng, S. Fan, Y. Wang, D. Yue, and B. Wang, "A novel cooperative resilient control method for energy storage systems under hybrid attacks," *IEEE Transactions on Industrial Electronics*, vol. 72, no. 2, pp. 1871–1880, 2024.

[55] Z. Lian, C. Deng, C. Wen, F. Guo, P. Lin, and W. Jiang, "Distributed event-triggered control for frequency restoration and active power allocation in microgrids with varying communication time delays," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 9, pp. 8367–8378, 2021.

[56] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, 2023.

[57] "European repository of cyber incidents," 2025. [Online]. Available: https://eurepoc.eu/table-view/

[58] "Cyber attack against ukrainian critical infrastructure," 2021. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[59] H. J. Van Waarde, C. De Persis, M. K. Camlibel, and P. Tesi, "Willems' fundamental lemma for state-space systems and its extension to multiple datasets," *IEEE Control Systems Letters*, vol. 4, no. 3, pp. 602–607, 2020.

[60] Y. Yu, G.-P. Liu, and W. Hu, "Blockchain protocol-based secondary predictive secure control for voltage restoration and current sharing of DC microgrids," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 1763–1776, 2023.