IEEE Open Journal of the
Industrial Electronics Society

Received 15 December 2024; revised 13 January 2025; accepted 23 January 2025. Date of publication 30 January 2025;
date of current version 7 February 2025. The review of this article was arranged by Associate Editor Jin-Gang Lai.

Digital Object Identifier 10.1109/OJIES.2025.3534588

A Hidden Surveillant Transmission Line Protection Layer for Cyber-Attack Resilience of Power Systems

HOSSEIN EBRAHIMI [1] **(Student Member, IEEE), SAJJAD GOLSHANNAVAZ** [1]**, AMIN YAZDANINEJADI** [2]**, AND EDRIS POURESMAEIL** [3] **(Senior Member, IEEE)**

[1]Department of Electrical and Computer Engineering, Urmia University, Urmia 57135, Iran
[2]Department of Electrical and Computer Engineering, Shahid Rajaee Teacher Training University, Tehran 16788-15811, Iran
[3]Department of Electrical and Computer Engineering, Aalto University, 11000 Espoo, Finland

CORRESPONDING AUTHOR: EDRIS POURESMAEIL (E-mail: edris.pouresmaeil@aalto.fi).

ABSTRACT This article proposes a framework to enhance the resilience of cyber-physical power systems (CPPSs) against cyber-attacks that are capable of bypassing the cyber-based defense mechanisms. To do so, a hidden and local surveillant protection layer is introduced that utilizes isolated measurement devices. Since this surveillance layer relies on local measurements, cyber-attackers cannot affect its performance. However, it requires highly accurate fault detection and classification units (FDCUs) which means requiring additional expenses. Therefore, at the outset, this article employs a deep-learning-based fault detection and classification method using a bidirectional long short-term memory (Bi-LSTM) model to achieve high accuracy with only local transmission line current measurements. The insight and knowledge of the FDCUs are also shared across their neighboring buses through the power-line-carrier communication system. Owing to the need for additional hardware, this system is modeled within a techno-economic framework. The established framework is applied to the CPPS through the evaluation based on distance from average solution (EDAS) method. The EDAS method allows for dynamic adjustments to the integration level of FDCUs based on an analysis of potential cascading failures from various cyber-attack target sets. Extensive simulations conducted on the IEEE 30-bus testbed validate the effectiveness of the proposed framework. The conducted evaluations show that the Bi-LSTM model achieves an impressive accuracy level exceeding 99.66%. This result highlights the robust performance of the proposed surveillant layer and demonstrates its superiority over existing fault detection and classification methods. The scalability of the proposed framework is also confirmed on the IEEE 118-bus testbed.

INDEX TERMS Deep-learning (DL), fault detection, multiattribute decision-making (MADM), resilience.

I. INTRODUCTION

Cyber-attacks are one of the high-impact low-probability events [1] that aim to deteriorate the confidentiality, integrity, and availability of data transmitted through power system communication networks. In this regard, the Department of Energy (DOE) of the United States outlined a roadmap in 2004 that paves the way for improving cyber-security in computer-based systems, including modern power systems, to enhance their operational quality and reliability. Based on this roadmap, regulators of these cyber-physical power systems (CPPSs) are obligated to adopt the same guidelines in hardening different subsystems including the protection schemes against cyber-attacks.

The robustness of individual and specific components of CPPSs is tackled in the early stages of studies. However, CPPSs traditionally consist of four distinct layers comprised of different components: the communications layer, the physical or power infrastructure layer, the sensors and actuators layer, and the application and management layer [2]. Typically, cyber-attackers intrude the communications layer to monitor and manipulate the processes in the applications and management layer, and/or sensors and actuators layer.

The final impact is intended to be seen on the physical or power infrastructure layer in the form of maloperations of different components, and consequently cascading failures and vast blackouts [3]. Specifically, in a false data injection attack (FDIA), initially, the attacker creates a backdoor into the application and management layer of the system through malware-infected e-mails, phishing messages, etc. [4]. Employing the backdoor gains access of the attacker to the communication layer to monitor the transmitted data for a long period. Therefore, taking advantage of the monitored data exchanged between the sensors and actuators layer with the application and management layer, and the damage priority along with the budget of the attacker, the attack points are determined [5]. By doing so, the attacker injects false measurement data exchanged by the sensors and protection devices resulting in the maloperation of target devices. These actions cause physical damages in the power infrastructure layer such as component outages and eventually, cascading outages followed by wide-range blackouts [6] which calls for the need for cyber-attack resilience enhancements in CPPSs.

Typically, the provided countermeasures for CPPSs' cyber-attack resilience are in the communications layer [4], [5], applications and management layer [6], [7], and some minor cases in the sensors and actuators layer [8]. Although such studies contribute to a high level of cyber-security enhancement, the mutual effects of layers' performance on each other and multilayer tasks in CPPSs are overlooked. Multilayer procedures such as central control of power systems include many details in the developed model and hence, complicate their cyber-security. Kundur et al. [9] not only emphasizes the importance of providing a vision for the multilayer impacts of cyber-attacks on CPPSs but also highlights the need for creating new layers. The protection schemes of power systems are one of the most important multilayer tasks of CPPSs which are required to be hardened against cyber intrusions. To this end, agent-based methods [10], game-theory models [11], [12], and development of a distributed security layer [13] are investigated in the literature. By the way, the cyber-resilience of CPPSs for different schemes such as the protection system through the inclusion of another layer among the typical layers translates to a new multilayer performance that provokes the economic aspect as a determinative factor. In this context, Shahzad [14] presents technical and economic assessment frameworks that evaluate these landscapes in multiple layers of the power system. Although the DOE report recommends the employment of data management systems for the cyber-resilience of CPPSs [8], cyber intrusions via the communications layer are still probable. That is, protection schemes and strategies that partially or generally incorporate the communication layer are prone to be sabotaged by more trained and capable attackers.

On the other hand, in the case of a sabotaged CPPS through the intrusion into its communications layer followed by a successful FDIA on the transmission line protection, the attacker either mimics a fake fault condition or displaces a real fault. Therefore, devising a hidden surveillance system upon the present protection schemes is of the essence. This mission can be accomplished by the deployment of a local and isolated fault detection unit that operates in parallel with the main protection system. Conventional fault detection approaches take advantage of a vast variety of methods including the wavelet transform [15], impedance calculation methods [16], [17], [18], mathematical methods such as summation of the squared signals [19], and the Furrier transform [20]. Although traditional methods have shown their merits, the implementation of artificial intelligence (AI) has proven to be more flexible and low-burdened for fast and accurate applications [21]. In this regard, different AI methods such as artificial neural networks [21], convolutional neural networks [22], logistic regression and AdaBoost [23], and recurrent neural networks (RNNs) [24] are deployed for fault detection, classification, and location. Among the AI methods, RNNs could obtain more accurate and robust results owing to their capability of interpreting the sequential dependencies of the measurement signals in power systems. Still, the data preparation stage in RNN implementation needs more attention, and the fine-tuning stage can also be challenging compared to other AI solutions. However, the isolated locality of the required fault detection unit forces high accuracy and single-sourced measurement. As discussed previously, employing the communication channels underrates the cyber-security of protection schemes, and acquiring different types of measurement increases the implementation cost. Therefore, a fast, reliable, and adapted AI-assisted fault detection and classification method is desired with a minimum number and types of measurements to minimize resilience enhancement costs.

TABLE 1. Research Gap

Reference Contribution	[3]	[6]	[13]	[14]	[17]	[21]	[24]	Proposed Method
Resilience Enhancement	✓	✓	✓	✓	×	×	×	✓
Fault Diagnosis	×	×	×	×	✓	✓	✓	✓
Surveillance Layer	×	×	×	×	×	×	×	✓
Protection-based	×	×	✓	×	✓	✓	✓	✓
DL-based	✓	✓	×	×	×	×	✓	✓
Single Measurement	×	×	×	×	×	×	×	✓
Isolated	×	×	×	×	✓	×	×	✓
Techno-Economic	×	×	×	✓	×	×	×	✓

Table 1 shows the research gap identified in the literature and presents the proposed solution of this study. The development of an isolated surveillance system with the aim of countering cyber-attacks in the final stage of CPPSs is crucial for enhancing the resilience of power systems. In contrast, Wilson et al. [3] and Moayyed et al. [6] focus on improving certain already-existing layers of CPPSs to enhance resilience. Meanwhile, the approach outlined by Choeum and Choi [12] introduces an additional layer among the typical layers; however, the integration of a surveillance system in the final stage of CPPSs has been overlooked. On the other hand, establishing such a layer requires the implementation of powerful fault detection methods. These methods should be capable of demonstrating high accuracy and operating effectively with a minimal variety and quantity of measurements, thereby ensuring cost efficiency. Although the new fault detection methods proposed in [17] and [21] demonstrate high accuracy, they rely on multiple types of measurements. Additionally, the developed method in [24] necessitates communication channels to enhance the accuracy of its fault detection method. The dependence on multiple types of measurements or communication channels diminishes their applicability for being used in this layer.

To address the discussed knowledge gap, this study introduces a local and hidden surveillant protection layer for transmission lines, specifically designed to enhance the resilience of CPPSs against FDIAs. The proposed layer functions at the final stage of a cyber-attack aiming at limiting the capability of the attacker to execute harmful protection actions. The proposed method employs fault detection and classification units (FDCUs) that utilize a deep-learning (DL) approach based on bidirectional long short-term memory (Bi-LSTM) model. These FDCUs are designed to operate using only current measurements from transmission lines connected to their respective installation buses.

These FDCUs play a surveillant role by executing online monitoring and rapid responses to various fault scenarios within a relatively short sampling window, employing the capability of the Bi-LSTM model in interpreting sequential data correlations. Furthermore, the situational awareness of the FDCUs is shared with neighboring buses through the deployment of the power-line-carrier (PLC) communication system whenever a malfunction or acceleration occurs in the main protection system. The operational expenses are increased by the installation of FDCUs on the buses of a CPPS. Therefore, a techno-economic tradeoff is established by the proposed framework through the employment of the evaluation based on distance from average solution (EDAS) method, which incorporates various attributes to identify the integration level of the FDCUs in the CPPS. In this regard, the most suitable candidate buses for FDCU installation are determined through an attack analysis that evaluates the potential impacts of cascading failures resulting from different cyber-attack target sets. The main contributions of this study include following.

1) A hidden surveillant protection layer is devised for enhancing CPPS resilience against cyber-attacks through the development of FDCUs.
2) A fast and accurate local DL-based FDCU is designed that utilizes only local transmission line current measurements to feed the Bi-LSTM model for fault detection and classification.
3) A proper scheme is considered to share the situational awareness of the FDCUs with neighboring buses whenever a malfunction or acceleration occurs in the main protection system.
4) A techno-economic framework is established to enhance the cyber-attack resilience considering the cost of FDCUs' integration based on the EDAS method.

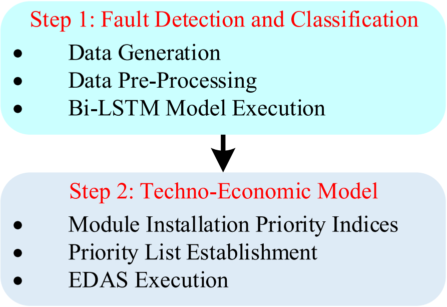

Step 1: Fault Detection and Classification
Data Generation
Data Pre-Processing
Bi-LSTM Model Execution
Step 2: Techno-Economic Model
Module Installation Priority Indices
Priority List Establishment
EDAS Execution

FIGURE 1. Workflow of the proposed method.

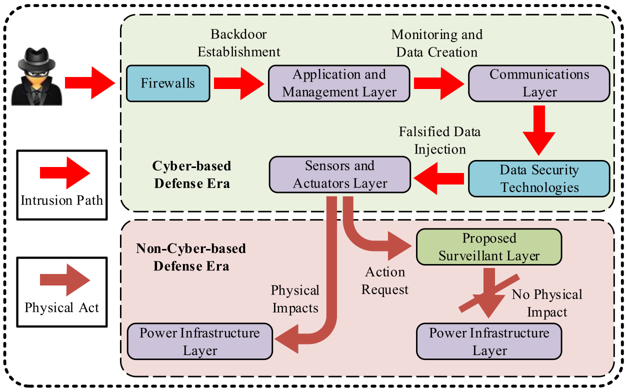

Backdoor Establishment
Monitoring and Data Creation
Firewalls
Application and Management Layer
Communications Layer
Falsified Data Injection
Cyber-based Defense Era
Sensors and Actuators Layer
Data Security Technologies
Intrusion Path
Non-Cyber-based Defense Era
Proposed Surveillant Layer
Action Request
Physical Impacts
No Physical Impact
Physical Act
Power Infrastructure Layer
Power Infrastructure Layer

FIGURE 2. Attack and defense processes.

The remainder of this article is organized as follows. Section II describes the backbone and main framework of the proposed model. Section III discusses the simulation cases and scenarios. Then, the obtained results are discussed in more detail. Eventually, Section IV concludes the article.

II. PROPOSED METHODOLOGY

The represented flowchart in Fig. 1 demonstrates the workflow of the proposed method. This section, first, gives an overall insight into the merit of the proposed surveillant protection layer. Next, explains the developed fault detection and classification method. Finally, the approach for resilience enhancement of the CPPS while satisfying the economic desires through the EDAS method is explained.

A. OVERALL INSIGHT ON THE PROPOSED LAYER

Although the DOE report recommends the employment of data management systems for the cyber-resilience of CPPSs [8], cyber intrusions via the communication layer are still probable. That is, protection schemes and strategies that partially or generally incorporate the communication layer are prone to penetration by more trained and capable attackers. As demonstrated in Fig. 2, if an attacker gains the ability to pass through the cyber-based defense mechanisms including firewalls and data security technologies of the application and management layer and the communications layer, it can launch a successful attack followed by harsh physical impacts.

Therefore, contemplating a noncyber-based defense mechanism as a last resort strategy makes sense to limit the ability of the attacker to physically damage the system.

A local, hidden, and surveillant transmission line protection layer for the resilience of CPPSs against FDIAs is presented in this study. The proposed layer stands in the last stage of an accomplished cyber-attack to interrupt the attacker's capability to perform undesired protection actions. The locality of the layer enhances the resilience of the CPPS by operating in parallel with the cyber-security layer and surveilling the main protection scheme. The proposed layer is comprised of FDCUs fed only by local transmission line current measurements to detect and classify electrical faults. Despite the local measurement system, the speed and accuracy of the FDCUs are guaranteed by using the Bi-LSTM model which is able to interpret the sequential dependencies of time-series data. On the other hand, the EDAS method balances the economic and technical resilience factors by determining the most deserving buses for FDCU installation and the integration level of the surveillance layer.

To apply the supervision of FDCUs on the main transmission line protection, the PLC system is employed. The operation of breakers in a FDCU-installed bus must be confirmed by the command of the FDCU. That is, FDCUs work in parallel with the main protection of the power system in a local manner. Let us consider three cases:

1) the occurrence of an internal fault detected by the main protection and FDCU;
2) the occurrence of an internal fault detected only by FDCU;
3) the occurrence of an FDIA.

In the first case, the main protection and FDCU detect the fault and send the trip signal resulting in a correct operation of the breaker. In the second case which may happen owing to many reasons such as highly resistive faults, special operational conditions, etc., the FDCU which is trained for various fault scenarios would correctly detect the fault and send the trip signal. In the third case, the main protection is compelled to send the trip signal based on the falsified data, but, the FDCU which uses local measurements does not detect any faults and does not send any trip signal. In this case, the breaker goes into the locked mode. Moreover, according to the demonstrated framework in Fig. 3, the far-end bus of each transmission line should also receive the confirmation signal of the FDCU carried by the PLC system to perform a breaking task. In the event of a false flag from the main protection, the FDCU is obligated to transmit alarm signals to the neighboring buses. Until all buses and consequently the central management unit receives the distress signal, the same task is done by each signal-received bus. Doing so, the main protection goes into the offline mode to apprehend the impact of the cyber-attack and terminate any redundant access points for the attacker. Meanwhile, the protection of the system is handled through the proposed supervisory layer by the corresponding FDCUs in a local manner. The main protection goes online after the detection and isolation of weak links. It is noteworthy that new expenses regarding the PLC system deployment are avoided owing to the fact that this system is already employed in the protection schemes.

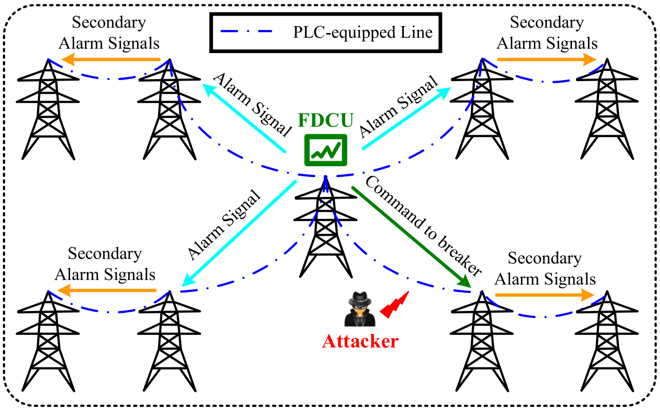


FIGURE 3. Role of PLC system in the proposed framework.

B. FAULT DETECTION AND CLASSIFICATION METHOD

The fault detection and classification context in power systems is a historical and well-studied field. However, the integration of renewable generations, employment of new power electronics-based technologies, and various operational issues raised by these devices introduce new challenges to the experts in this field. On the other hand, the manifestation and development of AI methods in the management, control, and protection of power systems have established a new substitute for the conventional methods. In this regard, many researchers have tried to reconstruct the power system applications and strategies, especially the protection section, based on AI methods. Here, a fault detection and classification method through the employment of a Bi-LSTM model is developed. The basis of the LSTM model, which is a special version of RNN, is previously provoked [25]. RNNs are a type of deep neural network that are capable of treating sequential data such as time series. They can extract features and learn from the data similar to other neural networks; except, they have the ability to learn from the sequential relations between the data points. But, in the conventional RNNs, as the number of time steps increases, the vanishing/exploding gradients issues emerge due to the inability of the early RNNs to keep up with the long-term dependencies. This issue renders legacy RNNs impractical for cases with long-term dependencies. However, the LSTM variation of RNNs is capable of retaining the long-term temporal dependencies of sequential data. The structure of an LSTM cell is represented in Fig. 4 and its equations for forward propagation are defined in the following:

$$\mathbf{i} = \text{sigmoid}\left(\mathbf{W_i h}^{(t-1)} + \mathbf{U_i x}^{(t)}\right) \tag{1}$$

$$\mathbf{f} = \text{sigmoid}\left(\mathbf{W_f h}^{(t-1)} + \mathbf{U_f x}^{(t)}\right) \tag{2}$$

$$\mathbf{o} = \text{sigmoid}\left(\mathbf{W_o h}^{(t-1)} + \mathbf{U_o x}^{(t)}\right) \tag{3}$$

$$\mathbf{g} = \tanh\left(\mathbf{W_g h}^{(t-1)} + \mathbf{U_g x}^{(t)}\right) \tag{4}$$

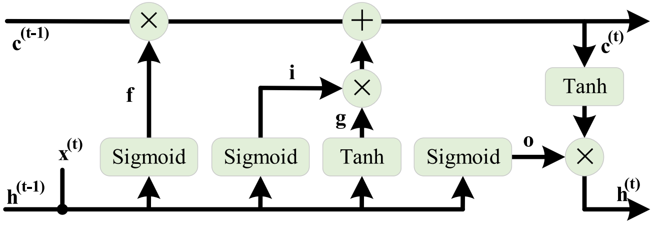


FIGURE 4. Structure of an LSTM cell.

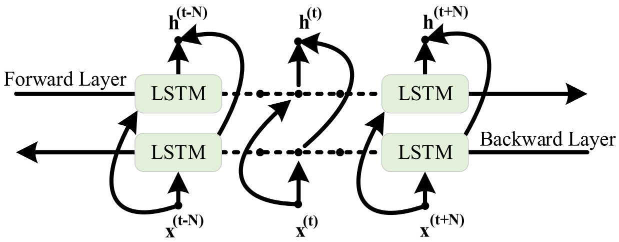


FIGURE 5. Graphical representation of a Bi-LSTM network.

$$\mathbf{c}^{(t)} = \left(\mathbf{c}^{(t-1)} \otimes \mathbf{f}\right) \oplus (\mathbf{g} \otimes \mathbf{i}) \tag{5}$$

$$\mathbf{h}^{(t)} = \tanh\left(\mathbf{c}^{(t)}\right) \otimes \mathbf{o}. \tag{6}$$

In these equations, **i**, **f**, **o**, and **g** stand for the input, forget, output, and internal hidden gates for the LSTM cell. Also, $(\mathbf{W_i}, \mathbf{U_i})$, $(\mathbf{W_f}, \mathbf{U_f})$, $(\mathbf{W_o}, \mathbf{U_o})$, and $(\mathbf{W_g}, \mathbf{U_g})$ are the weight matrices of hidden-hidden layers and input-hidden layers for input, forget, output, and internal hidden gates, respectively. The forward propagation equations are defined in (1)–(4). Moreover, (5) and (6) calculate the cell state and hidden state, respectively. It should be noted that LSTMs are also trained by BPTT similar to the other types of RNNs. For certain sequence prediction tasks, it can prove advantageous to enable the LSTM model to learn the input sequence in both forward and backward directions by the Bi-LSTM model, subsequently merging both interpretations. Fig. 5 shows a graphical representation of the Bi-LSTM architecture.

The input data considered to be fed into the Bi-LSTM model includes the fundamental component magnitudes and angles of the three-phase line currents connected to the considered bus. It can be obtained by applying the discrete Fourier transform (DFT) on the raw three-phase current signals. The fundamental component $\overline{I_1}$ of current I can be calculated by as [20]

$$\begin{aligned}\overline{I_1} &= \frac{2}{N}\sum_{k=0}^{N-1} i_k \exp\left(\frac{-2\pi jk}{N}\right) \\ &= \ldots \frac{2}{N}\sum_{k=0}^{N-1} i_k \cos\left(\frac{2\pi k}{N}\right) - j\frac{2}{N}\sum_{k=0}^{N-1} i_k \sin\left(\frac{2\pi k}{N}\right)\end{aligned} \tag{7}$$

here, if the first term is taken as I_c and the second term as I_s, the subsequent equation can be concluded as

$$\overline{I_1} = I_c + jI_s. \tag{8}$$

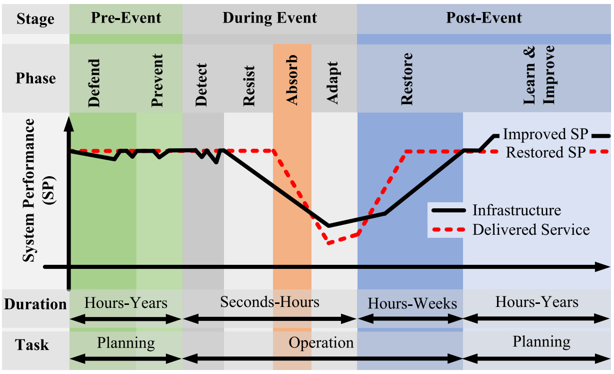


FIGURE 6. Fragility curve of a power system for infrastructure and service delivery [26].

Therefore

$$|I_1| = \left((I_c)^2 + (I_s)^2\right)^{1/2} \tag{9}$$

$$\angle\overline{I_1} = \tan^{-1}\left(-I_s/I_c\right). \tag{10}$$

By doing so, the proposed fault detection and classification method is robust to the harmonics-polluted measurements.

C. PROPOSED DECISION-MAKING APPROACH

The resilience of a CPPS in the proposed strategy is realized by adding a hidden surveillance transmission line protection layer into the set of layers. This surveillance layer works based on the proposed fault detection and classification method. By installing each individual FDCU in a candidate bus, its consequent awareness is partially propagated across the neighboring buses through the employment of PLC system which results in enhancing the resilience of the whole power system. According to the fragility curve of a power system shown in Fig. 6, the proposed approach improves the cyber-attack resilience of a CPPS in the "*Absorb*" stage. In the "*During Event*" level of a cyber-attack, the "*Detect*" and "*Resist*" stages are mostly performed by cybernetics security experts. However, the absorption of an attack can be carried out by performing offline countermeasures. In this stage, the impact of the cyber-attack and the ability of the attacker are restrained by employing the proposed FDCU and deploying awareness signals by the PLC system in the hidden layer.

According to the proposed decision-making approach for dispersing FDCUs of the presented layer, each bus is a candidate in the priority list. This priority list is built up based on prioritizing the buses with critical loads (CL). Then, the number of lost lines (NLL) in the event of the bus's disconnection, generator presence (GP) in the bus, and the number of lost generators (NLG) in the event of the bus's disconnection determine the priority of each bus. In the process of establishing the priority list, the main factor is the CL. Thereafter, if two buses have the same NLLs, the GP factor is the distinguishing one. The same goes for two buses with the same GPs where the NLG determines the significance. The NLL and the NLG indices are calculated based on the

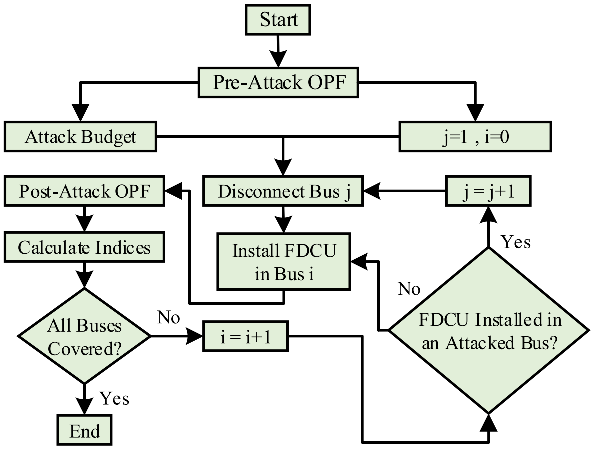


FIGURE 7. Flowchart of the attack-analysis procedure.

cascading outage calculations. After determining the priority of the buses for installing the FDCUs and by considering the priority of the attacker, namely the highest load-shedding (LS) value per attacked bus, and a hypothetical budget of the attacker, an attack-analysis procedure is carried out. According to Fig. 7, the attack analysis procedure commences with an optimal power flow (OPF) for the preattack condition. Then, according to the attack budget, the highest prioritized buses for attack are removed from the grid followed by the execution of an OPF in the postattack condition. Thereafter, at each iteration until the last bus, FDCUs are installed at the buses one by one according to the priority list (i) of the defender.

At each iteration of the attack-analysis procedure, the overall LS, the overall line congestion (LC), the overall reserve of generators (RG), the number of covered buses (NB) by the hidden layer, and the number of covered critical (NCC) loads are calculated and stored to be fed to the multi-attribute decision-making (MADM) model. The employed MADM method is the EDAS which has been previously applied to evaluate the airline services, air traffic, and staff choosing problems. The mathematical formulation of the EDAS method is emphasized as follows [27]. The input information of the EDAS method is called the decision matrix (D)

$$D = \begin{bmatrix} aa_{11} & \cdots & aa_{1j} & \cdots & aa_{1r} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ aa_{i1} & \cdots & aa_{ij} & \cdots & aa_{ir} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ aa_{l1} & \cdots & aa_{lj} & \cdots & aa_{lr} \end{bmatrix} \quad (11)$$

in which aa_{ij} is the ijth element of the decision matrix that represents the ith alternative for the jth attribute. Additionally, the decision maker provides attribute weights $W = \{w_1, w_2, \ldots, w_r\}$ which are discussed at the end of this section. Next, the average solution of each attribute is calculated

$$\mathrm{AVS}_j = \sum_{i=1}^{l} aa_{ij}/r\ ;\ j = 1, 2, \ldots, r. \quad (12)$$

The positive and negative distances from average solutions are calculated in the following based on the positivity or negativity of each attribute. The positive and negative distances from the average solution for positive attributes are

$$\mathrm{PDAVS}_{ij}^{P} = \max\left(0, \left(aa_{ij} - \mathrm{AVS}_j\right)\right)/\mathrm{AVS}_j \quad (13)$$

$$\mathrm{NDAVS}_{ij}^{P} = \max\left(0, \left(\mathrm{AVS}_j - aa_{ij}\right)\right)/\mathrm{AVS}_j. \quad (14)$$

Likewise, the positive and negative distances from the average solution for negative attributes are

$$\mathrm{PDAVS}_{ij}^{N} = \max\left(0, \left(\mathrm{AVS}_j - aa_{ij}\right)\right)/\mathrm{AVS}_j \quad (15)$$

$$\mathrm{NDAVS}_{ij}^{N} = \max\left(0, \left(aa_{ij} - \mathrm{AVS}_j\right)\right)/\mathrm{AVS}_j. \quad (16)$$

Considering the weight of each attribute, the weighted positive and negative distances of attributes from the average can be calculated by

$$\mathrm{WP}_i = \sum_{j=1}^{r} w_j \times \mathrm{PDAVS}_{ij}^{PorN} \quad (17)$$

$$\mathrm{WN}_i = \sum_{j=1}^{r} w_j \times \mathrm{NDAVS}_{ij}^{PorN}. \quad (18)$$

As the values of each attribute may differ in scale from others, normalization is suggested. Therefore, the weighted normalized positive and negative distances are calculated as

$$\mathrm{NWP}_i = \mathrm{WP}_i/\max_i\left(\mathrm{WP}_i\right) \quad (19)$$

$$\mathrm{NWN}_i = \mathrm{WN}_i/\max_i\left(\mathrm{WN}_i\right). \quad (20)$$

Now, the assessment score for each alternative is calculated based on NWP and NWN

$$\mathrm{AS}_i = \left(\mathrm{NWP}_i + \mathrm{NWN}_i\right)/2. \quad (21)$$

According to the descending order of assessment scores, the priority of alternatives can be obtained. The weights of each attribute W can be determined by various methods. In this study, the Entropy method is employed to govern the weights of the attributes. Initially, the normalized values of decision matrix elements are calculated

$$\overline{aa_{ij}} = aa_{ij}/\sum_{i=1}^{l} aa_{ij}. \quad (22)$$

The degree of entropy is computed by the following equation:

$$E_j = -1/\ln(l) \sum_{i=1}^{l} \overline{aa_{ij}} \times \ln\left(\overline{aa_{ij}}\right); \qquad 0 \le E_j \le 1. \quad (23)$$

Based on this equation, the deviation rate of the degree of entropy and the entropy weight of each attribute can be calculated as

$$\mathrm{Dev}_j = 1 - E_j \quad (24)$$

$$w_j = \mathrm{Dev}_j / \sum_{j=1}^{r} \mathrm{Dev}_j. \tag{25}$$

III. NUMERICAL STUDIES AND PERFORMANCE EVALUATIONS

This section is dedicated to reporting the numerical simulations and performance evaluation of the proposed surveillance transmission line protection layer. The impact of an FDIA is applied to the protection system of the testbed in this study.

A. TESTBED CHARACTERISTICS AND ASSUMPTIONS

Simulations are carried out on the IEEE 30-bus test system with some minor assumptions [28]. Four CLs are considered which are in buses 14, 17, 21, and 30. The attack budget is taken three bus-per-attack. Faulty and normal condition simulations and data generation for feeding the AI models are performed in the DigSILENT PowerFactory environment [29]. Moreover, Python software is employed to develop the Bi-LSTM model. Finally, the OPF simulations for the employed EDAS method are performed using the general algebraic modeling system studio 1.12.1 optimization environment.

In this study, two case studies are considered. At the outset, the efficiency of the proposed method is tested on only one of the buses of the testbed. In this regard, the performance of FDCU is explored based on different fault types, locations, and resistance in steady and power swing operational conditions of the power system. Afterward, in the next case, by dispersing the proposed FDCUs in the testbed based on the techno-economic model and employment of the PLC system, the performance of the surveillance layer is evaluated. In this case, the locations of FDCUs are determined by the EDAS method, and the resilience of the CPPS is investigated.

B. CASE 1: EVALUATION OF THE FDCU ON A SINGLE BUS

The proposed fault detection and classification method executes a Bi-LSTM model fed by the DFT-processed three-phase currents of the connected lines to the bus intended for FDCU installation. The raw data of three-phase currents of all lines are gathered; then, the fundamental component magnitudes and angles are extracted using (7)–(10). The developed module for fault detection and classification is considered to be installed in bus 6 with 5 transmission lines. This means that 30 features are fed into the Bi-LSTM model, including the amplitudes and angles of three-phase line currents. The fault detection model detects the normal or faulty conditions indicating the name of the faulty line. Therefore, in this model, six labels are created to show the normal and faulty states. Moreover, the fault classification model identifies the fault types illustrated in Fig. 8 with 11 labels for three-phase, two-phase, two-phase-ground, and one-phase-ground faults. A total of 2 million data points are generated by simulating normal state and 10 types of faults located in 0, 1, 2, . . ., 10, 20, . . ., 100% of 5 transmission lines considering 0, 1, 2, . . ., 10, 20, . . ., 100 Ω fault resistances in the steady state and power swing conditions. Each fault is simulated in a 100 msec period in which the fault is injected at 50 msec from the simulation initiation. The size of the samples used for training and testing the fault detection and classification which is determined by a trial-and-error procedure is five timesteps-per-sample. This resolution simultaneously provides high accuracy, affordable computational burden, and high detection and classification rates. The sampling frequency is 1 kHz which means timesteps are in 1 msec temporal distance.

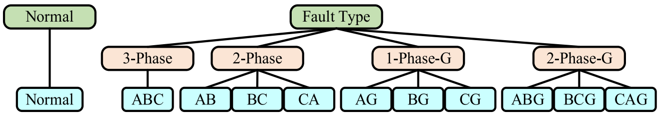


FIGURE 8. Fault type classes and labels.

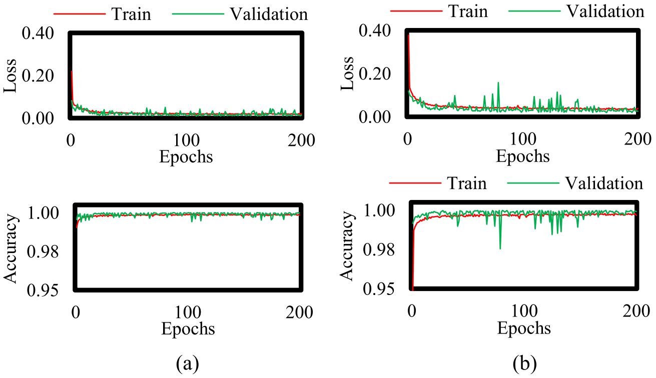
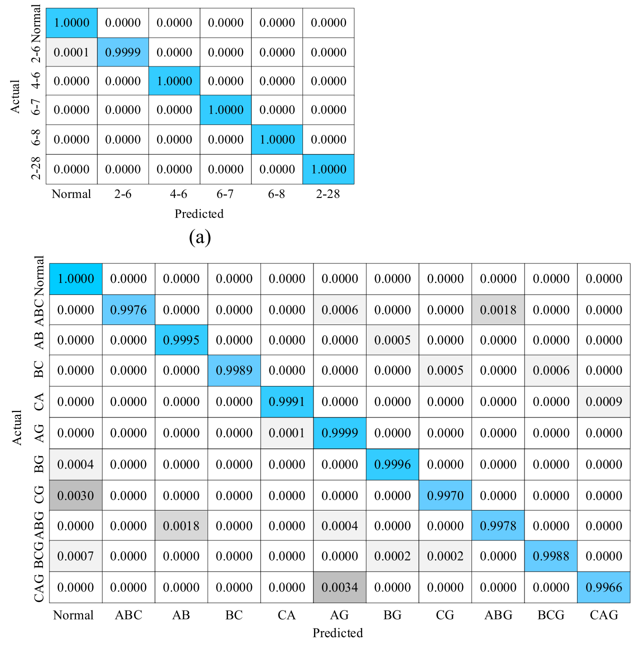


FIGURE 9. Learning and validation accuracies and losses of (a) fault detection and (b) fault type classification models.

The developed structures of Bi-LSTM models for fault detection and classification are the same. The model starts with a 30-neuron input layer. Three consecutive Bi-LSTM layers are stacked with 120, 60, and 30 LSTM cells, beginning after the input layer and ending at the output layer. The overfitting is evaded by a 50% recurrent dropout at each layer. Moreover, the L2 = 0.01 kernel regularization is contemplated for each layer to facilitate the optimal convergence of the model. The activation function of all three Bi-LSTM layers is "*tanh*" which is more stable compared to the "*Relu*" activation function, especially when recurrent dropout is used. Following these layers, an output layer with the "*Softmax*" activation function, 6 neurons for fault detection, and 11 neurons for fault classification models is added. The loss function of the model is the "*Categorical Cross-Entropy,*" and the adaptive moment estimation (*Adam*) optimizer is deployed as the optimization function with the default 0.001 learning rate. Moreover, 20% of the training data is split for validation. Also, 20% of the whole data is used for testing the model. The training process of each model is performed in 200 epochs with a batch size of 100 samples. Here, the training and validation accuracies and losses through the training processes of the detection and classification models are drawn in Fig. 9(a) and (b).



Actual \ Predicted	Normal	2-6	4-6	6-7	6-8	2-28
Normal	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000
2-6	0.0001	0.9999	0.0000	0.0000	0.0000	0.0000
4-6	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000
6-7	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000
6-8	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000
2-28	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000

(a)

Actual \ Predicted	Normal	ABC	AB	BC	CA	AG	BG	CG	ABG	BCG	CAG
Normal	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
ABC	0.0000	0.9976	0.0000	0.0000	0.0000	0.0006	0.0000	0.0000	0.0018	0.0000	0.0000
AB	0.0000	0.0000	0.9995	0.0000	0.0000	0.0000	0.0005	0.0000	0.0000	0.0000	0.0000
BC	0.0000	0.0000	0.0000	0.9989	0.0000	0.0000	0.0000	0.0005	0.0000	0.0006	0.0000
CA	0.0000	0.0000	0.0000	0.0000	0.9991	0.0000	0.0000	0.0000	0.0000	0.0000	0.0009
AG	0.0000	0.0000	0.0000	0.0000	0.0001	0.9999	0.0000	0.0000	0.0000	0.0000	0.0000
BG	0.0004	0.0000	0.0000	0.0000	0.0000	0.0000	0.9996	0.0000	0.0000	0.0000	0.0000
CG	0.0030	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.9970	0.0000	0.0000	0.0000
ABG	0.0000	0.0000	0.0018	0.0000	0.0000	0.0004	0.0000	0.0000	0.9978	0.0000	0.0000
BCG	0.0007	0.0000	0.0000	0.0000	0.0000	0.0000	0.0002	0.0002	0.0000	0.9988	0.0000
CAG	0.0000	0.0000	0.0000	0.0000	0.0000	0.0034	0.0000	0.0000	0.0000	0.0000	0.9966

(b)

FIGURE 10. **CM of fault (a) detection and (b) classification.**

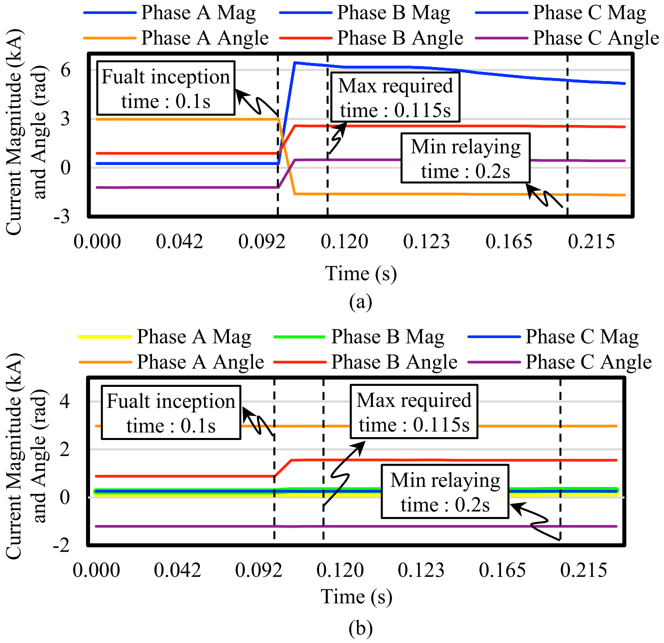


FIGURE 11. **Magnitudes and angles of all phases of lines 2–6 in the event of a (a) three-phase fault in 0% of the line with 0 Ω resistance and (b) a B-G fault in 80% of the line with 100 Ω resistance.**

After training both of the models for about 600 min, the testing stage is executed. As previously stated, 20% of all generated data is used in the testing stage. Considering the lower number of labels in the fault detection model compared to the fault classification model, the detection accuracy is obviously higher than that of classification. During the test process, two confusion matrices (CM) are created by evaluating the trained model based on the test data. Fig. 10 illustrates the CM for both fault detection and classification models using the concatenated steady and power swing conditions data. As seen in Fig. 10(a), the accuracy of the detection model is 100% for all labels except for one of them which is 99.99%. For the classification model, Fig. 10(b) shows that only the “*Normal*” label reaches 100% accuracy, and for other labels, lower accuracies are achieved.

Also, the lowest accuracy is obtained for the “*CAG*” label equal to 99.66%. It is noteworthy that the training process can be expanded to more epochs to achieve higher values of accuracy. It is noteworthy that the minimum operation time of relays is typically considered 100 msec. Considering the parallel operation of the detection and classification models in the FDCU, the 5 msec sampling window contemplated for the proposed model plus a maximum of 10 msec detection and classification times is considerably lower than the operation time of relays which can be seen in Fig. 11. According to the high current resulted from a near-end nonresistive three-phase fault in Fig. 11(a) and the considerably low current of a one-phase-to-ground fault in 80% of line with 100 Ω resistance in Fig. 11(b), the fault detection and classification by the proposed model is also impressively fast and accurate compared to conventional relaying characteristics.

The proposed fault detection and classification method uses only local current measurements at the installation buses of the FDCUs. Therefore, the proposed method relies solely on local current measurements obtained in the connected buses of the FDCUs. Although an increase in the number of connected lines to a bus may lead to longer training times and higher computational costs, this is not directly correlated with the overall scale of the power system. In practical applications, it is noted that the number of lines connected to any given bus is limited which mitigates the impact of the power system expansion on the training time and computational demands of the Bi-LSTM model. Therefore, despite an increase in the power system’s scale, a proportional increase in computational burden or training duration would not be anticipated.

C. CASE 2: EXPLORING THE TECNO-ECONOMIC APPROACH TO RESILIENCE ENHANCEMENT OF THE TEST SYSTEM

As comprehensively elaborated in Section II-B, FDCUs are required to be dispersed across the power system for constructing the surveillant protection layer hidden from the observation of any third party through communication channels. FDCU locations are determined based on the proposed decision-making approach. Table 2 shows the bus ranking according to their characteristics based on the specifications of the proposed strategy. The ranking of important buses is tabulated in Table 2. This table is organized based on the CL, NLL, GP, and NLG parameters. Thereafter, in the following, the attack priority list is determined based on the amount of LS caused by an accomplished attack on each individual busbar which is shown in Table 3.

TABLE 2. Ranking List of Buses

Rank	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Bus No.	21	30	14	17	6	12	10	2	27	1	22	15	4	28	24	25	9	8	7
CL	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
NLL	2	2	2	2	12	7	7	5	5	5	5	4	4	4	3	3	3	2	2
GP	-	-	-	-	-	-	-	*	-	*	*	-	-	-	-	-	-	-	-
NLG	1	1	0	0	1	1	1	1	1	2	1	0	1	0	0	1	0	0	0

TABLE 3. Attack Priority

Priority	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Bus No.	8	6	7	2	12	21	27	30	19	17	24	1	22	15	4	14	10	25	16
LS (MW)	30	23	22	21	19	17	13	11	10	9	9	8	8	8	8	6	6	3	3

TABLE 4. D Matrix of the EDAS Method

Cost	LS (MW)	LC (MW)	RG (MW)	NB	NCC
0, …, 3	70.3	722.028	216.1	0, 3, 6, 9, 11	0, 1, 2, 3
5, …, 7	74.5	953.526	220.3	18, 19, 20	4
8	62.3	1174.06	208.1	22	4
9, …, 17	35.8	1161.41	181.6	23, 24, 25, 26, 27, 27, 27, 27, 28, 29	4
18	16.5	1445.51	162.3	29	4
19	10.2	1397.02	156	29	4
20	9.9	1414.27	155.7	30	4
21	9.1	1211.1	154.9	30	4
22	8.3	1209.62	154.1	30	4
23	8.1	1409.04	153.9	30	4
24	5.7	1229.35	151.5	30	4
25	3.5	1197.23	149.3	30	4
26	3.5	1405.36	149.3	30	4
27	0	1416.06	145.8	30	4
28, …, 30	0	1497.7	145.8	30	4

TABLE 5. Entropy Weights of Each Attribute

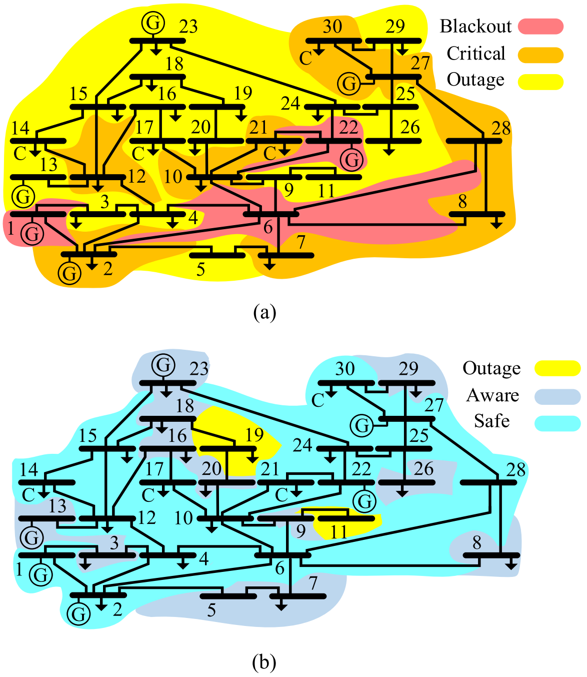
	Cost	LS	LC	RG	NB	NCC
Entropy Weight	0.2793	0.4774	0.0305	0.0148	0.1317	0.0663

In the next step, the D matrix elements provided for the EDAS method are calculated by the attack-analysis approach and brought in Table 4. In this table, when a bus is present at the target set in an iteration, the coverage list of the next iteration would be checked. If it is on the list, it should be removed from the target set and the next bus in the attack priority list must be added. The cost is determined by the number of installed FDCUs.

Afterward, the entropy weight of each attribute is calculated shown in Table 5. In the last step, the resulting priority of the coverage level for installing FDCUs of the hidden supervisory protection layer from the EDAS method is calculated and brought in Table 6. This table indicates that covering 16 buses is sufficient for balancing the economic and technical resilience aspects. Doing so, a total of 28 buses are either surveilled or made attack-aware, and all four critical-loaded buses are supervised by FDCUs. Consequently, if a cyber-attack occurs, the LS is reduced by 49.07%, the total LC is lowered by 60.85%, and the total RG is increased by 15.96% through the employment of the proposed method.

TABLE 6. Priority List for the Coverage Level of the Layer

Rank	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Coverage	16	15	17	14	18	13	12	11	10	19	9	20	21	22	23	24	25	8	7



(a)

(b)

FIGURE 12. Resilience state of the system against cyber-attacks (a) without and (b) with the proposed supervisory layer.

Fig. 12 shows the resilience state of the test system in the event of accomplished cyber-attacks. According to Fig. 12(a), an attack on red-colored areas results in severe cascading outages in the system followed by a probable blackout of the whole system. An attack on critical buses may cause some outages, but a blackout is not expected. Moreover, cyber-attacks on the buses in the outage category only cause the outage of those individual buses. On the contrary, Fig. 12(b) illustrates a tremendous improvement in the state of the system. As can be seen, only two low-rank buses are not covered by the proposed surveillant transmission line protection layer. Furthermore, the aware category stands for the buses without FDCU but in the vicinity of a surveilled bus. These buses do not benefit from the proposed fault detection and classification method, but in the event of an attack, the surveilled bus alerts them. Finally, the safe area is composed of FDCU-surveilled buses that do not get affected by cyber-attacks on the transmission line protection system.

TABLE 7. Performance Comparison for Fault Detection and Classification Methods

Parameter \ Reference	[21]	[22]	[23]	Proposed Method
Min Accuracy (%)	99.4	98.4	98.75	99.66
Max Accuracy (%)	99.8	100	99.29	100
Detection Time (ms)	20	8	23	10
Measurement	V (PMU)	V, I (Local)	V, I (Local)	I (Local)

D. RESULTS VALIDATION

In this section, to validate the obtained results, first, the performance of the proposed fault detection and classification models is compared to other developed AI-based methods. Then, in order to explore the scalability of the proposed surveillant layer in larger CPPSs, another analysis is conducted on a larger power grid which requires a wider range of FDCU installation. Finally, the effect of harmonics on the performance of the FDCUs is evaluated based on different harmonic levels. It should be emphasized that the performance of AI-based methods can be assessed through the comparison of their numerical indices, speed, and required inputs. By doing so, the suitability of these types of methods for detection and classification in different conditions of the electrical grid and different arrangements of system components can be revealed.

At the outset, a comparative analysis of AI-based fault detection and classification methods is carried out which compares the accuracy, required measurements, and detection time of the proposed model with those in the literature [21], [22], [23]. The reflected results in Table 7 demonstrate that the detection and classification accuracies achieved by the proposed method are higher than those of other studies. It is essential to point out that the proposed fault detection and classification method uses only local current measurements at the installation buses of the FDCUs. Therefore, the proposed method relies solely on local current measurements obtained in the connected buses of the FDCUs. Moreover, Tokel et al. [21] states that the detection time of its model is 20 ms; however, for Fahim et al. [22] and Baloch and Muhammad [23] only the sampling rates are expressed as 20 and 3.6 kHz which stand for 3 and 17 ms sampling times. In this article, the detection interval is 5 ms which is also added to the sampling times of other methods for making a fair comparison. Therefore, the detection time of the Bi-LSTM model which is 10 ms outperforms the models in [21] and [23]. Overall, the proposed fault detection and classification method shows a higher performance compared to the majority of other methods in accuracy, measurement requirements, and detection time.

In order to explore the scalability of the proposed surveillant layer, the IEEE 118-bus testbed [30] is put under investigation. In this regard, loads connected to buses 42, 90, 95, 112, and 116 are considered CLs. Similar to the main case study, the attack budget is taken three buses per attack. By preparation of the input data for the EDAS method, the developed model is executed. The obtained results are shown in Table 8 which indicates that the installation of FDCUs in 60 buses or 50.84% of the system covers 117 buses or 99.15% of the system. Moreover, the employment of the proposed layer in this level results in a 69.15% reduction in overall shed load, a 38% reduction in overall congestion of transmission lines of the system, and a 2.5% increment in overall reserve generation in the event of an attack compared to the base case. According to the results obtained from simulations on the IEEE 30-bus and IEEE 118-bus testbeds, the growth in the size of the network does not sensibly affect the performance of the proposed framework in the resilience of the system.

TABLE 8. Optimal Dispersion Level of the Surveillant Layer for IEEE 118-Bus Testbed

Case \ Parameter	Cost	NB	NCC
Base Case	0	0	0
Optimal Case	60	117	5
Case \ Parameter	LS (MW)	LC (MW)	RG (MW)
Base Case	645	4394.56	17817.6
Optimal Case	207	2726.26	17371.6

TABLE 9. Performance Comparison for Fault Detection and Classification Models in Different THD Levels

THD \ Model	Fault Detection Accuracy	Fault Classification Accuracy
5.3%	99.99%	99.66%
15.6%	99.98%	99.64%
21.2%	99.98%	99.63%
24.8%	99.97%	99.62%

Finally, herein, a suitable analysis is performed to evaluate the performance of the fault detection and classification models for different harmonics levels. The obtained results are reflected in Table 9. The total harmonic distortion (THD) is calculated [23] for different simulated harmonic levels of the transmission line currents for different fault scenarios. As it can be interpreted from the detection and classification accuracies higher than 99.62% in different THD levels, the proposed FDCU is highly robust to the harmonics of the current measurements. It is noteworthy that the reduction in the accuracy is related to the faults with very low currents resulting from their high distance from the measuring point and highly resistive nature.

IV. CONCLUSION

This article aimed to address the drawbacks of cyber-based defense mechanisms against cyber-attacks on CPPSs through the development of a power system protection-based cyber-attack-resilience framework. The security and privacy of the proposed framework were guaranteed through the employment of a highly accurate Bi-LSTM model fed by local transmission line current measurements of each FDCU-installed bus with a relatively low sampling window. Awareness of FDCUs was propagated across the CPPS by deploying the

PLC system, further enhancing the resilience of power system protection. Since implementing FDCUs in the power system entails additional expenses, the EDAS method was executed to determine the most to the least commendable buses of the CPPS and reach a balance among economic and technical attributes of power system resilience. Doing so, 16 buses or 53.34% of the IEEE 30-bus test system were chosen for FDCU installation which resulted in an awareness of 93.33% or 28 buses, 49.07% of LS reduction, 60.85% of line reserve capacity increment, and 15.96% of generation reserve increment compared to the no FDCU condition in the base case. It is noteworthy that the Bi-LSTM model achieved an accuracy of at least 99.66% in transmission line fault detection and classification with a maximum operation time of 15 ms.

The current study assumes that PLC systems can handle electromagnetic interferences (EMIs) effectively. However, EMIs can pose significant challenges for PLC systems, particularly when the PLC system lacks the capability to manage such disturbances. In situations where the PLC is unable to handle EMI effectively, this issue requires further investigation for future work, especially in the context of the proposed deep learning-based surveillant protection layer.

REFERENCES

[1] M. Izadi, S. H. Hosseinian, S. Dehghan, A. Fakharian, and N. Amjady, "A critical review on definitions, indices, and uncertainty characterization in resiliency-oriented operation of power systems," *Int. Trans. Elect. Energy Syst.*, vol. 31, no. 1, pp. 1–28, 2021, doi: 10.1002/2050-7038.12680.

[2] V. Venkataramanan, A. Srivastava, A. Hahn, and S. Zonouz, "Enhancing microgrid resiliency against cyber vulnerabilities," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting*, 2018, pp. 1–8, doi: 10.1109/IAS.2018.8544667.

[3] D. Wilson, Y. Tang, J. Yan, and Z. Lu, "Deep learning-aided cyber-attack detection in power transmission systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2018, pp. 1–5, doi: 10.1109/PESGM.2018.8586334.

[4] S. Mousavian, J. Valenzuela, and J. Wang, "A probabilistic risk mitigation model for cyber-attacks to PMU networks," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 156–165, Jan. 2015, doi: 10.1109/TPWRS.2014.2320230.

[5] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Attack-resilient measurement design methodology for state estimation to increase robustness against cyber attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2016, pp. 1–5, doi: 10.1109/PESGM.2016.7741979.

[6] H. Moayyed, A. Moradzadeh, B. Mohammadi-Ivatloo, A. P. Aguiar, and R. Ghorbani, "A cyber-secure generalized supermodel for wind power forecasting based on deep federated learning and image processing," *Energy Convers. Manage.*, vol. 267, 2022, Art. no. 115852, doi: 10.1016/j.enconman.2022.115852.

[7] A. Moradzadeh, M. Mohammadpourfard, I. Genc, Ş. S. Şeker, and B. Mohammadi-Ivatloo, "Deep learning-based cyber resilient dynamic line rating forecasting," *Int. J. Elect. Power Energy Syst.*, vol. 142, 2022, Art. no. 108257, doi: 10.1016/j.ijepes.2022.108257.

[8] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec. 2011, doi: 10.1109/TSG.2011.2160000.

[9] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 244–249, doi: 10.1109/smartgrid.2010.5622049.

[10] P. Wang and M. Govindarasu, "Multi intelligent agent based cyber attack resilient system protection and emergency control," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, 2016, pp. 1–5, doi: 10.1109/ISGT.2016.7781267.

[11] S. Hasan, A. Dubey, G. Karsai, and X. Koutsoukos, "A game-theoretic approach for power systems defense against dynamic cyber-attacks," *Int. J. Elect. Power Energy Syst.*, vol. 115, 2020, Art. no. 105432, doi: 10.1016/j.ijepes.2019.105432.

[12] D. Choeum and D. H. Choi, "Trilevel smart meter hardening strategy for mitigating cyber attacks against Volt/VAR optimization in smart power distribution systems," *Appl. Energy*, vol. 304, 2021, Art. no. 117710, doi: 10.1016/j.apenergy.2021.117710.

[13] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2019, doi: 10.1109/TII.2018.2884728.

[14] U. Shahzad, "Economic impact assessment of cyber attacks on the smart power system," *J. Elect. Eng., Electron., Control Comput. Sci.*, vol. 8, no. 2, pp. 39–46, 2022.

[15] I. Mousaviyan, S. G. Seifossadat, and M. Saniei, "An ultra-high-speed algorithm for fault classification in double circuit transmission lines using only the first group of received current traveling waves," *Electric Power Syst. Res.*, vol. 206, 2022, Art. no. 107841, doi: 10.1016/j.epsr.2022.107841.

[16] W. Fan and Y. Liao, "Wide area measurements based fault detection and location method for transmission lines," *Protection Control Modern Power Syst.*, vol. 4, no. 1, pp. 1–12, 2019, doi: 10.1186/s41601-019-0121-9.

[17] X. Tong and H. Wen, "A novel transmission line fault detection algorithm based on pilot impedance," *Electric Power Syst. Res.*, vol. 179, Jun. 2019, Art. no. 106062, doi: 10.1016/j.epsr.2019.106062.

[18] B. Taheri and S. A. Hosseini, "Detection of high impedance fault in DC microgrid using impedance prediction technique," in *Proc. 15th Int. Conf. Protection Automat. Power Syst.*, 2020, pp. 68–73, doi: 10.1109/IPAPS52181.2020.9375543.

[19] M. A. Jarrahi, H. Samet, and T. Ghanbari, "Fast current-only based fault detection method in transmission line," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1725–1736, Jun. 2019, doi: 10.1109/JSYST.2018.2822549.

[20] B. R. Kumar, A. Mohapatra, S. Chakrabarti, and A. Kumar, "Phase angle-based fault detection and classification for protection of transmission lines," *Int. J. Elect. Power Energy Syst.*, vol. 133, 2021, Art. no. 107258, doi: 10.1016/j.ijepes.2021.107258.

[21] H. A. Tokel, R. Al Halaseh, G. Alirezaei, and R. Mathar, "A new approach for machine learning-based fault detection and classification in power systems," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, 2018, pp. 1–5, doi: 10.1109/ISGT.2018.8403343.

[22] S. R. Fahim, Y. Sarker, S. K. Sarker, M. R. I. Sheikh, and S. K. Das, "Self attention convolutional neural network with time series imaging based feature extraction for transmission line fault detection and classification," *Electric Power Syst. Res.*, vol. 187, 2020, Art. no. 106437, doi: 10.1016/j.epsr.2020.106437.

[23] S. Baloch and M. S. Muhammad, "An intelligent data mining-based fault detection and classification strategy for microgrid," *IEEE Access*, vol. 9, pp. 22470–22479, 2021, doi: 10.1109/ACCESS.2021.3056534.

[24] W.-H. Kim, J.-Y. Kim, W.-K. Chae, G. Kim, and C.-K. Lee, "LSTM-based fault direction estimation and protection coordination for networked distribution system," *IEEE Access*, vol. 10, pp. 40348–40357, 2022, doi: 10.1109/ACCESS.2022.3166836.

[25] B. Jason, "Predict the future with MLPs, CNNs and LSTMs in Python," *Deep Learn. Time Ser. Forecasting*, vol. 1, no. 1, pp. 1–50, 2018.

[26] A. M. Stankovic et al., "Methods for analysis and quantification of power system resilience," *IEEE Trans. Power Syst.*, vol. 38, no. 5, pp. 4774–4787, Sep. 2023, doi: 10.1109/TPWRS.2022.3212688.

[27] S. Pal and A. Gulli, *Deep Learning With Keras: Implement Various Deep-Learning Algorithms in Keras and See How Deep-Learning Can be Used in Games*. Birmingham, U.K.: Packt Publishing Ltd., 2017.

[28] M. Shahidehpour and Y. Wang, "Appendix C: IEEE-30 bus system data," in *Communication and Control in Electric Power Systems: Application of Parallel and Distributed Processing*. New York, NY, USA: Wiley-IEEE Press, pp. 493–495, 2005, doi: 10.1002/0471462926.app3.

[29] DigSILENT GmbH, PowerFactory, Gomaringen, Germany. [Online]. Available: https://www.digsilent.de

[30] M. M. Emam, E. H. Houssein, M. A. Tolba, M. M. Zaky, and M. H. Ali, "Application of modified artificial hummingbird algorithm in optimal power flow and generation capacity in power networks considering renewable energy sources," *Sci. Rep.*, vol. 13, no. 1, 2023, Art. no. 21446, doi: 10.1038/s41598-023-48479-6.