A comprehensive review on cyber-attack detection and control of microgrid systems

Hamidreza Shafei[1*], Li Li[1*], Ricardo P. Aguilera[1]

1- School of Electrical and Data Engineering, University of Technology Sydney, Sydney, Australia

*Corresponding authors: Hamidreza.shafei@student.uts.edu.au, and Li.Li@uts.edu.au

Abstract:

Due to the fast progress of Microgrid (MG) systems and the development of advanced computing technologies and communication networks – all of which enhance the efficiency and reliability of power networks – MGs are at the risk of various cyber-attacks which can eventually lead to different glitches in the power distribution networks. There are many different kinds of cyber-attacks, some of which are the False Data Injection Attack, Denial of Service, Stealth Attack, and Covert Attack. The common goals of these attacks are to cause power outage, economic loss, and even system instability. Cyber-attacks could infiltrate MGs through the communication links, local controllers, or master control channels. In this chapter, a thorough review of the types of cyber-attacks and the problems caused by them in MGs has been presented, and some methods of cyber-attack detection, resilient control system design, and countermeasures against such attacks have been discussed. Numerous research works have already investigated the subject of cyber-attacks on both the Direct-Current (DC) and Alternating-Current (AC) MG systems. These studies can be divided into two main categories: (a) detection and mitigation approaches, and (b) resilient control system designs. Several subclasses of each of these categories, along with their advantages and disadvantages has been thoroughly investigated in this chapter. In the first category, after detecting a compromised agent, an active or passive mitigation mechanism is activated to prevent the spread of the agent's destructive effects to the whole system. This may impose some strict limitations on the MGs. In the second category, by developing the distributed attack-resilient control protocols, the resilience of a MG system against potential attacks/faults/noises is enhanced to the point where no detection and mitigation action will be required.

Keywords: Microgrid, Cyber-attack, Cyber-security, Attack detection, Resilient control

List of Abbreviations

AC	Alternating Current	KL	Kullback-Liebler
ANN	Artificial Neural Network	LMI	Linear Matrix Inequality
BLIA	Bias Load Injection Attack	LSTM	Long Short-Term Memory
BP	Back Propagation	MAS	Multi-Agent Systems
CKF	Cubature Kalman Filter	MG	Microgrid
CNN	Conventional Neural Network	MITM	Man-in-the-Middle
CPL	Constant Power Load	MPC	Model Predictive Control
CPS	Cyber-Physical Systems	NN	Neural Network
DC	Direct Current	PI	Proportional Integral
DER	Distributed Energy Resource	RESs	Renewable Energy Resources
DNN	Deep Neural Network	RNN	Recurrent Neural Network
DoS	Denial of Service	SCADA	Supervisory Control and Data Acquisition
DDoS	Distributed Denial of Service	SMC	Sliding Mode Control
DTL	Deep Transfer Learning	SMO	Sliding Mode Observer
EKF	Extended Kalman Filter	SVM	Support-Vector Machine
FDIA	False Data Injection Attack	UKF	Unscented Kalman Filter
GA	Genetic Algorithm	UIO	Unknown Input Observers

1- Introduction

Due to the use of Renewable Energy Resources (RESs), MGs are not only reliable and economical, but they also provide environmental benefits [1]. They offer more efficient and reliable operation than conventional power grids. For better integration of RESs, battery energy technology is introduced [2], which is very important to recuperate the supply's reliability and improve the power plant's efficiency. According to [3], the worldwide power demand increases by 2.5% each year and creates a significant deficiency that conventional power generation technology can hardly fulfil. In addition, the huge and undesirable power losses that occur in transmission lines due to their resistance emphasize the importance of Microgrid (MG) development. The unique features of MGs, i.e., their at-demand proximity, high efficiency, and quick installation, make them a practical solution for today’s growing power demands.

Due to their importance and ability to provide the needed power, MGs have been the subject of various studies. The recent technological advances in control, computing, and communications will allow the MGs to be more distributed and computer-networked. As a result, they will become more prone to cyber-attacks. Any type of attack on the

exchanged data signals will have serious consequences, such as economic loss, power outage, and system instability.

In order to prevent the system performance degradation resulting from different types of cyber-attacks, proactive and novel security schemes have to be developed and implemented. The main focus of this chapter is to review the techniques that have been previously developed to deal with the cyber-attacks on MGs. According to the literature, there are mainly two approaches in this respect. In the first scheme, after detecting the compromised agents, a mitigation mechanism is activated to prevent the spread of the destructive effects of cyber-attacks to the whole system [4]. To this end, Liu et al. [5] proposed an attack-resilient cooperative scheme by developing a properly designed observation network. In this approach, by monitoring the behaviour of all the neighbours of a distributed generation (DG), the misbehaving DGs will be isolated from the network. One of the most serious drawbacks of this strategy is the strict restrictions that have to be imposed. Fawzi et al. [6] showed that it is impossible to restore the states of an attacked system when more than half of its agents are attacked. A common strategy to alleviate the effects of the cyber-attacks is to isolate the attacked agents from the whole system. However, by doing so, the network's connectivity and, as a result, the whole system's performance can be degraded. In view of the abovementioned drawbacks of the first approach, a second method for dealing with the cyber-attacks has been developed. In this scheme, without having to detect and correct the compromised agents, the considered MGs can be made resilient against attacks, faults, and noises by just using a distributed attack-resilient control system [7]. By doing so, the resiliency of MGs will be achieved through distributed attack-resilient control protocols against potential noises/faults/attacks, without the need to detect, identify and correct/remove misbehaving agents. Unlike the noise and fault signals, which can be assumed to be bounded, the attack signals are not bounded, as they are intentionally designed to maximize their damage [6]. In this regard, Zuo et al. [8] developed a distributed resilient containment-based control system to regulate the voltage magnitudes of the MGs against unbounded attacks on different channels. Table 1 illustrates a comparison among this review chapter and with the previously published review papers.

Table 1. A comparison between this review chapter and previously published review papers

Reference	Main points
[9]	Investigating the effects of cyber-attacks on just load frequency control systems

[10]	Focusing on detection and protection schemes against FDIAs, but not on MGs.
[11]	Investigating the risk of FDIAs in power generation and distributed systems.
[12]	Studying the cybersecurity problem with a machine learning-based approach
[13]	Just focusing on all control schemes that have been used for attack mitigation.
[14]	Surveying on methods for attack detection, especially DoS, deception, and replay attacks.
Current work	Studying two different schemes to deal with cyberattacks in MGs: attack detection & resilient control system design

As can be seen, there is still a lack of a comprehensive literature review about the general approaches that deal with various types of cyber-attacks and the strategies employed to mitigate the impacts of such attacks on MGs. Therefore, a wide-ranging survey about the abovementioned issues has been provided in this chapter.

The rest of this chapter has been structured as follows: different types of cyber-attacks, their relevant mathematical expressions, and the importance of studying cyber-security are discussed in Sec. 2. In Sec. 3, the first approach for dealing with cyber-attacks (i.e., attack detection design) is investigated, and the subclasses of this approach are also reviewed. Then, in Sec. 4, the design of a resilient control system for the cyber-security of MGs is discussed. In each section, the advantages and disadvantages of the presented approaches are also outlined. Finally, this work is concluded in Sec. 5. For a better understanding of this review chapter, a flowchart of its structure is depicted in Figure 1.

2-1- Various kinds of cyber-attacks and the importance of studying cyber security

Thanks to the tremendous progress in the field of communication technology, a fundamental revolution has occurred in Cyber-Physical Systems (CPSs) [15]. Since becoming more distributed and network-integrated, the CPSs have become more prone to cyber threats and different types of network anomalies [16]. Cyber-attacks mostly occur on two fronts: software, and hardware. The software attacks generally lead to communication interference, manipulation, communication latency, etc. The hardware attacks usually cause physical damage to sensors or modify the sensor information. Of these two types of attacks, the hardware attacks are the most dangerous ones [17].

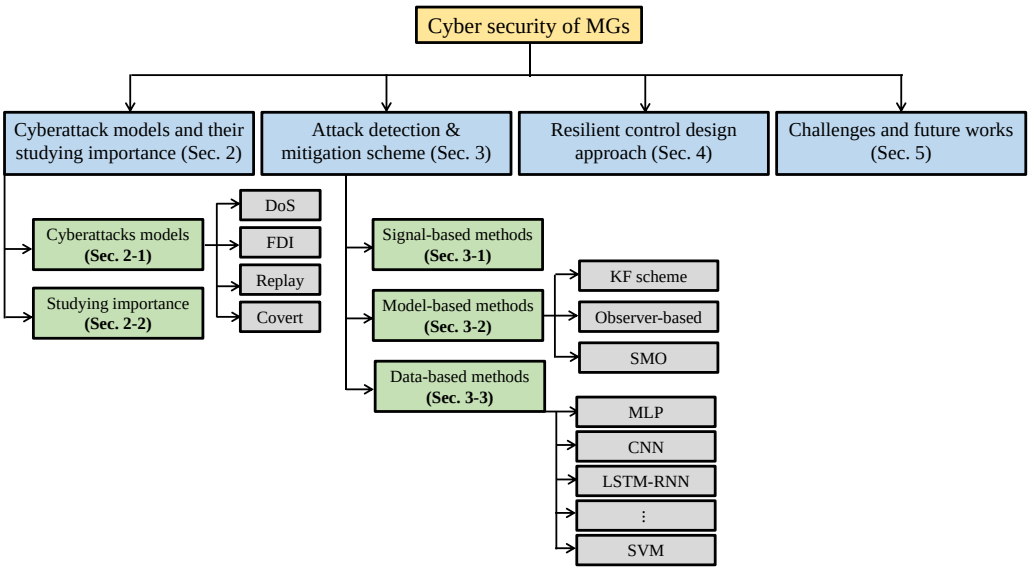

Figure 1. Organization of the chapter

The first step in dealing with cyber-attacks is to identify and model them. There are various kinds of cyber-attacks, each with its own particular goals and consequences. For example, some attacks may affect the actuators and controllers, some may focus on sensors, some may try to block the transmission data channels, and some others may attempt to falsify the information signals. As is depicted in Figure 2, the cyber-attacks could target different channels of a CPS and thus degrade the performance of a MG system by adversely affecting one of its essential features below (i.e., availability, integrity, timeliness, and confidentiality). The dotted lines denote the affected signals, while the solid lines represent the unaffected.

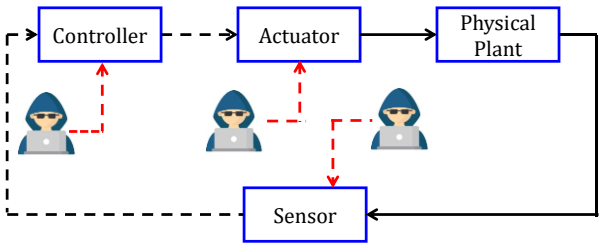

Figure 2. Cyber-attacks on different channels

In addition, Figure 3 depicts the framework of an MG in the presence of various kinds of cyberattacks through different channels. To get familiar with MGs, see the more recent review papers [18-20], as well as the references cited therein.

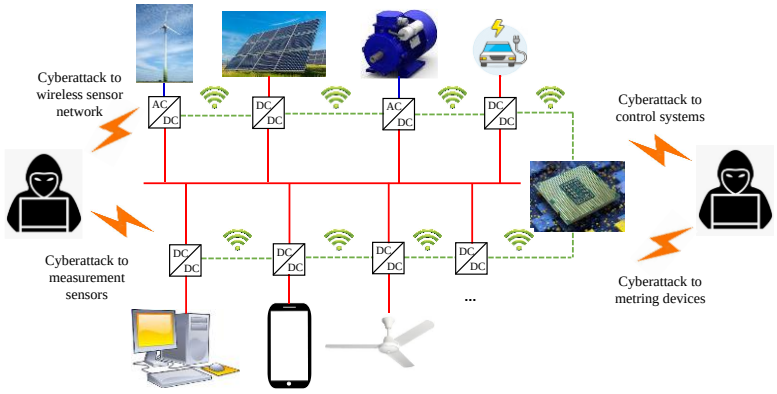

Figure 3. The framework of a MG in the presence of various cyberattacks.

Availability: Availability concerns the accessibility and availability of data at all times [21], which may be lost under DoS attacks.

Integrity: This feature demands that the data be clean and trustworthy. The process of generating, transmitting, and storing data must be genuine and free of any corruption [22]. The Replay and FDIAs may compromise the essential feature of data integrity.

Timeliness: This crucial feature concerns the real-time processing, generation, and availability of data [23], which may be lost with replay attacks.

Confidentiality: Confidentiality indicates the availability of data to the authorized users only [24], and it could be adversely affected by the Man-in-the-Middle (MITM) type of attacks.

Brief descriptions of different types of cyber-attacks, their mathematical models, and their impacts on the MG systems have been provided in the following sections. Due to the diversity of cyber-attacks, it is vital to know the characteristics of each one and to find practical means to mitigate their effects.

2-1-1 DoS attack

To disrupt the availability of data, the potential intruders try to make the communication networks inaccessible. DoS attacks can be performed in two ways, flooding services or crashing services. In flood attacks, aiming to slow down and eventually stop the services, attackers send too much traffic for the server to buffer. In addition, it can occurr by jamming signals to block the communication channels. To this end, the data from a sensor or actuator can be prevented from reaching their intended destination. Thus, a DoS attack on a sensor or actuator can be mathematically formulated with the following availability

function [25]:

$$p(t) = \begin{cases} 1 & for\ t \in \Pi_N \\ 0 & for\ t \in \Pi_D \end{cases} \quad (1)$$

where $\sigma_D = \{h_0,\ h_1,\ \cdots, h_k, \cdots\}$ is the time sequence in a DoS attack, and $\sigma_I = \{\tau_0,\ \tau_1,\ \cdots, \tau_k, \cdots\}$ is the time sequence in the DoS attack duration, where $h_{k+1} - h_k > \tau_k > 0$ means that there is a normal communication duration between two consecutive DoS attacks [26]. In the above equation, $\Pi_D(h,t)$ denotes all the time intervals in which the DoS attacks occur over $[h,t)$, where $t > h$. On the contrary, $\Pi_N(h,t)$ represents all the time intervals in which there is a normal communication over $[h,t)$. It is clear that $\Pi_N(h,t) \cap \Pi_D(h,t) = \emptyset$ and $\Pi_N(h,t) \cup \Pi_D(h,t) = [h,t)$. In (1), $p(t) = 0$ means the presence of a DoS attack and $p(t) = 1$ denotes the absence of a DoS attack. Figure 4 depicts the structure of a DoS attack, where $x(t) \in R^n$, $u(t) \in R^p$, $y(t) \in R^m$, and $w(t) \in R^n$ are the state variables, control input, output signal, and the process noise, respectively.

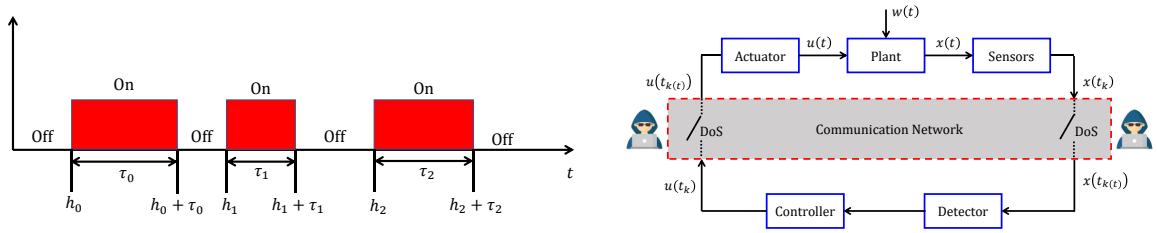

Figure 4. DoS attack representation [9]

2-1-2 FDI attack

To destroy the data integrity, attackers try to alter the states of a system by injecting false data into sensors [27, 28]. FDIA is launched through sensor spoofing, intrusion of communication links, magnetic field injection attacks, GPS spoofing, etc. In the systems with unstable modes, the dynamic FDIAs attempt to modify the system measurements so that some of the unstable system modes become unobservable. Similar to DoS attacks, FDIAs can also be applied to both the actuator and the sensor channels, and they are formulated as follows [9]:

$$\begin{aligned} \hat{u}_j(t) &= u_j(t) + u_{a_j}(t) \quad for\ j = 1, 2, \dots, p \\ \hat{y}_i(t) &= y_i(t) + y_{a_i}(t) \quad for\ i = 1, 2, \dots, m \end{aligned} \quad (2)$$

where $\hat{u}_j(t)$ and $\hat{y}_i(t)$ are the disrupted control input and output signals, respectively. $u_j(t)$ and $y_i(t)$ are the desired control input and measurement. In addition, $u_{a_j}(t)$ and $y_{a_i}(t)$ are the FDIA signals to the actuators and sensors which are defined as follows:

$$u_{a_j}(t) = \begin{cases} 0 & for\ t \notin \tau_{a_j} \\ \lambda_j\, \mathcal{F}_j(.) & for\ t \in \tau_{a_j} \end{cases} \quad (3)$$

$$y_{a_i}(t) = \begin{cases} 0 & for\ t \notin \tau_{a_i} \\ \lambda_i\, \mathcal{F}_i(.) & for\ t \in \tau_{a_i} \end{cases}$$

In the above equation, τ_a is the attack time period and λ is an attack parameter. $\mathcal{F}(\cdot)$ can either be a time/state-dependent function or completely independent.

2-1-3 Replay attack

A replay cyber-attack targets both the data integrity and the timeliness features of a system. This attack can occur practically through monitoring and recording sensor measurements during the invasion. Then, attackers use them instead of the actual measurements. In this type of attack, the attackers record a data sequence for a certain amount of time and then replay these readings in the system to deceive the operators. In the replay attacks, the attackers do not need any information about the system being targeted. To model this type of attack in a sensor channel, one can write

$$a_y(t) = -Cx(t) + y(t-\tau) \tag{4}$$

In the above equation, $0 < \tau < t$ and $a_y(t)$ is the replay attack in the sensor channel. Also, $x(t) \in R^n$ and $y(t-\tau) \in R^m$ are the state of the system and the sensor data gathered through monitoring, respectively. Two different stages should be considered in this procedure: 1) Monitoring phase, and 2) Replay phase. In the monitoring phase $(0 \le t < t_0)$, the collected measurements are stored in $J(t)$, and thus [9]

$$\begin{aligned} y_a(t) &= 0 \\ J(t) &= \Gamma^{y}.y(t) \end{aligned} \tag{5}$$

In this phase, cyber-attack is not applied yet (i.e. $y_a(t) = 0$). While in the replay phase, the gathered data from the monitoring stage are sent to the controller. So, we have

$$\begin{aligned} y_a(t) &= J(t-t_0) \\ J(t) &= J(t-1) \end{aligned} \tag{6}$$

The same procedure can be applied to model the replay attacks in an actuator channel. The structure of this type of attack is depicted in Figure 5, where u_a and y_a are the actuator and sensor attack signals, respectively. In addition, d is the external disturbance acting on the plant, and u is the infected control signal.

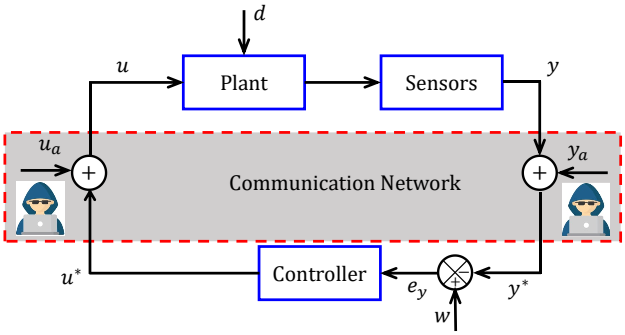

Figure 5. Replay attack representation

2-1-4 Covert attack

The covert attack is another hard-to-detect cyber-attack in which the attackers modify the measurements of a system in such a way that it cancels out all the effects of the attack on the system dynamics. To practically apply this kind of attack, attackers cancel the effect of attacks by calculating the system's output response and subtracting it from the measurement readings. In this type of attack, the attackers apparently have access to both the actuator and sensors. Therefore, a complete knowledge of the system is required. To mathematically model the covert attack, the following two steps should be taken [29].

1- The actuator of the system is manipulated by the attackers as follows:

$$\tilde{u}_t^i = u_t^i + a_t \quad (7)$$

In the above equation, u_t^i is the original control law, a_t is the corrupted signal injected by attackers, and $\tilde{u}_t^i$ is the corrupted control signal which will alter the system states at time $t+1$, as follows:

$$\tilde{x}_{t+1}^i = x_t^i + B_i a_t \quad (8)$$

As a result, the output signal changes to the following:

$$\tilde{y}_{t+1}^i = y_{t+1}^i + C_i B_i a_t \quad (9)$$

2- In this step, the sensor measurements are modified so that the attack cannot be detected. Thus,

$$\check{y}_{t+1}^i = \tilde{y}_{t+1}^i - \Upsilon \quad (10)$$

In the above equation, $\Upsilon = C_i B_i a_t$. By doing so, the altered measurements (i.e., $\check{y}_{t+1}^i$) get to be exactly equal to the original measurements in the absence of an attack (i.e., y_{t+1}^i). Therefore, this kind of attack is disguised.

2-2- Why is studying cybersecurity important?

A MG system is a typical CPS in which the physical units and the cyber environments work together [30]. In such systems, a supervisory control and data acquisition (SCADA)

system is in charge of management and control [31]. In the early days of such systems, the SCADA was secure when they had no communication with the outside [32]. With the advancement of technology, the next generation of SCADA systems (known as the distributed SCADA) emerged, which could be integrated with local area networks. Eventually, in the most recent generation of SCADA systems (the networked SCADA), the wide area networks can also be accessed. Compared to the previous SCADA generations, the networked SCADA systems enjoy lower cost, more straightforward installation, and easier maintenance, to name but a few. In spite of these positive features, these networked systems are highly susceptible to cyberattacks [33].

Considering the key role of the SCADA in controlling and managing sensitive industries like the smart grid systems, its security against cyber-attacks has attracted a great deal of attention [34]. In this respect, the NERC CIP[1] plan was established in 2006 with the aim of protecting the power control systems [35], the IEC TC57[2] was established to undertake the development of various security standards [36], the NIST[3] proposed the necessary procedures for securing the SCADA systems [37], and the ISA[4] presented its security protocols for industrial manufacturing [38].

A large number of cyber-attacks on CPSs have occurred in recent years. For example, in January 2003, intruders attacked the Dacis-Besse power plant in Oak Harbour (Ohio State, USA) with a slammer worm and shut down its safety display system [38]. In 2010, a malicious computer worm, known as the Stuxnet virus, targeted the SCADA system of the Natanz nuclear site in Iran and caused serious damage to numerous nuclear centrifuges [39]. In 2011, the SCADA system at an Illinois water plant was breached and, as a result, the supply pumps were disabled [40]. In another attack, in December 2015, the power grids in Ukraine were totally disrupted for hours by several FDI attacks [41]. A complete review of the previously occurring cyber-attacks is presented in [42]. Table 2 summarizes some of the major cyber-physical attacks that have occurred in the energy sector. These examples out of a long list of cyber-attacks clearly highlight the great importance of studying and researching the cyber-security matters related to MGs. A complete list of cyberattack events can be found in [43].

[1] North American Electric Reliability Corporation Critical Infrastructure Protection
[2] International Electrotechnical Commission Technical Committee
[3] National Institute of Standards and Technology
[4] International Society of Automation

Table 2: Some important events resulting from Cyber-attacks

Year	Location	Attacked Targets	Attack Type	Impact
2022	Finland	Minister of defence and foreign affairs	Distributed DoS attack	All affairs were suspended for 4 hours.
2022	Israeli	Telecommunication provider	DDOS attack	Multiple Israeli government websites were taken offline
2021	Australia	Telecommunications systems	A malicious code	Recorded all communication data
2021	Norway	Energy Technology Company Volue	Ransomware attack	Shutdown of water & water treatment facilities in 200 municipalities
2019	California & Utah, USA	Grid operators	DDOS attack	Disrupted their operation but not any outages
2015	Kiev, Ukraine	The breaker settings were attacked by the "BlackEnergy" malware	FDI Attack	More than 225,000 customers were affected for hours by the blackout
2013	New York, USA	The Bowman Dam was attacked when it was under maintenance	FDI Attack	Gaining remote access to the information on water levels and flow rates

3- Various cyber-security schemes

As was mentioned earlier, there are two main approaches for dealing with cyber-attacks, attack detection and mitigation, as well as the implementation of a resilient control system. The signal-based attack detection method implemented in microgrids is achieved by monitoring the signals in the communication links in real-time. However, in Model-based detection schemes, cyberattacks can be detected by utilizing the mathematical model of the system. In addition, data-based detection methods typically rely on machine learning or statistical mechanisms to infer a model of the system from historical data and measurement signals [44]. This section thoroughly discusses these two schemes and their positive and negative features.

3-1- Signal-based methods

In a signal-based method, the potential attacks can be detected by monitoring the state signals in real-time. For example, any discrepancy between the frequency of a system and its desired values could signal an attack [45]. In this paper, the detection and isolation of the attacked communication links are realized on time. Without a prior knowledge of system dynamics, Beg et al. [46] detected the FDI and DoS attacks on a complex DC MG system by using a temporal signal logic formula and comparing the system voltages and currents with their pre-set values. By monitoring the secondary sub-layer outputs and tracking the attacks' changes, a cooperative vulnerability factor was proposed to identify the FDIAs on the voltage measurements [28]. To identify the attacked nodes under a FDIA, a consensus algorithm based on the discordant elements was developed in [47]. By

examining the discrepancy between the received and forecasted measurements, Dong et al. [48] proposed a short-term state forecasting scheme for detecting FDIAs, which is integrated with the ∞-norm and L_2-norm residual measurement analysis. In another work, Madichetty et al. [17] proposed a low-computational-burden approach based on the adaptive state observer for estimating the system currents and voltages in the presence of FDIAs. In this paper, by analysing the error between the estimated and actual signals, the FDI attacks are detected in real-time.

As a sub-branch of the signal-based methods, the weighted least-square scheme is a reliable and efficient technique for attack detection in smart grids [49]. Using the graph signal processing technique, Drayer and Routtenberg [50] devised an attack detection scheme for the AC MGs. By comparing the maximum norm of the graph Fourier transform of an estimated grid state with a predefined threshold, they could detect the presence of FDIAs. In this approach, the high-frequency components related to the large eigenvalues of the Laplacian matrix are filtered out. The same approach is also used to detect the data integrity and data availability attacks on the power generation systems [51]. In another study, Hu et al. [52] introduced a residual skewness coefficient technique for detecting the stealth attacks via signal analysis. This method suffers from its dependence on the manual adjustment of parameters.

One of the major shortcomings of the signal-based methods is that the relationship between the measured data and the control signal is not investigated, which is necessary for reliable detection [44]. Also, the limitations of such schemes in detecting the stealth attacks are mentioned in [53].

3-2- Model-based methods

Another general approach developed for attack detection in the MGs is the use of the mathematical model-based methods. The Kalman filter [54], state estimation [55], observer-based detection [56], and the sliding mode observer (SMO) [57] schemes are some of the more common techniques in this category. In the face of model uncertainties, a lack of reliable measurements is the main limitation of the robust cyber-attack detection methods. Using both the graph and system-based theoretical approaches, the fundamental limitations in the monitoring of the CPSs under attack are investigated in [58]. Each of these schemes is discussed along with its positive and negative features in

this section.

3-2-1 Kalman filter-based techniques

The Kalman filter (KF) is a common scheme used for state estimation. In this method, an accurate state estimation can be achieved by applying an optimal recursive algorithm and using the previously-estimated states and the current measurements. Since previous measurements are not needed in this approach, it is considered as an efficient state estimation strategy. The KF method can be conducted in two steps: (a) the prediction step, and (b) the correction step [54].

Several filtering techniques have already been proposed for the estimation of dynamic states, such as the Extended Kalman Filter (EKF) [59], Particle Filter [60], Unscented Kalman Filter (UKF) [61], and the Cubature Kalman Filter (CKF) [62]. For example, Manandhar et al. [4] used the KF to estimate the state variables of a system. Then, the estimated states as well as the system readings were utilized by a χ^2-detector to detect the arising system faults and various kinds of attacks. In another paper, the KF method was employed to estimate the expected measurements, which were then used to obtain the deviations between the actual and the estimated values [63]. In this process, a Chi-square detector and the cosine similarity matching technique were applied to detect the cyber-attacks. For the real-time attack detection and state estimation in the presence of FDIA and measurement noise, Miao et al. [64] respectively employed a Chi-square test-based adaptive secure algorithm and an adaptive UKF scheme. Sargolzaei et al. [65] developed a KF-based observer for estimating the states of a system. In order to accurately deal with FDI attacks, they proposed a Neural Network (NN) architecture, whose weights were updated via an EKF. In another work, Soltani et al. [54] presented four different types of KFs (i.e., original KF, Adaptive KF, Fuzzy KF, and Fuzzy adaptive KF) for state estimation. These KF methods were integrated into a framework through an ordered weighted averaging operator, whose weighting factors are updated by a real covariance matrix and a theoretical covariance matrix. Abbaspour et al. [66] devised a resilient detection and mitigation-based controller for load frequency control against FDIAs. They proposed a Luenberger observer along with an Artificial Neural Network (ANN) enhanced by an EKF for online anomaly detection. The same approach was used for the detection of time-varying unknown FDIAs on sensors [67]. Li et al. [62] employed a robust CKF to dynamically estimate the states of a system under both the FDI and DoS

attacks in real-time. Their simulation results showed the superiority of the robust CKF over the CKF. A comparison between CKF and nonlinear observers was conducted in [68] to show the performance of each of these schemes in the dynamic estimation of system states in the presence of cyber-attacks and model uncertainties.

In another study, Adeli et al. [69] used a trust-based UKF and a modified secure node strategy to estimate the states of nonlinear systems under cyber-attacks. To prevent the spreading of the compromised data, they developed a cluster-based fusion approach. The shortcomings of the traditional KF approach in detecting the stealth attacks were investigated in [53], where a novel attack detection technique based on KF was also proposed. Using the upper bound of filtering error covariance minimization, a modified UKF was proposed in [70] for a specific class of nonlinear systems under sensor saturation and randomly occurring FDIAs. This paper also provides the sufficient conditions for the exponentially bounded filtering error. By employing a KF decomposition framework, the secure estimation of system states for linear time-invariant Gaussian systems under sparse integrity attacks was achieved in [71], and the sufficient conditions under which the proposed estimator is still stable were established.

In general, apart from the positive features of KF schemes in providing reasonable state estimation when the precise mathematical model of a system is available, the performance of the KF-based methods deteriorates in the absence of a good model or in the presence of external disturbances. In addition, the initial conditions of the considered states and covariance matrices can affect the estimation quality.

3-2-2 Observer-based methods

The observer-based schemes for state estimation and attack detection usually use a system's deterministic state–space mathematical model. A few examples of the wide-ranging observer-based methods include the high-gain observers [72], Kullback-Liebler (KL) observer [73], and the unknown input observer (UIO) [74]. These observers have been widely explored and used in various studies and applications.

The UIO is an observer-based scheme that detects the potential cyber-attacks on the CPSs by estimating the system states. For example, an UIO was developed in [56] to detect the compromised agents in a distributed manner. In this study, the attacked signal was considered as an external input with no prior information. Then, the sufficient and

necessary conditions for observing the system misbehaviours were established. Mustafa et al. [75] developed an attack detection scheme based on the KL divergence criterion for AC MGs. The KL divergence factors were then used to mitigate the effects of cyber-attacks by determining the trustworthiness of the information received from the other agents. Also, to inform the other agents of the reliability of the transmitted data, each agent generates a self-belief factor and communicates it with its neighbors. By comparing the KL criteria for both the healthy and the attacked systems, the FDIAs on the power grids can be detected [76]. The same approach has been employed to detect the DC MGs' attacks [77].

To secure the CPSs against the periodic DoS attacks in both the measurement and control channels, an $\mathcal{H}_\infty$ observer-based output feedback controller was developed in [78]. In this paper, by considering the DoS attacks with a cyclic dwell-time switching characteristic, an augmented system is achieved as a discrete-time cyclic dwell-time switched system with an unstable and a stable subsystem. For the resulting augmented system, the proposed observer-based controller is developed in a piecewise linear form. Attack detection and attack mitigation by a finite-time convergent observer-based output feedback controller were also investigated in [79], where two different cases are considered: a) when all the sensors are targeted, and b) when some of the sensors are attacked. By using the proposed observer with the adaptive gains, the applied sensor attacks are reconstructed. In this procedure, the corrupted measured outputs are cleared of the malicious content, and the output feedback controller uses these cleaned signals to mitigate the effects of the cyber-attacks.

In another article, Wang et al. [80] employed an UIO to detect the FDIAs on MGs under system uncertainties. To deal with the computational limitation of the predefined threshold, an interval residual-based detection criterion was proposed in this work. Moreover, for the undetectable FDIAs, an algorithm based on the local logic judgment matrix was applied to both detect and isolate the mentioned attacks. By solving a robust $\mathcal{H}_\infty$ multi-objective optimization problem and using an independent and cooperative detector, the existing anomalies in the multi-agent systems (MASs) subjected to both the FDIAs on their communication links and the physical faults in their facilities were detected [81]. By doing so, a compromise was made between robustness to disturbance and sensitivity to attack.

To detect the covert attacks on large-scale interconnected systems, Barboni et al. [82] proposed a distributed model-based observer. By augmenting an original system with a switched auxiliary one, the covert attacks were detected via a switched Luenberger observer [83]. In another study, Das and Madichetty [84] designed a Luenberger observer to estimate the DC-DC converter current based on the input voltage. This scheme has some positive features, such as the reduction of sensor requirement and computational burden as well as performance improvement. Gao et al. [85] developed a novel observer with a set of K-filters to detect the deceptive cyber-attacks in the sensor and actuator channels of the high-order nonlinear CPSs.

With the purpose of detecting the cyber-attacks in the presence of disturbance and measurement noise, Yan et al. [86] developed a new FDIA detection scheme by decomposing a large-scale MG into several interconnected subsystems and designing a set of dynamic reduced-order observers to generate residual signals, which were then compared with the adaptive detection thresholds using a prescribed performance benchmark. To deal with the biased load attacks, Wang et al. [87] proposed an unknown input interval-based observer that could mitigate the influences of the regionally-interconnected information and disturbances. They introduced a novel detection criterion in order to eliminate the prior threshold limitations.

Achieving cyber-security via the dynamic state estimation schemes was also reported in [88]. In this work, first, the incoming cyber-attacks are detected by the dynamic observers and by eliminating the effects of unknown inputs. Then a new attack-tolerant control scheme is used to eliminate the destructive effects of cyber-attacks on the operation and performance of power systems. The bias load injection attack (BLIA) is another kind of FDIA, which targets the vulnerable generator loads. Due to the destructive impact of the BLIA on MG systems, it is very important to develop a secure scheme to detect and mitigate this type of attack. In this regard, Wang et al. [89] proposed a three-stage approach to detecting the BLIAs. In this method, by applying a subregion division technique, first, the complexity of attack detection in a large-scale grid system is reduced. Then, a robust adaptive detection method is employed to accurately estimate the physical dynamics of the system. Finally, a logical judgment matrix is used to cope with the undetectability of sensor attacks under system vulnerability.

To estimate the states of continuous time-invariant linear systems under sparse sensor

attacks, An et al. [90] developed a supervisory state observer by utilizing a bank of candidate nonlinear sub-observers and applying a switching logic. In this scheme, a monitoring function is used to select the active sub-observers at every moment. In another work, Yang et al. [91] studied the estimation of distributed states in large-scale power systems under both the FDI and DoS attacks through the neighborhood coordination scheme. In this approach, the DoS attacks are compensated via a measurement predictor, where the FDIAs are treated as the measurement uncertainties.

Besides the positive features of the observer-based approaches in detecting cyberattacks, it is challenging to be applied to more complex systems because they utilize the exact mathematical model of the system.

3-2-3 Sliding mode observer

A common method of state estimation in MGs is the sliding mode observer (SMO) approach, which has an intrinsic robustness against uncertainties, noise, disturbances, and cyber-attacks [92-99]. In this approach, the system states are estimated in a finite time by forcing them toward a stable manifold in the presence of uncertainties and disturbances. Despite the positive features of the SMO approach, including its simple implementation, disturbance rejection ability, and robustness, it suffers from chattering due to its high-frequency switching around the sliding surface [100, 101]. In the following, we will review some research works related to attack detection by SMO.

Saha et al. [92] proposed a SMO-based fault diagnosis technique for estimating the sensor measurement errors arising from a possible cyber-attack or sensor faults in the DC MGs. To ensure a resilient system operation, the estimated errors are used to initiate a mitigation action. Most of the previously developed SMO-based methods assume a linear MG system, which is a restrictive assumption. In fact, in the presence of constant power loads (CPLs), the assumption of system linearity will not be valid anymore. In this regard, Cecilia et al. [102] proposed a distributed nonlinear observer that can robustly detect the FDIAs in both the cyber links and current sensors. In this work, the system equations are transformed into a form suitable for observer design purposes. For estimating the states of a system in the presence of time delay, a sliding mode estimation-based control system was presented in [93], which estimates the states of a MG system and also predicts the time delays. Furthermore, to ensure the system stability and the accuracy of the

estimated time delays, the estimation error was considered as a disturbance to the Sliding Mode Control (SMC) system and used to update it adaptively. For estimating the system states and detecting the sensor attacks, Ao et al. [94] proposed two adaptive SMOs, whose parameters are updated online. They also established the sufficient conditions for attack detection.

In another study, Rinaldi et al. [95] proposed a distributed adaptive dual-layer super-twisting SMO to isolate, reconstruct, and mitigate the adverse effects of both the disturbances and communication attacks. In this paper, similar to [94], the observer gains are adjusted with an adaptive law. After reconstructing the attacks, a standard Proportional Integral (PI) controller is employed to mitigate their destructive effects. The same procedures have also been used with the other types of SMO scheme, such as the integral SMO [103-105], terminal SMO [106], and the high-order SMO [107, 108]. To deal with the cyber-attacks on sensors, a SMO was proposed in [99], which is sensitive to the sensor attacks. This observer alarms the operators when at least one of the MG subsystems is under the sensor attack. Furthermore, to isolate the exact subsystems under attack, another SMO is proposed which is sensitive to the attack on the ith sensor but robust against the external disturbances and sensor attacks other than those on the ith agent.

Yang et al. [109] presented a SMO-based state and attack reconstruction scheme with the system augmentation and Linear Matrix Inequality (LMI) approach for detecting the FDI attacks in both the sensor and actuator channels. Li et al. [110] investigated an augmented state observer that uses a terminal integral adaptive SMC to estimate a system's states under sensor and actuator FDI attacks. Su et al. [97] modelled the MGs under the dynamic load-altering attacks and developed a robust SMO that generates a residual signal. The cyber-attacks are then detected by comparing this signal with a threshold value. A linear parameter-varying SMO with adaptive parameters that uses an equivalent output error injection algorithm to estimate the system states and reconstruct the sensor faults in the presence of erroneous scheduling parameter information was explored in [111]. By considering the unknown inputs and the sensor attacks, a linear discrete-time state-space and a sparse vector were devised to model the system and the cyber-attacks, respectively [98]. To estimate the states of the system under unknown inputs, a new model in the descriptor form that uses an iterative approach was developed.

In this model, a novel sparse SMO that employs a projection operator is proposed for estimating the system states affected by the cyber-attacks.

The weakness of the SMO-based methods in detecting the intelligent attacks with changing distributions can be considered as their drawback. Furthermore, in the presence of unknown system disturbances (e.g., voltage oscillations, load variations, and neighboring voltage variations), these methods may not be able to achieve a reliable state estimation [112]. Table 3 summarizes some of the recently published works in the field of cybersecurity with model-based schemes.

Table 3. A brief review of the attack detection and mitigation studies using the model-based approach

No	Study	Year	Attack type	method	advantages	Disadvantages
1	Saha et al. [92]	2018	FDI & Replay attack	Using a SMO to detect attacks	A complete and general model of MGs is considered. The effectiveness of the method against different undesired situations are examined.	This scheme can only deal with bounded cyberattacks; Required the exact model of the system
2	Abianeh et al. [113]	2021	FDIAs	With localized communication link quality observer & multi-objective SMC	This method can deal with unbounded and extreme cyberattacks. The vulnerability of the method to various FDIs and time delay is very low.	Besides being strongly model-dependent, this scheme is applicable to just FDIAs.
3	Shi et al. [114] and Li et al. [115]	2021	FDIAs	Adaptive distributed observer	The vulnerability of this method against FDIs is low. High reliability and scalability with robustness against cyber-attacks.	This scheme is highly vulnerable to time delays and other kinds of cyber-attack.
4	Sahoo et al. [116]	2021	FDIAs	Using localized observer	By this method, other kinds of cyber-attacks can also be detected.	They just considered frequency FDIAs. This method is vulnerable to time delay.
5	Li et al. [62]	2019	FDI & DoS attacks	Robust Cubature KF	Dynamic estimation of states in case that FDA & DoS attacks are applied	This method is validated with a simple system.
6	Afshari et al. [117]	2020	Time-varying & unbounded Deception attack	Using distributed state observer (DSO) to estimate the states and attack signals	The effects of battery are considered. The proposed method can deal with unbounded cyberattack.	This method is just for AC MGs, and deception attacks.
7	Barboni et al. [82]	2020	Covert attacks	Robust model-based observer	Using 2 robust decentralized & distributed observers based on the H_∞ solved by LMI. Besides the covert attacks, disturbances are also considered. Applicable to large-scale systems	The uncertainties & attacks should be bounded. The model accuracy affects the detection results.
8	Poudel et al. [77]	2020	FDIAs	Distributed Kullback-Liebler observer	Using an interior-belief factor to determine the reliability and an exterior-belief value to check the trustworthiness of the information.	Exact model of the system is required.
9	Cecilia et al. [57]	2021	FDIAs and Uncertainties	Extended Astolfi/Marconi plus linear Luenberger observers	Using 2 adaptive observers for observable and unobservable state estimation under FDIAs and CPL and other undesired conditions.	Not applicable for other kinds of attacks.
10	Cecilia et al. [102]	2021	FDIAs and Uncertainties	High-order SMO along with a nonlinear open loop observer	Using a distributed HOSMO for the observable states and an open-loop observer for the unobservable states under FDIAs and CPL condition.	The estimation of the power line currents relies on an open-loop integration which is not tuneable.
11	Sahoo et al. [28]	2019	FDIs and Stealth attack	Using cooperative vulnerability factor framework	The capability of proposed method in detecting stealth attacks. Proposing a CVF factor to alarm the attacked agents.	The method should be developed to be applicable to AC MGs.
12	Yan et al. [93]	2017	Time delay	Estimation error used as a disturbance in SMO	Controlling a system with several kinds of delays with a SMO-based SMC	Requires the exact model of a system.
13	Manandhar et al. [4]	2014	DoS	KF with X^2 detector	Resilient to spoof attacks; with low computational complexity	Dependent on model accuracy; vulnerable to disturbances; cannot be used for nonlinear systems

As mentioned, the model-based detection approaches are designed to compare the predicted and actual sensor measurements. In this scheme, detecting intelligent attacks in high dimension systems can be considered its primary challenge. The idea of developing data-based schemes for attack detection has been proposed to deal with this issue, which will be considered in the next section.

3-3- Data-based methods

The data-based methods are another approach for dealing with cyber-attacks in MGs. These methods use the historical data and measurement signals to learn the features of a MG system. Some of the more popular intelligent cyber-security schemes, such as the deep reinforcement learning, deep transfer learning, the generative adversarial network, and so on, will be discussed in this section. These techniques can be generally classified into the unsupervised, semi-supervised, supervised, and the reinforcement learning schemes.

For detecting the FDIAs with a machine learning-based approach, Ozay et al. [118] analysed the performances of the supervised, semi-supervised learning and the online learning algorithms in the detection of FDIAs on MGs. In another research, Habibi et al. [119] developed an intelligent-based method for detecting the FDI attacks and identifying the attacked agents in DC MGs. They proposed a time-series analysis and a nonlinear auto-regressive NN-based exogenous model to estimate the DC currents and voltages. These researchers proposed a Model Predictive Control (MPC)/ANN scheme for FDI attack detection in another article [120], where a MPC plays the role of attack mitigator, while an ANN detects the FDIAs on the DC MGs. In [121], an artificial intelligent method with a nonlinear autoregressive exogenous model based on NN is proposed for detecting the FDIAs on the voltage and current sensors. This method suffers from large computational burden in the real-time implementations.

As was mentioned previously, a drawback with the model-based detection methods is that they require an exact mathematical model of a system. To deal with this problem, researchers have proposed the idea of using the data-based techniques. Compared to the traditional machine learning techniques, the chief merit of the deep learning schemes is that they can better learn from the large security datasets. A comprehensive review of the above-mentioned intelligent attack detection methods has been provided in the following

sections.

3-3-1 Multi-layer Perceptron (MLP)

With a supervised learning algorithm, the MLP is a feedforward ANN that can be considered as the base architecture of the Deep Neural Network (DNNs). The structure of this network is illustrated in Figure 6. Back propagation (BP) is a widely-used supervised learning scheme for training the feedforward NNs. This approach has been used frequently in the field of cyber-attack detection. For example, Felipe et al. [122] applied this method as a real-time attack detection approach with low computation cost. This technique has also been employed for the detection of malicious botnet traffic attacks [123].

Due to the sensitivity of the MLP approach to the feature scales, this method requires sufficient numbers of neurons, hidden layers, and iterations, which increases the computation cost. However, this scheme is capable of dealing with nonlinear systems even in the online learning tasks and real-time operations [124]. By integrating a multilayer perceptron with a deep random NN, Huma et al. [125] developed a hybrid deep random NN method for cyber-attack detection. This scheme is 98-99% effective in classifying the different types of cyber-attacks.

3-3-2 Convolutional NN (CNN)

The CNN is another deep learning scheme that can learn without the need for manual feature extraction. The structure of this network, which comprises multiple layers, is depicted in Figure 7.

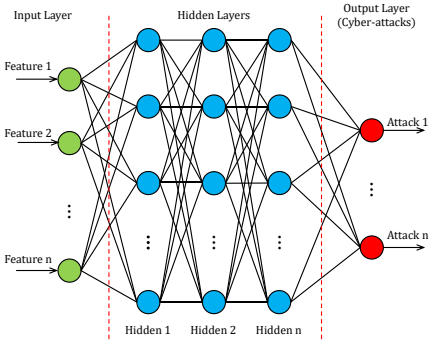

Figure 6. MLP network structure for attack detection

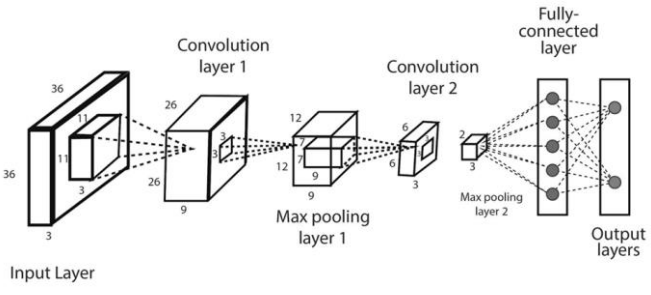

Figure 7. CNN structure with multiple convolution and pooling layers

The optimized parameters in each layer of the CNN help reduce the network complexity. In addition, the “dropout” layer is used to deal with the problem of over-fitting. This

network has been extensively employed in various cyber-security applications, such as DoS attack detection [126] and malware detection [127]. For example, Yanmiao et al. [128] devised a highly-accurate deep learning approach of low complexity based on multi-CNN fusion for the detection of intruders. With the aim of detecting the injected data measurements, He et al. [129] proposed a deep learning framework based on the CNN and Long Short-Term Memory (LSTM) network, which can monitor the data measurements and the network level features. To detect the possible cyber-attacks, a multi-CNN with the NSL-KDD evaluation dataset was presented in [128]. The good performance, high accuracy and low complexity of this model were verified by experimental results. Compared to the ANN, the CNN method is more expensive computationally, but it can be implemented automatically and without human intervention.

3-3-3 Long Short-Term Memory Recurrent Neural Network (RNN)

As another type of ANN, The RNN can process an input sequence and retain its states while processing the next input sequence. The feedback loops in the recurrent layer of RNN help sustain the data in the memory. The LSTM network is a specific type of RNN with a memory cell for long-time data storage. An example of this network is depicted in Figure 8 [130]. The LSTM scheme is also used for attack detection [131] and time-based botnet detection [132] purposes. By employing this technique, researchers have been able to detect the FDI attacks in the measurement channel [133] and classify the attacks by means of a hybrid deep learning method [134]. To optimize the RNNs and CNNs, Vasan et al. [135] proposed a robust malware detection model based on advanced ensemble learning, which has a very high precision and low computational burden. By integrating the LSTM modules into an ensemble detector, an advanced deep learning model was proposed in [136] for detecting the new kinds of cyber-attacks with high accuracy. A LSTM-RNN model requires a lot of time and resources to get fully trained; so it is able to improve the detection process and precision.

3-3-4 Auto Encoder (AE)

The AE is another type of ANN which can be trained in an unsupervised fashion [137]. However, to reduce the dimension sizes, it ignores the noise effects. The AE network has three different components: encoder, code, and decoder (Figure 9). An advantage of this

method in the propagation stage is its ability to extract the useful information and filter out the useless features [138].

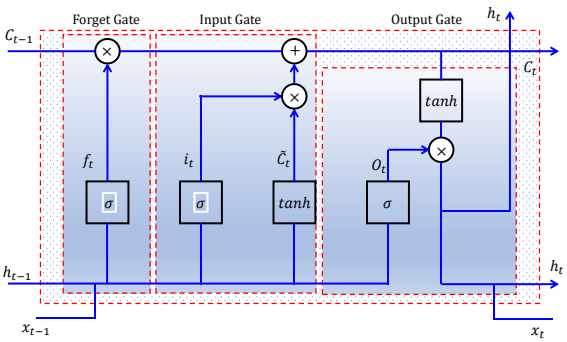

Figure 8. The LSTM network structure

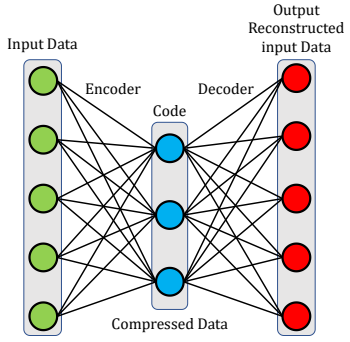

Figure 9. AE network structure with its components

As far as cyber-security is concerned, an effective security model can be built with a deep AE network, since it enjoys the minimum number of security features. For example, Yousefi-Azar et al. [139] devised a learning technique based on the AE network for the classification and detection of network attacks and anomalies. In another study, Binghao and Guodong [140] proposed a stacked sparse auto-encoder to improve the attack detection. Therefore, in view of its ability to capture the main data features, the AE approach can be useful in the field of cyber-security.

3-3-5 Restricted Boltzmann Machine (RBM)

The Boltzmann Machine (BM) is an unsupervised deep learning model with two types of nodes: visible and hidden. Among the various kinds of BMs, the RBM is a model with limited connections between the layers. By reducing the number of connections, the training algorithm becomes more efficient than the other types of BM networks [141] (Figure 10).

The RBM method has already been used in cyber-security matters. For instance, Fiore et al. [142] applied this technique for the detection of cyber-attacks, where the effectiveness of the proposed model was evaluated by combining the positive features of the generative models with the ability of the RBM to deduce new information from incomplete training data. In another study, the accuracy of DoS attack detection was improved by means of the RBM scheme [143]. By eliminating the noises from the input data and extracting new information from them, Seo et al. [144] could enhance the performance of this model in the attack detection tasks.

3-3-6 Deep Belief Network (DBN)

The DBN, with its structure depicted in Figure 11, is a probabilistic generative model composed of several RBMs. As is shown, this model consists of multiple RBMs and a BP-NN. In the DBN scheme, a two-stage training process is implemented: first, the pre-training of the model by an unsupervised layer-wise learning technique, which is considered as a contrastive divergence based training process; and second, the fine-tuning of the model by means of the BP-NN and a supervised learning approach [145].

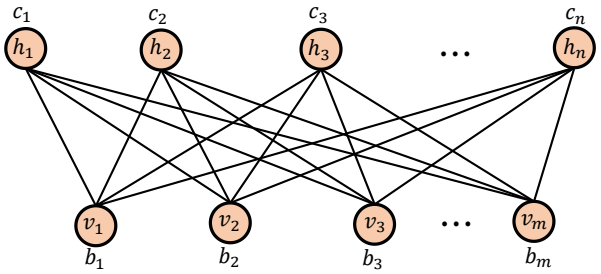

Figure 10. The RBM structure with n hidden and m visible nodes

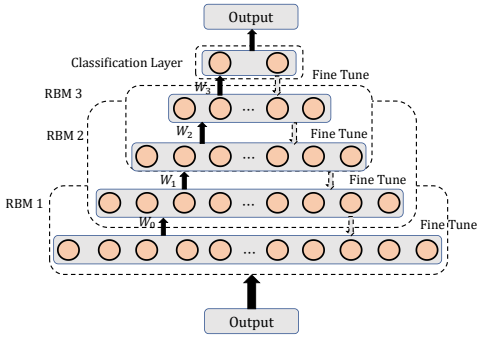

Figure 11. The DBN network structure

Due to the unique classification and feature extraction abilities of the DBN model in large-dimension applications, it plays a prominent role in cyber-security domains and has been considered in numerous relevant research studies. For example, Salama et al. [146] developed the DBN model as a feature reduction scheme and used it in the attack detection tasks. A DBN-based attack detection strategy was reported in [147], and its results were compared with those of the Support-Vector Machine (SVM) scheme, which revealed a higher accuracy and speed of attack detection by the DBN method. To achieve the same objectives, Peng et al. [145] proposed an optimization approach to DBN. For dealing with newer types of cyber-attacks, self-adaptive attack detection techniques have been developed. In this regard, Zhang et al. [148] presented a cyber-attack detection scheme based on the deep belief network and genetic algorithm (GA). In this work, the optimal numbers of the hidden layers and neurons are adaptively determined by the GA in order to boost the attack detection precision.

3-3-7 Generative Adversarial Network (GAN)

In the GAN model, two NNs, a discriminator (D) and a generator (G), are trained to compete with each other [149]. The structure of this learning scheme is depicted in Figure 12. The GAN framework has been widely used in the domain of cyber-security to make the learning models more robust against the intruders that try to manipulate the data systems. For example, Jin-Young et al. [150] devised a novel learning framework based

on the deep AE-based transmitted GANs and achieved a classification accuracy of over 95%. In this scheme, the fake malware could be distinguished from the real ones. By balancing the real datasets with additionally generated data, Merino et al. [151] proposed a technique which improves the detection of the cyber-attacks and is suitable for all kinds of learning schemes, including the reinforcement learning as well as the fully-supervised, semi-supervised, and unsupervised approaches. In this method, to balance the previously unbalanced datasets, the model generates additional data that mimic those distributed by different kinds of attacks.

3-3-8 Deep Transfer Learning (DTL)

The DTL is a powerful and common method for solving the problems that lack adequate training data. In this method, it is not necessary to train the artificial intelligent models, since it is able to train the NNs with just a small amount of data [152]. As is shown in Figure 13, the DTL scheme uses the pre-trained models for the tasks in the target domain. Considering the different cases, the DTL can be classified into three sub-classes: (a) inductive transfer learning, (b) transductive transfer learning, and (c) unsupervised transfer learning [153].

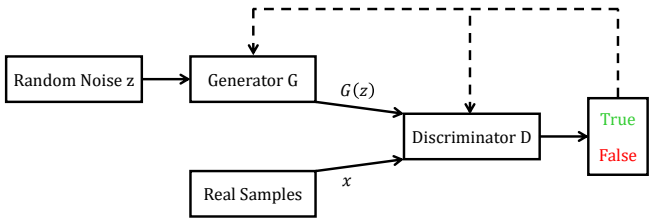

Figure 12. The GAN network structure

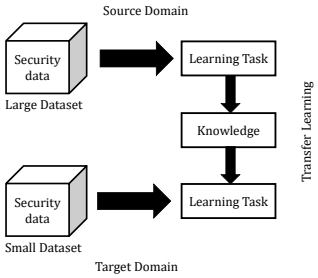

Figure 13. The DTL structure

Thanks to the positive features of the DTL scheme, including its shorter training, time, and higher output accuracy with fewer training data, it has attracted a lot of attention in the cyber-security field of study. For example, network attack detection was achieved in [154] with a ConvNet model based on the DTL scheme. Xianwei et al. [155] presented a novel semi-supervised DTL network for attack detection. In this paper, to avoid the disassembling of the files, a byte classifier is proposed that extracts the needed byte features from the programs and classifies them with an RNN. To improve the byte classifier accuracy from 94.72% to 96.90%, a new ASM classifier with a combination of ASM features is designed in this paper. In another work, Vu et al. [156] presented a DTL scheme for detecting the cyber-attacks in the IoT devices with a high level of precision.

Their proposed method can learn from the data collected from various labeled and unlabeled sources. Since this learning scheme can speed up the training process with high efficiency and precision even with small datasets, it has received a great deal of attention from the researchers in the cyber-security field.

3-3-9 Deep Reinforcement Learning (DRL)

The DRL is another kind of machine learning approach, in which the model can learn from its previous actions. This learning scheme, which is depicted in Figure 14, integrates the reinforcement and the deep learning methods together [157].

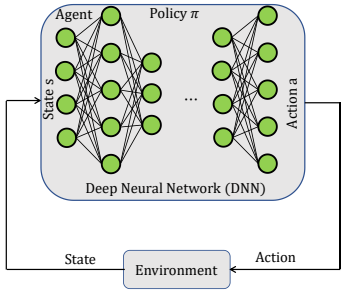

Figure 14. The DRL structure

The DRL scheme has been previously studied in the cyber-security related research works. For instance, using a labeled dataset, several supervised DRL algorithms for the detection of cyber-attacks were presented in [158]. By conceptually modifying the conventional DRL algorithms by the rewarding of the detection errors in the training phase, the cyber-attack detection process could be made faster and more precise than the traditional machine learning schemes. To deal with the inability of the conventional methods in maintaining a balance between high accuracy and low false positive rate against the new and unknown attacks, a DRL-based adaptive attack detection algorithm was proposed in [159]. By combining a deep learning model with an intrusion detection strategy, Li et al. [160] proposed a deep migration learning-based scheme for cyber-attack detection. Hughes et al. [161] proposed a model-free DRL method for intrusion detection and evaluated its performance by stopping two distinct multi-stage attack scenarios on a virtualized test-bed.

3-3-10 Support-Vector Machine Learning

By using the SVM learning datasets to build a series of hyperplanes, the SVM approach can be employed for cyber-attack detection in large-dimensional spaces. In this regard, two machine-learning-based methods (i.e., the supervised anomaly detection and the

unsupervised distributed SVM) have been proposed to detect the stealth attacks in the AC MGs [162]. Lee et al. [163] developed a 98%-accurate lightweight machine learning scheme for cyber-attack detection, in which an SVM algorithm is used for feature extraction and a deep auto encoder is applied for attack classification. Raman et al. [164] presented an adaptive and robust attack detection method in which the Hypergraph-based GA is used for parameter selection and the SVM technique is applied for feature extraction. In another study, Tang et al. [165] developed an algorithm based on the SVM that uses a nonlinear input data scaling scheme to detect the cyber-attacks. By comparing the results of the SVM method and the ANN model, they demonstrated the superiority of their proposed method in detecting the applied cyber-attacks. Also, a lightweight attack detection scheme based on the SVM approach, which is suitable for the low-resource IoT devices, was proposed in [166].

Table 4 summarizes the various types of the abovementioned learning schemes with their advantages and disadvantages. Despite the many advantages of these intelligent methods, they suffer from a heavy computational load, which makes them inappropriate for applications to large-scale distributed MGs.

Table 4. A brief review of the cyber-security studies using the data-based approach

No	Study	Year	Attack type	Method	Advantages	Disadvantages
1	Habibi et al. [167]	2021	FDIAs	Using artificial NN to detect cyberattacks.	This method can also be used when all units are under attacks. Deal with coordinated high domains & unfairly FDIAs.	It can detect coordinated FDI attacks on current channels.
2	Habibi et al. [119]	2020	FDIAs	Using NARX NN method for attack detection	It can detect FDI attacks in both current and voltage channels.	This method needs strong data base for training. It can only deal with constant FDIAs.
3	He et al. [129]	2017	FDIAs	Deep learning-based Conditional Deep Belief Network	Resilient to predicted FDIAs and GPS spoofing; suitable for large-dimensional data applications	High computational complexity; vulnerable to unforeseen attacks; low accuracy to abrupt attacks
4	Hughes et al. [161]	2022	DoS	Deep Reinforcement Learning	Do not need a system's model; suitable for solving complex problems; tuned by a small number of training episodes	High computation cost, and requires faster technologies for training purposes.
5	Kavousi Fard et al. [168]	2021	FDIAs	Using "Prediction interval" for the lower and upper estimation model	Highly accurate FDIA detection	High computational cost
6	Dehghani et al. [169]	2021	Constant FDIAs	Deep Machine Learning & Wavelet Singular Values Approach	Using a novel optimization scheme based on Gray Wolf to detect FDIAs. FDIA detection is achieved precisely and robustly.	Real-time implementation of this method to MGs is a challenge.
7	Gao et al. [155]	2020	Malware threats	Semi-supervised transfer learning with a Recurrent NN	Increased training speed; high efficiency and precision with small datasets; Not need to extract sensitive data.	This algorithm needs to be optimized for classification. For attack detection, it should be improved

This section has conducted a comprehensive overview of cybersecurity from the artificial NN and deep learning point of view. Reviewing recent studies in this domain has discussed how different kinds of NNs and deep learning methods can be used for cybersecurity solutions. The proposed security approach should possess the relevant deep learning modeling based on the data characteristics.

4- Resilient control design approach

In spite of the many advantages of the distributed control systems, such as greater flexibility, scalability, low communication burden, and faster system response, their vulnerability against the cyber-attacks is still a challenging issue that has to be fully addressed. That's why the cyber-security field has become more important than ever [170]. Considering the devastating consequences of the recent cyber-attacks, the subject of cyber-security, similar to the topic of attack detection and mitigation, has attracted the attentions of many researchers in the power industry. Given the various sources of uncertainties (e.g., the plug-and-play functionality of DGs, changes in microgrid topology, and uncertain and unknown dynamics), the resilient control systems are very important means of controlling the MGs. In the presence of various uncertainties and cyber-attacks, the resilient controllers can provide some relief in the form of bounded control signals, reference tracking with zero steady-state error, and an acceptable transient response [171].

The resilient control of MGs has been achieved by many techniques such as SMC [172], adaptive control [173], robust H_∞ [174], fuzzy controller [175], learning-based approach [176], etc. For example, Duan et al. [177] proposed a four-step attack-resilient distributed controller based on a detection-mitigation algorithm to immunize the DC MGs against the data integrity attacks. Unlike the grid-connected MGs, whose primary objective is to achieve proper power-sharing among all the DGs, in the islanded MGs, there should be fair power-sharing as well as accurate frequency and voltage regulation [178]. In this regard, a cyber-attack-resilient distributed controller is proposed for dealing with both the time-varying and successive attack signals in the communication links, local controllers, and master controller. The proposed method uses the periodically intermittent communication to detect and isolate the adversaries. The consensus-based secondary control systems have been employed to detect the FDIAs in both the DC [47] and AC MGs [116]. In these works, the cyber-attacks are detected through an asynchrony

index, a detection scheme which is highly dependent on the chosen threshold. In another study, Abhinav et al. [179] developed a resilient distributed secondary cooperative controller for the islanded AC MGs in the presence of cyber-attacks. The performance of the proposed controller was evaluated under the sensor and actuator attacks as well as the attacks on the communication links. In this study, a distributed observer-based controller was developed for dealing with the sensor/actuator attacks, while a trust/confidence-based control system was designed for mitigating the effects of the cyber-attacks on the communication links. Also, an attack detection scheme for partial primal-dual-based distributed frequency control was proposed in [180].

Although the terms “robustness” and “resilience” seem to have similar meanings, they actually refer to two different features in the context of power systems. In fact, resilience refers to a system’s active reactions in real-time to unexpected and extreme events. While robustness refers to the preservation of a controller’s desired performance in the presence of a given range of disturbance in a passive manner. The works that have adopted a detection and isolation scheme for boosting the resiliency of control systems have the following drawbacks: (a) they make a compromise between the timeliness of the real attack mitigation when tuning the isolation criterion and the controller’s robustness to normal disturbances, and (b) the number of cyber-attacks that can be mitigated is limited [177]. Some works have focused on improving the robustness of the distributed control system. For instance, Ding et al. [181] proposed a distributed resilient secondary control system for a battery energy storage system under the DoS attacks. To ensure the controller’s robustness against the DoS attacks, an acknowledgment attack detection scheme and a communication recovery mechanism were applied to repair the connectivity-paralyzed communication topology. By using the weighted mean subsequence reduced algorithm for each DER, the corrupted information received from other neighbouring agents could be discarded and, as a result, the security of a proposed distributed secondary controller against the FDI attacks could be ensured [182]. A distributed resilient control system based on an adaptive technique was employed in [183] to restore the frequency and voltage of an AC MG system, achieve a fair real power-sharing, and to balance the state-of-charge with multiple ESSs under the abnormal conditions. To ensure the stability of an AC microgrid system against unbounded attacks, Zou et al. [8] developed a fully distributed resilient controller for the secondary frequency regulation and voltage containment by introducing a virtual resilient layer with hidden

networks. However, they assumed that the hidden network is secure, which may not be true in the real applications. To address the threat of cyber-attacks in the AC MGs, a resilient distributed optimal frequency control system that uses a leader-follower consensus protocol was proposed in [170], where an auxiliary networked system is connected with the original control system.

The resilience of MGs against infrastructure failures has been enhanced by a novel master-slave control system [184]. A resilient SMC system that guarantees the exponential stability of MGs against the DoS attacks was proposed in [185]. Baghaee et al. [186] developed a distributed decentralized robust mixed $^{H_2}/_{H_\infty}$ voltage controller for disturbance rejection and set point tracking purposes. The LMI scheme was employed for solving a multi-objective optimization problem, where the fuzzy logic approach was also applied to improve the performance of the controller against the nonlinear loads and small/large disturbances.

Li et al. [187] proposed a resilient control system based on an adaptive control scheme for the islanded AC MGs whose communication links are under the cyber-attacks. The resiliency of the proposed method in voltage and frequency restoration and its power sharing capability were confirmed through computer simulations. To model the time-varying uncertainties of the power outputs and loads in multiple RESs, Lin et al. [188] proposed a novel offline probabilistic model and an online updating scheme. In this paper, a resilient stochastic optimization model that incorporates the concept of dynamic MGs is proposed to restore the voltage and frequency values. To achieve the sufficient conditions for a secure consensus among the neighboring agents in the absence of a continuous communication due to the DoS attacks, Xu [189] proposed a novel resilient leader-following event-triggered control protocol. Most of the research studies on the resilient control systems consider the sensor and actuator attacks separately with complex nonlinear systems, which increases the computational burden and makes it difficult to analyze and control the attacked MGs. To deal with this problem, Zhao et al. [190] designed a resilient control system based on feedback linearization for the MGs under both the sensor and actuator attacks. In this work, after simplifying the mathematical model of a targeted MG system, they used a hybrid resilient control scheme based on an adaptive terminal SMC.

A resilient cooperative output-regulated controller for the heterogeneous linear MASs with unknown switching exosystem dynamics under the DoS attack was proposed in [191]. In this paper, they designed a distributed resilient observer for estimating the auxiliary states and distributed controllers for individual agents. Song et al. [192] developed an adaptive resilient controller based on the fractional-order command filtered backstepping technique for the nonlinear systems affected by time-delays and unknown state-dependent deception attacks. To make the MASs resilient against both the actuator and sensor attacks, a resilient consensus control system based on a secure dynamic event-triggered scheme was proposed in [193]. In this work, a distributed adaptive compensator was also developed to predict the unavailable system states. To guarantee the stable operation of the wind turbines in redistributing the generated power among the converters under the system faults and cyber-attacks, a resilient DC voltage controller was developed [194]. Zuo et al. [195] investigated a fully distributed resilient controller for a multi-group network system under the unknown and unbounded FDIAs on both the cyber-physical and the virtual layers. In another study, Sadabadi et al. [196] proposed a resilient controller that doesn't need any information about the nature or location of an attack. In this work, a Lyapunov-based approach and the graph theory were applied to ensure average voltage regulation and proportional load sharing in the DC MGs affected by the FDIAs.

To rectify the effects of sensor faults in the islanded MGs, Saha et al. [197] proposed a SMO integrated with an H_∞ output feedback control law. The purpose of designing the SMO was to estimate the sensor faults, which were then used to develop the proposed robust fault-tolerant controller. A fully-distributed resilient control strategy based on an output formation containment scheme was proposed to control a high-order heterogeneous multigroup system under the unknown and unbounded attacks [198]. In this paper, the authors assumed that the unknown unbounded attacks can affect the actuators, the local state feedback, and the communication channels of each agent. A novel switching event-triggered resilient control scheme based on the droop control and MPC was proposed at the primary control level to achieve the frequency/voltage restoration as well as power sharing in the islanded MGs [199]. Moreover, a distributed consensus pinning-based control scheme was provided at the secondary level to manage the transient deviations and the response speed. Finally, to improve the immunity of the proposed system against severe accidents, a resilient control technique was designed by

integrating the primary and the secondary control levels.

Ma et al. [200] demonstrated that with a resilient neuroadaptive dynamic control technique based on the Gaussian radial basis function NN, the semi-global uniformity and the ultimate boundedness of all the signals under the FDI and DoS attacks, unknown control gains, system uncertainties, and output constraints can be guaranteed. A cascade 2 degree of freedom controller integrating a PI and an internal model controller was proposed in [201] as a resilient control scheme for managing the sustained operation of the MGs under the parametric uncertainties and unbalanced loads. A brief summary of the resilient control schemes in the field of cyber-security along with their merits and drawbacks has been provided in Table 5.

5- Future Direction

The cybersecurity of MGs is still at its early stage of progress, which makes it become a hot topic. Proposing and developing new and practical methods to mitigate the effects of cyber-attacks on MGs is an inevitable challenge that needs to be more considered. Some potential research topics regarding this problem have been proposed in the following.

- ✓ Developing a secure filter based on attacked measurement outputs is suggested as future work to achieve acceptable security performance. The existing KF methods can obtain the minimal variance of the filtering errors by using exact knowledge of noise statistics. However, since the statistical characteristics of signals transmitted by the attacker cannot be obtained, this assumption is usually not applicable to MGs [202].
- ✓ For practical applications, it is highly recommended to consider MGs under various kinds of attacks simultaneously.
- ✓ Developing a **General** resilient control system that can ensure the stability of MGs against multiple cyberattack models has paramount importance, which has not been considered yet. Most current methods are developed specifically for one specific attack and under particular conditions.
- ✓ To achieve accurate results from the data-based approach in cyber-attack detection, developing pre-processing methods or proposing new data preparation techniques is required to clean data from missing and ambiguous values, meaningless data, and outliers.
- ✓ As was mentioned, each approach has its merits and demerits. Integrating various

methods from different schemes can be considered a novel idea to benefit from the positive features of each technique. For instance, by developing a hybrid method based on the integration of model-based and data-based techniques, one can enjoy the low computation burden of the model-based approach; at the same time, the exact model of the system is not required.

- ✓ Most resilient control systems studied for controlling MGs against cyber-attacks, especially FDIAs, do not consider the communication channel time delays, which can quickly destroy the system's stability. Thus, this critical factor should be considered in the resilient control system for future work.
- ✓ Most works mainly focus on the cybersecurity of either DC or AC MGs. However, attack detection and mitigation of hybrid MGs have not been addressed well. Therefore, another future work that can be considered is attack detection and resilient control system design for hybrid MGs.
- ✓ Due to the low inertia of power electronics-based DERs, the frequency stability in hybrid MGs is one of the main concerns that must be considered. This situation can even be worse in the presence of cyber-attacks. Thus, proposing a proper and robust controller for attack detection and mitigation on the frequency control of hybrid MGs can be an important future topic.
- ✓ Like frequency control, any voltage variations on each side of a hybrid MG can transfer to the other side. As a result, it can deteriorate the stability of the system. Thus, voltage regulation of hybrid MGs under cyber-attacks is a challenging issue that has to be considered.

6- Conclusion

The importance of improving the security of CPSs against various types of cyberattacks has increased more and more in the recent years. A comprehensive review of the recently published works in the cybersecurity domain has been conducted in this chapter, which provides an overall picture of the historical, current, and future developments in this area. For this purpose, a new division regarding the existing approaches for addressing this problem in MGs has been proposed. Therefore, after introducing some of the most common cyberattack models, such as FDIA, DoS, covert, and replay attacks, we have reviewed the existing schemes that have been developed so far for cyber-attack detection,

including signal-based, model-based, and data-based schemes. By conducting an extensive survey for each of these methods, their advantages, disadvantages, and challenges in practice have been illuminated. Then, we have focused on the second approach of dealing with this problem, i.e., resilient control system design, by which the robustness and resiliency of the MGs against cyberattacks can be guaranteed. Finally, the future direction in this field of study has been expressed.

Table 5. A brief review of the resilient control system design approaches

No	Study	Year	Attack type	Method	Advantages	Disadvantages
1	Sahoo et al. [203]	2020	MITM	Multilayer event-driven detection based on diverging factor	Using a diverging factor to locate the compromised link(s); Good robustness against MITM attacks and disturbances	It can be developed for dealing with other attacks; the performance is prone to model uncertainties.
2	Chen et al. [204]	2022	DoS attack	Resilient distributed control based on PI & average consensus schemes	Providing average voltage regulation & load power sharing under line impedance and CPL, where the max allowed CPL is increased.	Resiliency drops against large time delays; it is effective only on the DoS attacks
3	Zhou et al. [45]	2020	FDIA on three channels	Signal-based approach by observing the switching frequency signal	Dealing with the cyberattacks on communication links; local and master controllers; resilient against time-varying attacks	Medium computation load; its performance is dependent on cyber graph connectivity
4	Liu et al. [26]	2021	FDI and DoS attacks	Controller based on a combined error with a pinning gain	Not needing any information about the cyber-attacks by proposing an adaptive gain; considering both the FDI and DoS attacks	Do not consider the control signals constraints, No robustness against time-delays and disturbances
5	Bidram et al. [182]	2019	Bounded FDIAs	Weighted Mean Subsequence Reduced algorithm	Time-varying communication graphs are used to improve the resiliency; has low processing load.	Medium computation burden; depends largely on the number of attacked cyber links/nodes
6	Sahoo et al. [205]	2020	Bounded FDIAs	Adaptive discord element & quick mitigation via an event-driven algorithm	Simple design; Heterogeneous to attack detection/mitigation; Resilient to single point of failure; PnP; has reduced communication cost	---
7	Zuo et al. [8]	2020	Unbounded FDIAs	Fully distributed controller consisting of a virtual MAS	Unbounded attacks are considered; attacks on various channels are considered; the controller does not require any global information	Has high computation load; its resiliency is maintained when less than $N/2$ nodes are under attack
8	Li et al. [115]	2021	FDIA	A novel adaptive resilient secondary control scheme	The proposed scheme is robust against FDIAs; The bounds of faults and attack do not need to be known;	Controller is highly vulnerable to other cyber-attacks and time-delays; considering one channel fault only
9	Zhao et al. [190]	2021	FDIA to actuators/sensors	Composite resilient controller based on terminal SMO with adaptive gains	Considering simultaneous attacks on actuators and sensors; easy to analyse; low computation cost; simple implementation	An exact model of the system is required.
10	Song et al. [192]	2022	DoS attack	Adaptive resilient control based on fractional-order backstepping scheme	Mitigating the effects of input delays and unknown sensor deception attacks; all the signals in the closed-loop systems are semi-globally UUB	High sensitivity to other kinds of attacks

References:

1. Eluri, H.B. and M.G. Naik, *Challenges of res with integration of power grids, control strategies, optimization techniques of microgrids: A review.* International Journal of Renewable Energy Research (IJRER), 2021. **11**(1): p. 1-19.
2. Upasani, M. and S. Patil. *Grid connected solar photovoltaic system with battery storage for energy management*. in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. 2018. IEEE.
3. GRID, S., *IEEE Vision for Smart Grid Controls: 2030 and Beyond.*
4. Manandhar, K., et al., *Detection of faults and attacks including false data injection attack in smart grid using Kalman filter.* IEEE transactions on control of network systems, 2014. **1**(4): p. 370-379.
5. Liu, Y., et al., *An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks.* IEEE Transactions on Smart Grid, 2016. **7**(6): p. 2923-2932.
6. Fawzi, H., P. Tabuada, and S. Diggavi, *Secure estimation and control for cyber-physical systems under adversarial attacks.* IEEE Transactions on Automatic control, 2014. **59**(6): p. 1454-1467.
7. Dehkordi, N.M., et al., *Distributed noise-resilient secondary voltage and frequency control for islanded microgrids.* IEEE Transactions on Smart Grid, 2018. **10**(4): p. 3780-3790.
8. Zuo, S., et al., *Resilient networked AC microgrids under unbounded cyber attacks.* IEEE Transactions on Smart Grid, 2020. **11**(5): p. 3785-3794.
9. Mohan, A.M., N. Meskin, and H. Mehrjerdi, *A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems.* Energies, 2020. **13**(15): p. 3860.
10. Nejabatkhah, F., et al., *Cyber-security of smart microgrids: A survey.* Energies, 2020. **14**(1): p. 27.
11. Xu, Y., *A review of cyber security risks of power systems: From static to dynamic false data attacks.* Protection and Control of Modern Power Systems, 2020. **5**(1): p. 1-12.
12. Bhamare, D., et al., *Cybersecurity for industrial control systems: A survey.* computers & security, 2020. **89**: p. 101677.
13. Sánchez, H.S., et al., *Bibliographical review on cyber attacks from a control oriented perspective.* Annual Reviews in Control, 2019. **48**: p. 103-128.
14. Mahmoud, M.S., M.M. Hamdan, and U.A. Baroudi, *Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges.* Neurocomputing, 2019. **338**: p. 101-115.
15. Villalonga, A., et al., *Cloud-based industrial cyber–physical system for data-driven reasoning: A review and use case on an industry 4.0 pilot line.* IEEE Transactions on Industrial Informatics, 2020. **16**(9): p. 5975-5984.
16. Tan, S., et al., *New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience.* IEEE Electrification Magazine, 2020. **8**(4): p. 98-106.
17. Madichetty, S. and S. Mishra, *Cyber Attack Detection and Correction Mechanisms in a Distributed DC Microgrid.* IEEE Transactions on Power Electronics, 2021. **37**(2): p. 1476-1485.
18. Ortiz, L., et al., *A review on control and fault-tolerant control systems of AC/DC microgrids.* Heliyon, 2020. **6**(8): p. e04799.
19. Sen, S. and V. Kumar, *Microgrid control: A comprehensive survey.* Annual Reviews in control, 2018. **45**: p. 118-151.
20. Martin-Martínez, F., A. Sánchez-Miralles, and M. Rivier, *A literature review of Microgrids: A functional layer based classification.* Renewable and sustainable energy reviews, 2016. **62**: p. 1133-1153.
21. Shirey, R., *Internet security glossary*. 2000, FYI 36, RFC 2828, May.
22. Pasqualetti, F., F. Dorfler, and F. Bullo, *Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems.* IEEE Control Systems Magazine, 2015. **35**(1): p. 110-127.
23. Hansen, P.B., *Operating system principles*. 1973: Prentice-Hall, Inc.
24. Zhu, B., A. Joseph, and S. Sastry. *A taxonomy of cyber attacks on SCADA systems*. in *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*. 2011. IEEE.
25. Liu, D. and D. Ye, *Cluster synchronization of complex networks under denial-of-service attacks with distributed adaptive strategies.* IEEE Transactions on Control of Network Systems, 2021.
26. Liu, X.-K., et al., *Resilient control and analysis for dc microgrid system under DoS and impulsive FDI attacks.* IEEE Transactions on Smart Grid, 2021. **12**(5): p. 3742-3754.
27. Liu, Y., P. Ning, and M.K. Reiter, *False data injection attacks against state estimation in electric power grids.* ACM Transactions on Information and System Security (TISSEC), 2011. **14**(1): p. 1-33.
28. Sahoo, S., et al., *A stealth cyber-attack detection strategy for DC microgrids.* IEEE Transactions on Power Electronics, 2018. **34**(8): p. 8162-8174.
29. Li, D., et al. *Deep learning based covert attack identification for industrial control systems*. in *2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA)*. 2020. IEEE.
30. Wang, C., et al., *Impacts of cyber system on microgrid operational reliability.* IEEE Transactions on Smart Grid, 2017. **10**(1): p. 105-115.
31. Keshk, M., et al., *An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems.* IEEE Transactions on Sustainable Computing, 2019. **6**(1): p. 66-79.
32. Yang, L., X. Cao, and J. Li, *A new cyber security risk evaluation method for oil and gas SCADA based on factor state space.* Chaos, Solitons & Fractals, 2016. **89**: p. 203-209.
33. Liu, S., et al., *Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks.* Neurocomputing, 2016. **207**: p. 708-716.

34. Granzer, W., F. Praus, and W. Kastner, *Security in building automation systems.* IEEE Transactions on Industrial Electronics, 2009. **57**(11): p. 3622-3630.
35. Hemme, K., *Critical infrastructure protection: Maintenance is national security.* Journal of Strategic Security, 2015. **8**(3): p. 25-39.
36. Cleveland, F. *IEC TC57 security standards for the power system's information infrastructure–beyond simple encryption*. in *Transmission and Distribution Conference and Exhibition*. 2005.
37. Stouffer, K., J. Falco, and K. Scarfone, *Guide to industrial control systems (ICS) security*. 2008, National Institute of Standards and Technology.
38. Cardenas, A., et al. *Challenges for securing cyber physical systems*. in *Workshop on future directions in cyber-physical systems security*. 2009. Citeseer.
39. Farwell, J.P. and R. Rohozinski, *Stuxnet and the future of cyber war.* Survival, 2011. **53**(1): p. 23-40.
40. Cao, X., et al. *The geological disasters defense expert system of the massive pipeline network SCADA system based on FNN*. in *Asia-Pacific Web Conference*. 2012. Springer.
41. Case, D.U., *Analysis of the cyber attack on the Ukrainian power grid.* Electricity Information Sharing and Analysis Center (E-ISAC), 2016. **388**: p. 1-29.
42. Hemsley, K.E. and E. Fisher, *History of industrial control system cyber incidents*. 2018, Idaho National Lab.(INL), Idaho Falls, ID (United States).
43. Strategic, C.f. and I. Studies, *Significant Cyber Incidents Since 2006.* Center for Strategic and International Studies, 2021.
44. Tan, S., et al., *False Data Injection Cyber-Attacks Detection for Multiple DC Microgrid Clusters.* Applied Energy, 2022. **310**: p. 118425.
45. Zhou, Q., et al., *A cyber-attack resilient distributed control strategy in islanded microgrids.* IEEE Transactions on Smart Grid, 2020. **11**(5): p. 3690-3701.
46. Beg, O.A., et al., *Signal temporal logic-based attack detection in DC microgrids.* IEEE Transactions on Smart Grid, 2018. **10**(4): p. 3585-3595.
47. Sahoo, S., et al., *On detection of false data in cooperative DC microgrids—A discordant element approach.* IEEE Transactions on Industrial Electronics, 2019. **67**(8): p. 6562-6571.
48. Zhao, J., et al., *Short-term state forecasting-aided method for detection of smart grid general false data injection attacks.* IEEE Transactions on Smart Grid, 2015. **8**(4): p. 1580-1590.
49. Lo, C.-H. and N. Ansari, *CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid.* IEEE Transactions on Emerging Topics in Computing, 2013. **1**(1): p. 33-44.
50. Drayer, E. and T. Routtenberg, *Detection of false data injection attacks in smart grids based on graph signal processing.* IEEE Systems Journal, 2019. **14**(2): p. 1886-1896.
51. Tu, H., et al., *A hybrid cyber attack model for cyber-physical power systems.* IEEE Access, 2020. **8**: p. 114876-114883.
52. Hu, Y., et al., *Detecting stealthy attacks against industrial control systems based on residual skewness analysis.* EURASIP Journal on Wireless Communications and Networking, 2019. **2019**(1): p. 1-14.
53. Liu, Y. and L. Cheng, *Relentless False Data Injection Attacks against Kalman Filter Based Detection in Smart Grid.* IEEE Transactions on Control of Network Systems, 2022.
54. Soltani, S., et al., *Improved estimation for well-logging problems based on fusion of four types of Kalman filters.* IEEE Transactions on Geoscience and Remote Sensing, 2017. **56**(2): p. 647-654.
55. Li, B., et al., *Detecting false data injection attacks against power system state estimation with fast go-decomposition approach.* IEEE Transactions on Industrial Informatics, 2018. **15**(5): p. 2892-2904.
56. Yan, J., F. Guo, and C. Wen, *Attack detection and isolation for distributed load shedding algorithm in microgrid systems.* IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 2020. **1**(1): p. 102-110.
57. Cecilia, A., et al., *On Addressing the Security and Stability Issues Due to False Data Injection Attacks in DC Microgrids—An Adaptive Observer Approach.* IEEE Transactions on Power Electronics, 2021. **37**(3): p. 2801-2814.
58. Pasqualetti, F., F. Dörfler, and F. Bullo, *Attack detection and identification in cyber-physical systems.* IEEE transactions on automatic control, 2013. **58**(11): p. 2715-2729.
59. Paul, A., I. Kamwa, and G. Joos, *Centralized dynamic state estimation using a federation of extended Kalman filters with intermittent PMU data from generator terminals.* IEEE Transactions on Power Systems, 2018. **33**(6): p. 6109-6119.
60. Pak, J.M., et al., *Improving reliability of particle filter-based localization in wireless sensor networks via hybrid particle/FIR filtering.* IEEE Transactions on Industrial Informatics, 2015. **11**(5): p. 1089-1098.
61. Anagnostou, G. and B.C. Pal, *Derivative-free Kalman filtering based approaches to dynamic state estimation for power systems with unknown inputs.* IEEE Transactions on Power Systems, 2017. **33**(1): p. 116-130.
62. Li, Y., Z. Li, and L. Chen, *Dynamic state estimation of generators under cyber attacks.* IEEE Access, 2019. **7**: p. 125253-125267.
63. Rawat, D.B. and C. Bajracharya, *Detection of false data injection attacks in smart grid communication systems.* IEEE Signal Processing Letters, 2015. **22**(10): p. 1652-1656.
64. Miao, K., W.A. Zhang, and X. Qiu, *An adaptive unscented Kalman filter approach to secure state estimation for wireless sensor networks.* Asian Journal of Control, 2022.
65. Sargolzaei, A., et al., *Detection and mitigation of false data injection attacks in networked control systems.* IEEE Transactions on Industrial Informatics, 2019. **16**(6): p. 4281-4292.
66. Abbaspour, A., et al., *Resilient control design for load frequency control system under false data injection attacks.*

IEEE Transactions on Industrial Electronics, 2019. **67**(9): p. 7951-7962.
67. Chattopadhyay, A. and U. Mitra, *Security against false data-injection attack in cyber-physical systems.* IEEE Transactions on Control of Network Systems, 2019. **7**(2): p. 1015-1027.
68. Qi, J., A.F. Taha, and J. Wang, *Comparing Kalman filters and observers for power system dynamic state estimation with model uncertainty and malicious cyber attacks.* IEEE Access, 2018. **6**: p. 77155-77168.
69. Adeli, M., et al., *Distributed trust-based unscented Kalman filter for non-linear state estimation under cyber-attacks: The application of manoeuvring target tracking over wireless sensor networks.* 2021.
70. Lu, J., et al., *Unscented Kalman filtering for nonlinear systems with sensor saturation and randomly occurring false data injection attacks.* Asian Journal of Control, 2021. **23**(2): p. 871-881.
71. Liu, X., Y. Mo, and E. Garone, *Local decomposition of kalman filters and its application for secure state estimation.* IEEE Transactions on Automatic Control, 2020. **66**(10): p. 5037-5044.
72. Kim, J., et al., *Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors.* IEEE Transactions on Automatic Control, 2018. **64**(3): p. 1162-1169.
73. Mao, Y., et al., *Novel stealthy attack and defense strategies for networked control systems.* IEEE Transactions on Automatic Control, 2020. **65**(9): p. 3847-3862.
74. Yamamoto, Y., N. Kuze, and T. Ushio, *Attack Detection and Defense System Using an Unknown Input Observer for Cooperative Adaptive Cruise Control Systems.* IEEE Access, 2021. **9**: p. 148810-148820.
75. Mustafa, A., et al., *Detection and mitigation of data manipulation attacks in AC microgrids.* IEEE Transactions on Smart Grid, 2019. **11**(3): p. 2588-2603.
76. Chaojun, G., P. Jirutitijaroen, and M. Motani, *Detecting false data injection attacks in AC state estimation.* IEEE Transactions on Smart Grid, 2015. **6**(5): p. 2476-2483.
77. Poudel, B.P., et al., *Detection and mitigation of cyber-threats in the DC microgrid distributed control system.* International Journal of Electrical Power & Energy Systems, 2020. **120**: p. 105968.
78. Zhu, Y. and W.X. Zheng, *Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy.* IEEE Transactions on Automatic Control, 2019. **65**(8): p. 3714-3721.
79. Nateghi, S., Y. Shtessel, and C. Edwards, *Cyber-attacks and faults reconstruction using finite time convergent observation algorithms: Electric power network application.* Journal of the Franklin Institute, 2020. **357**(1): p. 179-205.
80. Wang, X., et al., *Detection and isolation of false data injection attacks in smart grid via unknown input interval observer.* IEEE Internet of Things Journal, 2020. **7**(4): p. 3214-3229.
81. Li, Y., H. Fang, and J. Chen, *Anomaly detection and identification for multiagent systems subjected to physical faults and cyberattacks.* IEEE Transactions on Industrial Electronics, 2019. **67**(11): p. 9724-9733.
82. Barboni, A., et al., *Detection of covert cyber-attacks in interconnected systems: A distributed model-based approach.* IEEE Transactions on Automatic Control, 2020. **65**(9): p. 3728-3741.
83. Schellenberger, C. and P. Zhang. *Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system*. in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. 2017. IEEE.
84. Das, D., et al., *Luenberger observer based current estimated boost converter for PV maximum power extraction—A current sensorless approach.* IEEE Journal of Photovoltaics, 2018. **9**(1): p. 278-286.
85. Gao, R., et al., *K-filter-based adaptive output feedback control for high-order nonlinear systems subject to actuator and sensor attacks.* International Journal of Robust and Nonlinear Control, 2022. **32**(6): p. 3469-3484.
86. Yan, J., G.-H. Yang, and Y. Wang, *Dynamic Reduced-Order Observer-Based Detection of False Data Injection Attacks With Application to Smart Grid Systems.* IEEE Transactions on Industrial Informatics, 2022.
87. Wang, X., et al., *Detection and localization of biased load attacks in smart grids via interval observer.* Information Sciences, 2021. **552**: p. 291-309.
88. Alhelou, H.A.H. and P. Cuffe, *A Dynamic State Estimator Based Tolerance Control Method Against Cyberattack and Erroneous Measured Data for Power Systems.* IEEE Transactions on Industrial Informatics, 2021.
89. Wang, X., et al., *Detection and location of bias load injection attack in smart grid via robust adaptive observer.* IEEE Systems Journal, 2020. **14**(3): p. 4454-4465.
90. An, L. and G.-H. Yang, *Supervisory nonlinear state observers for adversarial sparse attacks.* IEEE Transactions on Cybernetics, 2020.
91. Yang, J., W.-A. Zhang, and F. Guo, *Adaptive distributed Kalman-like filter for power system with cyber attacks.* Automatica, 2022. **137**: p. 110091.
92. Saha, S., et al., *Sensor fault and cyber attack resilient operation of DC microgrids.* International Journal of Electrical Power & Energy Systems, 2018. **99**: p. 540-554.
93. Yan, H., et al., *A novel sliding mode estimation for microgrid control with communication time delays.* IEEE Transactions on Smart Grid, 2017. **10**(2): p. 1509-1520.
94. Ao, W., Y. Song, and C. Wen, *Adaptive cyber-physical system attack detection and reconstruction with application to power systems.* IET Control Theory & Applications, 2016. **10**(12): p. 1458-1468.
95. Rinaldi, G., et al., *Adaptive dual-layer super-twisting sliding mode observers to reconstruct and mitigate disturbances and communication attacks in power networks.* Automatica, 2021. **129**: p. 109656.
96. Zhang, Z., Y. Niu, and J. Song, *Input-to-state stabilization of interval type-2 fuzzy systems subject to cyberattacks: An observer-based adaptive sliding mode approach.* IEEE Transactions on Fuzzy Systems, 2019. **28**(1): p. 190-203.
97. Su, Q., et al., *Observer-based detection and reconstruction of dynamic load altering attack in smart grid.* Journal

of the Franklin Institute, 2021. **358**(7): p. 4013-4027.
98. Wu, C., et al., *Secure estimation for cyber-physical systems via sliding mode.* IEEE transactions on cybernetics, 2018. **48**(12): p. 3420-3431.
99. Ye, L., F. Zhu, and J. Zhang, *Sensor attack detection and isolation based on sliding mode observer for cyber-physical systems.* International Journal of Adaptive Control and Signal Processing, 2020. **34**(4): p. 469-483.
100. Utkin, V., J. Guldner, and J. Shi, *Sliding mode control in electro-mechanical systems*. 2017: CRC press.
101. Chen, G., Y. Song, and Y. Guan, *Terminal sliding mode-based consensus tracking control for networked uncertain mechanical systems on digraphs.* IEEE Transactions on Neural Networks and Learning Systems, 2016. **29**(3): p. 749-756.
102. Cecilia, A., et al., *Detection and mitigation of false data in cooperative dc microgrids with unknown constant power loads.* IEEE Transactions on Power Electronics, 2021. **36**(8): p. 9565-9577.
103. Lv, M., et al., *An integral sliding mode observer for CPS cyber security attack detection.* Chaos: An Interdisciplinary Journal of Nonlinear Science, 2019. **29**(4): p. 043120.
104. Ahmadizadeh, M., A. Shafei, and M. Fooladi, *A recursive algorithm for dynamics of multiple frictionless impact-contacts in open-loop robotic mechanisms.* Mechanism and Machine Theory, 2020. **146**: p. 103745.
105. Shafei, A. and H. Shafei, *Considering link flexibility in the dynamic synthesis of closed-loop mechanisms: A general approach.* Journal of Vibration and Acoustics, 2020. **142**(2).
106. Xu, L., et al., *A Continuous Terminal Sliding-Mode Observer-Based Anomaly Detection Approach for Industrial Communication Networks.* Symmetry, 2022. **14**(1): p. 124.
107. Wang, H., et al., *High-Order Observer-Based Sliding Mode Control for the Isolated Microgrid with Cyber Attacks and Physical Uncertainties.* Complexity, 2020. **2020**.
108. Shafei, H.R., M. Bahrami, and H.A. Talebi, *Disturbance observer-based two-Layer control strategy design to deal with both matched and mismatched uncertainties.* International Journal of Robust and Nonlinear Control, 2021. **31**(5): p. 1640-1656.
109. Yang, H., et al., *Sparse Actuator and Sensor Attacks Reconstruction for Linear Cyber-physical Systems with Sliding Mode Observer.* IEEE Transactions on Industrial Informatics, 2021.
110. Li, M., et al., *Adaptive sliding-mode tracking control of networked control systems with false data injection attacks.* Information Sciences, 2022. **585**: p. 194-208.
111. Chen, L., C. Edwards, and H. Alwi, *Sensor fault estimation using LPV sliding mode observers with erroneous scheduling parameters.* Automatica, 2019. **101**: p. 66-77.
112. Cui, S., et al., *Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions.* IEEE Signal Processing Magazine, 2012. **29**(5): p. 106-115.
113. Abianeh, A.J., et al., *Cyber-Resilient Sliding-Mode Consensus Secondary Control Scheme for Islanded AC Microgrids.* IEEE Transactions on Power Electronics, 2021. **37**(5): p. 6074-6089.
114. Shi, M., et al., *Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded AC microgrids.* IEEE Transactions on Smart Grid, 2021. **12**(3): p. 1953-1963.
115. Li, X., Q. Xu, and F. Blaabjerg, *Adaptive resilient secondary control for islanded AC microgrids with sensor faults.* IEEE Journal of Emerging and Selected Topics in Power Electronics, 2020. **9**(5): p. 5239-5248.
116. Sahoo, S., Y. Yang, and F. Blaabjerg, *Resilient synchronization strategy for AC microgrids under cyber attacks.* IEEE Transactions on Power Electronics, 2020. **36**(1): p. 73-77.
117. Afshari, A., et al., *Resilient synchronization of voltage/frequency in AC microgrids under deception attacks.* IEEE Systems Journal, 2020. **15**(2): p. 2125-2136.
118. Ozay, M., et al., *Machine learning methods for attack detection in the smart grid.* IEEE transactions on neural networks and learning systems, 2015. **27**(8): p. 1773-1786.
119. Habibi, M.R., et al., *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, 2020. **9**(5): p. 5294-5310.
120. Habibi, M.R., et al., *Secure MPC/ANN-Based False Data Injection Cyber-Attack Detection and Mitigation in DC Microgrids.* IEEE Systems Journal, 2021.
121. Zhao, S., F. Blaabjerg, and H. Wang, *An overview of artificial intelligence applications for power electronics.* IEEE Transactions on Power Electronics, 2020. **36**(4): p. 4633-4658.
122. de Almeida Florencio, F., et al. *Intrusion Detection via MLP Neural Network Using an Arduino Embedded System*. in *2018 VIII Brazilian Symposium on Computing Systems Engineering (SBESC)*. 2018. IEEE.
123. Javed, Y. and N. Rajabi. *Multi-layer perceptron artificial neural network based IoT botnet traffic classification*. in *Proceedings of the Future Technologies Conference*. 2019. Springer.
124. Pedregosa, F., et al., *Scikit-learn: Machine learning in Python.* the Journal of machine Learning research, 2011. **12**: p. 2825-2830.
125. Huma, Z.E., et al., *A hybrid deep random neural network for cyberattack detection in the industrial internet of things.* IEEE Access, 2021. **9**: p. 55595-55605.
126. Susilo, B. and R.F. Sari, *Intrusion detection in IoT networks using deep learning algorithm.* Information, 2020. **11**(5): p. 279.
127. Yan, J., Y. Qi, and Q. Rao, *Detecting malware with an ensemble method based on deep neural network.* Security and Communication Networks, 2018. **2018**.
128. Li, Y., et al., *Robust detection for network intrusion of industrial IoT based on multi-CNN fusion.* Measurement, 2020. **154**: p. 107450.
129. He, Y., G.J. Mendis, and J. Wei, *Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism.* IEEE Transactions on Smart Grid, 2017. **8**(5): p. 2505-2516.

130. Jiang, C., et al., *A mixed deep recurrent neural network for MEMS gyroscope noise suppressing.* Electronics, 2019. **8**(2): p. 181.
131. Kim, J., et al. *Long short term memory recurrent neural network classifier for intrusion detection*. in *2016 international conference on platform technology and service (PlatCon)*. 2016. IEEE.
132. Tran, D., et al., *A LSTM based framework for handling multiclass imbalance in DGA botnet detection.* Neurocomputing, 2018. **275**: p. 2401-2413.
133. Niu, X., et al. *Dynamic detection of false data injection attack in smart grid using deep learning*. in *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. 2019. IEEE.
134. Hassan, M.M., et al., *A hybrid deep learning model for efficient intrusion detection in big data environment.* Information Sciences, 2020. **513**: p. 386-396.
135. Vasan, D., et al., *MTHAEL: Cross-architecture IoT malware detection based on neural network advanced ensemble learning.* IEEE Transactions on Computers, 2020. **69**(11): p. 1654-1667.
136. Saharkhizan, M., et al., *An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic.* IEEE Internet of Things Journal, 2020. **7**(9): p. 8852-8859.
137. Goodfellow, I., Y. Bengio, and A. Courville, *Deep learning*. 2016: MIT press.
138. Liu, W., et al., *A survey of deep neural network architectures and their applications.* Neurocomputing, 2017. **234**: p. 11-26.
139. Yousefi-Azar, M., et al. *Autoencoder-based feature learning for cyber security applications*. in *2017 International joint conference on neural networks (IJCNN)*. 2017. IEEE.
140. Yan, B. and G. Han, *Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system.* IEEE Access, 2018. **6**: p. 41238-41248.
141. Memisevic, R. and G.E. Hinton, *Learning to represent spatial transformations with factored higher-order Boltzmann machines.* Neural computation, 2010. **22**(6): p. 1473-1492.
142. Fiore, U., et al., *Network anomaly detection with the restricted Boltzmann machine.* Neurocomputing, 2013. **122**: p. 13-23.
143. Imamverdiyev, Y. and F. Abdullayeva, *Deep learning method for denial of service attack detection based on restricted boltzmann machine.* Big data, 2018. **6**(2): p. 159-169.
144. Seo, S., S. Park, and J. Kim. *Improvement of network intrusion detection accuracy by using restricted Boltzmann machine*. in *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*. 2016. IEEE.
145. Wei, P., et al., *An optimization method for intrusion detection classification model based on deep belief network.* IEEE Access, 2019. **7**: p. 87593-87605.
146. Salama, M.A., et al., *Hybrid intelligent intrusion detection scheme*, in *Soft computing in industrial applications*. 2011, Springer. p. 293-303.
147. Qu, F., et al. *An intrusion detection model based on deep belief network*. in *Proceedings of the 2017 VI international conference on network, communication and computing*. 2017.
148. Zhang, Y., P. Li, and X. Wang, *Intrusion detection for IoT based on improved genetic algorithm and deep belief network.* IEEE Access, 2019. **7**: p. 31711-31722.
149. Goodfellow, I., et al., *Generative adversarial nets.* Advances in neural information processing systems, 2014. **27**.
150. Kim, J.-Y., S.-J. Bu, and S.-B. Cho, *Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders.* Information Sciences, 2018. **460**: p. 83-102.
151. Merino, T., et al. *Expansion of cyber attack data from unbalanced datasets using generative adversarial networks*. in *International Conference on Software Engineering Research, Management and Applications*. 2019. Springer.
152. Weiss, K., T.M. Khoshgoftaar, and D. Wang, *A survey of transfer learning.* Journal of Big data, 2016. **3**(1): p. 1-40.
153. Pan, S.J. and Q. Yang, *A survey on transfer learning.* IEEE Transactions on knowledge and data engineering, 2009. **22**(10): p. 1345-1359.
154. Wu, P., H. Guo, and R. Buckland. *A transfer learning approach for network intrusion detection*. in *2019 IEEE 4th international conference on big data analytics (ICBDA)*. 2019. IEEE.
155. Gao, X., et al., *Malware classification for the cloud via semi-supervised transfer learning.* Journal of Information Security and Applications, 2020. **55**: p. 102661.
156. Vu, L., et al., *Deep transfer learning for IoT attack detection.* IEEE Access, 2020. **8**: p. 107335-107344.
157. Arulkumaran, K., et al., *Deep reinforcement learning: A brief survey.* IEEE Signal Processing Magazine, 2017. **34**(6): p. 26-38.
158. Lopez-Martin, M., B. Carro, and A. Sanchez-Esguevillas, *Application of deep reinforcement learning to intrusion detection for supervised problems.* Expert Systems with Applications, 2020. **141**: p. 112963.
159. Sethi, K., et al. *Deep reinforcement learning based intrusion detection system for cloud infrastructure*. in *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*. 2020. IEEE.
160. Li, D., et al., *IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning.* International journal of information management, 2019. **49**: p. 533-545.
161. Hughes, K., K. McLaughlin, and S. Sezer, *A Model-Free Approach to Intrusion Response Systems.* Journal of Information Security and Applications, 2022. **66**: p. 103150.
162. Esmalifalak, M., et al., *Detecting stealthy false data injection using machine learning in smart grid.* IEEE Systems Journal, 2014. **11**(3): p. 1644-1652.

163. Lee, S.J., et al., *IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction.* IEEE Access, 2020. **8**: p. 65520-65529.
164. Raman, M.G., et al., *An efficient intrusion detection system based on hypergraph-Genetic algorithm for parameter optimization and feature selection in support vector machine.* Knowledge-Based Systems, 2017. **134**: p. 1-12.
165. Tang, X., S.X.-D. Tan, and H.-B. Chen. *SVM based intrusion detection using nonlinear scaling scheme*. in *2018 14th IEEE international conference on solid-state and integrated circuit technology (ICSICT)*. 2018. IEEE.
166. Shakhov, V., et al. *On Lightweight method for intrusions detection in the Internet of Things*. in *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. 2019. IEEE.
167. Habibi, M.R., et al., *Decentralized coordinated cyberattack detection and mitigation strategy in DC microgrids based on artificial neural networks.* IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021. **9**(4): p. 4629-4638.
168. Kavousi-Fard, A., W. Su, and T. Jin, *A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids.* IEEE Transactions on Industrial Informatics, 2020. **17**(1): p. 650-658.
169. Dehghani, M., et al., *Cyber-attack detection in dc microgrids based on deep machine learning and wavelet singular values approach.* Electronics, 2021. **10**(16): p. 1914.
170. Liu, Y., et al., *Robust and resilient distributed optimal frequency control for microgrids against cyber attacks.* IEEE Transactions on Industrial Informatics, 2021. **18**(1): p. 375-386.
171. Shafiee-Rad, M., et al., *Robust decentralized voltage control for uncertain DC microgrids.* International Journal of Electrical Power & Energy Systems, 2021. **125**: p. 106468.
172. Xu, L., Y. Chen, and M. Li, *Sliding Mode Resilient Control for TOD-based Servo System Under DoS Attack.* International Journal of Control, Automation and Systems, 2022. **20**(2): p. 526-535.
173. Sakthivel, R., et al., *Resilient sampled-data control for Markovian jump systems with an adaptive fault-tolerant mechanism.* IEEE Transactions on Circuits and Systems II: Express Briefs, 2017. **64**(11): p. 1312-1316.
174. Xu, Y., et al., *Resilient and robust control for event-triggered uncertain semi-Markov jump systems against stochastic cyber attacks.* International Journal of Robust and Nonlinear Control.
175. Xie, X., J. Lu, and D. Yue, *Resilient stabilization of discrete-time Takagi-Sugeno fuzzy systems: Dynamic trade-off between conservatism and complexity.* Information Sciences, 2022. **582**: p. 181-197.
176. Seyedi, Y., H. Karimi, and J. Mahseredjian, *A Data-Driven Method for Prediction of Post-Fault Voltage Stability in Hybrid AC/DC Microgrids.* IEEE Transactions on Power Systems, 2022.
177. Duan, J., W. Zeng, and M.-Y. Chow, *Resilient distributed DC optimal power flow against data integrity attack.* IEEE Transactions on Smart Grid, 2016. **9**(4): p. 3543-3552.
178. Zhang, H., et al., *Distributed load sharing under false data injection attack in an inverter-based microgrid.* IEEE Transactions on Industrial Electronics, 2018. **66**(2): p. 1543-1551.
179. Abhinav, S., et al., *Synchrony in networked microgrids under attacks.* IEEE Transactions on Smart Grid, 2017. **9**(6): p. 6731-6741.
180. Lu, L.-Y., et al., *Intrusion detection in distributed frequency control of isolated microgrids.* IEEE Transactions on Smart Grid, 2019. **10**(6): p. 6502-6515.
181. Ding, L., et al., *Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks.* IEEE Transactions on Industrial Informatics, 2019. **16**(7): p. 4909-4919.
182. Bidram, A., et al., *Resilient and cybersecure distributed control of inverter-based islanded microgrids.* IEEE Transactions on Industrial Informatics, 2019. **16**(6): p. 3881-3894.
183. Deng, C., et al., *Distributed resilient control for energy storage systems in cyber–physical microgrids.* IEEE Transactions on Industrial Informatics, 2020. **17**(2): p. 1331-1341.
184. Ding, T., et al., *A resilient microgrid formation strategy for load restoration considering master-slave distributed generators and topology reconfiguration.* Applied energy, 2017. **199**: p. 205-216.
185. Wu, C., et al., *Active defense-based resilient sliding mode control under denial-of-service attacks.* IEEE Transactions on Information Forensics and Security, 2019. **15**: p. 237-249.
186. Baghaee, H.R., et al., *A decentralized robust mixed $ h_ {{2}}/h_ {{{\infty}}} $ voltage control scheme to improve small/large-signal stability and frt capability of islanded multi-der microgrid considering load disturbances.* IEEE Systems Journal, 2017. **12**(3): p. 2610-2621.
187. Li, X., et al., *Adaptive resilient secondary control for microgrids with communication faults.* IEEE Transactions on Cybernetics, 2021.
188. Lin, C., et al., *Dynamic MGs-based load restoration for resilient urban power distribution systems considering intermittent RESs and droop control.* International Journal of Electrical Power & Energy Systems, 2022. **140**: p. 107975.
189. Xu, Y., *Resilient secure control of networked systems over unreliable communication networks.* IEEE Transactions on Industrial Informatics, 2021.
190. Zhao, Y., et al., *Adaptive Resilient Control of Cyber-Physical Systems under Actuator and Sensor Attacks.* IEEE Transactions on Industrial Informatics, 2021.
191. Deng, C., D. Zhang, and G. Feng, *Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks.* Automatica, 2022. **139**: p. 110172.
192. Song, S., et al., *Adaptive resilient control design for nonlinear time-delay systems against unknown state-dependent deception attacks.* International Journal of Robust and Nonlinear Control, 2022. **32**(4): p. 2159-2182.
193. Yang, Y., Y. Qian, and W. Yue, *A Secure Dynamic Event-Triggered Mechanism for Resilient Control of Multi-Agent*

Systems Under Sensor and Actuator Attacks. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021.
194. Meng, P., et al., *Resilient DC voltage control for islanded wind farms integration using cascaded hybrid HVDC system.* IEEE Transactions on Power Systems, 2021.
195. Zuo, S. and D. Yue, *Resilient Containment of Multigroup Systems Against Unknown Unbounded FDI Attacks.* IEEE Transactions on Industrial Electronics, 2021. **69**(3): p. 2864-2873.
196. Sadabadi, M.S., S. Sahoo, and F. Blaabjerg, *Stability-Oriented Design of Cyberattack-Resilient Controllers for Cooperative DC Microgrids.* IEEE Transactions on Power Electronics, 2021. **37**(2): p. 1310-1321.
197. Saha, S., S. Gholami, and M.K.K. Prince, *Sensor Fault-Resilient Control of Electronically Coupled Distributed Energy Resources in Islanded Microgrids.* IEEE Transactions on Industry Applications, 2021. **58**(1): p. 914-929.
198. Zuo, S. and D. Yue, *Resilient output formation containment of heterogeneous multigroup systems against unbounded attacks.* IEEE Transactions on Cybernetics, 2020.
199. Shan, Y., A. Pan, and H. Liu, *A switching event-triggered resilient control scheme for primary and secondary levels in AC microgrids.* ISA transactions, 2022.
200. Ma, X., et al., *Consensus tracking control for uncertain non-strict feedback multi-agent system under cyber attack via resilient neuroadaptive approach.* International Journal of Robust and Nonlinear Control.
201. Vigneysh, T., N. Pachauri, and V. Suresh, *Internal Model-Based Cascaded Control Approach for Multi-Functional Grid Interactive Converters.* IEEE Access, 2022. **10**: p. 19862-19874.
202. Wang, Z., et al., *Centralized security-guaranteed filtering in multirate-sensor fusion under deception attacks.* Journal of the Franklin Institute, 2018. **355**(1): p. 406-420.
203. Sahoo, S., T. Dragičević, and F. Blaabjerg, *Multilayer resilience paradigm against cyber attacks in DC microgrids.* IEEE Transactions on Power Electronics, 2020. **36**(3): p. 2522-2532.
204. Chen, X., et al., *Distributed resilient control against denial of service attacks in DC microgrids with constant power load.* Renewable and Sustainable Energy Reviews, 2022. **153**: p. 111792.
205. Sahoo, S., T. Dragičević, and F. Blaabjerg, *Resilient operation of heterogeneous sources in cooperative dc microgrids.* IEEE Transactions on Power Electronics, 2020. **35**(12): p. 12601-12605.