Please cite the Published Version

Additional Information: This is an open access article which first appeared in IET Renewable Power Generation

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Enhancing resilience of advanced power protection systems in smart grids against cyber–physical threats

Feras Alasali[1] | **Ali M. Hayajneh[1]** | **Salah Abu Ghalyon[2]** | **Naser El-Naily[3]** | **Anas AlMajali[2]** | **Awni Itradat[1]** | **William Holderbaume[4]** | **Eyad Zaroure[5]**

[1]Department of Electrical Engineering, Faculty of Engineering, The Hashemite University, Zarqa, Jordan

[2]Department of Computer Engineering, Faculty of Engineering, The Hashemite University, Zarqa, Jordan

[3]College of Electrical and Electronics Technology-Benghazi, Benghazi, Libya

[4]School of Science, Engineering and Environment, University of Salford, Salford, UK

[5]Electrical Engineering Department, The University of Jordan, Amman, Jordan

Correspondence
Feras Alasali, Department of Electrical Engineering, Faculty of Engineering, The Hashemite University, P.O. Box 330127, Zarqa 13133, Jordan.
Email: ferasasali@hu.edu.jo

William Holderbaum, School of Science, Engineering and Environment, University of Salford, Salford M5 4WT, UK.
Email: w.holderbaum@salford.ac.uk

Funding information
Scientific Research and Innovation Support Fund; Ministry of Higher Education Scientific Research; The Hashemite Kingdom of Jordan, Grant/Award Number: ENE/1/02/2022

Abstract

Recently, smart grids introduce significant challenges to power system protection due to the high integration with distributed energy resources (DERs) and communication systems. To effectively manage the impact of DERs on power networks, researchers are actively formulating adaptive protection strategies, requiring robust communication schemes. However, concerns remain over the occurrence of communication connection failures and the potential risks presented by cyber-attacks. This work addresses these challenges by investigating the impact of cyber-attacks on different adaptive overcurrent relays (OCRs) approaches. Here, modern adaptive OCR coordination approaches using different group settings has integrated in evaluating high voltage/medium/low voltage (HV/MV/LV) network model with real network parameters at the MV/LV level. Additionally, a voltage-based relay is developed and employed to enhance protection system performance under various cyber threats, aiming to reduce tripping time and to minimize energy that is not supplied. The results show that voltage-based scheme outperform the traditional adaptive OCRs in terms of response time and mis coordination events under cyber-attacks. In the proposed MV/LV real network scenario characterized by an 89% availability of a 4 MW photovoltaic system, even a brief interruption caused by cyber-attacks can result in significant cost consequences.

1 | INTRODUCTION

1.1 | Motivation and incitement

The concept of automatic-governed networks called "microgrids" holds promise for improving power grid reliability. However, to achieve a successful implementation, advanced automation, communication technologies, and environmentally friendly distributed energy resources (DER) are required. To efficiently meet the growing energy needs, wind and photovoltaic (PV) energy sources are commonly used in these

modern microgrids. Microgrids offer benefits such as islanding and multi-network operations for enhanced power supply security [1]. Despite this, their distinctive grid structure poses severe issues in the protection system, resulting in relay coordination failures. To overcome these issues, it is crucial to develop robust protection schemes and ensure the successful integration of microgrids in the power systems. In the domain of power protection systems, resilience denotes the system's capacity to withstand and mitigate the effects of external disturbances while preserving or restoring its functionality [2, 3]. A critical aspect to ensure safe and cost-effective operations of

TABLE 1 Modern adaptive protection schemes: State-of-the-art review.

Ref.		DER Technology	MG operation	Communication system	Cyber-attacks
		DN aspects considered			**Cyber-attacks**
[4]	2004	SBDG	Grid Connected	Phasor Measurement Unit	O
[5]	2014	SBDG	Islanded & Connected	IEC61850	O
[6]	2018	SBDG	Islanded & Connected	Phasor Measurement Unit	O
		IBDG			
[7]	2018	SBDG	Islanded Connected	IEC 61850	O
		IBDG			
[8]	2020	SBDG	Islanded & Connected	IEC61850	O
		IBDG			
[9]	2021	SBDG	Islanded & Connected	IEC 61850	O
		IBDG			
[10]	2021	SBDG	Islanded & Connected	IEC 61850	O
		IBDG			
[11]	2022	SBDG	Islanded & Connected	IEC 61850	O
		IBDG			
[12]	2022	IBDG	Islanded & Connected	IEC 61850	O
[13]	2022	SBDG	Islanded & Connected	IEC 61850	O
		IBDG			
[14]	2022	SBDG	Islanded & Connected	IEC 61850	O
		IBDG			
[15]	2022	SBDG	Islanded & Connected	IEC 61850	O
		IBDG			
[16]	2023	IBDG	Grid Connected	IEC 61850	O
[17]	2023	SBDG	Islanded & Connected	IEC 61850	O
		IBDG			

*SBDG, Synchronous-based distributed generations; IBDG, Inverter-based distributed generations.

microgrids lies in the coordination of protection relays. Hence, we can facilitate rapid, sensitive, and dependable relay operations during various fault scenarios. Consequently, as shown in Table 1, recent research efforts have focused on the formulation of new adaptive protection schemes to mitigate the potential impacts of DER integration on both radial and mesh power networks. These schemes rely on a communication infrastructure across the distributed network (DN) to overcome any miscoordination events in the grid. However, modern digital relays and adaptive protection scheme which relied on communication links are essential cyber physical components. For example, they are unable to perform internal validation checks to distinguish between real and fake faults or changing the groups setting of relays [4–6]. To the authors knowledge, there is lack of research on the resilience of modern adaptive power protection systems under cyber physical threats using real power distribution net-

work specifications. Therefore, in this research, we focus on cyber physical threats concerns for the modern adaptive overcurrent relays (OCR) protection schemes which is an essential aspect to establish a robust protection system for the studied smart grid.

1.2 | Literature review

Adaptive protection is an approach that involves adjusting protection functions to improve the prevailing power system conditions. This adaptability allows for dynamic adjustments of the relay trip characteristic, enhancing protection effectiveness, and is exemplified in protection coordination. Barra et al. [18] highlighted that there is a growing trend in research publications related to adaptive protection. There has been a notable

increase in the number of papers mentioning and employing terms "adaptive protection or relaying". This indicates a current and relevant interest in the field. The highest number of publications, suggesting a continued need for further research and exploration in the area of adaptive protection. For example, Mahat et al. [19] presented an adaptive OCR protection scheme for DN with DER. The protection system updates the trip characteristic of OCR based on the system's operating states (grid-connected or islanded) and faulted section. State detection algorithms are utilized by the relays to identify the system status and select appropriate tripping characteristics accordingly. The study conducts simulations for different scenarios, including normal DG operation, islanded mode, and contingency situations with DG disconnection. Similarly, Singh et al. [20] introduced an adaptive protection coordination scheme based on updating the settings of OCRs based on changes in grid topology. It uses an adaptive fuzzy-based technique for online selection of relay settings and optimizes them offline using the differential search algorithm. Several other works have been published within the same context of adaptive OCR protection schemes [21, 22] by proposing compact algorithms that utilize existing OCR relay setting groups. However, the previous literature did not discuss or investigate the grid and protection system resilience under cyber physical threats. It is important to highlight that in a considerable number of the research [23, 24], the implementation of an adaptive protection scheme for microgrids requires a well-established communication structure. Nonetheless, concern regarding the potential risks associated with communication link failures and cybersecurity threats can be noticed. Thus, successful deployment of a fast, robust, and reliable adaptive protection scheme is required on addressing these challenges. Therefore, it is apparent that the vulnerability of communication links and cyber threats shows a significant drawback for many of the existing adaptive protection proposals in microgrids. To address this concern, Habib et al. [25] conducted a comprehensive review on the consequences of communication failure in such schemes at the grid with energy storage system. They highlighted that, when communication breaks down, relay settings remain unchanged, rendering any adaptive protection scheme ineffective. Additionally, the authors [25] explored various types of cyber-attacks that could potentially impact adaptive protection systems. For instance, attackers could transmit malicious code to relay and overload it with oversized data. Another scenario involves attackers capturing and retaining GOOSE messages, enabling them to send a forged message and trip a circuit breaker during normal operation, thus triggering undesirable actions. Recent literature highlights the needs for integrating communication technologies into microgrids in order to effectively implement modern adaptive protection schemes [26]. However, the complex interaction between the cyber and physical components in these systems pose challenges in devising suitable control algorithms and limited research on analyzing the adaptive and grid performance under different cyber–physical threats scenarios. The difficulty arises from the highly interconnected nature of adaptive protection in microgrids, where even minor deviations in the cyber domain can lead to severe consequences

in the physical domain [27]. Hence, ensuring a reliable and robust operation for the adaptive protection schemes is critical to address the complex relations of dependence between the cyber and physical elements. One potential solution involves connecting all relays to a central management system, which delivers setting groups unidirectionally. However, this approach is costly in terms of the capital and the operational expenditures (CAPEX/OPEX) and communication systems, relying on standard communication protocols like GOOSE and SMV [26]. However, the work by [26] discussed the challenges in designing algorithms for optimal adaptive protection systems due to time limitations on fault-related signal communication imposed by standards such as IEC 61850 mandates a 4 ms time constraint on SMV and GOOSE messages.

Adaptive protection algorithm design, involving the collaboration of multiple relays to detect and isolate faults, becomes even more complex and time-critical [26, 27]. These factors present significant challenges in creating effective adaptive protection schemes. Therefore, this work aims to investigate and analyze the impact of different cyber threats on the performance of modern adaptive schemes and grid operation. Table 2 provides a comprehensive overview of the limitations that are associated with the adaptive protection schemes in microgrids, along with the limited research proposed in the existing literature for investigating the cyber–physical threats. Rahman et al. [28] and Mohamed and Salama [35] introduced two tools to identify cyber threats on the power protection system. However, the paper did not address the impact of cyber threats on different adaptive OCR with and without communication needs. Effective adaptive OCR protection in microgrids addressed faults in both grid-connected and islanded modes, which have different fault current levels and paths. In another work [38], the OCR tested and evaluated under cyber threats, however, the OCR is evaluated in only at location closest to the fault location. Current literature [26, 40] emphasizes the importance of incorporating communication technologies into microgrids to successfully achieve high performance for adaptive protection schemes. The authors in [26, 40] evaluated the performance of adaptive OCR under DOS and FDI attack in LV, respectively. The authors [26, 40] did not investigate the impact of different cyber-attack or network topology or voltage level. In addition, the interaction between cyber and physical components within these systems presents challenges in formulating appropriate control algorithms, and there is limited research available on assessing the adaptive and grid performance in the presence of various cyber–physical threat scenarios. Therefore, in this work adaptive protection scheme for OCRs based on voltage and current readings and without communication links is proposed and tested to minimize modern cyber challenges by be less relaying on communication links.

1.3 | Contributions

The difficulties associated with modern adaptive OCR approaches and lack of research on enhancing communication failure highlight the need to investigate the impact of

TABLE 2 Summary of dual overcurrent relays (OCRs) coordination approaches for a power network with distributed energy resources (DER).

Ref.	Year	Voltage level	ISC protocol	Type of cyber-attack	Study area	Real network parameters	Adaptive schemes
[28]	2016	HV	Phasor measurement unit	FDI DOS MITM IA RA	Protection System	O	O
[29]	2019	HV	IEC61850 GOOSE	FDI DOS	Distance relay	O	O
[30]	2020	HV	IEC61850 GOOSE SV	Spoofing with a false data injection	Distance relay	O	O
[31]	2020	MV	IEC61850 GOOSE	DOS	OCR	O	O
[32]	2021	HV	PMU	FDI DOS	Distance relay	O	O
[33]	2021	HV	IEC61850	FDI	Differential relay	O	O
[34]	2022	HV	IEC61850 GOOSE	Communication failure	Protection system	O	O
[35]	2022	MV	IEC61850 GOOSE	FDI DOS	OCR	O	O
[36]	2023	HV	IEC61850 GOOSE	FDI DOS	OCR	O	O
[37]	2023	HV	IEC61850 SV	FDI DOS	Differential relay	O	O
[38]	2023	HV	IEC61850 GOOSE	FDI DOS	OCR	O	O
[26]	2017	LV microgrid with 6-bus	O	DOS	OCR	O	P
[39]	2022	MV IEEE 34-bus distribution	O	DOS MITM	Protection relay	O	P
[40]	2023	CIGRE low voltage (radial LV)	GOOSE	FDI	OCR	O	P
The proposed study		HV/MV/LV with real network parameters at the MV/LV level	IEC61850 GOOSE	FDI DOS MITM	OCR	P	P

*MITM, man-in-the-middle; FDI, false data injection; IA, integrity attack; RA, replay attack; DoS, denial of service.

cyber-physical threats. In addition, this showed that developing a flexible protection scheme that enhanced selectivity and reliability with less reliance on communication is highly important.

The key outcomes and contributions of this study can be summarized as follows:

- Examining and demonstrating the impact of different cyber-attacks on modern adaptive OCR protection schemes and power system operations. The paper focuses on cyber-attack scenarios that exploit potential vulnerabilities within the GOOSE and other protocols where limited number of research as shown in Table 1 evaluated the adaptive OCR schemes under limited scenarios of cyber-attacks.

- Developing and evaluating a modern voltage-based OCR scheme without communication dependently to improve the protection system performance under different cyber threats in term of tripping time and energy not supplied.

- The modern adaptive OCRs coordination approaches based on employing different group setting are tested and evaluated on HV/MV/LV network model with a real network parameter and measurands under different cyber-attacks and physical fault scenarios compared to the literature which focused on level of voltage network and without real network parameters, as shown in Table 1.
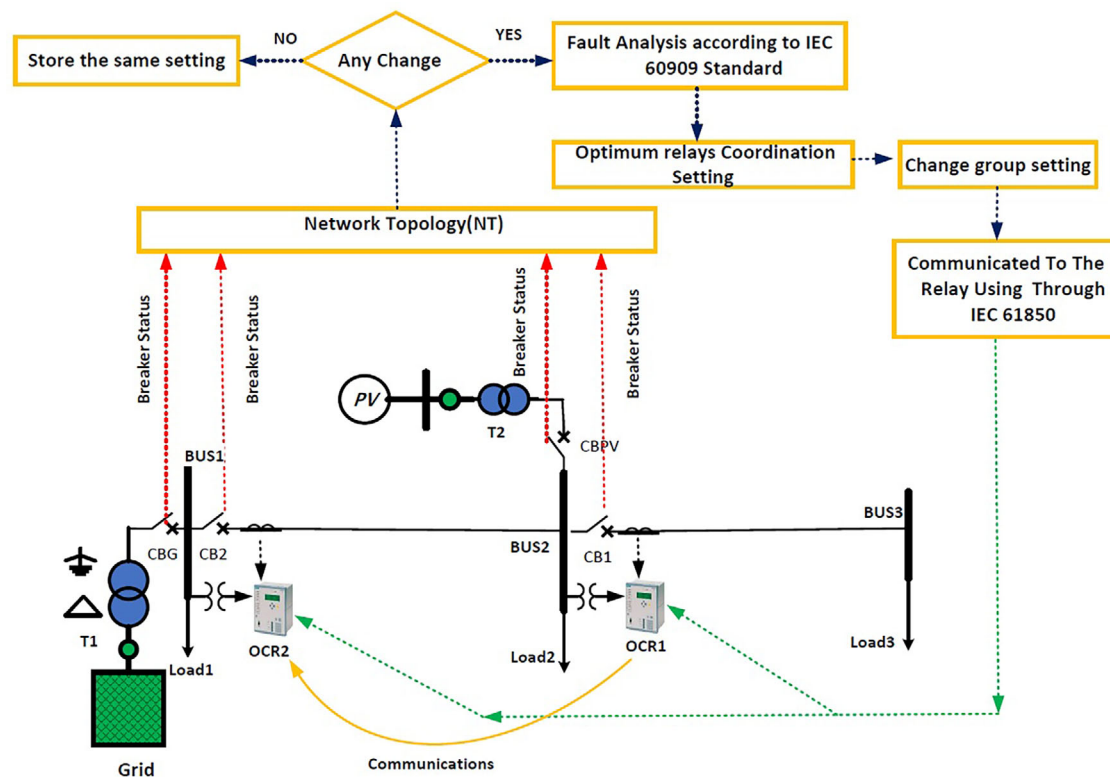
FIGURE 1 Adaptive overcurrent relays (OCR) schemes.

1.4 | Outline of the paper

The remaining of this work is organized as follows: Section 2 present the modern OCR protection schemes (adaptive OCR scheme and voltage-based relays). Section 3 introduce the potential cyber physical threats on adaptive protection system. Section 4 discuss the resilience evaluation process of adaptive protection system on the proposed HV/MV/LV grid. Section 5 present the results of the adaptive OCR scheme and voltage-based relays under different fault and cyber-attacks scenarios. Finally, the summary of this study is presented in Section 6.

2 | PROPOSED ADAPTIVE OCR SCHEME AND NEW VOLTAGE-BASED RELAYS

2.1 | Adaptive OCR scheme

Adaptive protection enhances the protection system's ability to handle the dynamic and evolving conditions of the power system by enabling it to make adjustments. In this research, modern adaptive protection systems, as presented in [41–43] are developed and evaluated. As shown in Figure 1, the common adaptive OCR schemes change the group setting of the OCR based on the network topology (NT), namely: traditional power network (only feeding by utility sources) or grid connected to PVs modes. Initially, the status of breakers and grid information is utilized to ascertain the network topology, whether it

TABLE 3 The group settings for the adaptive overcurrent relays (OCRs).

Group settings	Utility power source	PV power source
A	P	O
B	P	P

operates in grid-connected mode or islanding mode. Subsequently, the current state of the network topology is compared to its previous state, and if it remains unchanged, the previously saved settings are employed. However, if there's a change in the network topology, a combination of fault analysis and grid data is considered to identify the optimal configuration for OCRs by solving the specified objective function as outlined in Equations (1) and (2) [2, 3]. In this study, the water cycle algorithm, as a robust and powerful optimization technique for solving OCR coordination problems, is employed to determine the optimal OCR settings. The application and details of the water cycle algorithm for OCR coordination problem resolution are elaborated in [44]. The selected group settings for OCRs are then chosen and implemented via communication links. In this research, two group settings, as elaborated in Table 3, are employed to achieve OCRs' heightened sensitivity and selectivity. This modern adaptive OCR approach assumes continuous monitoring of electrical quantities and with full communication dependently for the OCR signals in real-time. To make the proposed approach practical for implementation, the OCR should also allow automatic real-time changes to their respective

settings [2, 3].

$$T = \min \sum_{n=1}^{N} \sum_{l=1}^{L} (t_{nl}) \quad (1)$$

$$t_n = \left[\frac{a}{\left(\frac{I_f}{I_p}\right)^b - 1} TMS \right] \quad (2)$$

The formulation of objective function in Equation (1) is conducted with a comprehensive consideration of selectivity constraints and the clearing time interval (CTI) that exists between primary and backup relays, as outlined by [2, 3]. Here, the variables N and L present the number of OCRs and the fault location, respectively. Additionally, t_{nl} denote the tripping times of the OCR number n for a fault transpiring at location l. In the context of OCRs, the commonly employed curve follows an inverse-time characteristic. The general mathematical representation for this characteristic is articulated through Equation 2, where t_n signifies the operating time of each individual OCR, I_f represents the short-circuit current, and I_P denotes the pickup current. The attributes of the time-inverse characteristic curve, notably a and b, are delineated in the relay characteristics. Additionally, these attributes are integral to the time multiplier setting (TMS) equation. In this work, the optimal TMS is selected to achieve the minimum tripping time.

2.2 | Modern voltage-based protection scheme

The adaptive protection scheme, as discussed in Section 2.1, relies on the current level and communication between the primary and backup relays to change the group setting of the OCR based on the NT. This included a high probability of operation risks under cyber-attacks. In this work, a modern voltage-based protection scheme without communication dependently is presented and employed to improve the protection system performance under different cyber threats compared to modern adaptive scheme, as presented in Section 4.1. This voltage-based protection scheme designed for distribution systems incorporating DER. By analyzing voltage behaviour during fault conditions, the OCR characteristic is formulated to detect power physical faults associated with voltage dips at the faulted line ends, as described in [45]. The proposed adaptive voltage-based scheme is independent of the type, size, and location of DER, as well as the grid-connected or islanded (the topology of the network). However, there is a lack of research on enhancing and investigating the impact of cyber-physical threats on different adaptive and voltage OCR schemes. Therefore, developing and employing a flexible protection scheme that obtain selectivity and reliability under cyber threats is highly important. In this work, the proposed voltage-based OCR scheme without communication dependently is employed and developed to improve the protection system performance under different cyber threats in term of tripping time and energy not supplied
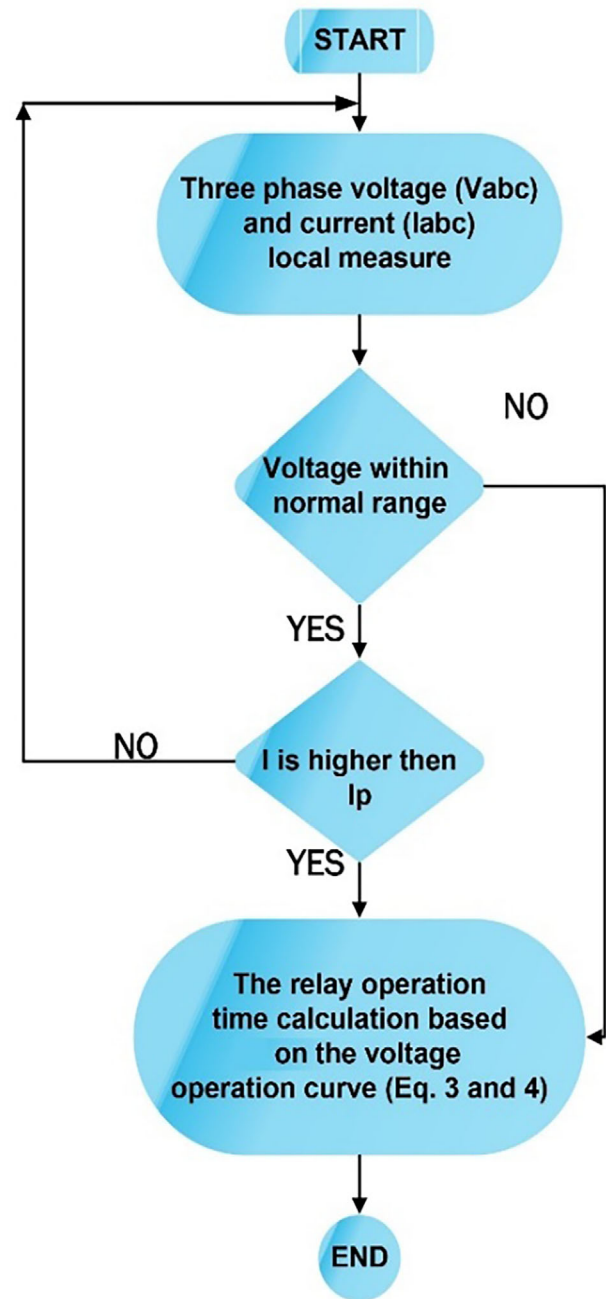
FIGURE 2 Voltage-based protection scheme approach process.

compared to traditional OCR and modern adaptive OCR with communication requirements. The modern voltage OCRs are tested and evaluated on HV/MV/LV network model with a real network parameter and measurands.

The proposed adaptive voltage-based scheme is developed in this work as communication-less and only relies on the local voltage magnitude to determine the operating time of relay, resulting in a cost-effective protection solution under cyber threats. The basic fundamental concept behind this scheme, as shown in Figure 2, is that in the event of a fault, a bus closer to the fault location consistently exhibits a lower voltage magnitude. A threshold voltage level is defined outside the nominal

voltage range. However, if under a fault condition, the voltage dip remains within the nominal range, a current starter is used to trigger the relay in case the current is higher than the pickup current. The proposed approach involves combining the inverse-time overcurrent curves from the IEC 255-3 standard with the logarithm curve of fuse to create a voltage relay curve, as expressed by Equation (3), compared to the traditional adaptive OCRs scheme in Section 2.1 and Equation (2).

$$OT = TMS \left[\frac{c}{\left(\frac{1}{V}\right)^p - 1} \right] \log_2 \left(\frac{1}{V}\right) \left(\frac{1}{V}\right) \qquad (3)$$

In Equation (1), the operating time for OCR (OT) is determined by TMS and constant parameters (c, p), which c has a value of 1. Additionally, the constant p is set to 2 to satisfy the extremely inverse curve of the IEC standard, and the function V is dependent on the fault voltage level (V_f) magnitude in per-unit and r as constant value, as described in Equation (4). The optimal value of TMS and r is selected by using optimization solver [44, 45], which ensure that identical settings are established for both modes of operation (islanding and grid-connected).

$$V = \left(\frac{V_f}{2} \left(1 - \frac{V_f}{2} \right) \right)^r \qquad (4)$$

## 3 | POTENTIAL CYBER–PHYSICAL THREATS FOR ADAPTIVE PROTECTION SYSTEM

OCRs play a crucial role in ensuring a reliable operation of electrical power systems by clearing faults within their protection zone. To ensure proper coordination, these relays typically incorporate a backup element situated upstream of the primary protection. However, in DN with multiple DER locations, protection becomes more complex. Dynamic changes in topology, generation, and load require adaptive OCR systems, as conventional protection schemes may not be adequate [46, 47]. Hence, implementing adaptive protection schemes (particularly in terms of communication failure, storing protective settings, operating curve functions, and cyber threats) presents a significant challenge. To exemplify this concern, Figure 3 demonstrates a radial system scenario with adaptive OCRs. In the event of a fault occurring in one of the lines, the primary relay is responsible for tripping the fault and disconnecting the faulty line. Subsequently, the backup relay comes into action with sufficient coordination time if the primary relay fails to trip the fault and isolate a healthy line for the same fault scenario. However, cyber-attack by changing the adaptive relay setting, blocking the relay trip signal or communication failure can lead to the isolation of healthy lines from the network, power outages, damages and disconnection of DER. As a result, the stability of the network and the energy supply to the network will be adversely affected.

The design and operation of intelligent power protection systems as part of smart grid and substations are guided by number of standards, where the design of communication networks specifically designed for high power utility automation. A modern power protection relays such as adaptive OCRs can be characterized as an advanced cyber-physical system that heavily relies on digital communication. Table 3 provides an introduction to the essential requirements of communication. The time transfer demands of these information exchanges are determined by their importance to the operation of the substation and protection system. Furthermore, Table 3 presents the main message categories found for protection systems in substation, along by the performance standards specified in IEC 61850–5 [39, 40]. The substation is structured into different message types, as described in IEC 61850–5, each with predetermined maximum time required for a transfer process. In Table 4, trip command holds the highly importance and which are intimately linked with protection systems, necessitating an extremely stringent maximum transfer time of only 3 ms, with zero room for tolerance of losses. However, commands such as close, block, unblock, and state can have a more relaxed time transfer requirement of 20 ms. Another type of messages classified as medium-speed possess lower criticality and can accommodate longer transfer durations, although they still rely on accurate time tagging methodologies. For low-speed time-tagged messages, their purpose pertains to gradual recording and configuring functions, events, system data, and non-electrical measurements, such as temperature. Furthermore, time synchronization messages are utilized to synchronize Intelligent electronic devices (IEDs) such as relays and meters inside the smart substation. However, it is important to note that these messages do not hold specific directives for time transmission. The purpose of messages related to station bus raw data is to transmit control instructions from the human–machine interface (HMI) operations. These messages do not require explicit time transmission standards; however, they do require enhanced security measures. However, it is crucial to transmit data in limited-size segments in order to prevent the obstruction or delay of other network connections.

In the literature, researchers have explored cyber-attacks that exploit the generic object-oriented substation event (GOOSE) and sampled value (SV) protocols, resulting in relay tripping and system destabilization [48]. To mitigate such attacks, a strategy is proposed in [49] that enables attackers to model their actions from a central perspective, calculating the attack's damage risk indication to increase its effectiveness and decrease detection chances. However, cyber-attacks on power protection systems extend beyond the communication layer. The primary categorization of cyber-attacks specifically targeted at the protection system level are:

- Man-in-the-middle (MITM): The attack involves unauthorized access to communication channels and modification of measurement devices, compromising both confidentiality and integrity. A specific instance of an MITM attack on GOOSE messages within the IEC 61850 protocol compromised protective relays in substations [50].
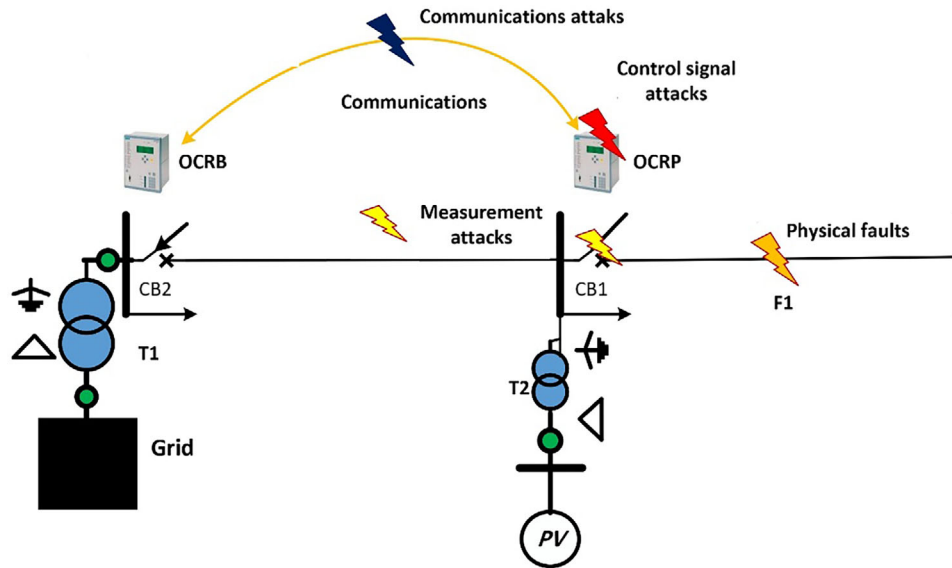
FIGURE 3 Basic adaptive overcurrent relays (OCR) protection scheme and highlight cyber threats.

TABLE 4 Types of messages and communication performance requirements, IEC 61850–5 standard.

Type	Description and speed	Maximum transfer time	Application example
1A	Tripping (fast) for C.B	3 ms	C.B commands (trip, close, block, states etc.
1B	Other (fast) for C.B	20 ms	
3	Alarms and configuration (low)	500 ms	Alarms and configuration at substation for sensors, relays such as temperature
5	File transfer	1000 ms	Data files for the purpose of recording and configuring etc.
6	Time synchronization	N/A	IED (such as relays and meters) internal clock synchronization

- False data injection (FDI): This attack aims to compromise the system's integrity by injecting fabricated data to perform deceptive control or protection operations. Researchers have proposed defence mechanisms, including anomaly detection and machine learning-based methods, to counter FDI attacks. Authors have also examined the impact of these attacks on smart power grids and developed novel detection algorithms to mitigate the risks. Vigilance and proactive measures are emphasized to safeguard electricity system operations against these threats [51].
- Integrity attack (IA) involves a false injection command that can potentially disrupt the operation of digital protection relays' control logic, compromising their integrity.
- The replay attack (RA) is characterized by attackers gaining access to the network's information flow and retransmitting a previously observed message at specific intervals to mimic past disruptions.
- Denial of service (DoS) attacks pose a significant threat with the primary objective of disrupting the online access. This attack involves delaying or halting communication lines and flooding the system with excessive data to overwhelm it. In the context of a power system, external forces may attempt to manipulate and disrupt its operation, leading to

DoS attacks that target the system's access feature by impeding communication links. Such attacks can occur at multiple communication layers, causing various repercussions, from message delays to system-wide failures. Common forms of DoS attacks include inundation, and blocking, which can lead to message delays and the inability to communicate with devices [52].

In summary, cyber-attacks represent a hidden threat by attacking hardware, software, or protocol of the smart grid layers (physical, communication, and cyber layers). Protective relays that system operators can remotely control are especially at risk of wireless network attacks, making them an enticing target for potential attackers.

4 | RESILIENCE EVALUATION OF ADAPTIVE PROTECTION SYSTEMS

As previously mentioned, power protection systems are vital to power network infrastructures which require secure and reliable operation. Within power networks, they hold the responsibility to detect and isolate faults and any abnormal

operating conditions. Because these systems rely on digital communication technology, vulnerabilities exist that cyber-attackers could capitalize on to compromise the functionality of the protection system and interrupt network operations. Such cyber-attacks on the OCR can lead to physical damage, operational disruptions, and power outages. To address these risks, implementing effective cybersecurity measures is a must for the power network operators to encompass both digital and physical security controls and to mitigate any potential threats. Therefore, we aim to assess the resilience of the DN with DER and modern adaptive OCR under different cyber–physical threats. We introduce a new approach to evaluate the resilience of the adaptive OCR performance at DN with DERs in terms of sensitivity and selectivity:

- Number of healthy line outages (energy not supplied).
- Total tripping time and mis coordination events at different fault and cyber threats scenarios.
- Furthermore, the impact of the cyber-attack on the clearing time for the circuit breaker and adaptive OCR are envaulted. This analysis provides valuable insights into the potential impact of the attack on the power system, particularly in terms of power grid quality.

4.1 | Proposed power network with adaptive protection scheme and cyber modelling

In order to introduce a comprehensive assessment for the resilience of a real power grid concerning power protection sensitivity, a systematic approach is essential to analyze the OCR protection components and interactions. In addition, a new approach for evaluating the resilience of smart grids particularly with regard to adaptive OCR protection sensitivity and selectivity is provided to improve the sustainability and resilience of future power and protection systems. To assess the resilience of power protection systems within the proposed real power grid, separate simulation tools are employed to model the cyber and physical (power) components of the system by using OMNeT and ETAP, respectively, as shown in Figure 4. The main aim is to provide a comprehensive understanding of the system's behaviour under different operation and cyber threats conditions, particularly by analyzing the events impacts from the cyber to the physical domain.

The work begins by developing and simulating the real power grid layer using the ETAP simulation tool, as illustrated in Figure 5. The power network configuration proposed in this study comprises two primary levels: the standard high voltage (HV) network and the real medium/low voltage (MV/LV) network levels.

- The proposed standard HV network is a standard 9-bus system with multiple power sources, including the utility grid and a PV unit. This grid is widely utilized in scientific literature to analyze power protection performance. The PV unit is connected to the system through a transformer, and the power network including adaptive OCRs. Detailed informa-

TABLE 5 The basic information of the photovoltaic farm.

Area	PV power (KWp)	# strings	Energy production (kWh/year)
P1	1011.84	32*6*17	1,880,504
P2	1011.84	32*6*17	1,880,504
P3	1011.84	32*6*17	1,880,504
P4	980.22	31*6*17	1,821,738
Total	4015.74		7,463,250

tion about the IEEE 9-bus system can be found in [2, 3]. The IEEE 9-bus (HV) network has been customized and adapted to supply the actual MV/LV system, as depicted in Figure 5.

- The actual MV/LV network: this research utilizes real power network data, specifications and measurements, specifically gathered for the purpose of designing the proposed power network. As shown in Figure 5, the network comprises a combination of traditional electricity sources, represented by two 33 KV (T19 and T20) lines from the local electricity company, and solar power sources and including 16 adaptive OCRS. The two 33 KV utility lines are fed from the HV network through a 132/33 KV transformers. The total connected solar power sources to the MV/LV network are 5 MWp, playing a substantial role in fulfilling the energy demands. As shown in Figure 5, the solar power sources are divided into two main groups:
- 1-The PV farm with total capacity of 4015 kWp and connected to the 33 KV bus through power transformers 12/33 KV (T15, T16, T17, and T18). The PV farm is included four main areas named P1 to P4, as shown in Figure 5 and detailed in Table 5.
- 2-The total capacity of 1016 kWp PVs has implemented as direct grid-connected project at the LV network level. The project creatively incorporates PV panels into walkways and car parks, providing both renewable energy generation and functional infrastructure. The grid-connected PV system is included nine areas named G1 to G9, as shown in Figure 5 and detailed in Table 6.
- The LV power network spans an extensive area of approximately 34475 km^2 including 36 buildings and covers an annual energy consumption of nearly 8.5 GWh. The LV network are fed by two main 33/11 KV transformers (T13 and T14), as shown in Figure 5. Then, twelve distribution transformers (T1 to T12: 11/0.415 KV) are used to supply the required power to the 37 buildings from B1 to B36. Table 7 describes the main information of the LV network and load demand.
- The simplified network configuration, as depicted in Figure 4, includes a total of 18 OCRs. The details of the current transformer ratio (CT), pickup current (I_P), and optimal TMS for each individual adaptive OCRs are conveniently provided in Tables 8 and 9. In the initial phases, a load flow analysis was conducted to ascertain the appropriate CT. Simultaneously, the derivation of short-circuit currents was executed in accordance with IEC-60909 guidelines, encompassing diverse fault types across different network sections under various
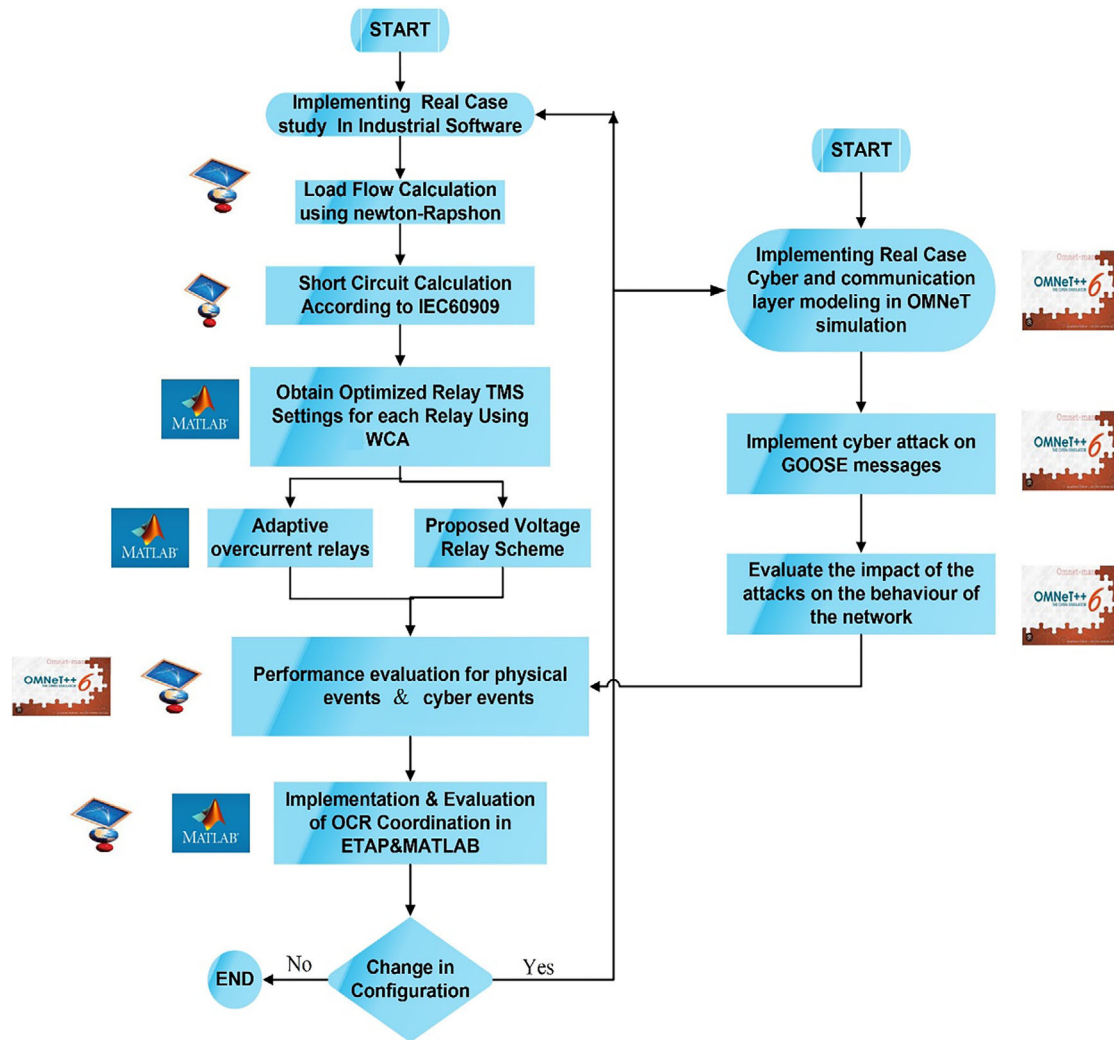
FIGURE 4 Simplified presentation of modelling the evaluation process of the proposed power network with optimal protection schemes under cyber-attacks scenarios using ETAP, Matlab, and OMNeT Simulations.

operational conditions. Furthermore, the short-circuit analysis was performed through the utilization of the ETAP software, leveraging available data to facilitate a comprehensive assessment.

4.1.1 | Cyber and communication layer modelling

In the proposed power network, the operator commands were initially sent through the SCADA WAN network to the station and then routed through an Ethernet switch. Within the substation, gateway devices like remote terminal units (RTUs) and routers are employed to collect and transmit internal data from the adaptive OCRs to the circuit breakers (CB) via the local area network (LAN). These processes ensure efficient monitoring and control of the substation. However, cyber-attack risks pose threats to the power system infrastructure and users, emphasizing the importance of strong cybersecurity measures. Therefore, in this research, the impact of cyber-attacks, including data

insertion, blocking, and manipulation, on the IEC 61850-based GOOSE protocol is evaluated. The GOOSE protocol, known for its efficiency and reliability, was initially designed for LAN-based power substations. However, the second version of this standard introduced routable GOOSE (R-GOOSE), making it applicable to WAN applications and distribution power grids. The proposed smart power network incorporates controllers (CBs), adaptive protection relays (OCRs), and a central control, all susceptible to hacking. To simulate the cyber-attack scenario, OMNeT simulation was utilized, and Figures 6 and 7 present the system setup captured from OMNeT simulation. for the HV side of the power network and part of the distribution power network.

To simulate the cyber-attack scenario, OMNeT simulation was utilized, and Figure 8 showcases a scenario involving delaying the signal between the adaptive OCR and circuit breaker during fault event. The average message delay in this example was 1 s as shown in Figure 9. This attack example outlines by using algorithm presented in Table 10. This algorithm describes
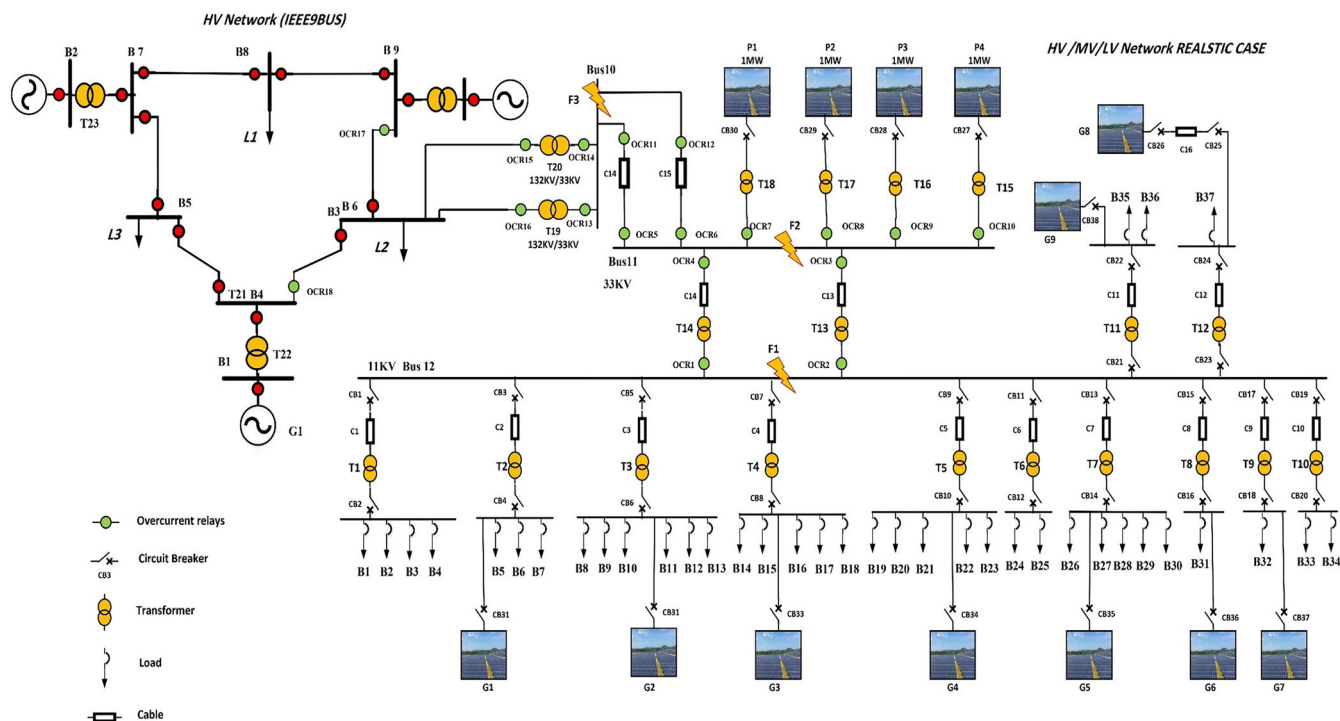
FIGURE 5 The proposed power networks (physical and communication layers).

TABLE 6 The basic information of the grid-connected photovoltaic system.

Area	# PV modules	PV power (KWp)	Energy production (kWh/year)
G1	72	22.320	36.873
G2	72	22.320	36.873
G3	72	22.320	36.873
G4	72	22.320	36.873
G5	76	23.560	41.324
G6	44	13.640	23.925
G7	74	22.940	38.310
G8	76	23.560	39.345
G9	72	22.320	41.939
Total	3279	1.016.490	1.711.161

the process for conducting network attacks using address resolution protocol (ARP) spoofing. In general, ARP is used to map IP addresses to MAC addresses in a local network. By spoofing ARP, the attacker tricks network devices into sending their traffic to the attacker's machine instead of the intended destination. This allows the attacker to intercept and monitor the network traffic. Once the ARP spoofing is in place, the attacker can monitor the network traffic passing through their machine. This could include analyzing data packets, looking for sensitive information, or identifying potential targets. If the attack type is selected as a "Drop Attack," the attacker intends to drop the intercepted message without forwarding it to the destina-

tion. This effectively prevents the target relay from receiving the message. On another scenario, if the attack type is identified as a "Delay Attack," the attacker introduces a delay time, during which the execution is paused for the specified duration. This delay simulates the attack's delay effect.

4.2 │ Cyber-attack tree and evaluation process

The main objective of creating the cyber-attack tree is to improve the abstraction level of the evaluation process by categorizing cyber-attacks according to their similar impacts. The attack tree, depicted in Figure 10, is developed to introduce the resilience evaluation process of the power grid and adaptive OCR protection. The developing of the cyber-attack tree follows a systematic and standard top-down methodology that includes the following key steps:

1. Cyber-attack objectives: The attacker's objective is defined, with the main goal being to induce disturb power system stability through causing power protection function failure, which results in system instability and the violation of critical grid operation standards. The focus is on deliberately disrupting the intended operation of the adaptive OCR. Specifically, two significant violations are targeted: inaccurately operating the OCRs and disturbing the reverse blocking ability for the OCRs.
2. Power physical consequences: This stage aims to identify and assess the physical impacts resulting from cyber-attacks that lead to function failure in power systems (cyber-attack objectives). The cyber-attacks can have various consequences

TABLE 7 The basic information of the load demand.

Transformer	Building	CB-rating	Transformer	Building	CB-rating
T1	B1	1250	T5	B19	400
	B2	600		B20	400
	B3	125		B21	125
	B4	125		B22	250
T2	B5	1250		B23	250
	B6	400	T6	B24	2500
	B7	60		B25	2500
T3	B8	150	T7	B26	400
	B9	200		B27	1250
	B10	125		B28	250
	B11	400		B29	400
	B12	200		B30	250
	B13	400	T8	B31	800
T4	B14	250	T9	B32	3200
	B15	400	T10	B33	2000
	B16	250		B34	2500
	B17	160	T11	B35	2500
	B18	400		B36	2500
			T12	B37	3200

TABLE 8 The current transformer ratio and pickup current (I_P) for overcurrent relays (OCRs).

OCR	CT	I_P	OCR	CT	I_P
OCR1	300/1	270	OCR10	50/1	18
OCR2	300/1	270	OCR11	100/1	50
OCR3	100/1	90	OCR12	100/1	50
OCR4	100/1	90	OCR13	200/1	100
OCR5	100/1	50	OCR14	200/1	100
OCR6	100/1	50	OCR15	50/1	25
OCR7	50/1	18	OCR16	50/1	25
OCR8	50/1	18	OCR17	300/1	120
OCR9	50/1	18	OCR18	300/1	120

TABLE 9 The optimal Scientific Research and Innovation Support Fund TMS for each individual adaptive overcurrent relays (OCRs) at group setting A and B.

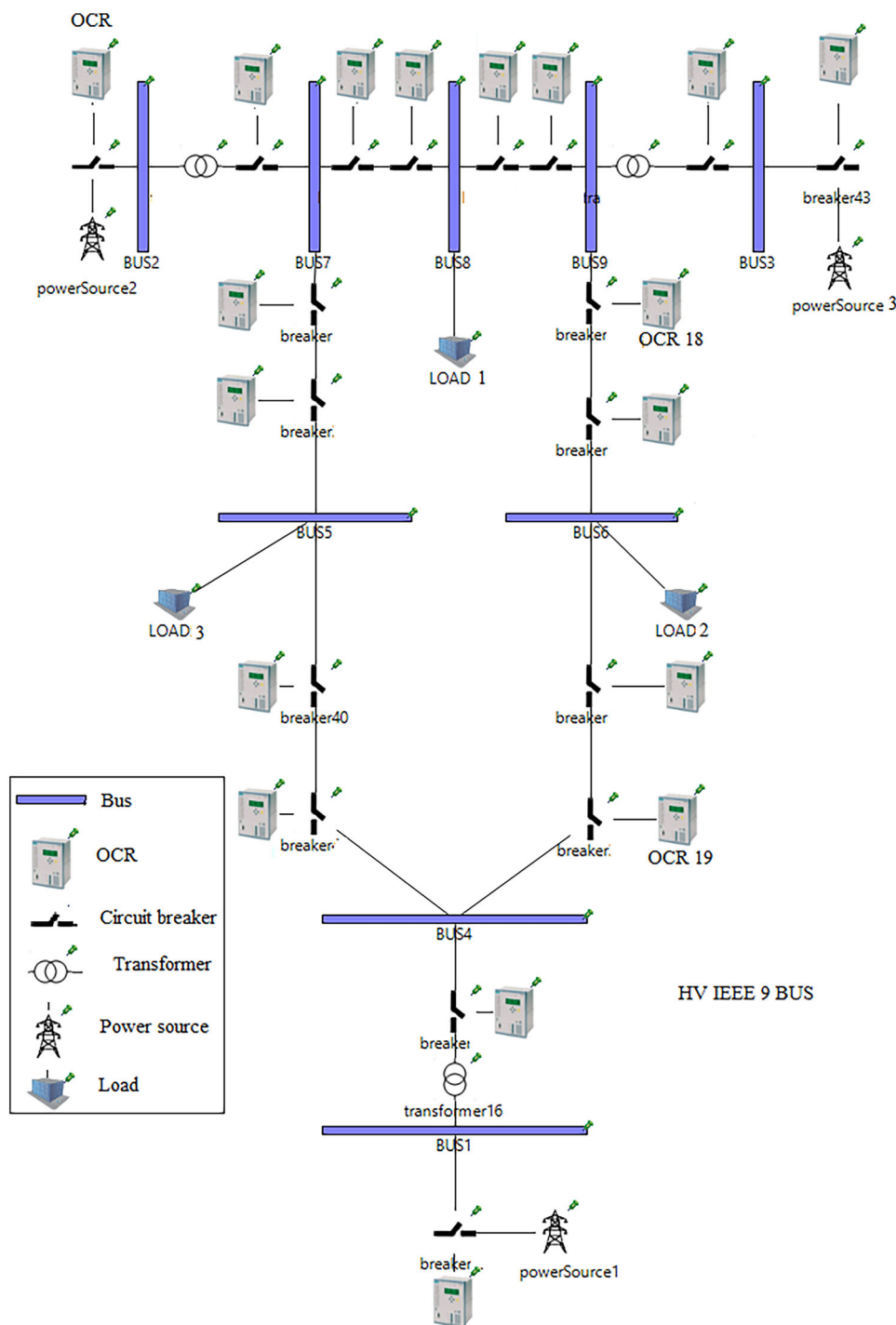| OCR	Group setting A TMS	Group setting B TMS
OCR1	0.01	0.01
OCR2	0.01	0.01
OCR3	0.102	0.103
OCR4	0.102	0.103
OCR5	0.25	0.249
OCR6	0.25	0.249
OCR7	0.01	0.029
OCR8	0.01	0.029
OCR9	0.01	0.029
OCR10	0.01	0.029
COR11	0.25	0.249
OCR12	0.25	0.249
OCR13	0.325	0.33
OCR14	0.325	0.33
OCR15	0.358	0347
OCR16	0.358	0.347
OCR17	0.09	0.097
OCR18	0.18	0.182

within the system, primarily leading to the loss of power sources, power outages, network damages and a reduction in power quality. For example, the operation of the CB depends on the communication network transmitting commands from the adaptive OCR to the CB. Blocking these commands within the communication network can prevent the CB from operating safely during power faults and normal operation scenarios, representing the desired physical factor for manipulation. This demonstrates how the attack extends from the virtual domain to the actual physical domain.

3. Cyber-attack category: The cyber-attacks that have the potential to cause physical impacts on power grid and
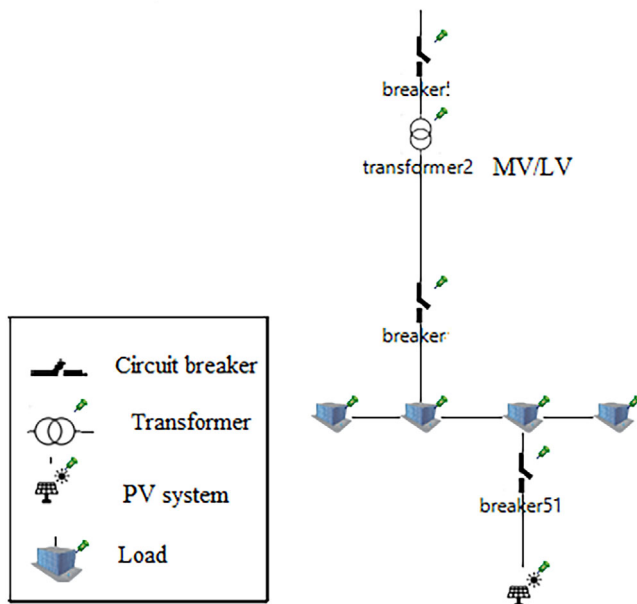
FIGURE 6 Captured of the OMNeT simulation for the proposed HV power network (IEEE 9 BUS).

adaptive OCRs are identified, as shown in Figure 10. By focusing on these specific cyber-attacks, this work aims to gain a deeper understanding of their potential consequences on the physical components of power systems. In the attack tree (Figure 10), the specific actions undertaken by the attacker to carry out the attack are outlined, describing the implementation process. In this work, the cyber-attacks include: block order to CB, drop command massages, change

adaptive OCR setting, block adaptive OCRs communication link, and send fake measurements to the adaptive OCR.

4. Cyber-attack techniques: The main focus of this stage is to identify the cyber-attack techniques that can potentially lead to cyber-attacks, as described in stage 3. For example, to disrupt the CB, an attacker might need to compromise the OCR, launch a DoS attack, or execute a MITM assault.

FIGURE 7 Captured of the OMNeT simulation for a part of the proposed real LV power network (IEEE 9 BUS).

TABLE 10 Algorithm process for the delay message attack.

Algorithm (1) for the delay message attack
1. while True do
2.   Spoof ARP to intercept traffic
3.   Monitor network traffic
4.   Check Intercepted Messages
5.   if Destination = target Relay then
6.   if Attack Type = Drop Attack then
7.   Do Nothing
8.   else if Attack Type = Delay Attack then
9.   sleep(delay time)
10.   send delayed Message(Message)
11.   end if
12.   else
13.   send Message(Message)
14.   end if
15. end while

During power faults, such as three-phase failures or abnormal overloads, it is very important that adaptive OCRs and CBs work timely and correctly in a power system. During normal grid operation, it is important for both CBs and adaptive OCRs to avoid unnecessary actions to keep the system stable and avoid outages. Evaluating the resilience of a power grid and its protection systems involves assessing their ability to meet standard power grid operation conditions, as specified by IEEE Std 3002.−2018, which may include voltage levels within 95–105% of the rated voltage. This work aims to focus on finding out how effectively the power grid can handle cyber-attacks by exam-ining aspects such as energy not supplied, total tripping time, OCR miss-coordination events, power availability, and the risk of grid infrastructure damages in the presence of cyber-attacks. This analysis is essential for enhancing the overall cybersecurity of the power grid and developing effective adaptive OCR schemes against potential threats.

5 | RESULT AND DISCUSSION

The proposed modern OCR protection schemes (adaptive OCR scheme and voltage-based relays), as presented in Section 2, for HV/MV/LV network model is developed with a real network parameter and measurands and evaluated under different cyber-attacks and physical fault scenarios. This section aims to present and discuss the results from the modern OCR protection schemes. Firstly, the performance of the adaptive OCR scheme is evaluated without cyber-attacks; then, the impact of four different cyber-attacks on the performance of the adaptive OCR scheme is shown. Secondly, the voltage-based relays result is presented for the proposed power network and under different fault scenarios and without cyber-attacks. Throughout this section, the voltage-based relays are compared to adaptive OCR scheme in term of tripping time, grid stability and energy not supplied.

5.1 | Adaptive OCRs results under normal operation conditions

To evaluate the performance of the adaptive OCRs approach, particularly its ability to minimize tripping time while maintaining appropriate CTI under different cyber-attack scenarios, the tripping time of OCR as presented for the normal operation conditions (before cyber-attack) in Tables 11 and 12. This table offers insights into the tripping times of all OCR under three different three phase fault location (F1, F2, and F3), shown in Figure 5, encompassing both primary and backup OCRs. Table 11 displays the tripping times of OCRs over fault scenarios (F1–F3) within a conventional power network configuration without PV (utilizing group setting A). For example, in F1, where the fault current is 2235 A, OCRs 1 and 2 with a PSM of 8.27 exhibit a tripping time of 0.032 seconds. OCRs 3 and 4, also with a PSM of 8.27, respond slower (as first backup relays) with a tripping time of 0.33 s. Similarly, OCRs 11 and 12, with a higher PSM of 14.9 as second backup relays, exhibit a relatively extended tripping time of 0.63 s. Here, the first and second backup OCRs maintain the CTI condition by considering CTI equal to 0.2–0.3 s.

Furthermore, Table 12 outlines the results obtained for group setting B, where the power grid is connected to PV sources. For example, examining F1, characterized by a fault current of 2267 A, OCRs 1 and 2 both had a PSM of 8.39, resulting in an impressively rapid tripping time of 0.032 s. The same PSM and tripping time with delay of 0.3 s are observed for OCRs 3 and 4, which correspond to a fault current of 756 A. Similarly, OCRs 11 and 12, with a PSM of 14.66, exhibit a tripping time of 0.63 s for
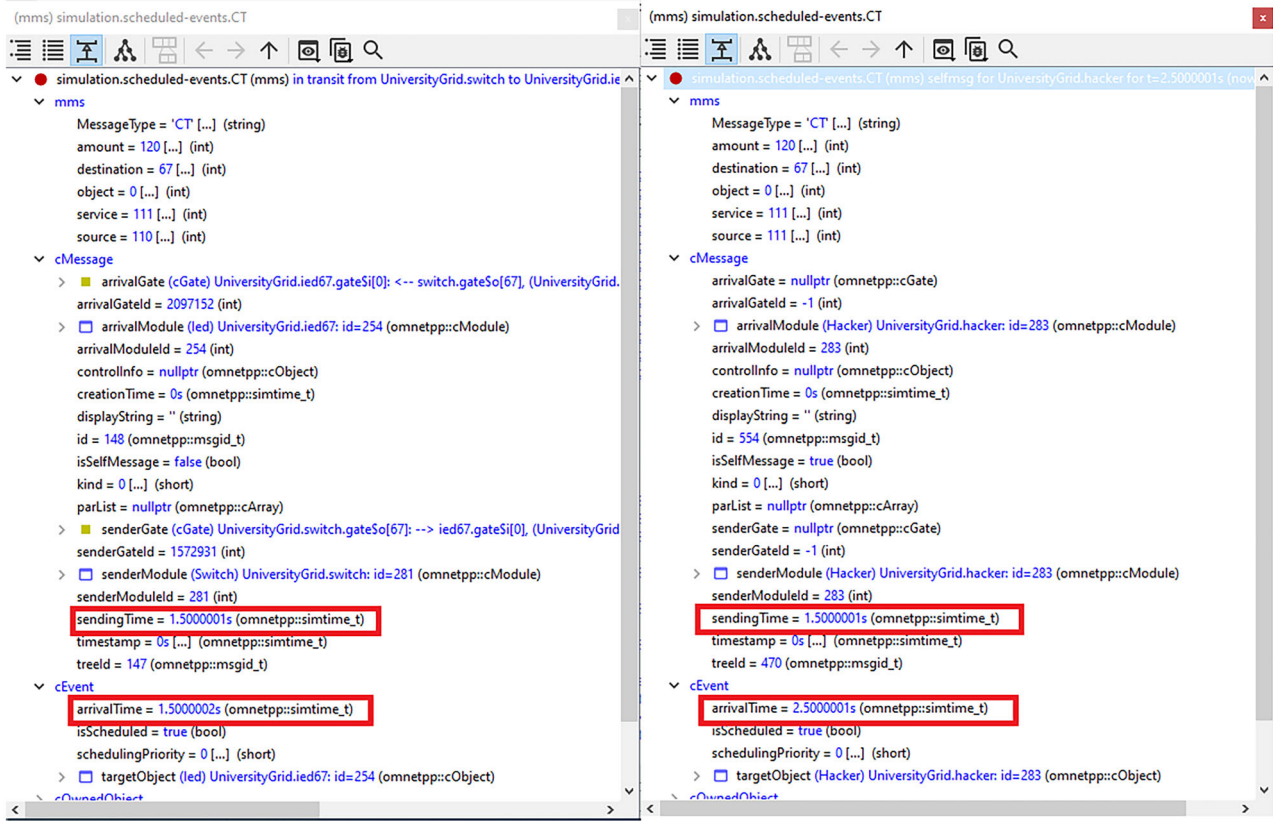
FIGURE 8 Captured of a cyber-attack scenario (delay the signal between the adaptive OCR and circuit breaker) in OMNeT simulation.
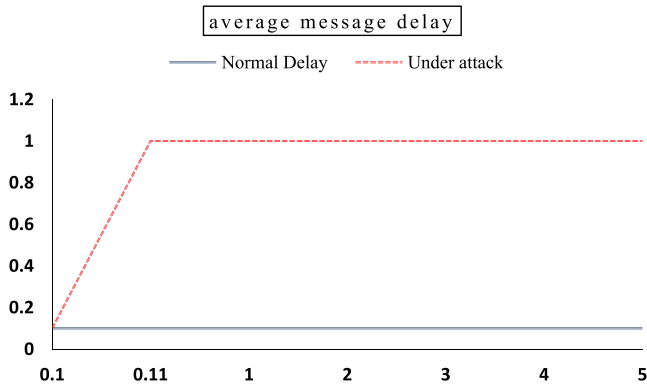

FIGURE 9 The average message delay for signal between the adaptive overcurrent relay (OCR) and circuit breaker in OMNeT simulation.

a fault current of 733 A. Meanwhile, OCRs 7, 8, 9, and 10, all with a PSM of 1.38, showcase tripping times of 0.61 s, although in response to a considerably lower fault current of 25 A.

5.2 | Adaptive OCRs performance under different cyber-attack scenarios

The cyber-attack tree, as depicted in Figure 10, categorize the cyber-attacks based on their impacts and the evaluation process. This attack tree is a vital tool for assessing the resilience of the power grid and adaptive OCR protection. In this section

TABLE 11 The tripping times of overcurrent relays(OCRs) over fault scenarios (F1–F3) within a power network without PV (group setting A).

Fault location	Fault current	OCR	PSM	Tripping time
F1	2235	OCR1	8.27	0.032
	2235	OCR2	8.27	0.032
	745	OCR3	8.27	0.33
	745	OCR4	8.27	0.33
	745	OCR11	14.9	0.63
	745	OCR12	14.9	0.63
F2	1682	OCR11	33.64	0.48
	1682	OCR12	33.64	0.48
	1682	OCR13	16.82	0.78
	1682	OCR14	16.82	0.78
	241	OCR15	9.64	1.08
	241	OCR16	9.64	1.08
F3	255	OCR15	10.2	1.05
	255	OCR16	10.2	1.05
	200	OCR17	1.66	1.22
	310	OCR18	2.583	1.31

four main cyber-attack scenarios are simulated to evaluate the adaptive protection performance:

- Attack-1: In this scenario, the attacker's targeted the operational setting of the adaptive OCRs. The attacker's does not
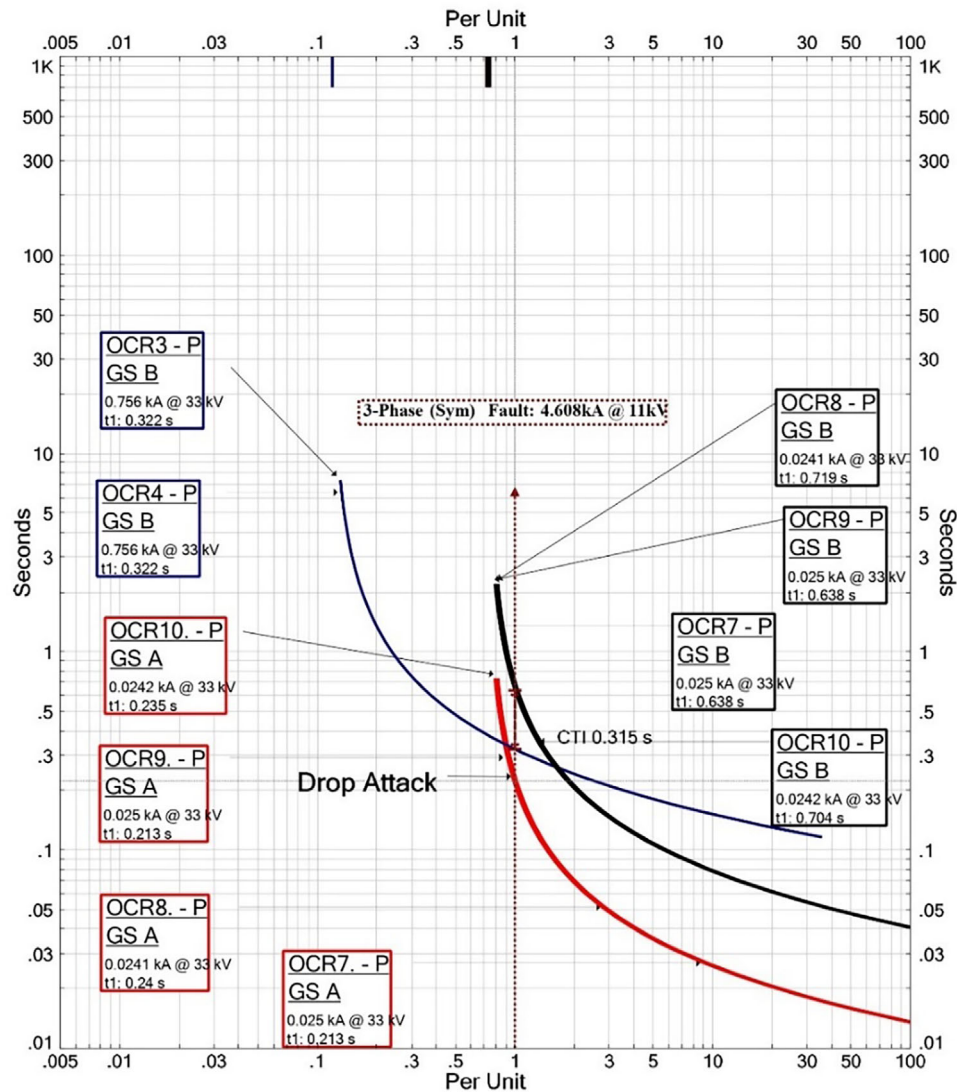
FIGURE 10 Cyber-attack tree for modern OCR protection schemes.

TABLE 12 The tripping times of overcurrent relay (OCRs) over fault scenarios (F1–F3) within a power network with PV (group setting B).

Fault location	Fault current	OCR	PSM	Tripping time
F1	2267	OCR1	8.39	0.032
	2267	OCR2	8.39	0.032
	756	OCR3	8.4	0.33
	756	OCR4	8.4	0.33
	733	OCR11	14.66	0.63
	733	OCR12	14.66	0.63
	25	OCR7	1.38	0.61
	25	OCR8	1.38	0.61
	25	OCR9	1.38	0.61
	25	OCR10	1.38	0.61
F2	1682	OCR11	33.64	0.47
	1682	OCR12	33.64	0.47
	1778	OCR13	17.78	0.77
	1778	OCR14	17.78	0.77
	225	OCR15	9	1.08
	225	OCR16	9	1.08
F3	255	OCR15	10.2	1.02
	255	OCR16	10.2	1.02
	200	OCR17	1.66	1.32
	310	OCR18	2.58	1.32

allow to adaptive OCRs to change the group setting from A to B and active the group setting B at OCRs when the topology of the grid change to grid connected with PV by generating a drop attack that aim to block the OCR from changing the group setting. Figure 11 shows the coordination of OCRs between the primary relays ORC3 and OCR4 (blue line) and backup relays OCR7, OCR 8, OCR9, and OCR 10 (black line) when a fault occurs at location F1. Here, during normal operation before any attack, when the OCR activates group setting B, both the primary and backup relays function with a CTI of 0.315 s. However, in the case of attack-1, the backup relays OCR7, OCR8, OCR9, and OCR10 adopt group setting A (as indicated by the red line). This unintended configuration leads to a mis-coordination event, where the backup relays initiate their operation prior to the primary relays. Consequently, the PV systems connected at the medium voltage level experience incorrect disconnection. This occurrence results in a loss of PV power generation.

- Attack-2: in this scenario, the attacker's objective is to disturb and block the reverse blocking functionality of the OCRs. The attacker intentionally interferes with the transmission of reverse blocking signals from the primary OCRs to the secondary OCRs. These reverse blocking signals are crucial, as they communicate to the secondary OCRs that the primary relays have already taken corrective actions to isolate the fault. Consequently, the activation of the backup relays becomes unnecessary. The primary intention behind this protection

FIGURE 11   Adaptive OCRs coordination performance under normal and attack-1 condition across F1.

link is to enhance the sensitivity and selectivity of the protection system. However, in this attack scenario, the attacker executes a strategy where the communication signal between the primary and backup relays is deliberately dropped. This disruption causes the backup protection to activate, leading to the disconnection of a wide area and resulting in the loss of power generation from the PV systems. Figure 12 illustrates the coordination between the primary relays OCR11 and OCR12 (depicted by the blue line) and the backup relays OCR13 and OCR14 (indicated by the red line) in response to a fault occurring at location F2 in the absence of PV systems. In the normal operational scenario, both the primary and backup relays actuate within a CTI timeframe of 0.3 s. However, in the context of attack-2, a disruption occurs and the backup relays OCR13 and OCR14 initiate their operations without considering the status of the primary relays. This attack configuration results in a coordination anomaly where the backup relays commence their actions prior to

the activation of the primary relays. This mis-coordination event subsequently leads to an increase in the unmet energy demand. To show the impact of this type of attack, Figure 13 shows the coordination scheme between the OCR at MV and HV side. The primary relays ORC15 and OCR16 (blue line) and backup relays OCR17 and OCR 18 (red line) when a fault occurs at location F3. Here, during normal operation before any attack, both the primary and backup relays function with a CTI of 0.3 s. However, in the case of attack-2, the backup relays OCR17 and OCR18 at the HV side of the network will operate and cause a high level of energy not supplied based on this mis-coordination event.

Figure 13 illustrates the occurrence of mis-coordination between the OCRs at the MV and HV sides, resulting from a fault and subsequent attack at the MV Overcurrent Relay level. This situation leads to the disconnection of bus 6 and the load (L2), which corresponds to approximately 92 MW, as depicted
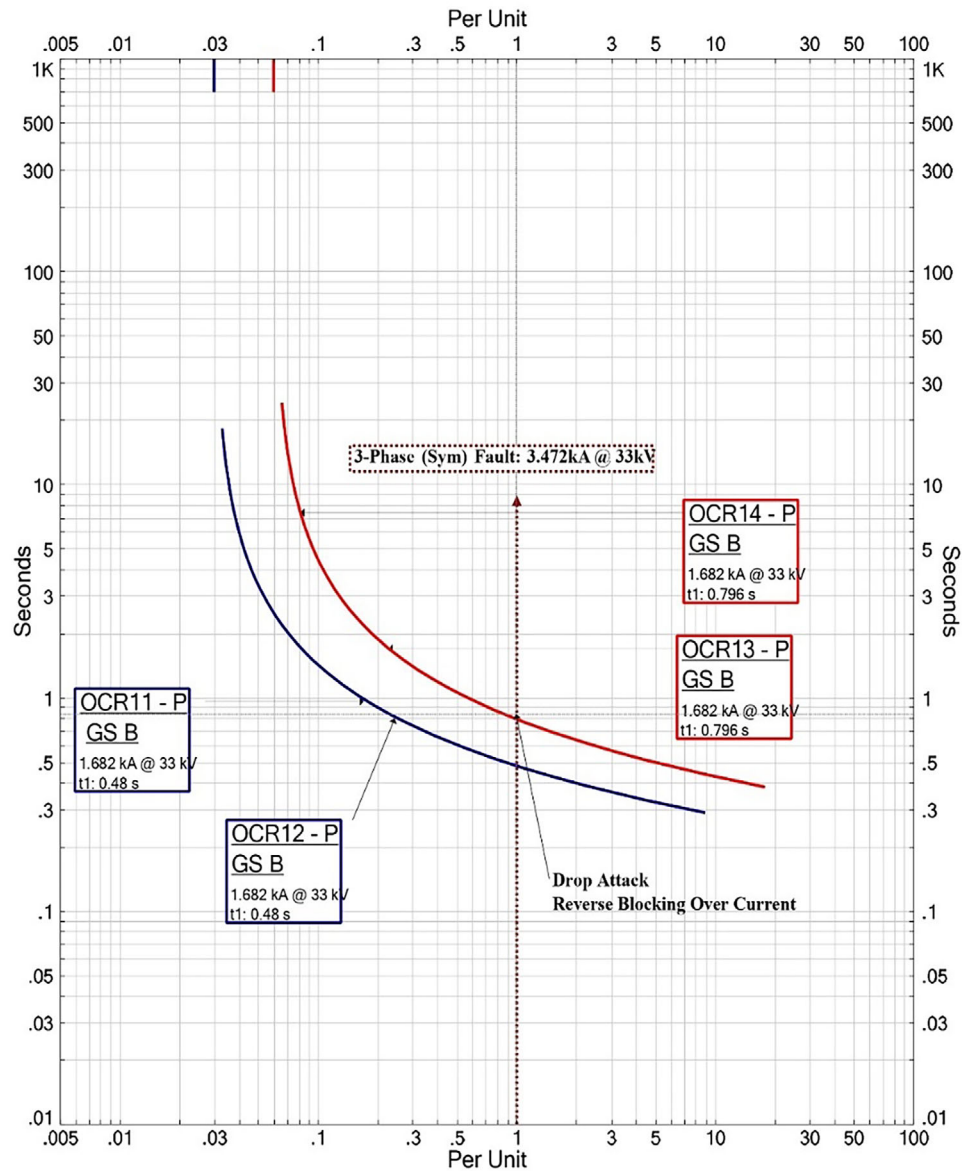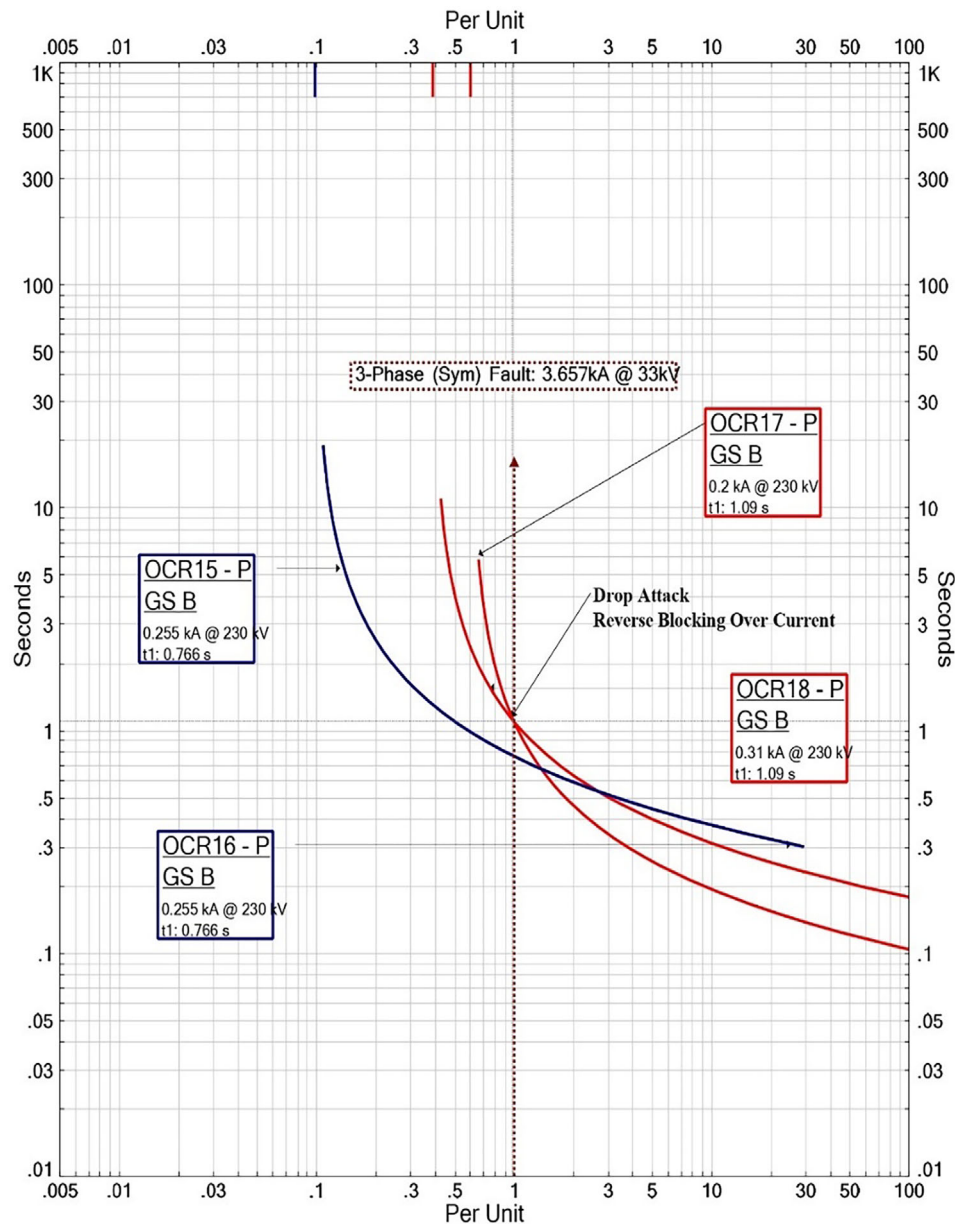
FIGURE 12 Adaptive overcurrent relays (OCRs) coordination performance under normal and attack-2 condition across F2.

in Figure 5. As a consequence, a significant degree of instability emerges within the grid, notably affecting voltage and frequency levels and lead to blackouts. Therefore, to show the impact of this attack and presenting the simulation results, OCR 17 assumed to be only targeted. Figure 14 showed the generator power angle and voltages results of the HV network (9 bus system) during normal operation. The instability is further highlighted in Figures 15 and 16, which demonstrates the fluctuating the generator power angle and voltages across the HV network, respectively. The power angle of generators (Gen 1, Gen 2, and Gen 3) experiences a significant and continues increasing for more 300°. Moreover, the voltage level undergoes a decrease of bus voltages under 95% Bus2, Bus 3, Bus 5, and Bus 9 across the HV network buses. As a consequence of these instability readings within the grid, the system faced a blackout condition.

- Attack-3: in the third scenario involving a DoS attack, the attacker blocks the relays' ability to respond and send suitable orders for a certain timeframe. To clarify, this particular form of attack is executed by introducing an intentional delay, rather than immediately transmitting a command, in the trip signal sent to the circuit breaker upon the occurrence of a failure. In attack-3, the attacker intentionally disturbs the primary OCRs by delay the tripping signal. Figure 17 shows that the primary relays ORC3 and OCR4 for F1 are converted to be act as backup due to the delay in tripping time and OCR 11 and OCR 12 will operate before it. This is will cause a mis-coronation event and a high level of energy not supplied.
- Attack-4: in this scenario involving a cyber-attack execution on sampled values (SV) attack on current measurements. This will lead to change the pickup current at the relay and

FIGURE 13   Adaptive overcurrent relays (OCRs) coordination performance under normal and attack-2 condition across F3.

the tripping time. To clarify, the parallel OCRs (ORC11 and OCR12) are supposed to take action on the same time during the fault condition. However, the attack-4 at OCR11 will lead to change the pickup current and tripping time compare to OCR12, as shown in Figure 18. This is will cause mis-coordination event and continue feeding the fault through OCR11 and cause thermal damages to the power network.

5.3 | Voltage-based relay results under normal operation conditions

In order to assess the efficacy of the voltage-based relay strategy, particularly its capability to minimize tripping time while upholding suitable CTI under varying cyber-attack scenarios, the tripping times of the relays are evaluated under normal operating conditions (pre cyber-attack) and presented in Tables 13 and 14. Firstly, Tables 13 conveniently provides the optimal TMS for each individual relay. Meanwhile, Table 14 presents an overview of the tripping times for all relays encompassing both primary and backup relays across three distinct three-phase fault locations (F1, F2, and F3), depicted in Figure 4. These results are obtained when the power grid is connected to photovoltaic (PV) sources. For instance, examining the case of F1, characterized by a fault voltage of 0.1 p.u, VRs 1 and 2 exhibit an impressive rapid tripping time of 0.0001 s. Moving to VRs 3 and 4, corresponding to a fault voltage of 0.62 A, the tripping time stands at 0.299 s. Similarly, VRs 11 and 12 demonstrate a

(a) Generator power angle
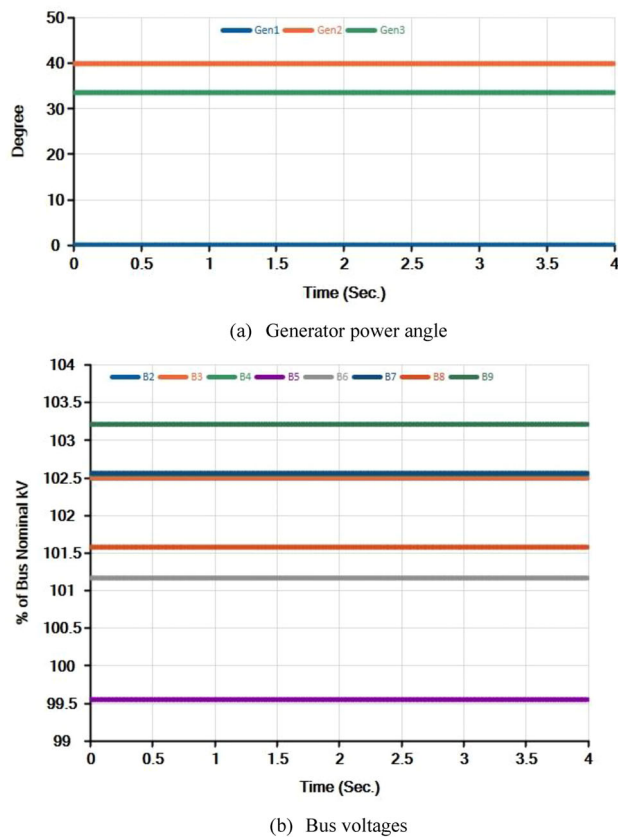
(b) Bus voltages

FIGURE 14 Generator power angle and voltages of the HV network (9 bus system) during normal operation. (a) Generator power angle, (b) bus voltages.

TABLE 13 The optimal TMS values for the voltage-based relays within the proposed power network with PV.

Voltage-based relay	Setting TMS
VR1	0.01
VR2	0.01
VR3	1.47
VR4	1.47
VR5	2.8
VR6	2.8
VR7	2.9
VR8	2.9
VR9	2.9
VR10	2.9
VR11	2.8
VR12	2.8
VR13	2.8
VR14	2.8
VR15	1.2
VR16	1.2
VR17	2.77
VR18	2.77

TABLE 14 The tripping times of voltage-based relays over fault scenarios (F1–F3).

Fault location	Fault voltage in per unit	Relay	Tripping time
F1	0.1	VR1	0.0001
	0.1	VR2	0.0001
	0.62	VR3	0.299
	0.62	VR4	0.299
	0.66	VR11	0.597
	0.66	VR12	0.597
	0.62	VR7	0.591
	0.62	VR8	0.591
	0.62	VR9	0.591
	0.62	VR10	0.591
F2	0.084	VR11	0.042
	0.084	VR12	0.042
	0.084	VR13	0.042
	0.084	VR14	0.042
	0.855	VR15	0.293
	0.855	VR16	0.293
F3	0.84	VR15	0.291
	0.84	VR16	0.291
	0.95	VR17	0.692
	0.95	VR18	0.692

tripping time of 0.597 s for a fault voltage of 0.66 p.u. Meanwhile, VRs 7, 8, 9, and 10 showcase tripping times of 0.591 s in the same context.

Figures 19–21 illustrate the coordination between the primary and backup voltage-based relays in response to a fault occurring at location F1, F2, and F3, respectively. The coordination for both the primary and backup relays successfully maintains the CTI timeframe within 0.2–0.4 s. For example, the primary relays VR15 and VR16 (blue line) recorded a tripping time equal to 0.29 s and backup relays VR17 and VR 18 (black line) recorded tripping time equal to 0.692 s when a fault occurred at location F3, as show in Figure 19. In Figure 20, the primary relays VR13 and VR14 (blue line) recorded a tripping time equal to 0.042 s and backup relays VR15 and VR 16 (black line) recorded tripping time equal to 0.293 s when a fault occurs at location F2.

5.4 | Voltage-based relay performance under different cyber-attack scenarios compare to adaptive OCRs

In this section four main cyber-attack scenarios are simulated to evaluate the voltage-based relay compare adaptive protection performance as described in Section 5.2 in terms of tripping time, mis coordination events and energy generation loss. Table 15 shows the tripping times of both adaptive OCRs and
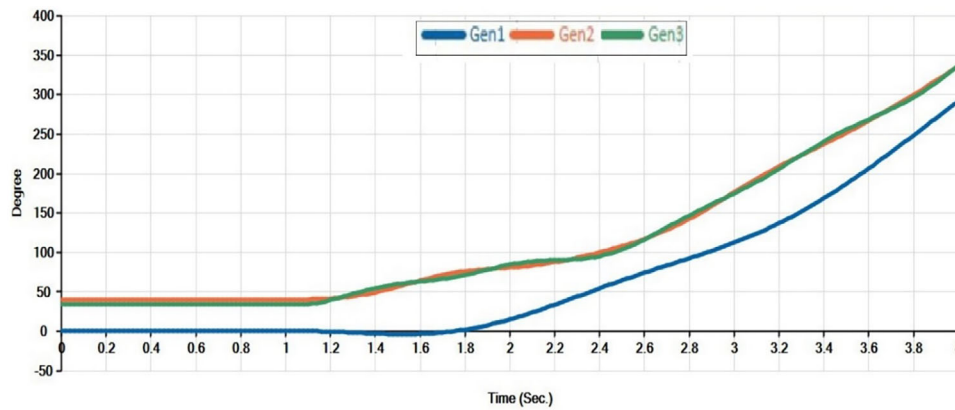
FIGURE 15 Generator power angle at the HV network during attack 2 operation (OCR17).
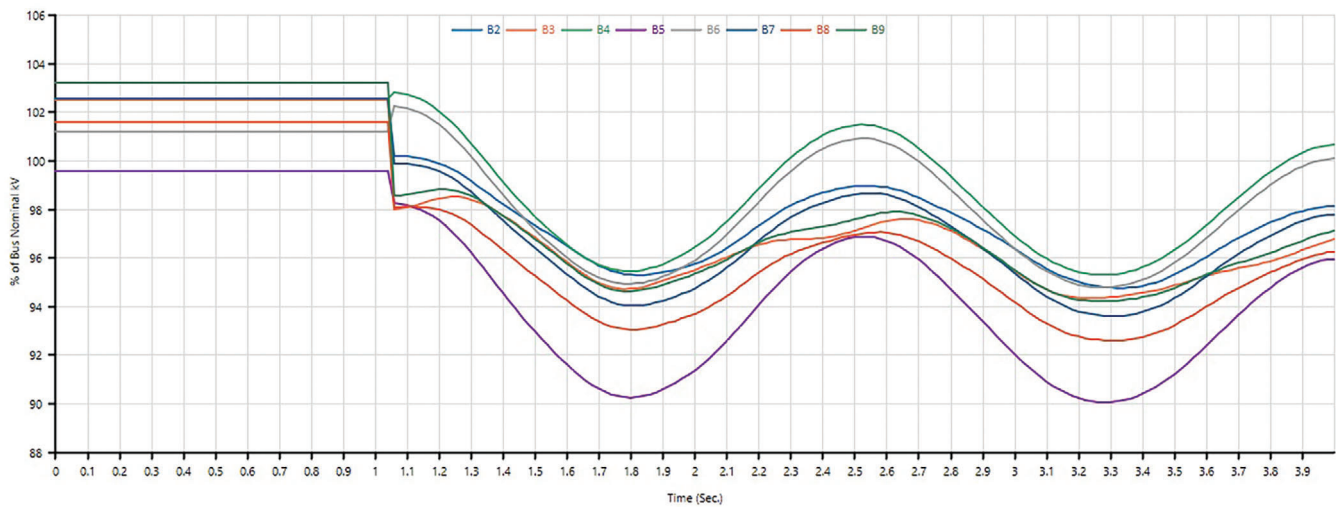
FIGURE 16 Bus voltages at the HV network during attack 2 operation (OCR17).

voltage-based relays in response to cyber-attack events (attack 1–4) across various fault scenarios (F1, F2, and F3). The results in Table 15 provides valuable insights into the performance of these protection mechanisms under different cyber-attack and fault conditions, as following:

- Firstly, OCR3 and OCR4 have tripping times of 0.33 s during F1 and attack 1, while the voltage-based relays (VR3 and VR4) respond remarkably faster with tripping times of approximately 0.2999 s. In addition, adaptive protection relays OCRs 7–10 reordered a miss-coordination event during attack 1 by recording 0.21 s lower than the primary relays (OCR3 and OCR4). The voltage-based relay successfully avoids the miss-coordination event during attack 1 and the backup relays VR7–VR10 operated after 0.3 s from the primary relays. In addition, for attack 3 during F1, OCR3 and OCR3 with tripping times of 0.63 s. In comparison, voltage-based relays VR3 and VR4 respond with tripping times around 0.299 s. OCR11 and OCR12 as backup relays have tripping times of 1.11 s, whereas

VR11 and VR12 respond with tripping times of around 0.0.597 s.
- Secondly, OCR11 and OCR12 during F2 and attack 2 have tripping times of 0.48 s. In contrast, voltage-based relays (VR11 and VR12) respond instantaneously, with tripping times as low as 0.0426 s. Similarly, attack 4 in F2 shows a significant difference in response times. OCR11 and OCR12 have different tripping times of 0.55 and 1.2 s, respectively, which lead to miss-coordination event. Whereas VR11 and VR12 respond almost instantly with tripping times of 0.0426 s.
- Thirdly, for attack 2 during F3, OCR15 and OCR16 with tripping times of 0.76 s. In comparison, voltage-based relays VR15 and VR16 respond with tripping times around 0.2911 s. OCR17 and OCR18 as backup relays have tripping times of 1.09 s, whereas VR17 and VR18 respond with tripping times of around 0.6929 s.

In summary, when responding to either physical fault events or cyber-attacks, voltage-based relays consistently demonstrate
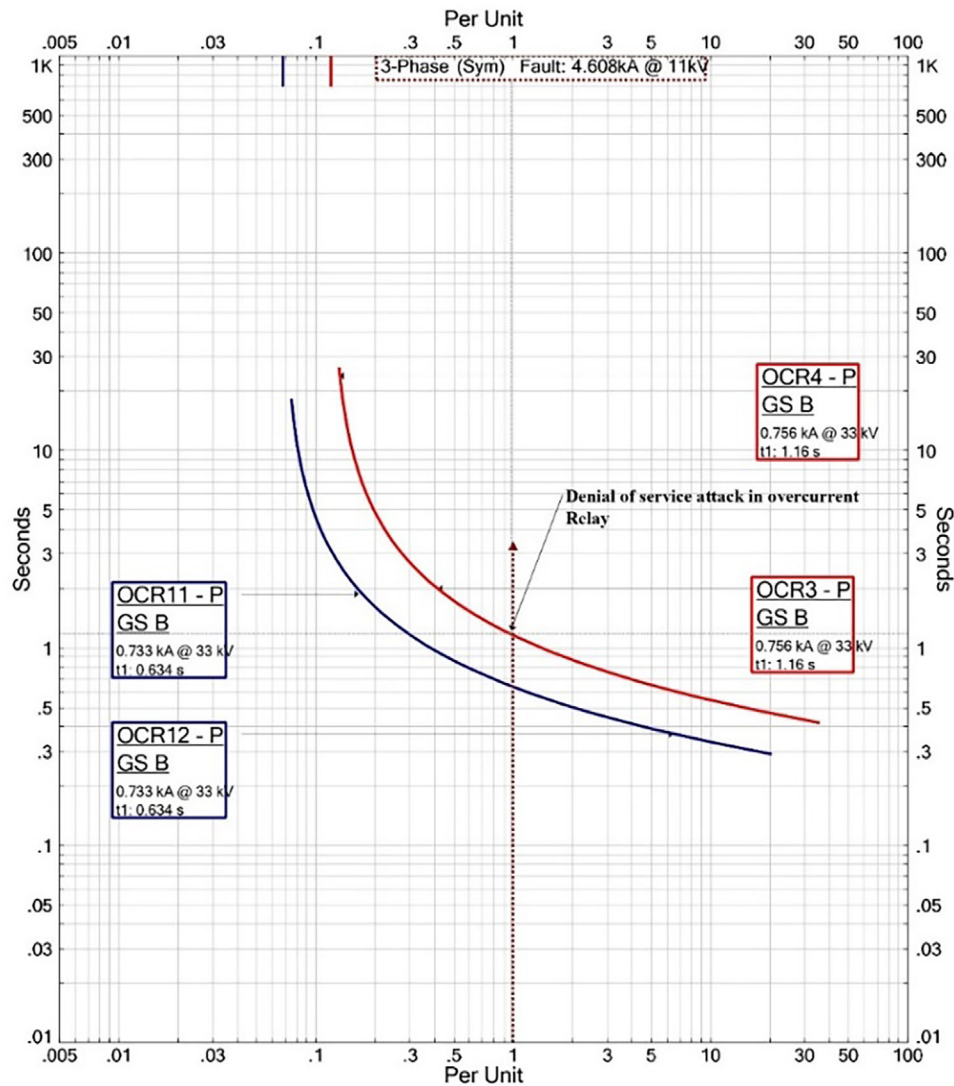
FIGURE 17   Adaptive OCRs coordination performance under normal and attack-3 condition across F1.

swifter reaction times than adaptive OCRs across all scenarios, and without any miss-coordination events. This indicates that, in situations with diverse fault locations and attack events, voltage-based relays may offer a more efficient protection, thus minimizing the chances of power system instability or outages. In addition, the miss-coordination events caused loss of the renewable generation units (PV) at the MV level. Table 16 shows the energy not supplied from PVs due to the miss-coordination event at adaptive OCR during attack 1 and F1 scenario. In case of 89% availability, the 4 MW PV system generates 3568 kW of power electricity, making it a reliable energy source. However, during a 1-h interruption due to attack 1 and miss-coordination event during F1, the entire 3568 kWh of energy could not be supplied, resulting in a loss of $1248 in benefits, based on the $0.35 per kWh energy rate. This emphasizes the importance of uninterrupted renewable energy generation and the financial consequences of even little disruptions, urging greater reliability mechanisms to protect these vital contributions to the energy system.

6 | CONCLUSION

The integration of DERs and communication systems into modern power grids offers high capabilities but also increases challenges of having robust power system protection. Researchers have diligently worked on developing adaptive protection; however, communication failures and the threat of cyber-attacks are highlighted as major concerns for using this approach. This research has addressed the modern power protection difficulties and investigated the impacts of cyber-attacks on modern OCR protection schemes (adaptive OCR scheme and voltage-based relays). Various physical faults and cyber-attacks were utilized in the proposed HV/MV/LV network model during the evaluation process. The power network model was developed based on actual network parameters at the MV/LV level.

In this work, the performance of voltage-based and adaptive OCR protection systems was compared under the impact of four different types of cyber-attacks by investigating the tripping
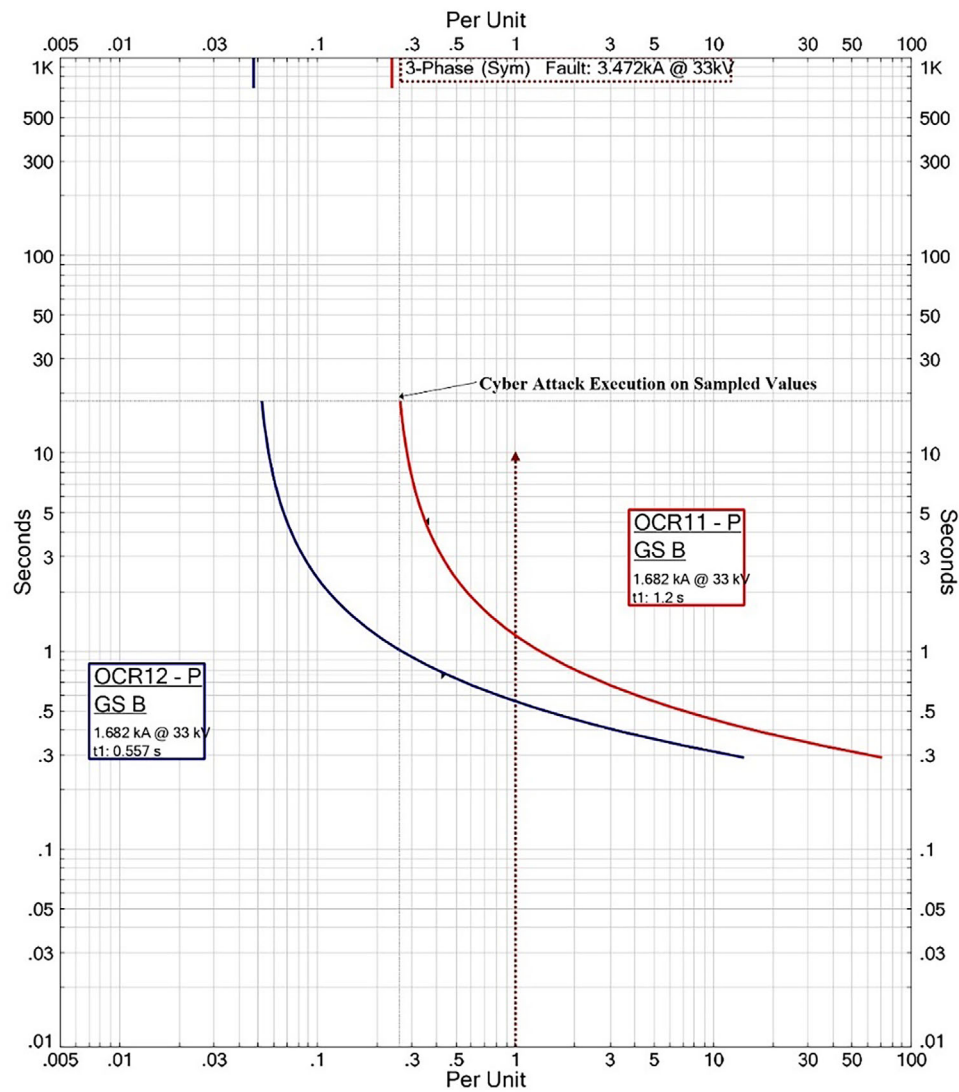
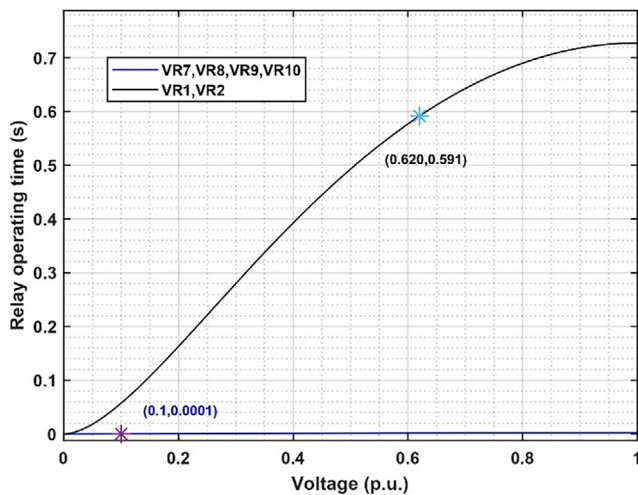**FIGURE 18** Adaptive overcurrent relays (OCRs) coordination performance under normal and attack-4.

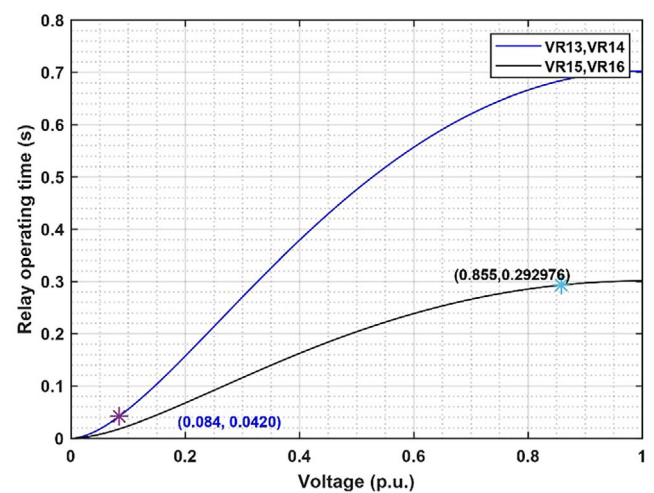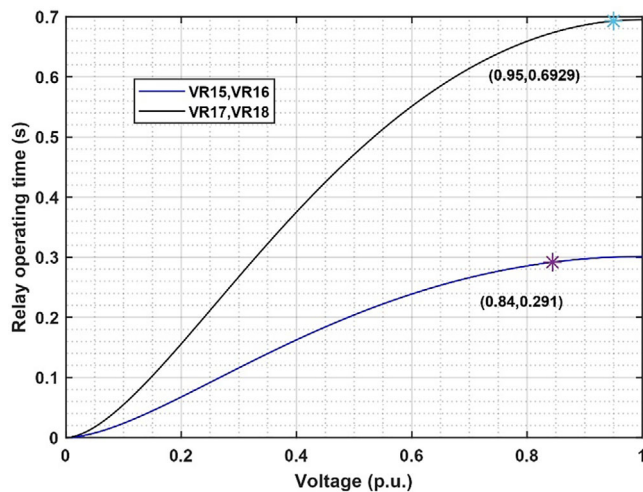**FIGURE 19** Voltage-based relays coordination during F1 scenario.

FIGURE 20 Voltage-based relays coordination during F2 scenario.

TABLE 15 The tripping times of voltage-based relays over fault scenarios (F1–F3).

Physical fault events	Cyber-attacks events	Adaptive OCRs		Voltage-based relay	
		Relay	Tripping time	Relay	Tripping time
F1	1	OCR3	0.33	VR3	0.2999
		OCR4	0.33	VR4	0.2999
		OCR7	0.21	VR7	0.597
		OCR8	0.21	VR8	0.597
		OCR9	0.21	VR9	0.591
		OCR10	0.21	VR10	0.591
F2	2	OCR11	0.48	VR11	0.0426
		OCR12	0.48	VR12	0.0426
		OCR13	0.79	VR13	0.0426
		OCR14	0.79	VR14	0.0426
F3	2	OCR15	0.76	VR15	0.291
		OCR16	0.76	VR16	0.2911
		OCR17	1.09	VR17	0.692
		OCR18	1.09	VR18	0.6929
F1	3	OCR3	0.63	VR3	0.2999
		OCR4	0.63	VR4	0.2999
		OCR11	1.16	VR11	0.597
		OCR12	1.16	VR12	0.597
F2	4	OCR11	0.55	VR11	0.0426
		OCR12	1.2	VR12	0.0426

FIGURE 21 Voltage-based relays coordination during F3 scenario.

times, miss-coordination events, and energy production losses. For example, during F1 and attack 1, OCR3 and OCR4 exhibited tripping times of 0.33 s, while voltage-based relays (VR3 and VR4) displayed remarkable responsiveness with tripping times of approximately 0.2999 s. Furthermore, adaptive protection relays OCRs 7–10 reordered a miss-coordination event during attack 1 resulting in a loss of \$1248/h in benefits from the PV systems. Therefore, this study highlights the significant of

TABLE 16 Energy not supplied from PVs due to the miss-coordination event at adaptive OCR during attack 1 and F1 scenario.

Description	Value
PV availability	0.89
Size of PV (MW)	4
Available PV (kW)	3568
Duration of interruption (Hour)	1
Energy not supplied (kWh)	3568
PV energy rate at this location (\$)	0.35
Benefits loss (\$)	1248

having less communicated protection systems such as voltage-based relays is presented to enhance the resilience of power grid protection systems against cyber-attacks.

NOMENCLATURE

DER	Distributed Energy Resource
OCR	Overcurrent Relay
HV	High Voltage
MV	Medium Voltage
LV	Low voltage
PV	Photovoltaic

DN	Distributed Network
SBDG	Synchronous-based distributed generations
IBDG	Inverter-based distributed generations
GOOSE	Generic Object Oriented Substation Event
SMV	sampled measured value
MITM	Man-In-The-Middle
FDI	False Data Injection
IA	Integrity attack
RA	Replay Attack
DoS	Denial of Service
NT	Network Topology
t_{nl}	tripping times of the OCR number n for a fault transpiring at location l Pickup Current
CTI	Clearing Time Interval
I_f	short-circuit current
I_P	pickup current
a and b	the relay characteristics constants
TMS	Time Multiplier Setting
OT	operating time for OCR
c, p and r	constant parameters
V	fault voltage level magnitude function
V_f	Fault voltage
OCRP	Primary OCR
OCRB	Backup OCR
IED	Intelligent Electronic Device
HMI	Human-Machine Interface
SV	Sampled Value

AUTHOR CONTRIBUTIONS

ACKNOWLEDGEMENTS

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Not applicable.

ORCID

Feras Alasali https://orcid.org/0000-0002-1413-059X
William Holderbaume https://orcid.org/0000-0002-1677-9624

REFERENCES

1. Holderbaum, W., Alasali, F., Sinha, A.: Energy Forecasting and Control Methods for Energy Storage Systems in Distribution Networks, Predictive Modelling and Control Techniques, 1st ed. Springer, Cham (2023)
2. Alasali, F., El-Naily, N., Zarour, E., Saad, S.: Highly sensitive and fast microgrid protection using optimal coordination scheme and nonstandard tripping characteristics. Int. J. Electr. Power Energy Syst. 128, 106756 (2021)
3. Alasali, F., Zarour, E., Holderbaum, W., Nusair, K.: Highly sensitive and fast microgrid protection using optimal coordination scheme and nonstandard tripping characteristics. Int. J. Electr. Power Energy Syst. 128, 106756 (2021)
4. Brahma, S.M., Girgis, A.A.: Development of adaptive protection scheme for distribution systems with high penetration of distributed generation. IEEE Trans. Power Delivery 19(1), 56–63 (2004)
5. Coffele, F., Booth, C., Dyśko, A.: An adaptive overcurrent protection scheme for distribution networks. IEEE Trans. Power Delivery 30(2), 561–568 (2014)
6. Ghalei, M., Mazlumi, K., Kamwa, I.: Application of μPMUs for adaptive protection of overcurrent relays in microgrids. IET Gener. Transm. Distrib. 12(18), 4061–4068 (2018)
7. Alam, M.N.: Adaptive protection coordination scheme using numerical directional overcurrent relays. IEEE Trans. Ind. Electron. 15(1), 64–73 (2018)
8. Hosseini, S.A., Sadeghi, S.H.H., Nasiri, A.: Decentralized adaptive protection coordination based on agents social activities for microgrids with topological and operational uncertainties. IEEE Trans. Ind. Appl. 57(1), 702–713 (2020)
9. Dos Reis, F.B., Pinto, J.O.C., Issicaba, D., Rolim, J.G.: Multi-agent dual strategy based adaptive protection for microgrids. Sustainable Energy Grids Network 27, 100501 (2021)
10. Abbaspour, E., Fani, B., Karami-Horestani, A.: Adaptive scheme protecting renewable-dominated micro-grids against usual topology-change events. IET Renewable Power Gener. 15(12), 2686–2698 (2021)
11. Aazami, R., Esmaeilbeigi, S., Valizadeh, M., Javadi, M.S.: Novel intelligent multi-agents system for hybrid adaptive protection of micro-grid. Sustainable Energy Grids Network 30, 100682 (2022)
12. Dorosti, P., Moazzami, M., Fani, B., Siano, P.: An adaptive protection coordination scheme for microgrids with optimum PV resources. J. Clean. Prod. 340, 130723 (2022)
13. Vasconcelos, L.H.P., Almeida, A.R., Dos Santos, B.F., Melo, N.X., Carvalho, J.G.S., De Oliveira, D.: Hybrid optimization algorithm applied to adaptive protection in distribution systems with distributed generation. Electr. Power Syst. Res. 202, 107605 (2022)
14. Ataei, M.A., Gitizadeh, M.: A distributed adaptive protection scheme based on multi-agent system for distribution networks in the presence of distributed generations. IET Gener. Transm. Distrib. 16(8), 1521–1540 (2022)
15. El-Hamrawy, A.H., Ebrahiem, A.A.M., Ebrahiem, A.I.M.: Improved adaptive protection scheme based combined centralized/decentralized communications for power systems equipped with distributed generation. IEEE Access 10, 97061–97074 (2022)
16. Bisheh, H., Fani, B., Shahgholian, G., Sadeghkhani, I., Guerrero, J.M.: An adaptive fuse-saving protection scheme for active distribution networks. Int. J. Electr. Power Energy Syst. 144, 108625 (2023)
17. Barranco-Carlos, A., Orozco-Henao, C., Marín-Quintero, J., Mora-Flórez, J., Herrera-Orozco, A.: Adaptive protection for active distribution

networks: An approach based on fuses and relays with multiple setting groups. IEEE Access 11, 31075–31091 (2023)

18. Barra, P.H.A., Coury, D.V., Fernandes, R.A.S.: A survey on adaptive protection of microgrids and distribution systems with distributed generators. Renewable Sustainable Energy Rev. 118, 109524 (2020)

19. Mahat, P., Chen, Z., Bak-Jensen, B., Bak, C.L.: A simple adaptive overcurrent protection of distribution systems with distributed generation. IEEE Trans. Smart Grid 2(3), 428–437 (2011). https://doi.org/10.1109/tsg.2011.2149550

20. Singh, M., Vishnuvardhan, T., Srivani, S.: Adaptive protection coordination scheme for power networks under penetration of distributed energy resources. IET Gener. Transm. Distrib. 10(15), 3919–3929 (2016). https://doi.org/10.1049/ietgtd.2016.0614

21. Purwar, E., Choudhary, M.M.: Novel adaptive algorithm for optimal relay setting with improved coordination. In: 2014 Students Conference on Engineering and Systems. Allahabad, India (2014). https://doi.org/10.1109/sces.2014.6880078

22. Nascimento, J.P., Brito, N.S.D., de Souza, B.A.: An adaptive protection algorithm for distribution systems with distributed generation. In: 2015 IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM). Montevideo, Uruguay (2015). https://doi.org/10.1109/isgt-la.2015.7381147

23. Nascimento, J.P., Brito, N.S.D., de Souza, B.A.: Proposition of an adaptive protection scheme for distribution systems with distributed generation. IEEE Lat. Am. Trans. 16(5), 1439–1444 (2018). https://doi.org/10.1109/tla.2018.8408439

24. Ma, J., Mi, C., Wang, T., Wu, J., Wang, Z.: An adaptive protection scheme for distributed systems with distributed generation. In: 2011 IEEE Power and Energy Society General Meeting. Detroit, MI, USA (2011). https://doi.org/10.1109/pes.2011.6039832

25. Habib, H.F., Lashway, C.R., Mohammed, O.A.: A review of communication failure impacts on adaptive microgrid protection schemes and the use of energy storage as a contingency. IEEE Trans. Ind. Appl. 54(2), 1194–1207 (2017). https://doi.org/10.1109/tia.2017.2776858

26. Habib, H.F., Mohamed, A., El Hariri, M., Mohammed, O.: Utilizing supercapacitors for resiliency enhancements and adaptive microgrid protection against communication failures. Electr. Power Syst. Res. 145, 223–233 (2017)

27. Akella, R., Tang, H., Bruce, M.M.: Analysis of information flow security in cyber-physical system. Int. J. Crit. Infrastruct. Prot. 3, 157–173 (2010)

28. Rahman, M., Mahmud, M., Oo, A.M.T., Pota, H.: Multi-agent approach for enhancing security of protection schemes in cyber physical energy systems. IEEE Trans. Ind. Inf. 13(2), 436–447 (2016)

29. Jahromi, A., Kemmeugne, A., Kundur, D., Haddadi, A.: Cyber physical attacks targeting communication-assisted protection schemes. IEEE Trans. Power Syst. 35(1), 440–450 (2019)

30. Rajkumar, V., Tealane, M., Ştefanov, A., Presekal, A., Palensky, P.: Cyber attacks on power system automation and protection and impact analysis. In: 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe). The Hague, Netherlands, pp. 247–254 (2020)

31. Choi, I., Hong, J., Kim, T.: Multi-agent based cyber attack detection and mitigation for distribution automation system. IEEE Access 8, 183495–183504 (2020)

32. Singh, V., Govindarasu, M.: A cyber physical anomaly detection for wide-area protection using machine learning. IEEE Trans. Smart Grid 12(4), 3514–3526 (2021)

33. Jahromi, M., Jahromi, A., Kundur, D., Sanner, S., Kassouf, M.: Data analytics for cybersecurity enhancement of transformer protection. ACM SIGENERGY Energy Inf. Rev. 1(1), 12–19 (2021)

34. Alrashide, A., Abdelrahman, M., Kharchouf, I., Mohammed, O.: GNS3 communication network emulation for substation GOOSE based protection schemes. In: 2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe). Prague, Czech Republic, pp. 1–6 (2022)

35. Mohamed, N., Salama, M.: Data mining-based cyber physical attack detection tool for attack-resilient adaptive protective relays. Energies 15(12), 4328 (2022)

36. Hussain, S., Aftab, M., Farooq, S., Ali, I., Ustun, T., Konstantinou, C.: An effective security scheme for attacks on sample value messages in IEC 61850 automated substations. IEEE J. Power Energy 10, 304–315 (2023)

37. Mo, J., Yang, H.: Sampled value attack detection for busbar differential protection based on a negative selection immune system. J. Mod. Power Syst. Clean Energy 11(2), 421–433 (2023)

38. Yousefi kia, M., Saniei, M., Seifossadat, S.: A novel cyber-attack modelling and detection in overcurrent protection relays based on wavelet signature analysis. IET Gener. Transm. Distrib. 17(7), 1585–1600 (2023). https://doi.org/10.1049/gtd2.12766

39. Mohamed, N., Salama, M.M.A.: Data mining-based cyber-physical attack detection tool for attack-resilient adaptive protective relays. Energies 15, 4328 (2022). https://doi.org/10.3390/en15124328D

40. Gutierrez-Rojas, I.D, Kontou, A., et al.: Operational issues on adaptive protection of microgrids due to cyber attacks. IEEE Trans. Circuits Syst. II Express Briefs 70(8), 2994–2998 (2023)

41. Alasali, F., Mustafa, H., Saidi, A.S., El-Naily, N., Abeid, S., Holderbaum, W., Saad, S.: The recent development of protection coordination schemes based on inverse of AC microgrid: A review. IET Gener. Transm. Distrib. 18, 1–23, (2023). https://doi.org/10.1049/gtd2.13074

42. Shih, M.Y., et al.: An adaptive overcurrent coordination scheme to improve relay sensitivity and overcome drawbacks due to distributed generation in smart grids. IEEE Trans. Ind. Appl. 53(6), 5217–5228 (2017)

43. Elnaily, N., Saad, S., Elhaffar, A., Zarour, E., Alasali, F.: Innovative adaptive protection approach to maximize the security and performance of phase/earth overcurrent relay for microgrid considering earth fault scenarios. Electr. Power Syst. Res. 206, 107844 (2022)

44. Alasali, F., Saad, S., El-Naily, N., Layas, A., Elhaffar, A., Hussein, T., Mohamed, F.A.: Application of time-voltage characteristics in overcurrent scheme to reduce Arc-flash incident energy for safety and reliability of microgrid protection. Energies 14, 8074 (2021)

45. Santos, G.P., Tsutsumi, A., Vieira, J.C.M.: Enhanced voltage relay for AC microgrid protection. Electr. Power Syst. Res. 220, 109310 (2023)

46. AlMajali, A., Viswanathan, A., Neuman, C.: Resilience evaluation of demand response as spinning reserve under cyber physical threats. Electronics 6(1), 2 (2016)

47. Wadhawan, Y., AlMajali, A., Neuman, C.: A comprehensive analysis of smart grid systems against cyber-physical attacks. Electronics 7, 249 (2018). https://doi.org/10.3390/electronics7100249

48. Rajkumar, V.S., et al.: Cyber attacks on power system automation and protection and impact analysis. In: IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe). The Hague, Netherlands, pp. 247–254 (2020)

49. Dai, Q., Shi, L., Ni, Y.: Multi-objective optimal cyber attack strategy in centralized feeder automation system. In: IEEE Power Energy Society General Meeting (PESGM). Atlanta, GA, USA, pp.1–5 (2019)

50. Kim, J., Tong, L.: On topology attack of a smart grid: Undetectable attacks and countermeasures. IEEE J. Sel. Areas Commun 31(7), 1294–1305 (2013)

51. Liu, Y., Ning, P., Reiter, M.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14(1), 1–33 (2011)

52. Jin, D., Nicol, D., Yan, G.: An event buffer flooding attack in dnp3 controlled SCADA systems. In: Proceedings of the 2011 Winter Simulation Conference (WSC). Phoenix, AZ, USA, pp. 2614–2626 (2013)

How to cite this article: Alasali, F., Hayajneh, A.M., Ghalyon, S.A., El-Naily, N., AlMajali, A., Itradat, A., Holderbaume, W., Zaroure, E.: Enhancing resilience of advanced power protection systems in smart grids against cyber–physical threats. IET Renew. Power Gener. 18, 837–862 (2024). https://doi.org/10.1049/rpg2.12957