

# Review of the State-of-the-Art on Adaptive Protection for Microgrids based on Communications

Daniel Gutierrez-Rojas, *Student Member, IEEE*, Pedro H. J. Nardelli, *Senior Member, IEEE*,  
Goncalo Mendes, Petar Popovski, *Fellow, IEEE*

**Abstract**—The dominance of distributed energy resources in microgrids and the associated weather dependency require flexible protection. They include devices capable of adapting their protective settings as a reaction to (potential) changes in system state. Communication technologies have a key role in this system since the reactions of the adaptive devices shall be coordinated. This coordination imposes strict requirements: communications must be available and ultra-reliable with bounded latency in the order of milliseconds. This paper reviews the state-of-the-art in the field and provides a thorough analysis of the main related communication technologies and optimization techniques. We also present our perspective on the future of communication deployments in microgrids, indicating the viability of 5G wireless systems and multi-connectivity to enable adaptive protection.

**Index Terms**—Microgrids, Adaptive protection, Communication Systems, RES DER, 5G, URLLC.

## LIST OF ACRONYMS

DER	Distributed Energy Resources.
DoS	Denial of service.
DPN3	Distributed network protocol.
GOOSE	Generic Object-Oriented Substation Event.
IEDs	Intelligent Electronic Devices.
IoT	Internet of Things.
LAN	Local Area Network.
MPMC	Microgrid Protection Management Controller.
NS	Network Slicing.
RES	Renewable Energy Sources.
RTPS	Real-Time Publish-Subscribe.
SCADA	Supervisory Control and Data Acquisition.
SMV	Sampled Measured Values.
SNTP	Simple Network Time Protocol.
URLLC	Ultra Reliable and Low Latency Communications.

## I. INTRODUCTION

The electrification of energy systems based on Renewable Energy Sources (RES) contributes towards reaching United Nations Sustainable Development Goal 7 — “Ensure access to affordable, reliable, sustainable and modern energy for

all”. Furthermore, to build transmission lines and distribution lines, as well as new communications infrastructure to serve the traditional power systems, is becoming more and more challenging due to, for instance, growing pressures over environmental licensing, funding allocation, etc. It has been suggested that the centralized paradigm of energy delivery is reaching its technical boundaries and no longer seems to constitute the most effective approach for granting continuous and reliable power supply to customers located at the edge of the grid, especially in countries with a high percentage of non-urban area installations [1]. The above trends have led to increasing interest in installing small scale generation closer to the consumption nodes – Distributed Energy Resources (DER).

Practical modernization of the electrical grid usually refers to small-scale cluster integration of DER and customer demand at the distribution level — microgrids. Microgrids are localized electrical systems with autonomous control and enhanced grid-demand interaction, which are also able to operate in grid-connected and islanded mode [2], [3]. Sophisticated features of microgrids as advanced power electronics and complex control configurations impose substantial technical challenges. Protection schemes and strategies against internal and external faults, which can harm system elements or consumer equipment are among those challenges. Microgrid operational conditions may vary rapidly due to DER contribution with low inertia of non-rotating elements and rapid changes in weather conditions (wind and solar radiation) [4] or due to sudden state changes between connected and islanded mode. External faults are normally cleared using conventional protection schemes at the distribution level, but these schemes may not be suitable to microgrid internal faults [5].

To ensure safe and appropriate operation, all variables of the microgrid elements shall be monitored and required changes shall be applied to the device protection settings dynamically when the operating conditions of the grid change (e.g., due to fault occurrence). Conventional protection schemes, however, rely on large inertia and long transient periods, which are insufficient in this new microgrid context dominated by DER. Thus, adaptive schemes become necessary [6], [7]. The self-implemented changes by adaptive protection devices are based on “intelligent” algorithms that process the available data, making the microgrid a cyber-physical system. This leads to an additional concern about the cyber domain: failures in algorithms may stress or even harm physical components [8].

In microgrids that rely on a central management controller, the communication of Intelligent Electronic Devices (IEDs) is

D. Gutierrez-Rojas, P. Nardelli and G. Mendez are with Lappeenranta-Lahti University of Technology, Lappeenranta, Finland. (e-mails: daniel.gutierrez.rojas@lut.fi, Pedro.Nardelli@lut.fi, Goncalo.Mendes@lut.fi). P. Popovski is with the Department of Electronic Systems, Aalborg University, Denmark (e-mail: petarp@es.aau.dk).

used to keep the system updated on the current state of the grid, tracking the operating currents and making proper fault detection [7], [9], [10]. A reliable communication between the system elements is therefore needed. In fact, any type of electrical protection scheme that relies on communication requires robustness, a virtually full-time availability and strictly bounded latency [11]. Those stringent requirements associated with communications are hard to meet for any current communication system (either wired or wireless). Latency as low as 10 ms, high reliability (i.e., packet error rate lower than 99.999%), high availability ( $\approx 99.999\%$ ) and time synchronization are some of the key requirements that the fifth generation of wireless mobile networks (5G) promise to achieve for safe operation of electrical protection systems and that previous technologies alone cannot satisfy due to lack of performance and cost-effective solutions. In particular, the integration of different existing technologies with 5G with other wireless interfaces (e.g., WiFi, LTE, or NB-IoT) to exploit the *interface diversity* also known as multi-connectivity offers an already feasible solution for many applications that requires high reliability with latency at order of milliseconds, as shown in [12]. Such a performance is only becoming possible due to major advancements in machine-type communications, adopting specific solutions for different regimes related to data rates, coverage, availability, reliability and latency. The deployment of Network Slicing (NS) and different types of control messages to establish connections are also examples of wireless communication engineering solutions to comply with the above mentioned strict quality of service requirements.

It is also important to consider the different protocols available for communications in grid protection. The Standard IEC 61850 includes messaging protocols for control and grid automation that are ideal for adaptive protection. Although various review papers on adaptive microgrid protection and their communication schemes have been published [6], [7], [13], [14], none of them actually considers the possibility of using emerging 5G mobile communications as part of their proposed solutions. We try here to fill this gap by reviewing of the state-of-the-art of adaptive protection focusing on the communication aspects and how 5G technologies can be deployed as an enabling technology.

The rest of this paper is divided as follows. Section II presents a generic case that highlights the need for adaptive protection schemes in microgrids. Section III presents a review of techniques for adaptive protection and communication approaches in microgrids. Section IV discusses finding done in previous chapters, introduces how 5G can become a reliable communication system for adaptive microgrid protection and elaborates on outstanding issues and challenges in this area. Conclusions are finally presented in Section V.

## II. ADAPTIVE PROTECTION SCHEMES IN MICROGRIDS

The most common type of protection in electrical distribution systems today is overcurrent-based protection. This mission-critical application requires from the communication system a latency between 12 and 20 ms with 99.999% of

reliability for sensing/metering and control purposes [15]. Overcurrent protection is impacted more than any other protection function by connection of DER [16] due to bidirectional current flow to faulted point. The state of the different circuit breakers in the electrical grid also plays a significant role in the protection settings. Consider a generic case representation of a microgrid depicted in Fig. 1 with a common IEC 61850 communication setup.

### A. Adaptive setting

The electrical system in Fig. 1 is composed by three main circuit breakers (CB1, CB2 and CB3) which are responsible for maintaining the power supply within the microgrid and two circuits breakers (CB4 and CB5) at the DER infeed. Given overcurrent protection functions for CB1 and CB2 associated with an IED located at BUS 1 and three different cases for their setting and reclosing:

1) *Case 1: CB1, CB2 Closed and CB3, CB4, CB5 Opened:* Without any infeed from DER at CB4 and CB5, and applying the rule of thumb where the overcurrent settings ( $CB_S$ ) is inside the interval of double the magnitude of load current  $I_l$  and half of the minimum current fault  $I_f$ , as shown in (1):

$$CB_S = \left[ I_l \times 2, \frac{I_f}{2} \right], \quad (1)$$

where currents are measured in A.

At CB1 the protection setting in relation to the current is given by:

$$CB_{S1} = \left[ 400 \times 2, \frac{2000}{2} \right] \Rightarrow [800, 1000]. \quad (2)$$

For CB1, the rule of thumb applies correctly and then we only have to choose a setting value given inside the limits showed in (2).

Likewise for CB2:

$$CB_{S2} = \left[ 500 \times 2, \frac{1000}{2} \right] \Rightarrow [1000, 500]. \quad (3)$$

In this case, when we do not have an optimal interval, in order to find a setting we sum the minimum fault current 500 (A) and load current 1000 (A) divided by 2, which returns a setting of 750 (A). The setting must be above load current and below minimal fault current.

2) *Case 2: CB2, CB3 Closed and CB1, CB4, CB5 Opened:* With CB3 closed, the setting at CB2 has lower margin from minimum fault current due to the increase of load current. Having 900 (A) of load current and 1000 (A) as minimum fault current, we must find a middle point for setting at 950 (A). As establish before, a setting below the maximum load current could make the protective device operate under normal operating conditions and a setting above minimal current fault the protective device would not be able to identify and clear any fault under faulty conditions. This means an increase in the setting at CB2 while the previous setting is inadequate for this case because at some point the load current may be seen as fault current by the IED causing complete isolation of both loads.

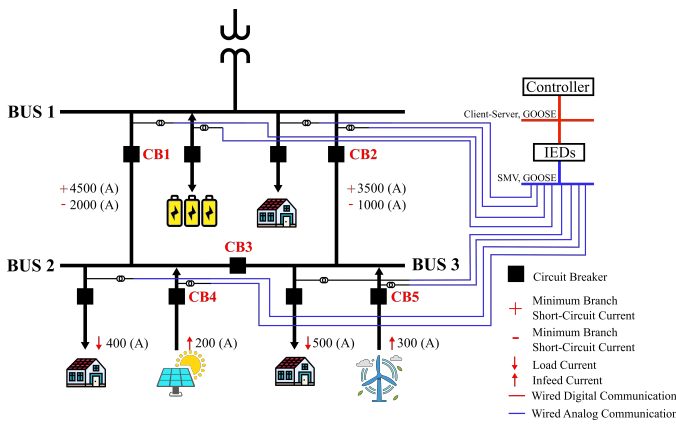


Fig. 1: Generic case of a microgrid adaptive setting with fault and load current.

3) *Case 3: CB2, CB3, CB4, CB5 Closed and CB1, Opened:* With the infeed of DER into the microgrid the protection setting at CB2 can also change. A total infeed of 500 A leaves the maximum load seen from the IED at 400 A and consequently a bigger margin for setting overcurrent protection function at CB2.

These different cases within a simple microgrid configuration shows the necessity of awareness of the IED to know operation conditions of the network so they can adapt to its actual state by changing their overcurrent settings and guarantee a reliable protection for all elements. This means, complete fault isolation including selectivity. Considering case 3 microgrid state, if there is a fault at BUS 2, both loads (or part of the load, if DER had a manageable way to supply part of the load at BUS 3) would get disconnected by operation of CB2, but with a centralized wireless proposed scheme, as shown in the following chapters, that situation could be avoided and power supply of load at BUS 3 could be ensured, by having a lower overcurrent setting at CB2 and operation of CB3 instead.

4) *Auto-reclosing:* Once a fault in a given microgrid network is cleared by protective devices, it is important to reclose as fast as possible to minimize the lack of power supply and provide stability to the system. Auto-reclosing, though, can degrade the life of some elements or even cause permanent damage if the attempt is unsuccessful. The auto-reclosing action is mostly a control function that can be easily performed at the Microgrid Protection Management Controller (MPMC) level, to mitigate any possible damage to the system; the line branches that have less current contribution are the ones to reclose first. This implies that the MPMC has to know the current state of the circuit breakers of the microgrid, along with real-time operation currents and fault currents, so that the line branches that reclose first can be determined. Since the current measuring is performed at IEDs, these devices need to communicate with the MPMC. Similarly to the protective system for fault clearance, wireless communication seems to be a more suitable solution for this task due to its flexibility.

### B. Adaptive protection algorithms

Traditional distribution systems are designed to have radial configuration, in order to supply power from a single power

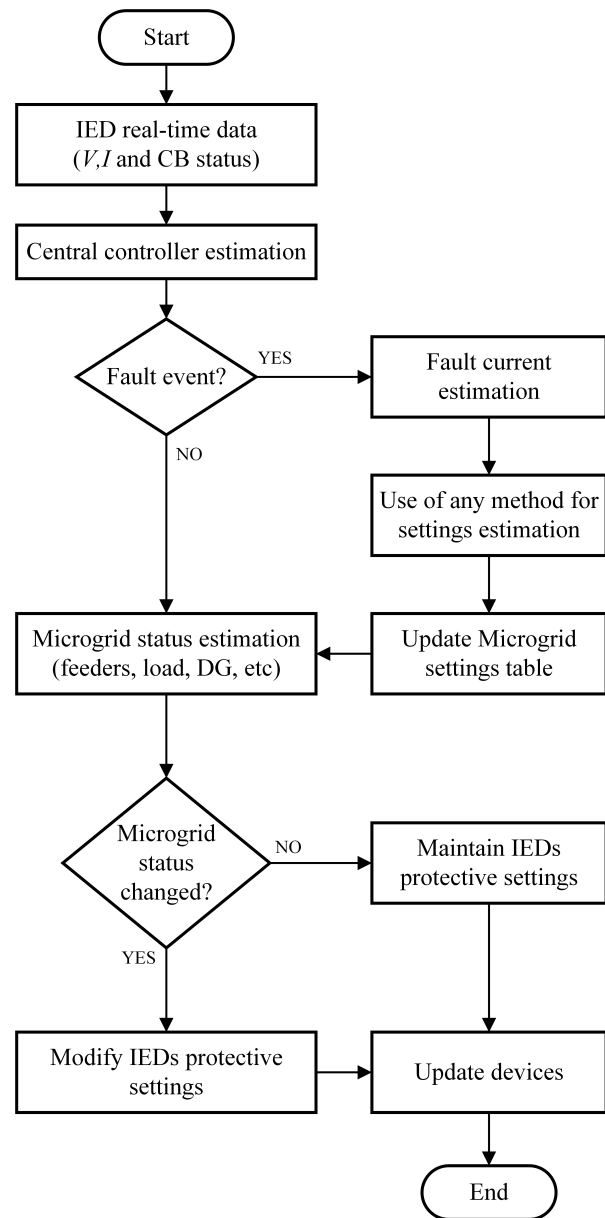


Fig. 2: Typical adaptive protection scheme (Adapted from [18], [19]).

source at a time. This means that current will flow only in one direction, i.e. from the source (distribution feeders) to the load (consumer). Protection functions for radial configuration usually include non-directional overcurrent relays or IEDs, with fixed settings and no need for communication within protective elements [17]. As microgrids start to proliferate and DER penetration in distribution networks increases, power flow and therefore also fault current become bidirectional. Adaptive protection schemes appear as an option to solve the fault clearance challenges that are imposed in this scenario.

Fig. 2 shows the flow chart of a typical adaptive protective scheme implementation. First the real-time data gathered by the IEDs is collected and sent through a wired communication channel (usually Ethernet-based) where it is received by the MPMC (Fig. 3) [20], which will analyse if a trip action was made and whether it was, or not, from a fault occurrence. Then, the microgrid state is evaluated for possible temporary

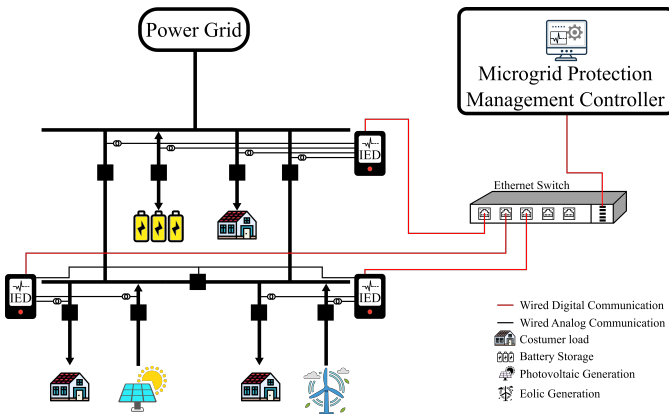


Fig. 3: Implementation of wired ethernet-base communications for an over-current adaptive protection scheme (Adapted from [18]).

conditions in the system after any possible reclose from the circuit breakers. Based on the fault currents the system will update the settings at the decision-making table and depending of the state of circuit breakers, a signal could be sent back to the IEDs to rewrite their actual settings for the new ones.

Additionally, in [19] after the measurements are gathered, a block of artificial neural networks and another of support vector machine algorithms estimate whether there is a fault and its location, respectively. A least square estimation is employed for comparison before updating the decision table. In [21], the whole tripping process is shown by dividing the flow chart into two main blocks (relay agent and central controller agent) performing an examination of grid state and updating the values of relays. After a fault occurs, the new state is evaluated to calculate new relay settings. A calculation of the average of total communication latency that involves the previous described blocks was described in [20]. Adaptive protection schemes use different methods to solve their setting adjustment when needed. Those methods also rely on different optimization techniques to find an efficient but fast method to change a predetermined variable of the IED. Examples include differential search algorithm [22], fuzzy logic and genetic algorithm [23], modified particle swarm optimization [24].

### III. EXISTING COMMUNICATION APPROACHES IN ADAPTIVE PROTECTION SYSTEMS

#### A. Wired and wireless implementations

In wired communication-based automation and adaptive protection implementations, the data transfer between IEDs and the MPMC takes place through cables installed at the substation level. Wireless communication, on the other hand, operates based on radio frequency signals. Both implementations have advantages and disadvantages and whether one is more appropriate than the other is entirely reliant of the use case. Table I presents a comparison between wired and wireless applications of some of the characteristics of substation control that are relevant for adaptive protection.

Wired connections are generally considered to be highly reliable but their total cost and lack of flexibility impose additional challenges when new equipment is installed at the substation. Wired and wireless communication can also be

TABLE I: Wired and wireless communication for substation automation.

Characteristics	Wired	Wireless
Reliability	- Once the installation is complete, probability to fail is very low	- Redundancy can lower probability to fail
Stability	- Not distorted by other connections or objects	- Variation in the latency could be experienced depending on the interference by other networks
Visibility	- Not visible by other wired connections but could be connected by nodes to facilitate data transfer	- Might be visible to other wireless connections depending of the bandwidth
Speed	- Independent cables avoid unexpected and unnecessary data making transfer faster	- Latency of 5G deployments can perform equal or better than wired networks
Security	- Firewall and other applications provide enough security when the installation is monitored	- Signals that propagate through can be intercepted. Proper encryption technologies can avoid this
Cost	- Design, space adequation and installation could be costly	- Cost of installation relatively inexpensive
Mobility	- Stationary without possibility of fast reallocation	- Flexible and easy to add new components or reallocation
Installation	- Depending on size and requirements, it can take longer to set up	- Requires less equipment and fast installation
Maintenance	- Potentially costly depending of number of elements	- Due to less elements, less costly and less frequent maintenance

combined to enhance the tasks performed by each element of the network, such as in [25], where a mix of technologies such as Fiber Optics, Broadband Power Line over medium voltage, and Wi-Fi are used for control and measuring. However, most work found in the literature adopts less sophisticated physical wired communications, for high reliability and low latency.

In this context, the role of emerging technologies in wireless communications (5G and integration of 5G other wireless communication interfaces) can be groundbreaking. Not only will these be able to efficiently address the drawbacks from legacy wireless communications, but also to significantly enhance its capabilities. Furthermore, the discussion on the need for more versatile communication technologies i.e. applicable to the generality of implementation use cases, increasing efficiency and reducing costs, is a valid one. Thus, the authors propose a change of paradigm of microgrid automation and control towards a scenario of prevalent adaptive protection implementations, which as explained constitute a significant departure from contemporary wired installations.

#### B. Traditional communication architectures

Recent literature on adaptive protection of microgrids has revealed a variety of approaches for analyzing the performance of the respective algorithms and methodologies. Some approaches focus on centralized or decentralized management for data processing and control, while others focus on the communication infrastructure to reduce times of on-line settings adjustment. Most of the utilized algorithms were tested in grid-connected operation conditions. A small set, however, can also

TABLE II: Mapping of communication approaches used in adaptive protection schemes for microgrids. Their main features are discussed throughout Sec. III.

Reference		Controller		Communication			Operation Mode	
Year	Cite	Centralized	Decentralized	Wired	Wireless	Standard/Protocol	Grid-connected	Islanded
2019	[19]	✓		✓		IEC 61850, SNTP	✓	✓
	[26]	✓		✓		IEC 61850	✓	
	[27]	✓		—	—	—	✓	
	[28]		✓	✓		—	✓	✓
	[29]	✓		✓		—	✓	
	[30]	✓		✓		RTPS		✓
	[31]			✓			✓	
2018	[32]		✓	✓			✓	✓
	[33], [34]		✓	—	—	—	✓	
	[35]		✓	✓		—	✓	
	[36]–[38]	✓		—	—	IEC 61850, DPN3	✓	✓
	[39]	✓		✓		IEC 61850	✓	✓
	[40]	✓		✓		—	✓	✓
	[41]	✓		✓		Telnet	✓	
	[42]	✓		✓		—	✓	
	[20]		✓	✓		IEC 61850	✓	
	[43], [44]	✓		✓	✓	IEC 61850,60870-5-101	✓	
	[21]	✓	✓	✓		IEC 61850	✓	✓
	[23]	✓		—	—	IEC 61850,60870-5-101	✓	
	[7]			✓	✓			✓
	[25]			✓	✓	IEC 61850	✓	
	[45]			✓	—	—	✓	✓
[46]	—	—	—	—	—	✓		
[47]–[53]	—	—	—	—	—	—	—	
2017	[54]	✓	✓	—	—	—	✓	✓
	[55]	✓		—	—	—	✓	✓
	[56]	✓		—	—	IEC 61850, DPN3	✓	✓
	[57]		✓	✓		—	✓	
	[58]		✓	✓	✓	—	✓	
	[59]	✓	✓	—	—	—	✓	✓
	[60]		✓	✓		—	✓	✓
	[61]	✓		✓		—	✓	
	[62]		✓	✓	✓	Point-to-Point	✓	
	[63]	✓		✓	✓	—	✓	✓
[24], [64]–[68]	—	—	—	—	—	✓		
2016	[69]–[71]	✓		✓		—	✓	
	[72]	✓		✓		IEC 61850	✓	✓
	[73]	✓		✓		IEC 61850, DPN3	✓	✓
	[22]	✓		✓		IEC 61850	✓	
	[74]	✓		✓		IEC 61850, DPN3	✓	
	[75]	—	—	—	✓	—	✓	
	[76]	✓		—	—	IEC 61850, IEEE 1588	✓	✓
	[77]	✓		—	—	—	✓	✓
	[78]	—	—	—	—	—	✓	✓
[79]–[84]	—	—	—	—	—	✓		
2015	[85]	✓		✓		IEC 61850	✓	
	[86]	✓		—	—	IEC 61850	✓	✓
	[87]	✓		—	—	—	✓	✓
	[88]	✓		—	—	—	✓	✓
	[89], [90]	✓		✓		—	✓	
	[91]			—		—	✓	
	[92]			—		—		✓
	[93], [94]	✓		—	—	—	✓	
	[18], [95], [96]	✓		✓		IEC61850	✓	✓
	[97]	✓	✓	—	—	—	✓	✓
	[98]	—	—	—	—	—	✓	✓
[99]–[101]	—	—	—	—	—	✓		

— Not specified

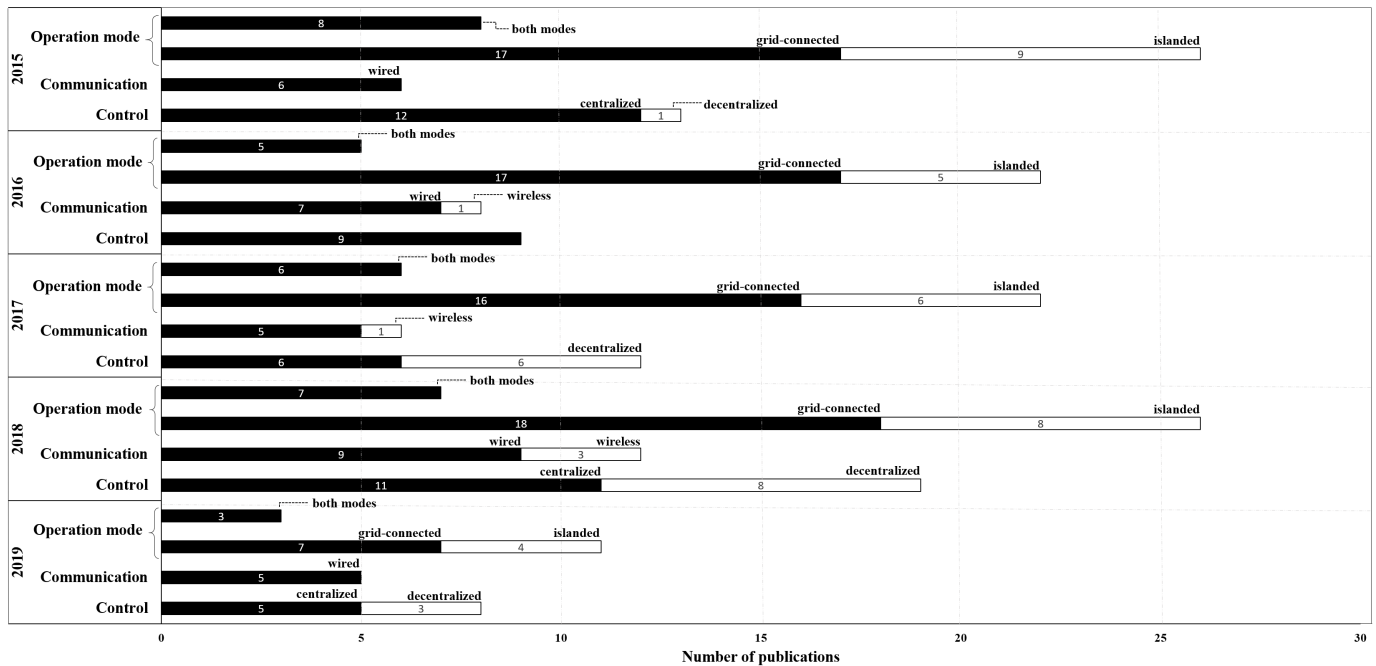


Fig. 4: Communication approaches found in microgrid adaptive protection literature, expressed in number of publications per year.

work under islanded mode, in order to test control robustness of adaptive protection in case of communication failures or disconnection from the grid, when DER are present.

Table II summarizes the aforementioned approaches to adaptive protection in microgrids, in the last five years. In [19], a centralized approach chosen. The paper states that the methodology requires database available before hand and it is obtained through simulation. It proposes a data mining methodology to quantitatively extract meaningful information from the database.

As for the implementation, the authors used a wired communication approach, along with Simple Network Time Protocol (SNTP) and Supervisory Control and Data Acquisition (SCADA), which includes the IEC 61850 standard. The authors considered both grid connected and island operation modes. A fractionalization of microgrid protection is made in [28] to avoid dependency of centralized management and to improve reliability, which can also work in grid-connected and island operation modes. In [20] and [25], a decentralized methodology is proposed using the IEC 61850 standard for grid-connected operation mode. A combination of adaptive communication-based decentralized (pre-contingency) and centralized (post-contingency) protection schemes is shown in [21], which is suitable for both grid-connected and islanded operation modes. Also in this paper, the IEC 61850 is used for communication between the elements.

When a microgrid is in island mode, it often loses its communication capabilities with a central server, leaving all protection devices operating with stationary settings or not being adjusted to the lower setting, which means the fault will not be detected. To overcome this problem, in case of communication failure, [54] proposes a solution using a supercapacitor with bidirectional Voltage Source Converter to

contribute for the fault current and raise current value to certain level, which is sensed by the relay and a comparison between high and low settings can be made. In [58], numerical relays and a global system for Mobile communications modem are connected to communicate with each other (schematic shown in [102]) and perform a decentralized adaptive protective action due to very good coverage. Also in [43], the authors propose a SCADA system with Advanced Meter Infrastructure (AMI) and 4G wireless communication.

The SCADA system is used to perform the online adaptive feature, by obtaining measurements from DER output and AMI. To acquire the mentioned data from the distribution system to the control center, a 4G wireless communication system was used. Lastly, in their work, [75] suggest that the information exchange between the elements can be accomplished by a Wireless Sensor Network.

Fig. 4 offers a quantitative analysis of the communication approaches used in adaptive protection of microgrids in recent literature, based on 85 compiled papers from the last five years. The analysis is expressed in terms of communication technology (wired or wireless), control approach (centralized or decentralized) and operation mode (grid-connected, islanded, or both operation modes). It is important to make the remark that the literature review spans from January 2015 to July 2019 i.e. publications compiled for 2019 do not reflect an entire year. The findings from this analysis are further discussed in Section IV.

### C. Communication standards and protocols for substation automation and control

When it comes to communications architecture, the IEC 61850 is a widely accepted standard for automation and equipment of power utilities and DER, specifically for defining

protocols for IEDs at electrical substations [103]. There are three main protocols defined by the IEC 61850:

**Generic Object-Oriented Substation Event (GOOSE):**

Used to send data from IED to IED or from IED to circuit breakers due to its high-speed and high priority characteristics, suitable for tasks such as command trips or alarms;

**Sampled Measured Values (SMV):** Used to transfer the analog channels of current and voltage to the IED;

**Manufacturing message specification:** Used for applications that are non-time-critical, such as communications between controller and between substations.

IEC 61850 also defines generic substations events which is a control model that provides a fast and reliable mechanism for data transferring over the electrical substation network. The generic substations events model is divided into earlier described GOOSE and generic substation state events. All of the above tasks, performed inside communication layers within a power system, are adequate for protection-related applications. The three protocols run over Transmission Control Protocol, Internet Protocol or a Local Area Network (LAN) that can use high speed switched Ethernet like in [18].

IEC 61850 entails additional features, such as data modelling, reporting schemes, fast transfer of events, setting groups, sampled data transfer, commands and data storage, which justify its use in substations and grid protection. A communication setup using IEC 61850 standard makes it relatively simple to achieve low latency, normally around 4 milliseconds, which is ideal for protection purposes. Although many of the current implementations using this standard use wired Ethernet or Fiber Optics physical layers, wireless communication may also be implemented using IEC 61850 for communications between the substation elements.

Other standards used are for instance the IEEE 1588, which describes a hierarchical master-slave architecture for clock distribution and introduces precision time protocol (PTP), used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control system applications [104].

PTP supports the transmission of GOOSE messages over an Ethernet network using IEC 61850. This is generally implemented in SCADA systems where several substations can be covered. For instance, reference [105] shows that monitoring three pulses per second (PPS) signals from master to slave can be synchronized within 200 ns and deliver accurate time stamps below 500 ns. Note that this delay has a much lower order of magnitude compared to the adaptive protection needs (order of milliseconds), making them negligible. Also, the IEC 60870-5 defines systems used for telecontrol, supervisory control and data acquisition in electrical engineering and power system automation applications. It provides the communication architecture for sending basic telecontrol messages between two elements (ex. IED and MPMC) that have permanent connected communication channels. IEC 60870-5-101 specifically refers to companion standards for basic telecontrol tasks, which are commonly used in substation control and protection in SCADA systems.

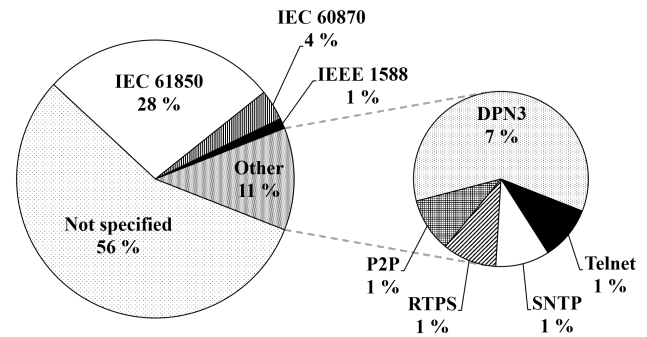


Fig. 5: Percent distribution of communication standards and protocols used in microgrid adaptive protection literature.

Other protocols used for control purposes found in the literature and listed in Table II are:

**Distributed network protocol (DPN3):** Used mainly for communication between a master and remote terminal unit or IEDs. It provides multiplexing, data fragmentation, error checking, link control, prioritization, and layer 2 addressing services for user data. The protocol is robust, efficient and compatible with many elements which is suitable for SCADA systems. Depending on the elements and the applications it can become very complex;

**Telnet:** Application protocol used in internet or LAN to provide interactive text-oriented communication systems using a virtual terminal connection and data being interspersed in-band with control information over 8-byte transmission control protocol. Telnet was often used to perform remote connection applications. It doesn't use, however, any form of encrypting mechanism, which makes it vulnerable in modern security terms;

**Real-Time Publish-Subscribe (RTPS):** Protocol which provides two main communication models, the publish-subscribe protocol that transfers data from publishers to subscribers, and the composite State Transfer protocol that transfers states. It features characteristics such as modularity, scalability and extensibility and it's suitable for real time applications running over standard internet protocol networks;

**Peer-to-peer:** Allows to connect a large number of users over a LAN. The scalability is no longer limited by the server. Its functions are distributed among a number of client peers, communicating in multicast mode. Messages are sent from one client directly to another client, without relying on a central server.

Fig. 5 shows the percent distribution of communication standards and protocols used in recent microgrid adaptive protection literature (based on the same 85-research paper sample). An immediate observation is the dominance of the IEC 61850 standard, which suggests its protocols are suitable for adaptive protection tasks even in the case of wireless deployments, as showed in Table II.

One additional consideration to communication standards and protocols is the physical capability of network elements. Adaptive protection requires robust and flexible elements for

data gathering and control. Due to their ability to receive and send data to form the closed loop of the adaptive process, IEDs comply fully with these strict requirements. IEDs must also count with sufficient flash memory capabilities to read/write protective settings [16] and successfully achieve the communication data exchange. Reference [75] also mentions that IEDs should have the ability of logging voluminous information about system parameters. In [43], [44], the authors selected the most suitable wireless technology for collecting data in real time and transfer it to the central controller, based on synergies with SCADA systems.

#### D. Cyber-security

The transition of microgrids to the cyber-physical domain comes with a number of cyber-security risks. Communication systems are vulnerable to malicious cyber-attacks. If the protection systems in place do not perform appropriately, such attacks can potentially harm the physical domain [13]. Cyber-attacks can be classified in two main categories: Network Security attacks and Goose & SMV message attacks [7]. Three types of attacks related to Network Security are:

**Denial of service (DoS):** DoS prevents authorized users to access a service and affects the timeliness of the information exchange, which can cause packet losses. [106] addresses the case of load frequency control in a power system where supply is limited from DoS attacks by transferring the model of multi-area power systems to a dependent time delay model, in order to tolerate a certain degree of data losses induced by energy-limited DoS. Many classical approaches address this type of attacks by using distribute topology formation techniques that are based upon the cooperation between IED nodes [107];

**Password cracking attempts:** This method is based on attempts to gain access to system devices (such as IEDs) to gain control over them, performing tripping actions or blocking them from protective signals. For techniques to detect type of attacks, see [108];

**Eavesdropping attacks:** This type of attack is done by accessing the communication link between the control center and the substation, and can be performed in both wired and wireless communication implementations. The data packets are intercepted by the intruder, who is able to replace real data for fabricated one. After, the controller can send back to the IEDs tripping signals out of wrong information provided by the intruder [109].

For GOOSE & SMV attacks, we have:

**Goose & SMV modification attacks:** In this type of attack, the intruder modifies the message data between the IED (GOOSE sender) and the circuit breaker (GOOSE receiver) without any notice. And as SMV the intruder can send wrong information about the analog variables of the system. In [110], a case where the minimum capabilities an intruder needs to inject a single message and perform undesirable actions is presented;

**Goose & SMV DoS attacks:** The intruder can prevent the correct operation of the IED by sending a great amount of

messages to a IED target causing communication collapse and making it unable to respond to other messages;

**Goose & SMV replay attacks:** Fault information packets are kept from the intruder and then sent back to the elements under normal operation, causing undesirable tripping and possible substation outages.

When a communication failure resulting from cyber-attacks takes place in a microgrid, it would usually trigger microgrid islanding, which poses challenges to protective devices. [7] envisions such a scenario, devising an approach to handle relying on energy storage. Under service of energy storage, the IEDs may be able to reach the overcurrent fixed setting to perform tripping actions in case of fault condition, guaranteeing protection actuation and therefore no damages to the microgrid.

The literature is abundant in terms of proposed approaches for evaluating and preventing cyber-attack in electrical networks [111]. However, for sake of effectiveness and robustness of operations, cyber-security should be approached holistically and from a project design stage. Therefore, to prevent those attacks, guaranteeing a reliable cyber-physical protective system embedded in the communication architecture of microgrids, substantial improvements, and thus investments in prevention, detection, mitigation and resilience must still be undertaken.

#### IV. DISCUSSION, OPEN ISSUES AND CHALLENGES

The increasing penetration of RES in electrical networks and the dissemination of microgrids are generating interest in developing communication technologies tailored to new uses and functionalities. For instance, islanded operation will become more relevant (as seen in Fig. 4), driving the need for further adaptability in protective units for system elements. Unprecedented changes have taken place in the ways in which people communicate during the last two decades. Changes in the communication infrastructure of distribution systems and microgrids are also important and ruled by the need for greater flexibility and more cost-effective solutions. The research presented in this paper highlights the predominance of wired, centralized communication approaches for adaptive protection in microgrids. On the other hand, it reveals no identifiable changing trend in terms of adopted communication technology (wired or wireless) in recent practical and theoretical research (Fig. 4). There is a dominant use of IEC 61850 standard because it addresses necessary communication protocols in the substation domain 5. IEC 61850 is suitable for wireless communications and can be used for future implementation of protection and control systems. Many further developments such as the Internet of Things (IoT), augmented reality, telemedicine, virtual reality and unmanned driving, have been applied to real businesses. These developments have brought significant changes to society and their mobile communication requirements became higher [112]–[114].

Section III showed that current microgrid sensing and monitoring rely largely on wired communications, even though wireless systems can meet increasing quality of service requirements (as ongoing discussions on 5G suggest). On a related note, the recent appearance of mobile 5G wireless communications, an evolution of 4G, as proposed by the

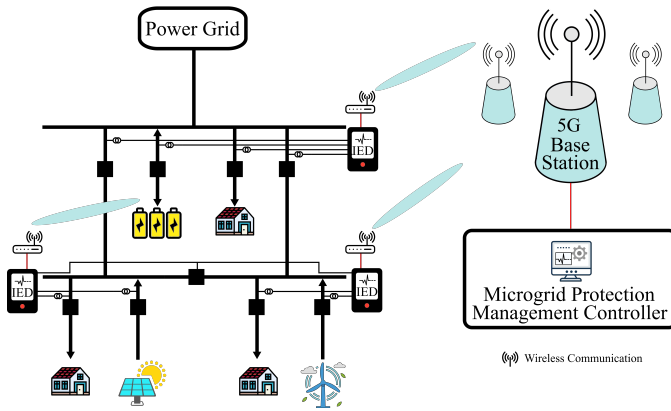


Fig. 6: Wireless 5G communications deployment with interface diversity in an overcurrent adaptive protection scheme.

latest realises of the 3rd Generation Partnership Project, has revealed highly promising for various vertical use cases, with reported efficient technical and economical solutions [115]. In the years to come, 5G networks shall include features targeted at improved performance for specific vertical use-cases (as the case of energy and automation verticals). Advantages of 5G communication infrastructure includes cost savings (no wired physical connections are needed), network virtualization, improved response time, efficiency, flexibility, redundancy and its platform-approach, where a single interface is used to provide different types of connectivity [116]. Microgrid protection will eventually benefit from 5G technology developments, as it matures, since all network communications within the different elements from traditional protection or adaptive protection can be made using a centralized scheme as show in Fig. 6.

In particular, 5G is framed as having three cornerstones:

**Enhanced Mobile Broadband:** More data rate and connectivity than previous technology (4G);

**Massive Machine Type Communication:** Larger number of devices connected than 4G and possibility of Machine-to-Machine communications;

**Ultra Reliable and Low Latency Communications (URLLC):** 1 ms latency and 99,999% reliability.

All the above features are relevant and will play a key role in substation control and grid automation. For instance, system operators can connect devices that are located in zones with difficult access. 5G would also allow for protection to become more distributed by installing IEDs at points closer to consumption, and DER generation without having to build new communication infrastructure. mMTC schemes could be used by IEDs to communicate without having to rely on central servers for actuation purposes (e.g., reclosing schemes or informing the current state of a branch), as well as including one or multiples IEDs to the network, maintaining the same base stations (scalability). If one considers a large network deployment, as in a big city, massive connectivity between the elements is needed.

However, URLLC is the most promising regime for adaptive protection in microgrids. Previous work shows that message latency should be constrained by 2 cycles (i.e., 40 ms for a 50 Hz power system) [117], while other indicates a stricter requirement between 12 and 20 ms [15]; both considering

high reliability. Current 4G systems can deliver an end-to-end latency of 20 ms, at best, which is a result of the constraint from the frame structure. For example, tests in a 4G industrial private network achieved in the most favourable settings a delay of 26 ms (in comparison to a wired Ethernet scenario that achieved a delay of 3 ms) [118]. It is important to mention that, although 5G URLLC targets latencies as low as 1 ms, our particular application is less strict requiring 12 ms latency at the most stringent cases.

In terms of reliability, the performance of 4G is reliant upon several parameters, from the size of the message to the number of users. In [12], the authors have proposed a quantitative relation between these key parameters based on field measurements. The URLLC regime in 5G relates latency and reliability in a sense that the target reliability should be achieved within a very low latency constrain; originally, this constraint was 1 ms, but in the latter years it has been relaxed according to some more elaborate requirements for Industrial IoT (see, for example, [119, Table 1]). Even these more relaxed versions, including the one we are using for the adaptive protection case, cannot be met by 4G.

In this case, the data-driven reliability guarantees based on a statistical learning framework seems a more suitable approach than the “deterministic” 1 ms potentially provided in URLLC regime [120]. Depending on the application, ultra-reliability is critical but the low latency is more flexible; the adaptive protection exemplifies this. Besides, recent results have proved that interface diversity where 5G combined with other wireless interfaces can provide ultra-reliability with bounded delay, which would satisfy the adaptive protection requirements [12].

The integration of these different quality of service can be done by NS, which is a concept that finds an efficient way for serving a determined application with 5G features on a common infrastructure [121], [122]. Various works in fields of communication for applications in Industry 4.0 show that NS using programmability and flexibility can be used to reduce complexity. This allows getting the best feature from a communication network, depending on the requirements from specific applications [123]. A slice can be considered an independent network, with corresponding advantages; in microgrid protection, it could be divided in many slices depending of the availability, latency or message type, as shown in [124]. This concept makes communications even more flexible. As RES penetration increases in distribution systems, particularly in microgrids, the bidirectional fault current magnitudes become bigger, more sensors need to be installed, and therefore more signals need to be monitored. It then becomes a growing challenge for communication systems to deliver different messages from sensing devices to controllers and actuators. NS architectures may be able to efficiently deal with the complexity of handling such different and demanding requirements, which can range from high reliability and low latency to high data rates on the same industrial application.

All in all, new ways to incorporate wireless technology in substation automation and control need to be researched in the upcoming years, to accompany the rapid changes electrical distribution systems are already undergoing. The wired communication infrastructure will not be able to catch up, due

to the lack of scalability and further prohibitive characteristics. A good approach would be multi-connectivity that combines wired and wireless, as those technologies have different failure patterns. 5G communications will open new frontiers in how these systems can be effectively integrated to perform tasks such as adaptive protection with very stringent requirements [125]. In particular, ultra-reliable communications with latency constraints required to perform adaptive protection should co-exist with other applications with multiple requirements, including massive connectivity of machine-type devices and more traditional broadband applications. While current 5G solutions are not yet capable of reaching the demanded performance in protection applications, upcoming releases of 5G – and even of 6G – are expected to focus on specific vertical applications and application-specific requirements. In this context, fast technological developments including potentially groundbreaking concepts, such as Semantic Filters [126] and Edge Intelligence, are expected to take place in the upcoming years [127]. These developments should allow for tailored wireless communication solutions i.e. based on specific applications and their particular requirements, that co-exist and share the same resources.

Usually, societal paradigm changes take place decades after key technologies (such as 5G) have been developed and rapid adoption is limited by conservative and progressive investment. The adoption of wireless connectivity in energy sector has not yet become mainstream. Some solutions like 4G and WiFi are deployed for some applications (mainly monitoring, metering and demand response), but not for adaptive protection, due to their performance limitations. Upgrading infrastructure to add 5G capabilities would bring additional capital costs considering incremental deployment in the existing grid infrastructure. On the other hand, it is expected that 5G brings down the operational costs related to communication network operations, due to its modularity and scalability [128]. In 5G, the concept of local operator and private cellular networks indicates the tendency of third-party service providers, which is expected to decrease the operational costs related to the communication network, compared to more expensive deployment and maintenance of wired networks [129].

5G has many potential advantages but also some challenges related to its effective implementation. These challenges are commonly associated with cyber-security. Careful examination of communication technologies has to be taken into consideration during a control and protection project design stage. The authors suggest this step to be essential for the economic viability of the project, since it can greatly reduce costs. This design should also include a robust system architecture to prevent or avoid possible cyber-attacks, given the vulnerability of wireless communication systems over wired communication systems. The reason for this is the wireless air propagation channel, where signals can be picked up from nearby locations without interfering in any hardware equipment.

It is worth restating that the proposed adaptive protection scheme can greatly reduce costs associated with communication network, bringing more flexibility in comparison to the traditional wired solutions. The benefits of using 5G would be also combined with already deployed solutions, leading

to gains from multi-connectivity, which is a popular way of attaining now that there are many wireless interfaces available [12]. In summary, we argue that the proposed solution generally complies with the current deployments, which yields a smooth transition that will bring not only technical benefits but also economical ones.

## V. CONCLUSION

This paper presented key technical aspects related to the communication system that is needed to perform adaptive protection in micro-grids with high penetration of DERs. We particularly focused on different exiting solutions for adaptive protection systems, which are dominantly based on wired solutions. We covered the traditional communication architectures (e.g., centralized or decentralized) and standards (e.g., GOOSE, SMV, RTPS among others). We also discussed aspects related to cyber-security, including potential threats and types of attacks. What is remarkable, though, is that current approaches mostly rely on wired networks despite the unquestionable performance gains of wireless technologies during the last decade. In this sense, we argue that 5G in combination with other existing solutions (e.g., WiFi) can already achieve the required reliability of 99.999 % with a bounded latency as low as 12 ms so that they should be seriously considered as a feasible enabler of adaptive protection applications. In the near future, we expect that these solutions will take over many traditionally wired applications since wireless solutions tend to be cheaper, more flexible and easier to implement than wired ones to perform the same tasks, including mission-critical ones. All in all, this review highlighted the state-of-the-art in the field indicating possible research directions that shall be taken to effectively deploy adaptive protection using wireless communications.

## ACKNOWLEDGEMENTS

This paper is partly supported by Academy of Finland via: (a) ee-IoT n.319009, (b) FIREMAN consortium CHIST-ERA/n.326270, and (c) EnergyNet Fellowship n.321265/n.328869. The authors would like to thank the funding from DIGI-USER research platform

## REFERENCES

- [1] H. Lee *et al.*, "An energy management system with optimum reserve power procurement function for microgrid resilience improvement," *IEEE Access*, vol. 7, pp. 42577–42585, 2019.
- [2] C. Marnay and J. Lai, "Serving electricity and heat requirements efficiently and with appropriate energy quality via microgrids," 2012.
- [3] P. H. Nardelli, N. Rubido, C. Wang, M. S. Baptista, C. Pomalaza-Raez, P. Cardieri, and M. Latva-aho, "Models for the modern power grid," *The European Physical Journal Special Topics*, vol. 223, no. 12, pp. 2423–2437, 2014.
- [4] M. A. Haj-ahmed and M. S. Illindala, "The influence of inverter-based DGs and their controllers on distribution network protection," in *2013 IEEE Industry Applications Society Annual Meeting*. IEEE, oct 2013.
- [5] M. Soshinskaya *et al.*, "Microgrids: Experiences, barriers and success factors," *Renewable and Sustain. Energy Reviews*, vol. 40, pp. 659–672, 2014.
- [6] T. S. Ustun, C. Ozansoy, and A. Zayegh, "A microgrid protection system with central protection unit and extensive communication," in *2011 10th International Conference on Environment and Electrical Engineering*. IEEE, may 2011.

- [7] H. F. Habib, C. R. Lashway, and O. A. Mohammed, "A review of communication failure impacts on adaptive microgrid protection schemes and the use of energy storage as a contingency," *IEEE Trans. Ind. Appl.*, vol. 54, no. 2, pp. 1194–1207, mar 2018.
- [8] M. H. Cintuglu *et al.*, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 2017.
- [9] H. Wan, K. K. Li, and K. P. Wong, "An adaptive multiagent approach to protection relay coordination with distributed generators in industrial power distribution system," *IEEE Transactions on Industry Applications*, vol. 46, no. 5, pp. 2118–2124, sep 2010.
- [10] H. F. Habib *et al.*, "Multi-agent-based technique for fault location, isolation, and service restoration," *IEEE Transactions on Industry Applications*, vol. 53, no. 3, pp. 1841–1851, may 2017.
- [11] M. Baranwal *et al.*, "A distributed architecture for robust and optimal control of DC microgrids," *IEEE Trans. Ind. Electron.*, vol. 66, no. 4, pp. 3082–3092, Apr. 2019.
- [12] J. J. Nielsen, R. Liu, and P. Popovski, "Ultra-reliable low latency communication using interface diversity," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1322–1334, March 2018.
- [13] S. Beheshtaein, R. Cuzner, M. Savaghebi, and J. M. Guerrero, "Review on microgrids protection," *IET Generation, Transmission & Distribution*, vol. 13, no. 6, pp. 743–759, mar 2019.
- [14] S. Beheshtaein *et al.*, "DC microgrid protection: A comprehensive review," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2019.
- [15] Y. Yan *et al.*, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 5–20, First 2013.
- [16] R. Moxley and F. Becker, "Adaptive protection — what does it mean and what can it do?" in *Proc. 71st Annual Conf. for Protective Relay Engineers (CPRE)*, Mar. 2018, pp. 1–4.
- [17] R. Bansal, *Power System Protection in Smart Grid Environ.* CRC Press, 2019.
- [18] C. Ozansoy, "A methodology for determining fault current impact coefficients of distributed energy resources in an adaptive protection scheme," in *2015 9th International Conference on Electrical and Electronics Engineering (ELECO)*. IEEE, nov 2015.
- [19] H. Lin *et al.*, "Adaptive protection combined with machine learning for microgrids," *Transmission Distribution IET Generation*, vol. 13, no. 6, pp. 770–779, 2019.
- [20] X. Jin *et al.*, "High speed digital distance relaying scheme using FPGA and IEC 61850," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4383–4393, Sep. 2018.
- [21] M. J. Daryani, A. E. Karkevandi, and O. Usta, "Multi-agent approach to wide-area integrated adaptive protection system of microgrid for pre- and post-contingency conditions," in *Proc. IEEE PES Innovative Smart Grid Technologies Conf. Europe (ISGT-Europe)*, Oct. 2018, pp. 1–6.
- [22] M. Singh, T. Vishnuvardhan, and S. Srivani, "Adaptive protection coordination scheme for power networks under penetration of distributed energy resources," *IET Generation, Transmission & Distribution*, vol. 10, no. 15, pp. 3919–3929, nov 2016.
- [23] N. E. Naily *et al.*, "On-line adaptive protection scheme to overcome operational variability of DG in smart grid via fuzzy logic and genetic algorithm," in *2018 9th International Renewable Energy Congress (IREC)*. IEEE, mar 2018.
- [24] A. I. Attaya, A. M. E. Zonkoly, and H. A. Ashour, "Optimal relay coordination of an adaptive protection scheme using modified PSO algorithm," in *2017 Nineteenth International Middle East Power Systems Conference (MEPCON)*. IEEE, dec 2017.
- [25] A. A. de Sotomayor *et al.*, "IEC 61850-based adaptive protection system for the MV distribution smart grid," *Sustainable Energy, Grids and Networks*, vol. 15, pp. 26–33, sep 2018.
- [26] M. N. Alam, "Adaptive protection coordination scheme using numerical directional overcurrent relays," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 64–73, Jan. 2019.
- [27] S. Teimourzadeh *et al.*, "Adaptive protection for preserving microgrid security," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 592–600, Jan. 2019.
- [28] M. Singh and P. Basak, "Adaptive protection methodology in microgrid for fault location and nature detection using q0 components of fault current," *Transmission Distribution IET Generation*, vol. 13, no. 6, pp. 760–769, 2019.
- [29] V. Nougain, S. Mishra, and A. K. Pradhan, "Mvdc microgrid protection using a centralized communication with a localized backup scheme of adaptive parameters," *IEEE Trans. Power Del.*, vol. 34, no. 3, pp. 869–878, Jun. 2019.
- [30] H. Habib, M. M. Esfahani, and O. A. Mohammed, "Investigation of protection strategy for microgrid system using lithium-ion battery during islanding," *IEEE Trans. on Industry Appl.*, pp. 1–1, 2019.
- [31] A. E. Momesso, W. M. S. Bernardes, and E. N. Asada, "Fuzzy adaptive setting for time-current-voltage based overcurrent relays in distribution systems," *International Journal of Electrical Power & Energy Systems*, vol. 108, pp. 135–144, 2019.
- [32] R. R. Ferreira *et al.*, "Method for identification of grid operating conditions for adaptive overcurrent protection during intentional islanding operation," *International Journal of Electrical Power & Energy Systems*, vol. 105, pp. 632–641, feb 2019.
- [33] S. A. Hosseini, A. Nasiri, and S. H. H. Sadeghi, "A decentralized adaptive scheme for protection coordination of microgrids based on team working of agents," in *Proc. 7th Int. Conf. Renewable Energy Research and Applications (ICRERA)*, Oct. 2018, pp. 1315–1320.
- [34] S. Paladhi and A. K. Pradhan, "Adaptive zone-1 Setting following structural and operational changes in power system," *IEEE Trans. Power Del.*, vol. 33, no. 2, pp. 560–569, Apr. 2018.
- [35] S. AsghariGovar *et al.*, "Adaptive cwt-based overcurrent protection for smart distribution grids considering CT saturation and high-impedance fault," *Transmission Distribution IET Generation*, vol. 12, no. 6, pp. 1366–1373, 2018.
- [36] C. Chandraratne, W. L. Woo, T. Logenthiran, and R. T. Naayagi, "Adaptive overcurrent protection for power systems with distributed generators," in *Proc. 8th Int. Conf. Power and Energy Systems (ICPES)*, Dec. 2018, pp. 98–103.
- [37] K. Sedghisigarchi and K. T. Sardari, "An adaptive protection strategy for reliable operation of microgrids," in *Proc. IEEE Int. Energy Conf. (ENERGYCON)*, Jun. 2018, pp. 1–6.
- [38] M. Amarantunge *et al.*, "Development of adaptive overcurrent relaying scheme for iidg microgrids," in *Proc. 2nd Int. Conf. On Electrical Engineering (EECon)*, Sep. 2018, pp. 71–75.
- [39] R. Shah, P. Goli, and W. Shireen, "Adaptive protection scheme for a microgrid with high levels of renewable energy generation," in *Proc. Clemson University Power Systems Conf. (PSC)*, Sep. 2018, pp. 1–7.
- [40] W. L. T. Peiris *et al.*, "An adaptive protection scheme for small scale microgrids based on fault current level," in *Proc. 2nd Int. Conf. On Electrical Engineering (EECon)*, Sep. 2018, pp. 64–70.
- [41] K. Q. da Silva *et al.*, "An adaptive protection system for distribution network with distributed generation," in *Proc. Simposio Brasileiro de Sistemas Eletricos (SBSE)*, May 2018, pp. 1–6.
- [42] M. Zanjani, K. Mazlumi, and I. Kamwa, "Application of pmus for adaptive protection of overcurrent relays in microgrids," *Transmiss. Distribution IET Gener.*, vol. 12, no. 18, pp. 4061–4068, 2018.
- [43] K. Xu and Y. Liao, "Intelligent method for online adaptive optimum coordination of overcurrent relays," in *Proc. Clemson University Power Systems Conf. (PSC)*, Sep. 2018, pp. 1–5.
- [44] —, "Online adaptive optimum coordination of overcurrent relays," in *Proc. SoutheastCon 2018*, Apr. 2018, pp. 1–6.
- [45] Z. Zhonghua *et al.*, "Topology self-identification and adaptive operation method of distribution network protection and self-healing system," in *Proc. Int. Conf. Power System Technology (POWERCON)*, Nov. 2018, pp. 3087–3092.
- [46] J. Ma *et al.*, "An adaptive directional current protection scheme for distribution network with DG integration based on fault steady-state component," *International Journal of Electrical Power & Energy Systems*, vol. 102, pp. 223–234, nov 2018.
- [47] Y. CAI *et al.*, "Research on adaptive protection and control algorithm for distribution network based on network description model," in *Proc. Int. Conf. Power System Technology (POWERCON)*, Nov. 2018, pp. 142–147.
- [48] Y. Kang and Z. Duan, "New algorithm for adaptive current protection setting of fan connected to distribution network," in *Proc. Electronic and Automation Control Conf 2018 IEEE 3rd Advanced Information Technology (IAEAC)*, Oct. 2018, pp. 1415–1419.
- [49] Z. Linli *et al.*, "Adaptive tripping for distribution network based on fault indicator recording data," in *Proc. China Int. Conf. Electricity Distribution (CICED)*, Sep. 2018, pp. 1659–1664.
- [50] A. K. Upadhiya *et al.*, "Adaptive fault location algorithm for double circuit line," in *Proc. Environment and Intelligent Control (PEEIC) 2018 Int. Conf. Power Energy*, Apr. 2018, pp. 801–806.
- [51] X. He *et al.*, "Adaptive traveling waves based protection of distribution lines," in *Proc. 2nd IEEE Conf. Energy Internet and Energy System Integration (EI2)*, Oct. 2018, pp. 1–5.
- [52] W. M. Elhadad, A. Y. Hatata, and E. A. Badran, "A proposed adaptive distance relay model in atpdraw," in *Proc. Twentieth Int. Middle East Power Systems Conf. (MEPCON)*, Dec. 2018, pp. 754–759.

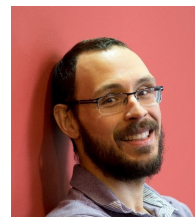
- [53] J. Zhao and R. Bian, "A new method of adaptive current protection for distribution lines with wind turbines," in *Proc. Electronic and Automation Control Conf 2018 IEEE 3rd Advanced Information Technology (IAEAC)*, Oct. 2018, pp. 269–273.
- [54] H. F. Habib *et al.*, "Utilizing supercapacitors for resiliency enhancements and adaptive microgrid protection against communication failures," *Electric Power Syst. Res.*, vol. 145, pp. 223–233, apr 2017.
- [55] E. Purwar, D. N. Vishwakarma, and S. P. Singh, "A new adaptive inverse-time protection scheme for modern distribution systems with distributed generation," in *Proc. IEEE Power Energy Society Innovative Smart Grid Technologies Conf. (ISGT)*, Apr. 2017, pp. 1–5.
- [56] B. A. Pacheco *et al.*, "A case study of adaptive microgrid protection during transitions and operations," in *Proc. Brazilian Power Electronics Conf. (COBEP)*, Nov. 2017, pp. 1–5.
- [57] K. A. Wheeler, S. O. Faried, and M. Elsamahy, "A microgrid protection scheme using differential and adaptive overcurrent relays," in *Proc. IEEE Electrical Power and Energy Conf. (EPEC)*, Oct. 2017, pp. 1–6.
- [58] N. E. Nailly *et al.*, "Adaptive overcurrent protection to mitigate high penetration of distributed generation in weak distribution systems," in *Proc. 9th IEEE-GCC Conf. and Exhib. (GCCCE)*, May 2017, pp. 1–9.
- [59] S. Gaber, K. Hassan, and A. Megahed, "A novel adaptive wide area protection scheme for smart grids with distributed generation," in *Proc. Nineteenth Int. Middle East Power Systems Conf. (MEPCON)*, Dec. 2017, pp. 802–810.
- [60] U. Orji *et al.*, "Adaptive zonal protection for ring microgrids," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1843–1851, Jul. 2017.
- [61] E. C. Piesciorsky and N. N. Schulz, "Fuse relay adaptive overcurrent protection scheme for microgrid with distributed generators," *Transmission Distribution IET Generation*, vol. 11, no. 2, pp. 540–549, 2017.
- [62] W. Tang and H. Yang, "Self-adaptive protection strategies for distribution system with dgs and fcls based on data mining and neural network," in *Proc. IEEE Int. Conf. Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I CPS Europe)*, Jun. 2017, pp. 1–5.
- [63] H. Muda and P. Jena, "Sequence currents based adaptive protection approach for dns with distributed energy resources," *Transmission Distribution IET Generation*, vol. 11, no. 1, pp. 154–165, 2017.
- [64] E. C. Piesciorsky and N. N. Schulz, "Comparison of non-real-time and real-time simulators with relays in-the-loop for adaptive overcurrent protection," *Electric Power Systems Research*, vol. 143, pp. 657–668, feb 2017.
- [65] S. Shen *et al.*, "An adaptive protection scheme for distribution systems with dgs based on optimized thevenin equivalent parameters estimation," *IEEE Trans. Power Del.*, vol. 32, no. 1, pp. 411–419, Feb. 2017.
- [66] S. P. George and S. Ashok, "Over current relay coordination in a real system with wind farm integration using hybrid genetic algorithm approach," in *Proc. IET Int. Conf. Resilience of Transmission and Distribution Networks (RTDN 2017)*, Sep. 2017, pp. 1–6.
- [67] X. Song *et al.*, "Adaptive protection scheme for distributed systems with dg," *The Journal of Engineering*, vol. 2017, no. 13, pp. 1432–1436, 2017.
- [68] A. Tjahjono *et al.*, "Adaptive modified firefly algorithm for optimal coordination of overcurrent relays," *Transmission Distribution IET Generation*, vol. 11, no. 10, pp. 2575–2585, 2017.
- [69] S. Misak *et al.*, "A novel approach to adaptive active relay protection system in single phase AC coupling off-grid systems," *Electric Power Systems Research*, vol. 131, pp. 159–167, feb 2016.
- [70] H. S. Sanca *et al.*, "Comparison frequency estimation methods on adaptive protection architecture applied on systems with distributed generation," in *Proc. 13th Int. Conf. Development in Power System Protection 2016 (DPSP)*, Mar. 2016, pp. 1–6.
- [71] H. Leite, E. Almeida, and N. Silva, "Real-time closed-loop test to adaptive protection in a smart-grid context," in *Proc. 13th Int. Conf. Develop. in Power Syst. Protection 2016 (DPSP)*, Mar. 2016, pp. 1–5.
- [72] Z. Liu and H. K. Høidalen, "A simple multi agent system based adaptive relay setting strategy for distribution system with wind generation integration," in *Proc. 13th Int. Conf. Development in Power System Protection 2016 (DPSP)*, Mar. 2016, pp. 1–6.
- [73] H. Lin *et al.*, "Adaptive overcurrent protection for microgrids in extensive distribution systems," in *Proc. IECON 2016 - 42nd Annual Conf. of the IEEE Ind. Electronics Soc.*, Oct. 2016, pp. 4042–4047.
- [74] M. Y. Shih *et al.*, "Mitigating the impact of distributed generation on directional overcurrent relay coordination by adaptive protection scheme," in *Proc. IEEE 16th Int. Conf. Environment and Electrical Engineering (EEEIC)*, Jun. 2016, pp. 1–6.
- [75] N. A. Bari and S. D. Jawale, "Smart and adaptive protection scheme for distribution network with distributed generation: A scoping review," in *2016 International Conference on Energy Efficient Technologies for Sustainability (ICEETS)*. IEEE, apr 2016.
- [76] O. V. Gnana Swathika and S. Hemamalini, "Prims-aided dijkstra algorithm for adaptive protection in microgrids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 4, no. 4, pp. 1279–1286, Dec. 2016.
- [77] H. Muda and P. Jena, "Real time simulation of new adaptive overcurrent technique for microgrid protection," in *Proc. National Power Systems Conf. (NPSC)*, Dec. 2016, pp. 1–6.
- [78] M. Pujiantara *et al.*, "Optimization technique based adaptive overcurrent protection in radial system with dg using genetic algorithm," in *Proc. Int. Seminar Intelligent Technology and Its Applications (ISITIA)*, Jul. 2016, pp. 83–88.
- [79] S. Chen *et al.*, "An adaptive current protection for distributed network with wind generators," in *Proc. IEEE Power and Energy Society General Meeting (PESGM)*, Jul. 2016, pp. 1–5.
- [80] J. H. He *et al.*, "An accelerated adaptive overcurrent protection for distribution networks with high dg penetration," in *Proc. 13th Int. Conf. Develop. in Power Syst. Protection 2016 (DPSP)*, Mar. 2016, pp. 1–5.
- [81] N. V. Grebchenko *et al.*, "Adaptive current short-circuit protection in electric systems with distributed generation," in *Proc. Automation and Motion (SPEEDAM) 2016 Int. Symp. Power Electronics, Electrical Drives*, Jun. 2016, pp. 1279–1283.
- [82] T. Bujanovic and P. Ghosh, "Adaptive algorithm for microprocessor based distance relays in smart grid," in *Proc. IEEE Smart Energy Grid Engineering (SEGE)*, Aug. 2016, pp. 358–364.
- [83] X. Guo *et al.*, "A novel adaptive zero-sequence current protection for low resistance grounding system," in *Proc. IEEE PES Asia-Pacific Power and Energy Eng. Conf. (APPEEC)*, Oct. 2016, pp. 2523–2528.
- [84] D. Jiandong *et al.*, "Research on adaptive current instantaneous trip protection for active distribution network line with dfigs," in *Proc. China Int. Conf. Electricity Distribution (CICED)*, Aug. 2016, pp. 1–5.
- [85] D. Della Giustina *et al.*, "Toward an adaptive protection system for the distribution grid by using the IEC 61850," in *Proc. IEEE Int. Conf. Industrial Technology (ICIT)*, Mar. 2015, pp. 2374–2378.
- [86] H. Lin *et al.*, "Adaptive distance protection for microgrids," in *Proc. IECON 2015 - 41st Annual Conf. of the IEEE Industrial Electronics Society*, Nov. 2015, pp. 000725–000730.
- [87] K. Vijitha, M. P. Selvan, and P. Raja, "Short circuit analysis and adaptive zonal protection of distribution system with distributed generators," in *Proc. Power and Environment: Towards Sustainable Growth (ICEPE) 2015 Int. Conf. Energy*, Jun. 2015, pp. 1–6.
- [88] M. Farsadi, A. Yazdani Nejadi, and A. Esmaeilnasab, "Reducing overcurrent relays operating times in adaptive protection of distribution networks considering dg penetration," in *Proc. 9th Int. Conf. Electrical and Electronics Engineering (ELECO)*, Nov. 2015, pp. 463–468.
- [89] V. A. Papaspiliotopoulos, G. N. Korres, and N. D. Hatziaargyriou, "Protection coordination in modern distribution grids integrating optimization techniques with adaptive relay setting," in *Proc. IEEE Eindhoven PowerTech*, Jun. 2015, pp. 1–6.
- [90] A. Gupta *et al.*, "Dual simplex algorithm aided adaptive protection of microgrid," in *Proc. Int. Conf. Computational Intelligence and Communication Networks (CICN)*, Dec. 2015, pp. 1505–1509.
- [91] W. Fan *et al.*, "Preliminary study on adaptive fast-tripping current protection for microgrid," in *Proc. IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, Nov. 2015, pp. 1–6.
- [92] R. R. Ferreira *et al.*, "Method for adaptive overcurrent protection of distribution systems with distributed synchronous generators," in *Proc. IEEE Power Energy Society General Meeting*, Jul. 2015, pp. 1–5.
- [93] S. P. George and S. Ashok, "Multiagent based adaptive relaying for distribution network with distributed generation," in *Proc. Power and Environment: Towards Sustainable Growth (ICEPE) 2015 Int. Conf. Energy*, Jun. 2015, pp. 1–6.
- [94] J. P. Nascimento, N. S. D. Brito, and B. A. de Souza, "An adaptive protection algorithm for distribution systems with distributed generation," in *Proc. IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM)*, Oct. 2015, pp. 165–170.
- [95] C. Ozansoy, "Design of an adaptive protection system for microgrids with distributed energy resources in accordance with IEC 61850-7-420," in *Proc. 9th Int. Conf. Electrical and Electronics Engineering (ELECO)*, Nov. 2015, pp. 474–478.
- [96] F. Coffele, C. Booth, and A. Dyško, "An adaptive overcurrent protection scheme for distribution networks," *IEEE Trans. Power Del.*, vol. 30, no. 2, pp. 561–568, Apr. 2015.
- [97] B. P. Bhattarai *et al.*, "An adaptive overcurrent protection in smart distribution grid," in *Proc. IEEE Eindhoven PowerTech*, Jun. 2015, pp. 1–6.

- [98] N. Tummasit, S. Premrudeepreechacharn, and N. Tantichayakorn, "Adaptive overcurrent protection considering critical clearing time for a microgrid system," in *Proc. IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, Nov. 2015, pp. 1–6.
- [99] P. Esmaili, A. A. b. M. Zin, and O. Shariati, "On-line overcurrent relays setting approach in distribution networks by implementing new adaptive protection algorithm," in *Proc. Sensor Networks and Information Processing (ISSNIP) 2015 IEEE Tenth Int. Conf. Intelligent Sensors*, Apr. 2015, pp. 1–6.
- [100] D. S. Kumar *et al.*, "An adaptive fuzzy based relay for protection of distribution networks," in *Proc. IEEE Int. Conf. Fuzzy Systems (FUZZ-IEEE)*, Aug. 2015, pp. 1–6.
- [101] J. López *et al.*, "Adaptive system protection scheme using generalized pattern search," in *Proc. 18th Int. Conf. Intelligent System Application to Power Systems (ISAP)*, Sep. 2015, pp. 1–6.
- [102] A. Elhaffar, N. El-Nailly, and K. El-Arroudi, "Management of distribution system protection with high penetration of dgs," in *Energy Systems and Management*. Springer, 2015, pp. 279–291.
- [103] "IEEE standard test methods for use in the evaluation of message communications between intelligent electronic devices in an integrated substation protection, control and data acquisition system."
- [104] "IEEE standard for a precision clock synchronization protocol for distributed measurement and control systems," *IEEE Std 1588-2002*, pp. 1–154, Oct. 2002.
- [105] Y. Liu, R. Zivanovic, S. Al-Sarawi, C. Marinescu, and R. Cochran, "A synchronized event logger for substation topology processing," in *2009 Australasian Universities Power Engineering Conference*, 2009, pp. 1–6.
- [106] C. Peng, J. Li, and M. Fei, "Resilient event-triggering  $h_\infty$  load frequency control for multi-area power systems with energy-limited DoS attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 4110–4118, sep 2017.
- [107] P. Srikantha and D. Kundur, "Denial of service attacks and mitigation for stability in cyber-enabled power grid," in *2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2015, pp. 1–5.
- [108] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, jan 2019.
- [109] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707–1721, jul 2015.
- [110] J. G. Wright and S. D. Wolthusen, "Stealthy injection attacks against IEC61850s GOOSE messaging service," in *2018 IEEE PES Innovative Smart Grid Technol. Conf. Europe (ISGT-Europe)*. IEEE, oct 2018.
- [111] M. S. Rahman *et al.*, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 436–447, apr 2017.
- [112] P. H. J. Nardelli *et al.*, "Energy internet via packetized management: Enabling technologies and deployment challenges," *IEEE Access*, vol. 7, pp. 16 909–16 924, 2019.
- [113] P. Wang *et al.*, "Key technology research on 5g mobile communications power system," in *Proc. IEEE Int. Telecommunications Energy Conf. (INTELEC)*, Oct. 2017, pp. 142–148.
- [114] G. Durisi, T. Koch, and P. Popovski, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.
- [115] P. Popovski *et al.*, "Wireless access for ultra-reliable low-latency communication: Principles and building blocks," *IEEE Network*, vol. 32, no. 2, pp. 16–23, Mar. 2018.
- [116] P. Hovila *et al.*, "5g networks enabling new smart grid protection solutions," in *25th Int. Conf. on Electricity Distribution (CIRED)*, Madrid, Spain, June, 2019.
- [117] T. S. Ustun *et al.*, "An adaptive microgrid protection scheme based on a wide-area smart grid communications network," in *2013 IEEE Latin-America Conference on Communications*, Nov 2013, pp. 1–5.
- [118] F. Polunin, D. C. Melgarejo, T. Lindh, A. Pinömaa, P. H. Nardelli, and O. Pyrhonen, "Demonstrating the impact of Ite communication latency for industrial applications," in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, vol. 1. IEEE, 2019, pp. 977–982.
- [119] "5g for connected industries and automation," 5G Alliance for Connected Industries and Automation (5G-ACIA), Tech. Rep., 2018.
- [120] M. Angjelichinoski, K. F. Trillingsgaard, and P. Popovski, "A statistical learning approach to ultra-reliable low latency communication," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 5153–5166, July 2019.
- [121] X. Foukas *et al.*, "Network slicing in 5g: Survey and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, may 2017.
- [122] A. E. Kalor *et al.*, "Network slicing in industry 4.0 Applications: Abstraction methods and end-to-end analysis," *IEEE Trans. Ind. Informat.*, vol. 14, no. 12, pp. 5419–5427, Dec. 2018.
- [123] P. Popovski *et al.*, "5g wireless network slicing for embb, urllc, and mmte: A communication-theoretic view," *IEEE Access*, vol. 6, pp. 55 765–55 779, 2018.
- [124] H. V. K. Mendis, P. E. Heegaard, and K. Krlevska, "5g network slicing for smart distribution grid operations," in *25th Int. Conf. on Electricity Distribution (CIRED)*, Madrid, Spain, June, 2019.
- [125] L. Thybom and Á. Kapovits, "5g and energy," in *5GPPP White paper*, 2015.
- [126] P. Popovski *et al.*, "Wireless access in ultra-reliable low-latency communication (URLLC)," *IEEE Trans. Commun.*, pp. 1–1, 2019.
- [127] J. Park *et al.*, "Wireless network intelligence at the edge," *Proceedings of the IEEE*, vol. 107, no. 11, pp. 2204–2239, 2019.
- [128] G. Bag, L. Thybom, and P. Ylianttila, "Challenges and opportunities of 5g in power grids," *CIRED-Open Access Proceedings Journal*, vol. 2017, no. 1, pp. 2145–2148, 2017.
- [129] Y. Siriwardhana, P. Porambage, M. Liyanage, J. S. Walia, M. Matinmikko-Blue, and M. Ylianttila, "Micro-operator driven local 5g network architecture for industrial internet," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–8.



systems and electrical protection systems.

**Daniel Gutierrez-Rojas** received the B.Sc. degree in Electrical Engineering from University of Antioquia, Colombia in 2016 and the M.Sc. degree in Protection of Power Systems University of São Paulo, Brazil, in 2017. From 2017 to 2019, he worked as security of operation and fault analyst for Colombia's National electrical operator. He is currently working toward the Ph.D. degree at the School of Energy Systems at LUT University, Finland. His research interests include predictive maintenance, power systems, microgrids, mobile communication



**Pedro H. J. Nardelli** received the B.S. and M.Sc. degrees in electrical engineering from the State University of Campinas, Brazil, in 2006 and 2008, respectively. In 2013, he received his doctoral degree from University of Oulu, Finland, and State University of Campinas following a dual degree agreement. He is currently Assistant Professor (tenure track) in IoT in Energy Systems at LUT University, Finland, and holds a position of Academy of Finland Research Fellow with a project called Building the Energy Internet as a large-scale IoT-based cyber-physical system that manages the energy inventory of distribution grids as discretized packets via machine-type communications (EnergyNet). He leads the Cyber-Physical Systems Group at LUT and is Project Coordinator of the CHIST-ERA European consortium Framework for the Identification of Rare Events via Machine Learning and IoT Networks (FIREMAN). He is also Adjunct Professor at University of Oulu in the topic of "communications strategies and information processing in energy systems". His research focuses on wireless communications particularly applied in industrial automation and energy systems. He received a best paper award of IEEE PES Innovative Smart Grid Technologies Latin America 2019 in the track "Big Data and Internet of Things". He is also IEEE Senior Member. More information: <https://sites.google.com/view/nardelli/>

