

Operational Issues on Adaptive Protection of Microgrids due to Cyber Attacks

Daniel Gutierrez-Rojas, *Member, IEEE*, Iurii Demidov, *Member, IEEE*, Alkistis Kontou, *Member, IEEE*, Dimitrios Lagos, *Member, IEEE*, Subham Sahoo, *Member, IEEE*, and Pedro J. Nardelli, *Senior Member, IEEE*

Abstract—This paper shows how false data injection attacks (FDIAs) affect adaptive protection in microgrids. Specifically, we implemented a directional over-current relay in the CIGRE low voltage benchmark system to carry out experiments to manipulate protection decisions via cyber-attacks. The aim of the newly proposed cyber-attack is to cause false relay tripping and unbalanced conditions in microgrid that can result in power outages and blackouts. The proposed study has been validated on commercial relays using a real-time digital simulator equipped with the IEC 61850 standard communication protocol. These results allow the power systems engineers to understand the cyber-physical interactions more closely and adapt their protection schemes accordingly.

Index Terms—Adaptive protection, cyber-attacks, microgrids, over current relays, communications.

I. INTRODUCTION

SAFE operation in modern electrical systems require complex interaction between smart devices and physical components of the grid. These smart devices known as relays or Intelligent Electronic Devices (IED) are in charge to detect and clear *contingent* events when they are present in the system by using different protection methods. These events in electrical system may damage or affect the life cycle of the components and appliances [1]. To ensure a reliable operation, protection relays must clear faults within their protection zone as quickly as possible, and depending on the topology, they also have a back-up element, which in most of the cases is another relay located up-stream from the location of the primary protection. Both primary and back-up protection must be timely coordinated by their settings.

In distribution system level, directional over-current relays (DOCR) are the most commonly used ones to protect line segments. In the case of microgrids that have multiple nodes of generation from Distributed Energy Resources (DER) in a single line segment, protection becomes even more challenging. Conventional DOCR is not adequate due to varying conditions (e.g., topology changes, generation, load, etc.) where schemes require adaptability [2]. The bidirectional current present in these systems, and changes in topology can cause maloperation of relays and therefore, interruption of electricity supply [3]. In

this regard, relay settings can no longer be static, and instead, they must be changed according to the current state of the grid ensuring effective protection to all zones. This technique is known as adaptive protection.

In adaptive protection, to store protective settings such as plug setting (PS), operating curve function or time-dial setting (TDS) in the relays is a big challenge [4]. The goal is to make an automatic relay group set, when the grid changes. This can be achieved by means of the central management system, where all relays are connected to one entity and the setting groups are delivered unidirectionally. This solution is expensive, as it requires more sophisticated infrastructure and communication systems. Communication infrastructure is needed, where standard communication protocols (DNP3, GOOSE, SV, etc.) are deemed to be sufficient for this. In [5], a communication-assisted strategy was implemented to perform adaptive protection and self-healing on microgrids. These types of methods are reliable as usually the Ethernet or optic fiber communication links between the central management system and relays have very low chance of failures. Also, [6], [7] presents adaptive setting with the use of a central controller that can either calculate online group settings or set them based on the off-line short circuit analysis.

Digitalization has also made electrical systems more prone to cyber-attacks due to the introduction of the cyber-layer, through the ICT technologies, on top of the physical layer and the interactions between them. There are several types of cyber-attacks such as Denial-of-Service (DoS) [8] or false data injection attacks (FDIAs) that can harm the cyber layer and consequently affect the physical-layer operation of the energy system [9]. An example of the coordinated attack is presented in [10]. Similarly a FDIA attack described as a multi-objective optimization problem is shown in [11]. Both centralized and distributed communication schemes for adaptive protection are susceptible to cyber-attacks. Centralized scheme is more vulnerable as attacks in a single communication link or device can lead to several failures in the grid. In [12], cyber-attacks that exploit GOOSE and SV protocols making relays trip and causing instability in the system have been modelled. Also, in [13], a strategy for modelling cyber-attacks from the perspective of the attacker in centralized systems is presented. This strategy presents a damage risk indicator where most of the impact will be made while minimizing the probability of being caught. Distributed communication schemes are more resilient to cyber-attacks [14]. This is because FDIA injection at only one device does not lead to system outages as long as the cyber graph is undirected.

DGR, ID and PHJN are with Lappeenranta–Lahti University of Technology, Finland; AK and DL are with National Technical University of Athens, Greece; SS is with Aalborg University, Denmark. This paper is partly supported by (1) Academy of Finland via: (a) FIREMAN consortium n.326270 as part of CHIST-ERA grant CHIST-ERA-17-BDSI-003, (b) EnergyNet Fellowship n.321265/n.328869/n.352654, and (c) X-SDEN project n.349965; (2) European Union's Horizon 2020 research and innovation programme under grant agreement No 870620 in the ERIGrid 2.0 project; (3) Baltic-Nordic Energy Research programme via Next-uGrid project n.117766.

The motivation to develop this research relies on the concerns described above, mainly on the vulnerability of cyber-layer against possible attacks, which may lead to harmful consequences related to the malfunctioning of the power grid, including localized outages or even blackouts. This paper proposes a centralized adaptive protection system, where relays communicate with their neighbor relay(s) to inform about the state of the grid at their own nodes, and inform the variables status at each particular node. Based on the information received by the different nodes, a set of rules define the optimal settings for each relay at that particular instant. This scheme highlights the vulnerability of relay coordination against FDIAs.

In our view, this paper allows the power systems engineers to understand the cyber-physical interactions more closely and adapt their protection schemes accordingly including a higher possibility of potential cyber attacks, which has harmful impacts in the physical grid infrastructure, as well as negative impact for the network operator and for the people living in the region covered by it. The contributions of this paper are:

- A newly proposed DOCR coordination implementation in CIGRE LV microgrid;
- A novel cyber-attack formulation of GOOSE messages under IEC 61850 protocol for FDIA.
- A demonstration of the proposed remote FDIA attack using Real Time Digital Simulator (RTDS).

II. MICROGRID ADAPTIVE PROTECTION

Coordination of DOCR in microgrids is a challenging task due to different locations of the DER. This means a need of changing DOCR settings for different scenarios compared to conventional coordination in radial distribution systems, where static settings and non-bidirectional elements are sufficient to protect the network. In microgrids, the considerations for DOCR coordination are as follows:

- Type of DOCR tripping curves (standard inverse, very inverse and extreme inverse)
- Primary and back-up relay pairing
- Plug setting optimization
- Time-dial setting optimization
- Change settings for every grid configuration (varying conditions)

Once the considerations are made, the coordination problem can be formulated as a minimization of the total operation time of the primary and back-up relays, while keeping a minimal operation time for each relay and Coordination Time Interval (CTI) between relays as

$$\min T_{op} = \min \sum_{i=1}^n (t_{pi} + t_{bi}) \quad (1)$$

where, T_{op} is the total operation time of primary and back-up relay pairs, t_p and t_b refer to the operation time of the primary and back-up relay, and n is the amount of primary/back-up relay pairs. Each relay operation time can be calculated as

$$t_p, t_b = \frac{\alpha \times TDS}{\left(\frac{I_f}{CTR \times PS}\right)^\beta - 1} \quad (2)$$

in which α and β are values depending on the curve characteristics of the DOCR relay shown in table I, I_f is the fault current seen by the relay and CTR is the current transformer ratio.

TABLE I: IEC Curve Characteristics of DOCR Relays.

Curve type	α	β
Standard inverse (C1)	0.14	0.02
Very inverse (C2)	13.5	1
Extreme inverse (C3)	80	2
Long-time inverse (C4)	120	1
Short-time inverse (C5)	0.05	0.04

For better coordination, instead of having one constant TDS or PS at time per optimization, they should be multi-objective variables in the problem. TDS have setting bounds of

$$0.025 \leq TDS \leq 1.2 \quad (3)$$

where these times are selected based on experimental results [15] and, the product of CTR times PS is known as pick-up current (I_{pu}) selected like in [16] in the interval of

$$1.3 * I_{load} \leq I_{pu} \leq I_{fmin} \quad (4)$$

where I_{load} is the nominal current under normal operation conditions, I_{fmin} is the minimal short circuit current and they are obtained by performing the power flow and short circuit analysis. Inequality shown in Eq. 4 is a useful guide to choose an adequate value of CTR . Both TDS and PS stepping size depends on the relay manufacturer.

The objective function has two constraints, e.g., Eqs. (5) and (6). They indicate the tripping time of DOCRs can not be below 100 ms and their coordination time between trips is around 250 ms . These constraint times are chosen arbitrarily based on experimental results to guarantee safety margins [15].

$$t_p, t_b \geq 0.1 \quad (5)$$

$$t_b - t_p \geq 0.25 \quad (6)$$

A. Proposed Microgrid Cases and Optimization

In this study, we used the CIGRE low voltage (LV) benchmark microgrid (see Fig. 1). It consists of five loads and five DER points distributed in the microgrid. The DOCRs are placed in a way that all zones are protected at all times.

The microgrid parameters are presented in Table II. The three microgrid scenarios analyzed in this paper include:

- 1) Grid connected: $SW1$ closed and both DER 1/DER 2 operating, see Fig. 1a
- 2) Islanded mode: $SW1$ open and both DER 1 DER 2 operating, see Fig. 1b
- 3) Partial DER: $SW1$ closed but only DER 2 operating, see Fig. 1c.

In this paper, the pair $R9$ and $R7$ of the main and back DOCR from Fig. 1 were implemented and tested at the fault point $F5$. To obtain the optimized setting values, first, a power flow and short circuit analysis is done for the three scenarios. The grid implementation was simulated using a Digital real-time simulator (DRTS). The information was used to adjust current transformer (CT) values and I_f from Eq. 2.

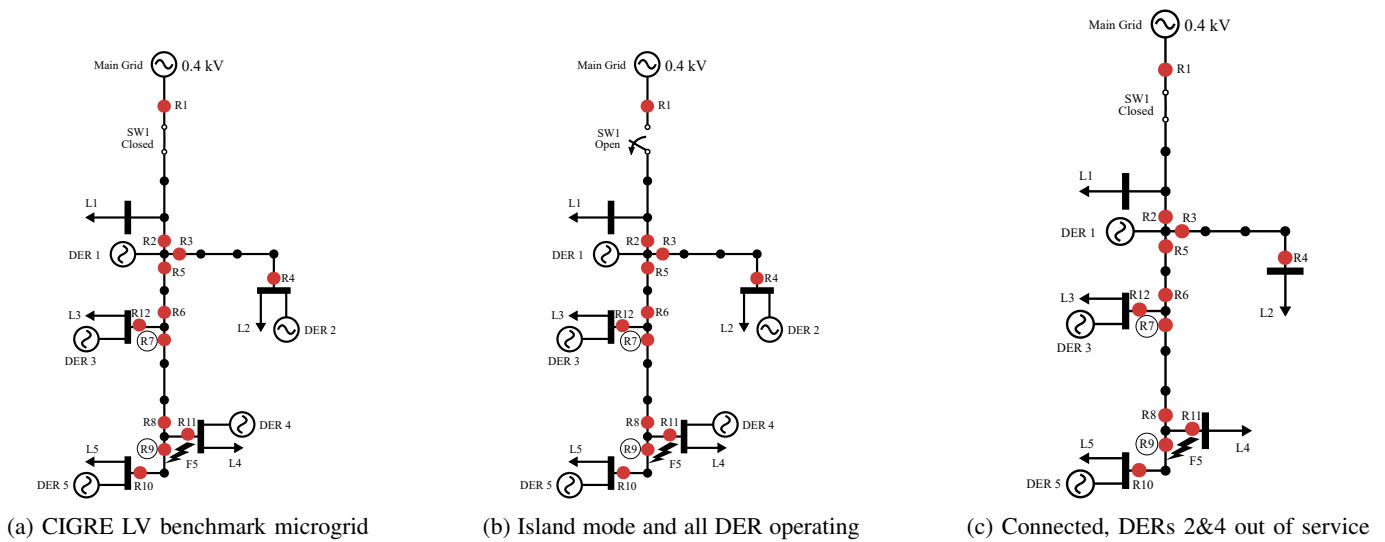


Fig. 1: Microgrid scenarios considered in this paper.

TABLE II: Microgrid Parameters.

Load	S_{max} [kVA]	S_0 [kVA]
L1	15	5.7
L2	72	57
L3	50	23
L4	15	5.7
L5	47	25
DER number	Type	Power [kW]
1	Batteries	30
2	Microturbine	30
3	Photovoltaic	4x2.5
4	Photovoltaic	40
5	Fuel Cell	40

TABLE III: Power Flow and Short Circuit for R9 and R7.

Scenario	DOCR			
	R9		R7	
	I_n (A)	I_f (A)	I_n (A)	I_f (A)
Grid connected	7.9	803.8	31.82	691.3
Islanded	23.08	266	71.16	119
DER 2&4 OFF	28.22	381.7	48.44	394.6

TABLE IV: DOCR Settings for the Microgrid Scenarios.

Scenario	Group settings	DOCR			
		R9		R7	
		PS	TMS	PS	TMS
Grid connected	1	1.736	0.01	1.389	0.03
Islanded	2	3.318	0.01	1	0.016
DER 2&4 OFF	3	0.5	0.0172	1.236	0.01

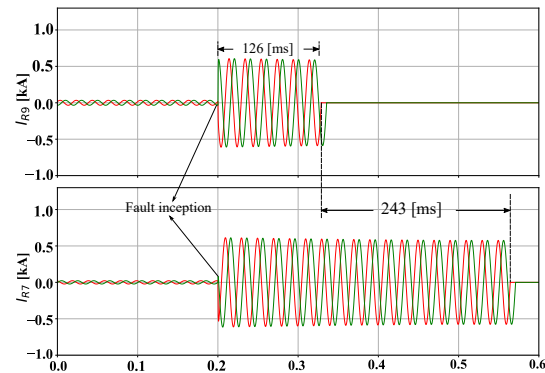


Fig. 2: Coordination time between R9 and R7 for BCG fault.

The obtained nominal values and fault currents at the point of interest are summarized in Table III (the algorithms used in this paper are available at https://github.com/daniel-gutierrez-rojas/Projections_cyber_attacks.git).

Next, using the values of Table III, we proceed to obtain DOCR settings according to the operational state of the grid. Due to the non-linear nature of the objective function, to minimize coordination time of relays, meta-heuristics are used to find the global optimal solution. In this paper we used Particle Swarm Optimization (PSO) to retrieve settings values. PSO is a swarm-based optimization technique, which has been inspired by bird flocks [17]. The optimization is initialized for one or several particles inside the constrains and they update their position according to the functions of speed and movement direction. It has been widely used in power systems and also in case of relay coordination [18]. The settings obtained employing the PSO are seen in Table IV. An example using the obtained settings for the scenario with the settings 3

on the fault point F5 is shown in Fig. 2, where the tripping of R9 occurs slightly after 100 ms while the time between the relays is maintained around 250 ms.

B. Cyber attack Formulation

Cyber attacks lead to a high risk both to the DER power system infrastructure and end consumers. The paper considers a data injection cyber attack on the GOOSE protocol of the IEC 61850 standard. GOOSE is a fast and reliable data transmission protocol. According to the first edition of IEC 61850, it is used at power substations utilizing only local area networks (LAN). The second edition extends the applicability of the GOOSE protocol with the introduction of routable GOOSE (R-GOOSE). It allows to use it with a wide area network (WAN), making it possible to utilize the protocol at a distribution grid [19]. R-GOOSE has security data field inside the data frame, which allows protecting the data flow from

cyber attacks, while the original GOOSE does not. The details about GOOSE and R-GOOSE can be founded in [20].

The current research focuses on the GOOSE protocol, assuming that a hacker gets access to a device at the LAN where the respective industrial IEDs and Raspberry Pi are also connected. The detailed description of hacking of the device in LAN is out of the scope of this research. One possible way of getting access to a LAN is the existence of an unsecured router that, for example, uses a default password, provides access to the WAN. Raspberry Pi's communication driver is able to access the L2-type network which is used to run GOOSE message streams. Therefore, it can both receive and send GOOSE messages within a LAN, and thus, is considered as a device in LAN which the hacker gets access to carry out its attack. Fig. 3 illustrates the communication network configuration of the testing setup which includes a digital real-time simulator, control and protection IEDs, Microgrid central control (MGCC) and RPi acting as a hacked device.

The initial stage of the attack is data collection from LAN and its analysis. It is done with Tshark which is a terminal-based version of the network analysis tool, Wireshark. Tshark allows the visualization of all fields of the GOOSE message including names of sending and receiving nodes, time to stay alive, and actual information about the setting group. GOOSE protocol is intended to be used at LAN only and it does not have any security hash fields. Therefore, using the collected information and after the definition of possible targets for the cyber attack, a modified GOOSE message with wrong information can be replicated using an open-source C++ library design by MZ Automation (<https://github.com/mz-automation/libiec61850>), which is ARM-compatible and allows to cross-compile applications for RPi. The library allows the transmission and reception of MMS, SV, and GOOSE messages on non-industrial devices like laptops and single-board computers. In the considered case MZ Automation library is used to compile and run a GOOSE publisher application. The sending frequency for the fake publisher is adjusted in a way to affect the control device.

After the hacking is initiated, there are two data streams: (1) with the fake information, which goes from hacked Raspberry Pi, and (2) the right information, going from the MGCC. In the case of equality of sampling rates of the hacker and controller, the setting fluctuates between right and wrong groups. These fluctuations lead to the constant and frequent tripping of the setting group relays that can damage protection IEDs and with the loss of its functionality.

In order to set up only the wrong parameters to the protection IEDs, there is a need to suppress the right data flow from the controller. It can be done with a high sampling frequency of the data flow going from the hacker device. The sampling rate of the fake data sent from Raspberry Pi should be 30-50 times higher than the sampling rate from control IEDs. Finally, the wrong setting group set up to the protection relay leads to the insensitivity of protection IEDs to the faults or false tripping of the protection.

As a result, a cyber attack can have dramatic consequences on the state of control and power equipment, and distribution grid. A cyber attack on adaptive protection affects their

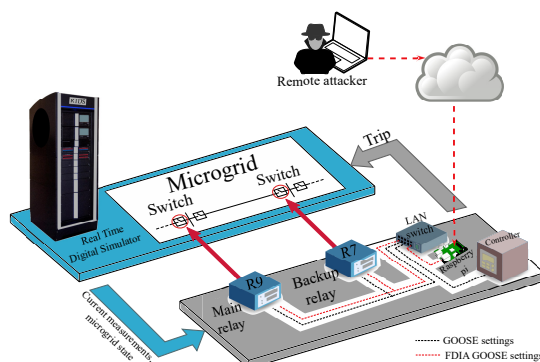


Fig. 3: Schematic of implemented cyber attacks in laboratory.

proper functionality. Therefore, there is a need to design cyber-security measures to prevent such attacks, ensuring safe operation of the control and protection IEDs.

III. CYBER-ATTACKS HIL TESTING

Traditionally, power system protection architecture has relied on centralized decision making and computational mechanisms. This includes adaptive protection, secondary and tertiary control schemes for microgrids. Due to its simplicity, centralized infrastructure has preferably been used in power systems and electronics applications. However, it suffers from issues like single-point-of-failure, high communication bandwidth requirements, aggregated computation, etc. As a result, the reliability of centralized philosophy is often challenged albeit its high cost. A single point of cyber intrusion (aimed at either manipulating or interrupting the information in the cyber layer) can cause immediate failures/unavailability of services.

To replicate a cyber attack, we followed the methodology presented in Section II-B. The test was performed using Hardware-in-the-loop (HIL) simulation on the DRTS. For this, we first simulated the CIGRE LV benchmark on the cyber layer including all control and measuring signals. Then, on the physical layer, we connected two commercial DOCR (R9 and R7 see Fig. 1) to the LAN network, along with a commercial controller and Raspberry Pi both controlled remotely. Finally, the communication signals were all set up so the system closes the loop by the DRTS sending information to the controller about the state of the grid, and the relays sending back command trips to simulated switches in the software interface. The schematic of the test setup is illustrated in Fig. 3.

The test begins with running the simulation on grid-connected operation. Then, by opening SW1 and switches located in DER 2 and DER 4 we change the microgrid scenarios. Both relays are checked so that they set accordingly to the scenario by the messages sent by the controller and the grid runs in steady state without the presence of faults. When the system is running on grid-connected mode with DER 2&4 OFF, the remote attacker sends GOOSE messages of a different setting group (islanded) through Raspberry Pi into the LAN network. These messages are sent in frequency higher as twice the frequency of what the controller sends GOOSE messages. The controller works on a way that it sends periodically GOOSE messages to the relays depending on the scenario and DOCRs receive the messages and it is able to

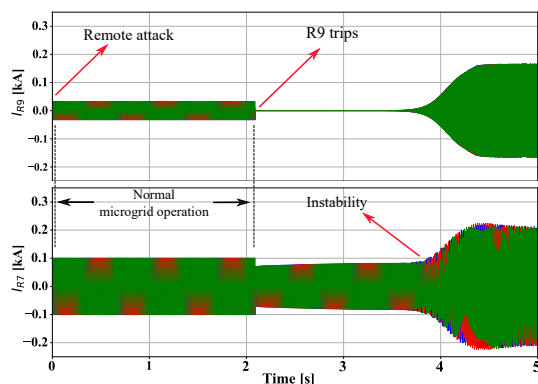


Fig. 4: Three-phase current of DOCR R9 and R7 during FDIA.

reset within less than one second. Once the attacker’s messages arrive into the LAN, due to the faster frequency, they overlap the ones sent by the controller, and DOCRs are only able to see the ones sent by the remote attacker and therefore change the setting group from DER 2&4 OFF to islanded.

From Fig. 4, we can examine the sequence of the event when the FDIA begins. When the message overlapping occurs and the attacker is able to change deliberately from group setting #2 to #3, due to the lower PS in DOCR R9, it perceives the change as an increase in the current similar to an electrical fault and then it trips. After R9 trips, it leads to initially lowering the current passing on DOCR R7, then the microgrid becomes unstable and it rapidly increases the current on R7 making it trip as well. The tripping times are according to the settings and operational time from Eq. (2). It is worth to notice that there is no coordination between the DOCRs R9 and R7 because of change in setting parameters. The time that passes between the moment the attacker sends the messages remotely and the DOCR receives the false settings is around 2 seconds. The experiments done using this type of FDIA were marked as successful even though the attacker will have limited access despite having a reasonable amount of knowledge of both physical and cyber components [21]; this article also contains a more detailed taxonomy of cyber-attacks in microgrids. The attacker was able to remotely trip the relay under normal microgrid operation and create instability.

The experiments were also conducted by trying different frequencies on which the attacker send the messages. To obtain a successful attack, is necessary at least double of the frequency that controller sends the messages. Above this, the DOCR enter in a mode where the group settings changes for about 3 seconds and then they block themselves.

IV. CONCLUSION

Cyber attacks are nowadays becoming a large topic of discussion in protection of power systems. Hackers have more access to information than in the past, which was thought to be exclusively from system operators and it is granted by accessing commercial equipment installed at vulnerable links of the grid. Since these equipment and the principle of operation is easily available, new schemes are needed to further ensure high levels of security. In this article, we proposed a centralized strategy for adaptive DOCR setting in microgrids. The DOCR

set their own protective setting group based on specific logic with the signal coming from a central controller. A remote FDIA was then formulated and implemented in HIL showing the vulnerabilities of a real deployment. Moreover, it has been identified that how conventional protection schemes might be subject to a relatively easy attack. This emphasizes that there is a need for adaptive protection in microgrids with high-level security.

REFERENCES

- [1] M. N. Alam, “Adaptive protection coordination scheme using numerical directional overcurrent relays,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 64–73, 2019.
- [2] A. S. Musleh *et al.*, “A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications,” *IEEE Systems Journal*, vol. 13, no. 1, pp. 710–719, 2019.
- [3] D. Gutierrez-Rojas *et al.*, “Review of the state of the art on adaptive protection for microgrids based on communications,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1539–1552, 2021.
- [4] S. Mukherjee *et al.*, “Adaptive protective relay settings – a vision to the future,” in *2022 IEEE Rural Electric Power Conference (REPC)*, pp. 25–30, 2022.
- [5] M. Monadi *et al.*, “Centralized protection strategy for medium voltage dc microgrids,” *IEEE Transactions on Power Delivery*, vol. 32, no. 1, pp. 430–440, 2017.
- [6] V. A. Papaspiliopoulos *et al.*, “Hardware-in-the-loop design and optimal setting of adaptive protection schemes for distribution systems with distributed generation,” *IEEE Transactions on Power Delivery*, vol. 32, no. 1, pp. 393–400, 2017.
- [7] H. Laaksonen, D. Ishchenko, and A. Oudalov, “Adaptive protection and microgrid control design for hailuoto island,” *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1486–1493, 2014.
- [8] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, “Denial-of-service attack on iec 61850-based substation automation system: A crucial cyber threat towards smart substation pathways,” *Sensors*, vol. 21, no. 19, 2021.
- [9] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, “Learning-based methods for cyber attacks detection in iot systems: A survey on methods, analysis, and future prospects,” *Electronics*, vol. 11, no. 9, 2022.
- [10] G. Liang *et al.*, “The 2015 ukraine blackout: Implications for false data injection attacks,” *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.
- [11] K.-D. Lu and Z.-G. Wu, “Multi-objective false data injection attacks of cyber-physical power systems,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 9, pp. 3924–3928, 2022.
- [12] V. S. Rajkumar *et al.*, “Cyber attacks on power system automation and protection and impact analysis,” in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, pp. 247–254, 2020.
- [13] Q. Dai, L. Shi, and Y. Ni, “Multi-objective optimal cyber-attack strategy in centralized feeder automation system,” in *2019 IEEE Power Energy Society General Meeting (PESGM)*, pp. 1–5, 2019.
- [14] Q. Zhou *et al.*, “Distributed control and communication strategies in networked microgrids,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2586–2633, 2020.
- [15] F. Adelnia, Z. Moravej, and M. Farzinfar, “A new formulation for coordination of directional overcurrent relays in interconnected networks,” *International Transactions on Electrical Energy Systems*, vol. 25, no. 1, pp. 120–137, 2015.
- [16] K. Xu and Y. Liao, “Online adaptive optimum coordination of overcurrent relays,” in *Proc. SoutheastCon 2018*, pp. 1–6, 2018.
- [17] R. Eberhart and J. Kennedy, “A new optimizer using particle swarm theory,” in *MHS’95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science*, pp. 39–43, Ieee, 1995.
- [18] A. Liu and M.-T. Yang, “Optimal coordination of directional overcurrent relays using nm-PSO technique,” in *Proc. Consumer and Control 2012 Int. Symp. Computer*, pp. 678–681, 2012.
- [19] Typhoon, *IEC 61850 GOOSE Protocol*. Typhoon HIL Documentation.
- [20] T. S. Ustun *et al.*, “Implementing secure routable goose and sv messages based on iec 61850-90-5,” *IEEE Access*, vol. 8, pp. 26162–26171, 2020.
- [21] M. Leng *et al.*, “Projections of cyberattacks on stability of dc microgrids—modeling principles and solution,” *IEEE Transactions on Power Electronics*, vol. 37, no. 10, pp. 11774–11786, 2022.