Journal of Integrated and Advanced Engineering (JIAE)
Vol. 1, No. 1, March 2021: 37-52
http://asasijournal.id/index.php/jiae
http://doi.org/10.51662/jiae.v1i1.11

Microgrid Communication and Security: State-Of-The-Art and Future Directions

Farah Aqilah Bohani[1,2], Sitti Rachmawati Yahya[3,*], Siti Norul Huda Sheikh Abdullah[4]
[1]Institute of Energy Infrastructure, The Energy University, Malaysia
[2]College of Computing & Informatics, The Energy University, Malaysia
[3]Department of Information System, Asia Cyber University, Indonesia
[4]Cyber Security, The National University of Malaysia, Malaysia

Abstract
The microgrid communication network with proper connectivity among microgrid resources is play important role to maintain a stability and reliability of the microgrid. Application of suitable communication network and protocol and highlighted the best security measurement is one of the elements to achieve those broad objectives. The communication network and protocol that has been implemented in existing microgrid has different types and objective which is depend on specific application. To secure the communication network and protocol, many security approaches is proposed. In this paper, a review of microgrid communication and its security is shown and future direction of communication network and protocol with its security also provided.

Keywords:
Cyber-physical System;
Cyber Security;
Intrusion Detection;
CPS Testbed;
Microgrid;

Article History:
Received: April 1, 2021
Revised: June 18, 2021
Accepted: June 19, 2021
Published: June 24, 2021

Corresponding Author:
Sitti Rachmawati Yahya
Department of Information System,
Asia Cyber University, Indonesia
Email: sitti.rachma@gmail.com

INTRODUCTION

A hardwired high-speed communication channel that conveys variables needing rapid processing for real-time control has been developed is to avoid that the high latency times of this network may not be compatible with real-time control requirements, to ensure a reliable and secure operation of a microgrid, it is crucial to design and implement an efficient communication network [1]. The consensus algorithm based on a communication system is employed in distributed hierarchical control to maintain the microgrid, operate stably and equalize the battery SoC. The structure of the microgrid communication system is closely related to microgrid control methods because the communication system in a microgrid is always spread along the power line [2]. The findings revealed that the magnitude varies depending on the MG's volatile operating conditions, the configuration of the MG converters (e.g., inductors and switches), and the length of the predicted delay periods associated with the ICT used within the MG. Based on the findings of this report, it is recommended that the design of MG take into account the limitations of the communication technologies used [3].

The energy management system (EMS), which sits in the top layer of the microgrid communication model and manages the overall operations of the island of microgrids, is one of three-layer architecture. The local controllers (LCs) that regulate operations within the local grid make up the middle layer. IoT devices, such as smart metres, fault recorders, and protective relays, make up the bottom layer, which continuously capturing and transmit the stream of sensed data. Consequently, reviewing from the past studies, communication network, security requirements, current and future trends about communications is included in this paper [4]. Smart microgrids are more vulnerable to cyber-attacks since they require cyber

systems and communication networks. Furthermore, because such microgrids are dominated by power electronics and have little inertia, cyber-attacks might have a negative impact on their stability and operation [5]. When compared to large-scale smart grids, the attack interface of microgrids is dramatically reduced. Isolation of faults is possible with less centralised and distributed semi-independent entities. As a result, key networks should continue to operate even if parts of the microgrid and the rest of the utility grid are disrupted [6].

Section 2 present architecture of microgrid and communication interface, Section 3 provides the overview of communication protocol in microgrid and its security, Section 4 review the communication network in microgrid and its security. Next, which is Section 5 discusses the future direction for microgrid research, finally, Section 6 concludes this paper.

ARCHITECTURE OF MICROGRID AND COMMUNICATION INTERFACE

The multi-agent system is extremely flexible in communication and can process in real time where necessary. The number of agents is subject to a communication protocol. The grid's electricity capacity can be increased [7]. Various microgrid architectures and control methodologies are compiled in [8] and the concepts of microgrid architecture and detailed microgrid analysis is presented inv [9]. The basic microgrid architecture is shown in Figure 1. Microgrids are interconnected systems consisting of central microgrid control (MGCC), control of micro generation (MC), load control (LC), Distributed Generation (DG) sources, energy storage and communication modules. A design and implementation of an efficient communication network is essential to ensure the reliable and secure operation of a microgrid. Contrary to popular belief, the design of this system may be more difficult because the communication needs change greatly depending on the system's nature, size, and scope, as well as the devices contained inside it [1].

Based on the voltage of the primary bus connecting all of its assets, a microgrid can be classified as DC, AC, or hybrid AC/DC MG. In AC MGs, all MG assets are connected to an AC bus, either through converters or directly, while the main grid is connected to a single AC bus. It's easier to construct and operate/control AC MG since it builds on our understanding of the main grid. Figure 2 depicts various architectures for DC, AC, and hybrid MGs [3].

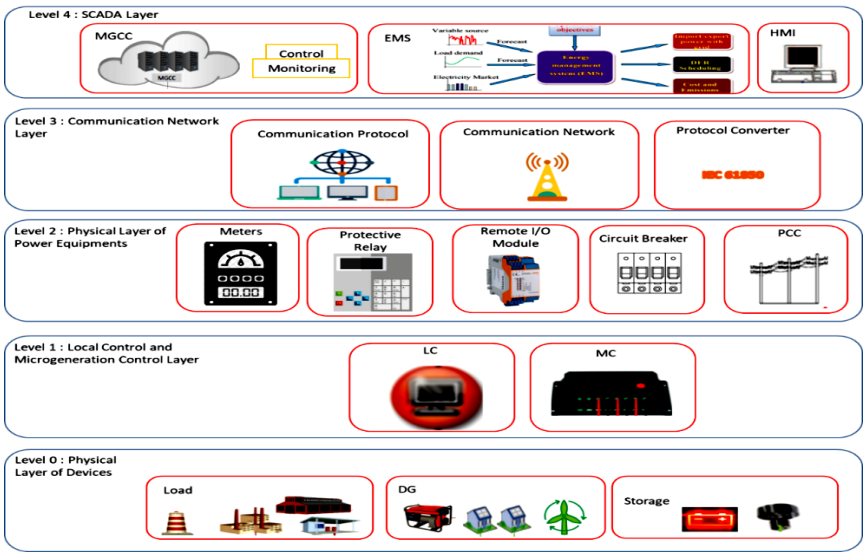

Figure 1. Basic architecture of microgrid.

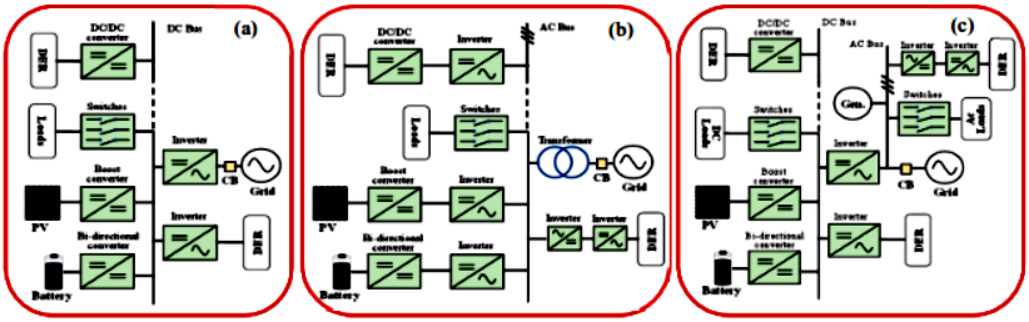

Figure 2. Examples of block diagrams for (a) DC, (b) AC, and (c) hybrid microgrids.

A DC bus collects the DC power supplied from a battery bank and a DC/AC power converter connects the whole system to the AC-50 Hz micro grid. This power converter is the same. Each power converter includes two data loggers outfitted with a variety of sensors for measuring the values of a variety of engine operating parameters that can be used to characterize the operation state of internal combustion engines and generate control signals [1]. Simulink was used to model the behaviour of the microgrid as delays increased. The severity of the problem varies depending on the MG's unpredictable operational conditions, the design of the MG converters (e.g., inductors and switches), and the length of the expected delay intervals associated with the ICT used within the MG [3]. There are two primary obstacles in developing a communication architecture for a multi-layer based smart micro-grid system. The communication and system control coordination are the first challenge. The coordination of communication between several tiers is the second challenge [10][11].

In fact, Microgrid communications provides a means of communication amongst its many pieces in order to be able to function properly and integrate them with main grid stations. The following requirements must be met by such a communication network: (i) Ensure real-time performance (ii) Ensure worst-case performance (iii) Ensure dependable and secure communication to ensure confidentiality and integrity (iv) Ensure access and availability However, while high bandwidth communication lines might reduce propagation delays, the delays produced by control elements, which are the primary source of communication messages, are outside the control of the communication network. This is due to the fact that most microgrid control devices (voltage regulators, protection relays, and so on) are equipped with low-cost, low-power processors with limited memory to perform operations. As a result, when creating an efficient security algorithm to assure confidentiality and integrity, the execution time of these devices must be taken into account [12].

COMMUNICATION PROTOCOL IN MICROGRID AND ITS SECURITY

Communication systems architecture, protocols, and tools are essential in microgrid implementation to ensure stable, reliable, and optimal operation. Microgrids components, as well as the other related system, currently work on different communication standards such as IEC 61850, Common Information Model (CIM), Open Platform Communication-Unified Architecture (OPC-UA), Modbus, and Distributed Network Protocol (DNP3) [13, 14, 15, 16]. Therefore, it requires a harmonization system to enable them to communicate each other.

As a platform to transfer data by using aforementioned communication standard, the ethernet and/or Internet Protocol (IP) is incorporated in microgrid communication. It has ability to reduce engineering cost and getting for easier setting of communication configuration. However, data delivery for microgrid communication network via the traditional TCP/IP and protocols is inefficiently performed. During the past three decades,

much more information and shared resources have become available and easy over the internet due to wide network interconnectivity.

Traditional internet which is based on TCP/IP protocol is known as the host centric model. Interestingly, this contrary to a study conducted by [17] which concludes that this protocol is impractical for microgrid since the connection involved several components/actors of the microgrid. An efficient content delivery is required since content delivery is more important than the location of data. Therefore, securing the internet demands for new requirements as the TCP/IP networks are presented with new challenges as a result of the widespread use of the Internet of Things (IoT) [18].

For communication between the microgrid controller and IEDs and other microgrid components, most microgrid use of the standard IEC 61850 via the Ethernet using the TCP/IP due to its faster speed, greater reliability and security levels. Data can be transferred from the sensors to the IEDs devices, which then produce commands to Distributed energy resources (DERs), which are the devices for storing energy, loads and interconnecting breakers or smart switches. The IEC 61850 is built with different data attributes and functionalities to ensure interoperability; hence it introduces some latencies in communication. This kind of protocol is more suitable to be applied in a microgrid particularly in distribution automation [19]. Modbus, is one of the communication protocols it also has been applied in microgrid. Reported in [20], Modbus is widely used in microgrid due to its simplicity. It can be transmitted over different physical networks of RS 485, RS 232 and the Ethernet TCP/IP [21]. However, Modbus protocol is inefficient for large data transmission from/to network.

Besides that, DNP3 is a power communication protocol originally developed by General Electric that was made public in 1993 is also has been used in microgrid communication. Usage in supervisory control and data acquisition (SCADA) applications was the initial purpose for the design of DNP3. At present, it is used largely in the oil and gas, security, water infrastructure, electrical and other industries in Asia, North America, South America, Australia and South Africa [22]. The initial design of DNP3 comprises of four layers which are the transport, application, data link, and physical layers [23]. Serial communication protocols such as the Recommended Standard (RS)-232, RS-422, or RS-485 became the basis for the design of the original physical layer. To support the current technologies in communication, the present day DNP3 has been moved over to the TCP/IP layer. It can therefore be considered as a three-layer network protocol which operates upon the TCP/IP layer [22] in supporting end-to-end communication. The slave of DNP3 is able to produce feedback with unsolicited responses to the master. Single DNP3 messages can demonstrate time stamped task and information on data quality and various data types [23].

It should be noted that DNP3 is intended to be replaced by IEC 61850 in substation communications. The general belief is that, in future power systems, IEC 61850 has the potential for usage outside of the substation communication although its usage is presently limited within a power substation [22]. Due to the inexistence of any security mechanism at the initial design of DNP3 and IEC 61850, the microgrid network can easily intercept or falsify the messages sent through them, thus resulting in either incorrect operation of power devices or information leakage. Working in tandem to rectify this problem, the security, power and network communities design microgrid applications with protocols that are secure and dependable.

The protocol that has been used in IEDs is the IEC 61850 that it includes GOOSE and SV and defines multicast message excludes a feature of cyber and information security [24]. The vulnerabilities of the IEC 61850 include packet modification, injection, replay spoofing and generation attack. Although the vulnerabilities of this protocol have been addressed through

the improvement made and the employment of the IEC 62351, it still contains some drawbacks [25]. Modification of the GOOSE packets for tripping the circuit breakers has been performed in [26]. The IEC 61850 protocol is also used in the SNAPE architecture for connecting power in which several microgrids coordinate the control and command. It has a strict timeframe for command response messages that implemented by this architecture caused by it takes a few milliseconds in communication process. Besides that, the system can also be affected in the event of additional latency in the communication.

The use of the DNP3 for the intra and inter-substation communications of the US power system is widespread [22]. The initial design of DNP3 was devoid of any security mechanism. However, the impracticality of upgrading all legacy DNP3-based power systems over a short period of time for them to be in line with the security requirements of the Smart Grid has resulted in the necessity for them to be modified or even overhauled to enable them to adopt greater security functionalities. Two major solutions were used as the basis for DNP3 security functionality design by these researchers [27, 28, 29]. Solutions: (1) the introduction of security mechanisms to the DNP3 stack through the modification of the original protocol, and (2) the insertion of a security layer between the DNP3 protocol stack and the TCP/IP layer.

The provision of suitable security solely for DNP3 is offered by the first solution. Nonetheless, the protocol stack needs to be repetitiously modified, while the communication systems in the power devices requires upgrading. As such, the compatibility of the legacy devices with the smart grid devices can be more desirably achieved through the insertion of a security layer between the DNP3 and TCP/IP. This security layer aims to specifically assist the DNP3 protocol in attaining the primary security requirements for confidentiality and integrity purposes. This is achieved through the interception of the DNP3 packets distributed to the TCP/IP layer by the security layer.

Next, the data that will be encrypted and the encrypted packets are then sent into the TCP/IP layer. All these are performed at the transmitter. Taking place at the receiver, the data packets are then passed to the application layer (DNP3 layers) after they have been decrypted by the security layer. The protection of DNP3 packets' confidentiality and integrity can be achieved either with symmetric or asymmetric algorithms. In [30] for instance, the design and implementation of MAC-based authentication are performed to function as an extension to the security of DNP3-based communication for distribution automation systems.

COMMUNICATION NETWORK IN MICROGRID AND ITS SECURITY

In light of the high penetration of RESs, this research developed a Load Frequency Control (LFC) and digital Over/Under Frequency Relay (OUFR) protection approach for an islanded microgrid system. This coordination technique is presented to ensure frequency stability and safeguard the islanded MG from high-frequency deviations, which have lately increased as a result of increased penetration of (RESs), random load changes, and system uncertainty. These modifications jeopardise the MG dynamic security by causing under/over frequency relaying and disconnecting some loads and generations, which could result in cascade failure and system collapse. The dynamic security problems of MG are shown in Figure 3. Due to the strong integration of RESs, one of these concerns is a lack of system inertia [31].

Currently, studies on the design of microgrid communication network focusing on the interaction between several microgrid components for control and monitoring purposes become an imperative topic is selected. The review shows that numerous types of communication networks are used in microgrid as shown in Table 1. That includes the Global System for Mobile Communications (GSM), Global Positioning System (GPS), optical, wireless, wired, fibers, and their associations [32].

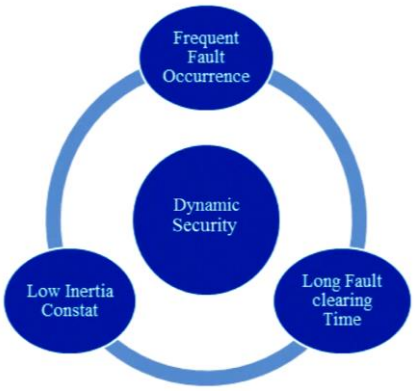

Figure 3. The microgrid dynamic security issues.

Currently, studies on the design of microgrid communication network focusing on the interaction between several microgrid components for control and monitoring purposes become an imperative topic is selected. The review shows that numerous types of communication networks are used in microgrid as shown in Table 1. That includes the Global System for Mobile Communications (GSM), Global Positioning System (GPS), optical, wireless, wired, fibers, and their associations [32].

Local Area Network (LAN) and Wide Area Networks (WANs) are some of the numerous types of communication networks available. LAN can be employed in any situation [8]. LAN could be expanded to WAN it can be used in managing broadcast/multicast communication architecture case. Both communication network has been implemented in microgrid system. WAN requires for emphasis to be placed on the level of service to all microgrid components including storage communication which has to be secure, reliable, safe, sustainable, and cost-effective. To fulfil all these requirements, the application of an internet communication protocol suite such as the Open System Interconnection (OCI) which consists of layered architecture can therefore be considered.

The Open System Interconnection (OSI) model is the benchmark communication architecture and contains 7 layers as seen in Figure 4. More than one protocol is included in each layer with a designated set of functions to be Figure 4performed under the condition of operations. Each layer is assigned a set of functions to perform under operating conditions. The most widely used and available suite is the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP normally has four layers: Application, Transport, Network, and Link layers as shown in Figure 4. Enhanced Performance Architecture (EPA) is often used in Supervisory Control and Data Acquisition (SCADA) systems that use direct communication links (i.e., no internet). This model uses only three of the seven layers defined in the OSI model [33] as depicted in Figure 4. The EPA model requires less overhead than the OSI model, at the expense of reduced functionality.

In microgrid communication, the connection between the internal and external networks, such as the enterprise network and the internet are widely exposed to cyber threats. A cyber-attack occurs with the intrusion of the microgrid power enclaves, through the attackers' exploitation of the vulnerabilities at network, system, and/or application level, thus compromising critical operations.

One of the factors of the microgrid vulnerability involves several entities when information is exchanged via WAN [34]. Further exploration on the event of an attack therefore requires for a study on the interaction between the physical system and the cyber system. For certain microgrid architectures, the researchers have chosen to follow the standards, such as NIST 800-53 [35] or IEC 62443 [36].

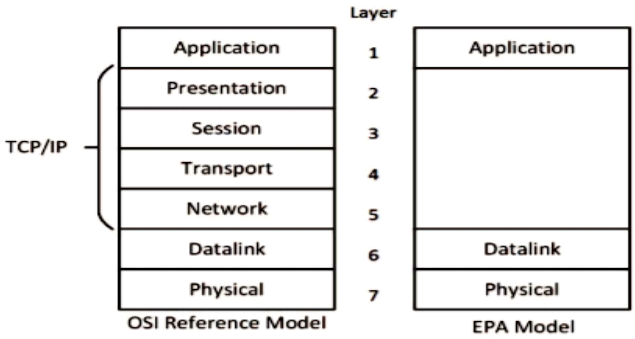

Figure 4. The Open System Interconnection (OSI) model showing the TCP/IP layers, and the Enhanced Performance Architecture (EPA) model

With lower security internal system design, majority of the systems would therefore depend on perimeter protection. This type of system is developed as part of a closed network. One of the drawbacks of the power network is it being designed without the security of the IEC 61850, which unnaturally supports security features. Owing to that, there is a requirement for the provision of a security mechanism for these protocols. However, this environment tends to offer security vulnerabilities that could be exploited by cyberattacks.

In [37], a study was performed on wired links in a system which manages microgrid energy in comparison to the Wi-Fi based servers. As indicated in the performance analysis, wireless infrastructure for a small sized microgrid control system is dependable, easy to build, and scalable. However, it demonstrated higher delays in communication compared to the wired LAN. It is therefore confirmed through tests data performed on wireless communication that Wi-Fi is a more befitting candidate for the WAN infrastructure [38][39]. This is because the communication system is slowed down due to the use of padding and wasted bandwidth in the microgrid control system since 1 to 8 bytes are utilised, while packets for the carrier are 64 bytes. However, the license-free condition of this channel increases for cyber security risks since an intruder can legally access the bandwidth. Thus, mechanisms of encryption and authentication are crucial for the integrity and confidentiality of data protection.

On the other hand, microgrid is an example of a real-life application of the WSN. The work of [40] discusses several types of attacks in a WSN system, as well as their counter measures. The work of [41] also studies the general attack on a WSN with the provision of the solutions. The solutions for a basic attack on the WSN are explained in the papers of [42, 43, 44]. Securing the wireless network through the use of standard protocols such as the IEEE 802.11i is discussed by [45], while for IEEE 802.16e is explained by [46].

Each different wireless protocol has its own security mechanism. Besides that, wired protocols are secured by virtual private networks (VPNs), firewalls, and IPSec technologies. Shell (SSH) and SSL/TLS are higher layer security mechanisms which have been used in [47]. Using secure protocols such as IPSec and SSH has been identified by system designers. However, skip the implementation details associated with establishing security associations between end points of communications. This kind approach in secure management purpose is smart grid communication system that it become complicated and make difficulty to the operations.

The mechanism of these secure protocol is that the customers will have provided with few options of key management, besides regularly have to pre-configuring symmetric keys in manually. In other words, the architects have not developed an essential management scheme which is integrated and comprehensive. Although the system designers may find the approach to be simple, yet the owners of the system find it to be expensive [48].

One of the attackers activities is access the AMI network from several nodes, such as the smart meter and local data collectors, apply the minimum level of cyber security protection. The attack on the AMI network is demonstrated in [49, 50, 51, 52], which includes customer information leakage, false data injection, and energy theft [49, 50, 51, 52]. The solution to overcome this cyber attack issues in microgrid is replacing these risk model with a parameter that is more asset-focused introduced by researchers at Sandia National Laboratories for the modification of the NIST risk model. An asset-focused parameter refers to the degree of difficulty in exploiting a vulnerability, which then causes an impact [53]. As a summary, the occurrence of risks is due to the existence of attack scenarios with difficulties at varying degrees. Each of the attack scenarios would take advantage of one or more vulnerabilities of the Cyber Physical System (CPS), thus resulting in a physical impact which consequently affect the system operation. Another secure framework which does not offer cyber security measures for microgrid-specific threats is OLE for Process Control – Unified Architecture (OPC UA) [54]. This framework is a standard-based communication backbone and has the advantage in larger scale of cyber security threats. The examples of threats include the sensitive control of network exposure, the complexities in achieving cyber security certification and the legacy of component integration.

The paper presented in [55] focuses on three problems. Firstly, several sub-networks created the internal network of a microgrid deployment, such as the microgrid control network and the SCADA network in which maintain the connection to the enterprise network. This interconnected environment can increase the probability of a cyberattack on a microgrid network. Before attempting to create chaos in the operation of other places in the microgrid control network, a malicious can exploit and attack the vector of any one of the breaking sub-networks. Secondly, many legacy devices have been implemented without security mechanisms such as message signing, encryption and message hashing. Thus, having strong and uniformed security police is difficult in the system. Lower-end devices have weaker security which can be compromised by the attackers if the security police are based on the capabilities of the device. Thirdly, in the U.S, the deployment of the Department of Defence installations requires for the certification from the Department of Defence Information Assurance Risk Management Framework (DIARMF). The existence of several sub-networks in a microgrid makes security assessment and certification tasks challenging and complex.

Even though the major reason for power outages is extreme weather events, yet they are also increasingly created and apprehensively caused by cyber-attacks [56]. The microgrid is made up of components such as the distributed energy resources (DER) which conduct transmit the power to the local load devices with also required communication, sensors, actuators, and field devices as an affective operation. Hence, a crucial role is played by methodologies in enhancing the situational awareness of cyber-attacks on the microgrid. Cyber intrusion in Cyber Physical System (CPS) can be categorized into several attacks such as a bias injection attack, replay attack, dynamic false data injection attack, denial of service attack, and eavesdropping attack [57, 58, 59, 60].

Nevertheless, the focus of all these attacks is still on one or more components of the CPS Data Confidentiality Integrity and Availability (CIA) triad, defined in common information security practices [15]. Each attack is launched at its own component based on the CIA-triad. For example, a DoS attack affects data availability, while a covert attack affects data confidentiality and integrity. An attacker has ability to manipulate a system by; 1) having ability to remote access on poorly configured firewall in a LAN network. 2) infecting the field devices [69].

A DoS event attack in microgrid can be recognized by the system operator. One type of attack which is the stealthy false data injection (FDI) is known to be the most severe cyberattack in power system. This attack is able to manipulate and corrupt the control data of the microgrid. The detection of False Data Injection (FDI) is found in [70, 71, 72, 73, 74]. The FDI detection that has been studied in microgrids on consensus control with direct current operation in which utilized by unknown input observer [70]. Nonetheless, the model of a microgrid network is defined as quasi-static. The reference work on Metasploit and rootkit in [75][76], are used in finding the exploits for most vulnerabilities, such as privilege escalation. Rootkits using known exploits easily attract attackers attention, and thus are more likely to be taken advantage. When an embedded rootkit vulnerability is exploited, it is possible to identify if it is caused by a malicious attack or the fault of the system.

The Secure Network of Assured Power Enclaves (SNAPE) architecture which based on network separation strategy was created for a large U.S. Army base where multiple power enclaves with secure communications were envisioned. A deployed microgrid system based on the SNAPE architecture would contribute to the energy security and net-zero goals of the U.S. Department of Defense. This security architecture has been designed for fast, real-time control from network and has advantages in minimization of the control network latency and also control network attack surface. The network segmentation is based on strongly cryptographic separation on hardware devices with also reduces the scope of certification to a subset of a microgrid network for solving burden of cyber security certification. The SNAPE architecture used OLE for Process Control – Unified Architecture (OPC UA) to implement the communications backbone. OPC UA is backward compatible with distributed control system protocols such as IEC 61850. OPC UA provides authentication and authorization services at the application layer.

Additionally, deploying IPv6-based networks potentially opens a number of security holes. If IPv6 and IPv4 are being run simultaneously, then IPv6 should be tunnelled over IPv4 or run independently. In the tunnelling mode, configuration problems can create security holes in the system [77]. If the two protocols are run in parallel, then firewalls have to be configured to filter the IPv6 traffic, which is not very common. A normal firewall does not filter IPv6 traffic; this insecure channel can be leveraged by an attacker to enter the system. Also, administrators must employ new (and better) ways to deploy, configure and monitor networks. Important tasks include troubleshooting networks, configuring firewalls, enforcing secure configurations, monitoring security logs, analyzing real-time behavior and performing network audits. Most intrusion detection/prevention systems are still not very effective at handling IPv6 traffic, which increases the potential of attacks.

The CERTSMicroGrid is a novel approach for integrating distributed energy resources in a microgrid to seamlessly island it from and reconnect it to the power grid [78]. To the control center, all the distributed energy resources appear to be a single entity for coordination and control. The traditional method has been to integrate a small number of distributed energy resources and to shut down the microgrid when problems arise according to the IEEE P1547 standard. However, unlike the SNAPE architecture, the CERTS model does not specifically focus on cyber security for microgrids. The Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Project is conducted jointly by the Department of Energy, Department of Defence and Department of Homeland Security [79][80]. The project goal is to provide secure control of on-base generation at military base by building secure and robust microgrids that incorporate renewable energy resources. Cyber security is provided by commercially-available technologies, so the technology itself is not novel.

Table 1. Characteristic of communication network, protocol and security level for existing microgrid

Microgrid Architecture / Framework/ Model	Year	Communication Protocol	Communication network	Supported by different communication links	Speed Communication	Implementation Level	Installation cost	Network Delay/ Latency time	Accessibility	Reliability	Security Level
Prince Lab [61]	2017	Modbus TCP/IP	Combination of fiber optic, copper, LAN	Yes	N.A.	Easy	Low	High	N.A.	N.A.	Low
Korea- KEPRI Microgrid [61, 62, 63, 64, 65]	2014, 2017	N.A	Optical fiber	N.A.	High	N.A.	N.A.	Low	N.A.	High	N.A.
Sendai Project [65][66]	2014, 2014	N.A.	GPS	N.A	N.A	N.A.	Low	N.A.	Global	Low	Low
Bronsbergen Holiday Park [67][68]	2014	N.A	Optical fiber	N.A.	High	N.A.	N.A.	Low	N.A.	High	N.A.
Kythnos [65, 66, 67]	2014, 2013	N.A.	Power line	N.A.	High	N.A.	Low	N.A.	N.A.	N.A.	Low

Unlike SNAPE, SPIDERS do not provide a comprehensive architecture to address all possible attack vectors. Mueller [81] discusses research undertaken under the NSF ERC FREEDM Project [81]. The project investigates the challenges of the cyber-physical nature of microgrids and highlights novel opportunities for providing selective power delivery during power outages. Mueller recognizes the need to secure microgrids from cyber attacks. However, the FREEDM Project does not propose any security solutions. SNAPE stands out because it recognizes the need to secure microgrids and presents a comprehensive cyber security architecture that adheres to industry standards and satisfies actual microgrid requirements.

Massie [82] presents a distributed control framework for microgrids to enhance coordination, communications and security. The framework, which uses IPv6-based communications, attempts to leverage security from IPv6 and the peer-to-peer distributed model, but it also inherits their problems. SNAPE provides all the security features provided by the framework and introduces many additional security mechanisms.

FUTURE DIRECTION FOR MICROGRID RESEARCH

In this section, we efforts to contribute to discuss and analyse the development of microgrid communication with open issues. In [33] claimed that the main point of communication platform in microgrid is reliability. This study used EPA to decrease transmission delays and complexity. Microgrid architecture and message exchange between components is based on the IEC60870-5-104 standard. The communication role for protecting the microgrid system has attention among researchers caused by produced stand-alone protection when in proper integration. Thus, IEC 61850 is introduced for a centralized microgrid protection system [83].

More research is needed on relevant technologies to highlight the best applicable communication system for microgrids, targeting overall microgrid operations, including transient response of distributed resources. More research is required for applying a suitably and the best communication for the overall operations of the microgrid. Due to producing better peer-to-peer communications and decentralized controls, extending the IEC 61850 is needed. The aim is to map the data model to traditional protocols such as DNP3. Protection of switches, fault detectors, and protective relays that grouped as sensitive data transmission is needed due to increase reliability and decrease delay. Protection of switches, fault detectors, and protective relays that grouped as sensitive data transmission is needed due to increase reliability and decrease delay. Control system functions such as reactive power control and power quality enhancement control also needed to be improved through optimizing communications technology.

Some research has been highlighted to architectures of agent–based communication which is burden of computational is integrated by a few of system components. The structure can accommodate the interconnection and operation of multiple existing legacy systems, and avoid problems associated with centralized system (i.e., single point) failure. The studied by Sandia Lab proposed a microgrid model with feedback control in multilayer environment. The model has two level of agent–based informatics architecture which is higher level consists of an agent–based informatics architecture that takes care of topology formation for the IEDs, while the lower level maintains stability of the topology chosen by the upper level. This agent–based microgrid controls and communication systems were developed and implemented using the JAVA Agent Development (JADE) framework were proposed in [84, 85, 86, 87]. Design of inverter and application of grid–tie agent–based microgrid operation is introduced in [88][89]. A comparison of Wi-Fi based servers to wired links in a microgrid

energy management system was presented in [37]. Analysis results show that wireless infrastructure is easy to build, reliable, and scalable infrastructure for implemented in small sized microgrid control system, and has limitation of communication delays is high than wired LAN. Data from tests conducted on wireless communications proven that the Wi-Fi is a suitable candidate for WAN infrastructure [38][39]. The microgrid control system uses from 1 to 8 bytes, while packets for the carrier are 64 bytes, which means padding is used and bandwidth is wasted slowing the communication system.

CONCLUSION

Securing the microgrid is important for stability and reliability of the microgrid. Vulnerabilities are increasingly present in the cyber-power system environment due to the growing dependency on computer systems and digital communication. This paper has been surveyed on communication network and protocol and its security. This paper also discussed about future direction of microgrid security. Based on literature, usage of SNAPE techniques in a more aggressive way that has been proposed.

Although several microgrid security approach have been proposed and tested for different sectors of a microgrid, there is no guarantee for the detection rate in practice. Finally, further research on coordinated cyber attacks is much needed. Also, the response of operators should be taken into account in the cyber security studies.

ACKNOWLEDGMENTS

The authors acknowledge the BOLD2018 grant from IRMC, UNITEN. Thank also to Ministry of Education, Malaysia for supporting this work under grant no. 20190102LRGS. Special thanks to U-TC-RD-19-09 and U-TE-RD-20-08 who also supported this project.

REFERENCES

[1] A. Cagnano, H. H. R. Sherazi and E. D. Tuglie, “Communication system architecture of an industrial-scale microgrid: A case study”, in *Journal of Internet Technology*, vol. 2, no. 14, pp. 1-6, August 2019, doi: 10.1002/itl2.126.

[2] H. Yang, Q. Li, and W. Chen, “Microgrid communication system and its application in hierarchical control”, in *Smart Power Distribution Systems - Control, Communication, and Optimization*, pp. 179-204, October 2019, doi: https://doi.org/10.1016/B978-0-12-812154-2.00009-2.

[3] M. Saleh, Y. Esa, M. E. Hariri and A. Mohamed, “Impact of Information and Communication Technology Limitations on Microgrid Operation”, *IEEE Transactions on Sustainable Energy*, vol. 12, pp. 1-24, July 2019, doi: 10.3390/en12152926.

[4] S. Kumar, S. Islam and A. Jolfaei, “Microgrid communications – protocols and standards”, in *book: Variability, Scalability and Stability of Microgrids*, pp. 291-326, July 2019, doi: 10.1049/PBPO139E_ch9.

[5] F. Nejabatkhah, Y. W. Li, H. Liang and R. R. Ahrabi, “Cyber-Security of Smart Microgrids: A Survey”, *IEEE Transactions on Sustainable Energy*, vol. 14, pp. 1-27, December 2020, doi: https://dx.doi.org/10.3390/en14010027.

[6] X. Zhong, L. Yu, R. Brooks and G. K. Venayagamoorthy, “Cyber Security in Smart DC Microgrid Operations”, in *IEEE First International Conference on DC Microgrids (ICDCM)*, pp. 86-91, July 2015, doi: 10.1109/ICDCM.2015.7152015.

[7] K. Khadedah, V. Lakshminarayanan, N. Cai and J. Mitra, “Development Of Communication Interface Between Power System and the Multi-Agents for Micro-Grid Control”, *North American Power Symposium (NAPS)*, pp. 1-6, October 2015, doi: 10.1109/NAPS.2015.7335083.

[8] L. Berrío and C. Zuluaga, "Concepts, standards and communication technologies in smart grid," *2012 IEEE 4th Colombian Workshop on Circuits and Systems (CWCAS)*, 2012, pp. 1-6, doi: 10.1109/CWCAS.2012.6404056.

[9] M. Bartsch, T. Ewich, C. Freckmann, R. Heming, M. Huckschtag, H. Kanisch et al., “VGB-s 175–IT Security for Generating Plants,” *VGB PowerTech eV Technical Report*, 2014.

[10] Y. Si, N. Korada and R. Ayyanar, "A High Performance Communication Architecture for a Smart Micro-Grid Testbed Using Customized Edge Intelligent Devices (EIDs) With SPI and Modbus TCP/IP Communication Protocols", in *IEEE Open Journal of Power Electronics*, vol. 2, pp. 2-17, February 2021, doi: 10.1109/OJPEL.2021.3051327.

[11] S. Khan and R. Khan, "Elgamal Elliptic Curve Based Secure Communication Architecture for Microgrids", *IEEE Transactions on Sustainable Energy*, vol. 11, no. 4, pp. 759-774, March 2018, doi: 10.3390/en11040759.

[12] M. Chlela, G. Joos and M. Kassouf, "Impact of cyber-attacks on islanded microgrid operation", *Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems*, June 2016, pp. 1-5, doi: 10.1145/2939940.2939943.

[13] V. C. Gungor et al., "A Survey on Smart Grid Potential Applications and Communication Requirements," in *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 28-42, Feb. 2013, doi: 10.1109/TII.2012.2218253

[14] R. Amin, J. Martin and Xuehai Zhou, "Smart Grid communication using next generation heterogeneous wireless networks," *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012, pp. 229-234, doi: 10.1109/SmartGridComm.2012.6485988

[15] M. A. Ahmed, Y. C. Kang, and Y-C. Kim, "Communication network architectures for smart-house with renewable energy resources," *Energies*, vol. 8, no. 8, pp. 8716-8735, 2015, doi: 10.3390/en8088716

[16] A. Usman and S. H. Shami, "Evolution of communication technologies for smart grid applications," *Renewable and Sustainable Energy Reviews*, vol. 19, pp. 191-199, March 2913, doi: 10.1016/j.rser.2012.11.002

[17] K. Monteiro, M. Marot and H. Ibn-khedher, "Review on microgrid communications solutions: a named data networking – fog approach," 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 2017, pp. 1-8, doi: 10.1109/MedHocNet.2017.8001656

[18] W. Shang, Y. Yu, R. Droms and L. Zhang, "Challenges in IoT networking via TCP/IP architecture," Technical Report, NDN-0038 NDN Project, 2016

[19] M. Chlela, G. Joos and M. Kassouf, "Impact of cyber-attacks on islanded microgrid operation," Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems, June 2016, pp. 1-5, doi: 10.1145/2939940.2939943

[20] F. Martin-Martínez, A. Sánchez-Miralles and M. Rivier, "A literature review of Microgrids: A functional layer based classification," Renewable and Sustainable Energy Reviews, vol. 62, pp. 1133-1153, doi: 10.1016/j.rser.2016.05.025

[21] A. Bani-Ahmed, L. Weber, A. Nasiri and H. Hosseini, "Microgrid communications: State of the art and future trends," 2014 International Conference on Renewable Energy Research and Application (ICRERA), 2014, pp. 780-785, doi: 10.1109/ICRERA.2014.7016491.

[22] S. Mohagheghi, J. Stoupis and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," *2009 IEEE/PES Power Systems Conference and Exposition*, 2009, pp. 1-9, doi: 10.1109/PSCE.2009.4840174.

[23] A. Segall, "Distributed network protocols", *IEEE transactions on Information Theory*, vol. 29, no. 1, pp. 23-35, 1983, doi: 10.1109/TIT.1983.1056620.

[24] J. Hong, C. Liu and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," *ISGT 2014*, 2014, pp. 1-5, doi: 10.1109/ISGT.2014.6816375

[25] M. Strobel, N. Wiedermann and C. Eckert, "Novel weaknesses in IEC 62351 protected Smart Grid control systems," *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2016, pp. 266-270, doi: 10.1109/SmartGridComm.2016.7778772

[26] J. Hong, C. Liu and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," in *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1643-1653, July 2014, doi: 10.1109/TSG.2013.2294473

[27] M. Majdalawieh, F. Parisi-Presicce and D. Wijesekera, "DNPSec: Distributed network protocol version 3 (DNP3) security framework," *Advances in Computer, Information, and Systems Sciences, and Engineering*, Springer; 2007, pp. 227-234

[28] L. Jeffrey, H. James and C. Sandip, "Cyber security enhancements for SCADA and DCS systems," *Technical Report TR-ISRL-07-02*, University of Louisville; 2007

[29] G. Gilchrist, "Secure authentication for DNP3," *2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp. 1-3

[30] I. H. Lim et al., "Security Protocols Against Cyber Attacks in the Distribution Automation System," in *IEEE Transactions on Power Delivery*, vol. 25, no. 1, pp. 448-455, Jan. 2010, doi: 10.1109/TPWRD.2009.2021083.

[31] G. Magdy, E. A. Mohamed, G. Shabib, A. A. Elbaset and Y. Mitani, "Microgrid dynamic security considering high penetration of renewable energy", Protection and Control of Modern Power Systems - Springer, August 2018, vol. 3, no. 23, pp. 1-11, doi: https://doi.org/10.1186/s41601-018-0093-1.

[32] H. Y. Li and B. Yunus, "Assessment of Switched Communication Network Availability for State Estimation of Distribution Networks With Generation," in *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1424-1432, July 2007, doi: 10.1109/TPWRD.2006.883019

[33] R. Bi, M. Ding and T. T. Xu, "Design of common communication platform of microgrid," *The 2nd International Symposium on Power Electronics for Distributed Generation Systems*, 2010, pp. 735-738, doi: 10.1109/PEDG.2010.5545914

[34] G. N. Ericsson, "Toward a Framework for Managing Information Security for an Electric Power Utility—CIGRÉ Experiences," in *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1461-1469, July 2007, doi: 10.1109/TPWRD.2007.900298.

[35] J. T. Force and T. Initiative, "Security and privacy controls for federal information systems and organizations," *NIST Special Publication*, vol. 800, pp. 8-13, 2013

[36] NN, "International Electrotechnical Commission," *IEC 62443*, Industrial Communications Networks – Network and System Security. Geneva, Switzerland, 2013.

[37] L. K. Siow, P. L. So, H. B. Gooi, F. L. Luo, C. J. Gajanayake and Q. N. Vo, "Wi-Fi based server in microgrid energy management system," *TENCON 2009 - 2009 IEEE Region 10 Conference*, 2009, pp. 1-5, doi: 10.1109/TENCON.2009.5395995

[38] S. Shukla, Yi Deng, S. Shukla and L. Mili, "Construction of a microgrid communication network," *Innovative Smart Grid Technologies (ISGT) 2014*, 2014, pp. 1-5, doi: 10.1109/ISGT.2014.6816412

[39] G. Stanciulescu, H. Farhangi, A. Palizban and N. Stanchev, "Communication technologies for BCIT Smart Microgrid," *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2012, pp. 1-7, doi: 10.1109/ISGT.2012.6175669

[40] T. Azzabi, H. Farhat and N. Sahli, "A survey on wireless sensor networks security issues and military specificities," *2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET)*, 2017, pp. 66-72, doi: 10.1109/ASET.2017.7983668.

[41] A. Rani and S. Kumar, "A survey of security in wireless sensor networks," *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, 2017, pp. 1-5, doi: 10.1109/CIACT.2017.7977334.

[42] H. Dai, H. Wang, H. Xiao, X. Li and Q. Wang, "On Eavesdropping Attacks in Wireless Networks," *2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES)*, 2016, pp. 138-141, doi: 10.1109/CSE-EUC-DCABES.2016.173

[43] M. H. Ahmed, S. W. Alam, N. Qureshi and I. Baig, "Security for WSN based on elliptic curve cryptography," *International Conference on Computer Networks and Information Technology*, 2011, pp. 75-79, doi: 10.1109/ICCNIT.2011.6020911.

[44] Singh RS, Prasad A, Moven RM, Sarma HKD. Denial of service attack in wireless data network: A survey. 2017 Devices for Integrated Circuit (DevIC): IEEE; 2017. p. 354-9.

[45] "IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)* , vol., no., pp.1-3534, 14 Dec. 2016, doi: 10.1109/IEEESTD.2016.7786995.

[46] Group IW, "Part 16: Air interface for fixed and mobile broadband wireless access systems," *IEEE P802 16e/D8*, 2005

[47] A. Bendahmane, M. Essaaidi, A. El Moussaoui and A. Younes, "Grid computing security mechanisms: State-of-the-art," *2009 International Conference on Multimedia Computing and Systems*, 2009, pp. 535-540, doi: 10.1109/MMCS.2009.5256638.

[48] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998-1010, Fourth Quarter 2012, doi: 10.1109/SURV.2012.010912.00035

[49] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi and W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," in *IEEE Systems Journal*, vol. 8, no. 2, pp. 509-520, June 2014, doi: 10.1109/JSYST.2013.2260700.
[50] X. Liang, X. Li, R. Lu, X. Lin and X. Shen, "UDP: Usage-Based Dynamic Pricing With Privacy Preservation for Smart Grid," in *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 141-150, March 2013, doi: 10.1109/TSG.2012.2228240.
[51] B. Krebs, "FBI: Smart meter hacks likely to spread. Krebs on Security," Available online: http://krebsonsecurity com/2012/04/fbi-smart-meter-hacks-likely-to-spread/(accessed on 25 April 2012). 2012.
[52] H. Rosenbaum, *Danville Utilities Sees Increase in Meter Tampering*, 2012.
[53] G. D. Wyss, J. F. Clem, J. L. Darby, K. Dunphy-Guzman, J. P. Hinton and K. W. Mitchiner, "Risk-based cost-benefit analysis for security assessment problems," *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, 2010, pp. 286-295, doi: 10.1109/CCST.2010.5678687.
[54] O. Foundation, *Unified Architecture*, Scottsdale, Arizona, 2015.
[55] A. Mohan, G. Brainard, H. Khurana and S. Fischer, "A cyber security architecture for microgrid deployments," *International Conference on Critical Infrastructure Protection*, Springer; 2015, pp. 245-259.
[56] M. Knowledge, "Microgrid Cybersecurity: Protecting and Building the Grid of the Future," *S&C Electric Company*, 2019, pp. 1-12.
[57] F. Pasqualetti, F. Dörfler and F. Bullo, "Attack Detection and Identification in Cyber-Physical Systems," in *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715-2729, Nov. 2013, doi: 10.1109/TAC.2013.2266831.
[58] A. Teixeira, I. Shames, H. Sandberg and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135-48, 2015
[59] D. I. Urbina, J. Giraldo, A. A. Cardenas, J. Valente, M. Faisal et al., "Survey and new directions for physics-based attack detection in control systems: US Department of Commerce," *National Institute of Standards and Technology*, 2016.
[60] Y. Mo and B. Sinopoli, "Secure control against replay attacks," *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2009, pp. 911-918, doi: 10.1109/ALLERTON.2009.5394956.
[61] A. Cagnano, E. De Tuglie and L. Cicognani, "Prince—Electrical Energy Systems Lab: A pilot project for smart microgrids," *Electric power systems research*, vol. 148, pp. 7-10, 2017
[62] E. Hossain, E. Kabalci, R. Bayindir and R. Perez, "Microgrid testbeds around the world: State of art," *Energy Conversion and Management*, vol. 86, pp. 132-153, 2014
[63] S. Bracco, F. Delfino, F. Pampararo, M. Robba and M. Rossi, "The University of Genoa smart polygeneration microgrid test-bed facility: The overall system, the technologies and the research challenges," *Renewable and sustainable energy reviews*, vol. 18, pp. 442-459, 2013
[64] J. Romankiewicz, C. Marnay, N. Zhou and M. Qu, "Lessons from international experience for China's microgrid demonstration program," *Energy Policy*, vol. 67, pp. 198-208, 2014
[65] M. Qu, *Microgrid policy review of selected major countries, regions, and organizations*, 2014
[66] C. Marnay, *International microgrid assessment: Governance, incentives, and experience (IMAGINE)*, 2014
[67] G. Kyriakarakos, D. D. Piromalis, A. I. Dounis. K. G. Arvanitis and G. Papadakis, "Intelligent demand side energy management system for autonomous polygeneration microgrids," *Applied Energy*, vol. 103, pp. 39-51, 2013
[68] T. Loix and K. Leuven, *The first micro grid in the Netherlands: Bronsbergen*, Available online on February 2009.
[69] Y. Mo et al., "Cyber–Physical Security of a Smart Grid Infrastructure," in *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012, doi: 10.1109/JPROC.2011.2161428.
[70] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini and G. Ferrari-Trecate, "Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids," *2018 European Control Conference (ECC)*, 2018, pp. 344-349, doi: 10.23919/ECC.2018.8550549.
[71] O. A. Beg, T. T. Johnson and A. Davoudi, "Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids," in *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2693-2703, Oct. 2017, doi: 10.1109/TII.2017.2656905.

[72] S. Sahoo, S. Mishra, J. C. Peng and T. Dragičević, "A Stealth Cyber-Attack Detection Strategy for DC Microgrids," in *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162-8174, Aug. 2019, doi: 10.1109/TPEL.2018.2879886.

[73] S. Abhinav, H. Modares, F. L. Lewis and A. Davoudi, "Resilient Cooperative Control of DC Microgrids," in *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1083-1085, Jan. 2019, doi: 10.1109/TSG.2018.2872252.

[74] M. M. Rana, L. Li and S. W. Su, "Cyber attack protection and control of microgrids," in *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 2, pp. 602-609, Mar. 2018, doi: 10.1109/JAS.2017.7510655.

[75] G. Hoglund and J. Butler, *Rootkits: subverting the Windows kernel*, Addison-Wesley Professional; 2006.

[76] Symantec, *Turning the tables: Loadable kernel module rootkits deployed in a honeypot environment*, 2006.

[77] J. Lyne, *Why IPv6 matters for your security*, Sophos, Oxford, United Kingdom, 2014.

[78] R. Lasseter, A. Akhil, C. Marnay, J. Stephens, J. Dagle, R. Guttromsom, et al., "Integration of distributed energy resources," *The CERTS Microgrid Concept. Lawrence Berkeley National Lab.(LBNL)*, Berkeley, CA (United States); 2003.

[79] J. Stamp, "The SPIDERS project - Smart Power Infrastructure Demonstration for Energy Reliability and Security at US military facilities," *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2012, pp. 1-1, doi: 10.1109/ISGT.2012.6175743.

[80] NN, *SPIDERS Microgrid Project secures military installations*, Sandia Labs News Release,. Albuquerque, New Mexico: Sandia National Laboratories; 2012.

[81] M. Frank, *Cyber-Physical Aspects Of Energy Systems For The 21st Century: A Perspective From The Nsf Erc Freedm Projec*, 2009.

[82] D. Massie, "Implementation of a cyber secure microgrid control system," *SPIDERS JCTD Industry Day*, 20114.

[83] T. S. Ustun, C. Ozansoy and A. Zayegh, "Simulation of communication infrastructure of a centralized microgrid protection system based on IEC 61850-7-420," *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012, pp. 492-497, doi: 10.1109/ SmartGridComm.2012.6486033.

[84] N. C. Ekneligoda and W. W. Weaver, "Game-Theoretic Communication Structures in Microgrids," in *IEEE Transactions on Power Delivery*, vol. 27, no. 4, pp. 2334-2341, Oct. 2012, doi: 10.1109/TPWRD.2012.2210057.

[85] E. Kuznetsova, Y-F. Li , C. Ruiz and E. Zio, "An integrated framework of agent-based modelling and robust optimization for microgrid energy management," *Applied Energy*, vol. 129, pp. 70-88, 2014

[86] T. Logenthiran, D. Srinivasan and D. Wong, "Multi-agent coordination for DER in MicroGrid," 2008 IEEE International Conference on Sustainable Energy Technologies, 2008, pp. 77-82, doi: 10.1109/ICSET.2008.4746976.

[87] A. Saleem, N. Honeth and L. Nordström, "A case study of multi-agent interoperability in IEC 61850 environments," *2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe)*, 2010, pp. 1-8, doi: 10.1109/ISGTEUROPE.2010.5638876.

[88] H. M. Abdar, A. Chakraverty, D. H. Moore, J. M. Murray and K. A. Loparo, "Design and implementation a specific grid-tie inverter for an agent-based microgrid," *2012 IEEE Energytech*, 2012, pp. 1-6, doi: 10.1109/EnergyTech.2012.6304676.

[89] G. Shahgholian, "A brief review on microgrids: Operation, applications, modeling, and control", in *Journal of International Transactions on Electrical Energy Systems*, vol. 31, no. 4, pp. 1-28, March 2021, doi: 10.1002/2050-7038.12885.