New Challenges in the Design of Microgrid Systems

Communication Networks, Cyberattacks, and Resilience

Tan, Sen; Wu, Yanpeng; Xie, Peilin; Guerrero, Josep M.; Vasquez, Juan C.; Abusorrah, Abdullah M.

Published in:
I E E E Electrification Magazine

DOI (link to publication from Publisher):
10.1109/MELE.2020.3026496

Publication date:
2020

Document Version
Early version, also known as pre-print

New Challenges in the Design of Microgrid Systems: Communication Network, Cyber-Attacks and Resilience

Microgrids (MGs), referred to as the next-generation power systems, are receiving considerable attention from both industry and academia. Integrated with distributed energy resources (DERs), energy storage system and a variety of loads, microgrid functions as a localized power grid which can be operated independently or connected to utility grids. With the rapid development of technology in communication networks, the framework of MGs tends to be more distributed, intelligent and tightly integrated with networks. Applications of MGs can be found on the Internet of Things (IoT), Industry 4.0, Smart Cities, etc.

However, due to the strong dependence on networks, the microgrid is more vulnerable to security threats. A malicious attacker can apply some kinds of attacks to the MG system, compromise the MG control and lead to disruptive events in the society. Such cases are posing new challenges to the design of the MG systems. Currently, the MGs are generally designed with technologies that can protect against communication delays or data dropouts and potential component failures during operations. However, due to the development of various intelligent attacks, traditional technologies behave very limitedly to secure the MGs. It is therefore essential to reexamine the existing techniques from the perspective of both cyber-layer and physical layer.

1. Communication Network

The microgrid is a robust platform that can help to build distributed electric power systems with high efficiency, sustainability, flexibility, intelligence. Due to the high penetration of renewable energy, microgrid usually works as a fully controllable unit. With the broad access to a variety of energy sources and loads, the distributed microgrid should possess the following features:

Efficient: Persistent low energy use minimize demand on grid resources and infrastructure.

Connected: Two-way communication with flexible technologies, the grid, and occupants.

Intelligent: Analytics supported by sensors and controls co-optimize efficiently, flexibility, and occupant preferences.

Flexible: Flexible loads and distributed generation/storage used to modulate energy distribution.

Toward these requirements, it is necessary to develop the microgrid with desirable performances, such as a fast response, efficient energy distribution and a satisfactory power balance between supply and demand. The realization of these goals heavily relies on an efficient and secure interaction within the microgrid, and thus addresses higher requirements for the communication network.

However, with the rapid development of advanced information and communications technology (ICT), the microgrid turns into a more complicated bi-directional P2P energy transaction network. Big data are generated and exchanged among heterogeneous resources to enhance the penetration of renewable energy and increase the flexibility of the consumption sector. Therefore, compared with the traditional communication system, the microgrid communication system is more complex and may be exposed to security threats. Considering an attacker can deliver the attacks at any communication nodes and compromise the

confidentiality, integrity, or availability of the microgrid, it is crucial to design a secure communication architecture for the microgrid to prevent the system from attacks.

1. 1 Microgrid Communication Stack

With the emergence of the Internet of Things, the concept of IoT-enabled microgrid emerges to facilitate communication among distributed energy resources, loads, energy storage system and the grid. As a consequence, the microgrid communication is constructed by a hybrid communicating network, including IoT-domain and energy-domain. Therefore, it is necessary to design the communication network in both IoT-based demand side and bus-based supply side.

Communication networks are generally established on the layered ISO/OSI (International Standards Organization/ Open Systems Interconnect reference) model. For example, the internet architecture is based on the TCP/IP model and Supervisory Control and Data Acquisition (SCADA) systems in the smart grid are based on Enhanced Performance Architecture (EPA) model. However, what is the difference among the standard OSI model, TCP/IP model, IoT model, EPA model and microgrid communication model? Fig. 1 presents the mapping of the microgrid communication stack model and standard communication stack model. It can be seen that the standard OSI model has seven layers while the TCP/IP model merging some of the OSI model layers provides a simplified concrete protocol suite for Internet communication. For the supply side, it uses EPA model which has only three layers to send and receive commands and data with SCADA through various protocols, such as Modbus, Profibus, CANbus, etc. For the demand side, more and more energy consumption sectors are being digitalized based on IoT architecture. Thousands of devices from different vendors are connected to serve various smart-X markets, such as smart homes, smart health, smart grids, smart transport, and so on.

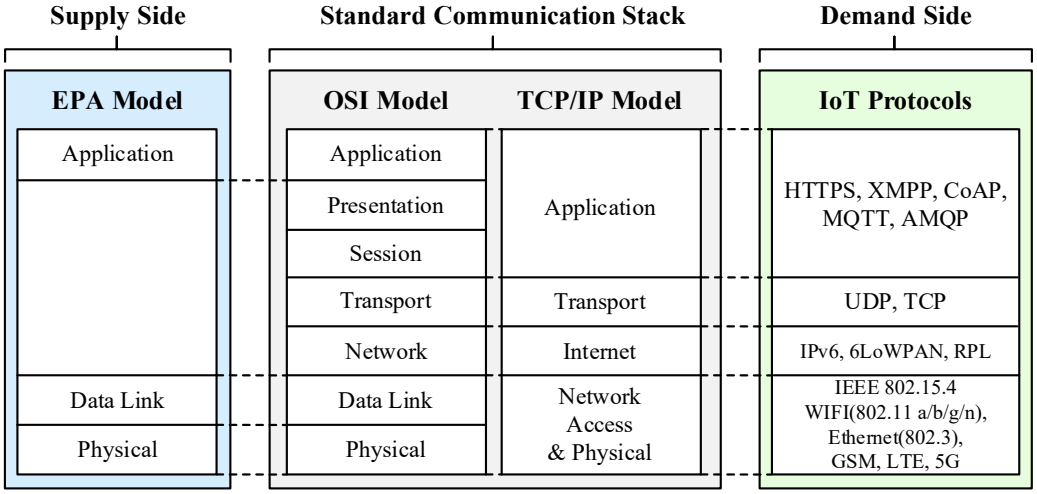

Fig. 1 Mapping of Microgrid communication stack model and standard communication stack model

1.2 Microgrid Communication Protocols

Just like people need the same language, the microgrid system requires predefined protocols to exchange information among a different layer of communication stack successfully. The communication network of the

microgrid can adopt the TCP/IP model as the backbone transmission protocol to access the public network. There are various types of protocols for the communication between two endpoints in the network access layer and application layer. Fig. 2 shows the microgrid communication protocols in these two layers concerning the supply and demand side, respectively. In the demand side, the IoT communication protocols are usually adopted. Different from the traditional request/response communication model, IoT prefers the publish/subscribe model, due to its high efficiency in exchange thousands of data via network. Whereas in the supply side, many popular electrical sectors used protocols such as MODBUS, PROFIBUS and DNP3 can be utilized based on Client-Server (Master-Slave) architectures using bus network topologies.

Additionally, some international standards designed for power communication networks can be used in the microgrid communication network. For example, the IEC 61850 is employed for communication between devices in transmission, distribution and substation automation system. IEEE 1547.x can be used for interconnecting DERs with an electric power system. IEC 61986 is introduced for data exchange between devices and networks in the distribution network.

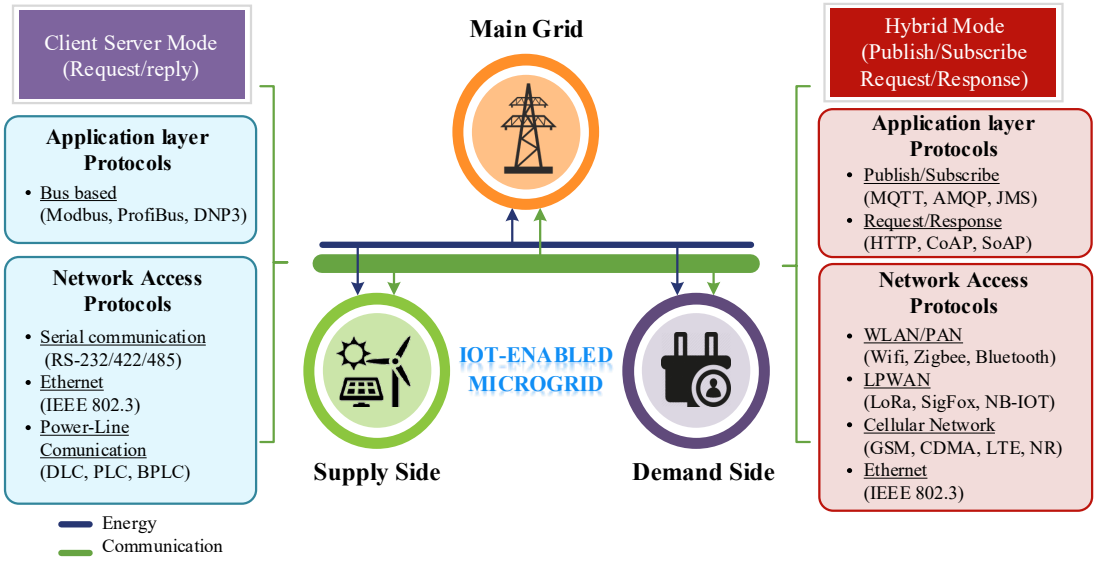

Fig. 2 Microgrid communication protocols in the network access layer and application layer

1.3 Microgrid Communication Models

From the operation perspective, it is also necessary to consider how devices from the supply and demand side connect and communicate with each other. It refers to communication modes. For the IoT-enabled microgrid system, there should be four types of communication modes, which are: (1) Device-To-Device communication model; (2) Device-To-Cloud communication model; (3) Device-To-Gateway communication model; (4) Back-End Data-Sharing Model. Each model has its framework and key features that will bring new and unique security challenges. Therefore, security and privacy should be considered respectively based on data transmission protocols of each model. Table I presents the summary of these four communication models in characteristics, typical protocols, considerations and challenges in security and privacy.

Table. I Summary of four communication models

Communication Models	Characteristics	Typical Protocols	Security & Privacy
Device-To-Device Model	▪ Devices connect and communicate directly without the intermediary layer ▪ Over heterogeneous communication wired or wireless networks ▪ Use small data packets of information to communicate ▪ vulnerable to security threats due to direct wireless connection, mobility of end users and privacy issues in social applications	▪ Bluetooth, ▪ Z-Wave, ▪ ZigBee4	▪ Authentication and Authorization ▪ Availability and Dependability ▪ Non-Repudiation ▪ Secure Routing and Transmission ▪ Confidentiality and Integrity ▪ Anonymity and Indistinguishability ▪ Context Privacy ▪ Unlinkability and Deniability
Device-To-Gateway Model	▪ Devices are converged on a gateway which as a conduit to reach upper level services ▪ The gateway layer takes over the combination of private networks and public networks. ▪ The gateway can provide security and other functionality such as data and protocol translation ▪ Usually used in the interoperability with non-IP devices.	▪ Bluetooth Smart ▪ IEEE 802.11 (Wi-Fi) ▪ IEEE 802.15.4 (LR-WPAN)	▪ Data Confidentiality ▪ Data Integrity ▪ Authentication of devices and services ▪ End-to-End Encryption ▪ Secure Onboarding ▪ Firmware Updates ▪ Integrity Management
Device-To-Cloud Model	▪ Devices connect directly to the cloud-based services ▪ Over the IP network ▪ The upper level energy-aware services and applications resident in the cloud. Outsourced storage and computation bring a new challenge to security and privacy issues.	▪ Ethernet, ▪ WIFI	▪ Identity Privacy ▪ Location Privacy ▪ Node Compromise Attack ▪ Layer Removing/Adding Attack ▪ Forward and Backward Security ▪ Semi-Trusted and/or Malicious Cloud Security
Back-End Data-Sharing Model	▪ Enable users to export and analyze smart object data from multi-data sources. ▪ Allows the data collected from single IoT device data streams to be aggregated and analyzed. ▪ An approach to achieve interoperability among these back-end systems.	▪ CoAP ▪ HTTP ▪ HTTPS ▪ Oauth 2.0 ▪ JSON	▪ End-to-End Encryption ▪ Platform & Application Integrity Verification ▪ Big Data Threats ▪ Public Key Infrastructure ▪ APIs Security ▪ Localization and Tracking

2. Microgrid Security Challenges

2.1 Cyber-attacks

Driven by the rapid development of technologies in communication networks, the MGs open a communication network over large geographical areas. The strong dependence on communication networks makes MGs vulnerable to cyber-attacks. Therefore, it is crucial to study the cyber-attacks of microgrid systems as well as their solutions. According to the different strategies performed by the attacker, various types of

attacks can be defined. Some of the most common cyber-attacks are: deny of service (DoS) attack, false data injection (FDI) attack, replay attack, etc.

The DoS attack is a kind of attempt to make the system resources unavailable. From the technology point of view, attackers can fill buffers of user domains or kernel domains, jam the shared network medium to prevent measurements and actuator data from reaching their destinations.

False data injection attack is a type of cyber-attack, in which the data integrity is modified among different cyber-parts. For instance, in microgrid systems, adversaries may launch attacks through hacking remote terminal units such as sensors in substations. It is worth mentioning that false data injection attacks in different scenarios can also be called deception attacks or malicious attacks.

A replay attack is a natural strategy, in which valid data transmission is fraudulently repeated or delayed. For instance, attackers can replicate the data recorded from the compromised sensors or actuators at a particular time.

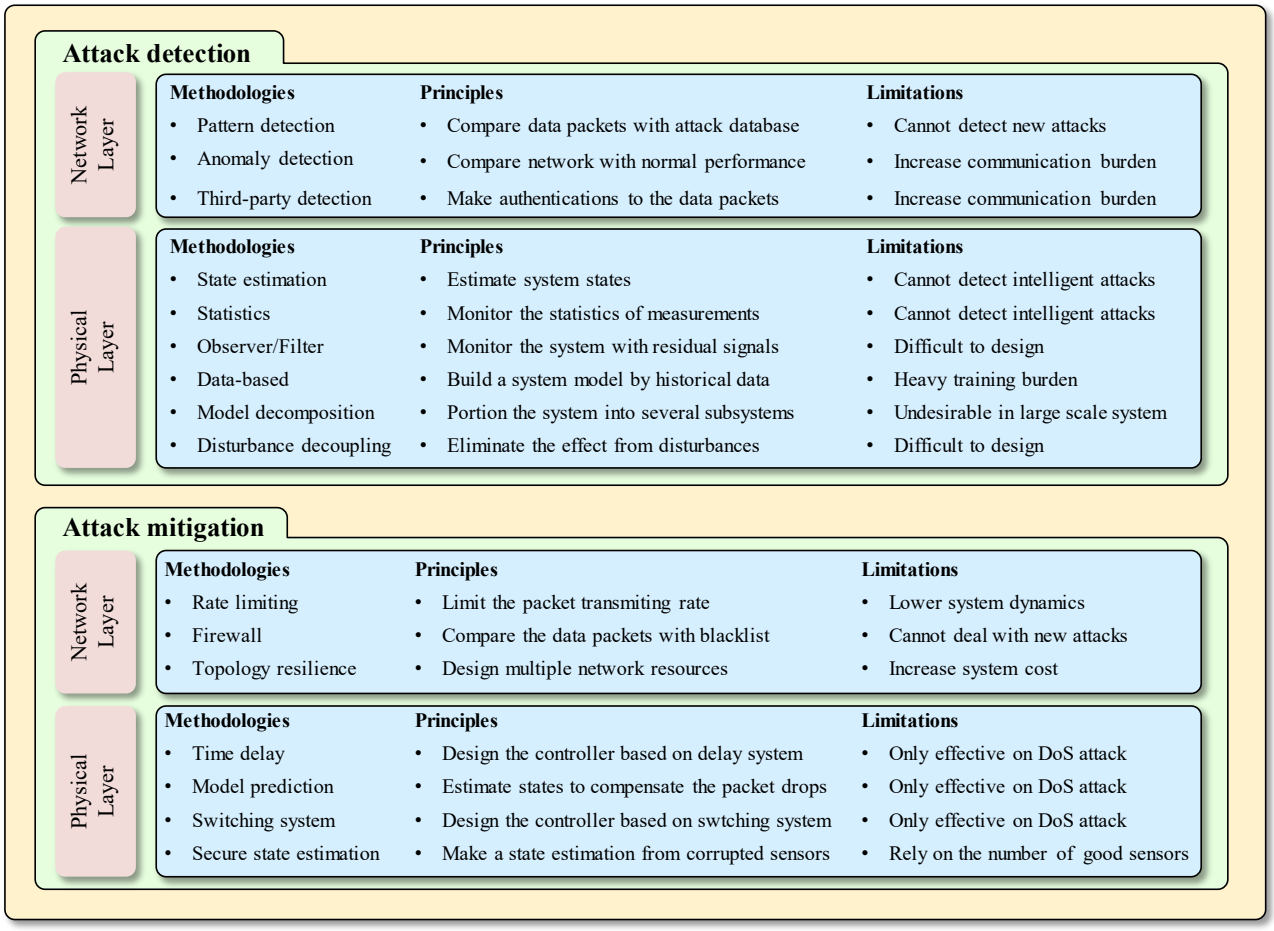

Fig. 3 Summary of attack detection and mitigation methods

2.2 Cyber-attack Detections

For systems without enough security protection strategies, malicious attacks may induce damage to power supplies and thus leads to significant societal benefits or the loss of human lives. Different from system faults

whose characteristics are generally known in advance and act in a straight way to the system, on the contrary, the cyber-attacks are usually occurred randomly and perform in a coordinated fashion to prevent themselves from being detected. Thus, it leads to the requirements of increasing the sensitivity of detection schemes to cyber-attacks. Taking the security issues into consideration, the design and analysis of attack detection schemes for microgrid have been recognized more and more attractive, which can be designed in the network layer and physical layer. Fig. 3 presents a summary of various attack detection and mitigation methods.

2.2.1 Network layer

Attack detection mechanisms deployed in the network layer can be divided into pattern detection, anomaly detection and third-party detection. Pattern detection monitors the communication network with a database that stores the signatures of known attacks. The obvious drawback is that it cannot detect new attacks. The anomaly detection method periodically compares the system performance with a predefined model under normal conditions. The model can be a fixed standard model or a well-trained time-varying model. The third-party detection approach, such as authentication, watermarking, encryption methods and key management methods, relies on the external message that can provide characterizations to the secure signals, by a variety of protocols or low-cost hardware. The data without the related characterizations are deemed as malicious attacks. However, the cost of this approach is the delay performance becaue it needs to encode and decode the external message before and after data communication. The longer and complicated the message, the more secure the authentication scheme is, the worse the delay performance. Therefore, there is a tradeoff between communication security and computational efficiency.

2.2.2 Physical layer

In the physical layer, the detection is mainly achieved by well-designed controllers of microgrid and converters. For such detection schemes, all kinds of attacks can be treated as the modification of operations and measurements, which is FDI attack. Generally speaking, the studies on attack detection can be classified into two categories, i.e., model-based scheme and data-based scheme. The model-based scheme such as state estimation, observer-based and statistical methods rely much on the system model. Thus, the appropriate model-based detection scheme should have a high model fidelity to handle parameter uncertainties and unknown disturbances. Furthermore, data-based approaches rely on machine learning or statistical mechanisms technique to infer a model for the system under inspection from both historical data and online measured signals. However, these methods usually face a heavy computational burden to train a fully connected network.

Although remarkable progress has been made in detecting attacks during the past decade, most of the studies mainly focus on centralized architectures. Indeed, these approaches are becoming increasingly unpractical to deal with attacks as a result of the complexity induced by large scale distributed MG systems. Therefore, distributed attack detection schemes should be further investigated in terms of different ways to deal with the relationships among interconnected subsystems. Model decomposition methods and disturbance decoupling methods can be addressed to deal with distributed attack detection problems for small scale and large scale MG systems, respectively.

2.3 Attack Mitigation

Attack mitigation of the microgrid plays a key role in securing the system. It aims at maintaining stability and providing acceptable performances to the grids under malicious attacks, especially in some cases where it is not possible to shut down a system, e.g. hospitals and large power plants.

2.3.1 Network layer

The principle of attack mitigation in the network layer is to reduce the impact of the attack on the communication links. Rate-limiting is one approach that imposes a rate limit on the packets, such that it can prevent DoS attacks. Furthermore, the packets can be dropped if their source addresses come from a blacklist. Another way to mitigate the attack is to add more communication channels or topologies. An attacker can delay, alter, drop or inject new packets in the communication link. Thus, once detecting an attack in a specific channel, the system can isolate the channel and move to another predefined channel, thus isolating the attack sources or machines.

2.3.2 Physical layer

The essence of attack mitigation in the physical layer is the discussion of different ways to recover system states and to achieve secure control. In terms of DoS attack and false data injection attack, a variety of attack mitigation strategies can be designed, respectively.

According to the impact of DoS attacks on the system, they can be defined as weak attack scenarios and strong attack scenarios. Weak attack scenarios are relatively moderate, which presents cases that only additional time delay and packet loss are introduced into the system. Thus, a simple secure control strategy can be obtained by considering the network under attack as a time-delay system. In other cases that the induced packet loss has compromised some of the communication links, model prediction, or state prediction can be adopted to compensate the data dropouts, and thus leads to secure control. Strong attack scenarios are situations that the communication networks between controllers and plants are almost completely congested. In such cases, the secure control can be obtained by considering the networks as switching systems between normal conditions and attacked conditions.

The FDI attacks can generate more intense effects on the system than DoS attacks, thus making it unreliable to model the system as either a time-delay system or a switching system. To provide secure control, secure state estimation, which aims to estimate the states from corrupted measurements has attracted considerable attention. The secure state estimation problems can be categorized into attack space search method, convex relaxation method and attack estimation method. It is worthy to point out that the output signals are only guaranteed to be reconstructible if a particular upper bound on the number of attacked sensors is met. Therefore, redundant sensors can help to achieve a state recovery.

2.4 Research Challenges

Although considerable attack detection and secure control approaches have been reported in recent years, some security issues remain several challenges. In the real world, many industrial processes involve nonlinear properties due to their characteristics and external environment, which make the detection more challenging compared with linear systems. Additionally, multiple sensors or meters links can be hijacked at the same time, especially in the case where a large number of sensors are considered. However, most attack detection methods

assume the single attack hypothesis in the system. Attack detection approaches for multiple attacks require to be further investigated. Furthermore, most methods can only detect one specific kind of attack. They may fail in detecting other types of attacks. For example, a well-designed detection method for DoS attack may be ineffective for a replay attack. Therefore, the design of algorithms that can deal with various kinds of attacks is of extreme importance. Apart from this, traditional attack detections are usually designed separately at the network layer and physical layer. The co-design of detection approaches may handle attacks in more sophisticated and complex cases. Concerning the secure control strategies, most of the methods only consider a single common system. Those methods are undesirable for large scale MG system due to high computational resources and communication bandwidth limitations. Therefore, secure control in a distributed manner deserves to be studied.

3. Microgrid Resilience

Although the attack detection and mitigation method can eliminate the effect of malicious attacks, they all perform in the controller layer. Additional actions must be designed in the system level to handle accidental events. This means that the resilience of microgrid requires to be strengthened to prevent physical destruction from cyber-attacks. The resilience of microgrid can be defined as the capability to prepare for, respond to, and recover from attacks and extreme events. Fig. 4 list the summary of microgrid resilience. Conceptually, it differs from the reliability that mainly focuses on potential low-impact events and can be studied case by case. Whereas, the resilience is dealing with unknown high impact events. Furthermore, the occurrence of these events is highly uncertain and cannot be predicted. Therefore, the system with high reliability may not be remarkably resilient. As the potential cyber-attacks may lead to a power blackout and cause severe social impacts, the microgrid must have the self-healing ability to continue operations in the presence of attacks. However, different from existing methods, the restoration procedure should be completely automated independent of demand from network operators. Therefore, the microgrid system needs to present some autonomous characteristics to achieve system restoration. This askes the microgrid to have a sense of situational awareness that is preparedness, perception and responsiveness, shown as Fig. 5.

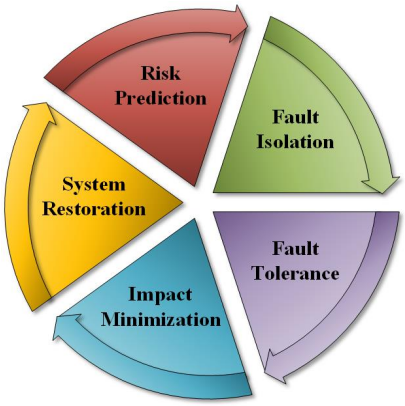

Fig. 4 The microgrid resilience

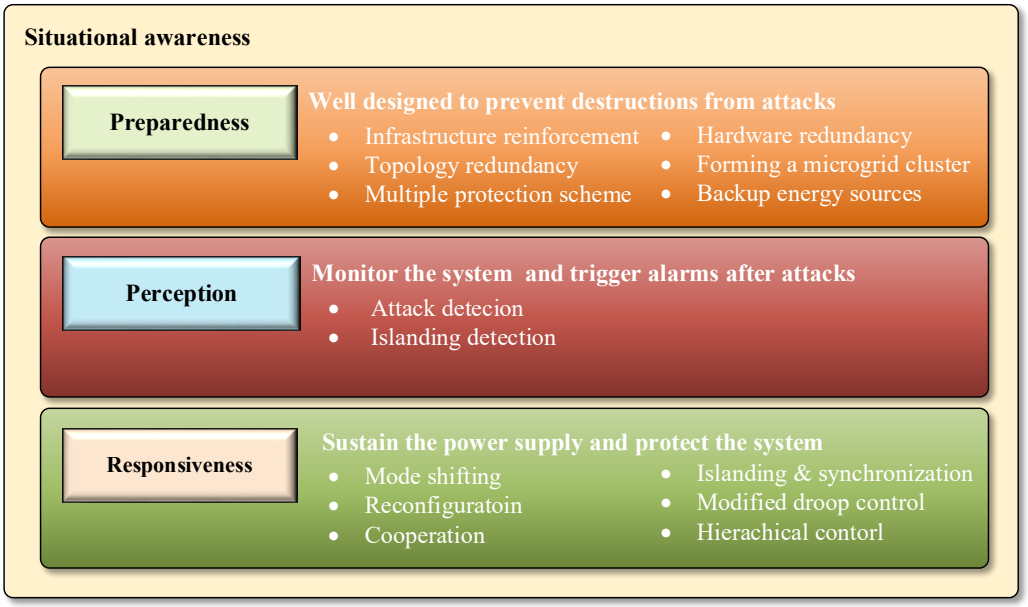

Fig. 5 The situation awareness

3.1 Preparedness

The microgrid should also be well prepared to face the security threats, to continue working and prevent the system from destructions after an attack. Firstly, the microgrid can employ a reinforced power infrastructure, such as fortified PCCs, cables, or power devices, to withstand severe events. Secondly, the system could have a certain resilience with redundant topology design such that it can guarantee the fault ride-through operation. For example, a loop-based topology can enhance microgrid resilience, as it provides multiple paths for delivering power. Thirdly, the converter controller can be developed with multiple protection schemes to allow the unfaulty switches running and bypass the faulty switches by modifying the modulation method. Fourthly, the implementation of an adaptive topology or extra hardware is also helpful in improving the microgrid resilience. The use of parallel redundant converters is a typical example of industrial applications. It is worthy to point out that such a method requires high precision to determine the time for switching the redundant hardware. Fifthly, the implementation of microgrid clusters can increase the stability of the entire system. Compared with only one microgrid, the microgrid cluster has more capability in the prevention of power blackouts. Last, the microgrid in some communities can be equipped with backup power sources or hybrid energy sources in case of device or system failures.

3.2 Perception

The microgrid system needs to have the ability to continuously monitor the system states in real-time, such that the system can prepare operational measures to limit the impact of potential damage in advance. The monitoring scheme should include distributed attack detection and islanding detection. Attack detection is the first step towards securing the system. The converter must be equipped with a robust attack detection scheme to deal with various types of attacks. Furthermore, unintended islanding may be triggered by an attack, which must be detected as fast as possible. Because the islanding detection methods usually rely on the analysis of

voltage and frequency deviation, voltage unbalances and harmonic distortion, a trustworthy PLL technique of crucial importance.

3.3 Responsiveness

The microgrid is expected to have the responsiveness, which can respond to the severe situation in a reliable manner and provide some restoration capabilities to the entire system after the occurrences of potential attacks. At the converter level, the converter should possess a self-awareness that can react to the system with local information and resources. While, at the microgrid level, the converter keeps cooperation awareness, which can collaborate with other converters in the system.

3.3.1 Converter level

Typically, the microgrid usually operates as grid feeding in grid-connected mode. To maintain the functionality of the power system, the converter can shift automatically to grid forming mode, which helps to restore the power system without enduring significant transients. However, this requires a reliable plug and play control design and stability analysis for the converters.

3.3.2 Microgrid level

The responsiveness in the microgrid level consists of reconfiguration and cooperation awareness. Reconfiguration scheme can achieve a self-healing awareness to reconfigure the network and utilize local energy sources. If the main grid or the neighbor microgrid is corrupted by the attacks, the microgrids can perform an islanding option, operate autonomously and schedule optimally, thus mitigating the impact of attacks within the microgrid. In this case, the local energy storage system and backup generation sources should sustain the power supply correctively. Possible load curtailment may be a necessity under severe conditions. Additionally, the islanded microgrids shall be reconnected to the main grid seamlessly when the main grid has ridden through the extreme conditions. This method requires powerful islanding and synchronization technologies.

Cooperation awareness allows the various energy sources to work in a coordinated way to sustain the microgrid. A typical problem in this perspective is the power-sharing, which can be performed by a standardized droop-based hierarchical control approach. However, it may fail when dealing with the reactive power and harmonic current sharing problem, especially in severe conditions. How to share and compensate the reactive power and harmonic current between each DGU is becoming a new challenge in microgrid design. Modified droop and virtual impedance methods are two alternative solutions to solve this problem.

3.4 Discussion

The resilience of microgrid can be improved by introducing the situational awareness to the system. With sufficient preparedness, the microgrids can withstand severe disruptions and maintain functionality during attacks. The perception of the microgrid can monitor the system performance and trigger an alarm in the presence of attacks. The responsiveness is the countermeasures that can avoid system failures or destructions. In practice, the preparedness, perception and responsiveness are complementary. The responsiveness actions

cannot perform an acceptable operation without a good perception scheme. The restoration may also be limited without appropriate preparedness measures.

It is easy to notice that the implementation of redundancy relies much on redundant hardware, e.g. switches, energy meters and even backup energy sources, thus leads to low efficiency and high cost. The designer should make a balance between efficiency and resilience. Usually, the requirement for resilience level is different, considering a wide range of situations. In applications such as hospitals, military uses, or large power plants, the demand for uninterruptable power supplies usually calls for a high resilience of the system. Furthermore, although the concept of resilience is important in nowadays applications, it still lacks evident indices that can perform a proper evaluation of the microgrid resilience. Therefore, how to evaluate the system resilience require to be further discussed.

4. Conclusions

The microgrid system, highly integrated with networks faces new challenges concerning security issues. This article focused on enhancing the security of microgrid systems from both the cyber layer and the physical layer. In this perspective, the communication security, attack detection, mitigation and resilience improvement technologies for the microgrid system have been presented.

Involved with ICT, the IoT-enabled microgrid plays a crucial role in the distributed power system, which contributes to a more complicated P2P energy transaction network. Therefore, the microgrid communication network (stacks, protocols and models) should be constructed both in IoT-domain and energy-domain.

The attack detection and mitigation strategies are new technologies that should be introduced to address cybersecurity issues for the microgrid system. The attack detection schemes attempt to generate an alarm during attacks, while attack mitigation methods aim to eliminate the consequent effects in the presence of attacks.

To present some actions to achieve restoration and prevent the system from physical destruction, the resilience of microgrid required to be improved. This can be achieved by increasing the situational awareness of microgrid, which consists of preparedness, perception and responsiveness. The preparation generally requests a reinforced and redundant hardware design of the system. The perception is responsible for monitoring the operational environment. And eventually, the responsiveness forces the microgrids to performs effectively to deal with cyber-attacks.

Further Reading

[1] Ying Wu, Yanpeng Wu, Josep M. Guerrero, Juan C. Vasquez, Emilio J. Palacios-Garcia, Jiao Li, IoT-enabled Microgrids Endowing Convergence and Interoperability for Energy Internet, IEEE industrial electronics magazine, 2020 (second review)

[2] Wu, Y.; Wu, Y.; Guerrero, J.M.; Vasquez, J.C.; Palacios-García, E.J.; Guan, Y. IoT-enabled Microgrid for Intelligent Energy-aware Buildings: A Novel Hierarchical Self-consumption Scheme with Renewables. Electronics, 9(4), 550, 2020.

[3] IEC, IEC 61850-7-420. Communication networks and system in power utility automation - Part 7-420: Basic communication structure - distributed energy resources logical nodes; 2009.

[4] S. Marzal, R. Salas, R. González-Medina, G. Garcerá, and E. Figueres,"Current challenges and future trends in the field of communication architectures for microgrids," Renew. Sustain. Energy Rev., vol. 82, pp. 3610–3622, Feb. 2018.

[5] Fang X, Satyajayant M, Guoliang X, Dejun Y. Smart grid — the new and improved power grid: a survey [pp. 944,980]. IEEE Commun Surv Tutor 2012;14(4). [pp. 944,980].

[6] Dizdarevic J, Carpio F, Jukan A, Masip-Bruin J. A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Comput Surv (CSUR). 2019;51(6):116.

[7] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries, " Automatica, vol. 51, pp. 135–148, 2015.

[8] S. Tan, J. M. Guerrero, P. Xie, R. Han and J. C. Vasquez, "Brief Survey on Attack Detection Method for Cyber-Physical Systems," in IEEE Systems Journal, doi: 10.1109/JSYST.2020.2991258.

[9] C. Peng, H. Sun, M. Yang and Y. Wang, "A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554-1569, Aug. 2019.

[10] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab and Y. Al-Turki, "Networked Microgrids for Enhancing the Power System Resilience," in *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1289-1310, July 2017.

5. Biographies

Sen Tan (sta@et.aau.dk) is with the Department of Energy Technology, Aalborg University, Denmark.

Yanpeng Wu (ywu@et.aau.dk) is with the Department of Energy Technology, Aalborg University, Denmark.

Peilin Xie (pxi@et.aau.dk) is with the Department of Energy Technology, Aalborg University, Denmark.

Josep M. Guerrero (joz@et.aau.dk) is with the Department of Energy Technology, Aalborg University, Denmark.

Juan C. Vasquez (juq@et.aau.dk) is with the Department of Energy Technology, Aalborg University, Denmark.

Abdullah Abusorrah (aabusorrah@kau.edu.sa) is with Department of Electrical and Computer Engineering, King Abdulaziz University, Saudi Arabia.