On the Control of Microgrids Against Cyber-Attacks: A Review of Methods and Applications

Solat, Amirhossein ; B. Gharehpetian, Gevork; Salay Naderi, Mehdi ; Anvari-Moghaddam, Amjad

Published in:
Applied Energy

DOI (link to publication from Publisher):
https://doi.org/10.1016/j.apenergy.2023.122037

Publication date:
2024

Document Version
Accepted author manuscript, peer reviewed version

On the Control of Microgrids Against Cyber-Attacks: A Review of Methods and Applications

Amirhossein Solat[a], G. B. Gharehpetian[a,*], Mehdi Salay Naderi[b], Amjad Anvari-Moghaddam[c]

[a] *Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran*

[b] *Iran Grid Secure Operation Research Center, Amirkabir University of Technology, Tehran, Iran*

[c] *Department of Energy (AAU Energy), Aalborg University, 9220 Aalborg, Denmark*

[*] *corresponding author email: grptian@aut.ac.ir*

Abstract

Nowadays, the use of renewable generations, energy storage systems (ESSs) and microgrids (MGs) has been developed due to better controllability of distributed energy resources (DERs) as well as their cost-effective and emission-aware operation. The development of MGs as well as the use of hierarchical control has led to data transmission in the communication platform. As a result, the expansion of communication infrastructure has made MGs as cyber-physical systems (CPSs) vulnerable to cyber-attacks (CAs). Accordingly, prevention, detection and isolation of CAs during proper control of MGs is essential. In this paper, a comprehensive review on the control strategies of microgrids against CAs and its defense mechanisms has been done. The general structure of the paper is as follows: firstly, MGs operational conditions, i.e., the secure or insecure mode of the physical and cyber layers are investigated and the appropriate control to return to a safer mode are presented. Then, the common MGs communication system is described which is generally used for multi-agent systems (MASs). Also, classification of CAs in MGs has been reviewed. Afterwards, a comprehensive survey of available researches in the field of prevention, detection and isolation of CA and MG control against CA are summarized. Finally, future trends in this context are clarified.

Keywords: Microgrid, Cyber-Attacks, Cyber-Physical Systems, Detection and Isolation of Attack, Resilient Control, Communication System

Abbreviations

MG	Microgrid
CPS	Cyber-Physical System
CA	Cyber-Attack
DER	Distributed Energy Resource
ESS	Energy Storage System
FDI	Fault Data Injection
DoS	Denial of Service
MAS	Multi-Agent System
SCADA	Supervisory Control And Data Acquisition
PLC	Programmable Logic Controller
LSS	Large-Scale System
RTU	Remote Terminal Unit

PMU Phasor Measurement Unit

PCC Point of Common Coupling

1. Introduction

A small-scale power system that includes distributed energy resources (DERs) such as wind turbines, fuel cells and photovoltaic panels, energy storage systems (ESSs) and electrical power loads and heat loads, is called a microgrid (MG) that can be operated in grid-connected or islanded mode [1-2]. Communication infrastructures play an important role in monitoring and control of MGs. On the other hand, a cyber-physical system (CPS) is an intelligent system including physical and communication parts. Thus, the MG is a CPS with interconnected electrical and communication networks [3-6].

MG as a powerful platform makes power systems efficient, secure, stable, reliable and resilient. These small grids can play a role in reducing the effect of power system disruptions caused by unexpected but catastrophic incidents such as natural disasters and cyber-attacks (CAs). The catastrophic power outage after Sandy Hurricane, which left much of the eastern United States with a population of about 7.5 million in October 2012 without electricity for several days, was an obvious example about the lack of power system resilience. Today, reliability and resilience are two essential aspects of the operation of power systems, which has led the electrical power grid to deploy MGs. Because of the increasing number of severe weather events, which are often ascribed to global warming, resiliency in providing electricity services to customers has become more and more important [7-8]. The increased use of information and communication technologies can improve the performance of the power system, but if not properly managed, the power system may be inadvertently exposed to cyber threats. Generally, CA is any attempt to gain unauthorized access to a computer, computing system or communication network with the intent to cause damage. CAs aim to disable, disrupt, destroy or control communication systems or to alter, block, delete, manipulate or steal the data held within these systems. Cyber incidents can have disastrous effects on the performance of the power system. Table 1 shows a list of major power outages caused by cyber incidents. These cases indicate that CAs could potentially cause widespread blackouts in the power system. For example, on December 23, 2015, attackers with the help of malware called Black Energy Trojan cut the breakers in the Ukrainian power system remotely, which cut off more than 30 substations and approximately 225,000 consumers for about 6 hours without electricity. As the number of CAs aimed at disrupting the power system supply is increasing worldwide, power systems need to address this new issue to manage system resilience in their operation [9-13].

Table 1 Power Outages Related to Cyber Incidents [9-13]

Event	Cause	Consequence
Northeastern United States blackout in 2003	Alarm system failure due to software bugs	More than 50 million consumers lost electricity
Italy blackout in 2003	Cascading failures between power and communication infrastructures	About 56 million people across Italy were affected
Arizona blackout in 2007	Unexpected activation of the load shedding program	About 100,000 customers lost 400 MW load
Florida blackout in 2008	Disbled relay protection during a diagnostic process	About 1 million customers lost 3,650 MW load
Southern China blackout in 2008	Cyber-physical coupling failures transmission towers collapsed due to severe ice storm and accretion	About 53,982 industrial customers and 6.42 million resident customers lost 14.82 GW load

Southwest United States blackout in 2011	Monitoring equipment failure at a substation	More than 2.7 million consumers lost electricity
Ukraine blackout in 2015	Remote cyber intrusions after the malware installation	Around 2.7 million consumers lost electricity
Xiamen blackout in 2016	Failures of optical fibers and transmission lines due to violent Typhoon Meranti	About 3 million people were affected
Venezuela blackout in 2019	several cyber-attacks resulting in massive blackouts	About 20 million people were affected

The necessity of attack detection and efficient control of the physical system in order to maintain the system resiliency against the CA is one of the current areas of research [14-17]. This paper offers a thorough examination of the methodologies presented in various papers, uniquely categorizing defense mechanisms against CAs. This distinction sets it apart from existing review papers, which lack such comparative analyses. Furthermore, this article breaks new ground by providing a comprehensive introduction to prerequisite topics, including the different types of CAs, the susceptibility of MG communication systems to these attacks, and the various types of control structures. This holistic approach ensures that readers gain a solid understanding of the topic, surpassing the level of comprehensiveness found in other review papers. Fig 1 shows the research trend of recent papers in the context of MG control against CAs and related keywords. As can be seen, the fundamental keywords in this topic mainly include attack, denial of service (DoS) attack, false data injection (FDI) attack, algorithm, control method, proposed controller, resiliency, communication link, agent, time delay, smart grid, DC microgrid, renewable energy and DGs.

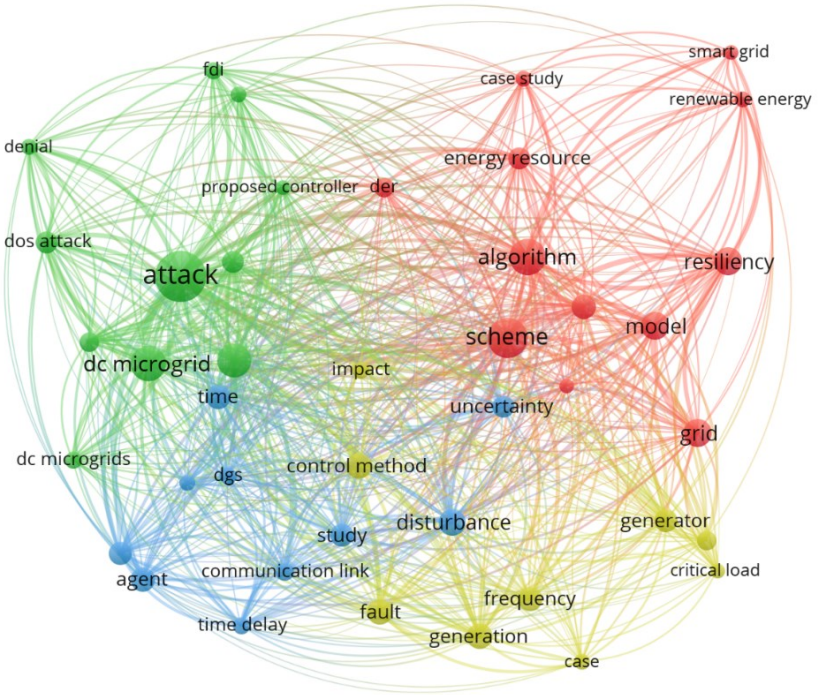


Fig. 1 Research Trends in The Context of MG Control Against CAs

The introductory section of the paper establishes the importance of control over CAs and provides a historical overview of CAs in the power system. Subsequently, the following section classifies the operational conditions of MGs based on cyber and physical security considerations. Furthermore, the paper proceeds to delineate the categorization of different types of CAs. Considering that CAs primarily target the communication infrastructure, it becomes crucial to expound on the communication system and its modeling (Section 4) to effectively address MG control against CAs (Section 5). Consequently, the paper delves into the various types of

communication systems and provides a comprehensive understanding of their characteristics. Moving forward, section 6 presents a classification of defense mechanisms against CAs based on current literature, accompanied by a review of pertinent papers in Table 2. The literature review offers concrete examples of these defense mechanisms, highlighting their dependence on the type of CAs and the nature of the communication system (centralized, decentralized, or distributed). In the final section, a summary of the paper is presented, encompassing both the conclusions drawn from the reviewed papers and an overview of future trends in the field.

2. Classification of MG Operational Conditions

In recent years, due to the rapid development of communication technologies and control theories, MG as a CPS has attracted much attention. MGs include the physical layer and the cyber layer which takes care of control, computing and communication functions [18-20]. The cyber system of MG gathers, transfers, processes, shows and saves the data of MG operation through data streams [21-23]. The data is displayed as monitoring and measuring data, control rules and MG settings. It is clear that effective and trustworthy data streams are necessary for the management of continuous physical processes [24-25].

The operational conditions of a MG with physical-cyber interactions can be categorized into 4 modes (Fig 2) [9, 26-29]:

- Secure mode: both cyber security and physical security are retained. In this mode, MG will operate normally.

- Alert mode: physical security is retained but cyber security is destroyed. In this mode, the monitoring control rules are blocked and the equipment must be able to stabilize the physical process using its default settings.

- Emergency mode: cyber security is retained but physical security is destroyed. In this mode, the events such as outage of a line, generator, over/under voltage, frequency drifts and increased line currents happen.

- Extreme mode: both cyber security and physical security are destroyed at the same time. In this mode, a natural disaster destroys both physical equipment and communication network.

Generally, there are four types of reactions for safer mode recovery [9, 30-31]:

- Preventive control: by recovering cyber security and retaining physical security, it restores the secure mode from the alert mode.

- Corrective control: by recovering physical security and retaining cyber security, it restores the secure mode from the emergency mode.

- Remedial control: restores the emergency mode from extreme mode by removing any cyber insecurity and stopping further destruction of physical security.

- Restorative control: restores the alert mode from extreme mode by removing any physical insecurity and stopping further destruction of cyber security.

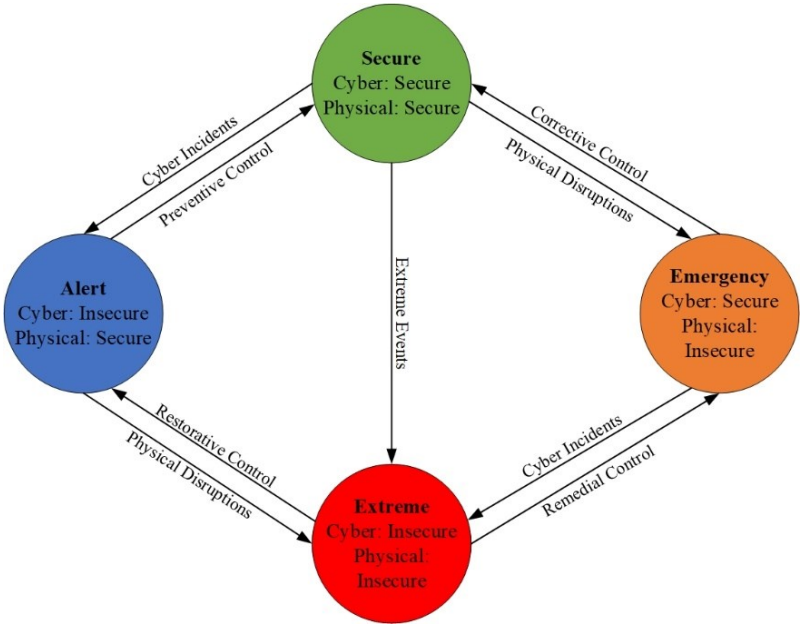


Fig. 2 Operational Conditions of MG [9, 26-29]

3. Classification of Cyber-Attacks in MGs

High reliance on communication networks makes the system vulnerable to CAs. In order to detect and control CAs, the modeling of MG communication network is essential, which will be explained in the next section. CAs not only cause damage to the cyber layer, but may also damage the physical layer. In such cases, CAs causes destruction of the system and the destroyed system does not follow the commands sent to it. Thus, the attack leaves the cyber layer and the physical layer will deal with the effect of the attack [32-35].
There are different types of CAs. The most important categories of attacks include the following:

- **Deception attack**

This attack is also called FDI. In this attack, the data integrity of the sent packets changes between different cyber segments. Deception attacks involve one or more components (sensors, actuators, or controllers) that receive false data and believe it to be true. For example, Stuxnet is a well-known malware worm which has the ability to reprogram code in programmable logic controllers (PLCs) in supervisory control and data acquisition (SCADA) systems [36-41]. In FDI attack, data packets are randomly generated or mathematically formulated. A simple modeling of these attacks is the addition of false data to the original sent data before it reaches the receiving module, as shown in (1):

$$x_r = x_s + x_f \tag{1}$$

where x_f is false data, which can be a constant dc bias injection or a time varying function, x_s is sent data, and x_r is received data [42-43].

- **Denial of service (DoS)**

A DoS attack is an attack in which an attacker sends too many requests to a part of the control system, causing it to overuse its resources. In this condition, due to the high volume of processing,

the system suffers from interruptions or malfunctions, or even becomes completely inaccessible. DoS attacks may target cyber systems or physical systems. These attacks target communication links or attempt to disable programs that control the system, data and communications [44-47]. In DoS, the receptor cannot receive the data sent by the sender. The attacker sends the same data from different sources to the receptor until the communication links is lost. Let μ be a criterion variable for receptor availability that becomes zero during an attack [42–43]. Eq. (2) indicates a simple modeling of DoS attacks.

$$x_r = \mu x_s \tag{2}$$

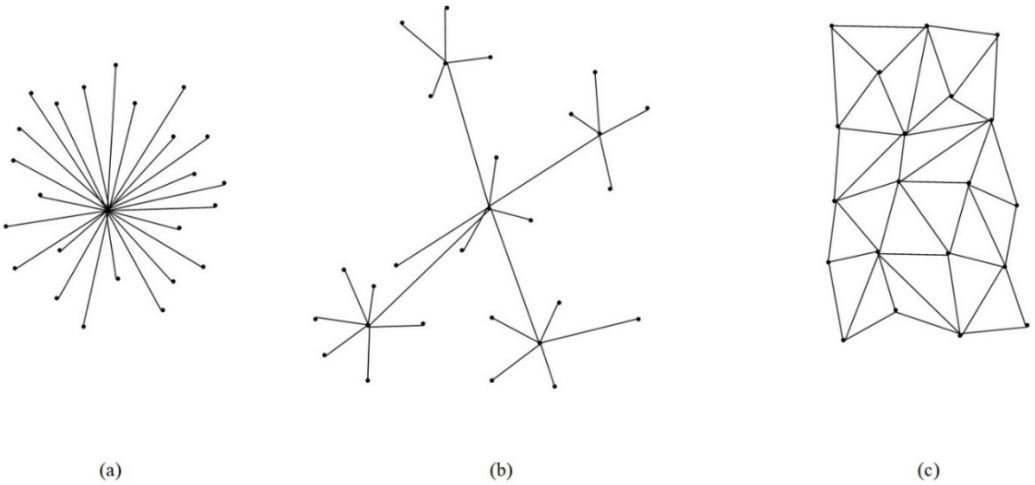
- **Replay attack**

Replay attacks are a special type of deception attack. In this attack, the attacker first records the measurements from the sensors. Then, the manipulated data is replaced with a log file, which worsens the performance of the control system and potentially allows other types of physical attacks without being detected. Such an attack cannot be easily detected due to the ability to check the cryptographic keys. In this attack, the attacker sends the previously tracked data to the receptor without any changes. For example, when a fault happens in the power system, the attacker can send data during normal condition, which causes the operation center to wrongly think that the system is still in normal condition. Consequently, the error processing time increases and the impact of the error extends due to the ignorance of the protection system. On the other hand, when the power system is in normal condition, sending data during an error condition, causes the control center to give a wrong control command [40, 48-49]. Let $x_h = (x_y, x_{y+1}, \ldots, x_{y+n})$ be a set of old data packets saved by the attacker [42-43]. A simple modeling of DoS attacks had been represented by (3).

$$x_r = x_s + x_h \tag{3}$$

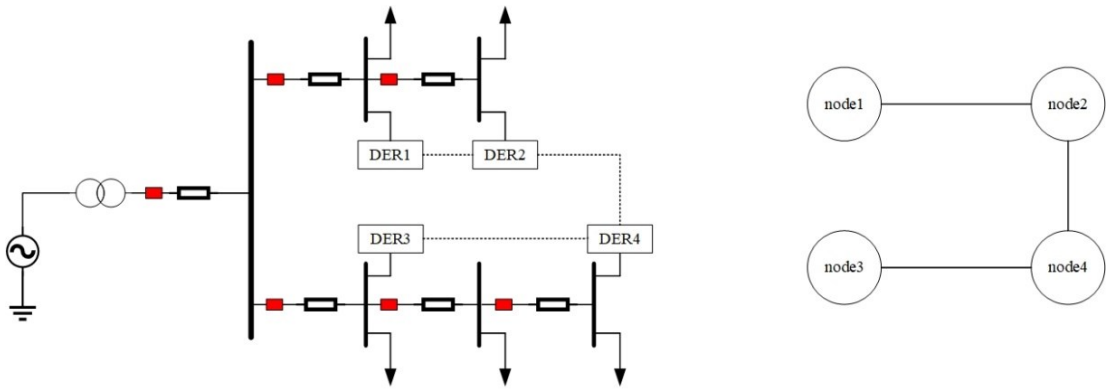
4. MG Communication System

As mentioned in the literature, it is necessary to model MG communication system for investigating the effect of CAs. Consider an islanded MG with *N* controllable inverter-based DERs. Depending on their role in the various control states, the resources participate in regulating the voltage and frequency of MG or the power supply of the MG loads. In the communication system, the DERs as agents exchange data with neighbors through communication links. Generally, agents are independent units that are developed based on a bottom-up approach. They process the information and share it with other agents. Communication systems can be centralized, decentralized and distributed. Centralized systems are multi-agent systems (MASs) where all agents are directly connected to a central agent. Decentralized systems break the process done in centralized systems into smaller parts only. In this way, several agents are connected to a central node, and the central nodes are connected with the main node of the entire network. In distributed systems, all agents are locally connected with their neighboring agents, and no agent plays a central role. Fig 3 displays the interaction of controllers or nodes for various control systems. Centralized systems need high bandwidth communication channels and are more vulnerable to attacks in the communication links. Generally, in the equivalent graph of the communication network of a MG, the nodes are DERs and the lines are their communication links [50-52]. Fig 4 (a) and (b) shows a simple MG with 4 DERs and their communication links and its corresponding graph, respectively.



(a) (b) (c)

Fig. 3 (a) Centralized System (b) Decentralized System (c) Distributed System [50-52]



(a) (b)

Fig. 4 (a) Simple MG with 4 DERs (b) Corresponding Graph

The theory of MASs describes the relationship between nodes and lines in MG communication system [53-57]. Considering MASs, the communication topology is described by an indirect graph [58-65].

It is assumed that each DER is considered as an agent. Therefore, there are N agents that are governed by the relationships of the first-order dynamic systems. The set $V = \{1, 2, \ldots, N\}$ represents all the agents or in other words the nodes of the graph. The graph $G = (V, E)$ also indicates how the agents interact. E is the set of all links among agents, which is a subset of Cartesian multiplication V. In other words, E is a subset of $V \times V$.

Also, each agent i has the information in the form of a variable such as x_i, which is changed and updated in interaction with neighboring agents. All neighboring agents of agent i are represented by the symbol N_i where $N_i = \{j \in v\ (i, j)\}$. The $x(t)$ vector also contains information about all the agents at moment t. In other words, this vector consists of a column and N rows, each row of which corresponds to one of the agents and is defined as follows:

$$x^T(T)=[x_1(t),x_2(t),...,x_N(t)] \tag{4}$$

Thus, the information of each agent can be updated by the following relationship. The rate of

update corresponding to the agent i is equal to the sum of the difference between this agent and its neighbors.

$$\dot{x}_i(t) = \sum_{j \in N_i} (x_j(t) - x_i(t)), \quad x_i(0) \in R \tag{5}$$

It should be noted that the above relationship is established in a situation where no weight is provided for the communication links among the agents. When the graph of communication links is considered weighted, this relationship will change as follows:

$$\dot{x}_i(t) = \sum_{j \in N_i} a_{ij}(x_j(t) - x_i(t)), \qquad x_i(0) \in R \tag{6}$$

where a_{ij} represents the weight of the communication link between agent i and agent j. The above relationships can be written in the form of a matrix:

$$\dot{x} = -Lx(t) \tag{7}$$

where L is called the Laplacian matrix of graph. The Laplacian matrix stores the basic properties of a graph, and by examining it, one can understand all the properties of a graph. This matrix is defined by the following formula:

$$L = D - A \tag{8}$$

where A is the adjacency matrix of the graph and its elements are weighted equal to a_{ij}. Also, D is the matrix of the graph degree. This is a diagonal matrix which principal diameter elements are equal to the sum of the corresponding row elements in the adjacency matrix, in other words:

$$D_{ii} = \sum_j a_{ij} \tag{9}$$

It is thus quite clear that each of the elements of the Laplacian matrix will be valued in the following order:

$$l_{ij} = \begin{cases} -1 & j \in N_i \\ N_i & j = i \end{cases} \tag{10}$$

Likewise, by referring to the relationships, it can be easily shown that the sum of the rows of the Laplacian matrix will be equal to zero. So, if I is an N vector symbol that all elements are equal to 1, we have:

$$l_{ij} = \begin{cases} -a_{ij} & j \in N_i \\ \sum_j a_{ij} & j = i \end{cases} \tag{11}$$

This relationship implies that the Laplacian matrix of any graph (regardless of whether it is weighted or not or connected or not) will always have at least an eigenvalue of zero. This eigenvalue called the explicit eigenvalue of the Laplacian matrix, corresponding to eigenvector 1.

5. MG Control Against CA

As mentioned, CPSs such as smart energy systems have attracted a great deal of attention in recent decades. These systems are vulnerable to CAs due to the presence of cyber layers. Therefore, designing a controller that is resilient and robust against the attacks is one of the new research trends in this field [66-68]. The resilience and robustness are two distinct and fundumental characteristics in the field of power systems, but sometimes they are mistakenly considered the same [24]. Resilience is a real-time active response to severe and unexpected incidents, whereas robustness is the passive maintenance of control function under a certain range of perturbations [69]. In other words, a robust and resilient MG must have CA prevention, CA detection and isolation and MG efficient control against CA [70]. To well manage MG's operation against CAs, the concepts of large-scale systems (LSSs) control should be applied.

5.1. Large-Scale Systems Control

LSSs can be used for several MGs. LSSs control is generally divided into three categories: centralized, decentralized and distributed. In centralized manner, controlled systems consist of separate and independent subsystems, with separate controllers for each of their quantities. All calculations are performed in the central controller and the control command is sent to the actuators. Designing centralized controller for LSSs will be very complex due to computational complexity, reliability realization, and communication bandwidth constraints. In decentralized control, a set of controlled systems consists of subsystems that are considered as separate controllers for each. But unlike centralized control, there are interactions among subsystems, and the weaker the interactions, the closer they are to the optimal state. Distributed control of LSSs is actually a subset of a decentralized control strategy in which the controllers of the subsystems exchange information with each other. Hence, it has higher reliability than the centralized control and decentralized control systems [71-72]. Hierarchical control of LSSs is a compromise between fully centralized control and fully decentralized control, in which the upstream control layers command the downstream control layers [73-75]. In general, hierarchical control has three layers of primary control, secondary control and tertiary control The main difference between control layers is their response speed and the infrastructure they require. In hierarchical control, the closer to the physical layer (the lowest control layer), the faster the controllers operate. In the system with droop control, each of the primary, secondary, and tertiary structures can be implemented on the basis of centralized, decentralized, or distributed control. Primary control, known as local control, is dedicated to controlling local variables such as frequency and voltage as well as current injection. These local controllers include the implementation of droop control and virtual impedance control techniques in each of the distributed power electronic converters connected to the microgrids. The most important features of this layer are more speed than secondary and tertiary layers and no need for communication links. The secondary control acts as an automatic generation control (AGC) and eliminates the steady-state error of the voltage and frequency of the microgrids. Tertiary control optimizes the operation of the microgrid and regulating its interactions with the distribution network by setting the active and reactive power references for each DG unit. This optimization is usually based on an economic criterion that determines the balance between demand and energy supply [76-79].

5.2. MG Control Strategies in Presence of CA

The structure of a MG including physical layer and cyber layer is shown in Fig 5. As can be seen, the physical layer includes different types of DERs such as photovoltaic panels, wind turbines,

ESSs along with their power electronic converters. The cyber layer consists of control and communication parts. The control of inverters is based on the LSSs control methods. Secondary control is at risk of CAs due to the use of communication links. Therefore, a resilient control method against CAs is vital [80-84]. CAs are mainly carried out on sensors (e.g., Remote Terminal Units (RTUs) and Phasor Measurement Units (PMUs)), actuators (e.g., angle changer for solar panels, rotor speed changer of wind turbines and protective relays), control layers with communication links. The performance of cyber layer, including the manner of sending measured data by sensors and receiving control commands by actuators, is demonstrated in Fig 6. As can be seen, sensors measure data in the physical system. Then, the measurement data is given to the controllers through the communication system. After controlling the parameters based on the desired goals, the controllers transmit the control commands created by the control system to the actuators through the communication system. Finally, actuators execute the desired command in the physical system [31, 41, 85-87].

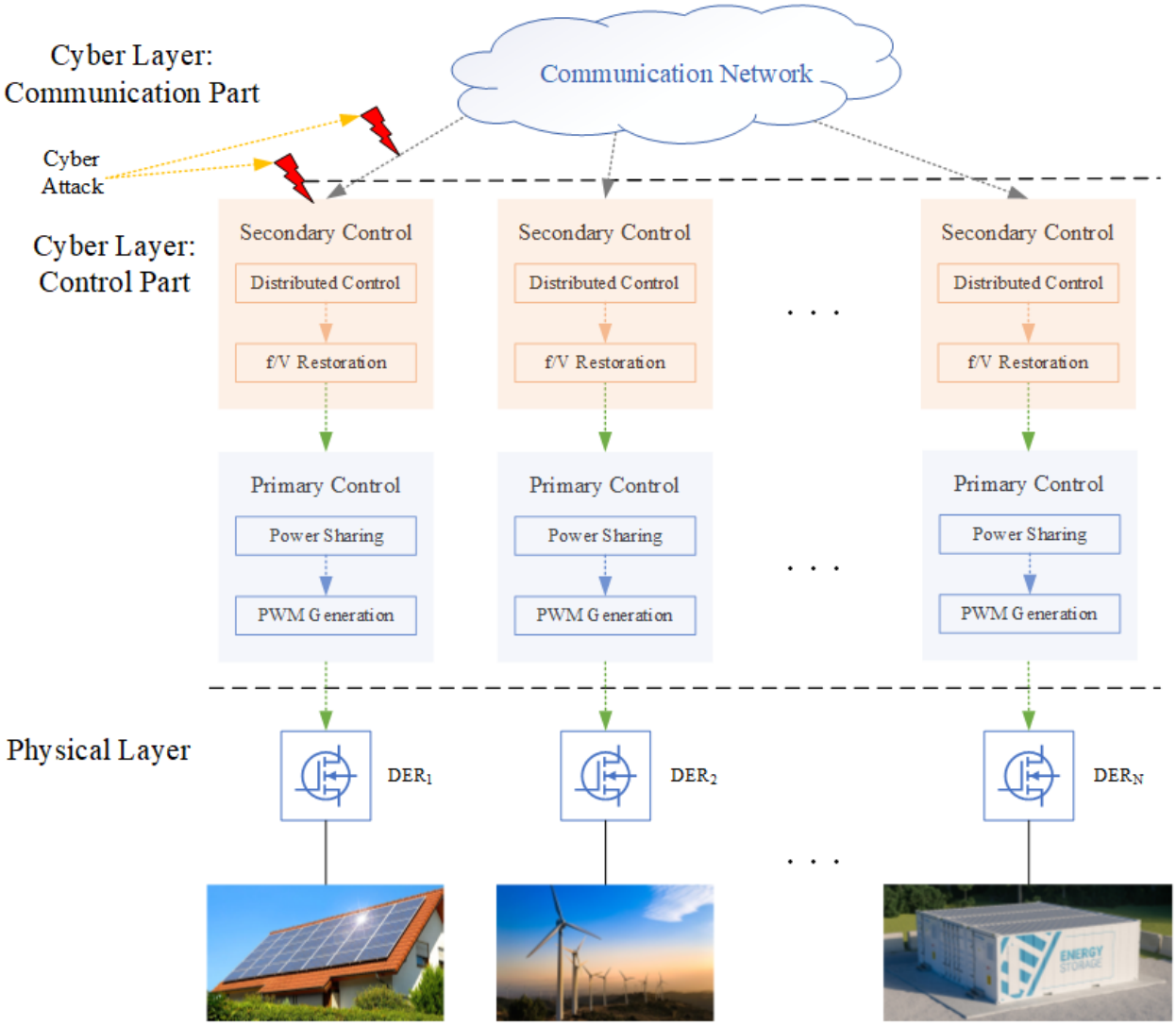


Fig. 5 A MG with Cyber and Physical Layers

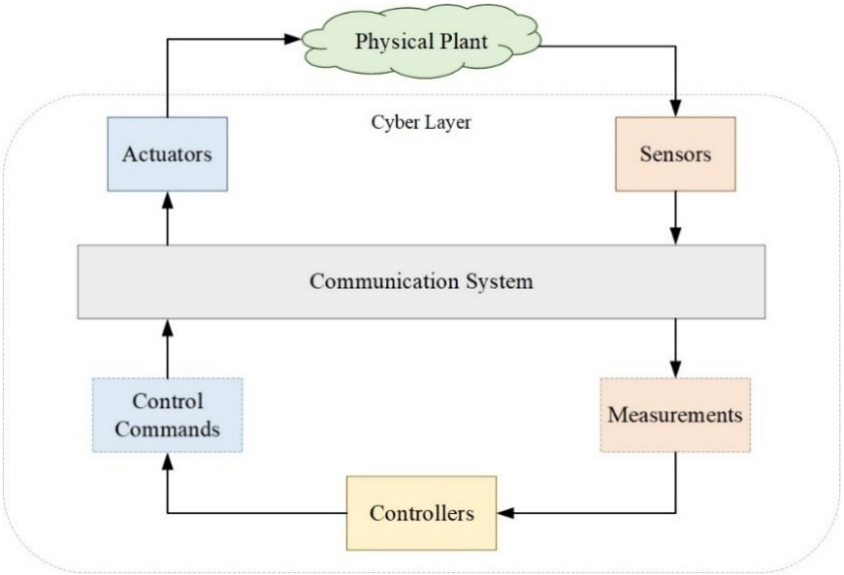


Fig. 6 The Performance of MG Cyber Layer

According to the duty of each DER in MG, inverters can have two roles: grid-following converters for control of the active and reactive power supplied to MG and grid-forming converters for control of the voltage and frequency of MG. Another common type of converters can play both roles to some extent through droop control [88-92].

In grid-following converters or PQ controllers, the active and reactive output powers of each converter are maintained at predetermined values. This type of controller always tries to maintain its output power, regardless of the operation mode of MG. [93-96]. The power converter acts as a current source. In the PQ controller with droop, the main purpose is not only to supply the load, but also to regulate the voltage and frequency of MG. The operation of this power converter is often regulated by an upstream controller such as the maximum power point tracking (MPPT) controller or the power plant controller operator that determines the P and Q references. Inner control loop in PQ controller regulates the injected current into the MG. Outer control loop determine the current reference of the inner loop to adjust the injected power to the MG [97-100].

In grid-forming converters or V/f controllers act similarly to the controllers of synchronous generators. That is, they use active power to control the frequency and reactive power to control the voltage. In fact, they play the role of the main grid in the islanded mode. V/f controllers regulate the frequency of MG and the voltage that will supply the loads. The power converter acts as an ac voltage source. In the V/f controller with droop, the main purpose is not only to regulate the voltage and frequency of MG but also control the active and reactive power delivered by the power converter [101-103]. The controller is implemented using two cascaded synchronous controllers in the d-q reference framework. The inputs of the control system are the reference values of the voltage magnitude and frequency at the point of common coupling (PCC) of MG. The outer control loop controls the voltage of MG. Besides, the inner loop regulates the fed current by the converter with the aim of tracking the generated current reference by the outer voltage control loop. It should be noted that there must be a grid-forming converter to control the voltage and frequency of MG in the islanded mode [104-105].

Fig 7 illustrated the structure of a (V/f)/(PQ) controller with droop along with the vulnerable points against CA. As explained earlier, the vulnerable points are sensors, communication links of

secondary control with the neighbor agents and another control layers. After CAs, the control system changes according to the considered defense mechanism, which is reviewed in next section [106-108].

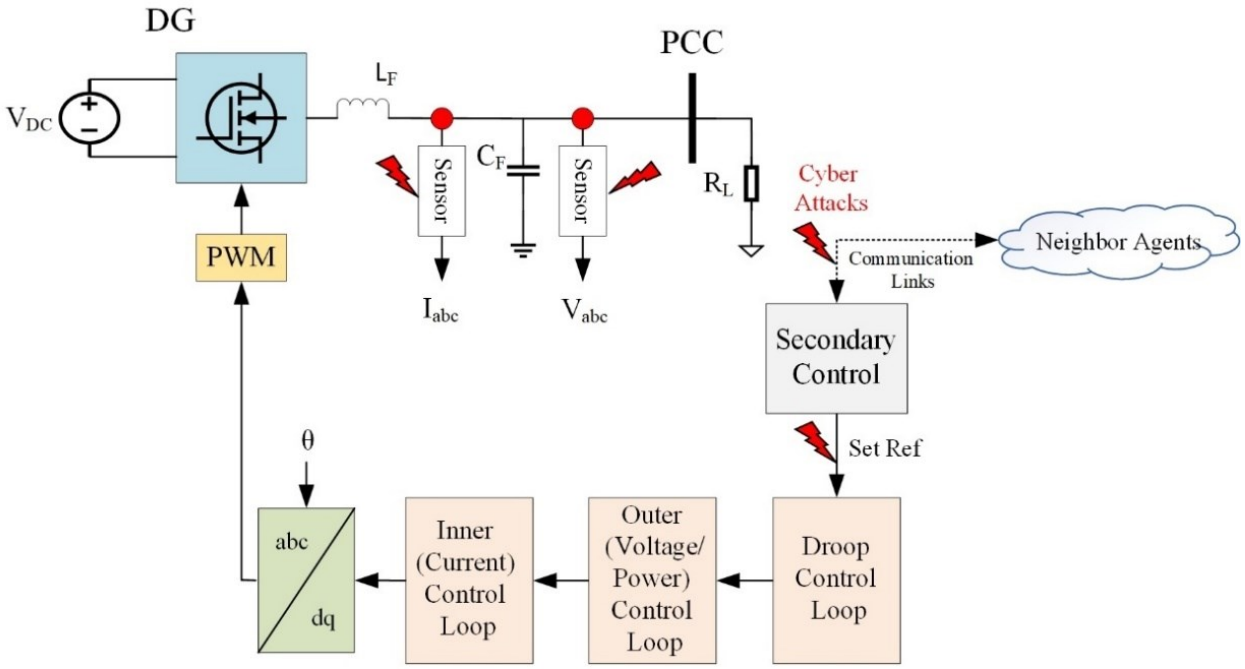


Fig. 7 The structure of a (V/f)/(PQ) controller with droop along with the vulnerable points against CA

6. Defense Mechanisms Against CA

To maintain the security of CPSs against various CAs, appropriate defense mechanisms should be designed. In the available researches, defense mechanisms can be divided into three categories [109-112].

- Prevention mechanism: this defense mechanism postpones the attack. Prevention algorithms are important in the face of CAs as the first defense mechanism of CPSs.
- Resilience enhancement: this defense mechanism improves tolerating the maximum effect of attack and helps operating in the closest possible state to normal.
- Detection and isolation: this defense mechanism detects the source of the attack, isolates the damaged subsystems and restores normal state as soon as possible.

The effect of these defense mechanisms is shown in Fig 8. As can be seen, the prevention algorithms delay the attack initiation time. Resilience algorithms reduce the effect of attack or in other words increase tolerance against attack. Also, the detection and isolation algorithms mitigate the effect of attack after isolation time. In fact, after the attack is isolated, there is no more attack in a CPS [31, 113-115].

Some efforts on CPSs and cyber threats problems, namely, CA prevention algorithms, CA detection and isolation algorithms, fault-tolerant control, CA mitigation, and resilient control in the presence of attacks, have been investigated in [116-117]. Moreover, table 2 shows the review of available references on CPS control against cyber threats.

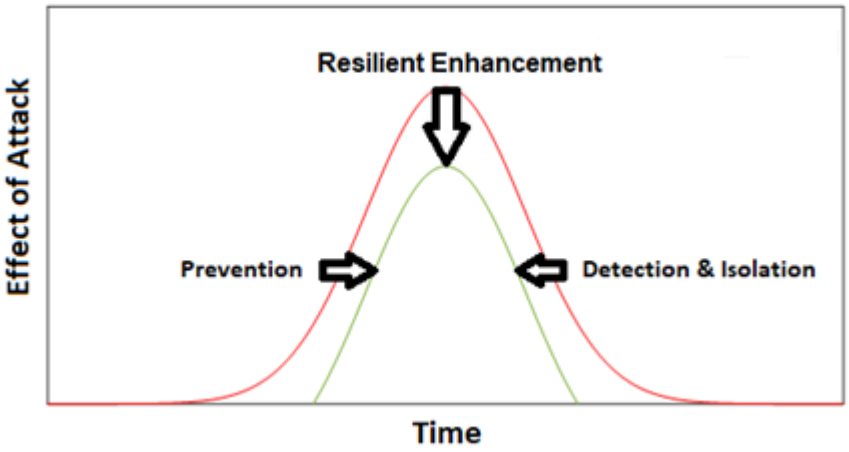


Fig. 8 The Effect of Defense Mechanisms [31, 113-115]

Table 2 Review of Available References on CPS Control Against Cyber Threats

Taxonomy	Ref	Year	Types of Attack	Description
Prevention Algorithm	[118]	2016	DoS attack	An immune system for improving the accuracy rate of attack prevention and reducing the false alarm rate
	[119]	2020	HELLO flood attack (a type of DoS)	Using optimized deep learning method in clustering and optimal shortest path selection
	[120]	2018	Man in the Middle attack	Using lightweight encryption for Intrusion Prevention System (IPS)
	[121]	2019	DoS attack	Design and implementation of an Intrusion Detection and Prevention System (IDPS) using Software-Defined Networking (SDN)
	[122]	2020	Aging attack	Forecasting attacks by means of convex optimization and Lyapunov method
	[123]	2016	Cloud-based attack	Classify cloud-based attacks and provide a taxonomy and intrusion detection and prevention as a service
	[124]	2018	Unknown	Attack detection and prevention in Siemens S7 1200 PLC by means of mirroring technique
	[125]	2016	DoS attack	Trust-based intrusion detection and prevention technology
	[126]	2018	Cybercrime such as ransomware	Factor analysis of information risk model combined with Crime Prevention Through Environmental Design (CPTED)
	[127]	2022	Man in the Middle attack	Proposal of a regression modelling technique
Detection and Isolation Algorithm	[16]	2020	Stealth attack	An event-driven resilient strategy for dc microgrids, which immediately replaces the attacked signal with a trusted event-driven signal constructed using True transmitted measurements
	[40]	2020	FDI and Replay attack	Using the Weighted Mean Subsequence Reduced (W-MSR) algorithm for attack detection
	[57]	2020	Time-varying attacks on communication links and controllers	Proposing a resilient distributed control for detection and isolation of corrupted communication links and controllers
	[86]	2019	Bias injection attack	Applying a distributed detection and isolation scheme on the IEEE 8-bus and IEEE 118-bus smart energy grid system
	[128]	2020	FDI attack	Proposing cyber-threat detection and mitigation technique that relies on a Kullback-Liebler divergence-based criterion in DC MG
	[129]	2022	FDI attack	Designing robust H-infinity observers based on linear matrix inequalities (LMIs) for attack isolation (AI) and attack location (AL)
	[130]	2022	FDI attack	Proposing a distributed CA detection method in communication channels for a class of discrete-time, nonlinear, heterogeneous, multi-agent systems controlled by our formation-based controller
	[131]	2017	Replay attack	Proposing a multiplicative watermarking scheme, where each sensor's output is separately watermarked by being fed to a single input single output (SISO) watermark generator, for detection and isolation of replay attacks on sensor measurements
	[132]	2022	FDI attack	Designing a robust attack detector based on the mixed H_{-}/H_{∞}
	[133]	2019	FDI attack	A nonlinear unknown input observer -based distributed detection method and a distributed isolation scheme with two steps (isolation of the possible actuator attack set and the possible subarea attack set) applied on IEEE 28-bus and IEEE 128-bus
	[134]	2019	Replay attack	A frequency-based approach for the detection of attacks by employing a sinusoidal signal with a time-varying frequency (authentication signal) into the closed-loop system
	[135]	2020	Covert cyber attack	Achieving detection and isolation by associating the controller with two observers for a class of interconnected system, estimating the states of the plant by means of the observers and comparing the estimated states to determine
	[136]	2018	FDI attack	Proposing an observer-based algorithm for detection and isolation of CA by using real-time synchrophasor measurements.
	[137]	2018	Malicious attack on the communication link	Adopting a model-based approach in order to detect anomalies, formalizing the problem as a binary hypothesis test in a linear system equipped with a Model Predictive Controller (MPC)
	[138]	2007	Wormhole attack	Presenting a lightweight countermeasure for the wormhole attack (called LiteWorp) relying on overhearing neighbor communication.
	[139]	2020	Unknown	A new approach to model the closed-loop system subject to control delays and attacks in networked control system
	[140]	2018	Unknown	A benchmark for the detection and isolation of CA in a non-linear controlled interconnected system based on a two tank system
	[141]	2022	Unknown attack vectors	A new sliding mode observer (SMO)-based attack detector with parameter adjustment using an optimization algorithm
	[142]	2022	Malicious attack	Introducing a stacked deep learning method to detect malicious attacks in SCADA systems
	[143]	2022	Kernel attack	Reliable attack detection without loss of control performance.
	[144]	2022	Unknown	Detection of cyber-attacks on communication links between smart devices based on Convolutional Neural Networks (CNN)
	[145]	2022	FDI attack	Proposing extremely randomized trees algorithm in smart grids (on IEEE 14-bus, 30-bus, 57-bus and 118-bus systems)
Resilient Algorithm	[36]	2022	FDI attack	Event-triggered adaptive sliding mode control (ASMC) for the CPSs, the adaptive technique for estimating the upper bound of the attack and Lyapunov's stability theory for proving the admissibility of the formed event-triggered ASMC design scheme

	[39]	2019	Deception attack	Resilient consensus control of discrete-time complex CPSs
	[44]	2021	DoS attack	Resilient observer-based control for CPSs with multiple transmissions and applying linear matrix inequalities (LMIs)
	[46]	2019	DoS attack	Designing a set of partial observers for estimating partial states corresponding to different channels and using the finite-time observer technique and a switching scheme for resilient observer-based controller
	[47]	2020	DoS attack	Distributed resilient control problem of a class of CPSs for more general heterogeneous linear multiagent systems (MASs) with nonuniform communication delays
	[53]	2020	Malicious data injection attack	The consensus problem of the multi-agent systems by means of a competitive strategy for establishing a hidden layer of virtual system interconnected with the original system
	[61]	2022	DoS attack	Distributed resilient control based on the average consensus algorithm in DC microgrids with constant power load
	[109]	2020	FDI attack	Distributed resilient control in islanded MGs for frequency/voltage restoration, fair real power sharing, and state-of-charge balancing in MGs with multiple ESSs in abnormal condition
	[146]	2018	DoS attack	resilient strategy for a class of CPS in wireless network between sensor and remote estimation
	[147]	2018	DoS attack	Proposing a novel event-triggered control strategy for CPSs with disturbance and measurement noise
	[148]	2019	DoS attack	A resilient distributed event-triggered secure consensus scheme for multi-agent systems (MASs)
	[149]	2020	Stochastic attacks	An observer-based event-triggered output feedback control for fractional-order CPSs with stochastic network attacks
	[150]	2020	DoS attack	A resilient consensus-based distributed control strategy of a platoon of automated vehicles
	[151]	2019	Stochastic attacks	An improved adaptive event-triggered control for a class of networked control systems to reduce the unnecessary data transmissions
	[152]	2020	DoS attack	Design of the resilient decentralized sampled-data filter for linear interconnected systems by means of Lyapunov function-based method
	[153]	2020	min-max, surge, geometric, and replay attacks	resilient operation strategies for nonlinear processes by a modified Lyapunov-based Economic Model Predictive Controller (LEMPC)
	[154]	2020	malicious actuator attack	A new secure control scheme (SCS) with a robust dynamic compensation for CPSs
	[155]	2020	jamming attacks	Resilient tracking control (a novel model-free adaptive control (MFAC)) for nonlinear unknown CPS in the wireless transmission channel
	[156]	2021	FDI attack	An adaptive integral sliding-mode control scheme for developing the attack tolerant controller by using the Lyapunov stability theory
	[157]	2021	Deception attack	resilient adaptive dynamic surface control for a class of switched nonlinear CPSs by applying Lyapunov function and neural networks for approximating the nonlinear terms
	[158]	2022	Covert attack	A resilience-based frequency regulation scheme in an isolated MG under different operational conditions, such as, step and random change in load and different wind speed patterns
	[159]	2021	DoS attack	A novel gain-switched observer-based resilient control scheme with the utilization of an equivalent switching control method
	[160]	2021	DoS and random deception attack	A new switched stochastic time-delay closed-loop system under sampled-data and full state feedback controller by utilizing piecewise Lyapunov-Krasovskii functional analysis theory
	[161]	2022	DoS attack	An observer-based sliding mode control (SMC)) for estimating the relative acceleration between neighbor vehicles in connected vehicles
	[162]	2022	DoS attack	Resilient current controller design for the networked DC microgrid system with multiple constant power loads
	[163]	2022	DoS and random deception attack	A resilient optimized dynamic event-triggered mechanism (RODETM) for reducing the unnecessary costs of system operation and mitigating the impact caused by attacks
	[164]	2021	Periodic DoS attack	A novel attack-resilient event-triggered mechanism (ARETM) for formation shape problems of the system
	[165]	2022	FDI attack	An adaptive resilient control scheme by an improved sliding mode control strategy for Markovian jump CPS (MJCPS)
	[166]	2022	Asynchronous data injection attack	Proposing a two sides asynchronous Adaptive Event-triggered Resilient Control Scheme (AERCS) for CPSs
	[167]	2022	DoS attack	The resilient sliding mode control problem for cyber-physical systems (CPSs) with multiple transmission channels
	[168]	2022	Unknown actuator attack	Proposing a resilient control strategy by adopting Barrier Lyapunov function, Hyperbolic tangent sigmoid function, and the Nussbaum function for CPSs under actuator saturation resulting from cyberattacks
	[169]	2022	DoS attack	A resilient decentralized control for nonlinear interconnected systems with unknown control directions and a novel switched sampled-data observer and an adaptive control architecture for each subsystem

7. Conclusion and Future Trends

With the development of MGs as CPSs and the vulnerability of these systems against CAs due to the presence of communication systems, the problem of resilient control as well as detection and isolation of attacks has become important. In this paper, firstly, the operational conditions of the physical and cyber parts of CPS and necessary control to return to a more stable state were examined. In the following, the types of CAs and their impact on system performance were explained. Graph theory and system modeling were introduced for better understand of the communication systems performance. The three strategies to deal with cyber threats namely, prevention, detection and isolation, and resilient control were discussed afterwards. The available researches in this category were summarized. Finally, various control methods of inverter-based microgrids were reviewed.

The review of the paper found the following results:

- CAs are carried out on MG communication infrastructure. Therefore, secondary control and communication links are vulnerable to CAs.

- There are three types of defense mechanisms (prevention, detection & isolation and resilient algorithm) to protect the MG against CAs.

- Based on the type of attack, papers have made contributions on control and protection of MG against CAs, which are reviewed in this paper.

The future directions for research in the control of CPSs against CAs can be suggested as follows:

- Development of new methods for CA prevention, detection and isolation.

- Designing new resilient control methods to increase CPSs resilience. These methods can be based on conventional control methods or modern control methods and artificial intelligence.

- Retrofitting existing equipment (Cyber-Retrofit Services), accommodating advanced technologies into networks and using of methods such as the configuration modification of the microgrid or the use of multi-microgrids and exchange the energy between MGs, the use of methods such as load shedding in order to compensate for the generation in the isolated part caused by CA.

References

[1] Lamnatou, Chr, D. Chemisana, and C. Cristofari. "Smart grids and smart technologies in relation to photovoltaics, storage systems, buildings and the environment." *Renewable Energy* (2021).

[2] Molderink, Albert, et al. "Management and control of domestic smart grid technology." *IEEE transactions on Smart Grid* 1.2 (2010): 109-119.

[3] Salvi, Andrea, Paolo Spagnoletti, and Nadia Saad Noori. "Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem." *Computers & Security* 112 (2022): 102507.

[4] Peng, Chen, et al. "A survey on security communication and control for smart grids under malicious cyber attacks." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49.8 (2019): 1554-1569.

[5] Sen, Ömer, et al. "On using contextual correlation to detect multi-stage cyber attacks in smart grids." *Sustainable Energy, Grids and Networks* 32 (2022): 100821.

[6] Çelik, Doğan, and Mehmet Emin Meral. "Multi-objective control scheme for operation of parallel inverter-based microgrids during asymmetrical grid faults." *IET Renewable Power Generation* 14.13 (2020): 2487-2498.

[7] Shahidehpour, Mohammad, and Joseph F. Clair. "A functional microgrid for enhancing reliability, sustainability, and energy efficiency." *The Electricity Journal* 25.8 (2012): 21-28.

[8] Guo, Qinglai, et al. "Power system cyber-physical modelling and security assessment: motivation and ideas." *Proceedings of the CSEE* 36.6 (2016): 1481-1489.

[9] Li, Zhiyi, Mohammad Shahidehpour, and Farrokh Aminifar. "Cybersecurity in distributed power systems." *Proceedings of the IEEE* 105.7 (2017): 1367-1388.

[10] Xu, Luo, et al. "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective." *Renewable and Sustainable Energy Reviews* 152 (2021): 111642.

[11] Liang, Gaoqi, et al. "The 2015 ukraine blackout: Implications for false data injection attacks." *IEEE Transactions on Power Systems* 32.4 (2016): 3317-3318.

[12] T. Liu and T. Shu, "On the security of ANN-based AC state estimation in smart grid," *Computers & Security,* vol. 105, p. 102265, 2021.

[13] H. Long, Z. Wu, C. Fang, W. Gu, X. Wei, and H. Zhan, "Cyber-attack detection strategy based on distribution system state estimation," *Journal of Modern Power Systems and Clean Energy,* vol. 8, no. 4, pp. 669-678, 2020.

[14] Priyadharshini, N., S. Gomathy, and M. Sabarimuthu. "A review on microgrid architecture, cyber security threats and standards." *Materials Today: Proceedings* (2020).

[15] Shan, Yinghao, Anqi Pan, and Huashan Liu. "A switching event-triggered resilient control scheme for primary and secondary levels in AC microgrids." *ISA transactions* (2022).

[16] Sahoo, Subham, Tomislav Dragičević, and Frede Blaabjerg. "An event-driven resilient control strategy for dc microgrids." *IEEE Transactions on Power Electronics* 35.12 (2020): 13714-13724.

[17] Yuan, Minghan, et al. "Hierarchical control of DC microgrid with dynamical load power sharing." *Applied energy* 239 (2019): 1-11.

[18] Zhang, Yiwei, et al. "Modeling and vulnerability assessment of cyber physical system considering coupling characteristics." *International Journal of Electrical Power & Energy Systems* 142 (2022): 108321.

[19] Yohanandhan, Rajaa Vikhram, et al. "Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications." *IEEE Access* 8 (2020): 151019-151064.

[20] Jin, Ming, et al. "Energy-cyber-physical systems." *Applied Energy* 256 (2019): 113939.

[21] Orumwense, Efe Francis, and Khaled Abo-Al-Ez. "A systematic review to aligning research paths: Energy cyber-physical systems." *Cogent Engineering* 6.1 (2019): 1700738.

[22] Shi, Libao, Qiangsheng Dai, and Yixin Ni. "Cyber–physical interactions in power systems: A review of models, methods, and applications." *Electric power systems research* 163 (2018): 396-412.

[23] Jovanov, Ilija, and Miroslav Pajic. "Relaxing integrity requirements for attack-resilient cyber-physical systems." *IEEE Transactions on Automatic Control* 64.12 (2019): 4843-4858.

[24] Arghandeh, Reza, et al. "On the definition of cyber-physical resilience in power systems." *Renewable and Sustainable Energy Reviews* 58 (2016): 1060-1069.

[25] Hu, Fei, et al. "Robust cyber–physical systems: Concept, models, and implementation." *Future generation computer systems* 56 (2016): 449-475.

[26] Tobajas, Javier, et al. "Resilience-oriented schedule of microgrids with hybrid energy storage system using model predictive control." *Applied Energy* 306 (2022): 118092.

[27] Zhang, Dongdong, et al. "A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems." *Renewable Energy* (2022).

[28] Yang, Xiaodong, et al. "Impact analysis of cyber system in microgrids: Perspective from economy and reliability." *International Journal of Electrical Power & Energy Systems* 135 (2022): 107422.

[29] Khodaei, Amin. "Resiliency-oriented microgrid optimal scheduling." *IEEE Transactions on Smart Grid* 5.4

(2014): 1584-1591.
[30] Cai, Xingpu, et al. "Review of cyber-attacks and defense research on cyber physical power system." *2019 IEEE Sustainable Power and Energy Conference (iSPEC)*. IEEE, 2019.
[31] Sánchez, Helem S., et al. "Bibliographical review on cyber attacks from a control oriented perspective." *Annual Reviews in Control* 48 (2019): 103-128.
[32] Morris, Thomas H., and Wei Gao. "Industrial control system cyber attacks." *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1*. 2013.
[33] Liu, Yonggui, Ziyuan Li, and Zhiping Shen. "Resilient consensus of discrete-time connected vehicle systems with interaction network against cyber-attacks." *Journal of the Franklin Institute* 358.5 (2021): 2780-2800.
[34] Ogie, Robert Ighodaro. "Cyber security incidents on critical infrastructure and industrial networks." *Proceedings of the 9th International Conference on Computer and Automation Engineering*. 2017.
[35] Shi, Xingyu, et al. "Cyber-physical electrical energy systems: challenges and issues." *CSEE Journal of Power and Energy Systems* 1.2 (2015): 36-42.
[36] Xue, Yanmei, et al. "Event-triggered adaptive sliding mode control of cyber-physical systems under false data injection attack." *Applied Mathematics and Computation* 433 (2022): 127403.
[37] Zhuang, Peng, and Hao Liang. "False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks." *IEEE Transactions on Smart Grid* 12.3 (2020): 2566-2577.
[38] Reda, Haftu Tasew, Adnan Anwar, and Abdun Mahmood. "Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts." *Renewable and Sustainable Energy Reviews* 163 (2022): 112423.
[39] Fu, Weiming, et al. "Resilient consensus of discrete-time complex cyber-physical networks under deception attacks." *IEEE Transactions on Industrial Informatics* 16.7 (2019): 4868-4877.
[40] Yassaie, Negar, et al. "Resilient control of multi-microgrids against false data injection attack." *ISA transactions* 110 (2021): 238-246.
[41] Ding, Derui, et al. "A survey on security control and attack detection for industrial cyber-physical systems." *Neurocomputing* 275 (2018): 1674-1683.
[42] Rath, Suman, et al. "A cyber-secure distributed control architecture for autonomous AC microgrid." *IEEE Systems Journal* 15.3 (2020): 3324-3335.
[43] Tian, Jiwei, et al. "Data-Driven False Data Injection Attacks against Cyber-Physical Power Systems." *Computers & Security* (2022): 102836.
[44] Zhang, Chun-Lei, Guang-Hong Yang, and An-Yang Lu. "Resilient observer-based control for cyber-physical systems under denial-of-service attacks." *Information Sciences* 545 (2021): 102-117.
[45] Mahmoud, Magdi S., Mutaz M. Hamdan, and Uthman A. Baroudi. "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges." *Neurocomputing* 338 (2019): 101-115.
[46] Lu, An-Yang, and Guang-Hong Yang. "Resilient observer-based control for cyber-physical systems with multiple transmission channels under denial-of-service." *IEEE Transactions on Cybernetics* 50.11 (2019): 4796-4807.
[47] Deng, Chao, and Changyun Wen. "MAS-based distributed resilient control for a class of cyber-physical systems with communication delays under DoS attacks." *IEEE transactions on cybernetics* 51.5 (2020): 2347-2358.
[48] Zhao, Junfeng, Jing Wang, and Lei Yin. "Detection and control against replay attacks in smart grid." *2016 12th International Conference on Computational Intelligence and Security (CIS)*. IEEE, 2016.
[49] Li, Feng, et al. "A review of cyber-attack methods in cyber-physical power system." *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*. IEEE, 2019.
[50] Ma, Xiangyu, Huijie Zhou, and Zhiyi Li. "On the resilience of modern power systems: A complex network perspective." *Renewable and Sustainable Energy Reviews* 152 (2021): 111646.
[51] Xia, Lina, et al. "Leader-follower time-varying output formation control of heterogeneous systems under cyber attack with active leader." *Information Sciences* 585 (2022): 24-40.
[52] Li, Hongyang, Junfeng Zhang, and Xiao He. "Design of data-injection attacks for cyber-physical systems based on Kullback–Leibler divergence." *Neurocomputing* 361 (2019): 77-84.
[53] Dong, Hangning, Chaoyong Li, and Yonghe Zhang. "Resilient consensus of multi-agent systems against malicious data injections." *Journal of the Franklin Institute* 357.4 (2020): 2217-2231.
[54] Sharma, Desh Deepak, et al. "Agent-based distributed control schemes for distributed energy storage systems under cyber attacks." *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 7.2 (2017): 307-318.
[55] Rezaee, Hamed, Thomas Parisini, and Marios M. Polycarpou. "Resiliency in dynamic leader–follower multiagent systems." *Automatica* 125 (2021): 109384.
[56] Sahoo, Subham, et al. "Adaptive resilient operation of cooperative grid-forming converters under cyber attacks." *2020 IEEE CyberPELS (CyberPELS)*. IEEE, 2020.

[57] Zhou, Quan, et al. "A cyber-attack resilient distributed control strategy in islanded microgrids." *IEEE Transactions on Smart Grid* 11.5 (2020): 3690-3701.
[58] Mesbahi, Mehran, and Magnus Egerstedt. "Graph theoretic methods in multiagent networks." *Graph Theoretic Methods in Multiagent Networks*. Princeton University Press, 2010.
[59] Rocchetta, Roberto. "Enhancing the resilience of critical infrastructures: Statistical analysis of power grid spectral clustering and post-contingency vulnerability metrics." *Renewable and Sustainable Energy Reviews* 159 (2022): 112185.
[60] Shobole, Abdulfetah Abdela, and Mohammed Wadi. "Multiagent systems application for the smart grid protection." *Renewable and Sustainable Energy Reviews* 149 (2021): 111352.
[61] Ramasubramanian, Bhaskar, et al. "Resilience to denial-of-service and integrity attacks: A structured systems approach." *European Journal of Control* 63 (2022): 61-69.
[62] Iqbal, Muhammad, Zhihua Qu, and Azwirman Gusrialdi. "Distributed resilient consensus on general digraphs under cyber-attacks." *European Journal of Control* (2022): 100681.
[63] Severson, Tracie A., et al. "A resilient framework for sensor-based attacks on cyber–physical systems using trust-based consensus and self-triggered control." *Control Engineering Practice* 101 (2020): 104509.
[64] Alcaraz, Cristina, Javier Lopez, and Kim-Kwang Raymond Choo. "Resilient interconnection in cyber-physical control systems." *Computers & Security* 71 (2017): 2-14.
[65] Dibaji, Seyed Mehran, and Hideaki Ishii. "Resilient consensus of second-order agent networks: Asynchronous update rules with delays." *Automatica* 81 (2017): 123-132.
[66] Li, Zhiqiang, et al. "Robust resilient control for nonlinear systems under denial-of-service attacks." *IEEE Transactions on Fuzzy Systems* 29.11 (2020): 3415-3427.
[67] Chen, Xiaoli, et al. "Event-based fuzzy resilient control of nonlinear DC Microgrids under denial-of-service attacks." *ISA transactions* (2022).
[68] Aubouin, Bob, et al. "Resilient tube-based MPC for Cyber-Physical Systems Under DoS Attacks." *11th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes-SAFEPROCESS 2022*. 2022.
[69] Liu, Yun, et al. "Robust and resilient distributed optimal frequency control for microgrids against cyber attacks." *IEEE Transactions on Industrial Informatics* 18.1 (2021): 375-386.
[70] Hopkins, Stephen, Ezhil Kalaimannan, and Caroline Sangeetha John. "Cyber resilience using state estimation updates based on cyber attack matrix classification." *2020 IEEE Kansas Power and Energy Conference (KPEC)*. IEEE, 2020.
[71] Meng, Lexuan, et al. "Review on control of DC microgrids and multiple microgrid clusters." *IEEE journal of emerging and selected topics in power electronics* 5.3 (2017): 928-948.
[72] Ge, Xiaohua, Fuwen Yang, and Qing-Long Han. "Distributed networked control systems: A brief overview." *Information Sciences* 380 (2017): 117-131.
[73] Sen, Sachidananda, and Vishal Kumar. "Microgrid control: A comprehensive survey." *Annual Reviews in Control* 45 (2018): 118-151.
[74] Guerrero, Josep M., et al. "Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization." *IEEE Transactions on industrial electronics* 58.1 (2010): 158-172.
[75] Tan, Sen, et al. "Brief survey on attack detection methods for cyber-physical systems." *IEEE Systems Journal* 14.4 (2020): 5329-5339.
[76] Scattolini, Riccardo. "Architectures for distributed and hierarchical model predictive control–a review." *Journal of process control* 19.5 (2009): 723-731.
[77] Hou, Xiaochao, et al. "Distributed hierarchical control of AC microgrid operating in grid-connected, islanded and their transition modes." *Ieee Access* 6 (2018): 77388-77401.
[78] Sahoo, Subham. "Cyber security in power electronic systems." *Control of Power Electronic Converters and Systems*. Academic Press, 2021. 199-220.
[79] Çelik, Doğan, and Hafiz Ahmed. "Enhanced control of superconducting magnetic energy storage integrated UPQC for power quality improvement in EV charging station." *Journal of Energy Storage* 62 (2023): 106843.
[80] Alhasnawi, Bilal Naji, Basil H. Jasim, and Bishoy E. Sedhom. "Distributed secondary consensus fault tolerant control method for voltage and frequency restoration and power sharing control in multi-agent microgrid." *International Journal of Electrical Power & Energy Systems* 133 (2021): 107251.
[81] Guo, Fanghong, et al. "Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids." *IEEE Transactions on industrial Electronics* 62.7 (2014): 4355-4364.
[82] Smith, Edward J., Duane A. Robinson, and Ashish P. Agalgaonkar. "A secondary strategy for unbalance consensus in an islanded voltage source converter-based microgrid using cooperative gain control." *Electric Power Systems Research* 210 (2022): 108097.
[83] Dong, Jiawei, et al. "Secondary frequency regulation and stabilization method of islanded droop inverters based

on integral leading compensator." *Energy Reports* 8 (2022): 1718-1730.
[84] Lu, Lin-Yu, Hao Jan Liu, and Hao Zhu. "Distributed secondary control for isolated microgrids under malicious attacks." *2016 North American Power Symposium (NAPS)*. IEEE, 2016.
[85] Liu, Shichao, Peter X. Liu, and Xiaoyu Wang. "Effects of cyber attacks on islanded microgrid frequency control." *2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 2016.
[86] Luo, Xiaoyuan, et al. "Distributed detection and isolation of bias injection attack in smart energy grid via interval observer." *Applied energy* 256 (2019): 113703.
[87] Rocabert, Joan, et al. "Control of power converters in AC microgrids." *IEEE transactions on power electronics* 27.11 (2012): 4734-4749.
[88] Zhang, Xiaomeng, et al. "Consensus enhanced droop control strategy for islanding mode multi converter system." *Energy Reports* 8 (2022): 301-309.
[89] Tayab, Usman Bashir, et al. "A review of droop control techniques for microgrid." *Renewable and Sustainable Energy Reviews* 76 (2017): 717-727.
[90] Lin, Xin, Ramon Zamora, and Craig Baguley. "Droop control based on improved virtual impedance in a stand-alone microgrid." *2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia)*. IEEE, 2019.
[91] Shahbazi, Zahra, et al. "Performance and Vulnerability of Distributed Secondary Control of AC Microgrids under Cyber-Attack." *2021 7th International Conference on Control, Instrumentation and Automation (ICCIA)*. IEEE, 2021.
[92] Wang, Bin, and Yupeng Sang. "Dual-mode operation control of smart micro grid based on droop strategy." *Energy Reports* 8 (2022): 9017-9024.
[93] Araia, Junichi, and Yasuhiro Taguchi. "Coordinated control between a grid forming inverter and grid following inverters suppling power in a standalone microgrid." *Global Energy Interconnection* 5.3 (2022): 259-265.
[94] Zeineldin, H. H., E. F. El-Saadany, and M. M. A. Salama. "Distributed generation micro-grid operation: Control and protection." *2006 Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*. IEEE, 2006.
[95] Nguyen, Tung Lam, et al. "Agent based distributed control of islanded microgrid—Real-time cyber-physical implementation." *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 2017.
[96] Rajesh, K. S., et al. "A review on control of ac microgrid." *Renewable and sustainable energy reviews* 71 (2017): 814-819.
[97] Zuo, Yihui, et al. "Performance assessment of grid-forming and grid-following converter-interfaced battery energy storage systems on frequency regulation in low-inertia power grids." *Sustainable Energy, Grids and Networks* 27 (2021): 100496.
[98] Zhang, Bo, et al. "A cyber-physical cooperative hierarchical control strategy for islanded microgrid facing with random communication failure." *IEEE Systems Journal* 14.2 (2020): 2849-2860.
[99] Gavriluta, Catalin, et al. "Cyber-physical framework for emulating distributed control systems in smart grids." *International journal of electrical power & energy systems* 114 (2020): 105375.
[100] Guo, Renqi, Quan Li, and Nan Zhao. "An overview of grid-connected fuel cell system for grid support." *Energy Reports* 8 (2022): 884-892.
[101] Driesen, Johan, and Klaas Visscher. "Virtual synchronous generators." *2008 IEEE power and energy society general meeting-conversion and delivery of electrical energy in the 21st century*. IEEE, 2008.
[102] Teng, Yuting, et al. "Review on grid-forming converter control methods in high-proportion renewable energy power systems." *Global Energy Interconnection* 5.3 (2022): 328-342.
[103] Unruh, Peter, et al. "Overview on grid-forming inverter control methods." *Energies* 13.10 (2020): 2589.
[104] Maherani, Mahshid, Jens Denecke, and Hendrik Vennegeerts. "Flexible parameterizable grid-forming converter control by separated fast synchronization and slow inertia response control loops of Direct Voltage Control." *IFAC-PapersOnLine* 55.9 (2022): 448-453.
[105] Ge, Pudong, et al. "A resilience-oriented centralised-to-decentralised framework for networked microgrids management." *Applied Energy* 308 (2022): 118234.
[106] Ortiz, Leony, et al. "A review on control and fault-tolerant control systems of AC/DC microgrids." *Heliyon* 6.8 (2020): e04799.
[107] Nguyen, Tung-Lam, et al. "A Distributed Hierarchical Control Framework in Islanded Microgrids and Its Agent-Based Design for Cyber–Physical Implementations." *IEEE Transactions on Industrial Electronics* 68.10 (2020): 9685-9695.
[108] Sardashti, Abolghasem, and Amin Ramezani. "Fault tolerant control of islanded AC microgrids under sensor and communication link faults using online recursive reduced-order estimation." *International Journal of Electrical Power & Energy Systems* 126 (2021): 106578.

[109] Deng, Chao, et al. "Distributed resilient control for energy storage systems in cyber–physical microgrids." *IEEE Transactions on Industrial Informatics* 17.2 (2020): 1331-1341.
[110] You, Youngin, et al. "A review of cyber security controls from an ICS perspective." *2018 International Conference on Platform Technology and Service (PlatCon)*. IEEE, 2018.
[111] Tyagi, Amit Kumar, and N. Sreenath. "Cyber Physical Systems: Analyses, challenges and possible solutions." *Internet of Things and Cyber-Physical Systems* 1 (2021): 22-33.
[112] Chen, Xia, et al. "Distributed resilient control against denial of service attacks in DC microgrids with constant power load." *Renewable and Sustainable Energy Reviews* 153 (2022): 111792.
[113] Wang, Yu, et al. "Cyber-resilient cooperative control of bidirectional interlinking converters in networked AC/DC microgrids." *IEEE Transactions on Industrial Electronics* 68.10 (2020): 9707-9718.
[114] Li, Yuchong, and Qinghui Liu. "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments." *Energy Reports* 7 (2021): 8176-8186.
[115] Dibaji, Seyed Mehran, et al. "A systems and control perspective of CPS security." *Annual reviews in control* 47 (2019): 394-411.
[116] Ashok, Aditya, Manimaran Govindarasu, and Jianhui Wang. "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid." *Proceedings of the IEEE* 105.7 (2017): 1389-1407.
[117] Sadu, Abhinav, et al. "Resilient design of distribution grid automation system against cyber-physical attacks using blockchain and smart contract." *Blockchain: Research and Applications* 2.1 (2021): 100010.
[118] Patil, Shital, and Sangita Chaudhari. "DoS attack prevention technique in wireless sensor networks." *Procedia Computer Science* 79 (2016): 715-721.
[119] Srinivas, T. Aditya Sai, and S. S. Manivannan. "Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm." *Computer Communications* 163 (2020): 162-175.
[120] Aliyu, Farouq, Tarek Sheltami, and Elhadi M. Shakshuki. "A detection and prevention technique for man in the middle attack in fog computing." *Procedia computer science* 141 (2018): 24-31.
[121] Birkinshaw, Celyn, Elpida Rouka, and Vassilios G. Vassilakis. "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks." *Journal of Network and Computer Applications* 136 (2019): 71-85.
[122] Escudero, Cédric, et al. "Security of control systems: prevention of aging attacks by means of convex robust simulation forecasts." *IFAC-PapersOnLine* 53.2 (2020): 4452-4459.
[123] Iqbal, Salman, et al. "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service." *Journal of Network and Computer Applications* 74 (2016): 98-120.
[124] Yılmaz, Ercan Nurcan, and Serkan Gönen. "Attack detection/prevention system against cyber attack in industrial control systems." *Computers & Security* 77 (2018): 94-105.
[125] Chalamasetty, Goutham K., Paras Mandal, and Tzu-Liang Tseng. "Secure SCADA communication network for detecting and preventing cyber-attacks on power systems." *2016 Clemson University Power Systems Conference (PSC)*. IEEE, 2016.
[126] Joo, Minhee, et al. "Situational awareness framework for cyber crime prevention model in cyber physical system." *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2018.
[127] Sivasankari, N., and S. Kamalakkannan. "Detection and prevention of man-in-the-middle attack in iot network using regression modeling." *Advances in Engineering Software* 169 (2022): 103126.
[128] Poudel, Binod P., et al. "Detection and mitigation of cyber-threats in the DC microgrid distributed control system." *International Journal of Electrical Power & Energy Systems* 120 (2020): 105968.
[129] Zhang, Xiangming, et al. "Attack isolation and location for a complex network cyber-physical system via zonotope theory." *Neurocomputing* 469 (2022): 239-250.
[130] Mousavi, Amirreza, Kiarash Aryankia, and Rastko R. Selmic. "A distributed FDI cyber-attack detection in discrete-time nonlinear multi-agent systems using neural networks." *European Journal of Control* 66 (2022): 100646.
[131] Ferrari, Riccardo MG, and André MH Teixeira. "Detection and isolation of replay attacks through sensor watermarking." *IFAC-PapersOnLine* 50.1 (2017): 7363-7368.
[132] Li, Lu, et al. "Adaptive robust FDI attack detection for cyber–physical systems with disturbance." *ICT Express* (2022).
[133] Wang, Xinyu, et al. "Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers." *International Journal of Electrical Power & Energy Systems* 110 (2019): 208-222.
[134] Sanchez, Helem Sabina, et al. "Detection of replay attacks in cyber-physical systems using a frequency-based signature." *Journal of the Franklin Institute* 356.5 (2019): 2798-2824.
[135] Al-Dabbagh, Ahmad W., Angelo Barboni, and Thomas Parisini. "Distributed Detection and Isolation of Covert

Cyber Attacks for a Class of Interconnected Systems." *IFAC-PapersOnLine* 53.2 (2020): 772-777.
[136] Luo, Xiaoyuan, et al. "Observer-based cyber attack detection and isolation in smart grids." *International Journal of Electrical Power & Energy Systems* 101 (2018): 127-138.
[137] Barboni, Angelo, Francesca Boem, and Thomas Parisini. "Model-based detection of cyber-attacks in networked MPC-based control systems." *IFAC-PapersOnLine* 51.24 (2018): 963-968.
[138] Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff. "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks." *Computer networks* 51.13 (2007): 3750-3772.
[139] Li, Yike, Yin Tong, and Alessandro Giua. "Detection and Prevention of Cyber-Attacks in Networked Control Systems." *IFAC-PapersOnLine* 53.4 (2020): 7-13.
[140] Quevedo, Joseba, et al. "A two-tank benchmark for detection and isolation of cyber attacks." *IFAC-PapersOnLine* 51.24 (2018): 770-775.
[141] Adeli, Mahdieh, et al. "Optimized cyber-attack detection method of power systems using sliding mode observer." *Electric Power Systems Research* 205 (2022): 107745.
[142] Wang, Wu, et al. "Cyber-attacks detection in industrial systems using artificial intelligence-driven methods." *International Journal of Critical Infrastructure Protection* 38 (2022): 100542.
[143] Ding, Steven X., et al. "Application of the unified control and detection framework to detecting stealthy integrity cyber-attacks on feedback control systems." *Automatica* 142 (2022): 110352.
[144] Nedeljkovic, Dusan, and Zivana Jakovljevic. "CNN based method for the development of cyber-attacks detection algorithms in industrial control systems." *Computers & Security* 114 (2022): 102585.
[145] Tan, Sen, et al. "False Data Injection Cyber-Attacks Detection for Multiple DC Microgrid Clusters." *Applied Energy* 310 (2022): 118425.
[146] Yuan, Huanhuan, and Yuanqing Xia. "Resilient strategy design for cyber-physical system under DoS attack over a multi-channel framework." *Information Sciences* 454 (2018): 312-327.
[147] Sun, Yuan-Cheng, and Guang-Hong Yang. "Event-triggered resilient control for cyber-physical systems under asynchronous DoS attacks." *Information Sciences* 465 (2018): 340-352.
[148] Zha, Lijuan, Jinliang Liu, and Jinde Cao. "Resilient event-triggered consensus control for nonlinear muti-agent systems with DoS attacks." *Journal of the Franklin Institute* 356.13 (2019): 7071-7090.
[149] Xiong, Menghui, et al. "Observer-based event-triggered output feedback control for fractional-order cyber–physical systems subject to stochastic network attacks." *ISA transactions* 104 (2020): 15-25.
[150] Xiao, Shunyuan, et al. "Resilient Distributed Event-Triggered Control of Vehicle Platooning Under DoS Attacks." *IFAC-PapersOnLine* 53.2 (2020): 1807-1812.
[151] Li, Tao, et al. "Improved event-triggered control for networked control systems under stochastic cyber-attacks." *Neurocomputing* 350 (2019): 33-43.
[152] Gao, Rui, and Guang-Hong Yang. "Resilient decentralized sampled-data H∞ filter design for linear interconnected systems subject to denial-of-service attacks." *Information Sciences* 538 (2020): 467-485.
[153] Chen, Scarlett, Zhe Wu, and Panagiotis D. Christofides. "Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control." *Computers & Chemical Engineering* 136 (2020): 106806.
[154] Huang, Xin, and Jiuxiang Dong. "A robust dynamic compensation approach for cyber-physical systems against multiple types of actuator attacks." *Applied Mathematics and Computation* 380 (2020): 125284.
[155] Qiu, Xiaojie, et al. "Resilient model-free adaptive control for cyber-physical systems against jamming attack." *Neurocomputing* 413 (2020): 422-430.
[156] Lü, Shaoyu, et al. "Adaptive sliding-mode control of a class of disturbed cyber–physical systems against actuator attacks." *Computers & Electrical Engineering* 96 (2021): 107492.
[157] Li, Zhanjie, and Jun Zhao. "Resilient adaptive control of switched nonlinear cyber-physical systems under uncertain deception attacks." *Information Sciences* 543 (2021): 398-409.
[158] Mishra, Dillip Kumar, et al. "Resilient control based frequency regulation scheme of isolated microgrids considering cyber attack and parameter uncertainties." *Applied Energy* 306 (2022): 118054.
[159] Yan, Jing-Jing, and Guang-Hong Yang. "Switching resilient control scheme for cyber-physical systems against DoS attacks." *Journal of the Franklin Institute* 358.8 (2021): 4257-4276.
[160] Zeng, Pengyu, et al. "Sampled-data resilient H∞ control for networked stochastic systems subject to multiple attacks." *Applied Mathematics and Computation* 405 (2021): 126265.
[161] Xu, Yangguang, Ge Guo, and Shuanghe Yu. "Resilient observer-based sliding mode control of connected vehicles with denial-of-service attacks." *Journal of the Franklin Institute* 359.7 (2022): 2886-2905.
[162] Hu, Songlin, et al. "Resilient control design for networked DC microgrids under time-constrained DoS attacks." *ISA transactions* (2022).
[163] Ma, Yan, et al. "A resilient optimized dynamic event-triggered mechanism on networked control system with switching behavior under mixed attacks." *Applied Mathematics and Computation* 430 (2022): 127300.

[164] Wang, Jiaqi, Jinfeng Gao, and Ping Wu. "Attack-resilient event-triggered formation control of multi-agent systems under periodic DoS attacks using complex Laplacian." *ISA transactions* (2021).
[165] Yang, Hongyan, et al. "Sliding mode-based adaptive resilient control for Markovian jump cyber–physical systems in face of simultaneous actuator and sensor attacks." *Automatica* 142 (2022): 110345.
[166] Sun, Ziwen, et al. "Adaptive event-triggered resilient control of industrial cyber physical systems under asynchronous data injection attack." *Journal of the Franklin Institute* 359.7 (2022): 3000-3023.
[167] Li, Jiahao, et al. "Resilient Sliding Mode Control for a Class of Cyber-Physical Systems With Multiple Transmission Channels Under Denial-of-Service Attacks." *Journal of the Franklin Institute* (2022).
[168] Zhao, Yue, et al. "Anti-saturation resilient control of cyber-physical systems under actuator attacks." *Information Sciences* 608 (2022): 1245-1260.
[169] Zhang, Zhipeng, and Huimin Wang. "Resilient decentralized adaptive tracking control for nonlinear interconnected systems with unknown control directions against DoS attacks." *Applied Mathematics and Computation* 415 (2022): 126717.