A Feasibility Area Approach for Early Stage Detection of Stealthy Infiltrated Cyberattacks in Power Systems

Ahmed Abd Elaziz Elsayed, *Member, IEEE*, Hadi Khani, *Member, IEEE*, and Hany Essa Zidan Farag, *Senior Member, IEEE*

***Abstract*— Advanced stealthy cyberattacks are capable of infiltrating the cybersecurity layers of power grids and alter their operating conditions, resulting in adverse effects on the system performance. Detecting such Stealthy Infiltrated Cyberattacks (SICA) at the earliest opportunity becomes crucial in order to enable power system operators to implement appropriate corrective measures. To that end, this paper proposes the addition of a new cybersecurity layer for SICA after they have broken through existing cyberattack prevention layers. The paper develops the Feasibility Area (FA) as a classifier mechanism to detect SICA in the collected data of Power System State Variables (PSSV). The proposed detection layer consists of two computational stages. The first stage involves estimating the FA parameters through a historical window of data over a specified period of time, which is then inputted to the second stage. In the second stage, the position of each PSSV with respect to the estimated FA is assessed and utilized by the SICA detection mechanism to identify broken through attacks. A flag vector is created indicating the location of each PSSV with respect to the defined FA. The location of each PSSV and its pattern represented in the flag vector are utilized to identify the existence of SICA. Various SICA detection mechanisms using mathematical techniques and the Pattern Recognition Neural Network (PRNN) have been applied. The numerical results from the evaluation of the proposed FA approach demonstrate a promising performance in detecting the SICA using the proposed method.**

***Index Terms*— Cybersecurity, false data injection, stealthy infiltrated attacks, bad data detection layer, feasibility area, pattern recognition neural network.**

NOMENCLATURE

A. Notation	
R	Real component.
I	Imaginary component.
HL	Healthy operation.
A	Attacked operation.
B. Indices	
t	Index of time interval.
n	Index of PSSV.
b	Index of power system bus.
C. Sets	
H_D	Set of deterministic FA classes.
H_{ND}	Set of non-deterministic FA classes.
H	Set of FA classes.
S	Set of PSSV samples for the data window.
τ^{HL}	Set of historical healthy operation data.
τ^{A}	Set of historical attack operation data.
$\mathbb{T}$	Set of simulation time step.
$\mathbb{T}^D$, $\mathbb{T}^G$	Set of time steps for adjustable load/ generation.
$\mathbb{B}$	Set of power system buses.
D. Parameters	
ψ	Bad data detection and FA-based SICA detection mechanisms threshold values.
M	FA window size.
$c_1 - c_4$	Cost function coefficients for generation unit.
Δt	Simulation time step (hr).
E. Variables	
γ	Normalized Residual.
z	Field measurements.
$\widehat{z}$	Estimated measurements.
h_{Rec}	Rectangular FA classifier.
h_{Cir}	Circular FA classifier.
h_{Ell}	Elliptic FA classifier.
h_{CH}	Convex-Hull FA classifier.
$\mathscr{L}_S(h)$	Binary empirical loss of Classifier h using Samples S.
$x_{n,t}$	PSSV n at Time t.
r_n	Circular FA classifier radius of PSSV n at Time t.
$X_{n,Cen}$	Circular FA classifier center of PSSV n at Time t.
A_n	Elliptic FA classifier shape matrix of PSSV n at Time t.
C_n	Elliptic FA classifier center matrix of PSSV n at Time t.
$TP_{h,n}$	True positive value of the PSSV n using FA Classifier h.
$FN_{h,n}$	False negative value of the PSSV n using FA Classifier h.
AO, HO	Ratio parameters for attacked and healthy operation.
$Fg_{h(n,t)}$	Flag value of the PSSV n at Time t using FA Classifier h.
$FAUR_{h,t}$	FA Classifier h uncertainty ratio at Time t.
$Al(t)$	FA-based SICA detection alarm at Time t.

Manuscript received 16 October 2023; revised 29 February 2024 and 26 May 2024; accepted 18 June 2024. Date of publication 27 June 2024; date of current version 3 July 2024. This work was funded by the Natural Science and Engineering Resources Canada (NSERC). The associate editor coordinating the review of this article and approving it for publication was Dr. Erisa Karafili. *(Corresponding author: Ahmed Abd Elaziz Elsayed.)*

The authors are with the Department of Electrical Engineering and Computer Science, Lassonde School of Engineering, York University, Toronto, ON M3J 1L4, Canada (e-mail: elsayed7@yorku.ca; hefarag@yorku.ca).

Digital Object Identifier 10.1109/TIFS.2024.3420075

$WSR_{h,t}$	FA Classifier h weighted sum ratio at Time t.
$w_{h,n}$	Weight of PSSV n for the FA Classifier h.
G_h	FA Classifier h overall gain.
W_{Li}	FA-PRNN Layer i weight matrix.
A_{Li}	FA-PRNN Layer i unactivated output.
N_{Li}	FA-PRNN Layer i number of neurons.
B_{Li}	FA-PRNN Layer i bias.
Z_{Li}	FA-PRNN Layer i activated output.
W	Feasibility area PSSVs weight vector.
$v_{t,b}$, $v_{t,b'}$	Voltage of Bus b and adjacent Bus b' at Time t (p.u.).
$P_{t,b}$, $P_{t,bb'}$	Injected/Branch power at Bus b/b to Bus b' at Time t (p.u.).
$G_{bb'}$, $B_{bb'}$	Conductance and susceptance of Branch bb' (p.u.).
$\theta_{bb'}$	Angle difference between Bus b and adjacent Bus b' at Time t (p.u.).
$P_{t,b}^{Dad}$, $P_{t,b}^{Gad}$	Demand/generation at Bus b at Time t (p.u.).
Z_t	State estimation measurement vector at Time t.
X_t	State estimation state vector at Time t.
J, e_t	State estimation Jacobian matrix and error vector at Time t.
a_t, C_t	State estimation attacked measurements and state variation vectors at Time t.

I. Introduction

A. Background and Motivation

THE aging infrastructures in power systems are being modernized throughout the grid that would enable two-way communications between consumers and energy providers. Active information exchange between various assets of the grid and customer-owned Distributed Energy Resources (DERs) can enhance the overall system performance [1]. Advanced Metering Infrastructure and two-way communications are the main pillars of the so-called modern power systems. Utilization of these advanced technologies, however, opens the door for cyberattacks [2]. Based on the industrial cybersecurity reports, over half of the industrial companies in 21 countries suffered from cyberattacks in 2019-2020 [3]. Cyberattacks on the critical infrastructure of energy systems are considered to be the most vital threat [4], [5].

Cybersecurity issues in power systems have been widely studied in the literature considering attacks against physical assets, networks, and communication systems. Among all types of attacks, False Data Injection Attacks (FDIA) are considered to be the most complex and common type due to its ability to mask the power system normal operation behavior by manipulating the state vector and sneaking through the Bad Data Detection (BDD) layer [6].

Research on the FDIA in power grids can be divided into three key areas: attack formulation, attack targets, and defense mechanisms. FDIA can be categorized into two main types: basic and stealthy. Basic attacks, conducted by attackers with limited knowledge, are typically easier to counter using traditional BDD layers. In contrast, stealthy attacks, orchestrated by skilled attackers with critical network information, pose a greater challenge as they can conceal their activities and bypass existing security layers [7]. Regarding attack targets, FDIA aims to impact the economic and/or stability aspects of power systems. Economic impact studies explore how FDIA manipulates various factors such as system topology, protection systems, market prices, and measurement data to undermine the system profitability [8], [9], [10]. On the other hand, stability impact studies focus on FDIA that target field-measured data, which can lead to instability problems. These issues include adverse effects on generation scheduling, load shedding, Automatic Generation Control (AGC) malfunctions, Load Frequency Control (LFC), electric vehicle grid vibrations, and secondary voltage controller performance in power grids [11], [12], [13], [14]. In recent years, research efforts have been predominantly directed towards addressing basic and stealthy cyberattacks on the active shared information between the power system and the central control unit. The primary goal has been to thwart these attacks and prevent them from manipulating the system. However, a fundamental research query remained unanswered. Even with cybersecurity prevention layers in place, these layers cannot guarantee 100% accuracy in preventing all cyberattacks. Consequently, certain stealthy cyberattacks manage to infiltrate these layers and impact the system. Hence, there arises a necessity for a framework capable of detecting Stealthily Infiltrated Cyberattacks (SICA). The next section provides a review on the works related to the defence mechanisms of FDIA and highlights research gaps in addressing SCIA.

B. Related Work

Defense mechanisms against FDIA can be developed using model-based techniques, data-driven approaches, or a combination of both [15], [16], [17]. Model-based techniques involve estimating the power system's state using static or dynamic state estimation methods and then subjecting the estimated state to detection tests like the Euclidean distance test or Chi-square test to identify potential FDIA [18]. In [19], a hierarchical knowledge-sharing algorithm utilizing Phasor Measurement Units (PMUs) measurements are employed to facilitate secure decentralized state estimation and residual calculation. This distributed process is subsequently complemented by a centralized FDIA detector to protect the power system against the FDIA. In [20], dynamic state estimation is proposed to detect cyberattacks using stochastic unknown inputs presented by output power variations of the renewable energy sources and power demand fluctuations caused by the stochastic behavior of customers.

Data-driven techniques, on the other hand, leverage historical data without requiring detailed system parameters. They include supervised and unsupervised machine learning methods such as Support Vector Machine (SVM) and Artificial Neural Networks (ANN), K-means, and Fuzzy clustering for FDIA detection [21], [22], [23], [24]. A linear combined multikernel with multifusion SVM supervised machine learning is employed in [21] for the detection of stealthy FDIA. This approach relies on PMUs measurements along side with state estimation to create labeled data and features extraction under both the healthy and attacked data types, which is used to

TABLE I
SUMMARY OF THE LITERATURE REVIEW

Reference	BDD	Primary Information cybersecurity		Secondary Information cybersecurity		SICA	FDIA Modeling
		Model Base	Data Driven	Model Base	Data Driven		
[5],[9]	✓	✓	✗	-	-	✗	✗
[10]	✗	-	-	✓	✗	✗	✓
[6],[18]–[20]	✓	✓	✗	-	-	✗	✓
[12],[21],[23]	✓	✗	✓	-	-	✗	✓
[14]	✗	-	-	✗	✓	✗	✓
[15]	✓	-	-	✓	✗	✗	✓
[16]	✗	✗	✓	-	-	✗	✗
[22]	✓	✗	✓	✗	✓	✗	✗
[24]–[25]	✗	-	-	✗	✓	✗	✓
[26]–[27]	✓	✓	✓	-	-	-	✓
Proposed	✓	✗	✓	✗	✓	✓	✓

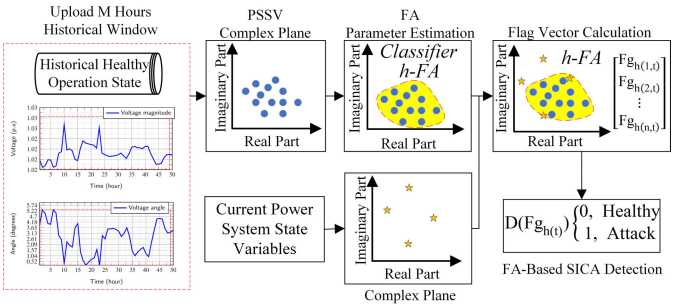


Fig. 1. Process of the proposed SICA detection layer.

train the model. The model exhibits a detection accuracy of 95.6%, however, it faces notable challenges in distinguishing between various anomalies, including those associated with stealthy FDIA, system failures and line outages. In [24], a hybrid approach involving fuzzy logic and ANN is employed to detect FDIA during dynamic LFC operations, considering renewable energy integration. Initially, a fuzzy layer processes input data from multiple LFC areas to identify unrealistic changes. Subsequently, an ANN is employed to detect variations and FDIA across various measurement samples. While the method achieves a high detection accuracy of up to 95%, the performance of the method varies significantly with changes in the fuzzy rules and membership functions. In [25], unsupervised machine learning techniques are employed for electricity imbalance detection using data from advanced meter infrastructure. A wavelet-based feature extraction method is utilized to extract data window features, which are then inputted into Fuzzy C-Means (FCM) clustering. Anomaly scores are generated based on the degree of cluster membership information produced by the FCM clustering to identify abnormal patterns. However, this approach has several limitations since it requires a significant number of smart meters for each consumer. Hybrid model and data-driven FDI detection approaches are presented in [26] and [27], utilizing distributed state estimation for the local area, and the local state estimation output is used as a trained data set for the ANN to detect stealthy FDIA in different areas.

Previous research works have given particular emphasis on improving the efficacy of cybersecurity detection algorithms with the aim of blocking a higher percentage of upcoming FDIA. However, even with the recent advancements in real-time detection algorithms, it is not guaranteed to fully protect the system against all future attacks since there is always a possibility that some of these attacks infiltrate through and manipulate the Power System State Variables (PSSV). Detecting such SICA at the earliest opportunity becomes crucial in order to enable power system operators to implement appropriate corrective measures. To alleviate the potential long-lasting impacts of SICA, e.g., system stability and economic factors, there is a paramount need to incorporate additional layers of cybersecurity that are able to store and analyze the system states over a specified period of time against past occurred and infiltrated attacks [28], [29]. To the best of the authors' knowledge, previous works have not given careful attention to the development of such post-occurrence detection mechanisms for SICA; putting the overall reliability and financial viability of the power system under a major risk. Table I provides a summary of previous efforts aimed at detecting stealthy FDIA in both the primary and secondary information, including the models and/or data-driven approaches. As shown in the table, several works have adopted model and data-driven techniques to detect FDIAs. This paper specifically focuses on detecting SICA, i.e., attacks that bypass the implementer BDD and modeler/data-driven base detection layer(s), using a novel FA-based data-driven approach.

C. Contribution

To fill in the identified research gap, this paper proposes the incorporation of an additional layer for SICA detection in the cybersecurity of power systems. The objective of this additional layer is to effectively detect the past occurred and infiltrated stealthy attacks via performing deep analytic of the collected and stored system states over a specific period of time. The concept of Feasibility Area (FA), which identifies the region where each PSSV stays under normal operating conditions, is introduced in this paper as a novel and superior mechanism to detect the SICA. Fig. 1 depicts the process of the proposed SICA detection layer, which is structured as a two-step cascaded process. In the initial stage, named FA-parameter estimation, a historical healthy window spanning M hours is uploaded for each PSSV and is represented within the complex plane. This representation serves as input for the FA parameter estimation, where classifier parameters are derived to define the normal operation region, representing the typical existence of PSSVs. Simultaneously, the current PSSVs at Time t are also mapped onto the complex plane, and their positions relative to the FA of each Classifier h are assessed. A flag vector is subsequently computed, indicating which PSSVs reside within the normal operation zone. This flag vector becomes integral to the second stage FA-Based SICA detection mechanism, where it is employed to make a final determination regarding the system state, particularly assessing whether SICA has impacted the ongoing system operation. This dual-stage process leverages historical and real-time information to effectively detect and respond to potential SICA-induced deviations from the normal operational state. In the previous work [29], the definition of the SICA problem is given and introduced the concept of the FA. This paper aims to extend the preliminary work presented in [29] via the following: 1) presenting the detailed mathematical formulation and implementation mechanism of the FA framework, along with proposing SICA detection mechanisms,

2) offering a mathematical model to estimate the SICA by integrating traditional cybersecurity prevention layers within the framework, 3) introducing a cyberattack model over the shared information to generate the SICA dataset, 4) conducting an in-depth analysis of the performance of the proposed FA classifier highlighting their ability to indicate normal and abnormal conditions, and 5) presenting an in-depth evaluation of the proposed FA-based SICA detection cybersecurity layer under different operating conditions, including limited cyberattack training data, unseen cyberattacks and new system configurations, data reliability and quality issues, and assessing the impact of cyberattacks on the SICA cybersecurity layer.

The main contributions of this paper are summarized in the following:

1) A new cybersecurity layer is proposed to detect SICA in power systems. The proposed method aims to detect stealthy cyberattacks that could not have been blocked by the existing cybersecurity measures and have broken through.
2) The concept of the FA is proposed as a new classification mechanism for the detection of SICA, where the position of each PSSV is compared against the estimated FA; it is then decided if the system has been impacted by SICA.
3) A flag vector is created indicating the location of each PSSV with respect to the defined FA. The location of each PSSV and its pattern represented in the flag vector are utilized to identify the existence of SICA. Various SICA detection mechanisms using mathematical techniques and the Pattern Recognition Neural Network (PRNN) have been applied.
4) True Positive (TP) and False Negative (FN) metrics are proposed with the aim of evaluating the effectiveness of the deterministic and non-deterministic classes for accurately representing FA shapes, and assessing the ability of the proposed FA-based model in detecting infiltrated cyberattacks.

II. The Proposed Framework of the FA-Based SICA Detection Mechanism

The BDD layer is considered the first line of defense against FDIA. An alarm is initiated by the BDD layer if the Largest Normalized Residual (LNR) (γ) between the actual measurement (z) and the estimated values ($\widehat{z}$) is greater than a given threshold value (ψ), which is defined using the Chi-squared test. Eq. (1) represents the BDD layer as the first cybersecurity protection stage:

$$\begin{cases} \text{FDIA Detection } \gamma = \dfrac{|z-\widehat{z}|}{\|z-\widehat{z}\|_2} \geq \psi \\ \text{No FDIA } \quad \gamma = \dfrac{|z-\widehat{z}|}{\|z-\widehat{z}\|_2} \leq \psi. \end{cases} \tag{1}$$

Traditional BDD layer can be broken through by professional attackers who are penetrating stealthy attacks with low LNR using previous knowledge of the system parameters i.e., Jacobian matrix [30]. As such, advanced FDIA prevention frameworks with multiple detection layers are needed to strengthen the cybersecurity of power systems as described hereunder.

Fig. 2 illustrates the proposed cybersecurity framework in which the BDD layer utilizes the state estimation of the power system measurement and primary information vector, such as power system field measurement and weather information, to detect FDIA. When the FDIA break through the BDD, another test is established using model-based and data-driven techniques as a second cybersecurity layer for the primary information. Then, the primary information is utilized by computational algorithms to measure the optimal state set points, known as the secondary information, which is sent to the control components of the power system via the cloud/communication network. Both the primary and secondary datasets represent the active data exchanged between the power system and the control unit via cloud/communication networks. FDIA over the secondary information could be also detected using another advanced cybersecurity prevention layer. Stealthy attacks that infiltrate through these protection layer, manipulate the system state and lead to hard-to-detect forms. Thus, another cybersecurity layer is proposed to be added in order to detect infiltrated SICA in an early stage to avoid severe damages.

The term FA is defined as the region where PSSV are commonly located based on a window of historical healthy data [28], [29]. In order to define an SICA operation state, PSSV are collected and examined using the FA-based SICA detection mechanisms. It is noteworthy that the proposed technique receives the power system state after the attack takes place and analyzes the power system state to identify the SICA. The FA-based SICA detection method utilizes the PSSV variation as an indication of the SICA on any parameter of the power system where PSSV acts as universal features to detect these SICAs. As such, this layer provides an alarming function to the operator to evaluate the state of the system and take the necessary actions if the operator confirms that an attack did in fact infiltrate the cybersecurity protection layers.

The SICA detection layer depicted in Fig. 2 represents the procedures linked to the proposed SICA detection layer and the integration of the new proposed layer alongside the FDIA detection layers for both the primary and secondary information to improve the overall performance of the cybersecurity systems. The FA is defined in a two-dimensional complex plane by using the real and imaginary parts of the PSSV. At each Time instance t, the current PSSV are sent to the SICA detection layer to verify if the system has been compromised. For every PSSV $x_{n,t}$, the corresponding M-hour window, denoted as $[x_{n,t-M} : x_{n,t-1}]$, is passed onto the complex plane representation block. In the complex plane stage, the window $[x_{n,t-M} : x_{n,t-1}]$ is transformed into a complex plane representation (real and imaginary axes) to facilitate the estimation of FA measures. The magnitude and angle of voltages and currents are converted into real and imaginary parts and placed in the complex plane. For the apparent power, the complex plane is represented by the active and reactive powers. Subsequently, the FA parameters, including rectangular boundaries, circular center and radius, elliptic center and shape matrix, as well as the convex-hull polygon outlier points are estimated for each PSSV $x_{n,t}$. These FA parameters are then shared with the flag vector calculation stage, which determines the location of the current

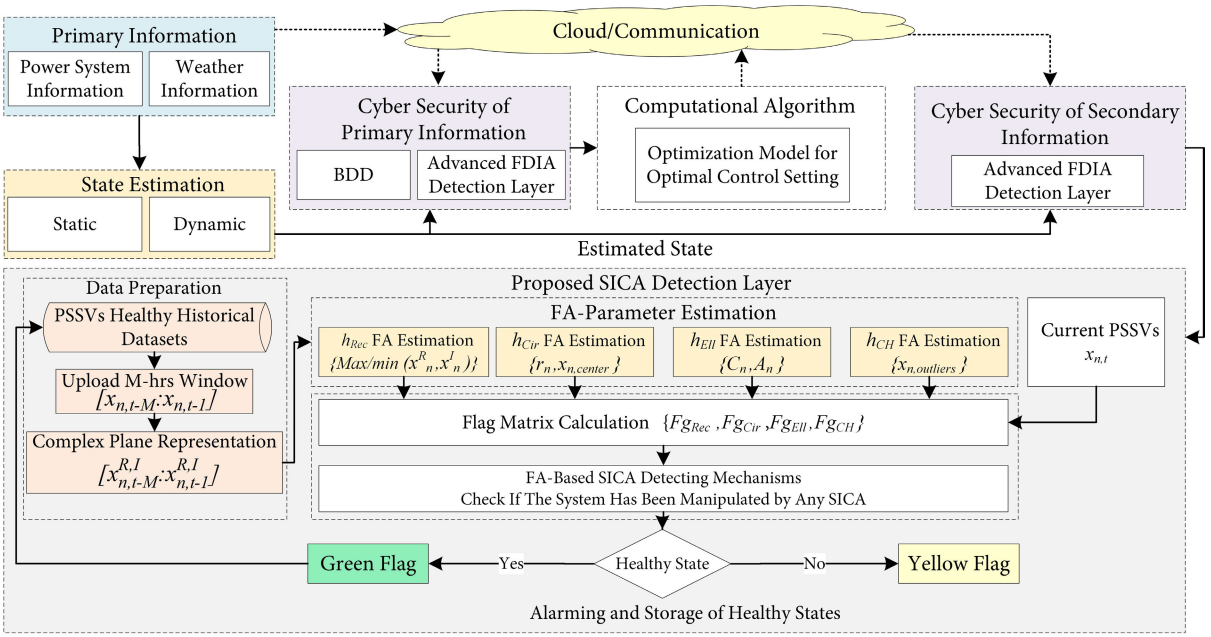


Fig. 2. Cyberattack detection in an electric power system with an additional SICA detection layer.

PSSV at Time t in relation to each FA region (inside or outside rectangular, circular, elliptic, and convex-hull FA). The information obtained from the flag vector stage is utilized by the FA-based SICA detection mechanisms to determine if the system has been manipulated by any SICA. When a green flag is received, the current state is added to the historical healthy data buffer for future tests. Conversely, if a yellow flag is raised, an alarm is sent to the operator to reassess the system's optimal state and take appropriate corrective actions.

Two classes are used to represent the FA: deterministic and non-deterministic. The deterministic class, defined by rectangular, circular, and elliptic shapes, is used to estimate a FA with deterministic borders, i.e., regular FA. In contrast, the non-deterministic class is defined by the Convex-Hull polygon with a non-deterministic border used to represent irregular FA. The proposed SICA detection layer consists of two computational stages. The first stage involves estimating the FA through a historical window of data over a specified period of time, which is then inputted to the second stage. In the second stage, the position of each PSSV with respect to the estimated FA is assessed and utilized by the SICA detection mechanism to identify instances of attacks. A flag vector is created indicating the location of each PSSV with respect to the defined FA. The location of PSSVs and their patterns represented in the flag matrix are utilized to identify the existence of SICA using the detection mechanism. In this regard, four SICA detection mechanisms are proposed using mathematical techniques (single flag, FA uncertainty ratio, weighted sum ratio) and the PRNN. The proficiency of the FA estimation in the first phase is evaluated using TP and FN metrics. The ability of the SICA detection mechanisms, in the second stage, to accurately identify SICA and normal operations is used to assess the model performance.

III. Proposed FA Estimation Technique

Estimating the actual FA characteristics of each PSSV could be very complex since it depends on different variables and conditions, e.g., operation target (objective function), power generation level, load demand, and system configuration. Thus, it requires full knowledge of the distribution function for each PSSV. Such data is not possible to be acquired in most cases due primarily to the dynamic change of the power system operation and the non-linearity in the system operation objectives and constraints. Hence, a group of deterministic and non-deterministic classes is assumed and investigated in this paper to evaluate the FA performance as a mechanism for the SICA detection layer. The deterministic class uses rectangular, circular, and elliptic shapes as a classifier to represent the FA defined as $H_D = \{h_{Rec}, h_{Cir}, h_{Ell}\}$. The non-deterministic class uses Convex-Hull optimization to estimate the irregular polygon classifier to represent the FA $H_{ND} = \{h_{CH}\}$. The general estimation criteria of each Classifier $h \in H$ can be defined as the minimization of the classifier area while ensuring that all the historical data set $S \in$M-hour are located inside the classifier area, or in other words, the binary empirical loss of the Classifier h equals zero, which could be represented mathematically as follows:

$$\text{Minimize Area}(h)\ ,\ S.t\ \mathscr{L}_S(h) = 0\ \forall h \in H$$
$$H = \{H_D \cup H_{ND}\},\ \begin{cases} H_D = \{h_{Rec},\ h_{Cir},\ h_{Ell}\} \\ H_{ND} = \{h_{CH}\}. \end{cases} \tag{2}$$

It is worth noting that the term classifier is used here for the FA shapes since they classify each PSSV into a normal or abnormal pattern (inside or outside the area).

A. Parameter Estimation for the FA Classes

Determining the parameters for each classifier is crucial for assessing the changes in PSSV caused by SICA. This section presents the formulated optimization model aimed at estimating the FA parameters.

1) Rectangular Feasibility Area: A window of M-hour on the historical healthy data is used for the FA estimation. To estimate the rectangular boundaries, the maximum and

minimum values of the PSSV ($X_n^{R,I}$) (real and imaginary parts) are determined, i.e., the most left and right as well as lower and upper points for each PSSV $X_{n,t} \forall n \in N_{var}$ & $\forall t \in M$. Equation (3) states the main estimation criteria of the rectangular FA classifier h_{Rec}.

$$\text{Minimize Area}(h_{Rec}),\ \text{S.t}\ \mathscr{L}_S(h_{Rec}) = 0. \tag{3}$$

2) Circular Feasibility Area: Circular and elliptic classifier-based FAs are estimated using a learning algorithm that needs to solve an optimization problem [29]. The circle center and radius are the decision variables of the optimization problem. The objective function is to find the minimum area, e.g. the minimum radius, and to ensure that all the historical points S inside the M-hour window are within the circle boundaries. To ensure that this criterion is met, the distance between the historical window points and the estimated circle center should be less than or equal to the circle radius. The main estimation criterion is defined by (4), and the corresponding optimization problem is described in detail by (5):

$$\text{Minimize Area}(h_{Cir}),\ \text{S.t}\ \mathscr{L}_S(h_{Cir}) = 0 \tag{4}$$

$$\text{Minimize}(r_n),\ \text{S.t}$$
$$\sqrt{(X^R_{n,Cen} - X^R_{n,t})^2 + (X^I_{n,Cen} - X^I_{n,t})^2} \le r_n, \forall t \in M. \tag{5}$$

3) Elliptic Feasibility Area: The main criterion for estimating the elliptic FA is to minimize the area of the elliptic classifier h_{Ell}, while ensuring that all the data points $S \in$ M are inside this area as defined by (6):

$$\text{Minimize Area}(h_{Ell}),\ \text{s.t}\ \mathscr{L}_S(h_{Ell}) = 0. \tag{6}$$

To define the learning algorithm that would validate (6), the optimization problem for estimation is required to be defined. Elliptic characteristics in the center form is represented by (7):

$$(X_{outer} - C)^T A (X_{outer} - C) = 1 \tag{7}$$

where X_{outer} represents the points that lie in the ellipse boundaries. The FA is estimated by defining the ellipse shape A_n and the center C_n matrices that has the minimum area and ensures that all the healthy historical points $S \in$ M are within the classifier area. A set of points with left hand side of the area defined by (7) less than 1 are inside the ellipse. The elliptic FA estimation optimization problem is stated by (8).

$$\text{Minimize}(|A_n^{-1}|),\ \text{S.t}$$
$$(X_{n,t} - C_n)^T A_n (X_{n,t} - C_n) \le 1,\ \forall t \in M. \tag{8}$$

4) Convex-Hull Feasibility Area: The second class H_{ND} estimates the irregular FA. Convex-Hull is used to represent the irregular classifier FA. This classifier emulates a polygon that encloses all the points inside the historical M-hour window. In order to ensure a fast and accurate estimation of the Convex-Hull polygon, the high-dimension estimation Graham's scan algorithm introduced in [31] is utilized in this paper, which shows a lower computational effort and faster estimation of the Convex-Hull parameters compared to traditional algorithms. The basic idea of this algorithm is to find the lowest point (the point with the minimum imaginary value in the complex plane), indicating the outer boundaries of the polygon. Then, the motion direction between the current point and all other nearby points are measured. The next point is selected to ensure that the motion direction is always counter clockwise. The algorithm returns the outer point representing the border of the polygon. Fig. 3a shows the output of the Graham's scan algorithm. Then, the enhanced grid-based approach for point-in-polygon tests proposed in [32] is used to check if PSSV corresponding to the current state is inside the estimated Convex-Hull polygon. The concept of the algorithm is to draw a straight line from the tested point in the complex plane in any direction. If the point is inside the Convex-hull polygon, the line and the polygon will have an intersection in one point only. Otherwise, the point is considered outside the polygon. For illustration purposes, Fig. 3b and Fig. 3c show how the estimated regular and irregular FA using rectangular, circular, elliptic, and the Convex-Hull polygon have been used to capture healthy (i.e., non-attacked) data of the system. The healthy data represent phasor values of the voltages that have been produced using a 48-hour window (i.e., M=48 hours) of the system data.

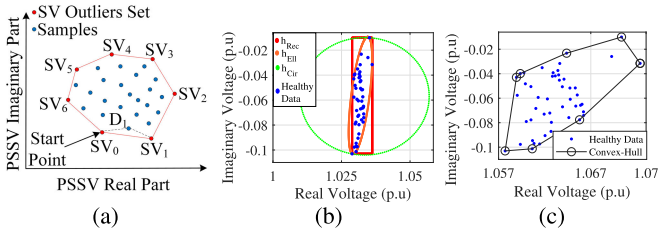


Fig. 3. The estimated feasibility area represented by a)The Graham's scan algorithm output b) regular rectangular, circular, and elliptic shapes c) irregular using the Convex-Hull polygon.

B. Performance Metrics for the FA-Based SICA Detection

In order to investigate the performance of the proposed FA-based SICA detection layer, the TP and FN ratios are defined for each PSSV. The TP index indicates the ability of the Classifier $h \in H$ to correctly identify the healthy operation of each PSSV to reside inside the FA represented by the classifier. Meanwhile, the FN index indicates the ability of the Classifier $h \in H$ to correctly identify the SICA operation of each PSSV to reside outside the FA represented by the classifier. In other words, both the TP and FN indexes indicate the quality of each FA represented by the Classifier $h \in H$ to accurately identify the actual operation (healthy or attacked) for the PSSV n. Hence, PSSV with high TP and FN (ideally 100%) using the FA represented by the Classifier h can be used as a strong indication of the system operation state. By using τ^{HL} healthy and τ^{A} attacked data sets, the TP and FN ratios with their complement (FP and TN) for each PSSV using the Classifier h can be expressed as:

$$\text{TP}_{\text{h,n}} = \frac{\sum_{t=1}^{\tau^{HL}} 1[X_{n,t} \in h]}{|\tau^{HL}|}, \text{FP}_{\text{h,n}} = 1 - \text{TP}_{\text{h,n}}$$
$$\text{FN}_{\text{h,n}} = \frac{\sum_{t=1}^{\tau^{A}} 1[X_{n,t} \notin h]}{|\tau^{A}|}, \text{TN}_{\text{h,n}} = 1 - \text{FN}_{\text{h,n}}. \tag{9}$$

Here, the operation $1[C]$ equals 1 if the constraint C is valid and zero otherwise.

The second set of parameters that are used to evaluate the performance of the proposed technique include the Attacked Operation (AO) and the Healthy Operation (HO) ratios. These ratios indicate the overall performance of the FA-based SICA detection mechanism. The AO indicates the ability of the FA-Based SICA detection mechanism to correctly identify the attacked state of the power system and raise an alarm by utilizing the FA information, e.g, PSSV locations. On the other hand, the HO indicates the ability of the FA-Based SICA detection mechanism to correctly identify the healthy state of the power system without raising false alarms, which is measured by counting the number of false alarms. The ideal AO and HO values are 100% and 0% respectively, which indicates that all the SICAs are correctly captured and no false alarms are raised. By using τ^{HL} healthy and τ^{A} attacked data sets, the AO and HO could be defined as expressed in (10).

$$\text{AO} = \frac{\text{Correct Captured SICA}}{|\tau^{A}|}, \ \text{HO} = \frac{\text{Wrong SICA}}{|\tau^{HL}|} \tag{10}$$

IV. FA-Based SICA Detection Mechanisms

An SICA detection mechanism is developed to identify the existence of cyberattacks. Various investigations are conducted in this paper to study the performance of each PSSV, via utilization of PSSV and different FA-based SICA detection mechanisms. Such mechanisms utilize the information of all the PSSV locations with respect to the estimated FA of each classifier $H = \{h_{Rec}, h_{Cir}, h_{Ell}, h_{CH}\}$. At each operation Time t, a binary flag vector $Fg \in \{0,1\}^{N_{var}\times 1}$ is defined for each Classifier $h \in H$ to indicate the PSSV location with respect to the FA represented by the Classifier h. Equation (11) represents the mathematical expression of the flag vector:

$$Fg_{h(n,t)} = 1[X_{n,t} \notin h] \ \forall h \in H. \tag{11}$$

As described below, four FA-based SICA detection mechanisms are proposed to detect the existence of the SICA.

A. Single Flag SICA

In this mechanisms, if any element in the flag vector $Fg_{h(n,t)}$ $\forall h \in H$ equals one, the corresponding operation state at Time t is considered an FDIA attack, and a yellow flag is raised. If all state variables of the power system are within the estimated FA, a green flag is raised to indicate the absence of cyberattacks [29].

B. Feasibility Area Uncertainty Ratio

To evaluate the existence of SICA based on all the PSSV locations with respect to the FA of each Classifier $h \in H$, $\text{FAUR}_{\text{h,t}}$ is defined as the ratio between the PSSV located outside the Classifier h of the FA to the total number of the PSSV. The matrix form of the $\text{FAUR}_{\text{h,t}}$ is represented by (12), where I shows a vector of ones $\in \{1\}^{N_{var}\times 1}$.

$$\text{FAUR}_{\text{h,t}} = \frac{1}{N_{var}}[I^{T}.Fg_{h(n,t)}]. \tag{12}$$

Once the $\text{FAUR}_{\text{h,t}}$ at a Time t becomes larger than a previously defined threshold value ψ of a certain Classifier h, the SICA alarm is initiated. The value of ψ is estimated using the labeled healthy and attacked data to ensure the optimal performance of the proposed FA-based SICA detection mechanism. Using the labeled healthy and attacked data set of τ-hour, the selected ψ value would allow for the maximum SICA detection while bypassing the healthy operation without raising an alarm. Using the labeled data, the flag matrices are defined for each data set (healthy data flag matrix $Fg_h^{HL} \in \{0,1\}^{N_{var}\times\tau}$ and attacked data flag matrix $Fg_h^{A} \in \{0,1\}^{N_{var}\times\tau}$). Then, the FAUR is defined using (12) for each healthy and attacked data set of $\text{FAUR}_{\text{h}}{}^{\text{HL}}$ and $\text{FAUR}_{\text{h}}{}^{\text{A}}$, respectively. The threshold value is then estimated to minimize the number of healthy data alarms and maximize the number of attacked data alarms. The objective function can be defined by (13), where the decision variable is ψ for each Classifier h.

$$\text{Minimize} \sum_{t=1}^{t=\tau} \left(Al_h^{HL}(t) - Al_h^{A}(t) \right). \tag{13}$$

C. Weighted Sum Ratio

Each PSSV has a certain quality in detecting the SICA using the concept of the FA. Under an attack, some PSSV are more sensitive to the attack drifting from the normal FA and will be located outside the normal operating region. Therefore, each PSSV is given a weight between 0 and 1, which indicates the quality of using this PSSV to identify the SICA. Assume that $W_h \in [0,1]^{N_{var}\times 1}$ is the weight vector of the total PSSV (N_{var}) for Classifier $h \in H$; then, for every operation Time t, the Weighted Sum Ratio ($\text{WSR}_{\text{h,t}}$) is defined as the ratio between the weighted sum of PSSV outside the FA of the Classifier h to the overall weights of all PSSV. The matrix form of the $\text{WSR}_{\text{h,t}}$ is stated by (14).

$$\text{WSR}_{\text{h,t}} = \frac{1}{\sum_{n=1}^{N_{var}} w_{h,n}}[W_h^{T}.Fg_{h(n,t)}], \ \forall h \in H. \tag{14}$$

Similarly, the $\text{WSR}_{\text{h,t}}$ of each class $h \in H$ is associated with a gain G_h between 0 and 1, which indicates the effectiveness of each classifier to accurately represent the FA. If the weighted average of all classifiers indicates that the FA is higher than a threshold value ψ, an SICA detection alarm is initiated. The FA-based SICA detection mechanism using WSR could be expressed as follows:

$$\begin{aligned} Al(t) = 1[&\frac{1}{|H|}(G_{Rec}\text{WSR}_{\text{Rec}} + G_{Cir}\text{WSR}_{\text{Cir}} \\ &+ G_{Ell}\text{WSR}_{\text{Ell}} + G_{CH}\text{WSR}_{\text{CH}}) > \psi]. \end{aligned} \tag{15}$$

The classifier weight vector $W_h| \ \forall h \in H$, overall gains for $G_h| \ \forall h \in H$, and the threshold value ψ are estimated using the labeled healthy and attacked data to maximize the SICA detection performance. The objective function of the optimization problem is defined in (16). The main goal is to minimize the number of healthy data alarms Al^{HL} and increase the detection rate of the SICA Al^{A} as given below.

$$\begin{aligned} &\text{Minimize} \sum_{t=1}^{t=\tau} Al^{HL}(t) - Al^{A}(t), \ \text{S.t} \\ &0 \le W_h, G_h \le 1, \ \forall h \in H. \end{aligned} \tag{16}$$

In order to relax the number of decision variables, the optimization problem is solved in two stages. In the first stage, the weight vector $W_h|\ \forall h \in H$ is determined for each Classifier h separately. Then, the estimated weight vector of each Classifier $h \in H$ is added as an input to the general optimization frame in (15). In the second stage, the optimization problem is solved to estimate the value of the gains $G_h|\ \forall h \in H$ and the threshold value ψ, which reduces the number of decision variables to $|H|+1$.

D. Machine Learning-Pattern Recognition Neural Network

During normal operating conditions, the PSSV follows a certain pattern of operation. Thus, their location with respect to the FA also follows a certain pattern. In the case of SICA, the pattern deviates from the normal operation, and hence, can be used as an indication for cyberattacks. Therefore, an FA-PRNN, which comprises of a two-layer feed-forward network with Sigmoid and Softmax output neurons, is used and trained with labeled healthy and attacked data to differentiate between the normal and attacked operation.

The FA-PRRN utilizes the combined information from the flag matrices of all classifiers within the set $h \in H$ to create a consolidated input vector referred to as the overall flag vector, denoted as Fg; equation (17) represents this input vector:

$$Fg = [Fg_{Rec}^T, Fg_{Cir}^T, Fg_{Ell}^T, Fg_{CH}^T, B_{L1}]^T \tag{17}$$

It is worth noting that utilizing the flag vector as input without directly incorporating the PSSV values aids in the generalization of detecting new SICA. The primary objective is to train the FA-PRNN to recognize patterns of positional variation caused by SICA. The FA-PRNN generates an output that corresponds to the system state, indicating whether it is healthy or attacked. To train the FA-PRNN model, the healthy and attacked data sets, τ^{HL} and τ^{A} respectively, are utilized. 70% of the data is used for training purposes, 15% is allocated for testing, and the remaining 15% is utilized for model validation to prevent over-fitting.

The input vector Fg is multiplied by the weight matrix W_{L1}, which belongs to the first layer and has dimensions of $R^{N_{L1}\times(|H|.N_{Var}+1)}$. This multiplication process yields the non-activated output of the first layer denoted as A_{L1}, as indicated by equation (18):

$$A_{L1} = W_{L1} \times Fg \tag{18}$$

The non-activated output of the first layer, A_{L1}, undergoes a sigmoid activation function. This activation function transforms the non-activated output into the activated output of the first layer, Z_{L1}, which has dimensions of $R^{N_{L1}\times 1}$. The transformation is illustrated by (19):

$$Z_{L1} = \frac{1}{1+e^{-A_{L1}}}. \tag{19}$$

The activated output of the first layer, Z_{L1}, is multiplied by the weight matrix of the output layer, denoted as W_{L2}, which has dimensions of $R^{1\times N_{L1}}$. This multiplication yields the non-activated output of the layer, denoted as A_{L2}, with a dimension of $R^{N_{L2}\times 1}$.

Subsequently, the non-activated output is passed through the Softmax activation function to obtain the activated output, denoted as Z_{L2}. The activated output represents the condition of the power system state, indicating whether it is healthy or attacked. The calculation of the activated output of the output layer is stated by (20) in the context of the FA-PRNN:

$$Z_{L2}^j = \frac{e^{A_{L2}^j}}{\sum_{k=1}^{N_{L2}} e^{A_{L2}^k}},\ \text{where}\ A_{L2} = W_{L2} \times Z_{L1}. \tag{20}$$

The FA-PRNN input layer consists of $N_{var}\times|H|+1$ neurons where one neuron is used for each PSSV in each Classifier $h \in H$. The hidden layer consists of several neurons with a Sigmoid activation function. The output layer has single neurons with a Softmax activation function, which represents the SICA alarms. For learning purposes, a Stochastic Conjugated Gradient (SGD) is used where Cross-Entropy is utilized as the learning objective function [33]. The learning process is designed to stop when the change in the gradient becomes less than 10^{-6}, which was achieved by 70-90 iterations.

V. Simulation Setups

This section delves into the computational algorithm and cyberattack model as presented hereunder.

A. Computational Algorithm

In order to test the performance of the proposed FA-based SICA detection layer, the IEEE-30 bus transmission system shown in Fig. 4 is used. The operation set points of the dispatchable/adjustable units are calculated to meet the normal system operation requirement, while minimize the operation cost associated with the generated power. The computational algorithm objective is defined by (21):

$$\text{Minimize:}\ \Delta t \sum_{t\in\mathbb{T}}\sum_{b\in\mathbb{B}} c_1 {P_{t,b}^G}^2 + c_2 P_{t,b}^G + c_3 P_{t,b}^{Gad} + c_4 \tag{21}$$

The objective in (21) is subject to the operation constraints for the bus voltage and the branch power (22).

$$\underline{V_b} \le v_{t,b} \le \overline{V_b},\ \ \underline{P_{bb'}} \le P_{t,bb'} \le \overline{P_{bb'}},\ \ \forall t \in \mathbb{T} \cap b \in \mathbb{B} \tag{22}$$

Also, the estimated state by the designed computational algorithm should satisfy the power balance equation represented by the following:

$$P_{t,b}^G + P_{t,b}^{Gad} + P_{t,b}^{DER} - P_{t,b}^D - P_{t,b}^{Dad} = v_{t,b} \sum_{b'\in\mathbb{B}} v_{t,b'} \times (G_{bb'} Cos(\theta_{t,bb'}) + B_{bb'} Sin(\theta_{t,bb'})) \tag{23}$$

$$Q_{t,b}^G - Q_{t,b}^D = v_{t,b} \sum_{b'\in\mathbb{B}} v_{t,b'} \times (G_{bb'} Sin(\theta_{t,bb'}) - B_{bb'} Cos(\theta_{t,bb'})) \tag{24}$$

The set point of the adjustable units $(P_{t,b}^{Gad}, P_{t,b}^{Dad})$ serves as the decision variables. The adjustable load units are constrained by the energy requirement, while the adjustable generation is limited by the generation energy capacity and operational constraints as described by (25) and (26).

$$\Delta t \sum_{t\in\mathbb{T}^{D,b}} P_{t,b}^{Dad} = E_b^{Dad},\ \ \Delta t \sum_{t\in\mathbb{T}^{G,b}} P_{t,b}^{Gad} \le E_b^{Gad} \tag{25}$$

$$\underline{P_b^{Gad}} \le P_{t,b}^{Gad} \le \overline{P_b^{Gad}}, \forall t \in \mathbb{T} \cap b \in \mathbb{B} \tag{26}$$

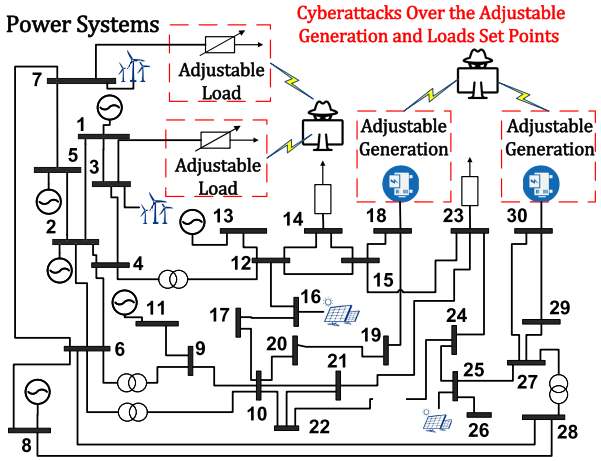


Fig. 4. The IEEE 30-bus transmission system employed for numerical studies.

The computational algorithm utilizes primary information, including power demand, to estimate the optimal set point, known as the secondary information. This secondary information is then transmitted to the adjustable units via the cloud. The model of cyberattacks over both the primary and secondary datasets is discussed in the next paragraphs.

B. Cyberattack Model

Cyberattacks target both the primary and secondary information transmitted via cloud and communication networks. In the case of primary information, the attacker manipulates the SCADA active and reactive power measurements of renewable energy generated by PV and wind farms installed at Buses 3, 7, 16, and 26. The goal is to affect the state estimation and computational algorithm results, resulting in financial losses. For secondary information, the attacker alters the set points of adjustable units directly, changing active and reactive power demand and generation settings to induce financial losses [34]. This manipulation aims at increasing power system operation costs and corrupting the computational results, causing financial losses without violating system operation limits or causing instability. It is assumed that SCADA measurements at renewable energy farm locations and adjustable unit communications are insecure and susceptible to manipulation by professional attackers. Conversely, Phasor Measurement Units (PMUs) are placed to ensure system observability, with voltage and current phasor measurements are assumed to be secure. This assumption regarding PMUs is supported by their advanced communication protocols, encrypted data, and the use of digital signatures, message authentication codes, and data encryption techniques [35].

Cyberattacks over the primary information are designed to bypass the BDD. This is made by adopting the stealthy FDIA model in [26]. The relation between the system state and input measurement vector is defined by (27):

$$Z_t = J X_t + e_t \tag{27}$$

The stealthy cyberattacks are then designed by the attacker as follows:

$$\hat{Z}_t = Z_t + a_t, \text{S.t } a_t = J C_t, \;\; \hat{X}_t = X_t + C_t \;\forall\; t \in \mathbb{T} \tag{28}$$

The vector a_t represents the affected measurements targeting the primary information of the active and reactive power of the PV and wind farms.

Cyberattacks on the secondary information are designed as stealthy attacks, aiming to reduce the system revenue. Therefore, the same computational algorithm is employed to craft the cyberattacks on the secondary information. The attacker only needs to alter the objective function of the computational algorithm while introducing variation constraints on the PSSV to prevent detection by cybersecurity layers. This modification can be represented by (29) and (30):

$$\text{Maximize: } \Delta t \sum_{t\in\mathbb{T}} \sum_{b\in\mathbb{B}} c_1 P_{t,b}^{G\,2} + c_2 P_{t,b}^{G} + c_3 P_{t,b}^{Gad} + c_4 \tag{29}$$

$$|v_{t,b} - \hat{v}_{t,b}| \le \psi_v, \;\; \forall t \in \mathbb{T} \cap b \in \mathbb{B} \tag{30}$$

It is worth noting that, stealthy cyberattacks constitute a specific subset of cyberattacks capable of evading the BDD. However, not all stealthy cyberattacks fall under the classification of SICA. SICA represents a subset of stealthy cyberattacks that not only successfully bypasses the BDD but also traverse the primary and secondary information advanced model or data-driven base cybersecurity layers. While all designed attacks are categorized as stealthy cyberattacks, only those with the ability to infiltrate all cybersecurity layers are acknowledged as SICA. Therefore, there is a need to implement cybersecurity layers for both the primary and secondary datasets to extract the SICA subset.

Fig. 5 illustrates the simulation setup and data preparation steps. Initially, simulation parameters are uploaded at each Time t, and healthy PSSV is obtained by applying the primary information without modification to the computational algorithm. The resulting output is stored in the healthy PSSV data storage. In contrast, the modeling of stealthy cyberattacks involves the utilization of primary and secondary stealthy cyberattack models. To extract SICA, the manipulated measurements undergo verification by advanced cybersecurity layers, namely the Continuous Wavelet Transform Convolutional Neural Network (CWT-CNN) and Class-based Regression Deep Neural Network (Cal-Reg DNN), for primary and secondary information, respectively. If the attack is detected by any of these layers, a new attack is formulated with a smaller change margin, and the process iterates until the attacks successfully bypass all cybersecurity layers, storing the outputs in the SICA datasets. For the power system under study, in each bus, the bus phasor voltages, injected currents to the bus, and injected complex apparent powers to the bus are used as PSSV. Meanwhile, for the power system transmission lines, sending and receiving end current and complex apparent power values are used as PSSV. In particular, three and four PSSV are tested for each bus and transmission line, respectively.

Due to the scarcity of real-world attack data steaming from the confidential nature of cyber incidents, legal restrictions, and privacy concerns [17], a one-year simulation of healthy and attacked operation is performed, and the resulting data is stored for $\tau^{HL} = \tau^{A} = 8760$ hours. These historical data sets are utilized to determine the optimal tuning of the FA-based SICA detection mechanisms. The healthy PSSVs are then employed to estimate FA parameters at each Time t. For each

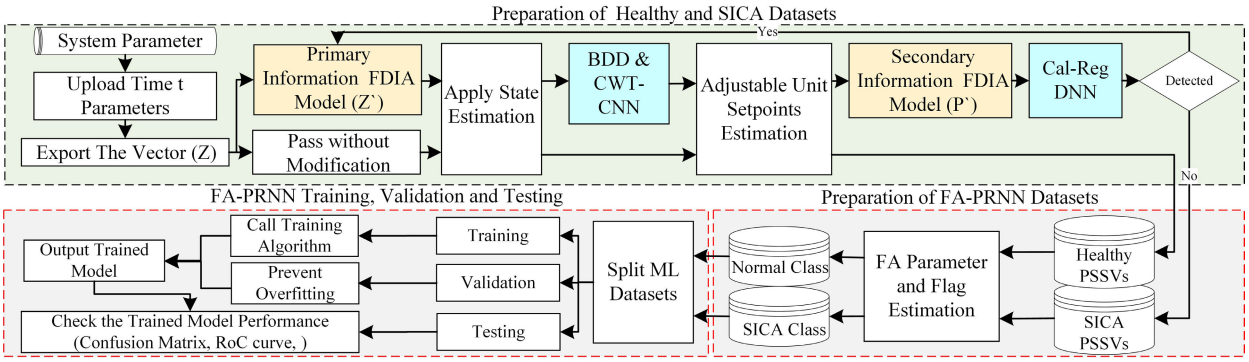


Fig. 5. Healthy and SICA scenario generation flowchart.

Classifier h belonging to Set H, two flag vectors Fg_h^{HL} and Fg_h^{A} are constructed by estimating the FA for a sliding window of M hours using the healthy PSSVs. The optimization process for the FAUR is performed by solving the problem stated by (13), while the Weighted Sum Ratio optimization problem is solved as described in (16). Additionally, the PRNN is trained using the flag matrices of all classifier via SGD, aiming to optimize the performance of the FA-based SICA detection mechanisms.

VI. Case Studies and Simulation Results

The optimization problem and the cyberattacks models for both the primary and secondary datasets are constructed as Quadratic programming optimization problems solved by global optimization techniques within the MATLAB environment. The optimization is solved for one year with $\Delta t = 1$ hour under healthy and attacked operation using a computer with the following specifications: Intel Core i9 2.1 GHz, 12th Gen workstation with 32 GB RAM. The computational workload of the proposed SICA detection layer scales linearly with the size of the PSSV, denoted as $O(SICA) = |PSSV| \times \sum_{h \in H}(O(h))$, and for the FA parameter estimation and flag vector calculation stage, it scales linearly for all $h \in H$, where $O(h) \propto |S|$. The total computational time for the algorithm ranges from 4 to 8 milliseconds, demonstrating its capability to rapidly determining the system's state.

Four case studies are conducted to assess the effectiveness of the proposed SICA detection layer as follows: 1) The first case study evaluates the performance of each Classifier $h \in H$ in implementing the FA concept, analyzing the FAUR, and comparing the performance of the FA-based SICA detection mechanisms with other common machine learning FDIA detection techniques; 2) the second case study examines the robustness of the proposed SICA detection layer when faced with limited SICA datasets; 3) the third case study investigates the performance of the proposed SICA detection layer when encountering unseen SICA and new system configurations, and 4) the final case study assesses the performance of the proposed SICA detection layer in the presence of measurement noise and errors.

A. Performance Evaluation for FA Classifier and SICA Detection Mechanisms

In this study, the system is simulated under healthy and attacked operations for one year with attacks on the set points of the adjustable unit. The collected data is used to investigate the following: a) the performance of each Classifier $h \in H$ in representing the FA is studied by analyzing each TP and FN ratio of each parameter; b) the FAUR is studied for different classifiers in order to indicate the performance of each classifier in detecting the SICA attack based on all the PSSV patterns with respect to the FA defined by each classifier, c) the performance of each designed FA-based SICA detection mechanism is evaluated and compared with other common classification methods such as SVM and ANN for detecting SICA and the decision making process is analyzed.

Fig. 6 shows the TP and FN for each classifier and the Index of PSSV (IoPSSV), which represents the PSSV types and locations. Table II reports how IoPSSV have been assigned to represent various system operating parameters. For instance, IoPSSV from 1 to 30 represent the system bus voltages. The TP and FN values indicate how successful each classifier is for accurately capturing healthy data and rejecting attacked data using a power system variable. Table III reports the mean and standard deviation of the TP and FN values for each Classifier h considering all the PSSV for one year of data in both the healthy and attacked scenarios. A high mean value is an indication of a well-shaped FA where all the healthy data is captured inside the FA and is separated from the attacked misoperations created by the SICA. Also, a low standard deviation value is an indication of the robustness of the assumed FA to represent different PSSV effectively, e.g., voltage and apparent power phasor values. Acceptable FA representation by any Classifier h for a PSSV should present high mean and low standard deviation values for both the TP and FN. It is clear from the results that each PSSV has a different TP and FN percentage, and hence, the given weight to each PSSV in detecting the attack is very effective; this is because some PSSV are better than the others in detecting the attack based on their sensitivity to the attack. It is important to mention that the mean values of FP and TN are the complements of the reported values $1 - TP$ and $1 - FN$, respectively, while the standard deviation remains the same for both.

The results show that the rectangular shape provides the highest performance for the healthy data capture when compared to other shapes. The low standard deviation represents the ability of the rectangular shape to accurately create a healthy operation region for all the PSSV. The elliptic shape, on the other hand, provides the highest performance

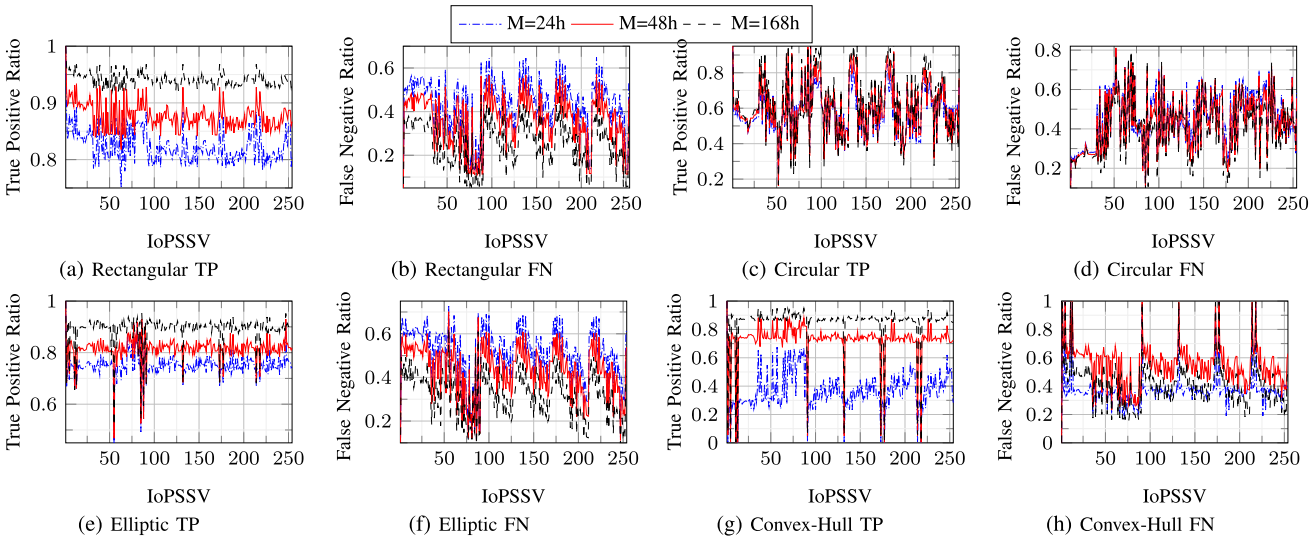


Fig. 6. The TP and FN matrices performance measurement for various feasibility area classifiers.

TABLE II
INDEX OF PSSV AND THE CORRESPONDING PARAMETERS THEY REPRESENT

IoPSSV	Type of PSSV
1-30	Bus Voltages
31-60	Bus Injected Current
61-90	Bus Injected Apparent Power
91-131	Line Current at the Sending End
132-172	Line Current at the Receiving End
173-213	Line Apparent Power at the Sending End
214-254	Line Apparent Power at the Receiving End

TABLE III
TP AND FN MEAN AND STANDARD DEVIATION (STD) OF EACH CLASSIFIER FOR A ONE-YEAR DATA SET

Feasibility Area		True Positive Window			False Negative Window		
		24	48	168	24	48	168
h_{Rec}	Mean	82.42	87.47	94.11	43.14	36.22	25.83
	STD	2.97	2.39	1.22	12.91	11.7	10.56
h_{Cir}	Mean	58.33	60.22	62.73	45.36	43.63	41.06
	STD	13.37	15.04	17.41	14.33	14.28	14.74
h_{Ell}	Mean	75.2	81.43	89.16	50.96	43.47	32.2
	STD	5.06	5.03	5.95	12.9	11.72	10.48
h_{CH}	Mean	36.63	72.38	84.4	37.45	55.06	41.82
	STD	13.62	14.73	16.6	13.33	14.68	16.09

in detecting the SICA. Compared with the circular shape, the elliptic form shows a low standard deviation in representing the SICA of all the PSSV. The circular shape shows a moderate performance for the TP and FN percentages. The Convex-hull shows a poor performance for a small historical data window but when the window span increases, a significant improvement in the Convex-hull performance occurs. For all four shapes, as the window size becomes wider, the TP percentage increases and the FN value decreases. This is because the possibility of having similar operating conditions in the historical data window increases, and hence, the number of PSSV outside the FA decreases. In general, for any FA characteristic (rectangular, circular, elliptic, and Convex-hull), Table III indicates that under the SICA conditions, the number of PSSV outside the FA is always greater than the number of PSSV inside the FA in case of the healthy operation. Hence, the FA can be used as a clear indication for stealthy SICA that bypass the FDIA prevention layers.

An ideal PSSV should show 100% TP and FN. However, each PSSV shows a different TP and FN acceptable ratio. PSSV with higher TP and FN ratios are better than other PSSV with a low ratio in detecting SICA using the FA. Fig. 7 shows the number of PSSV, which can be considered effective in detecting the SICA using the FA, as the threshold of acceptable TP and FN ratio changes ($n \in$ Effective state variables, $if\ TP_n \& FN_n \geq threshold$). When a small historical data window is used, the Convex-Hull polygon shows the lowest performance but with increasing the window size, the number of effective PSSV of h_{CH} increases more than other classifiers. In other words, the performance of the Convex-Hull polygon improves gradually and more PSSV can be used as an indication of the SICA as the window size increases. The maximum values of TP and FN threshold ratio achieved for all classifiers $h \in H$ is 70%, which means there is always a probability of around 30% for having a false SICA alarm using the FA if only one PSSV is used to detect the attacks. Thus, utilizing the pattern of all the PSSV is more promising towards improving the SICA detection.

In order to evaluate the power system operation state using all state variables, FAUR is calculated as the percentage of the PSSV outside the FA. Unlike TP and FN ratios, calculated based on each PSSV performance, FAUR is an index that utilizes all state variables information. In an ideal case, FAUR under SICA is required to be high while it should be low for normal operation. In order to investigate the FAUR index in detecting the SICA, the FAUR is calculated using several PSSV for healthy and attacked studied cases. Then, the difference between the FAUR in attack and healthy cases at the same operation hour is measured as $\partial \mathrm{FAUR_t} = \mathrm{FAUR_{A,t}} - \mathrm{FAUR_{HL,t}}$. If the difference is positive, this indicates that the number of PSSV outside the FA in case of an attack is larger than the number of PSSV outside the FA in case

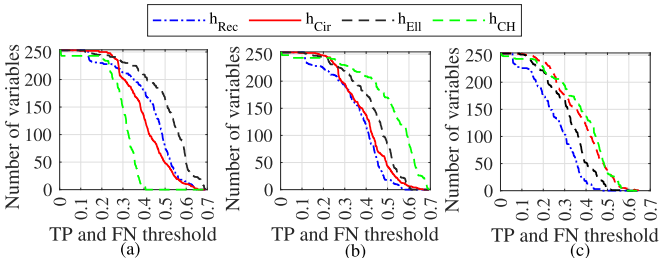


Fig. 7. The number of effective state variables for different lengths of historical data window a) M=24-hour, b) M=48-hour, c) M=168-hour.

TABLE IV
PERCENTAGE OF OPERATION STATES ∂FAUR > 0

Feasibility Area	Window M-hour		
	24	48	168
h_{Rec}	82.0205	82.2945	83.6073
h_{Cir}	64.4977	64.9772	64.4863
h_{Ell}	80.5936	80.5708	79.8288
h_{CH}	81.29	81.9863	83.9612

of a healthy operation. Fig. 8 shows the value of ∂FAUR of each classifier for the whole year and the effect of historical window variation. The red rectangular indicates the positive ∂FAUR zone for all classifiers. As shown in the figure, for all classifiers, in most cases, the number of PSSV located outside the FA during an SICA is greater than during normal operation. The Rectangular and Convex-hull classifiers demonstrate the highest performance. It can be seen in Table IV that for more than 83.6% of the operation cases, the number of PSSV located outside the FA in the SICA cases is higher than those of healthy operation cases. Hence, in case of attacks, the system operation state drifts away from the normal region where it exists normally.

From the first investigation, it can be seen that each PSSV has a different TP and FN ratio, which indicates the different quality of each PSSV in detecting attacks. Meanwhile, the second investigation shows that the FAUR in case of attacks is normally higher than FAUR in case of healthy operation, which implies that the number of PSSV located outside the FA is usually larger compared to normal operation cases. By combining the two means of investigation, the WSR is used by assigning different weights to each PSSV, indicating the PSSV sensitivity to the attacks. In such a case, there is a need to adjust the PSSV weights for each classifier and seek to increase the margin between WSR in case of attacks. Hence, increasing the percentage of $\partial \text{WSR} = \text{WSR}_{\text{attack,t}} - \text{WSR}_{\text{health,t}}$, would help in maximizing the performance of the FA-based SICA detection mechanism.

Table V summarizes the performance of the four FA-based SICA detection mechanisms: 1) single flag, 2) FAUR, 3) WSR, and 4) FA-PRNN, using the FA area concept. The Single Flag SICA detection method shows the worst performance in the identification of SICA and healthy data, making it an impractical option, and the method loses its dependability by considering all the healthy data as SICA. This is because it requires all the PSSV to be inside the FA, i.e., $\psi = 0$. As reported in Table V, WSR demonstrates the best performance compared with Single Flag and FAUR for all window sizes. Since it provides a higher flexibility and gives weights

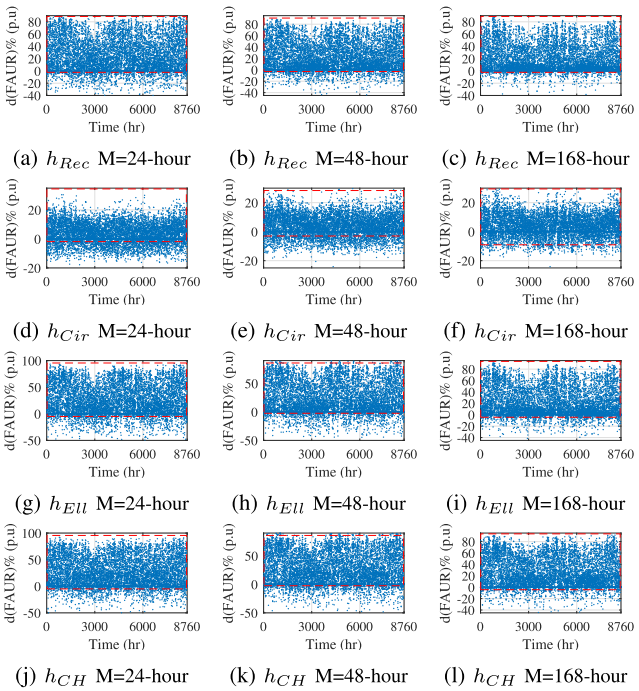


Fig. 8. The difference between $FAUR$ values during a cyberattack and when the system is in the healthy state $\partial\text{FAUR} = FAUR^{A} - FAUR^{HL}$.

TABLE V
PERFORMANCE OF THE PROPOSED FEASIBILITY AREA-BASED SICA DETECTION LAYER

Window Size		24	48	168
Single Flag SICA detection	AO	99.86	99.86	99.86
	HO	99.86	99.86	99.86
FAUR SICA detection	AO	67.65	73.39	65.06
	HO	29.09	34.12	24.95
WSR SICA detection	AO	85.03	81.6	90.48
	HO	33.68	25.47	41.94
FA-PRNN	AO	92.32	95.35	94.73
	HO	7.5	3.27	2.69

to each PSSV for the SICA identification, WSR shows a better performance. As indicated in the table, the proposed FA-PRNN demonstrates superior performance compared with other classification methods. By incorporating the FA concept, the PRNN is able to effectively detect the patterns of SICA through the use of flag vector information for each classifier.

The addition of the FA concept provides further advantages, making the learning process superior via the following avenues: 1) reducing the overlap between healthy and attacked operation states; 2) considering the time frame as a factor that indicates the existence of the attack, and 3) taking into consideration the sensitivity to measurement noise and reduced sensitivity to state variations issues encountered in traditional machine learning methods. This is emphasized in Fig. 9, where the proposed FA-PRNN is compared with other Deep Neural Network (DNN) and common machine learning methods, including traditional PRNNs without incorporating the FA concept. The FA-PRNN method demonstrates an average accuracy of 96%, surpassing the accuracy of all other methods by a notable margin, ranging between 4% to 30% improvement. Moreover, in terms of complexity, the proposed FA-PRNN

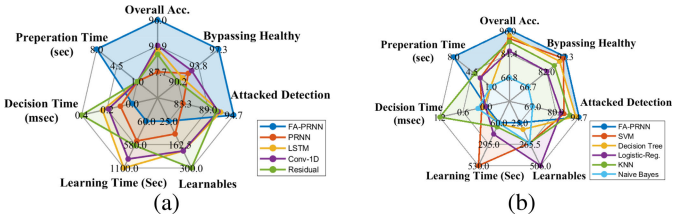


Fig. 9. Various performance metrics a) Proposed FA-PRNN VS DNN b) Proposed FA-PRNN VS common machine learning methods [7].

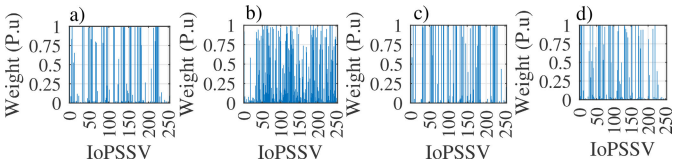


Fig. 10. Weights associated with the FA-PRNN Decision making for a) h_{Rec}, b) h_{Cir}, c) h_{Ell}, d) h_{CH}.

requires a smaller network size and a fewer learnable number, enabling faster training and decision-making times. However, it should be noted that the proposed method necessitates preparation time of around 8 seconds for the FA parameter estimation and flag vector calculation. The weights depicted in Fig. 10 illustrate the significance of each PSSV's weight in relation to various FA classifiers within the decision-making process of the FA-PRNN. A high weight, approaching 1, signifies that the FA classifier h effectively captures the representation of the normal operation region of the PSSV n, while a low weight suggests a less accurate representation by the FA classifier. In simpler terms, an FA classifier h is assigned a high weight when it can accurately represent the normal operation of the PSSV n and distinguish abnormal operation caused by SICA outside the FA. These weights are multiplied by the overall flag vector Fg at the FA-PRNN input layer, allowing for the aggregation of information from all PSSVs and facilitating decision-making using cumulative weighted flag values compared to the output neural threshold.

Fig.11 presents a comparison between the proposed FA-PRNN and traditional machine learning methods under different numbers of SICA affecting the active and reactive power set points of adjustable units. As depicted in Fig. 11a, when the attacker manipulates the set points with larger values, detecting the SICA becomes easier. However, when the variation range is smaller than 5%, the proposed FA-PRNN method demonstrates a greater capability, achieving detection accuracy of up to 88.5%, whereas traditional methods achieve a maximum accuracy of 52.1%. Furthermore, as the number of manipulated buses by SICA increases, the detection rate improves due to more significant changes caused by the PSSVs [35]. Fig. 11b illustrates the detection accuracy as a function of the changes in power system state (voltage and angle) caused by SICA. When SICAs induce small changes in the power system state, the performance of the traditional method degrades significantly, as indicated by the blue surface. In contrast, the proposed method maintains a stable performance with slight changes in the detection level, depicted by the yellow surface, demonstrating its ability to detect SICA even with minor variations in the PSSV. Fig. 11c displays the FAUR under different numbers of attacked buses by SICA. It is evident that as the number of attacked buses increases,

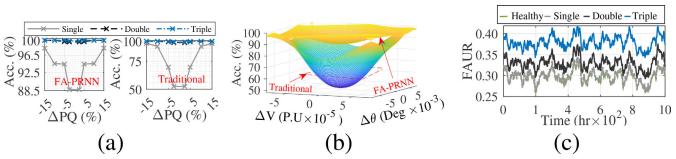


Fig. 11. Performance of the proposed FA-PRNN under different attacked buses a) Accuracy with respect to SICA over active and reactive power set points, b) Accuracy with respect to power system state variation c) FAUR under healthy and attacked operation.

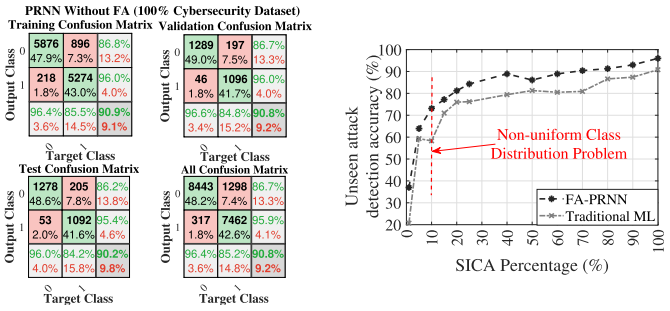


Fig. 12. Detection performance of the proposed FA-PRNN and traditional machine learning compared under various percentages of SICA during training and unseen attack. a) Confusion matrix of traditional PRNN using 100% SICA dataset for training, b) various percentages of SICA during training and unseen attack.

more PSSV depart from the FA, resulting in a higher FAUR. This increase allows the proposed method to detect SICA effectively.

B. Limited SICA Training Dataset

Most supervised machine learning methods face challenges achieving target performance with limited real-world cyber-attack data, necessitating an examination on the impact of the limited cyberattack data. Fig. 12 compares the detection performance of unseen SICA (not used during training) between the proposed FA-PRNN and traditional machine learning methods. In each test round, the percentage of SICA used during training progressively decreases, relying more on healthy data for model training. As illustrated, the FA-PRNN demonstrates superior performance with lower percentages of training data compared to traditional data-driven models, indicating its proficiency with smaller datasets. Notably, with just 20% (1752) samples, the model detects 80% of new SICA types. Conversely, traditional machine learning models experience decreased detection accuracy below 70% when SICA drops below 80%. Furthermore, performance declines significantly for both models when samples fall below 10%, highlighting the minimum sample requirement for training of 876 samples. Below this threshold, the model becomes uniclass due to the non-uniform distribution of input samples, favoring one class over the attacked class. To improve the accessibility of SICA datasets and enhance machine learning-based performance, cyber ranges or smart grid digital twins are employed for real-time analysis and practical data generation. In this paper, the computational algorithms simulate the optimal power flow process and the power-flow analysis replicate the power system operations under manipulated conditions caused by SICA [34], [36].

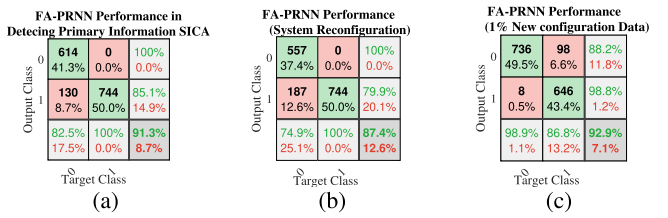


Fig. 13. Performance of the proposed FA-PRNN under a) unseen type of SICA over the primary information, b) system reconfiguration with no previous knowledge, c) system reconfiguration with 1% retrain on new system configuration.

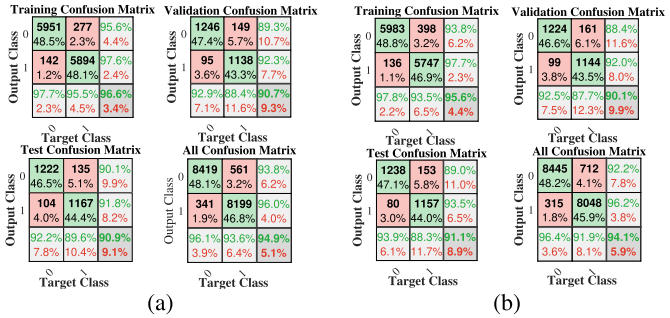


Fig. 14. Training, validation and testing confusion matrices for assessment of the FA-PRNN effectiveness under a) absence of two samples for every M-hour window and each PSSV, b) measurements uncertainty stemming from errors and noise with STD= 5%.

C. Unseen SICA and New System Configuration

To assess the model's capability to detect unseen SICA, the FA-PRNN is trained using cyberattacks targeting the secondary information on adjustable unit's set points. Subsequently, in this test, the model is evaluated against a new, unseen type of SICA targeting the primary information. In this scenario, the attacker is assumed to have access to the wind speed information at Bus 3, enabling them to manipulate the wind farm output power. The cyberattack is designed to be a sophisticated SICA, with enhanced capabilities to bypass existing cybersecurity layers. The attack is simulated over 744 hours distributed throughout the year.

Fig. 13a illustrates the performance of the proposed FA-PRNN in detecting the new type of SICA over the primary information. The true negative value (the detected SICA is 100% accurate in detecting the new pattern of SICA). The test demonstrates the capability of the proposed FA-PRNN in detecting new patterns in SICA. This is because the FA-PRNN learns the abnormal changes of the PSSV from normal operating FA rather than specific PSSV values, leading to a more generalized learning capability.

To evaluate the model's ability to operate under the system reconfiguration, the system is initially trained using data obtained under normal configurations. Subsequently, reconfiguration switches are added and simulated, including open circuits at Line 16 with the PV farm, the line between Buses 12 through 15, and the line between Buses 21 through 23. A dataset comprising 744 hours under both the normal and attacked operations is created and used for test purposes. The FA-PRNN is trained using the traditional system configuration, and the new data is solely used for testing in the first case.

Fig. 13b displays the performance of the proposed FA-PRNN under the reconfiguration case without prior training on the new configuration. The model achieves an average accuracy of 87.4%; however, the normal operating data have been mis-classified due to changes in the location of the PSSV relative to the FA. In Fig. 13c, the performance of the FA-PRNN is presented where the new configuration data for training is depicted, resulting in an accuracy of up to 93% under the new configuration.

D. Data Reliability and Quality Issues

Data missing due to communication failures and measurement uncertainty stemming from measurement device noises and errors are practical challenges that affect the performance of machine learning techniques. Therefore, it is crucial to evaluate the performance of the proposed FA-PRNN under these circumstances. To gauge the impact of missing data on the method's performance, the FA-PRNN is retrained using a new dataset containing two missing samples within each 24-hour window. Fig. 14a illustrates the FA-PRNN's performance under the scenario of two missing data samples. The overall accuracy experiences a slight change of (2.1-1.1%) compared to the original performance. This minor alteration is attributed to the unlikelihood of significant changes occurring within the FA parameters. Such changes may only occur if outlier points are missing, and any impact is also contingent on the availability of nearby points to replace the missing samples.

In another avenue, measurement noise and error are represented by the error function associated with measurements obtained from each device. Typically, the error is assumed to follow a Gaussian distribution, with a mean value of $\mathbb{E}(e(x)) = 0$ and a standard deviation $\sigma(x)$ representing the error attributed to noise factors. For PMU measurements, the standard deviations for magnitude and angle values are 0.7% and 0.7 crad, respectively. Conversely, PQ sensors have a standard deviation of 1% for active and reactive power measurements [30]. The introduction of measurement error and noise expands the probability distribution within which each measurement may fall. Instead of having a single value for each measurement, now each measurement is represented by a range, with higher probability at the center and decreasing probability as it moves away. This effect is also reflected in the representation on the complex plane. In the absence of error, each measurement is represented by a single point in the complex plane. However, with the introduction of error, each measurement is now represented by a circular range, indicating the potential locations of the point due to the error. The variation within each point, in the worst case, is bounded by the maximum possible error value. Given that the variation induced by introducing the measurement error and noise is minimal, the impact on the FA estimated parameters is bounded by $|2 \times \max(e(x))|$. To explore the effects of introducing error and noise on the proposed FA-PRNN, the noise and error function of each measurement type are simulated to introduce uncertainties in the measurement location. It is important to note that the uncertainty is assumed to be 5% for all measurements, representing the worst-case scenario for both PMUs and PQ sensors. Fig. 14b depicts the performance of the proposed FA-PRNN when introducing a 5% measurement error and noise function. The data indicates

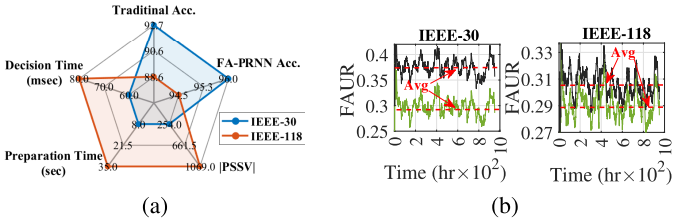


Fig. 15. Performance of the proposed FA-PRNN method when applied to the IEEE 30 and 118 bus test systems a) performance parameters b) FAUR.

that the overall performance has experienced a slight change from the baseline, approximately ranging from 1.9% to 2.9%.

In summary, the impact of data quality, in the form of missing data and measurement device error and noise, can be summarized as follows: 1) Data missing results in a narrower FA, potentially leading to cases of healthy operation being misidentified as attacks, as they fall outside the FA. In Fig. 14a, the True Negative Rate (healthy data detected as attacks) increases to 1.9% compared to 1.1% in the baseline case. However, the overall performance of the proposed FA-PRNN is only slightly impacted, by 1.1-2.1%. 2) Representation of measurement device error and noise leads to a wider FA, potentially resulting in cases of attacked operation being misidentified as healthy, as they fall within the FA. In Fig. 14b, the False Negative Rate (attacked data bypassed) increases to 4.1% compared to 1.8% in the baseline case. However, the overall performance of the proposed FA-PRNN is only slightly impacted, by 1.9-2.9%.

It's important to emphasize that the proposed SICA detection layer operates within a localized environment, wherein historical data is stored in a local server, and FA parameter estimation and FA-based SICA detection occur on a local machine. As a result, cyberattacks on the proposed FA-PRNN can only target data shared from the local server and transmitted to the local machine via local communication network. Cyberattacks on the historical data window used for the FA parameter estimation can occur in two different ways as follows: 1) by removing data from the data window, and 2) by introducing false data through manipulation of the PSSVs within the historical window. The former method resembles the impact of data missing issues, resulting in a smaller FA estimation with similar consequences discussed. Meanwhile, the latter method is akin to introducing noise within the measurements as discussed, albeit with an unknown $e(x)$.

E. Scalability of the Proposed Feasibility Area Concept

The IEEE 118-bus system is utilized to investigate the performance of the proposed FA-PRNN method when applied to large power systems. Fig. 15a compares different performance metrics between the IEEE 30 and 118 bus test systems. The results show that FA-PRNN exhibits superior performance in SICA detection for both test systems compared to traditional methods. From the computational perspective, utilizing the FA concept for larger systems increases the time required for FA parameters and flag vector estimation due to increasing the size of PSSV $|PSSV|$. The preparation time increases linearly with the size of the PSSV, where ratio between data preparation time and PSSV size remains constant, keeping the estimation time within a range of seconds, which satisfies the computational requirements for detecting stealthy attacks. However, considering that the proposed method aims at detecting SICA that have already impacted the system, this layer is designed for deep assessment of the system state of health, where accuracy takes precedence over computational time. Fig. 15b illustrates the FAUR of the IEEE 30 and 118-bus systems, indicating the number of PSSV located outside the FA under SICA conditions for each operation hour. As noted in both systems, the FAUR under the attack is larger than the one during normal operations. However, since the IEEE 118-bus system has a larger number of PSSVs, the FAUR is associated with a smaller scale, and the gap between the healthy and attacked operation becomes narrower. Nevertheless, the FA-PRNN demonstrates its superiority in the detection of SICA for large power systems.

VII. Conclusion

In this paper, a new method is proposed for SICA detection to identify cyberattacks that have bypassed the BDD and the pre-occurrence FDIA detection layers. The concept of the FA is developed and applied to form deterministic and non-deterministic classes to improve the accuracy of the SICA detection. Using a window of historical data, rectangular, circular, elliptic, and convex-hull shapes are developed to represent the FAs for PSSV. Various performance metrics, including TP and FN are used to numerically evaluate the performance of the proposed method. Among various FA characteristics, the elliptic shape shows the highest ability to detect SICA while the rectangular shape has the highest accuracy for allowing the healthy data to pass through. However, each shape shows a very unique performance for a certain group of PSSV; hence, for each shape, every PSSV is associated with a weighting factor representing the quality of that FA shape. Via incorporating the proposed FA concept, the PRNN is able to more effectively detect the patterns of SICA through the use of flag vector information for each classifier. Using the PRNN to detect the pattern of PSSV with respect to the FA, a very high performance up to 95.35% is achieved in detecting stealthy attacks infiltrated through the BDD and correctly bypassing 97.31% of healthy operation. The utilization of the FA concept provides further advantages, making the learning process superior via: 1) reducing the overlap between healthy and attacked operation states, 2) considering the time frame as a factor that indicates the existence of the attack and 3) heightened sensitivity to measurement noise, and reduced sensitivity to state variations—common issues encountered in traditional machine learning methods. Thus, the proposed FA-PRNN demonstrates superior performance compared with other classification methods.

References

[1] Y. You, Z. Li, and T. J. Oechtering, "Non-cooperative games for privacy-preserving and cost-efficient smart grid energy management," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 423–434, 2023.

[2] Z. Zhang, R. Deng, Y. Tian, P. Cheng, and J. Ma, "SPMA: Stealthy physics-manipulated attack and countermeasures in cyber-physical smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 581–596, 2022.

[3] T. Menze. (2020). *The State of Industrial Cybersecurity in the Era of Digitalization*. [Online]. Available: https://ics.kaspersky.com/media/KasperskyARCICS-2020-Trend-Report.pdf

[4] J. Henriques, F. Caldeira, T. Cruz, and P. Simões, "A survey on forensics and compliance auditing for critical infrastructure protection," *IEEE Access*, vol. 12, pp. 2409–2444, 2024.

[5] M. Jafari, M. A. Rahman, and S. Paudyal, "Optimal false data injection attack against load-frequency control in power systems," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5200–5212, 2023.

[6] W. Xu, I. M. Jaimoukha, and F. Teng, "Robust moving target defence against false data injection attacks in power grids," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 29–40, 2023.

[7] D. Du et al., "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *J. Modern Power Syst. Clean Energy*, vol. 11, no. 3, pp. 727–743, May 2023, doi: 10.35833/MPCE.2021.000604.

[8] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1592–1602, Jul. 2016.

[9] H. Yang and Z. Wang, "A false data injection attack approach without knowledge of system parameters considering measurement noise," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 1452–1464, Jan. 2024, doi: 10.1109/JIOT.2023.3288983.

[10] Q. Zhang, F. Li, and X. Wang, "Cyber-impact analysis for ISO revenue adequacy considering FDIA in real-time market operations," *IEEE Trans. Power Syst.*, vol. 38, no. 5, pp. 4042–4053, Sep. 2023.

[11] Y. Suo, S. Chai, R. Chai, Z.-H. Pang, Y. Xia, and G.-P. Liu, "Security defense of large-scale networks under false data injection attacks: An attack detection scheduling approach," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 1908–1921, 2024.

[12] A. S. Musleh, G. Chen, Z. Yang Dong, C. Wang, and S. Chen, "Attack detection in automatic generation control systems using LSTM-based stacked autoencoders," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 153–165, Jan. 2023.

[13] Z. Zhang, R. Deng, and D. K. Y. Yau, "Vulnerability of the load frequency control against the network parameter attack," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 921–933, Jan. 2024.

[14] M. Ali, G. Kaddoum, W.-T. Li, C. Yuen, M. Tariq, and H. V. Poor, "A smart digital twin enabled security framework for vehicle-to-grid cyber-physical systems," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5258–5271, 2023.

[15] S. Ghosh, M. R. Bhatnagar, W. Saad, and B. K. Panigrahi, "Defending false data injection on state estimation over fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1424–1439, 2021.

[16] H. Zhang, K. Zeng, and S. Lin, "Federated graph neural network for fast anomaly detection in controller area networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1566–1579, 2023.

[17] K. Grosse, L. Bieringer, T. R. Besold, B. Biggio, and K. Krombholz, "Machine learning security in industry: A quantitative survey," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1749–1762, 2023.

[18] M. N. Kurt, Y. Yilmaz, and X. Wang, "Secure distributed dynamic state estimation in wide-area smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 800–815, 2020.

[19] B. Li, R. Lu, G. Xiao, T. Li, and K.-K. R. Choo, "Detection of false data injection attacks on smart grids: A resilience-enhanced scheme," *IEEE Trans. Power Syst.*, vol. 37, no. 4, pp. 2679–2692, Jul. 2022.

[20] H. H. Alhelou and P. Cuffe, "A dynamic-state-estimator-based tolerance control method against cyberattack and erroneous measured data for power systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4990–4999, Jul. 2022.

[21] W. Qiu et al., "Cyber-attack identification of synchrophasor data via VMD and multifusion SVM," *IEEE Trans. Ind. Appl.*, vol. 58, no. 2, pp. 1456–1465, Mar. 2022.

[22] A. M. Sawas, H. Khani, and H. E. Z. Farag, "On the resiliency of power and gas integration resources against cyber attacks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3099–3110, May 2021.

[23] H. T. Reda, A. Anwar, A. Mahmood, and N. Chilamkurti, "Data-driven approach for state prediction and detection of false data injection attacks in smart grid," *J. Modern Power Syst. Clean Energy*, vol. 11, no. 2, pp. 455–467, Mar. 2023.

[24] Z. Chen, J. Zhu, S. Li, Y. Liu, and T. Luo, "Detection of false data injection attacks on load frequency control system with renewable energy based on fuzzy logic and neural networks," *J. Modern Power Syst. Clean Energy*, vol. 10, no. 6, pp. 1576–1587, Nov. 2022.

[25] R. Qi, J. Zheng, Z. Luo, and Q. Li, "A novel unsupervised data-driven method for electricity theft detection in AMI using observer meters," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–10, 2022.

[26] J. Shi, S. Liu, B. Chen, and L. Yu, "Distributed data-driven intrusion detection for sparse stealthy FDI attacks in smart grids," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 3, pp. 993–997, Mar. 2021.

[27] J. Xu, Z. Wu, T. Zhang, Q. Hu, and Q. Wu, "A secure forecasting-aided state estimation framework for power distribution systems against false data injection attacks," *Appl. Energy*, vol. 328, Dec. 2022, Art. no. 120107.

[28] A. A. E. Elsayed, H. E. Z. Farag, and A. Asif, "Cyber physical security of energy hubs using feasibility area estimation," in *Proc. Int. Telecommun. Conf. (ITC-Egypt)*, Jul. 2023, pp. 696–700.

[29] A. A. E. Elsayed, E. Z. H. Farag, A. Tauqeer, F. Shahid, and A. Asif, "Application of feasibility area for cybersecurity of electric power systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2023, pp. 1–5.

[30] A. Bhattacharjee, A. K. Mondal, A. Verma, S. Mishra, and T. K. Saha, "Deep latent space clustering for detection of stealthy false data injection attacks against AC state estimation in power systems," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2338–2351, May 2023.

[31] F. Cheng, S. Shu, L. Zhang, M. Tan, and J. Qiu, "An evolutionary multitasking method for high-dimensional receiver operating characteristic convex hull maximization," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 8, no. 2, pp. 1699–1713, Apr. 2024.

[32] W. Wang and S. Wang, "Efficient point-in-polygon tests by grids without the trouble of tuning the grid resolutions," *IEEE Trans. Vis. Comput. Graphics*, vol. 28, no. 12, pp. 4073–4084, Dec. 2022.

[33] Z. Yang, "Adaptive powerball stochastic conjugate gradient for large-scale learning," *IEEE Trans. Big Data*, vol. 9, no. 6, pp. 1598–1606, Dec. 2023.

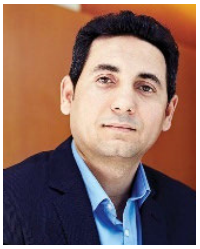
[34] M. M. Roomi, S. M. S. Hussain, D. Mashima, E.-C. Chang, and T. S. Ustun, "Analysis of false data injection attacks against automated control for parallel generators in IEC 61850-based smart grid systems," *IEEE Syst. J*, vol. 17, no. 3, pp. 4603–4614, Sep. 2023, doi: 10.1109/JSYST.2023.3236951.

[35] M. Zhang, Z. Wu, J. Yan, R. Lu, and X. Guan, "Attack-resilient optimal PMU placement via reinforcement learning guided tree search in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1919–1929, 2022.

[36] D. Mashima, M. M. Roomi, B. Ng, Z. Kalberczyk, S. M. Suhail Hussain, and E.-C. Chang, "Towards automated generation of smart grid cyber range for cybersecurity experiments and training," in *Proc. 53rd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.-Supplemental Volume (DSN-S)*, Jun. 2023, pp. 49–55.

Ahmed Abd Elaziz Elsayed (Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) in electrical engineering from Assiut University, Egypt, in 2018 and 2020, respectively. He is currently pursuing the Ph.D. degree with York University, Toronto, ON, Canada. His research interests include smart grid operation and management, cybersecurity, machine learning, and synchronized real-time monitoring systems.

Hadi Khani (Member, IEEE), photograph and biography not available at the time of publication.



Hany Essa Zidan Farag (Senior Member, IEEE) received the B.Sc. (Hons.) and M.Sc. degrees in electrical engineering from Assiut University, Assiut, Egypt, in 2004 and 2007, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2013. Since 2013, he has been with the Department of Electrical Engineering and Computer Science, Lassonde School of Engineering, York University, Toronto, ON, Canada, where he is currently an Associate Professor and the York Research Chair in integrated smart energy grids. His current research interests include the integration of distributed and renewable energy resources, transportation electrification, green hydrogen generation and storage, modeling, analysis, design of microgrids, applications of agents, and blockchain technologies in smart grids.