A Lightweight Time-Adaptive Data-Driven Method for Detecting Multi-False Data Injection in Smart Meters

Zhenyuan Du, *Graduate Student Member, IEEE*, Ziming Yan, *Member, IEEE*, and Yan Xu, *Senior Member, IEEE*

***Abstract*— False data injection attacks (FDIA) in smart meters are growing concerns. Conventional detection methods are difficult to be deployed on resource-limited edge devices and insufficiently adaptive to different attack scenarios and random attack commencement times. To address these issues, this paper proposes a lightweight time-adaptive data-driven FDIA detection method. First, a lightweight hybrid FDIA detector is developed, integrating the MobileNet and a statistical indicator computing block for features extraction, and a deep learning process for classification. The load data is dimensionally augmented by recurrence plots (RPs) and fed into a series of detectors operating at different time scales. Then, a time-adaptive structure to accommodate diverse attack types and timing is designed, comprising multiple FDIA detectors and a credibility evaluation process. The detection decision can be made at an appropriately early time and with high accuracy. To optimize the overall performance, NSGA-II is used to search trade-off solutions between detection speed and accuracy. Simulation results on a dataset including 20 residents and eight types of FDIA demonstrate that the proposed method outperforms benchmarks in terms of detection accuracy and speed. Moreover, the proposed method can adapt to different detection scenarios by offering different solutions with balanced speed-accuracy.**

***Index Terms*—Cyber-attack, false data injection attack, MobileNet, time-adaptive, multi-objective optimization.**

I. Introduction

A. Research Background and Motivation

Nowadays, the cybersecurity of smart meters is receiving increasing attention [1] for both end users and power grids. A common cyber-attack on smart meters is the false data injection attack (FDIA), which usually manipulates meter readings to interfere with energy management and demand response of the users [2]. While a number of detection methods have been developed to counter FDIA, many are designed for specific types of attacks and fail to account for the practical challenges of real-world deployment, such as random attack timing, multiple types of attacks, and hardware resource limitations. This paper aims to propose a lightweight, time-adaptive, and generalized FDIA detection method that can handle diverse FDIA types and adapt to varying conditions in smart meter environments.

B. Literature Review

The detection of diverse FDIA types in smart meters is a widely studied topic. Typical FDIA types include scaling, ramping, and pulse attacks. To detect various FDIA types in real-world scenarios, it is crucial to develop a versatile detection method capable of handling a wide range of attack types. In the literature, [3] identifies four distinct FDIA types. The FDIA attacks to evade state estimation detection are also investigated by adhering to physical laws. However, in practical scenarios, attackers may only have limited knowledge of the internal structure and operational state of the power system or smart meters [4]-[5]. [6] named this phenomenon as imperfect FDIA and proposes an unbalanced distribution networks state estimation for FDIA detection and [7] analyzes the impact of the degrees of freedom of attack vectors available on the detector. Consequently, practical modeling of FDIA tend to rely on simpler and effective attack strategies—such as injecting noise, modifying meter readings in specific patterns rather than perfectly coordinated attacks that require full system knowledge.

In addition to the research on FDIA attack methods, many FDIA defense methods are also proposed. A support vector machine (SVM)-based method and a parallel computing-based deep learning method are proposed in [8] and [9]. [10] proposes an electricity theft detection method for smart meters, combining maximum information coefficient (MIC) and clustering using the CFSFDP technique. Furthermore, [11] proposes a temporal graph neural network (T-GNN)-based FDIA detection method, which is mainly focusing on localization of FDIA in microgrids. [12] and [13] are also trying to solve the FDIA problem by proposing a Fourier transformation-based method and ensemble learning. Besides the previously introduced work, [14] proposes a big data-based FDIA detection method and modeled 6 different FDIA types, federated learning and semi-supervised deep learning is also considered to detect the FDIA in [15] and [16]. A system information-free AC FDIA detection method is also proposed in [17]. Although detectors for a particular type of FDIA have been constructed for either smart grids or smart meters, they remain limited in their versatility to detect a board spectrum of different FDIA types. As distributed computing in power systems is becoming prevalent, the deployability of smart meters FDIA detection method is also becoming imperative [18]-[20]. Recently, there has been a rise of research in lightweight model [21] and training cost reduction [22]-[24] in the field of load forecasting. [25] proposes a lightweight principal component analysis (PCA)-canonical correlation analysis (CCA)-based FDIA detection in wide-area monitoring system. In our previous work [26], we proposed a dimensional augmentation-based FDIA detection method to detect Gaussian-distributed additive stealthy attacks with VGGNet applied to augmented 1-D load data. However, prior research rarely discusses the deployability of lightweight FDIA detection models for smart meters.

Besides, while previous works mainly focus on FDIA detection accuracy, versatility, and model deployability, most of them ignore the timing of attacks, often assuming that input data window is either entirely clean or fully attacked. In practice, FDIA in smart meters can initiate randomly, and the attack may continuously affect subsequent data. As a result, when FDIA

The authors are with the Center for Power Engineering, School of Electrical and Electronic Engineering, Nanyang Technological University, 639798, Singapore (e-mail: e220188@e.ntu.edu.sg; yanzmics@gmail.com; xuyan@ntu.edu.sg)

begins, the input data to detection model consists of a mix of genuine and compromised information over time. This mixture of genuine and attacked data could affect the efficacy of existing models. If delayed, by the time these models detect FDIA, the input data would be already fully compromised. In addition to the [14]-[16], [27]-[28] also can support this statement. The FDIA modeling part of [15] and [27] is partially attacked data-based, [16] shows the load data attacked by fully interfered FDIA. [28] expressed the attack process of the fully interfered FDIA considered in a functional way. Similar challenge has been reported in power converter fault diagnosis area, where the fault may happen randomly [29].

C. Contributions of This Paper

To address the challenges in smart meter FDIA detection model deployability and versatility for diverse FDIA types and random attack commencement times, this paper proposes a novel lightweight time-adaptive data-driven FDIA detection method. The proposed method consists of a series of modified MobileNet-based FDIA detectors under a time-adaptive decision-making structure, and NSGA-II based off-line optimization of credibility thresholds. While the proposed method may be potentially adaptable to other smart grid time series data FDIA detection, this paper mainly investigated frameworks for superior performance in smart meter FDIA detection. The main contributions of this paper are summarized as follows:

- To enhance versatility of FDIA detection against a wide range of attack types, a modified MobileNet-based FDIA detector is proposed. The proposed detector integrates the features from dimensionally augmented smart meter data (as 2-dimensional image) and the statistical indicators, showing better versatility for a broader range for FDIA types.
- A lightweight framework is developed in the modified MobileNet-based FDIA detector, based on the Depthwise convolution, RELU6 activation function, and inverted residual structure. The size, running time and computational complexity of the FDIA detector is reduced to improve deployability for edge devices, while maintaining sound detection accuracy, making it highly suitable for deployment in edge computing environments such as smart meters.
- A time-adaptive detection process for dynamic and random timing of attack onsets, which leverages a credibility-based time-adaptive structure and series of modified MobileNet-based FDIA detectors to sequentially determine credibility and detector size. The time-adaptive structure can detect the smart meter data of different time scales and detect FDIA in a timely manner. By using the NSGA-II to off-line optimize the credibility thresholds, the proposed method balances performance across various smart meter environments, ensuring adaptability to varying detection requirements in real-world applications.

The rest of the paper is organized as follows. Section II describes the problem formulation. The proposed lightweight time-adaptive data-drive FDIA detection method is presented in Section III. Simulation results and numerical analysis are shown in Section IV, followed by the conclusions in Section V.

II. Problem Descriptions

A. Dimensional-Augmentation-based Feature Extraction

The attacked data sample of smart meters D_{sm}^{att} is formulated as:

$$D_{sm}^{att} = f_{FDIA}\left(D_{sm}^{gen}\right) \tag{1}$$

where $D_{sm}^{gen} = (x_c^{sm}, \cdots, x_{c+n}^{sm})$ denotes the sample with n load data measurements $x_{(\cdot)}^{sm}$, and x_c^{sm} represents the data point at current time.

Dimensional augmentation-based methods are effective at detecting stealth FDIA by augmenting features of smart meter data [26]. To augment smart meter data dimension, based on recurrence plots (RPs) [30], the 1-dimensional smart meter data can be converted into 2-dimensional image data. The dimensionally augmentation processing of RPs is formulated as:

$$\boldsymbol{R} = \begin{bmatrix} R_{1,1} & \cdots & R_{1,n} \\ \vdots & \ddots & \vdots \\ R_{n,1} & \cdots & R_{n,n} \end{bmatrix} \tag{2}$$

$$R_{i,j}(\varepsilon) = \Theta(\varepsilon - ||x_i - x_j||), \quad i,j = 1,\ldots,n \tag{3}$$

where $R_{i,j}$ represents the ith row jth column element of the 2-dimensional RPs matrix, n is the number of measured data points $\{x_i\}_{i=1}^{n}$, ε is a threshold distance, $\Theta()$ is the Heaviside function [26], $||\cdot||$ is a norm (L_1-norm in this paper).

According to (3), once the FDIA satisfied the condition in (4), the difference between genuine smart meter data and attacked data will not be reflected in RPs. Some types of FDIA, such as scaling attacks, meet the condition in (4). The smaller the differences between both sides of (4), the less distinguishable via the RPs for genuine data and attacked data. Therefore, (4) also indicates a lack of detection capability for existing dimensional augmentation-based methods when the attacks are highly similar to actual data.

$$\left\|x_i^{sm} - x_j^{sm}\right\| = \left\|x_i^{sm,att} - x_j^{sm,att}\right\|, i,j = 1,\ldots,n, \forall i,j \tag{4}$$

When a FDIA type satisfies (4), this FDIA type can also be established by

$$x_i^{sm,att} = ax_i^{sm} + b, \forall i \in [1,n] \tag{5}$$

where disturbance parameters a is a non-zero constant and b is a constant. The general formulation of FDIA may evade detection by preserving statistical consistency (e.g., mean/variance) while distorting temporal correlations, bypassing conventional detectors' reliance on residual thresholds for anomalies.

B. Deployability of Model

The main concern on the deployability of an ANN model in the hardware device is the running random access memory (RAM) size M_{Detect} and computational complexity of forward propagation C_{Detect}, which are formulated by:

$$M_{Detect} = PN_{Detect} \cdot s \tag{6}$$

$$C_{Detect} = C_{mul} + C_{add} \tag{7}$$

where s denotes the memory size of the model parameter, PN_{Detect} is the number of parameters in a detector. C_{mul} and C_{add} are the number of multiplication and addition in once forward propagation, representatively. A smaller M_{Detect} and C_{Detect} facilitate the deployment of the model on edge devices.

C. Random FDIA Commencement Timing in Smart Meter's Data

For most existing FDIA detection methods, the attack timing is not considered in the model design. One common assumption is that the input window of data D_{sm}^{gen} is fully interfered by FDIA:

$$D_{sm}^{att,all} = \{x_c^{sm,att}, \cdots, x_{c+n}^{sm,att}\} \quad (8)$$

$$x_i^{sm,att} = f_{FDIA}(x_i^{sm}) \quad (9)$$

where $x_c^{sm,att}$ and $x_{c+n}^{sm,att}$ are the smart meter data points at c and $c+n$ time, $c+n$ is later than c. However, the attack starting time of FDIA to D_{sm}^{gen} is always random in practice, so that input data could be partially affected by FDIA. The partially attacked data $D_{sm}^{att,part}$ can be formulated as

$$D_{sm}^{att,part} = \{x_c^{sm}, \cdots, x_{c+k}^{sm}, x_{c+k+1}^{sm,att}, \cdots x_{c+n}^{sm,att}\} \quad (10)$$

where k represents the attack starting time, which reflects a mixture of genuine and attacked data in the input to attack detector.

In most existing methods, only the fully attacked attack data is used in training and testing process, and their objective function can be established as:

$$min_{\omega_{FDIA}} L\left(\omega_{FDIA}, D_{sm}^{att,all}\right) \quad (11)$$

where ω_{FDIA} is the initial parameters of FDIA detection model, $L(\cdot)$ denotes the loss function. However, when the genuine data is mixed into attacked data as (9) shows, the detection performance of model that is trained by fully covered attack data degrades significantly. Arising from the above, the input of partially covered attack data will lead to the low-quality detection result of existing FDIA detection model.

III. Proposed Methodology

A. Framework of The Proposed Method

The framework of the proposed method is shown in Fig. 1. The real-time smart meter data and their historical data are collected from the smart meter and partitioned into different samples with different time scales. The samples are dimensionally augmented into 2-dimensional image data by RPs as shown (2)-(3). The RPs and the 1-dimensional smart meter data of different samples are fed into the corresponding modified MobileNet-based FDIA detector for attack detection [31].

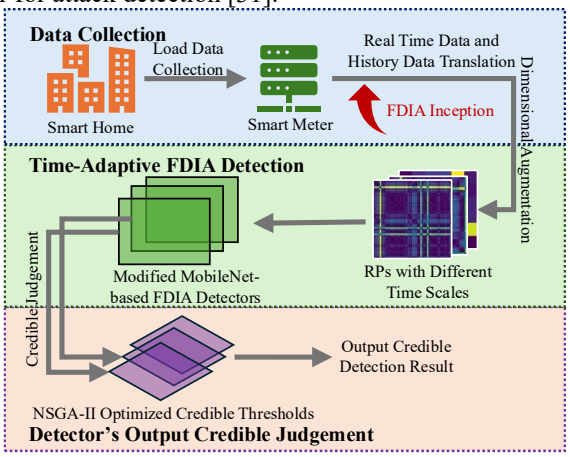


Fig.1. The framework of the proposed method

Furthermore, this paper particularly designs RPs for smart meter data, as the RPs has superior ability to capture the variety features of different smart meter data. The randomness of smart meter data can also be captured and mapped into visual distinguishable 2-dimensional data by RPs. Each modified MobileNet-based FDIA detector, a credible threshold optimized by NSGA-II [32] is checked, which is to judge whether the detection result is credible. The credibility judgement process is sequential, once a detector's detection result is credible, the remaining detectors will not process the data in current time.

B. Lightweight MobileNet-based FDIA Detector

A modified MobileNet-based FDIA detector is proposed to meet the requirements of high efficiency, lightweight and universality for FDIA detectors. The structure of the modified MobileNet-based FDIA detector is shown in Fig. 2, which consists of three parts: a MobileNet, statistical indicators computing block, and an ANN. In the process, first, the RPs data generated by (2)-(3) is fed into MobileNet to identify the output probabilities of class (i.e., attack type probability). Due to the MobileNet only accepting the image data, an extra ANN is leveraged to aggregate the results from MobileNet and statistical indicators, which subsequently determines classification result (i.e., type of attacks). The reason for using 1-d data to calculate statistical indicators is that RPs will distort the original numerical characteristics of the data while processing the load data to further powerlessness when facing certain FDIA types (detailed in (4)-(5)). Therefore, 1-d data is used to calculate the numerical statistical indicators of the original load data and ANN is used to assist in determining the type of FDIA.

As the proposed method aggregates both statistical indicators and image input, the detector can identify the parameters of disturbance parameters a and b in (5). Note that the parameter size of extra ANN is small enough to not significantly affect the practical deployability of whole detector.

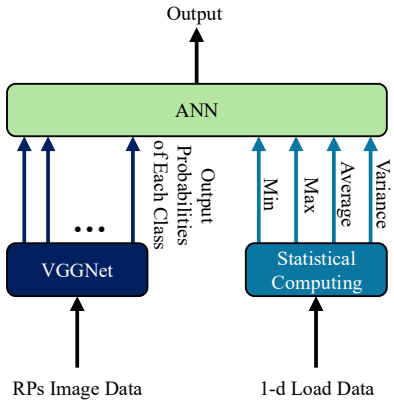


Fig. 2. Structure of the modified MobileNet-based FDIA detector.

The objective function of modified MobileNet-based FDIA detector is modeled as:

$$min_{\omega_i} L\left(\omega_i, \left(D_i^{R,Gen}, D_i^{X,Gen}\right), \left(D_i^{R,Gau}, D_i^{X,Gau}\right), \cdots\right) \quad (12)$$

where ω_i represents the model parameters of ith modified MobileNet-based FDIA detector, $L(\cdot)$ is loss function, $D_i^{X,Gen}$ and $D_i^{X,Gau}$ are genuine and Gaussian attacked 1-dimensional sample datasets of detector i, $D_i^{R,Gen}$ and $D_i^{R,Gau}$ are the RPs datasets of genuine and gaussian attack.

As the modified MobileNet-based FDIA detector is partitioned into two parts, objective function (12) is segmented into two parts:

$$\omega_i^{MobileNet,*} = argmin_{\omega_i^{MobileNet}} L\left(\omega_i^{MobileNet}, D_i^{R,Gen}, D_i^{R,Gau}, \cdots\right) \quad (13)$$

$$\omega_i^{ANN,*} = argmin_{\omega_i^{ANN,*}} L\begin{pmatrix}\omega_i^{ANN}, F_{MobileNet}\left(\omega_i^{MobileNet,*}, D_i^{R,Gen}, \cdots\right) \\ , D_i^{SI,Gen}, D_i^{SI,Gau}, \cdots\end{pmatrix} \quad (14)$$

where $\omega_i^{MobileNet,*}$ and $\omega_i^{MobileNet}$ are the optimal and initial parameters of MobileNet, $\omega_i^{ANN,*}$ and ω_i^{ANN} are the optimal and initial parameters of ANN, $F_{MobileNet}$ is the MobileNet model, $D_i^{SI,Gen}$ and $D_i^{SI,Gau}$ are the genuine and Gaussian attack statistical indicators (max, min, average, and variance) datasets of 1-dimensional smart meter data.

The network structure and parameters setting of the MobileNet is shown in Fig. 3 and Table I. The MobileNet uses 2 different types of bottlenecks, which is shown in Fig. 3. Depthwise convolution [33] and ReLU6 [34] activation function are also deployed in both types of bottlenecks. The first type of bottleneck is residual connection-based, the second type of bottleneck is linear conntection-based. Based on these two types of bottleneck block, the detail network parameters setting is shown in Table I. Where in Table I, *t* is the expansion factor of current stage, *c* is the number of channels in current stage, *n* is the repeat number of bottleneck block, *s* is stride size, when s=2, the second type of bottleneck is used, otherwise the first type of bottleneck is used.

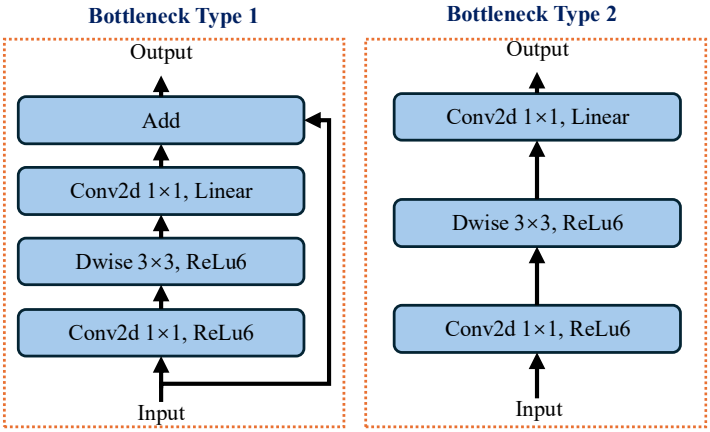


Fig. 3. Two types of bottlenecks used in MobileNet for image feature extraction on the dimensionally augmented smart meter data.

TABLE I
PARAMETERS SETTING OF MOBILENET

Input shape of image	Operator	*t*	*c*	*n*	*s*
224*224*3	Conv2d	-	32	1	2
112*112*32	Bottleneck	1	16	1	1
112*112*16	Bottleneck	6	24	2	2
56*56*24	Bottleneck	6	32	3	2
28*28*32	Bottleneck	6	64	4	2
14*14*64	Bottleneck	6	96	5	1
14*14*96	Bottleneck	6	160	5	2
7*7*160	Bottleneck	6	320	1	1
7*7*320	conv2d 1*1	-	1280	1	1
7*7*1280	avgpool 7*7	-	-	1	-
1*1*1280	conv2d 1*1	-	k	-	-

In Table I, the first convolution layer in each bottleneck serves as the expansion layer, which increases the data's dimensionality, while the third convolution layer acts as the projection layer, compressing the data back to its original dimension. This compress-expand-compress structure is also known as the inverted residuals. The expansion factor *t* in Table I also represents the proportion of data's dimensionality in current block. In convolution operations, higher-dimensional data usually contains more information, so the MobileNet first improves the dimensions of the data, and then performs convolution operations in higher dimensions to obtain more effective features of the data. However, the above inverted structure undoubtedly increases the computational and complexity of the model. Thus, as shown in Fig. 3, the MobileNet deploys Depthwise convolution and ReLU6 activation function to remedy the high computational and complexity caused by inverted residuals, even enhance the lightweight of the model.

The computing process of Depthwise convolution is divided into Depthwise $C^{Dep}(\cdot)$ and pointwise $C^{Poi}(\cdot)$ convolution, which are formulated as:

$$C^{Dep}(k,i,j) = \sum_{m,n} x(k, i+m, j+n) \cdot w(k,m,n) \quad (15)$$

$$C^{Poi}(k',i,j) = \sum_{k} C^{Dep}(k,i,j) \cdot w(k',k) \quad (16)$$

where *k'* is the index of output channels.

To study the resources reduction, the proportion of computation complexity of standard Conv2d and Depthwise is formulated as:

$$\frac{o(C^{Dep}+C^{Poi})}{o(C)} = \frac{1}{D^{k'}} + \frac{1}{mn} \quad (17)$$

where, $D^{k'}$ is the number of output channels, C is the standard Conv2d operation, *m* and *n* are the size of convolution kernel. This equation implies that compared with standard convolution operation, the reduction in computation of Depthwise convolution is significant.

To further optimize for edge deployment, MobileNet also utilizes the ReLU6 activation function, a variation of the ReLU function that limits maximum output to 6, which is particularly effective for low-precision computation often found in edge devices. The differentiation for ReLU6 is formulated as:

$$\frac{d\mathrm{ReLu6}(x)}{dx} = \begin{cases} 0 & x \geq 6 \\ \frac{d\mathrm{ReLu}(x)}{dx} & x < 6 \end{cases} \quad (18)$$

where, the differentiation above implies that a low-resource inference can be achieved and the excessive fluctuations in activation values and gradients can be mitigated.

To summarize, the modified MobileNet above has a lightweight model scale and fewer computing power requirements, while also providing excellent detection performance. The design enables efficient feature extraction while minimizing computational complexity and model size, making it well-suited for resource-constrained edge devices. And the ANN in Fig. 2 make sure the proposed detector can effectively tackle the shortcoming of our previous work. This combination maintains MobileNet's performance, enabling lightweight, high-efficiency inference. The modified MobileNet-based FDIA detector enhances detection accuracy and is adaptable for real-time deployment. Consequently, the modified lightweight MobileNet-based FDIA detector can compensate for the detection deficiencies of the models mentioned in Section II.A. Then, the modified MobileNet-based FDIA detector will be deployed in the time-adaptive structure for each time scale.

C. Time-Adaptive FDIA Detection Process

The modified MobileNet-based FDIA detector leverages a time adaptive structure, which has been initially proposed and discussed [35]-[36]. The principle of time-adaptive structure is to deploy a series of detectors for different time scales. Each detector corresponds to a specific time scale, determining classification probabilities for genuine data or attacked data. The structure of the proposed time-adaptive FDIA detection method is shown in Fig. 4. In Fig. 4, the real-time smart meter data point and its previous k-1 data points are marked as x_0 and x_1 to x_k. When m time scales, T_1 to T_m, from x_1 to x_k, are chosen, then $T_i \neq x_i$ and $i \leq k$ for any time scale i. For each time scale, a sample $X(T_i) = \{x_0, \cdots, x_j\}$ is generated, where x_j is the corresponding data point of T_i.

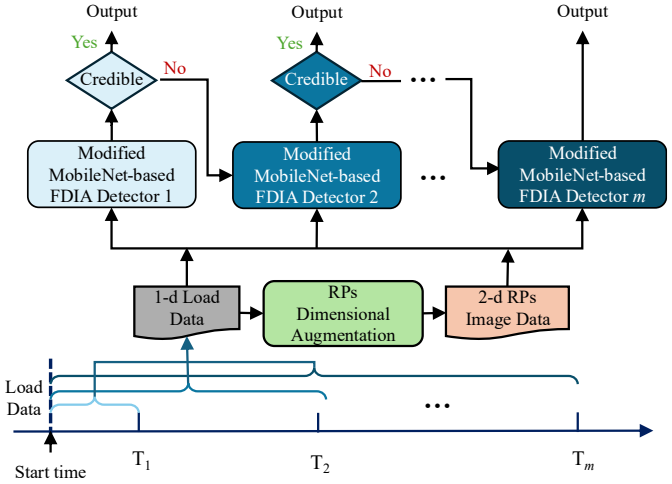


Fig. 4. Time-adaptive process for smart meter FDIA detection.

After sample generation, $X(T_i)$ is dimensional-augmented into 2-dimensional image data by RPs, shown in (9)-(10). The RPs of samples marked by $R\big(X(T_i)\big)$ and $X(T_i)$ are input into the modified MobileNet-based FDIA detector together. The objective function for the ith modified MobileNet FDIA detector is formulated in (11).

The FDIA detector F_i^{Detect} of time scale i is responsible for outputting classification probability, which is formulated as

$$F_i^{Detect}\Big(R\big(X(T_i)\big), X(T_i)\Big) = \big(P_i^{Gen}, P_i^{Gau}, \cdots, P_i^{Pul}\big) \quad (19)$$

where P_i^{Gen}, P_i^{Gau}, and P_i^{Pul} are the probabilities that $X(T_i)$ belongs to genuine, gaussian attack, and pulse attack classes. From (12), the detectors in the time-adaptive structure are trained and used to detect FDIA with different time scales. Thus, the proposed method can detect FDIA in a timely manner and is not confused by partially covered attack data defined in (10).

However, the detection result of F_i^{Detect} with smaller i is not sufficiently credible, as the smaller i implies the shorter length in $X(T_i)$ and less information provided to F_i^{Detect}. To address this issue, the time-adaptive structure should not always output the detection result of F_i^{Detect}. Therefore, a credibility threshold Th_i is set for each F_i^{Detect}, and only the outlier of F_i^{Detect}'s result is higher than Th_i, the detection result is output. The whole processing is summarized in Fig. 5.

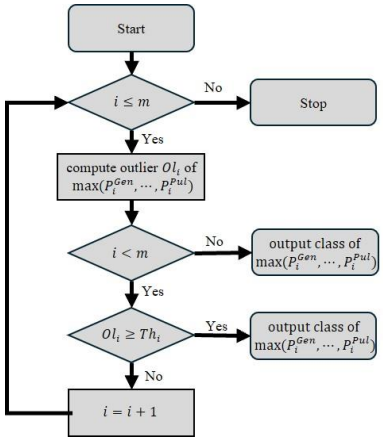


Fig. 5. Credibility judgement process of the time-adaptive structure

To obtain optimized threshold Th_i, NSGA-II is employed in this paper. The target of NSGA-II is optimizing a series of solutions which minimizing detection time (smaller time scale number) and maximizing detection accuracy, that is formulated as

$$\big(Th_1^h, \cdots Th_m^h\big)_{h=1}^{pn} = F^{NSGA}(F_i^{Detect}(D_i^R, D_i^X)_{i=1}^m) \quad (20)$$

where Th_1^m to Th_n^m are optimized credibility thresholds of each time scale in one Pareto front solution, pn represents the solution number of Pareto front, F^{NSGA} is the NSGA-II algorithm, D_i^R and D_i^X are the RPs and 1-dimensional sample datasets of time scale i. The detailed optimization process of NSGA-II in time-adaptive structure is introduced in Section III.C. It is worth noting that the above process is performed on current real-time data point, which is repeated when next real-time data is transmitted.

Consequently, the proposed time-adaptive structure enables timely detection of FDIA and prevents confusion with partially covered attack data. The detector with a short time span input will not output incredible detection results thanks to the credibility threshold mechanism. Furthermore, by using NSGA-II, the thresholds for detectors are optimally set.

D. Credibility Threshold Optimization

To evaluate the credibility of the detection result generated by each detector and make the proposed method adaptable to different scenarios, the credibility thresholds in Fig. 5 are modeled as a multi-objective optimization problem aimed at maximizing detection accuracy and minimizing detection time with NSGA-II is used to solve the optimization problem. The NSGA-II optimization operation is one-time and only exists in the training phase of the method, which will greatly reduce the computational burden. In the actual deployment phase, NSGA-II will only provide a few pre-optimized values, which will not affect the deployability of the proposed method.

The outlier of the class with the highest probability in the ith sample and jth detector in Fig. 5 is computed as

$$Ol_{i,j} = \frac{max(r_{i,j,1}, \cdots r_{i,j,m}) - \frac{1}{m}\sum_{s=1}^{m} r_{i,j,s}}{\sqrt{\frac{1}{m}\sum_{l=1}^{m}\Big(r_{i,j,l} - \frac{1}{m}\sum_{s=1}^{m} r_{i,j,s}\Big)^2}} \quad (21)$$

where $r_{i,j,l}$ represents the lth class's probability of ith sample under detection of jth detector. Since a higher outlier indicates greater

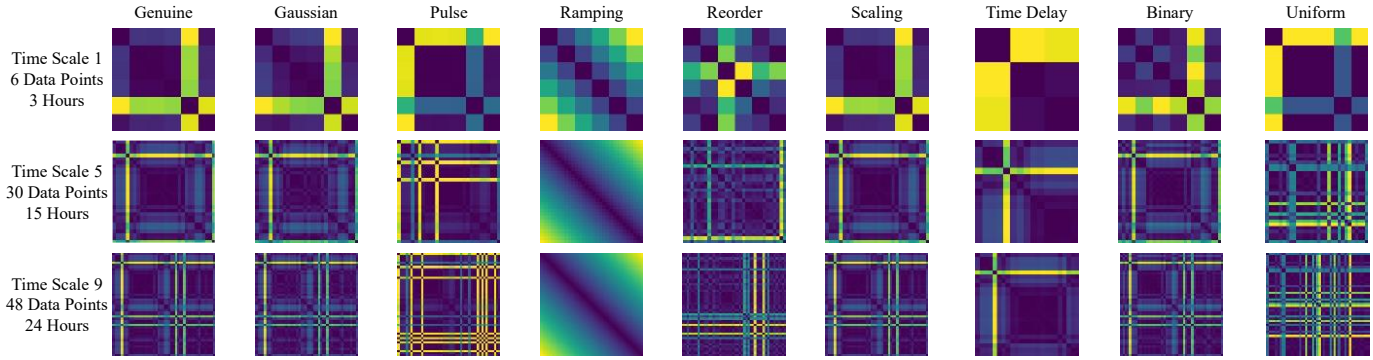


Fig. 6. Nine different classes of RPs image data of the same smart meter data in three time scales with different time scales.

confidence in the class result, the outlier of the class with the highest probability in the detector's result is optimized by NSGA-II.

The dataset $D^{opt} = \left(\left(r_{i,j,1}, r_{i,j,2}, \cdots, r_{i,j,nl}\right)_{j=1}^{m}\right)_{i=1}^{ns}$ has ns samples, wherein each sample saves the nl classes probability detection results of m detectors. Then, the dataset of outliers $D^{opt,outlier} = \left(Ol_{i,j}\right)_{i,j=1}^{n,k}$ is constructed, and the corresponding predict label and real label of $D^{opt,outlier}$ are marked by $D^{P} = \left(Lable_{i,j}^{P}\right)_{i,j=1}^{n,k}$ and $D^{R} = \left(Lable_{i,j}^{R}\right)_{i,j=1}^{n,k}$.

The constraint of credibility threshold value is defined in (22), and the objective functions of NSGA-II are defined in (23)-(26)

$$th_j \geq 0, \forall j \in [1, k-1] \tag{22}$$

$$f^{acc} = -\sum_i^{ns}\sum_j^{m-1} u\left(Score_{i,j}^{acc}\right)/ns \tag{23}$$

$$f^{spe} = \sum_i^{ns}\sum_j^{m-1} u\left(Score_{i,j}^{spe}\right) \tag{24}$$

$$Score_{i,j}^{acc} = \begin{cases} 1 & \text{if } j = 1, th_j > ol_{i,j}, Lable_{i,j}^{P} = Lable_{i,j}^{R} \\ -1 & \text{if } j = 1, th_j > ol_{i,j}, Lable_{i,j}^{P} \neq Lable_{i,j}^{R} \\ 1 \cdot 1_{\left\{Score_{i,j-1}^{acc} \neq 1,-1\right\}} & \text{if } j \neq 1, th_j > ol_{i,j}, Lable_{i,j}^{P} = Lable_{i,j}^{R} \\ -1 \cdot 1_{\left\{Score_{i,j-1}^{acc} \neq 1,-1\right\}} & \text{if } j \neq 1, th_j > ol_{i,j}, Lable_{i,j}^{P} \neq Lable_{i,j}^{R} \\ -2 & \text{if } th_j < ol_{i,j} \end{cases} \tag{25}$$

$$Score_{i,j}^{spe} = j \cdot 1_{\left\{Score_{i,j}^{acc} = 1,-1\right\}} \tag{26}$$

where, f^{acc} is the objective function of detection accuracy, f^{spe} is the objective function of detection speed.

As (23)-(26) shown, for each sample, we check the output of each detector in order, once an output is credible, the rest detection results are dropped. Since NSGA-II can only optimize the minimum of objective function, therefore subtraction applied to f^{acc} when the output is credible, and the prediction is correct. f^{spe} is updated when the output is credible, and the prediction is correct. Furthermore, the value added to f^{spe} is equal to the detector's index, the larger the index of detector that outputs a credible result, the greater the penalty for f^{spe}. For m detectors, when the output of the previous m-1 detectors is incredible, the last detector must output a detection result to maintain consistency in decision-making. Therefore, only m-1 credible thresholds are optimized in (23)-(24), as shown in Fig. 4.

As both objective functions described in (23)-(26) are nonlinear, and there is strong non-convexity of the neural networks [37]-[39], the detection result credibility optimization problem is considered a nonlinear and non-convex problem. Thus, NSGA-II is chosen to optimize the credibility thresholds in time-adaptive structure.

IV. Simulation Tests

A. Simulation Settings

In this paper, a public user-level load dataset including 20 residential buildings is utilized to validate the performance of the proposed method. The dataset contains smart meter data of 20 residential customers in Loughborough, UK [40]. We encode the dataset to get the total electricity load for each resident at 30-minute intervals. Since the length of each resident is different, 4000 consecutive data points in each encoded dataset are randomly selected.

Additionally, the genuine data and eight different FDIA types, including Gaussian-based additive noise [29], pulse, ramping attack, scaling attack [10], reorder, time delay, Uniform-based additive noise, and binary attack are configured. The above-mentioned eight types of attacks cover most of the possible FDIA in smart meters. The attack processes are formulated in the Appendix (1)-(8).

In practical scenarios, the attackers may only have limited knowledge of the internal structure and operational state of the power system or smart meters [4]-[5]. As a result, practical FDIA implementations tend to rely on simpler and effective attack strategies—such as injecting noise, modifying meter readings in specific patterns (e.g., pulse, scaling, and ramping), or introducing delays—rather than perfectly coordinated attacks that require full system knowledge. So, this paper focuses on those simpler and effective attack strategies.

Furthermore, due to FDIA-like natural noise (e.g., Gaussian) also has a negative impact on the subsequent data analysis of smart meters, so the proposed method will not make a special distinction between the two.

To evaluate the attack intensity of different types of FDIA, signal-to-noise rate (SNR) is used. The configured SNR and constants of each FDIA attack are shown in Table II.

For each resident in the dataset, average accuracy and F1-Score of each class are used to evaluate the performance. To verify the performance of the model's accuracy and detection speed in FDIA detection, The AWV [13], FFT-SVD [12], and the VGGNet [29] are used as benchmarks. To further verify the superior FDIA

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2025.3575249

detection performance of the modified MobileNet FDIA detector in the proposed method, ResNet [41] and time adaptive ResNet (Using ResNet replace the FDIA detector in the proposed method) are used in ablation experiment and credibility thresholds optimization.

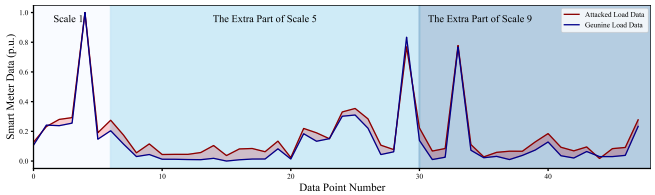
TABLE II
SNR AND CONSTANTS SETTING OF EACH FDIA TO THE SMART METER DATA

FDIA Type	Constant Setting	SNR (dB)
Gaussian	$\mu = 0, \sigma = 100$	21.77 (±5.22)
Pulse	-	-12.98 (±8.22)
Ramping	$i_s = 0, i_e = \text{len}(D)$	-0.42 (±6.15)
Reorder	-	-1.61 (±1.27)
Scaling	$a = 0.3$	3.09 (±8.88)
Time Delay	$c = 2$	-1.66 (±1.16)
Binary	-	10.61 (±2.64)
Uniform	-	-10.28 (±7.89)

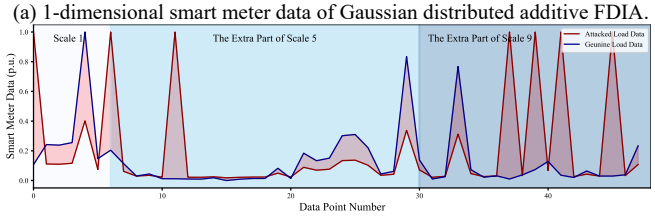
B. Test Results

1) Data Processing and Dimensional Augmentation

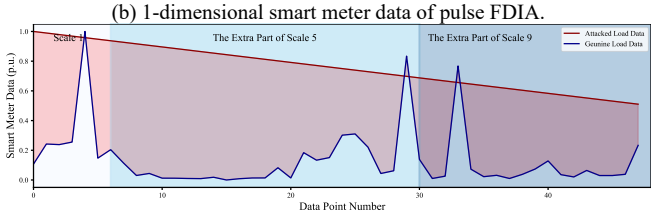
The number of data points at each time scale is set as 6, 12, 18, 24, 30, 32, 36, 42, and 48, total in 9 time scales, so we also set 9 detectors. Fig. 6 shows the RPs image data of nine classes on time scales 1, 5, and 9. Fig. 7 shows the corresponding 1-dimensional smart meter data. As Fig. 6 and Fig. 7 depict, we find that the time scale with longer time scales contains more complex information about data but also require more detection time. Furthermore, some different FDIA types in Fig. 7 are extremely similar, which brings great difficulty to the detector. However, the PRs can extract more information than 1-dimensional smart meter data, which benefits the FDIA detection. As a result, data that is difficult to distinguish in 1-dimensional smart meter data becomes visual-distinguishable in RPs. Note that the RPs between genuine data and Scaling FDIA are totally same, which is consistent with (5). So, the detection method that only considers RPs will not be able to effectively detect FDIA that satisfies (5), which is also proved by following simulation.



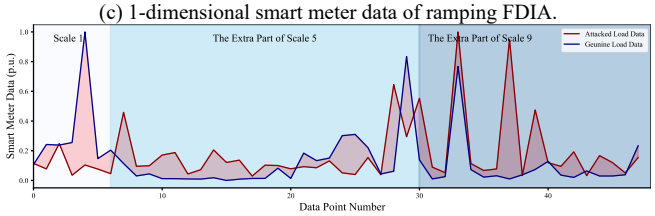
(a) 1-dimensional smart meter data of Gaussian distributed additive FDIA.



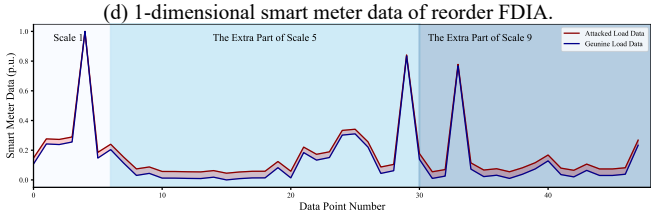
(b) 1-dimensional smart meter data of pulse FDIA.



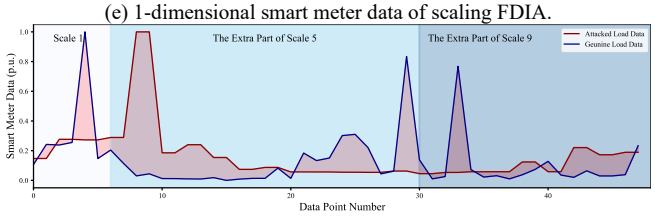
(c) 1-dimensional smart meter data of ramping FDIA.



(d) 1-dimensional smart meter data of reorder FDIA.



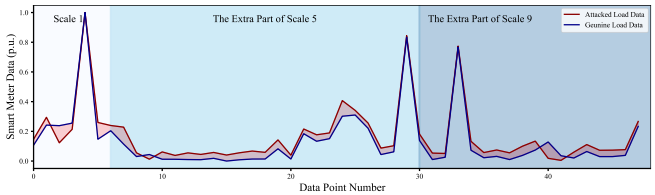
(e) 1-dimensional smart meter data of scaling FDIA.



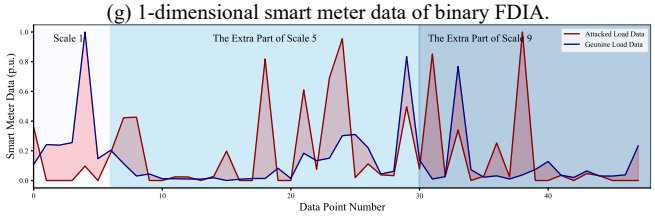
(f) 1-dimensional smart meter data of time-delay FDIA.

TABLE III
COMPARISON OF DETECTION ACCURACY AND DETECTION SPEED BETWEEN THE PROPOSED METHOD AND THREE BENCHMARKS

Opt. Sol.	Stat. Ind.	Accuracy				F1-Score				Credibility Classification Time (According to The Numbering of Detector)			
		The Prop.	FFT-SVD	AWV	VGG-based	The Prop.	FFT-SVD	AWV	VGG-based	The Prop.	FFT-SVD	AWV	VGG-based
Highest Det. Acc.	Ave.	92.00%	82.32%	76.23%	38.08%	0.9215	0.7411	0.7609	0.3792	2.3797	4.5577	4.1462	5.8489
	Med.	91.95%	87.20%	77.21%	38.16%	0.9212	0.7789	0.7723	0.3790	2.4010	4.3841	4.1481	5.8341
	Max	95.01%	99.68%	88.08%	44.95%	0.9506	0.9917	0.8841	0.4710	2.7520	6.2351	4.8792	6.2125
	Min	87.44%	61.35%	60.86%	33.98%	0.8755	0.5437	0.6085	0.3398	1.9388	3.3027	3.3140	5.2061
Comp.	Ave.	81.98%	-	-	-	0.8223	-	-	-	1.5735	-	-	-
	Med.	81.64%	-	-	-	0.8182	-	-	-	1.5765	-	-	-
	Max	87.44%	-	-	-	0.8757	-	-	-	1.8084	-	-	-
	Min	74.56%	-	-	-	0.7552	-	-	-	1.3478	-	-	-
Fastest Det. Time	Ave.	70.30%	-	-	-	0.7107	-	-	-	1.0065	-	-	-
	Med.	69.73%	-	-	-	0.7050	-	-	-	1.0032	-	-	-
	Max	80.19%	-	-	-	0.8056	-	-	-	1.0386	-	-	-
	Min	65.38%	-	-	-	0.6638	-	-	-	1.0016	-	-	-



(g) 1-dimensional smart meter data of binary FDIA.



(h) 1-dimensional smart meter data of Uniform distributed additive FDIA.

Fig. 7. 1-dimensional smart meter data of different FDIA types in different time scales with different time scales.

2) *Credibility Threshold Optimization*

After RPs generation for each detector and each FDIA type, the time-adaptive structure with modified MobileNet-based FDIA detector is trained. 230 samples and their corresponding RPs data of each FDIA and genuine class are used to train and test for each resident by leveraging rolling window, thus a total of 2070 data samples are used, the detailed processing of sample generation is shown in Fig. 8.

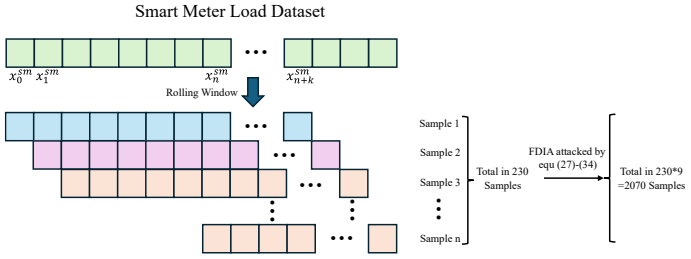


Fig.8 Sample generation and FDIA processes of smart meter data in the proposed method.

The ratio of the training set and the testing set is 70% (1449):30% (621), the categorical cross-entropy loss function and root mean square propagation (RMSprop) optimizer is used in the modified MobileNet-based detector. The batch size, epochs, and learning rate are set as 5, 10, and 0.0002, respectively.

The Pareto fronts optimized by the proposed method and time-adaptive ResNet are shown in Fig. 9. In Fig. 9, the Pareto front of the proposed method is superior to that of the time-adaptive ResNet, which is due to the difference in the quality between the output results of different detectors. Moreover, consistent with the analysis in Section III.C, the optimization problem is non-convex.

3) *FDIA Detection Performance*

The classification results and detection speed of the proposed method and three benchmarks are shown in Table III. Since many different credible threshold solutions are obtained from the Pareto front optimized by NSGA-II, only the solutions with the best detection accuracy, fastest detection speed, and one compromise solution between accuracy and speed are adopted. The average, median, max, and min values of "Accuracy", " F1-score", and "Credibility Classification Time" over 20 residents are listed in Table III. It should be noticed that ResNet and VGG don't have the credible threshold mechanism, so when testing the credibility classification time, the data in different time scale is input by order, and the time is recorded when the method first makes correct classification decision, which is more tolerant.

It is observed that the proposed method is superior in terms of detection accuracy and F1-score compared to the benchmarks for the three credibility thresholds solutions. On the one hand, the proposed method has a 25.11% increase in detection accuracy and a 0.2471 increase in F1-score compared with time-adaptive ResNet. This indicates the superiority of the proposed modified MobileNet-based FDIA detector. On the other hand, the time-adaptive ResNet shows a 3.69 increase in detection speed compared with ResNet, verifying the effectiveness of the proposed time-adaptive structure. To summarize, the proposed method has the fastest detection speed and detection accuracy compared with all benchmarks.

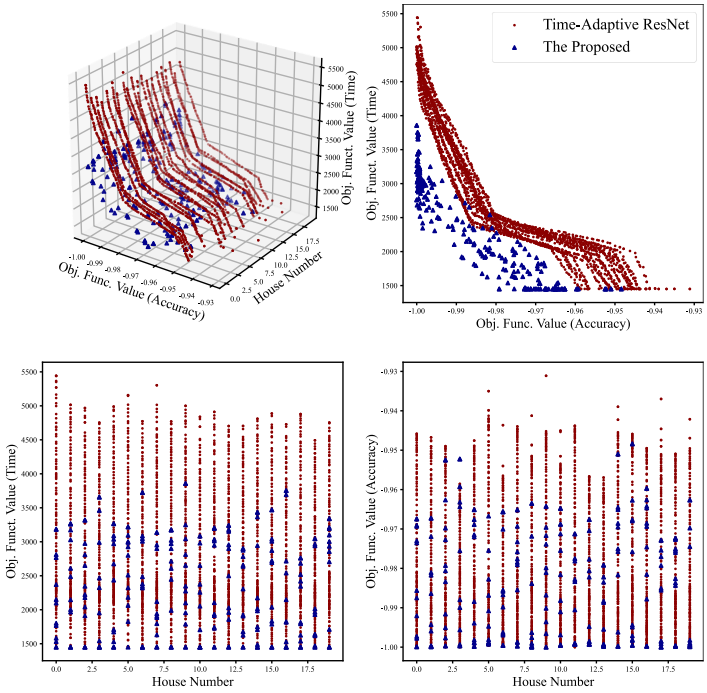


Fig. 9. Comparison of optimized Pareto front between the proposed method and benchmark of time-adaptive ResNet method in four perspectives.

The confusion matrices of different methods with the same compromise solution are shown in Fig. 10. In Fig. 10, compared with benchmarks, the proposed model has better detection performance in most of eight FDIA types and genuine data compared with benchmarks. While VGGNet shows inefficient results cause the outdated model structure and does not target optimizations for FDIA types that satisfy (5) and (10).

Furthermore, the proposed method is superior in detecting some special FDIA types (e.g. scaling and Uniform) and some extremely similar FDIA types (e.g. genuine, Gaussian, scaling, binary, and Uniform). This superior ability to distinguish between different FDIA types is not observed in the benchmarks. Note that due to the benchmark FFT-SVD only suitable for binary classification, thus FFT-SVD is not included in Fig. 10.

To compare the setting strategies for different objectives in the credibility threshold optimization, the average value of credibility thresholds of the proposed method over 20 residents are shown in Fig. 11. In Fig. 11, *Di* represents the index of detectors, as we set 9 time scales and 8 time scales' credibility thresholds is optimized, so the index of *Di* is from 1 to 8. From Fig. 11, to obtain the

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2025.3575249

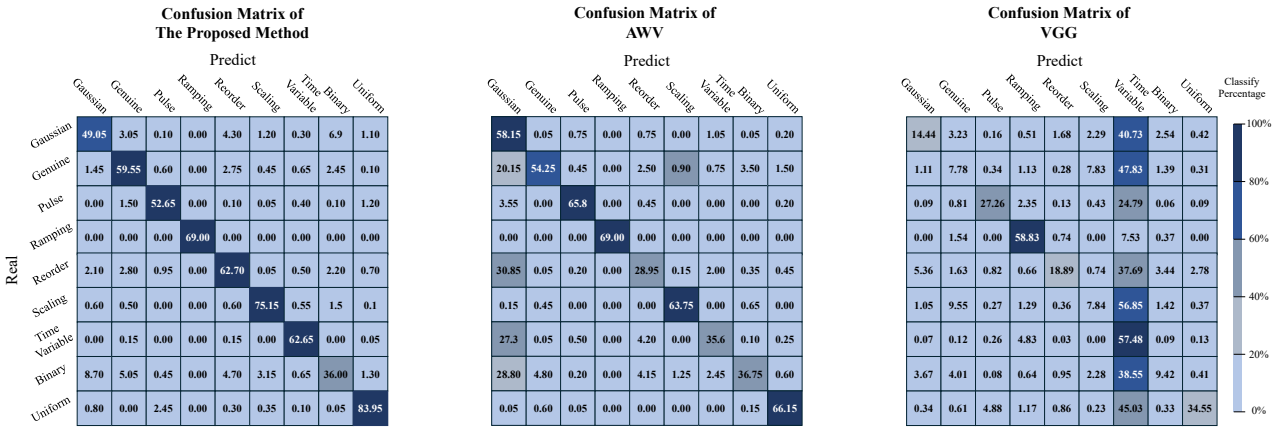


Fig. 10. Confusion matrix comparison between the proposed method and three benchmarks in eight types of FDIA data and genuine data.

tradeoff solution between the best detection accuracy and the fastest detection speed, different strategies are used by NSGA-II. For the fastest detection speed strategy, NSGA-II chooses to relax the credibility requirements for the earlier time scale detector, so that the detection results are prone to be judged as credible. Since the earlier detectors obtain very little information, while the later detectors gather more. Therefore, with the credibility thresholds under the best detection accuracy strategy, NSGA-II shows sufficient distrust in the results of the earlier time scales and chooses to relax the threshold requirement after detector 4. With the credibility thresholds under the compromise solution, NSGA-II combines the characteristics of two extreme solutions, including relaxing the threshold requirements for early detectors in pursuit for faster detection speed and not fully trusting early time scales.

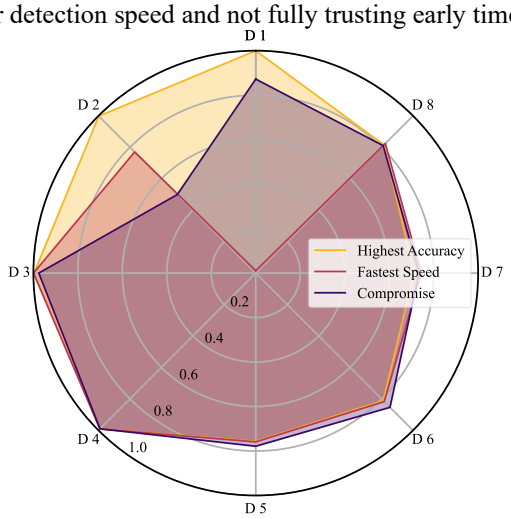


Fig. 11. Credibility thresholds of the proposed method under three solutions of Pareto front.

During the training phase, the proposed method recognizes inherent noise (such as Gaussian noise) in smart meter data as part of the normal data features. When additional noise-based FDIA is introduced, it results in a secondary distortion of the original data. Therefore, the proposed method is capable of processing smart meter data that contains inherent noise as well as detecting FDIA-induced secondary noise.

4) Practical Deployability

Furthermore, to evaluate the deployability of the proposed method, the RAM sizes and counts of additive+multiplication of the different methods are listed in Table IV. The proposed time-adaptive structure is computed serially, so its RAM size is computed by considering one detector at a time. In Table IV, the "Count of Additive+Multiplication" with one detector/all detectors are also provided.

TABLE IV
COMPARISON OF DEPLOYABILITY IN THE PROPOSED METHOD AND BENCHMARKS

Method	RAM Size	Count of Additive+Multiplication	Running Time (s/epoch)
The Proposed ResNet/Time-Adaptive	26.21 Mb	$0.69*10^8/6.21*10^8$	4.0431
	49.58 Mb	$6.87*10^8/61.83*10^8$	6.4398
VGGNet	18.07 Mb	$19.5*10^8$	5.5343

In Table IV, the RAM size of the proposed method is the second lowest, but the computational complexity of the proposed method is 28 times lower than VGGNet for a single detector. The proposed method also has the fastest running time in practical experiments. Furthermore, the proposed method has higher accuracy compared with ResNet and VGGNet. Therefore, the proposed method is more advantageous for practical deployment.

To summarize, the simulation results show that the proposed method can adapt to different detection scenarios, accelerate detection speed for various FDIA types with outstanding quality, and has greater potential for deployment.

5) Ablation Experiments

To further analyze the impact of each subnetwork on the overall performance, a comprehensive ablation experiment is conducted, where 4 different combination scenarios are considered:

1. Time Adaptive Structure + ResNet + ANN: measuring the performance contribution of MobileNet to the proposed method.
2. Time Adaptive Structure + ResNet: measure the performance contribution of the modified MobileNet FDIA detector (MobileNet+ANN) to the proposed method.
3. Time Adaptive Structure + MobileNet: measuring the contribution of ANN (statistical characteristics of 1-d load data) to the performance of the proposed method.
4. MobileNet + ANN + Thresholds: measuring the contribution of time adaptive structure to the performance of the proposed method.

The test results of ablation experiments are shown in Table V and Fig. 11.

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2025.3575249

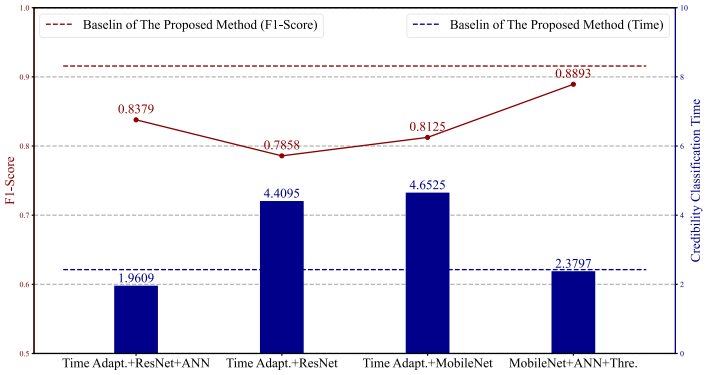


Fig. 11. Performance of different ablation scenarios and the baseline of the proposed method in ablation experiments.

From Table V and Fig. 11, MobileNet + ANN + thresholds has the best performance in FDIA detection, and the time adaptive structure ResNet + ANN has the second highest accuracy, which indicates that the fusion of 1-d load data's statistical indicators efficiently increases the performance of detector. In addition, when ANN is not included, the performance of MobileNet is slightly higher than that of ResNet, which shows that many advanced CV techniques used in MobileNet do help improve detection performance. The performance of both time adaptive structure + ResNet and time adaptive structure + MobileNet is higher than the baseline of the proposed method, which further illustrates that the fusion of statistical indicators helps to reduce the credibility detection time of the model.

Finally, MobileNet + ANN + Thresholds reduces the detection performance while using almost the same credibility classification time as the baseline, which shows that the proposed time adaptive structure can reasonably set the credibility thresholds of detectors in different moments.

V. Conclusions

This paper proposes a lightweight time-adaptive data-driven method for smart meter multi-FDIA detection based on the proposed modified MobileNet-based FDIA detector, the time-adaptive structure, and multi-objective optimization strategy-based credibility threshold mechanism. The proposed method is theoretically adaptable to other time series data anomaly detection tasks, but the randomness and diversity of user behaviors are highly considered in the design of method.

To tackle the inadequacy of existing methods including detection capability and deployability, the modified MobileNet-based FDIA detector consisting of MobileNet, statistical indicator computing block, and ANN is proposed first. The proposed modified MobileNet-based FDIA detector is a lightweight detector, which saves computing resources and is easier to deploy in edge devices in practice. By providing a time-adaptive structure, the proposed method bridges the gap in smart meters FDIA detection when the randomness of FDIA start time is considered. The time-adaptive structure consists of multiple modified MobileNet-based FDIA detectors and NSGA-II based credibility threshold optimization mechanism. The NSGA-II based credibility threshold optimization mechanism is used to optimize the credibility thresholds of different detectors, which also can provide comprehensive solutions by making the tradeoff between detection accuracy and detection speed. The different credibility threshold solutions in the Pareto front provided by NSGA-II give the proposed method the ability to adapt to different scenarios with varying detection requirements in smart meters. The simulation results demonstrate the outstanding detection accuracy and speed of the proposed lightweight time-adaptive method, and the method also can detect various FDIA.

In the deployment stage, the proposed method with low-hardware requirements is suitable for running on embedded processors such as AMI [42]-[43]. IEEE 2030.5 also shows a potential communication protocol in deployment stage [44]. Furthermore, it is valuable to explore how the FDIA detector can effectively detect and classify both known and unknown FDIA types, rather than solely focusing on expanding the number of known attack types. Open-set classification and out-of-distribution detection methods in artificial intelligence have strong potential to address this challenge in future research.

TABLE V
Performance Comparison of Four Different Combination Scenarios in Ablation Experiments

Opt. Sol.	Stat. Ind.	Accuracy				F1-Score				Credibility Classification Time (According to The Numbering of Detector)			
		TA+Res +ANN	TA+Res	TA+Mob ile	Mobile+ ANN+Th re	TA+R es+AN N	TA+R es+AN N	TA+R es	TA+M obile	TA+R es+AN N	TA+R es	TA+M obile	Mobile +ANN+ Thre
Highest Det. Acc.	Ave.	83.49%	77.30%	80.20%	88.68%	0.8379	0.7858	0.8125	0.8893	1.9609	4.4095	4.6525	2.0073
	Med.	84.06%	77.70%	80.19%	88.73%	0.8414	0.7862	0.8065	0.8890	1.9605	4.4082	4.7230	2.0145
	Max	87.92%	80.52%	82.77%	92.91%	0.8810	0.8266	0.8409	0.9297	2.3897	4.9549	5.0386	2.3510
	Min	79.71%	70.69%	76.01%	83.74%	0.8001	0.7114	0.7711	0.8400	1.5330	4.0612	4.0483	1.6264
Comp.	Ave.	75.23%	56.19%	64.85%	-	0.7560	0.5696	0.6615	-	1.3753	1.8729	2.4846	-
	Med.	75.52%	55.56%	65.38%	-	0.7569	0.5645	0.6682	-	1.3744	1.8671	2.4147	-
	Max	80.35%	61.84%	74.24%	-	0.8127	0.6399	0.7626	-	1.5990	2.1852	2.9919	-
	Min	68.76%	52.50%	57.97%	-	0.6918	0.5279	0.5852	-	1.1820	1.7118	2.2770	-
Fastest Det. Time	Ave.	67.67%	41.08%	40.74%	-	0.6757	0.4251	0.4366	-	1.0038	1.019	1.0059	-
	Med.	67.23%	40.10%	39.77%	-	0.6760	0.4216	0.4259	-	1.0024	1.0056	1.0032	-
	Max	72.95%	47.02%	45.25%	-	0.7326	0.482	0.4944	-	1.0113	1.1063	1.0274	-
	Min	59.42%	36.88%	38.16%	-	0.5790	0.3864	0.4074	-	1.0016	1.0016	1.0016	-

REFERENCES

[1] C. C. Sun, D. J. S. Cardenas, A. Hahn, et al., "Intrusion detection for cybersecurity of smart meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612-622, 2020.

[2] A. Alrasheedi, O. E. Egbomwan, S. Liu, et al., "Vulnerability assessment of machine learning based short-term residential load forecast against cyber attacks on smart meters," *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, 2022, pp. 309-314.

[3] M. Cui, J. Wang, M. Yue, "Machine learning-based anomaly detection for load forecasting under cyberattacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5724-5734, 2019.

[4] Rahman, Md Ashfaqur, and Hamed Mohsenian-Rad. "False data injection attacks with incomplete information against smart power grids." 2012 IEEE Global Communications Conference (GLOBECOM). IEEE, 2012.

[5] Lakshminarayana, Subhash, et al. "Data-driven false data injection attacks against power grids: A random matrix approach." IEEE Transactions on Smart Grid 12.1 (2020): 635-646.

[6] S. Wei, J. Xu, Z. Wu, Q. Hu, and X. Yu, "A False Data Injection Attack Detection Strategy for Unbalanced Distribution Networks State Estimation," IEEE Trans. Smart Grid, vol. 14, no. 5, pp. 3992-4006, 2023.

[7] T. S. Sreeram and S. Krishna, "Protection Against False Data Injection Attacks Considering Degrees of Freedom in Attack Vectors," IEEE TSG, vol. 12, no. 6, pp. 5258-5267, 2021.

[8] Y. Zhang, L. Wang, W. Sun, et al., "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796-808, 2011.

[9] F. Ünal, A. Almalaq, S. Ekici, et al., "Big data-driven detection of false data injection attacks in smart meters," *IEEE Access,* vol. 9, pp. 144313-144326, 2021.

[10] K. Zheng, Q. Chen, Y. Wang, et al., "A novel combined data-driven approach for electricity theft detection," *IEEE Trans. Ind. Inform*., vol. 15, no. 3, pp. 1809-1819, 2018.

[11] Haghshenas, Seyed Hamed, Md Abul Hasnat, and Mia Naeini. "A temporal graph neural network for cyber attack detection and localization in smart grids." 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2023.

[12] Dehghani, Moslem, et al. "Fourier singular values-based false data injection attack detection in AC smart-grids." Applied Sciences 11.12 (2021): 5706.

[13] Wang, Defu, et al. "Detection of power grid disturbances and cyber-attacks based on machine learning." Journal of information security and applications 46 (2019): 42-52.

[14] Ünal, Fatih, et al. "Big data-driven detection of false data injection attacks in smart meters." IEEE Access 9 (2021): 144313-144326.

[15] Raihan Uddin, Md, Ratun Rahman, and Dinh C. Nguyen. "False Data Injection Attack Detection in Edge-based Smart Metering Networks with Federated Learning." arXiv e-prints (2024): arXiv-2411.

[16] Zhang, Ying, Jianhui Wang, and Bo Chen. "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach." IEEE Transactions on Smart Grid 12.1 (2020): 623-634.

[17] R. Jiao, G. Xun, X. Liu, and G. Yan, "A New AC False Data Injection Attack Method Without Network Information," IEEE TSG, vol. 12, no. 6, pp. 5280-5289, 2021.

[18] N. Peng, R. Liang, G. Wang, et al., "Edge computing-based fault location in distribution networks by using asynchronous transient amplitudes at limited nodes," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 574-588, 2020.

[19] K. Saxena, A. R. Abhyankar, "Agent-based distributed computing for power system state estimation," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5193-5202, 2020.

[20] V. Chamola, A. Sancheti, S. Chakravarty, et al., "An IoT and edge computing based framework for charge scheduling and EV selection in V2G systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 10569-10580, 2020.

[21] W. Lin, D. Wu, M. Jenkin, "Electric load forecasting for individual households via spatial-temporal knowledge distillation," *IEEE Trans. Power Syst.*, 2024.

[22] Y. He, F. Luo, G. Ranzi, "Transferrable model-agnostic meta-learning for short-term household load forecasting with limited training data," *IEEE Trans. Power Syst.*, vol. 37, no. 4, pp. 3177-3180, 2022.

[23] K. J. Park, S. Y. Son, "Residential load forecasting using modified federated learning algorithm," *IEEE Access*, 2023.

[24] E. Lee, W. Rhee, "Individualized short-term electric load forecasting with deep neural network based transfer learning and meta learning," *IEEE Access*, vol. 9, pp. 15413-15425, 2021.

[25] A. Musleh, G. Chen, Z. Y. Dong, C. Wang, and S. Chen, "Online Characterization and Detection of False Data Injection Attacks in Wide-Area Monitoring Systems," IEEE TPWRS, vol. 37, no. 4, pp. 2549-2562, 2022, doi: 10.1109/tpwrs.2021.

[26] Z. Du, Z. Yan, Y. Xu, "A dimensional augmentation-based data-driven method for detecting false data injection in smart meters," *IEEE Trans. Smart Grid*, 2023.

[27] Li, Xueping, Yaokun Wang, and Zhigang Lu. "Graph-based detection for false data injection attacks in power grid." Energy 263 (2023): 125865.

[28] Sethi, Basant K., et al. "Smart home energy management system under false data injection attack." International Transactions on Electrical Energy Systems 30.7 (2020): e12411.

[29] B. Gou, Y. Xu, Y. Xia, et al., "An intelligent time-adaptive data-driven method for sensor fault diagnosis in induction motor drive system," *IEEE Trans. Ind. Electron.*, vol. 66, no. 12, pp. 9817-9827, 2018.

[30] N. Marwan, M. C. Romano, M. Thiel, et al., "Recurrence plots for the analysis of complex systems," *Physics Reports*, vol. 438, no. 5-6, pp. 237-329, 2007.

[31] M. Sandler, A. Howard, M. Zhu, et al., "MobilenetV2: Inverted residuals and linear bottlenecks," *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 4510-4520.

[32] T. T. Teo, T. Logenthiran, W. L. Woo, et al., "Optimization of fuzzy energy-management system for grid-connected microgrid using NSGA-II," *IEEE Trans. Cybern*., vol. 51, no. 11, pp. 5375-5386, 2020.

[33] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2017, pp. 1251-1258.

[34] A. G. Howard, M. Zhu, B. Chen, et al., "MobileNets: Efficient convolutional neural networks for mobile vision applications," *arXiv* preprint arXiv:1704.04861, 2017.

[35] R. Zhang, Y. Xu, Z.Y. Dong, and K.P. Wong, "Post-disturbance transient stability assessment of power systems by a self-adaptive intelligent system," *IET Gen. Trans. & Dist.*, vol.9, no.3, pp. 296-305, Feb. 2015.

[36] Y. Zhang, Y. Xu*, Z.Y. Dong, R. Zhang, and K.P. Wong, "A Hierarchical Self-Adaptive Data-Analytics Method for Power System Short-term Voltage Stability Assessment," *IEEE Trans. Ind. Info.*, vol. 15, no.1, pp. 74-84, 2019.

[37] X. Glorot, A. Bordes, Y. Bengio, "Deep sparse rectifier neural networks," Proc. *14th Int. Conf. Artif. Intell. Stat., JMLR Workshop and Conf. Proc.,* pp. 315-323, 2011.

[38] R. Pascanu, Y. N. Dauphin, S. Ganguli, et al., "On the saddle point problem for non-convex optimization," *arXiv* preprint arXiv:1405.4604, 2014.

[39] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," *Proc. 13th Int. Conf. Artif. Intell. Stat., JMLR Workshop and Conf. Proc.*, pp. 249-256, 2010.

[40] M. David, S. Lina and S. Vladimir, "REFIT: Electrical Load Measurements(Cleaned)",https://pureportal.strath.ac.uk/en/datasets/refit-electrical-load-measurem ents-cleaned.

[41] He, Kaiming, et al. "Identity mappings in deep residual networks." *Computer Vision–ECCV 2016: 14th European Conference, 2016.*

[42] Molokomme, Daisy Nkele, Adeiza James Onumanyi, and Adnan M. Abu-Mahfouz. "Edge intelligence in Smart Grids: A survey on architectures, offloading models, cyber security measures, and challenges." *Jour. of Sens. and Act. Net. 11.3, 2022.*

[43] Huang, Can, et al. "Smart meter pinging and reading through AMI two-way communication networks to monitor grid edge devices and DERs." *IEEE Trans. on Smart Grid 13.5, 4144-4153, 2021.*

[44] Ghalib, Marwan, et al. "Implementation of a smart grid communication system compliant with IEEE 2030.5." *2018 IEEE Intern. Conf. on Commu. Wor. (ICC Workshops),* 2018.

APPENDIX

$$f^{Gau}(x_i) = x_i + \varepsilon, \varepsilon \sim N(\mu, \sigma^2) \quad (1)$$

$$f^{Pul}(x_i) = \begin{cases} max(D) & \text{if } r \geq 0.65 \\ x_i & else \end{cases}, r \sim U(0,1) \quad (2)$$

$$f^{Ram}(x_i) = max(D) - \frac{i - i_s}{i_e - i_s}\frac{max(D)}{2}, i_s \leq i \leq i_e \quad (3)$$

$$f^{Sca}(x_i) = a \times x_i, a \in \mathbb{Q} \quad (4)$$

$$f^{Reo}(D) = \left(\gamma(x_i)_{i=1}^{len(D)}\right), \gamma \sim U(S_n) \quad (5)$$

$$f^{Tim}(x_i) = x_{int(i/c)}, c \geq 1 \quad (6)$$

$$f^{Uni}(x_i) = x_i + \varepsilon, \varepsilon \sim U(min(x_i), max(x_i)) \quad (7)$$

$$f^{Bin}(x_i) = \begin{cases} RS(x_i) = 1 & \text{if } RS(x_i) = 0 \\ RS(x_i) = 0 & \text{if } RS(x_i) = 1 \end{cases} \quad (8)$$

where D is the input sample of smart meter data, x_i is the data point in D, i_s and i_e are the start and end data point of ramping attack, ε, a, and γ are constants, $RS(x_i)$ is an operation that selects a random digit in the binary x_i.