Robust Overcurrent-differential Agent-based Relaying Scheme with a False Data Rejection Tool

Mohamed Elgamal, Abdelfattah A. Eladl, Bishoy E. Sedhom, *Member*, *IEEE*, and Akram Elmitwally, *Member*, *IEEE*

***Abstract*—Recent developments in agent-based systems provide an effective solution to many operational problems of power systems. This paper proposes a protection scheme that uses agent-based relays in a cooperative multiagent structure. The relay primarily starts as an overcurrent relay to detect the fault. Then, it starts data exchange with one peer relay in case of line faults or few neighboring relays in case of busbar faults to confirm the fault location. At this later step, it acts as a differential relay that compares the current phasors at both line ends in the case of line faults and computes the net outgoing current in the case of busbar faults. The scheme design is presented, and the agent cooperation protocol is described. To enforce the scheme against false data injected by hackers via intruding communication facilities, an anomaly detection device is prepared and integrated into each agent. The proposed tool is based on a one-class support vector machine and can firmly discriminate real fault data from injected false data. The tool also enables the relay to recognize the challenging high impedance fault. The proposed method is tested by dynamic simulation on the IEEE 9- and 39-bus systems under various conditions. The performance is evaluated by comparing it with that of other recent techniques.**

***Index Terms*—Overcurrent protection, differential relay, multiagent system, cyberattack.**

I. Introduction

Rapid fault clearance is a basic requirement for developing protection measures. To ensure that network components are not damaged in case of a fault in the power system, the faulty area must be located and isolated from the entire system as quickly as possible [1], [2]. The integration of distributed generation resources (DGRs) into radial distribution systems can lead to problems related to protection relay coordination and fault location accuracy. This is because DGRs transform the distribution networks from a conventional radial configuration to multi-ended configurations, thereby changing the direction and magnitude of the fault current [3], [4]. Some conventional fault detection techniques disconnect the DGRs during faults to eliminate their effects on the fault current [5]. Conventional protection systems based on overcurrent relays (OCRs) have also become inadequate for distribution networks with DGRs because of discrimination and miscoordination problems [6]. Additionally, traditional directional OCRs (DOCRs) are costly option for distribution networks because they require accompanying voltage transformers [6]. Therefore, many studies, such as references [7] and [8], have suggested the current-only DOCR (CODR) for distribution networks. CODR detects the direction of faults using a fault direction indicator (FDI). However, FDI precision relies on the detection of the fault current angle, which is greatly affected by fault resistance. In fact, references [7], [8] have tested CODR under fairly low fault resistances up to 5 Ω only. Therefore, CODR may not perform well under high-resistance faults (HRFs) thus limiting its techno-economic feasibility.

On the other hand, the line current differential relay (LCDR) is employed in transmission systems to protect critical transmission lines. It is also being gradually used in distribution systems to handle the issues caused by the integration of DGRs [9]. LCDRs can sense small differences between two or more similar quantities, and thus, they are more sensitive, faster, and more reliable than DOCRs for detecting all types of low/high resistance faults inside their protection zones [9], [10].

Received: May 22, 2024
Accepted: October 30, 2024
Published Online: May 1, 2025

Mohamed Elgamal (corresponding author) is with the Electrical Engineering Department, Mansoura University, Mansoura 35516, Egypt, and the Department of Automated Electrical Systems, Ural Power Engineering Institute, Ural Federal University, Yekaterinburg 620002, Russia (e-mail: engineer_elgamal@mans.edu.eg).

Abdelfattah A. Eladl, Bishoy E. Sedhom, and Akram Elmitwally are with the Electrical Engineering Department, Mansoura University, Mansoura 35516, Egypt (e-mail: eladle7@mans.edu.eg; eng_bishoy90@mans.edu.eg; akram@mans.edu.eg).

DOI: 10.23919/PCMP.2024.000015

But LCDRs require advanced communication and rigorous continuous synchronization to exchange information at both ends of the protected line [9]. Thus, LCDRs are an expensive solution to protect distribution lines. Moreover, LCDRs are more vulnerable to cyberattacks than DOCRs and distance relays. Therefore, these considerations restrain the use of LCDRs in distribution networks [9].

Various centralized artificial intelligence (AI)-based techniques, such as radial basis function network [11], genetic algorithm and grey wolf optimization [12], wild horse optimization algorithm [6], linear programming and firefly algorithm [13], particle swarm optimization [3], gravitational search algorithm, and sequential quadrating programming [10], have been proposed to solve miscoordination problems between protective devices in distribution networks. However, the application of centralized AI-based techniques requires a control center (CC) to collect measurements of voltages and currents from all parts of the network using scattered phasor measurement units (PMUs) [2], [8]. Then, measurements are processed by a dedicated protection algorithm to make control decisions. Therefore, a breakdown in the CC (i.e., single-point failure problem) can completely halt the protection system. Additionally, as CC uses optimization techniques, it incurs significant computational costs to determine optimal settings of relays [14]. However, the coordination of some relays may be lost, especially in large-scale electrical systems, because of inaccurate optimization or unseen operational conditions [2], [8].

To overcome these shortcomings, distributed AI-based techniques, such as multiagent system (MAS), have been used to detect and locate faults in distribution networks [8]. MAS is used in various electrical applications [15], such as microgrid energy management [16], fault location, and service restoration [17], [18]. An agent-based relay (ABR) is a protective relay enhanced by agent characteristics. Thus, it can interact, communicate, negotiate, and exchange data and messages autonomously through a common communication network with other ABRs to make more rational decisions. It employs a well-designed set of rules that govern the agent behavior. Thus, the ABR can combine the operating principles of two or more conventional relays. The proposed ABR in this paper integrates overcurrent and differential relays to detect and locate faults quickly and accurately. The ABR also can detect failures in its communication channels and its corresponding circuit breaker (CB), and can then adapt its behavior via a built-in backup protection strategy. Therefore, the ABR can be equipped with multiple backup protection plans and a cyberattack detection tool to increase the reliability of the protection system. In summary, the ABR is an open-source smarter relay with higher adaptability. Many recent studies have confirmed that ABRs outperform traditional relays, including digital ones, in terms of accuracy and response time against faults [2], [8].

ABRs have been proposed for fault localization and service restoration in radial distribution networks with DGRs in [2], [18], [19]. In [20], an MAS-based protection scheme was introduced to adjust the coordination between OCRs in looped microgrids. In [8], an MAS-based protection method was presented to adjust the coordination between CODRs in looped distribution networks. However, the protection schemes reported in [8], [18], [20] exhibit low sensitivity to HRFs with a typical low fault current. In [2] and [19], each line was protected by a single ABR located at the midpoint. Any ABR can detect faults on its line by comparing the current phasors measured using two PMUs located at both ends of its line. Thus, these protection schemes have high sensitivity for detecting low-resistance faults and HRFs. Nonetheless, they require advanced communications and strict continuous synchronization, as in differential protection, to continuously compare the data transmitted from both PMUs. Therefore, the protection schemes in [2], [19] are more costly and more vulnerable to cyberattacks than those in [8], [18], [20]. Cyberattacks can be blocked in [8], [18], [20] by equipping the ABR at each line end with a local data-based method to detect cyberattacks, where hackers cannot manipulate local measurements [21]. In summary, the shortcomings of previous MAS-based protection research can be abridged as follows.

1) Except for [2], [8], [19], the previous methods do not accurately determine the fault current direction. The methods reported in [2], [19] require advanced communication and strict continuous synchronization to continuously compare data transmitted from PMUs located at both ends of the protected line.

2) Most studies do not consider the fault location on the busbar.

3) These studies lack an approach to identify the type of fault.

4) Most studies have addressed only symmetrical faults in distribution networks.

5) If they can deal with HRFs, they are not secured against cyberattacks.

6) Most studies do not provide backup protection strategies to manage failures.

Malicious individuals can hack and eavesdrop on data of an ABR located on one side of a given protected zone (i.e., line/bus). Hence, they can send messages containing false data over communications to an ABR on the other side of a protected zone, resulting in false tripping problems [21], [22]. The SCADA system databases of Ukrainian electricity companies were hacked in 2015, and attacks knocked out power to approximately 225 000 users for up to six hours [23]. Therefore, securing ABRs from cyberattacks is crucial.

Recently, several machine learning-based studies have been conducted to enhance the cybersecurity of protective relays [21]–[23]. Anomaly detection algorithms focus on learning normal operating conditions of power systems rather than recognizing different cyberattack instances [21], [22]. References [24] and [25] proposed anomaly detection algorithms to detect false data injection attacks on measurements collected via distributed sensors to perform state estimation in smart grids. In [26], an offline analytical method was presented to identify vulnerabilities implemented through cyberattacks against LCDRs. Reference [22] introduced a 1D-convolutional autoencoder-based approach to identify such cyberattacks, but there may be a weakness in this approach because hackers can manipulate remote measurements sent from one end of the transmission line to the other by hacking into the communication network. The weakness of [22] can be addressed by the anomaly detection scheme presented in [21], which only uses local measurements of each LCDR to detect cyberattacks using the isolation forest algorithm (IFA). The one-class support vector machine (OCSVM) was found to be superior to IFA [27], [28], as the OCSVM model can be trained on uncontaminated or normal data without including anomalous data. However, most studies addressing the problem of cyberattacks only considered traditional protection relays such as LCDRs, OCRs, and distance relays, while the cybersecurity of MAS-based protection schemes has not been reported.

In this paper, a CODR-based relaying scheme is proposed to detect, isolate, classify, and locate low/high resistance faults in looped/radial distribution networks. Each line is equipped with two ABRs installed at both ends, while each bus is protected by neighboring ABRs. Additionally, the ABR includes an OCSVM-based model to perform two main functions: the first function is to secure the ABR from false tripping cyberattacks; the second function is to increase the sensitivity of the ABR in HRF detection. The OCSVM model is basically trained on a dataset that includes normal operating fluctuations in the power system. The OCSVM can distinguish the normal state from any other conditions.

Accordingly, the proposed relaying scheme offers the following advantages.

1) It is robust and scalable because it comprises independently distributed ABRs without a central processor. Therefore, there is no risk of complete system failure due to central processing failure.

2) It is economical because ABRs do not require costly voltage measuring equipment. Each ABR also does not require massive communications and continuous synchronization, as in LCDRs.

3) It is also applicable to radial and looped networks.

4) It can detect, classify, and locate all types of faults on buses, lines, and other branches.

5) It works well for a very wide fault resistance range.

6) It blocks cyberattacks and employs a backup strategy.

The main contributions of this paper are as follows.

1) A new distributed MAS-based relaying scheme is proposed. The proposed protection scheme relies only on current measurements, has high sensitivity for HRF detection, and requires a much lower communication rate than classic LCDRs and recent MAS-based protection schemes, such as [2]. This makes the proposed relaying scheme more economical and applicable to large-scale distribution networks.

2) Developing a decentralized anomaly detection tool (ADT) to activate and enable ABRs to detect subtle HRFs and false data injection attacks (FDIAs) to secure ABRs from false tripping cyberattacks. The proposed ADT scheme relies solely on local current measurements, which makes it more secure because intruders cannot easily manipulate local measurements.

3) Developing a backup protection strategy to overcome possible software and hardware failures against ABRs.

To verify these contributions, the performance of the proposed ABR scheme is evaluated under different faults with different types, locations, and resistances, and FDIA scenarios, while the performance of the proposed ABR scheme is compared with that of recent literature.

The remainder of this paper is organized as follows. The proposed protection method is presented in Section II. Cyberattacks and anomaly detection are described in Section III. The simulation setup, results, analysis, and performance comparison with recent literature are presented in Section IV, and finally, Section V concludes the paper.

II. Proposed Protection Method

Figure 1 shows the communication topology of the proposed ABR system for a sample distribution network. Each line is protected by two peer ABRs located at both ends of the line. Each bus is protected by neighboring ABRs located at the ends of the lines, DGR terminals, and transformer terminals that connect to the bus, as shown in Fig. 1. For example, B_2 is protected by ABR_2, ABR_3, and ABR_6. Each ABR is equipped with a current transformer (CT) to measure three-phase currents (I_{abc}).

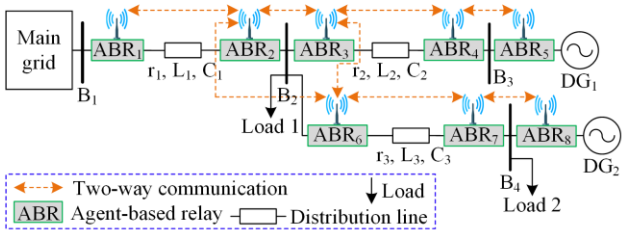


Fig. 1. Topology of the proposed ABR system for a sample distribution network.

The proposed ABR comprises a fault diagnosis algorithm (FDA) and an ADT. The FDA's role is to detect, classify, and locate faults. The ADT's role is to protect the ABR from false tripping attacks and also enable the ABR to detect HRFs, as explained later in Section IV. Figure 2 demonstrates the structure of the proposed ABR. Both the FDA and ADT process local three-phase currents sensed by the CT of ABR. The input features of the ADT are extracted from local measurements. In contrast to cyberattacks, significant changes in feature values are noticed during a fault. Therefore, if the output signal of the ADT S_{AD} equals 1, then it indicates a fault based on the features derived from the secure local measurements at the ABR site. If $S_{AD}=0$, then it indicates either an attack or a normal state. To determine whether an ABR is under cyberattack or fault, the following rules can be used (S_{FDA} is the output signal from the FDA):

1) If $S_{FDA}=0$ and $S_{AD}=0$, then there is a normal state (i.e., no fault and no cyberattack).

2) If $S_{FDA}=1$ and $S_{AD}=0$, then this ABR is under cyberattack, and there is no fault.

3) If $S_{FDA}=0$ and $S_{AD}=1$, then there is an external fault near the ABR location, and there is no cyberattack against this ABR.

4) If $S_{FDA}=1$ and $S_{AD}=1$, then there is an internal fault, and no cyberattack against this ABR. In this case, the ABR issues a trip command to its CB (i.e., $S_{trip}=1$).

Therefore, no ABR will trip its CB unless S_{FDA} and S_{AD} confirm a real internal fault in its protection zone.

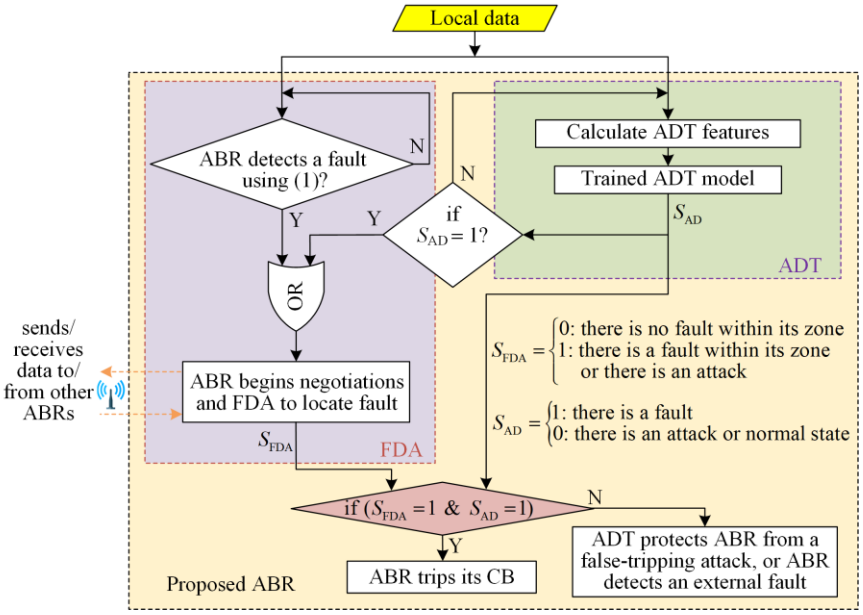


Fig. 2. Structure of the proposed ABR.

A. Algorithm of the Proposed ABR

The ABR must identify the fault status, location (i.e., line/bus), and type. Next subsections present the ABR algorithms.

1) Fault Detection

The ABR detects a fault as soon as the fault current exceeds the preset pickup current of the ABR. This method is suitable for covering most low- and medium-resistance faults for which the fault currents exceed the preset pickup current of the ABR. The next relationship represents the fault detection status indicator (FDSI) of the three-phase currents for a given ABR:

$$i_{\substack{\text{FDS}\\h=\text{a,b,c}}}=\begin{cases}1, & I^{\text{L}}_{h,\text{rms}}\geqslant I_{\text{Pickup}}\\0, & \text{else}\end{cases} \tag{1}$$

where i_{FDS} is the FDSI; h is the phase index; $I^{L}_{h,rms}$ is the local RMS current of phase h; and I_{Pickup} is the preset pickup current for a given ABR, which is taken as 1.5 times of the line's rated load current [8].

If one of the FDSI elements equals one, the ABR will see a fault and initiate communications to locate the fault. Practically, this method cannot detect HRFs whose fault currents are less than the pickup current of the ABR. Therefore, a second method is proposed in Section III to overcome this problem, which is based on the machine learning model of ADT built into the proposed ABR.

2) Fault Location and Type

Each ABR constantly monitors its local three-phase currents to detect faults using the FDSI in (1). Concurrently, the built-in ADT system continuously checks a set of features determined by the local three-phase currents to detect anomalies (i.e., possible faults) and avoid cyberattacks. If a particular ABR detects a fault either by the FDSI in (1) or by its ADT, it will begin locating that fault, as explained in the following steps.

1) Due to the long distance between any two peer ABRs located at both ends of a protected line, communication between them takes time. Therefore, any two peer ABRs must first synchronize with each other before exchanging their local data.

2) Once a given ABR detects a fault, it sends a time-stamped request message (RM) with a sequence number to its peer ABR to initiate synchronization and then exchanges local measurements. Simultaneously, it also starts a timer.

3) Once an ABR receives a synchronization RM from its peer ABR, the timer of the initiator peer ABR reaches a specific time delay (as will be explained later). At this time, both peer ABRs can start exchanging the phasor values of their local three-phase currents by sending time-stamped inform messages (IMs) with the same sequence number.

4) The peer ABRs now have each other's time-stamped current phasor measurements. If one of the two peer ABRs finds a difference beyond a threshold value (i.e., 3 ms) between the time stamps of its captured local current and the received remote current, it can determine the offset and shift its current measurements in time to align them properly with the remote current measurements [29].

5) After ensuring that the data are synchronized, concerned ABRs have each other's synchronized data. Therefore, each ABR can check whether the fault is on its own line or not using:

$$l_{\underset{h=\mathrm{a,b,c}}{\mathrm{LF}}} = \begin{cases} 1, & \left| I_h^{\mathrm{L}} + I_h^{\mathrm{P}} \right| > I_{\mathrm{threshold}} \\ 0, & \text{else} \end{cases} \tag{2}$$

$$I_{\mathrm{threshold}} = 2\pi f C \left(\frac{V_{\mathrm{L,max}}}{\sqrt{3}} \right) \tag{3}$$

where l_{LF} is the line fault locator (LFL); f, C, and $V_{\mathrm{L,max}}$ are the nominal system frequency, the total charging capacitance of the line, and the maximum nominal value of the line voltage, respectively.

6) According to (2), each concerned ABR computes the sum of the current phasors at both ends of its line. If the sum of currents at both ends for any phase h exceeds the threshold value, the ABR assumes a fault on its line and marks phase h as faulty.

7) For bus protection, ABRs are very close to each other and can exchange data directly using hard wires. Thus, the synchronization problem is not a concern for bus protection. Hence, all ABRs adjacent to any potentially faulty bus immediately exchange local three-phase current phasors to verify whether the fault is located on their bus. Each concerned ABR determines the next indicator as:

$$l_{\underset{h=\mathrm{a,b,c}}{\mathrm{BF}}} = \begin{cases} 1, & \left| I_h^{\mathrm{L}} + \sum_{j=1}^{N_{\mathrm{A}}} I_h^{\mathrm{A},j} \right| > I_{\mathrm{threshold}} \\ 0, & \text{else} \end{cases} \tag{4}$$

$$I_{\mathrm{threshold}} = I_{\mathrm{Load,max}} + \epsilon \tag{5}$$

where l_{BF} is the busbar fault locator (BFL); I_h^{L} is the phasor value of the hth phase current for the local ABR; $I_h^{\mathrm{A},j}$ is the phasor value of the hth phase current for the jth adjacent ABR; N_{A} is the number of ABRs adjacent to the concerned ABR; $I_{\mathrm{Load,max}}$ is the maximum magnitude of the load current at the bus; and ϵ is a small tolerance value.

8) If a concerned ABR finds that one or more elements of the BFL vector in (4) equal one, then it approves the fault on its own bus and can find out which phases are faulty.

9) If the ADT of the concerned ABR also finds anomalous behavior (i.e., fault), the concerned ABR will send confirm messages (CMs) to its peer ABR or neighboring ABRs to issue trip signals.

10) The ABR that approves a fault estimates the local zero-sequence current value (I_{Z}) given by (6). If I_{Z} is greater than a threshold (ξ), then the fault is connected to the ground.

$$I_{\mathrm{Z}} = \frac{1}{3}(I_{\mathrm{a}}^{\mathrm{L}} + I_{\mathrm{b}}^{\mathrm{L}} + I_{\mathrm{c}}^{\mathrm{L}}) \tag{6}$$

B. Backup Protection Strategy

Agent failure (AF) or CB failure (CBF) affects the scheme performance. AF can be caused by malfunction in hardware, communication link, or built-in algorithms. However, the proposed relaying scheme can function properly even under AF or CBF with a backup protection strategy, as described in the next two subsections. According to previous investigations and estimations mentioned in [30], the backup protection time delay must be set to more than 86 ms. Therefore, in this study, a waiting time of 120 ms is selected for the backup protection strategy, which allows sufficient time for coordination with primary protection strategy.

1) AF Backup Protection Strategy

For a line fault, if one of the two peer ABRs fails to respond, the healthy peer ABR starts an individual timer and retries to communicate with it every 40 ms up to three times. If the waiting time interval (i.e., 120 ms) [30] or number of attempts is passed without an answer, the ABR assumes that its peer ABR has failed. If the fault is still present, the healthy ABR assumes that the fault exists on its line. Thus, it sends a trip command to its CB and trip commands to the neighboring ABRs of its affected peer ABR to trip their CBs. Similarly, for a possible fault on a bus, if one of the ABRs does not respond to its neighboring ones, they send it three sequential RMs separated by a 40 ms interval. If no response is received, the healthy neighboring ABRs assume a fault on the bus and send direct trip commands to all CBs located around the faulty bus using the hard wires.

2) CBF Backup Protection Strategy

When two peer ABRs of a given line successfully locate a fault on that line, each ABR sends a trip command to its corresponding CB and then starts an individual timer simultaneously. If one of the two peer ABRs still detects the fault due to a possible failure of its CB, it will re-send a trip command to its CB every 40 ms up to three times. If the waiting time interval (i.e., 120 ms) [30] passes, the affected ABR assumes that its CB has failed. Therefore, it sends trip commands to the neighboring ABRs at the near-line end to trip their corresponding CBs.

Conversely, if ABRs adjacent to a given bus locate a fault on that bus, each ABR sends a trip command to its corresponding CB and then starts an individual timer simultaneously. If one of these adjacent ABRs suspects its CBF, it will re-send a trip command to this CB every 40 ms, up to three times. If the waiting time interval (i.e., 120 ms) [30] passes, the affected ABR assumes that its CB has failed. Therefore, it sends a trip command to its peer ABR at the other end of the line to open its corresponding CB.

III. Cyberattacks and Anomaly Detection

Cyberattacks on relays can occur randomly multiple times each year [21]. Consequently, it is essential to equip ABRs with ADT to mitigate cyberattack exposure. Practically, ADT is trained to learn normal behaviors of power system operation. Therefore, it can reveal an emulated fault introduced by hackers [21]. Secured local measurements of currents under various normal operating conditions are used to create the ADT training dataset. Because anomalous fluctuations in local measurements often originate from real faults, ADT can differentiate between faults and cyberattacks.

A. Input Feature Selection

The purpose of the input feature selection process in ADT is to maximize the correlation of features with fault perturbations. In contrast to cyberattacks, significant changes in the feature values of local data can be noticed during a fault. On the basis of secured local current measurements, five proposed input features are determined for each phase. The first two features are the changes in magnitude and phase angle of the currents at the present and previous time steps. The remaining three features are the changes in unbalance, total harmonic distortion (THD), and kurtosis factors of the present and previous step currents. These five features change dramatically during the fault, in contrast to normal operation [21], [31]. Additionally, kurtosis is an effective diagnostic tool for HRF detection [32]. The selected features are estimated every half power cycle.

For the current of phase a, the unbalance ratio, THD, and kurtosis factor are computed as in (7), (9), and (10), respectively [32], [33].

$$\mathcal{U}_{\mathrm{a}}^{\mathrm{L}}(t)=\left|\frac{I_{\mathrm{a,rms}}^{\mathrm{L}}(t)-I_{\mathrm{mean}}^{\mathrm{L}}(t)}{I_{\mathrm{mean}}^{L}(t)}\right| \tag{7}$$

$$I_{\mathrm{mean}}^{\mathrm{L}}(t)=\frac{1}{3}\sum_{h=\mathrm{a,b,c}} I_{h,\mathrm{rms}}^{\mathrm{L}}(t) \tag{8}$$

$$\mathcal{H}_{a}^{\mathrm{L}}(t)=\sqrt{\left(\frac{I_{\mathrm{a,rms}}^{\mathrm{L}}(t)}{I_{\mathrm{a,1,rms}}^{\mathrm{L}}(t)}\right)^{2}-1} \tag{9}$$

$$\mathcal{K}_{a}^{\mathrm{L}}(t)=\frac{E\left(I_{\mathrm{a}}^{\mathrm{L}}(t)-\mu_{\mathrm{I_a}}\right)^{4}}{\sigma_{\mathrm{I_a}}^{4}} \tag{10}$$

where $I_{\mathrm{a,rms}}^{\mathrm{L}}(t)$ is the root mean square (RMS) value of the local current of phase *a* at time *t*; and $I_{\mathrm{a,1,rms}}^{\mathrm{L}}(t)$ is the RMS value of the fundamental component of the local current of phase *a* at time *t*; $\mu_{\mathrm{I_a}}$ and $\sigma_{\mathrm{I_a}}$ are the mean value and standard deviation of $I_{\mathrm{a}}^{\mathrm{L}}(t)$, respectively; while $E(\cdot)$ denotes the expected inner value.

B. Dimensionality Reduction of Features

Principal component analysis (PCA) transforms feature data from an original high-dimensional space to a new lower-dimensional space. Almost all information in the input features is covered by the new dimensions, and no duplicate data are used [21].

Equation (11) transforms the $n\times m$ input feature matrix $\boldsymbol{F}$ into an $n\times p$ feature matrix $\boldsymbol{X}$, where $p \leqslant m$.

$$[\boldsymbol{X}]_{n\times p}=\left([\boldsymbol{F}]_{n\times m}-[\boldsymbol{M}]_{n\times m}\right)\times[\boldsymbol{\delta}]_{m\times p} \tag{11}$$

$$[\boldsymbol{\delta},\boldsymbol{\nu},\boldsymbol{M}]=\mathrm{Pca}\left([\boldsymbol{F}]_{n\times m}\right) \tag{12}$$

where *n*, *m*, and *p* are the numbers of measurements of the input features, dimensions of the input features, and new dimensions, respectively; $\boldsymbol{\delta}$ and $\boldsymbol{M}$ are the principal component coefficients' matrix of the input features and the estimated mean matrix of each feature in the input data, respectively, $\boldsymbol{\delta}$ and $\boldsymbol{M}$ are obtained using (12); while 'Pca' is a function for calculating $\boldsymbol{\delta}$, $\boldsymbol{\nu}$, and $\boldsymbol{M}$ from the input feature data using the singular value decomposition algorithm [34]; and $\boldsymbol{\nu}$ is a $m\times 1$ vector that includes the percentage of the total variance in each new dimension, where the cumulative sum of $\boldsymbol{\nu}$ equals 100%.

In fact, only the first few elements of $\boldsymbol{\nu}$ are important in most correlated systems, such as power systems. Typically, the smallest value of *p* satisfying the following criteria is selected:

$$p=\mathrm{find}\left(\sum_{i=1}^{m}\nu_i \geqslant \kappa\right) \tag{13}$$

where κ is taken as 95% in this paper to adequately represent the original features [26], [34].

C. OCSVM-based Anomaly Detection

It is assumed in OCSVM that there are only available data of one-class (the target class). The OCSVM attempts to identify the hyperplane or boundary that sep-

arates the target class data points from the remaining space. According to Fig. 3, the OCSVM classifier considers the origin point as a second-class sample. Then, it attempts to identify a hyperplane between the origin and instances of the target class while maximizing the margin (ρ/ω) between them [35]. The OCSVM maps the PCA-transformed training dataset $X=\{x_1, x_2, \cdots, x_p\}$ to a high-dimensional feature space using the feature map $\varphi(X)$ [35]. The purpose of mapping is to make the training dataset linearly separable in the new feature space. To separate the target class data samples from the origin, we must solve the next optimization equation:

$$\min_{\xi,\rho,\omega} \frac{1}{2}\omega^2 - \rho + \lambda\sum_{i=1}^{p}\xi_i \tag{14}$$

For any feature map (x_i), there is:

$$\varphi(x_i) \geqslant \left(\frac{\rho}{\omega} - \frac{\xi_i}{\omega}\right), \ \xi_i \geqslant 0 \tag{15}$$

where ρ, ω, and ξ are a bias term, a weight term, and nonzero positive slack variables, respectively, the slack variables represent training data samples that fall on the origin side of the hyperplane; and λ is a parameter that controls the actual trade-off between the target class and origin.

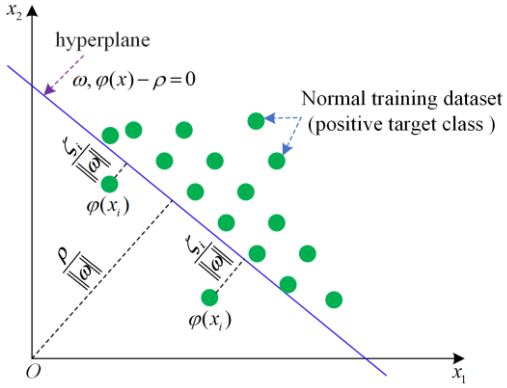


Fig. 3. Schematic diagram of OCSVM.

To obtain the optimal parameters of the hyperplane equation (i.e., ρ and ω), the OCSVM equation in (14) is solved using the Lagrangian multipliers $\alpha_i \geqslant 0$ and $\gamma_i \geqslant 0$ [35]:

$$\begin{aligned} L(\xi,\rho,\omega) = &\frac{1}{2}\|\omega\|^2 - \rho + \lambda\sum_{i=1}^{p}\xi_i + \\ &\sum_{i=1}^{p}\alpha_i(\omega\varphi(x_i) - \rho + \xi_i) - \sum_{i=1}^{p}\gamma_i\xi_i \end{aligned} \tag{16}$$

Partially differentiating L with respect to ω, ξ and ρ yields:

$$\begin{cases} \omega = \sum_{i=1}^{p}\alpha_i \ \varphi(x_i) \\ \sum_{i=1}^{p}\alpha_i \geqslant 1 \\ 0 \leqslant \alpha_i \leqslant 1 \end{cases} \tag{17}$$

By substituting ω from (17) into the hyperplane equation $(f(x)=\omega, \ \varphi(x)-\rho=0)$, the optimal value of ρ can be obtained by selecting random sample x_j that exists on the hyperplane.

$$f(x_j) = \sum_{i=1}^{p}\omega\varphi(x_j) - \rho = 0 \tag{18}$$

$$\rho_{\text{opt}} = \sum_{i=1}^{p}\alpha_i\varphi(x_i)\varphi(x_j) = \sum_{i=1}^{p}\alpha_i K(x_i, x_j) \tag{19}$$

where K is a Gaussian kernel function, and given as:

$$K(x_i, x_j) = \varphi(x_i)\varphi(x_j) = \mathrm{e}^{-\beta\|x_i - x_j\|^2} \tag{20}$$

where β defines the bandwidth of the Gaussian kernel.

Finally, we obtain the hyperplane equation for any sample point x as:

$$f(x) = \sum_{i=1}^{p}\alpha_i K(x_i, x) - \rho_{\text{opt}} \tag{21}$$

If the sign of $f(x)$ is equal to +1, then the sample point x is labeled as a normal point (i.e., normal operation or attack, $S_{\text{AD}}=0$); if the sign of $f(x)$ is equal to −1, then the sample point x is labeled as an abnormal point (i.e., fault, $S_{\text{AD}}=1$), i.e.:

$$S_{\text{AD}} = \begin{cases} 0, & f(x) \geqslant 0 \\ 1, & f(x) < 0 \end{cases} \tag{22}$$

IV. Simulation Setup and Results

A. Test System Description

Figure 4 shows the modified IEEE 9-bus system used to test the scheme efficacy [10].

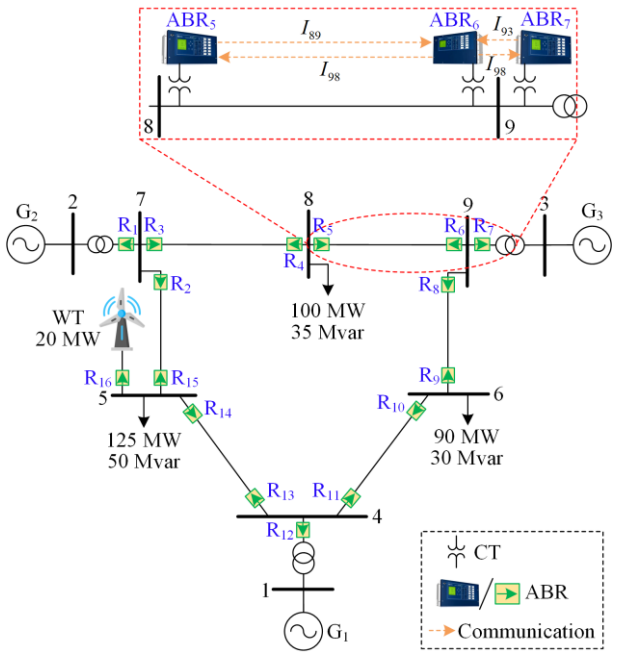


Fig. 4. Modified IEEE 9-bus system with focus on line 8–9 and bus 9.

A 20-MW wind turbine (WT) is installed on bus 5, and the WT generator operates at a unity power factor. ABRs are placed at both ends of all lines and at the DGR terminals. The proposed ABR only needs a pickup current setting. Datasets are first collected from the modified IEEE 9-bus system and used to train and build the ADT model based on the OCSVM. The scheme is then subjected to various tests.

B. ADT Design

Initially, R_5 is employed to create an anomaly detection model based on the OCSVM. ADT is trained using the normal operation dataset collected from line 8–9 measurements. Subsequently, a further healthy dataset containing normal variations in the three-phase currents is used to validate the performance of the trained OCSVM model of R_5. Finally, the validated OCSVM model of R_5 can be applied to all relays in the system and examined online under various test cases.

To obtain the training data for R_5, we record normal fluctuations in the three-phase current measurements of line 8–9 caused by varying loading conditions and determine the corresponding five features discussed in Section III.A for different time samples. Dimensionality and correlation of the collected feature data are reduced using PCA transform, as described in Section III.B. Next, the transformed feature data are grouped into two equally sized sets using a cross-validation tool [36]. The first set of transformed feature data is used for training the OCSVM model, and the second set is used to validate the trained OCSVM model. Because the test dataset consists of normal fluctuations irrelevant to faults, all samples are 100% classified as no fault.

C. Performance Analysis

An interactive simulation model is developed in Matlab/Simulink to validate the proposed protective mechanism. Matlab m-file is used to model and simulate the proposed ADT. The ABRs are implemented using the Java agent development framework (JADE) [16], [37]. A Java-based real-time link is created between Matlab and JADE to facilitate data exchange. The two interface functions SetVar and GetVar are coded in Java. Their role is to transmit data from Matlab to the ABRs in JADE and transmit the decisions made by the ABRs to Matlab. A graphical representation of the connection between the JADE and Matlab environments is shown in Fig. 5.

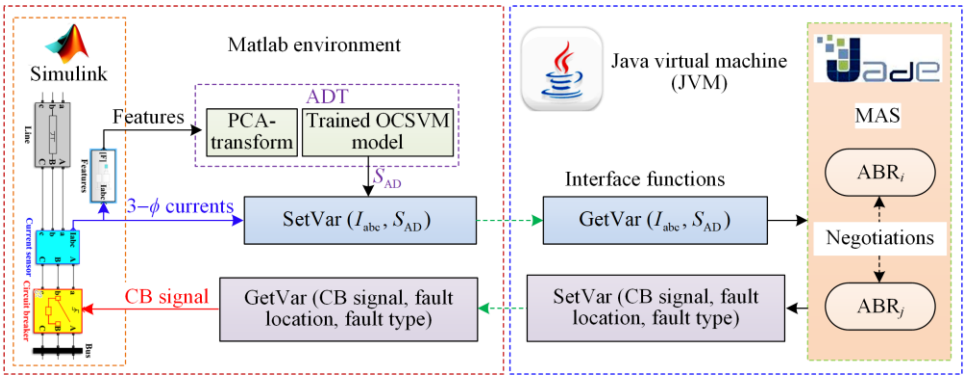


Fig. 5. Graphical layout of simulation structure.

The proposed scheme is tested on 120 different cases with various fault types, locations, and resistances and cyberattack situations. The faults are simulated at different locations, such as 5%, 30%, 50%, 70%, and 95% of the line length. Fault resistance values of 0.01 Ω, 10 Ω, 50 Ω, 100 Ω, 150 Ω, 200 Ω, 300 Ω, 500 Ω, 700 Ω, 1000 Ω, 1200 Ω, 1500 Ω, and 2000 Ω are examined. Both the IEEE 9- and 39-bus test systems are studied. The proposed scheme successfully locates and classifies faults, and effectively differentiates between faults and cyberattacks in all cases. For example, a few cases are presented as follows.

1) IEEE 9-bus System

Case 1: LL-G fault on line 6–9 with $R_f = 200\,\Omega$

At time $t = 0.1\,\text{s}$, a double line to ground fault through a fault resistance of 200 Ω occurs on line 6–9. The performance of the proposed scheme is demonstrated in Figs. 6 and 7. During the fault (for $t > 0.1\,\text{s}$), ABR_4 to ABR_8 and ABR_{10} to ABR_{11} detected that a fault had occurred because its sensed current was greater than its preset pickup current. However, ABR_9 did not detect faults, as shown in Figs. 6(b) and 7(a); the fault current of ABR_9 is below its preset pickup current. Additionally, the ADT signals of ABR_8 and ABR_9 indicate anomalies, as depicted in Figs. 7(e) and (f). By data exchange, ABR_4 to ABR_7 found that the fault location was outside their protection zones. Conversely, ABR_8 and ABR_9 agree that the fault is located on their own line (line 6–9) because their LFL indicators are [1, 1, 0], as shown in Figs. 7(c) and (d). Subsequently, at $t = 0.1153\,\text{s}$, ABR_8 and ABR_9 send trip commands to their CBs to isolate line 6–9, as shown in Figs. 7(g) and (h).

If the scheme in [2] were applied under the same conditions as in this case, the performance of the ABR in [2] would be similar to that of the proposed method.

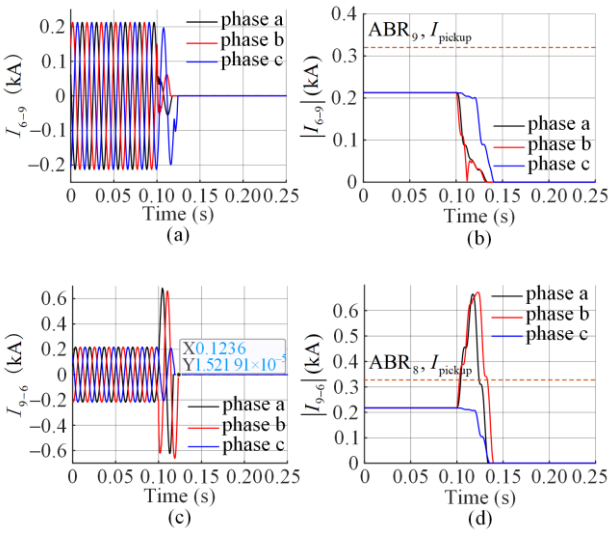


Fig. 6. Three-phase currents for pre-fault, during fault, and postfault for ABR9 and ABR8. (a) Current waveforms for ABR9. (b) Current magnitudes for ABR9. (c) Current waveforms for ABR8. (d) Current magnitudes for ABR8.

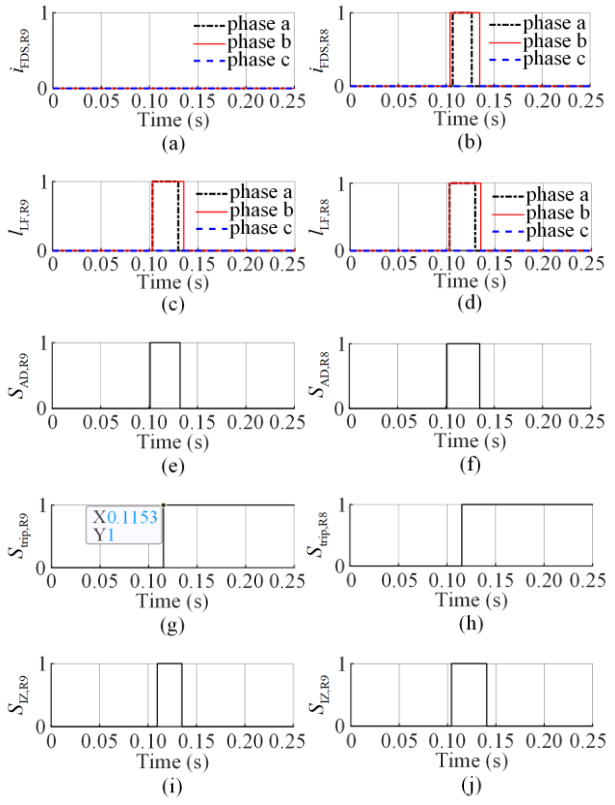


Fig. 7. Local indicators of ABR9 and ABR8 for detecting and locating faults. (a) FDSI of ABR9. (b) FDSI of ABR8. (c) LFL of ABR9. (d) LFL of ABR8. (e) ADT signal (S_{AD}) of ABR9. (f) S_{AD} of ABR8. (g) Trip signal (S_{trip}) of ABR9. (h) S_{trip} of ABR8. (i) state of IZ (S_{IZ}) of ABR9. (j) S_{IZ} of ABR8.

However, the scheme proposed in [2] is more costly, requires voltage sensors, can be more misled by cyberattacks, and has no ADT compared with the proposed one. However, the framework in [8] failed to correctly locate and isolate the fault on line 6–9. This is because the method in [8] identifies the fault current direction (i.e., forward or reverse) based on the FDI, which requires the difference between a reference phasor angle and the fault current angle ($\angle I_F$). Therefore, the method in [8] relies on the fault current angle, which is greatly affected by the fault resistance value above 100 Ω. Moreover, when the method in [8] is applied under the same conditions as in this case, its performance is demonstrated in Fig. 8. During the fault, ABRs from ABR_4 to ABR_8 and ABR_{10} to ABR_{11} detect faults. Therefore, they begin identifying their FDIs and then begin their communications to locate the fault.

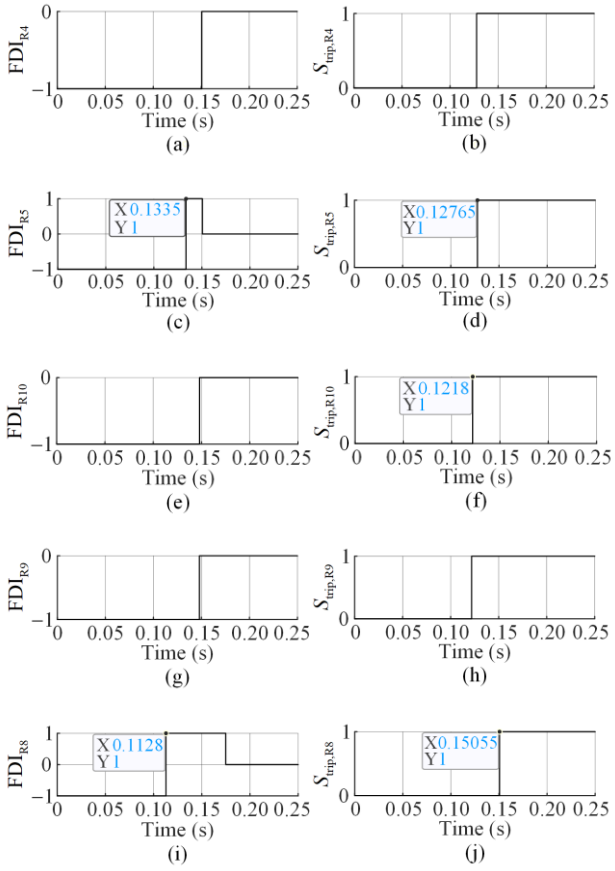


Fig. 8. Local indicators of ABR_4, ABR_5, ABR_8, ABR_9, and ABR_{10} using the method of [8]. (a) FDI of ABR_4. (b) S_{trip} of ABR_4. (c) FDI of ABR_5. (d) S_{trip} of ABR_5. (e) FDI of ABR_{10}. (f) S_{trip} of ABR_{10}. (g) FDI of ABR_9. (h) S_{trip} of ABR_9. (i) FDI of ABR_8. (j) S_{trip} of ABR_8.

According to Fig. 8, ABR_5 and ABR_9 fail to correctly identify their FDIs because they see the fault direction as reverse. Consequently, ABR_9 and ABR_{10} trip their CBs to isolate the incorrectly identified fault on bus 9 at about $t = 0.1218$ s. ABR_4 and ABR_5 also trip their CBs to isolate the incorrectly identified fault on their bus 8 at $t = 0.1276$ s. After the current of ABR_9 reaches zero

(i.e., FDI_{ABR9} is 0), ABR_8 successfully locates the fault on its line 6–9 and then sends a trip command to its CB to isolate the fault on its line 6–9, at $t = 0.150\ 55$ s. Table I summarizes the tripped CBs using the proposed scheme and those in [2] and [8].

TABLE I
COMPARISON OF TRIPPED CBS IN CASE 1

Item	Proposed method	[2]	[8]
Tripped CBs	8, 9	8, 9	4, 5, 8, 9, 10

Case 2: Cyberattacks against ABR_4 and ABR_5

Assume that at $t = 0.1$ s, hackers perform false tripping attacks on ABR_4, by sending messages containing false data pretending to be from its peer ABR_3. Likewise, false tripping attacks on ABR_5 are also performed by sending messages containing false data pretending to be from its peer ABR_6. Assuming that the real three-phase currents seen by ABR_3 are $[264.75\angle 4.2;\ 264.75\angle -115.8;\ 264.75\angle 124.2]$, , the hackers send manipulated data to ABR_4 as $[264.75\angle -175.8;\ 264.75\angle 64.2;\ 264.75\angle -55.8]$ thus reversing the direction of the ABR_3 current. Thus, ABR_4 will trip because current reversal is a situation that occurs when there is an internal fault on line 7–8 using (2). We assume that the hackers use another scenario to deceive ABR_5 by tripling the sent current magnitude of ABR_6. Therefore, ABR_5 would trip because overcurrent is a situation that occurs when there is an internal fault on line 9–8 using (2). However, the built-in ADT of ABR_4 and ABR_5 prevents false tripping, as shown in Figs. 9 (a) and (b).

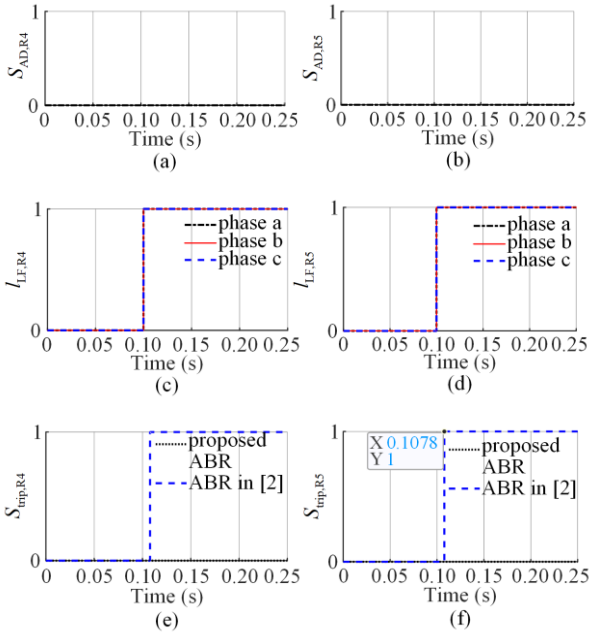


Fig. 9. Local indicators of ABR_4 and ABR_5. (a) S_{AD} of ABR_4. (b) S_{AD} of ABR_5. (c) LFL of ABR_4. (d) LFL of ABR_5. (e) S_{trip} of ABR_4 using proposed ABR and ABR in [2]. (f) S_{trip} of ABR_5 using the proposed ABR and ABR in [2].

The ADTs of ABR_4 and ABR_5 do not detect anomalies in their local measurements for $t \geqslant 0.1$ s. Although the LFL indicators of ABR_4 and ABR_5 identify an internal three-phase fault, as shown in Figs. 9(c) and (d), the ADTs protect ABR_4 and ABR_5 from falling into the trap of false tripping attacks, as shown in Figs. 9(e) and (f). If the ABRs in [2], [8] were applied under the same conditions as in this case, both ABRs in [2] and [8] would fail to avoid false tripping attacks. This is because the protection methods in [2] and [8] do not consider false tripping cyberattacks against ABRs.

2) IEEE 39-bus System

The IEEE 39-bus test system is shown in Fig. 10. The trained ADT model used in the test cases of the modified IEEE 9-bus system is also used in the IEEE 39-bus test system.

Case 1: ABC fault on line 17–18 with $R_f = 800\ \Omega$

Assume an ABC symmetrical fault with a high resistance of 800 Ω happens at $t = 0.1$ s. The fault location is 30% of the length of line 17–18 from bus 18, and assume that there are no cyberattacks.

During the fault (for $t \geqslant 0.1$ s), none of the ABRs in the system detect this fault initially because the fault current level is lower than the pickup current.

Figure 11 and Figs. 12(a) and (b) show the fault detection status (i.e., FDSI) of ABR_{34} and ABR_{35} on the faulty line. Both ABR_{34} and ABR_{35} do not detect the fault, but the output signals of ADTs integrated with ABR_{25}, ABR_{34}, ABR_{35}, ABR_{39}, and ABR_{40} classify the state as anomaly (i.e., fault conditions). So, these ABRs are triggered to check whether there is a fault or not. Consequently, ABR_{35} sends a synchronization RM to ABR_{34} to start the synchronization and then local measurements are exchanged with each other to check the status of line 17–18. Also, ABR_{35} exchanges its local measurements with its neighboring ABR_{39} and ABR_{40} directly using the hard wires to check the status of bus 17. Once ABR_{34} receives a synchronization RM, both ABR_{34} and ABR_{35} send to each other time-stamped IMs containing their local three-phase current phasors. Likewise, ABR_{38} and ABR_{39} communicate with each other to check line 17–27, ABR_{40} and ABR_{41} communicate with each other to examine line 16–17, and ABR_{24} and ABR_{25} communicate with each other to check line 3–18. Also, ABR_{25} and ABR_{34} exchange their local measurements with each other to examine bus 18. Once the involved ABRs have finished exchanging their local data with their peer ABRs and neighboring ABRs, they determine the LFL and BFL indicators using (2) and (4).

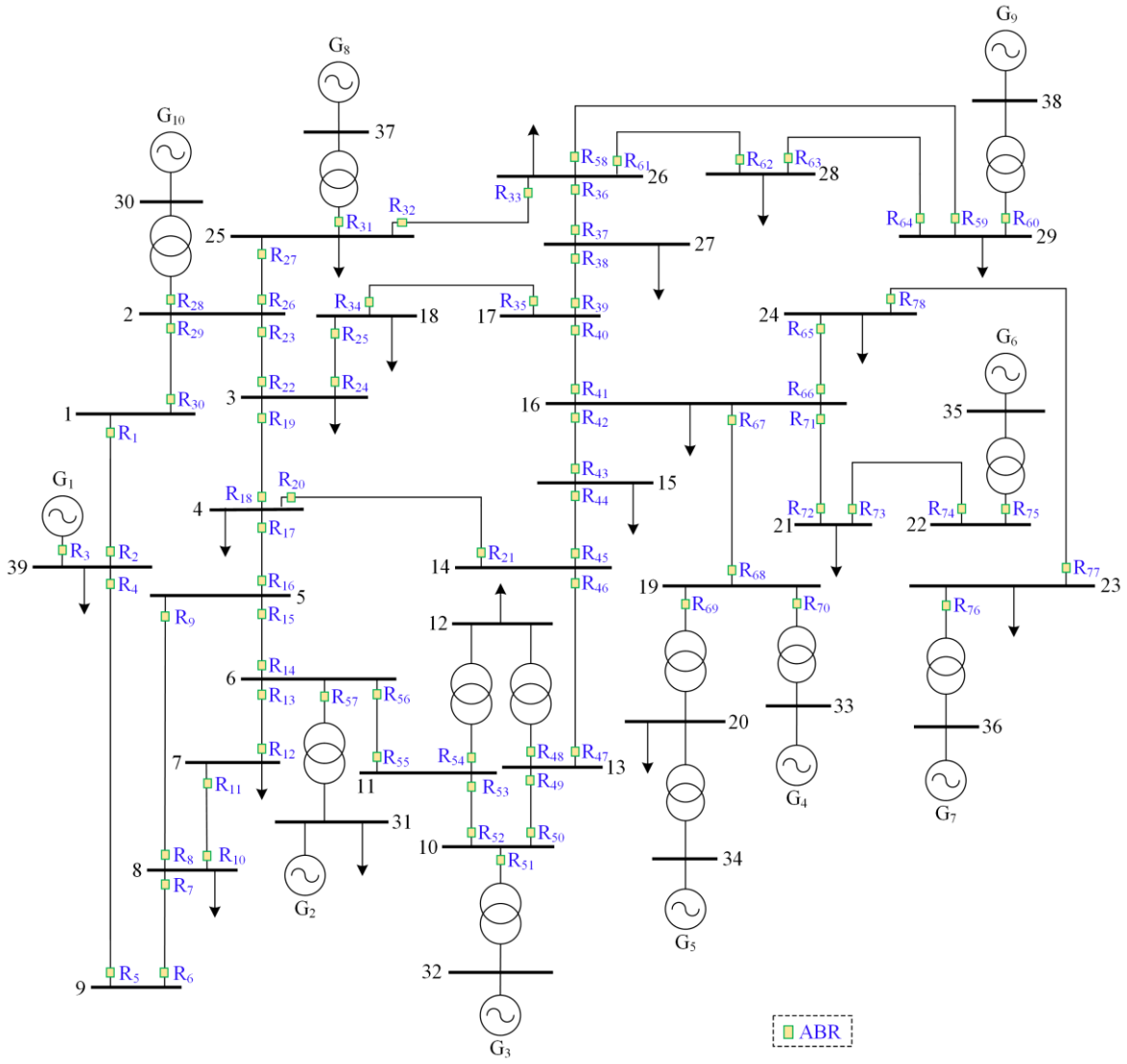
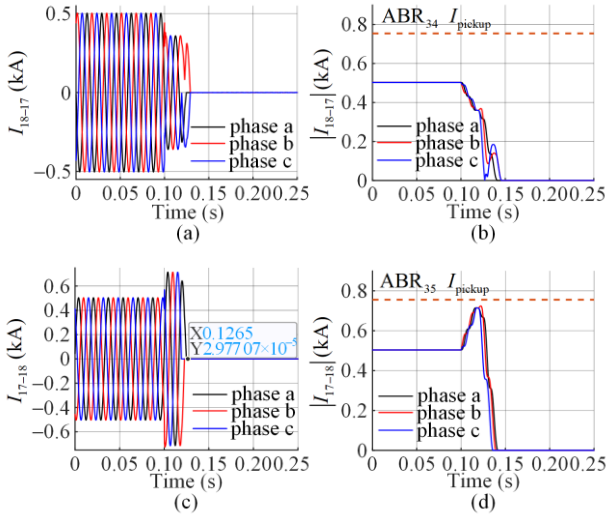


Fig. 10. One-line diagram of IEEE 39-bus system with ABRs [10].



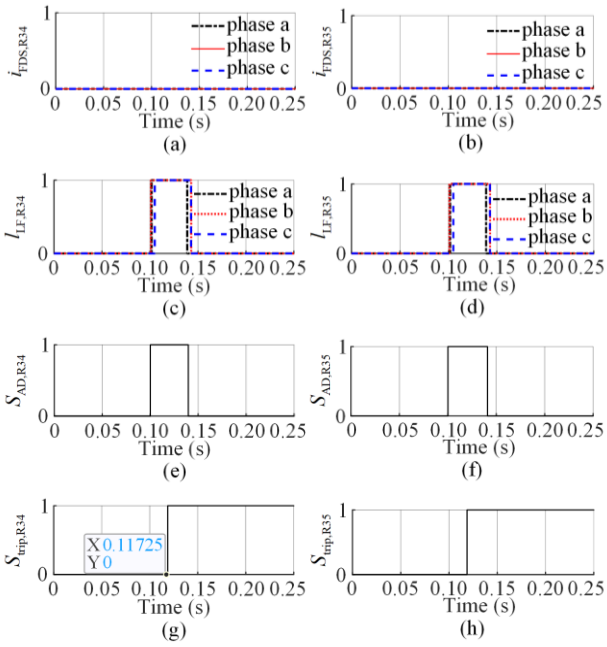


Fig. 11. Three-phase currents for pre-fault, during fault, and postfault for ABR_{34} and ABR_{35}. (a) Current waveforms for ABR_{34}. (b) Current magnitudes for ABR_{34}. (c) Current waveforms for ABR_{35}. (d) Current magnitudes for ABR_{35}.

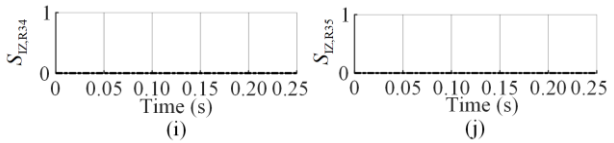


Fig. 12. Local indicators of ABR_{34} and ABR_{35}. (a) FDSI of ABR_{34}. (b) FDSI of ABR_{35}. (c) LFL of ABR_{34}. (d) LFL of ABR_{35}. (e) S_{AD} of ABR_{34}. (f) S_{AD} of ABR_{35}. (g) S_{trip} of ABR_{34}. (h) S_{trip} of ABR_{35}. (i) S_{IZ} of ABR_{34}. (j) S_{IZ} of ABR_{35}.

ABR_{34} and ABR_{35} LFL indicators are [1, 1, 1], meaning that there is a fault on phases a, b and c of line 17–18, as shown in Figs. 11(c) and (d). Subsequently, ABR_{34} and ABR_{35} send CMs to each other to isolate the induced fault on line 17–18. Hence, at $t = 0.117\ 25$ s, ABR_{34} and ABR_{35} send trip commands to their CBs, to isolate the faulty line 17–18. ABR_{34} and ABR_{35} define the fault type as ABC fault, where both get zero-sequence current state ($S_{IZ} = 0$) during the fault time.

If the system in [8] were applied under the same fault conditions, it would even fail to detect the fault. This is because the fault currents sensed by ABRs are less than the pickup current values, and no ADTs are integrated as backup fault detectors. On the other hand, if the scheme in [2] were applied, the performance would be similar to the proposed one. But, the scheme in [2] is more costly and vulnerable to cyberattacks.

Case 2: Backup protection strategy for L-G fault on bus 4 with $R_f = 220\ \Omega$

Assume that at $t = 0.1$ s, a single phase to ground (L-G) fault occurs on bus 4 with a fault resistance of 220 Ω. There are no cyberattacks and in this case ABR_{20} has the next failures.

a) CBF of ABR_{20}

During the fault (for $t \geqslant 0.1$ s), ABR_{16}, ABR_{17}, ABR_{18}, ABR_{20}, and ABR_{21} detect this fault because the fault current level is higher than the pickup current. Figure 13 and Figs. 14(a)–(c) show the fault detection status (i.e., FDSI) of ABR_{17}, ABR_{18}, and ABR_{20} located around the faulty bus 4. Also, the output signals of ADTs integrated with ABR_{16}, ABR_{17}, ABR_{18}, ABR_{20}, and ABR_{21} classify the state as an anomaly (i.e., fault conditions), as shown in Figs. 14(g)–(i). ABR_{17} detects this fault earlier, as shown in Fig. 17(a). So, ABR_{17} sends a synchronization RM to ABR_{16} to start the synchronization and then the two exchange local measurements to check the status of line 4–5. Also, ABR_{17} exchanges its local measurements with its neighboring ABR_{18} and ABR_{20} directly using the hard wires to check the status of bus 4. Once ABR_{17} receives a synchronization RM, both ABR_{16} and ABR_{17} send to each other time-stamped IMs containing their local three-phase current phasors. Likewise, ABR_{18} and ABR_{19} communicate with each other to check line 3–4, whereas ABR_{20} and ABR_{21} communicate with each other to examine line 4–14. ABR_{19}, ABR_{22}, and ABR_{24} communicate with each other to check bus 3, ABR_9, ABR_{15}, and ABR_{16} communicate with each other to check bus 5, and ABR_{21}, ABR_{45}, and ABR_{46} exchange their local measurements with each other to examine bus 14. Once the involved ABRs have finished exchanging their local data with their peer ABRs and neighboring ABRs, they determine the LFL and BFL indicators using (2) and (4). ABR_{17}, ABR_{18}, and ABR_{20} BFL indicators are [1, 0, 0], meaning that there is a fault on phase a of bus 4, as shown in Figs. 14(d)–(f). Subsequently, ABR_{17}, ABR_{18}, and ABR_{20} send CMs to each other to isolate the induced fault on bus 4. Hence, at $t = 0.1146$ s, ABR_{17}, ABR_{18}, and ABR_{20} send trip commands to their CBs, to isolate the faulty bus 4, as shown in Figs. 15(a)–(c). The CBs of ABR_{17} and ABR_{18} have succeeded in isolating the fault currents but ABR_{20} has a CBF, and its CB fails to isolate the fault current. Therefore, ABR_{20} starts an individual timer and then re-send a trip signal to its CB. After three attempts in 120 ms, the CB of ABR_{20} is not responding and still does not work. Consequently, ABR_{20} assumes that its CB has failed to operate and sends an RM to its peer ABR (ABR_{21}) to trip its corresponding CB to isolate the faulty bus. As shown in Fig. 15(d), ABR_{21} issues a trip signal to its corresponding CB at $t = 0.2354$ s.

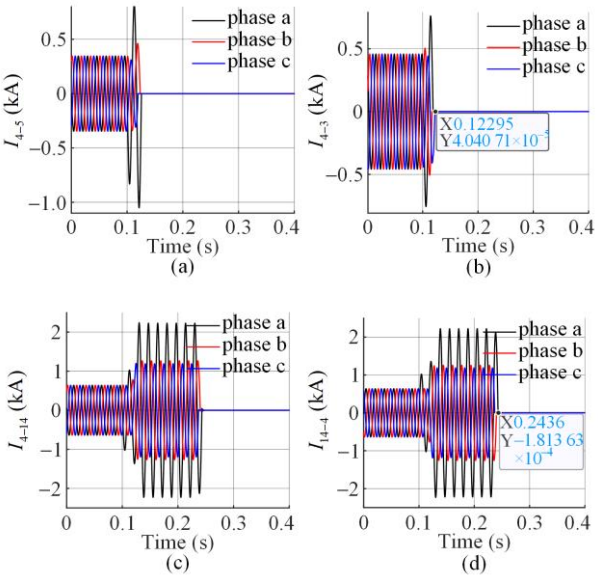
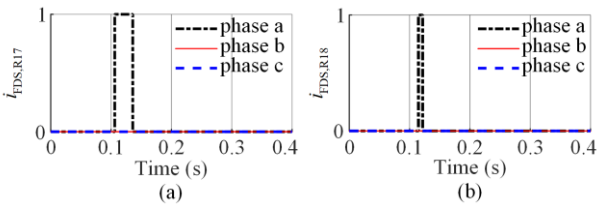


Fig. 13. Three-phase currents for pre-fault, during fault, and postfault for ABR_{17}, ABR_{18}, ABR_{20} and ABR_{21}. (a) Current waveforms for ABR_{17}. (b) Current waveforms for ABR_{18}. (c) Current waveforms for ABR_{20}. (d) Current waveforms for ABR_{21}.



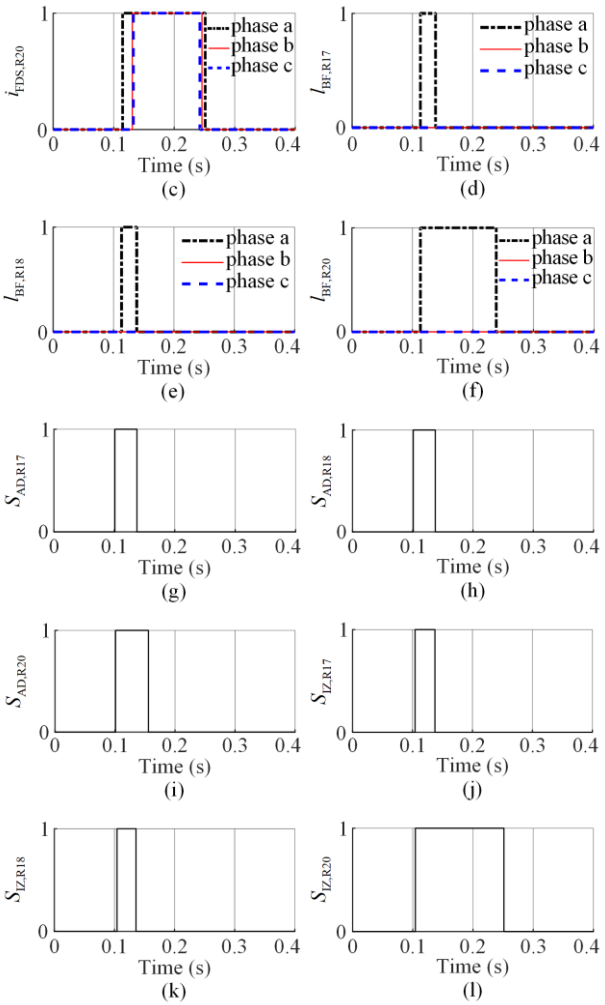


Fig. 14. Local indicators of ABR_{17}, ABR_{18}, and ABR_{20}. (a) FDSI of ABR_{17}. (b) FDSI of ABR_{18}. (c) FDSI of ABR_{20}. (d) BFL of ABR_{17}. (f) BFL of ABR_{18}. (d) BFL of ABR_{20}. (g) S_{AD} of ABR_{17}. (h) S_{AD} of ABR_{18}. (i) S_{AD} of ABR_{20}. (j) S_{IZ} of ABR_{17}. (k) S_{IZ} of ABR_{18}. (l) S_{IZ} of ABR_{20}.

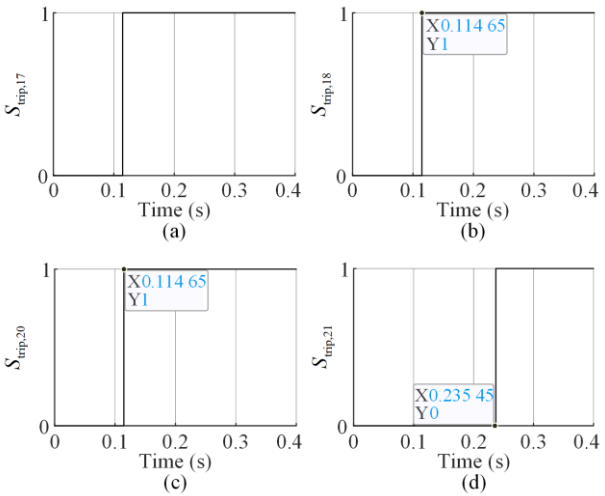


Fig. 15. Trip signals (S_{trip}) for ABR_{17}, ABR_{18}, ABR_{20}, and ABR_{21}. (a) ABR_{17}. (b) ABR_{18}. (c) ABR_{20}. (d) ABR_{21}.

ABR_{17}, ABR_{18}, and ABR_{20} find that the zero-sequence current exist ($S_{IZ}=1$) during the fault, as shown in Figs. 14(j)–(l). In addition, only the phase a BFLs of ABR_{17}, ABR_{18}, and ABR_{20} are one, as shown in Figs. 14(d)–(f). Accordingly, ABR_{17}, ABR_{18}, and ABR_{20} define the fault type as A-G fault.

b) AF of ABR_{20}

This case assumes that ABR_{20} has an AF condition. Figure 16 and Figs. 17(a)–(c) show the FDSI of ABR_{17}, ABR_{18}, and ABR_{20} located around the faulty bus 4. Also, the output signals of ADTs integrated with ABR_{16}, ABR_{17}, ABR_{18}, ABR_{20}, and ABR_{21} classify the state as an anomaly (i.e., fault conditions), as shown in Figs. 17(g)–(i). Similarly, as mentioned above, at $t=0.11$ s, ABR_{17} exchanges its local measurements with its neighboring ABR_{18} and ABR_{20} directly using the hard wires to check the status of bus 4.

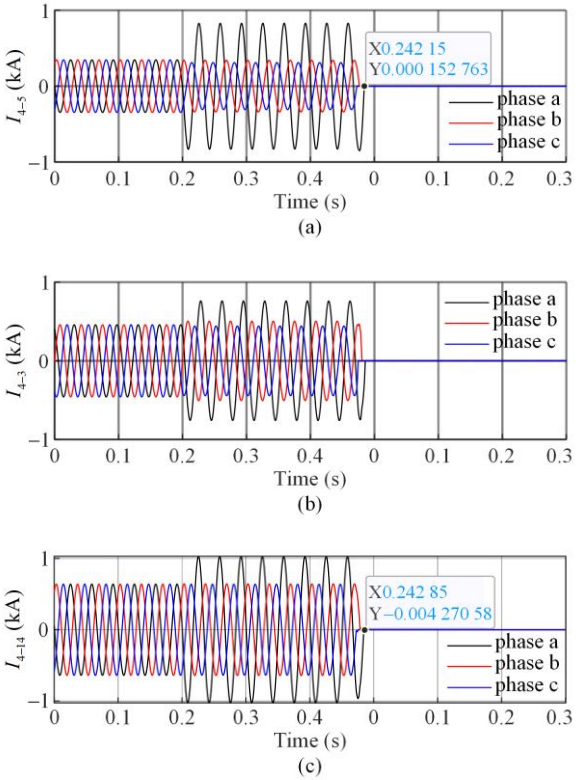
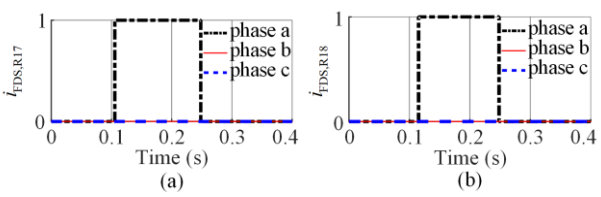


Fig. 16. Three-phase currents for pre-fault, during-fault, and post-fault for ABR_{17}, ABR_{18}, ABR_{20} and ABR_{21}. (a) Current waveforms for ABR_{17}. (b) Current waveforms for ABR_{18}. (c) Current waveforms for ABR_{20}. (d) Current waveforms for ABR_{21}.



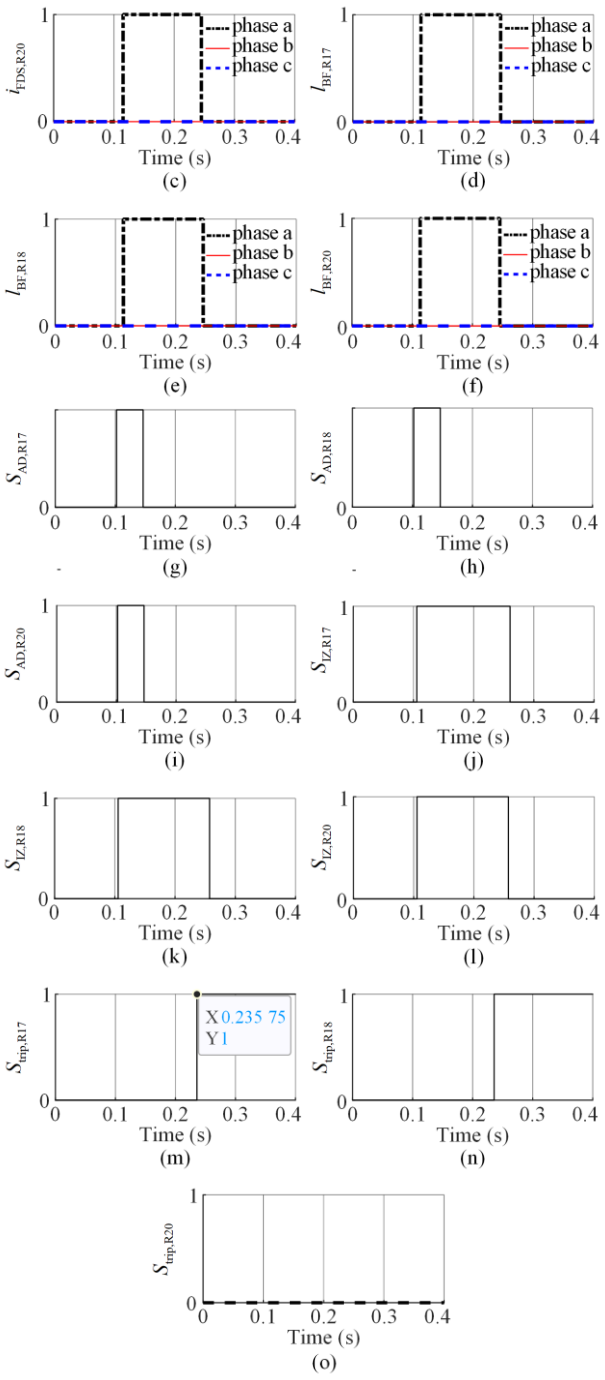


Fig. 17. Local indicators of ABR_{17}, ABR_{18}, and ABR_{20}. (a) FDSI of ABR_{17}. (b) FDSI of ABR_{18}. (c) FDSI of ABR_{20}. (d) BFL of ABR_{17}. (e) BFL of ABR_{18}. (f) BFL of ABR_{20}. (g) S_{AD} of ABR_{17}. (h) S_{AD} of ABR_{18}. (i) S_{AD} of ABR_{20}. (j) S_{IZ} of ABR_{17}. (k) S_{IZ} of ABR_{18}. (l) S_{IZ} of ABR_{20}. (m) S_{trip} of ABR_{17}. (n) S_{trip} of ABR_{18}. (o) S_{trip} of ABR_{20}.

At $t = 0.125$ s, ABR_{20} and ABR_{21} communicate with each other to examine line 4–14. However, ABR_{17}, ABR_{18}, and ABR_{21} do not receive response from the failing ABR_{20}. Consequently, at $t = 0.115$ s, ABR_{17} starts individual timer and repeatedly sends RMs to the failing ABR_{20}. After three attempts in 120 ms, the failing ABR_{20} does not respond. Therefore, at $t = 0.2357$ s, ABR_{17} assumes that its neighboring ABR_{20} has failed, the fault is on its bus, and so sends direct trip commands to all its neighboring CBs located around the faulty bus 4 using the hard wires, as shown in Fig. 17(m).

D. Comparison to Recent Literature

The PCA-aided OCSVM arrangement described in this work detects anomalies with 100% classification accuracy. In comparison, the PCA-IFA classification model presented very recently in [21] is trained and tested on the same feature dataset used in this paper. It is found that the performances of the trained IFA model and the OCSVM are the same. The training time is also similar. However, the IFA model takes 1.17 s to obtain the classification results for the test dataset while the OCSVM model consumes only 0.21 s. Therefore, the OCSVM model is about 6 times faster than the IFS model in detecting anomalies, and can better match the needs of the protection system. On the other hand, if the PCA technique is not combined with the OCSVM, the classification accuracy of the trained OCSVM model for the same test data is still 100%, but the computation time will increase by approximately 19%. In comparison, if the PCA technique is not combined with the IFA, the classification accuracy of the trained IFA model is also 100%, but the computing time increases by about 15%.

Table II provides a comparison between the proposed protection scheme and those presented in [2], [8].

TABLE II
COMPARISON TO SCHEMES IN [2], [8]

Item	Scheme in [2]	Scheme in [8]	Proposed scheme
Cost	High	Low	Low
Communications rate	High and continuous	Low and discontinuous	Low and discontinuous
Cyberattacks risk	Very high	High	Almost none
Sensitivity	High, for line faults None, for bus faults	Low, for line faults Low, for bus faults	High, for line faults High, for bus faults
Consider busbar faults	No	Yes	Yes
Fault classification	No	No	Yes
Reliability	Low	Low	High
Tested fault locations on the line (%)	50	50	5, 30, 50, 70 and 95
Tested fault resistances (Ω)	0.5	2	0.01 → 2000

The scheme in [2] is more costly than that in [8] and the proposed one, as its ABR requires advanced communications and strict continuous synchronization to continuously compare the data transmitted from PMUs located at both ends of its line. On the other hand, the

proposed ABR scheme only uses communications once it primarily detects a fault. In addition, the risk of cyberattacks against the ABR in [2] and [8] is very high because both ABRs don't consider cyberattacks. The proposed scheme has much higher sensitivity for locating HRFs than that in [8], while the scheme in [2] handles HRFs but cannot locate busbar faults. On the other hand, the proposed scheme can classify the type of fault, but those in [2], [8] cannot. Further, it can locate faults anywhere on the line, but those in [2], [8] are only tested under faults at the middle of the line.

V. Conclusion

This paper proposes an MAS-based relaying scheme that detects, classifies, locates, and trips faults, with only current sensing. The agents act independently and cooperatively without referring to a central controller. In principle, each ABR behaves as a non-DOCR to detect faults. Then, it communicates with one or more next-neighbor agents to form a virtual current differential relay to locate the fault on a line or busbar. This makes the scheme insensitive to fault impedance. To secure the scheme against false data imposed by cyberattacks, each ABR is supported by an embedded OCSVM-based customized anomaly detection mechanism. Dynamic simulation setups are constructed to examine the scheme in the IEEE 9- and 39-bus test systems. The proposed scheme has responded successfully to all test cases, including various faults and cyberattack situations. The performance of the proposed scheme is compared with that of recent agent-based protection frameworks. The proposed scheme works smoothly for close-in line faults and HRFs, while other recent schemes may respond incorrectly. The economic feasibility of the method will be considered for future work.

Acknowledgment

Not applicable.

Authors' Contributions

Mohamed Elgamal: designing the model and computational framework, coding&debugging, and writing the initial draft of the manuscript. Abdelfattah A. Eladl: conceiving the study, performing the calculations, and revising the manuscript. Bishoy E. Sedhom: conceiving the study, analyzing the data, and revising the manuscript. Akram Elmitwally: designing the model and computational framework, analyzing the data, and revising the manuscript. All authors read and approved the final manuscript.

Funding

This work is carried out without the support of any funding agency.

Availability of Data and Materials

Not applicable.

Declarations

Competing interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

Authors' Information

Mohamed Elgamal received the B.Sc. and M.Sc. degrees in electrical power engineering from Mansoura University, Egypt, in 2009, and 2014, respectively. He received the Ph.D. degree in electrical power engineering from Peter the Great St. Petersburg Polytechnic University, Russia, in 2021. He is currently an assistant professor with the Electrical Engineering Department, Mansoura University, Egypt. In 2015, he received the Best Master's Thesis Award from Mansoura University, Egypt. His fields of interest include smart grids, hybrid energy systems, power system protection, cybersecurity, and applications of artificial intelligence and multiagent systems in power systems.

Abdelfattah A. Eladl received the B.Sc. (ranked first, with honor), M.Sc., and Ph.D. degrees all are in electrical engineering from Faculty of Engineering, Mansoura University, Mansoura, Egypt. Currently, he is an associate professor with the Electrical Engineering Department, Mansoura University, Egypt. In 2016, he received the best Ph.D. thesis award from Mansoura University. His fields of interest include power system economics, planning, protection, and energy hubs.

Bishoy E. Sedhom received the B.Sc. (ranked first, with honor), M.Sc., and Ph.D. degrees all in Electrical Engineering from the Faculty of Engineering, Mansoura University, Mansoura, Egypt. He is an assistant professor with the Electrical Engineering Department, at Mansoura University, Egypt. In 2019, he received the best Ph.D. thesis award from Mansoura University. In 2023, he received the University Encouragement Award from Mansoura University. His fields of interest include energy management, microgrid operation and control, power system protection, power quality, internet of things, optimization methods, islanding detection, system restoration, high voltage DC transmission grids, microgrid protection, smart manufacturing, and cybersecurity.

Akram Elmitwally received the B.Sc., M.Sc., and Ph.D. degrees in electrical power engineering from Mansoura University, Egypt, in 1989, 1995, and 2002, respectively. He has been a visiting researcher at the Electronic and Electrical Engineering Department,

University of Bath, UK, from 1998 to 2000. He is currently a full professor with the Electrical Engineering Department, Mansoura University. He has authored more than 60 articles in journals and conferences. His fields of interests include power quality, power system protection, distributed generation, and AI applications in energy systems.

REFERENCES

[1] A. M. Tsimtsios and V. C. Nikolaidis, "Towards plug-and-play protection for meshed distribution systems with DG," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 1980-1995, May 2020.

[2] M. Azeroual, Y. Boujoudar, and K. Bhagat *et al.*, "Fault location and detection techniques in power distribution systems with distributed generation: Kenitra City (Morocco) as a case study," *Electric Power Systems Research*, vol. 209, pp. 1-14, Aug. 2022.

[3] A. Elmitwally, M. F. Kotb, and E. Gouda *et al.*, "A coordination scheme for a combined protection system considering dynamic behavior and wind dgs fault ride-through constraints," *Electric Power Systems Research*, vol. 213, pp. 1-14, Dec. 2022.

[4] A. N. Sheta, G. M. Abdulsalam, and B. E. Sedhom *et al.*, "Comparative framework for AC-microgrid protection schemes: challenges, solutions, real applications, and future trends," *Protection and Control of Modern Power Systems*, vol. 8, no. 2, pp. 1-40, Apr. 2023.

[5] M. A. Aftab, S. M. S. Hussain, and I. Ali *et al.*, "Dynamic protection of power systems with high penetration of renewables: a review of the traveling wave based fault location techniques," *International Journal of Electrical Power and Energy Systems*, vol. 114, pp. 1-13, Jan. 2020.

[6] S. El-Tawab, H. S. Mohamed, and A. M. Abdel-Aziz, "A novel proposed algorithm to enhance the overcurrent relays' performance in active distribution networks," *International Transactions on Electrical Energy Systems*, vol. 2022, pp. 1-16, Nov. 2022.

[7] H. S. Hosseini, A. Koochaki, and S. H. Hosseinian, "A novel scheme for current only directional overcurrent protection based on post-fault current phasor estimation," *Journal of Electrical Engineering and Technology*, vol. 14, pp. 1517-1527, May 2019.

[8] M. A. Ataei, M. Gitizadeh, and M. Lehtonen *et al.*, "Multi-agent based protection scheme using current-only directional overcurrent relays for looped/meshed distribution systems," *IET Generation, Transmission and Distribution*, vol. 16, no. 8, pp. 1567-1581, Jun. 2022.

[9] W. Jin, S. Zhang, and J. Li *et al.*, "A novel differential protection scheme for distribution lines under weak synchronization conditions considering DG characteristics," *IEEE Access*, vol. 11, pp. 86561-86574, Aug. 2023.

[10] A. Assouak and R. Benabid, "A new coordination scheme of directional overcurrent and distance protection relays considering time-voltage-current characteristics," *International Journal of Electrical Power and Energy Systems*, vol. 150, pp. 1-9, Aug. 2023.

[11] U. U. Uma, D. Nmadu, and N. Ugwuanyi *et al.*, "Adaptive overcurrent protection scheme coordination in presence of distributed generation using radial basis neural network," *Protection and Control of Modern Power Systems*, vol. 8, no. 4, pp. 1-19, Oct. 2023.

[12] R. Tiwari, R. K. Singh, and N. K. Choudhary, "Coordination of dual setting overcurrent relays in microgrid with optimally determined relay characteristics for dual operating modes," *Protection and Control of Modern Power Systems*, vol. 7, no. 1, pp. 1-18, Jan. 2022.

[13] S. P. Ramli, H. Mokhlis, and W. R. Wong *et al.*, "Optimal coordination of directional overcurrent relay based on combination of firefly algorithm and linear programming," *Ain Shams Engineering Journal*, vol. 13, no. 6, pp. 1-16, Nov. 2022.

[14] J. P. Nascimento, N. S. D. Brito, and B. A. Souza, "An adaptive overcurrent protection system applied to distribution systems," *Computers and Electrical Engineering*, vol. 81, pp. 1-16, Jan. 2020.

[15] O. P. Mahela, M. Khosravy, and N. Gupta *et al.*, "Comprehensive overview of multi-agent systems for controlling smart grids," *CSEE Journal of Power and Energy Systems*, vol. 8, no. 1, pp. 115-131, Jan. 2022.

[16] M. Elgamal, A. Elmitwally, and J. M. Guerrero, "An adaptive multiagent control system for autonomous economic operation and resilience assurance in a hybrid-energy islanded microgrid," *International Journal of Electrical Power and Energy Systems*, vol. 140, pp. 1-18, Sept. 2022.

[17] G. B. Costa, J. S. Damiani, and G. Marchesan *et al.*, "A multi-agent approach to distribution system fault section estimation in smart grid environment," *Electric Power Systems Research*, vol. 204, pp. 1-9, Mar. 2022.

[18] F. C. Sampaio, R. P. S. Leão, and R. F. Sampaio *et al.*, "A multi-agent-based integrated self-healing and adaptive protection system for power distribution systems with distributed generation," *Electric Power Systems Research*, vol. 188, pp. 1-7, Nov. 2020.

[19] H. F. Habib, T. Youssef, and M. H. Cintuglu *et al.*, "Multi-agent-based technique for fault location, isolation, and service restoration," *IEEE Transactions on Industry Applications*, vol. 53, no. 3, pp. 1841-1851, May 2017.

[20] H. Karimi, B. Fani, and G. Shahgholian, "Multi agent-based strategy protecting the loop-based micro-grid via intelligent electronic device-assisted relays," *IET Renewable Power Generation*, vol. 14, no. 19, pp. 4132-4141, Feb. 2020.

[21] A. Mohammad Saber, A. Youssef, and D. Svetinovic *et al.*, "Anomaly-based detection of cyberattacks on line current differential relays," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4787-4800, Nov. 2022.

[22] Y. M. Khaw, A. Abiri Jahromi, and M. F. M. Arani *et al.*, "A deep learning-based cyberattack detection system for transmission protective relays," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2554-2565, May 2021.

[23] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218-2234, May 2020.

[24] H. Karimipour, A. Dehghantanha, and R. M. Parizi *et*

al., "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *IEEE Access*, vol. 7, pp. 80778-80788, Jul. 2019.

[25] J. Yang, G. Sun, and J. Yin, "Coordinated cyber-physical attack considering false overload of lines," *Protection and Control of Modern Power Systems*, vol. 7, no. 4, pp. 1-13, Oct. 2022.

[26] A. Ahmed, V. V. G. Krishnan, and S. A. Foroutan *et al.*, "Cyber physical security analytics for anomalies in transmission protection systems," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 6313-6323, Nov. 2019.

[27] M. Verkerken, L. D'Hooge, and T. Wauters *et al.*, "Unsupervised machine learning techniques for network intrusion detection on modern data," in *2020 4th Cyber Security in Networking Conference (CSNet)*, Lausanne, Switzerland, Nov. 2020, pp. 1-8.

[28] M. Verkerken, L. D'hooge, and T. Wauters *et al.*, "Towards model generalization for intrusion detection: unsupervised machine learning techniques," *Journal of Network and Systems Management*, vol. 30, no. 1, pp. 1-25, Oct. 2022.

[29] Z. Idrees, J. Granados, and Y. Sun *et al.*, "IEEE 1588 for clock synchronization in industrial IoT and related applications: a review on contributing technologies, protocols and enhancement methodologies," *IEEE Access*, vol. 8, pp. 155660-155678, Aug. 2020.

[30] P. Gadde, S. Brahma, and T. Patel, "Real-time hardware-in-the-loop implementation of protection and self-healing of microgrids," *IEEE Transactions on Industry Applications*, vol. 59, no. 1, pp. 403-411, Jan. 2023.

[31] A. Ameli, A. Hooshyar, and E. F. El-Saadany *et al.*, "An intrusion detection method for line current differential relays," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 329-344, May 2020.

[32] K. Rai, F. Hojatpanah, and F. B. Ajaei *et al.*, "Deep learning for high-impedance fault detection and classification: transformer-CNN," *Neural Computing and Applications*, vol. 34, no. 16, pp. 14067-14084, Aug. 2022.

[33] W. Al Hanaineh, J. Matas, and J. Elmariachet *et al.*, "A harmonic-based fault detection algorithm for microgrids," in *Proceedings of the Interdisciplinary Conference on Mechanics, Computers and Electrics (ICMECE 2022)*, Barcelona, Spain, Oct. 2022, pp. 1-5.

[34] K. Zhang, Z. Chen, and L. Yang *et al.*, "Principal component analysis (PCA) based sparrow search algorithm (SSA) for optimal learning vector quantized (LVQ) neural network for mechanical fault diagnosis of high voltage circuit breakers," *Energy Reports*, vol. 9, pp. 954-962, Mar. 2023.

[35] Z. Ghafoori, S. M. Erfani, and S. Rajasegarar *et al.*, "Efficient unsupervised parameter estimation for one-class support vector machines," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 10, pp. 5057-5070, Oct. 2018.

[36] D. Berrar, "Cross-validation," in *Encyclopedia of Bioinformatics and Computational Biology*, Amsterdam, the Netherlands: Elsevier, 2019, pp. 542-545.

[37] F. Bellifemine, G. Caire, and A. Poggi *et al.*, "JADE: a software framework for developing multi-agent applications. lessons learned," *Information and Software Technology*, vol. 50, no. 1-2, pp. 10-21, Jan. 2008.