Multisource Heterogeneous Specific Emitter Identification Using Attention Mechanism-Based RFF Fusion Method

Yibin Zhang, *Graduate Student Member, IEEE*, Qianyun Zhang, *Member, IEEE*, Haitao Zhao, *Senior Member, IEEE*, Yun Lin, *Senior Member, IEEE*, Guan Gui, *Fellow, IEEE*, and Hikmet Sari, *Life Fellow, IEEE*

***Abstract*— Cyber security has always been an important issue in the Internet of Everything topic. In the physical layer of the Internet, specific emitter identification (SEI) technology is widely researched as a simple and effective intrusion prevention technology. Existing SEI research only focused on radio frequency (RF) signals from a single receiver. However, in real scenes such as the Industrial Internet of Things (IIoT), vehicle-to-everything applications, and intelligent sensing systems, etc., RF signals are received from different types of sensors deployed at different locations. Therefore, this paper proposes a multisource heterogeneous SEI (MH-SEI) method and proposes a multi-source heterogeneous attention-based feature fusion network (MHAFFN) to achieve excellent identification performance. The proposed MHAFFN utilizes a multi-channel convolutional network as the RF fingerprinting (RFF) extraction module for multisource heterogeneous RF signals and equips an attention-based RFF fusion module to obtain mixed RFF for the automatic classifier. The experimental results show that the identification accuracy of MHAFFN is 99.196% in a perfect environment. Furthermore, robustness verification has proved that MHAFFN keeps advantages in noisy environments. Through fault tolerance mechanism verification experiment, it is proved that MHAFFN is able to work stably in real-world complex scenarios.**

***Index Terms*— Multisource heterogeneous specific emitter identification (MH-SEI), radio frequency fingerprinting (RFF), multi-channel convolutional network, attention based RFF fusion.**

I. Introduction

THE new industrial revolution leads to new technologies springing up, such as Industrial Internet of Things (IIoT), digital twins, vehicle-to-everything (V2X), etc. At the same time, it has also raised some urgent security issues that need to be addressed, such as illegal device intrusion, data leakage, hacker attacks and so on [1], [2], [3], [4]. In order to ensure the cyber security, there are several technical methods. The specific emitter identification (SEI) technology [5] has become a popular research topic among numerous solutions. The core idea of SEI is to achieve precise authentication of access devices based on the specific hardware defects of different wireless devices. In other words, no leaves are exactly the same in the world, so are wireless devices. Even devices produced in the same model and batch may have slight differences and hardware defects [6], [7], which are defined as radio frequency fingerprinting (RFF).

A typical SEI approach operates in two stages, the first stage extracts proper characteristics from captured signals and the second stage builds an automatic classifier for identifying wireless devices [8]. With the help of artificial intelligence, especially deep learning (DL) technology, the computer can quickly and accurately extract RFF from massive in-phase/quadrature (I/Q) signals. It is not difficult to find that research on signal processing utilizing DL technology has mushroomed recently, e.g., for automatic modulation recognition [9], [10], [11], channel state information prediction and feedback [12], [13], fast beamforming design [14], intrusion detection [15], industrial boundary tracking [16], [17], malware traffic classification [18], flight delay prediction [19], indoor localization [20] and other topics. At the same time, DL methods has also been widely utilized in SEI technology. The key idea of DL application is to convert I/Q signals into images for RFF extraction. Lin et al. first proposed to preprocess IQ signals to contour stella image, and then utilized neural network to extract RFF and achieve wireless device identification [21]. Similarly, Yin et al. [22] proposed differential constellation trace figure, combined with multi-channel convolutional neural network (CNN) to complete the identification of devices. Meanwhile, Li et al. [23] improved the accuracy of SEI by converting the I/Q signals into time-frequency graph. Peng et al. [24] proposed a novel supervised contrastive learning based RFF identification method, which can achieve great performance with limited samples. Yao et al. [25] proposed a few-shot specific emitter identification method using asymmetric masked auto-encoder.

However, the researches mentioned above were aimed at identifying equipment by captured signals from only one single source. Actually, the signals captured in real world,

Manuscript received 24 August 2023; revised 15 December 2023; accepted 8 January 2024. Date of publication 12 January 2024; date of current version 24 January 2024. This work was supported in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX22-0948 and in part by the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province under Grant 22KJA510002. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Valeria Loscri. *(Corresponding authors: Qianyun Zhang; Guan Gui.)*

Yibin Zhang, Haitao Zhao, Guan Gui, and Hikmet Sari are with the College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: 2021010208@njupt.edu.cn; zhaoht@njupt.edu.cn; guiguan@njupt.edu.cn; hsari@ieee.org).

Qianyun Zhang is with the School of Cyber Science and Technology, Beihang University, Beijing 100191, China (e-mail: zhangqianyun@buaa.edu.cn).

Yun Lin is with the College of Information and Communication Engineering, Harbin Engineering University, Harbin 150009, China (e-mail: linyun@hrbeu.edu.cn).

Digital Object Identifier 10.1109/TIFS.2024.3353594

especially in IIoT scenario, are usually from multi-source sensors and under different types [26], [27], [28], [29]. Although the wireless device authenticated can be completed using partial signals from single source, the multi-source heterogeneous signals still plays an important role in the SEI technology. Therefore, this paper explores a multisource heterogeneous SEI method (MH-SEI), which is based on real-world multisource heterogeneous radio frequency signals. To our best knowledge, this is the first attempt to use the MH-SEI method. The main contributions of this paper are highlighted as below.

- In order to fully utilize sensors of different locations and types deployed in real-world scenarios, we first propose the MH-SEI method.
- To deal with wireless signals from different receivers and formats, we propose a RFF fusion algorithm based on attention mechanism to mix multiple RFFs. The fused RFF will be input into an automatic classifier to implement MH-SEI technology.
- To validate the proposed MH-SEI method, we construct a multisource heterogeneous experimental environment consisting of one transmitter and three different receivers. We prove the effectiveness of our algorithm through real-world signals data.

The remainder of this paper is organized as follows. In section II, we give a survey about several SEI research directions in recent years, including lightweight SEI, semi-supervised SEI and open-set SEI methods. Section III shows the system model and the corresponding mathematical problem model. In section IV, we discuss our proposed MH-SEI method in detail, including four composed modules and the algorithm flow chart. The experimental results and some comparative analysis are given in section V. Furthermore, the complexity analysis of the proposed method is shown in this part. Finally, section VI concludes this paper.

II. Related Works

A. Various SEI Technology

With the development of Internet of Things (IoT) technology, information security has always been an unavoidable issue. As mentioned in the previous section, SEI technology plays a crucial role in ensuring information security. While continuously improving the accuracy of SEI, there are also many hot topics worth researching. Similar to this paper, many researchers have proposed various SEI technologies based on the technological bottlenecks encountered in the real world.

1) Lightweight SEI: Considering the huge computing overhead of DL technology, it is not suitable for the deployment of IIoT. Deng et al. [30] explored a lightweight transformer-based network for SEI and achieved great performance. Hua et al. [31] proposed a knowledge graph based electromagnetic signal feature library to replace the traditional RFF extraction module, significantly reducing computational overhead. Unlike deep learning, Xu et al. [32] proposed a broad learning architecture based on radio frequency (RF) signal feature embedding to address the SEI problem. Furthermore, Zhang et al. [33] introduced nonlinear enhancement nodes and signal feature nodes, significantly improving the performance and reducing the parameter and computational overhead.

2) Semi-Supervised SEI: In the real world, the labels of RF signals are often more difficult to be obtained than RF signals, so semi-supervised learning [34], [35] has become a popular research topic. Wu et al. [36] introduced a new approach to semi-supervised SEI (SS-SEI) using contrastive learning to address the problem of limited labeled data. The proposed method used a two-stage semi-supervised training scheme, where the feature extractor and projection head are trained with self-supervised contrastive learning on unlabeled data in the first stage, followed by fine-tuning with a combination of cross-entropy and supervised contrastive learning loss on a small amount of labeled data in the second stage. Fu et al. [37] proposed to use metric-adversarial training to achieve SS-SEI and evaluated their algorithm on an open-source automatic dependent surveillance-broadcast (ADS-B) dataset. Furthermore, Liu et al. [38] proposed a novelty adversarial augmentation powered self-supervised learning to overcome the limitation of sample dependence. Considering noncooperative areas like electronic reconnaissance and spectrum monitoring, there are unknown devices and complex electromagnetic environments, making it hard to capture data distribution and labeled samples. Tan et al. [39] proposed a self-classification generative adversarial network (GAN) using bispectrum-based feature extraction and semi-supervised learning in SS-SEI.

3) Open-Set SEI: The current SEI methods usually assume that important factors of the learning process remain constant, but with the rise of open-environment scenarios where these factors can change, the SEI technology faces a grand challenge [40], [41], [42]. Therefore, open-set SEI became the technology which urgently needs to be researched and broken through. Zhou et al. [43] proposed a verification algorithm based on the generative Gaussian probabilistic linear discriminant analysis model to achieve open-set SEI method. The author claimed that the equal error rate of the verification experiments with six authorized devices versus six unseen unauthorized devices is as low as 0.63%. Dong et al. [44] aimed to learn a framework that can distinguish not only known classes but also unlabeled unknowns. The author proposed a deep CNN-based zero-shot learning framework for open-set signal recognition and extensive experiments on various signal datasets show that the proposed method can discriminate not only known classes but also unknown classes. Xie et al. [45] proposed a new end-to-end deep learning framework including a novel preprocessing module called neural synchronization (NS). NS estimates offsets using two learnable deep neural networks jointly trained by the RFF extractor. Furthermore, a hypersphere representation is also proposed to improve RFF discrimination. Shen et al. [8] proposed a new framework for RFF identification, which used DL to train an RFF extractor and channel independent features to achieve scalability and channel robustness.

B. Multisource Heterogeneous Solution

Similar to the attention of the above researches, this paper also explores a solution that is more suitable for practical

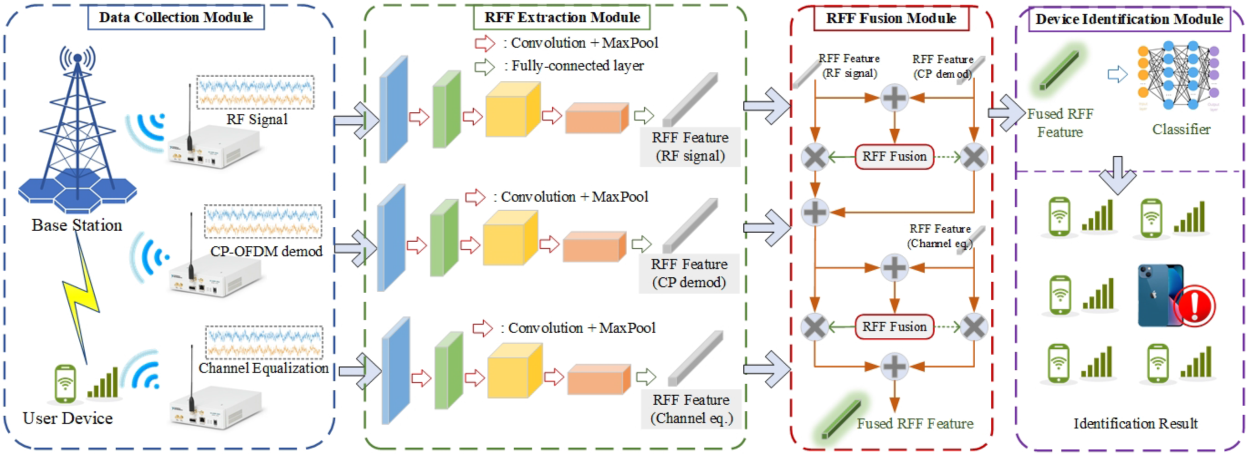


Fig. 1. Illustration of the proposed MH-SEI method. It is composed of data collection module, RFF extraction module, RFF fusion module and device identification module.

scenarios. The development of perception technology bring up tremendous smart applications, such as IIoT, V2X, smart factories, and so on. Massive different sensors complement each other to achieve a smart life which is defined as the era of Internet of Everything. Therefore, considering the data collected by different types of sensors in different locations, the multisource heterogeneous solutions are becoming a hot research topic. To address multisource heterogeneous data, Wang et al. [46] proposed a tensor deep learning model, which uses tensors to model the complexity of heterogeneous data and extends feature extraction to the tensor space. The experimental results proved that the proposed model performs well in heterogeneous data fusion. As for the issue of multisource and multisensor satellites, Gao et al. [47] proposed a heterogeneous support tensor machines by integrating rank-R decomposition of multitensors, which allowed for effective processing of multisource data represented as heterogeneous tensors. And then take another example of ship classification, Lang et al. [48] proposed a multisource heterogeneous transfer learning method that allows each domain to be represented by a more appropriate feature, improving ship classification performance. In the topic of V2X, many researches have also emerged focusing on multisource heterogeneous data. Wang et al. [49] proposed a multi-task hypergraph convolutional neural network for the multisource traffic prediction problem. The proposed method achieves superior performance compared to state-of-the-art methods in node-level traffic forecasting on historical datasets of Beijing. Fang et al. [50] proposed a meta learning feature fusion strategy to integrate external multisource heterogeneous traffic data. The superiority of the proposed model is demonstrated through experiments on three real-world traffic datasets.

III. System Model and Problem Formulation

A. System Model

In this section, we describe the system model of MH-SEI method in detail. Without loss of generality, this paper explores the rapid authentication of wireless devices identification based on multisource captured wireless signals under long term evolution (LTE) standard (a representative SEI application), aiming to quickly detect illegal user equipment. As is shown in Fig. 1, the proposed MH-SEI method is composed of four modules: data collection module, RFF extraction module, RFF fusion module and device identification module.

1) Data Collection Module: At this stage, universal software radio peripheral (USRP) is used to capture wireless signals between user devices and base stations.[1] We set the USRP used for transmission to the LTE communication system and deployed other three USRPs to capture signals. The USRPs used as receivers are deployed in different locations and set to different reception modes. The signals collection workflow will be described in detail in the subsequent section.

2) RFF Extraction Module: In this part, convolutional layers and fully connected layers are used to extract deep hidden features from I/Q signals. In the MH-SEI method, this module has multiple different branches corresponding to multiple heterogeneous wireless signals. In this paper, we set up three receivers with different positions and modes to receive the original RF signals, the signals after CP-OFDM demodulation, and the signals after channel equalization.

3) RFF Fusion Module: Here, an attention mechanism based feature fusion algorithm is used to mix three different RFFs. This module is the core module used to solve the MH-SEI problem, which uses attention mechanism to mix multi-source heterogeneous signals and their corresponding RFFs to generate a fused RFF. The fused RFF is used for the subsequent automatic classifier to achieve device recognition.

4) Device Identification Module: The last module contains an automatic classifier neural network to identify different devices from the fused RFF. Finally, based on the classification results, legitimate devices will be authorized and illegal devices will be reported.

B. Problem Formulation

This paper aims at proposing an MH-SEI method to solve the multisource heterogeneous signals in real-world IIoT

[1] In order to ensure the legitimacy of our research, we did not capture signals from commercial base stations directly, but instead chose an additional USRP to simulate the signals transmitted by the user device.

scene. Suppose there are N signal sources, denoted by $S = \{s_1, s_2, \ldots, s_N\}$, and a set of M receiver sensors, denoted by $R = \{r_1, r_2, \ldots, r_M\}$. The signals transmitted by the sources are denoted by $X = \{x_2, x_3, \ldots, x_N\}$. Assume that each sensor measures a different signal model due to their different locations and sensitivities. We define H_{ij} as the signal propagation model from the i-th source to the j-th sensor, where $i = 1, 2, 3, \ldots, N$ and $j = 1, 2, \ldots, M$. Then, the received signal $\boldsymbol{y}_{ij}$ at the j-th sensor from the i-th source can be expressed as,

$$\boldsymbol{y}_{ij} = \mathbf{H}_{ij}(\boldsymbol{x}_i) + \boldsymbol{n}_{ij}, \tag{1}$$

where $\boldsymbol{n}_{ij}$ is the noise and interference at the j-th sensor. The goal of the multisource heterogeneous SEI problem is to identify the source of each signal based on the received signals measured by the sensors. Let C_i be the class label of the i-th source, where $C_i = 1, 2, \ldots, N$. Then, the problem can be stated as follows: Given a set of labeled training data $\{[(\boldsymbol{y}_{i1}, \boldsymbol{y}_{i2}, \ldots, \boldsymbol{y}_{iM}), c_i]\}$, where $i = 1, 2, \ldots, N$, the goal is to learn a classifier $f_{SEI}((\boldsymbol{y}_{i1}, \boldsymbol{y}_{i2}, \ldots, \boldsymbol{y}_{iM}), \omega)$ that can accurately predict the source label c_i of a new received signal $(\boldsymbol{y}_{i1}, \boldsymbol{y}_{i2}, \ldots, \boldsymbol{y}_{iM})$. The issue can be summarized as,

$$\widetilde{\omega} = \arg min \xi\{f_{SEI}(\boldsymbol{y}_{i1}, \boldsymbol{y}_{i2}, \ldots, \boldsymbol{y}_{iM}), c_i\}, \tag{2}$$

where $\widetilde{\omega}$ is the optimized weight of the SEI model and $\xi(\cdot)$ is the loss function of training strategy.

IV. Proposed MH-SEI Method

This section provides a detailed description of the proposed MH-SEI method. The data collection module is a hardware platform. The RFF extraction module, RFF fusion module, and automatic classifier compose the neural network proposed in this paper, called multisource heterogenous attention fingerprinting fusion network (MHAFFN).

A. Data Collection Module

We collected the dataset in a laboratory environment. As shown in Fig. 2, all data collection devices are deployed in an office 15 meters long and 8 meters wide. In order to simulate the actual environment more realistically, we have arranged desks and a glass wall in the office. The communication procedure is under LTE standard with frequency of 800 MHz. There are a total of 4 USRPs in operation in the entire laboratory each time, including 1 transmitter and the other 3 receivers. Three receivers are deployed at different locations in the laboratory and receive signals from different stages of the LTE communication system. The data collected in this paper is for verifying the MH-SEI method, so we have made the following deployment:

- Multisource: Three receivers are deployed in different positions, covering both LOS and NLOS channels.
- Heterogeneous: Three receivers collect signals from different stages of the LTE communication process, including the original signal, the signal for CP-OFDM demodulation, and the signal after channel equalization.

The detailed data information is shown in the Tab. I. Among them, $\boldsymbol{y}_{R1} \in \mathbb{R}^{30720\times 2}$ means a complex vector with a time slot length of 30720 bits for the LTE signal. And $\boldsymbol{y}_{R2} \in \mathbb{R}^{14\times 2048\times 2}$ is a complex matrix that represents the signal after removing the OFDM cyclic prefix, containing 14 OFDM symbol numbers and corresponding 2048 bits of information. Finally, $\boldsymbol{y}_{R2} \in \mathbb{R}^{12\times 1200\times 2}$ is also a complex matrix which represents the signal after channel equalization, including 12 sub-carriers and corresponding 1200 bits of information.

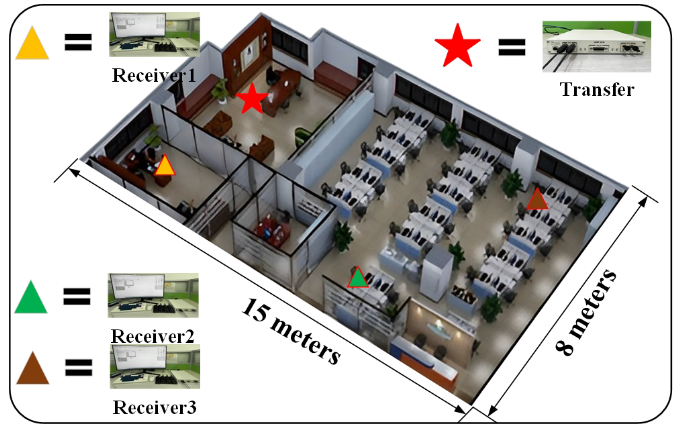


Fig. 2. Illustration of the data collection environment.

TABLE I
Information of Multi Source Heterogeneous Dataset

Source	Category	Shape	Symbol
Receiver1	Original RF signals	30720×2	$\boldsymbol{y}_{R1}$
Receiver2	Signals of lifting OFDM cyclic prefix	$14 \times 2048 \times 2$	$\boldsymbol{y}_{R2}$
Receiver3	Signals passing through channel equalization filter	$12 \times 1200 \times 2$	$\boldsymbol{y}_{R3}$

B. RFF Extraction Module

After the data collection module, this part introduces a multi branch parallel RFF extraction module. We design a multi branch and multi-scale CNN to extract RFF corresponding to different receiver signals. Fig. 3 shows the workflow of the proposed multi-channel RFF feature extraction module. Each branch starts with different received data ($\boldsymbol{y}_{Ri}$), then passes through some well-designed network layers, and finally outputs the corresponding RFF (Γ_{Ri}) of that branch. The structure of each layer and the detailed hyper-parameter setting are shown in Tab. II. As shown in Fig. 3, considering the different structural lengths of $\boldsymbol{y}_{R1}$ and $\boldsymbol{y}_{R2}, \boldsymbol{y}_{R3}$, we mixed one-dimensional convolutional layers and two-dimensional convolutional layers. Among them, after each convolutional layer, we add a maximum pooling layer to compress the signal dimension and further explore deep features. The last layer of all branches in this module is designed with a fixed fully connected layer, aiming to obtain RFFs with the same length for the next RFF fusion module. In summary, we define this module as,

$$\Gamma_{Ri} = \mathcal{L}_{Fi}\left\{\delta_r\left\{\mathcal{L}^4_{Pi}\left[\mathcal{L}^4_{*i}\left(\boldsymbol{y}_{Ri}, \boldsymbol{\omega}_{*i}\right)\right]\right\}, \boldsymbol{\omega}_{Fi}\right\}, \tag{3}$$

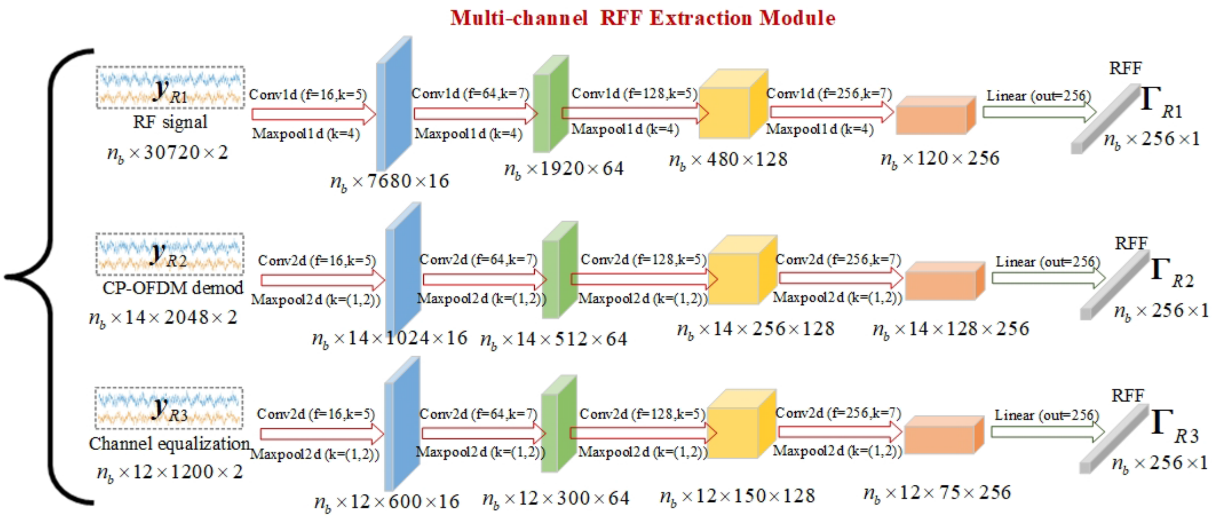


Fig. 3. Illustration of the proposed RFF extraction module. It is composed of three different channels to extract RFFs from multisource heterogeneous data.

TABLE II
STRUCTURE OF MULTI-CHANNEL RFF EXTRACTION MODULE AND THE CORRESPONDING HYPER-PARAMETERS SETTING

Branch	Layer	Hyper-parameters
	Input Data	Shape = $[n_b \times 30720 \times 2]$
	Conv1D+Relu+BN+Relu	Filter=16, Kernel=5
	MaxPooling1D	Kernel=4
	Conv1D+Relu+BN+Relu	Filter=64 ,Kernel=7
	MaxPooling1D	Kernel=4
$\boldsymbol{y}_{R1}$	Conv1D+Relu+BN+Relu	Filter=128, Kernel=5
	MaxPooling1D	Kernel=4
	Conv1D+Relu+BN+Relu	Filter=256, Kernel=7
	MaxPooling1D	Kernel=4
	Fully-Connected+Linear	Filter=256
	Output RFF Γ_{R1}	Shape = $[n_b \times 256 \times 1]$
	Input Data	Shape = $[n_b \times 14 \times 2048 \times 2]$
	Conv2D+Relu+BN+Relu	Filter=16, Kernel=5
	MaxPooling2D	Kernel=(1,2)
	Conv2D+Relu+BN+Relu	Filter=64, Kernel=7
	MaxPooling2D	Kernel=(1,2)
$\boldsymbol{y}_{R2}$	Conv2D+Relu+BN+Relu	Filter=128, Kernel=5
	MaxPooling2D	Kernel=(1,2)
	Conv2D+Relu+BN+Relu	Filter=256, Kernel=7
	MaxPooling2D	Kernel=(1,2)
	Fully-Connected+Linear	Filter=256
	Output RFF Γ_{R2}	Shape = $[n_b \times 256 \times 1]$
	Input Data	Shape = $[n_b \times 1024 \times 1200 \times 2]$
	Conv2D+Relu+BN+Relu	Filter=16, Kernel=5
	MaxPooling2D	Kernel=(1,2)
	Conv2D+Relu+BN+Relu	Filter=64, Kernel=7
	MaxPooling1D	Kernel=(1,2)
$\boldsymbol{y}_{R3}$	Conv2D+Relu+BN+Relu	Filter=128, Kernel=5
	MaxPooling2D	Kernel=(1,2)
	Conv2D+Relu+BN+Relu	Filter=256, Kernel=7
	MaxPooling2D	Kernel=(1,2)
	Fully-Connected+Linear	Filter=256
	Output RFF Γ_{R3}	Shape = $[n_b \times 256 \times 1]$

NOTE: The "Filter" and "Kernel" are the corresponding key values in layer settings. The "shape" refers to the size of the tensor in neural network, and n_b represents the batch size.

where Γ_{Ri} represents the RFF extracted from the i-th receiver signals $\boldsymbol{y}_{R_i}$, $\mathcal{L}_{Fi}$, $\mathcal{L}_{Pi}$, $\mathcal{L}_{*i}$ are fully connected layer, maximum pooling layer and convolutional layer, respectively, $\boldsymbol{\omega}_{Fi}$, $\boldsymbol{\omega}_{*i}$ are the corresponding weight of fully connected layer and

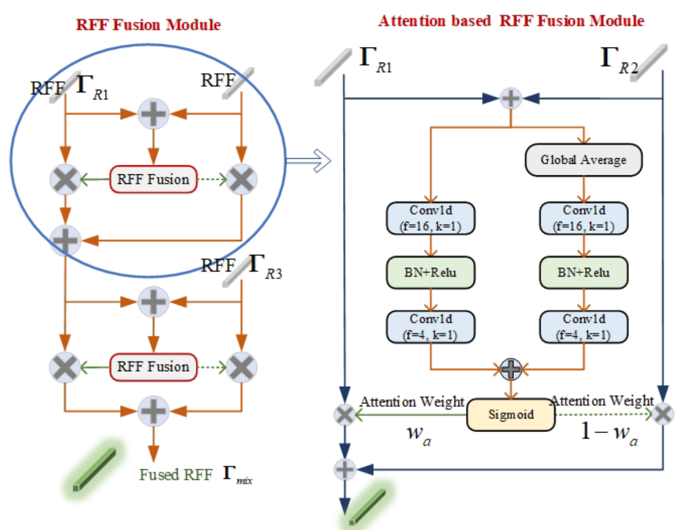


Fig. 4. Illustration of the RFF fusion module. It is designed based on attention mechanism. This module is used to fuse RFFs from multiple channels.

convolutional layer, and δ_r means the Relu activation function utilized in this module. The Relu function is defined as $f(x) = max(0, x)$. It should be claimed that the activation function can be replaced for different scenarios. The Relu activation function is determined to be utilized in this manuscript based on the results of several attempts.

C. RFF Fusion Module

The RFF fusion module is considered as the key module for the MH-SEI method. The biggest difference between MH-SEI and traditional SEI methods is that MH-SEI obtains multiple RFF features from several branches by the RFF extraction module, which cannot be directly used for automatic classifiers. Therefore, we design a feature fusion module [51] based on attention mechanism for the fusion of multiple RFFs. There is no denying that the attention mechanism is one of the greatest invention in the history of deep learning development.

The design inspiration for the attention mechanism comes from the subjective ability of the human eye to capture information. Humans always first see what they are concerned about and ignore irrelevant background items. In the MH-SEI problem, we hope that the proposed method is able to focus on RFFs which play a critical role in SEI and ignore some less important parts. As is shown in Fig. 4, this part is designed in a modular manner, and RFFs from multiple branches will be fused in pairs. One of the fusion modules is expanded on the right side of Fig. 4. The mixed RFF is defined as,

$$\begin{cases} \Gamma_{mix} &= \omega_{ai} \otimes \Gamma_{Ri} + (1 - \omega_{ai}) \otimes \Gamma_{R(i+1)}, i = 1 \\ \Gamma_{mix} &= \omega_{ai} \otimes \Gamma_{mix} + (1 - \omega_{ai}) \otimes \Gamma_{R(i+1)}, i = 2, 3, \ldots, N \end{cases} \tag{4}$$

where Γ_{mix} denotes the fused RFF, and $\otimes$ represents the multiplication operation of corresponding elements. And ω_{ai} is the attention weight between Γ_{Ri} and $\Gamma_{R(i+1)}$ obtained by RFF fusion algorithm, which is defined as,

$$\omega_a = \sigma \left[\cap(\Gamma_{R1} \oplus \Gamma_{R2}) \oplus \cup(\Gamma_{R1} \oplus \Gamma_{R2}) \right], \tag{5}$$

where σ is the sigmoid activation function, $\cap(\cdot)$ and $\cup(\cdot)$ correspond to the two branches in Fig. 4, respectively. The $\cap(\cdot)$ operation consists of convolutional layers and the batch normalization (BN) layer, and the $\cup(\cdot)$ has an additional global average pooling layer than $\cap(\cdot)$.

$$\cap(x) = \mathcal{L}_* \left\{ \delta_r \left\{ \mathcal{L}_{BN} \left[\mathcal{L}_*(x, \boldsymbol{\omega}_*) \right] \right\}, \boldsymbol{\omega}_* \right\}, \tag{6}$$

$$\cup(x) = \mathcal{L}_* \left\{ \delta_r \left\{ \mathcal{L}_{BN} \left\{ \mathcal{L}_{*1} \left[\mathcal{L}_{GL}(x), \boldsymbol{\omega}_* \right] \right\} \right\}, \boldsymbol{\omega}_* \right\}, \tag{7}$$

where $\mathcal{L}_*$, $\mathcal{L}_{BN}$, $\mathcal{L}_{GL}$ are convolutional layer, BN layer, global average pooling layer, respectively, $\boldsymbol{\omega}_*$ is the corresponding weight of $\mathcal{L}_*$, and δ_r is the same activation function with Eq. 3. The Relu activation function is also determined based on several training attempts.

After the above operations, the ω_a and corresponding $(1 - \omega_a)$ obtained are the weights of two different RFFs. In other words, the more important RFF will get the higher weight. In Eq. 4, the fusion process of different RFFs is influenced by the weight ω_a. The result is that the more important RFF will play a more important and even decisive role in Γ_{mix}. This is the RFF fusion module based on attention mechanism, where important RFFs are assigned higher weights and have a greater impact on MH-SEI performance.

D. Automatic Classifier Module

This part describes the automatic classifier in the MHAFNN in detail. As is shown in Fig. 5, the input of this module is the fused RFF, and the final output is the result of device identification. The automatic classification module consists of three fully-connected layers, with the first two layers using the Relu activation function and the last layer using the Softmax activation function. It should be noted that the output hyper-parameter of the last fully-connected layer is defined by the number of MH-SEI device categories and must meet the condition of $out = C_k$.

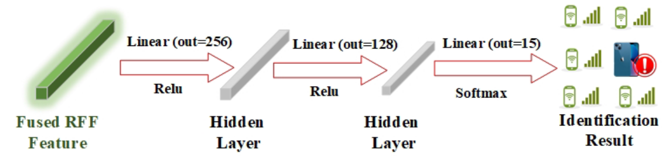


Fig. 5. Illustration of the automatic classifier module. It is composed three fully-connected layers.

E. Summary and Workflow

In summary, the RFF extraction module and RFF fusion module introduced above constitute the proposed MHAFFN neural network, aiming to solve the MH-SEI problem. The collected multi-source heterogeneous RF signals are first input into multi-channel convolutional neural network to extract RFF of different modes. Then multiple RFFs will be input into the RFF fusion module, and important RFFs will be filtered out and given greater weight by the attention mechanism. Finally, the mixed RFF is input into automatic classifier to complete MH-SEI technology. The workflow of MHAFFN process is shown in **Algorithm.** 1. As for large-scale MH-SEI scenarios, the proposed MHAFFN is still able to be deployed. The multi-channel RFF extraction module adopts parallel logic, where the perception data from multiple receivers is extracted in parallel. The number of the channels can be increased or decreased according to different demands. Similarly, the RFF fusion module is also designed with scalability, which is shown in Eq. 4. A large number of RFFs from different channels are sequentially fused in this module. It theoretically supports the fusion of infinite RFFs.

V. Experimental Results

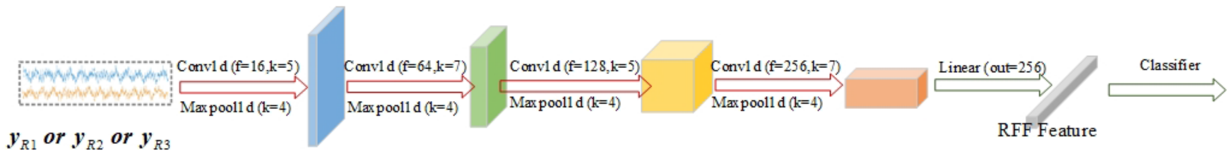
A. Dataset and Experimental Platform

1) Dataset: This paper employs a total of 18 USRP devices to facilitate comprehensive data collection [52]. Within this set, 15 USRP devices operate as distinct radiation sources, sequentially transmitting signals. The remaining 3 USRP devices, on the other hand, function as a diverse ensemble of multi-source receivers. A visual representation of the data collection environment and the strategic arrangement of these devices is depicted in Fig. 2. Notably, each individual receiver yields 10,000 samples per acquisition cycle. To ensure an effective training regimen, the distribution of samples for training, validation, and testing adheres to a 6:2:2 ratio. For a more intricate understanding of the variations in data samples across disparate receivers, the taxonomy and structural attributes are detailed in Table I.

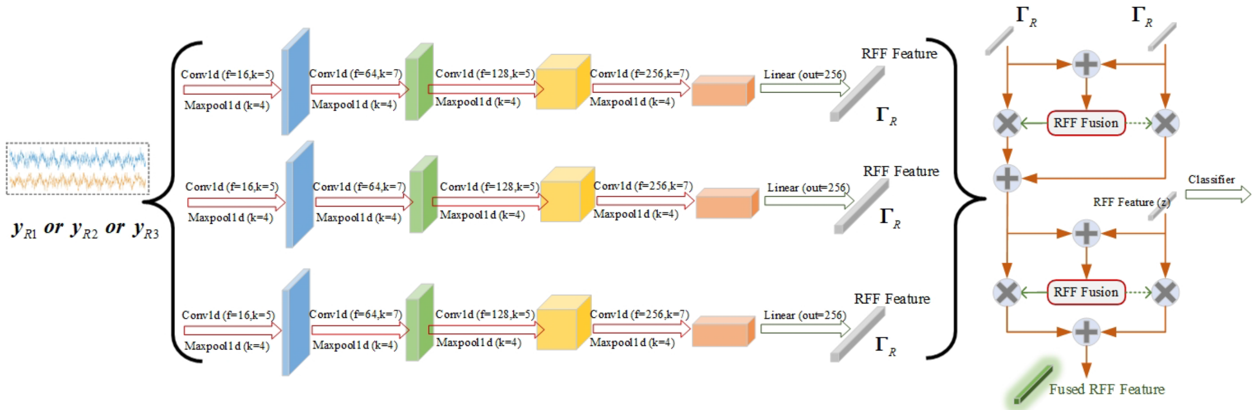
2) Experimental Platform: All the simulations are carried out on a workstation equipped with two Intel(R) Xeon(R) Silver 4210R CPUs and four Nvidia RTX 2080Ti GPUs.

B. Benchmarks And Metrics

To verify the effectiveness of the MH-SEI method and the robustness of the proposed MHAFFN, we design two benchmarks. The flowchart of the benchmark algorithm is shown in Fig. 6.



(a) Illustration of Benchmark1: CNN-R_i



(b) Illustration of Benchmark2: AFFCNN-R_i

Fig. 6. Illustration of the benchmarks applied in the experimental part. CNN-R_i & AFFCNN-R_i.

Algorithm 1 The Algorithm Statement of Proposed MHAFFN Identification System for MH-SEI Problem

Input: $\boldsymbol{y}_{k-R1}, \boldsymbol{y}_{k-R2}, \boldsymbol{y}_{k-R3} \leftarrow$ RF signals; $C_k \leftarrow$ Device labels; $\eta \leftarrow$ Initial learning rate; $\tau \leftarrow$ Maximum epoch number;

Output: $\widehat{C_k} \leftarrow$ Identified device labels

Training stage:

Load training data: $\boldsymbol{y}_{k-R1}(n) \in \mathbb{R}^{30720\times 2}$, $\boldsymbol{y}_{k-R2}(n) \in \mathbb{R}^{14\times 2048\times 2}$, $\boldsymbol{y}_{k-R2}(n) \in \mathbb{R}^{12\times 1200\times 2}$, C_k;

Randomly initialize NN weight parameters $\boldsymbol{\omega}_{*i}, \boldsymbol{\omega}_{Fi}$;

for $t = 1, \cdots, \tau$ **do**

  Multi-channel RFF Extraction:

  $\Gamma_{R1} = \mathcal{L}_{F1}\left\{\delta_r\left\{\mathcal{L}_{P1}^4\left[\mathcal{L}_{*1}^4\left(\boldsymbol{y}_{R1}, \boldsymbol{\omega}_{*1}\right)\right]\right\}, \boldsymbol{\omega}_{F1}\right\}$

  $\Gamma_{R2} = \mathcal{L}_{F2}\left\{\delta_r\left\{\mathcal{L}_{P2}^4\left[\mathcal{L}_{*2}^4\left(\boldsymbol{y}_{R2}, \boldsymbol{\omega}_{*2}\right)\right]\right\}, \boldsymbol{\omega}_{F2}\right\}$

  $\Gamma_{R3} = \mathcal{L}_{F3}\left\{\delta_r\left\{\mathcal{L}_{P3}^4\left[\mathcal{L}_{*3}^4\left(\boldsymbol{y}_{R3}, \boldsymbol{\omega}_{*3}\right)\right]\right\}, \boldsymbol{\omega}_{F3}\right\}$

  RFF Fusion:

  $\omega_{a_1} = \sigma\left[\cap(\Gamma_{R1} \oplus \Gamma_{R2}) \oplus \cup(\Gamma_{R1} \oplus \Gamma_{R2})\right]$

  $\Gamma_{mix} = \omega_{a1} \otimes \Gamma_{R1} + (1 - \omega_{a1}) \otimes \Gamma_{R2}$

  $\omega_{a_2} = \sigma\left[\cap(\Gamma_{mix} \oplus \Gamma_{R3}) \oplus \cup(\Gamma_{mix} \oplus \Gamma_{R3})\right]$

  $\Gamma_{mix} = \omega_{a2} \otimes \Gamma_{mix} + (1 - \omega_{a2}) \otimes \Gamma_{R3}$

  $loss_t = -\sum_{k=1} C_k \cdot \log(\hat{C}_k)$

  if *$loss_t$ converges to $loss^*$* **then**

    break;

  end

  if *$loss_t$ is not updated after 20 loops* **then**

    $\eta = \eta \times 0.7$;

  end

  $\boldsymbol{\omega}_{*i}, \boldsymbol{\omega}_{Fi} \leftarrow \mathrm{Adam}(\boldsymbol{\omega}_{*i}, \boldsymbol{\omega}_{Fi}, \eta, \nabla loss_t)$

end

- CNN-R_i: We selected a branch in MAFFN and removed the RFF fusion module as the benchmark, named CNN. The input of CNN are I/Q signals from one of three receivers, namely CNN-R1, CNN-R2, and CNN-R3.
- AFFCNN-R_i: To further ensure algorithm fairness, we define the second benchmark algorithm, which keeps the same network architecture with MHAFFN, named attention feature fused CNN (AFFCNN). The difference is that the input data of three branches are from the same receiver, that is, AFFCNN-R1, AFFCNN-R2, and AFFCNN-R3.

The metrics used to measure the performance of the algorithm in this paper are accuracy, precision, recall, and F1 score, which are defined as,

$$\begin{cases} Acc &= \dfrac{TP + TN}{TP + TM + FP + FN} \times 100\%, \\ Pre &= \dfrac{TP}{TP + FP} \times 100\%, \\ Rec &= \dfrac{TP}{TP + FN} \times 100\%, \\ F1 &= \dfrac{2 \times Pre \times Rec}{Pre + Rec}, \end{cases} \tag{8}$$

where TP predicts positive classes as positive class numbers, TN predicts negative classes as negative class numbers, FP predicts negative classes as positive class numbers, and FN predicts positive classes as negative class numbers. Accuracy is the proportion of all correctly judged results in total observed values. Precision is the proportion of prediction right among all the results predicted by the model as positive. Recall is the proportion of predicted right in all results where the true value is Positive.

C. Experimental Results

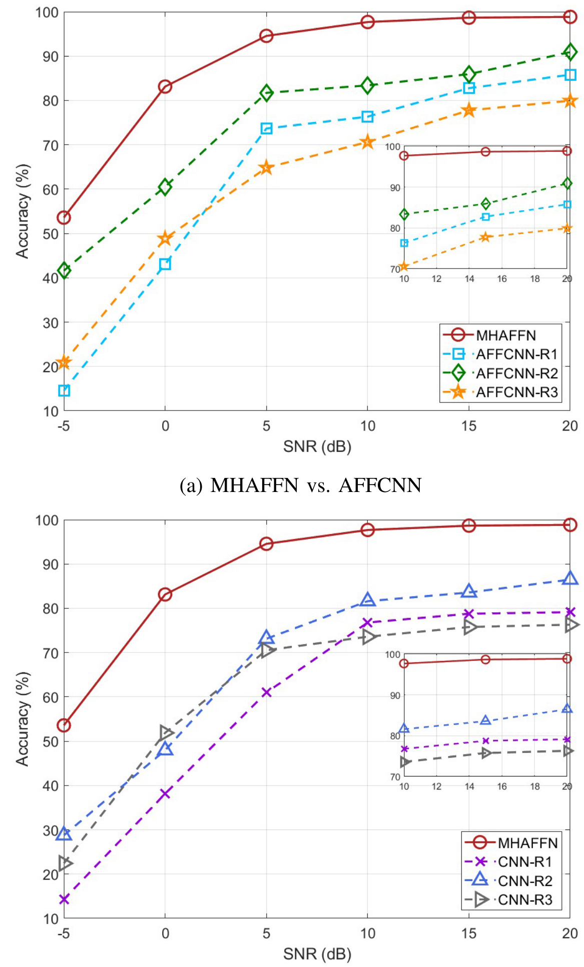
In this subsection, we devise three experiments to validate the proposed methodology, namely MHAFFN, and demonstrate its exceptional performance in addressing the MH-SEI challenge. Firstly, we conduct a feasibility verification, assessing the efficacy of the introduced MHAFFN using

TABLE III
RESULTS OF FOUR INDICATORS OF MHAFFN AND BENCHMARKS

Methods	Acc (%)	Pre (%)	Rec (%)	F1
MHAFFN (proposed)	**99.196**	**99.208**	**99.196**	**0.9920**
AFFCNN-R1	90.089	90.101	90.089	0.8998
AFFCNN-R2	91.339	87.817	91.339	0.8896
AFFCNN-R3	80.982	81.833	80.982	0.8118
CNN-R1	83.839	84.424	83.839	0.8356
CNN-R2	88.892	87.383	88.892	0.8763
CNN-R3	76.071	76.841	76.071	0.7590

key performance indicators: accuracy (Acc), precision (Pre), recall (Rec), and F1-score. Subsequent to this, we design a robustness validation experiment, wherein we emulate the influence of complex electromagnetic environments on RF signal propagation through the introduction of additive white Gaussian noise (AWGN). We examine the performance across diverse signal-to-noise ratios, thereby affirming the pronounced robustness of the MHAFFN proposal. Finally, we carry on a fault tolerance mechanism verification. This experiment uses a certain length of Gaussian white noise to randomly mask the corresponding length I/Q values in RF signal samples. This emulation of real-world sensor failure scenarios serves to validate the heightened adaptability inherent in the proposed MHAFFN, further underscoring its fault tolerance mechanism.

1) Feasibility Verification: This part verifies the feasibility and superiority of our proposed solution MHAFFN. We trained MHAFFN with 6000 samples and tested with an additional 2000 samples. We set an automatic stop strategy during the training process. If the Acc index does not improve within 20 epochs, the training will be terminated early to reduce the training overhead. The CNN-R1/R2/R3 denotes the performance of benchmark1 with the simple CNN. The MCNN-R1/R2/R3 denotes the performance of benchmark2 with multi-branch CNN and attention feature fusion module. For the sake of fairness in comparison, all benchmark algorithms were set the same training strategy as MHAFFN. After experimental verification, in an ideal environment without noise, the Acc, Pre, Rec, and F1-score of MHAFFN in solving MH-SEI problems are 99.196%, 99.208%, 99.196%, and 99.197%, respectively. Correspondingly, the best performance of AFFCNN under the four indicators is 91.339%, 90.101%, 91.339%, and 89.976%, respectively. This is a 10% decrease compared to the proposed MHAFFN. The best scores for the four indicators of another benchmark algorithm CNN are 88.892%, 87.383%, 88.892%, and 87.634%, respectively. This is the worst grade, approximately 13% worse than the proposed MHAFFN. In summary, the MHAFFN proposed in this paper demonstrates sufficient feasibility and significant performance advantages in solving MH-SEI problems. It is not difficult to find from the experimental results that the benchmark algorithms selected in the manuscript are not applicable to the MH-SEI problem. These traditional SEI methods can only input and identify single receiver's data, so they are not suitable for MH-SEI problems. This is a design bug of the traditional algorithms that leads to the waste of a large amount of multi-source heterogeneous data. In other words, only a small portion of the multi-source heterogeneous data can be utilized by the benchmark algorithm. It can be foreseen that if traditional SEI methods are forcibly applied to complex IIoT scenarios, a large amount of heterogeneous data from multiple sources will be wasted, inevitably leading to poor performance.



(a) MHAFFN vs. AFFCNN

(b) MHAFFN vs. CNN

Fig. 7. Performance comparison under different SNR environments.

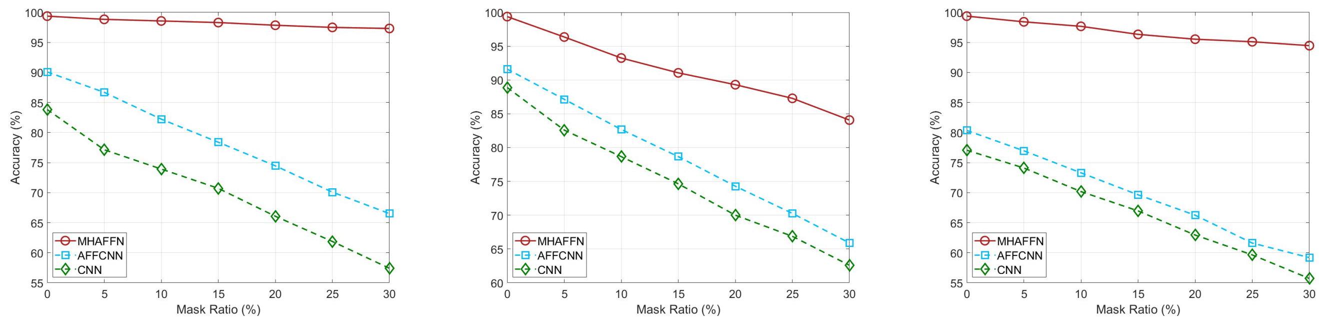
2) Robustness Verification: This part verifies the robustness under noise environment of our proposed solution MHAFFN. We introduce AWGN to simulate SEI tasks in imperfect environments. The model robustness is tested at different signal-to-noise ratios $SNR = \{-5, 0, 5, 10, 15, 20\}$ (dB). The SNR and AWGN are defined as follows,

$$SNR = 10 \cdot \log\left(\frac{P_x}{P_n}\right) \text{ (dB)}, \tag{9}$$

$$noise \sim N(0, P_n) = \frac{1}{\sqrt{2\pi P_n}} \cdot \exp\left(-\frac{x^2}{2P_n}\right), \tag{10}$$

where P_x and P_n are the respective powers of ADS-B signals and $noise$, $N(0, P_n)$ represents a normal distribution with $mean = 0$ and $variance = P_n$. It is not difficult to find that $SNR = 0$ is a critical point, under which the effective information and noise power are the same.

The results of the robustness verification are shown in Fig. 7, the x-axis represents the magnitude of noise, the higher the



(a) Receiver-1 damaged (b) Receiver-2 damaged (c) Receiver-3 damaged

Fig. 8. Identification performance evaluation in different sensor damage scenarios.

SNR, the smaller the noise, and the y-axis represents the accuracy that different algorithms can achieve under different noise conditions. The solid red lines in both Fig. 7a and 7b represent the performance curve of the proposed MHAFFN, The dashed lines in cyan, green, and orange in Fig. 7a represent the performance of the benchmark AFFCNN with received signals from only receiver-1, receiver-2, and receiver-3, respectively. Similarly, the dashed lines in purple, blue, and gray in Fig. 7b indicate the performance of the benchmark CNN with received signals from only receiver-1, receiver-2, and receiver-3, respectively. From the graph, it can be seen that the solid red line can maintain a high recognition accuracy under any SNR condition, and is about 10% – 15% higher than other dashed lines. This is consistent with the conclusion we reached in the feasibility verification part. From the curve analysis in the figure, there is no doubt that MHAFFN can keep higher identification accuracy than the two benchmarks in any SNR environment.

3) Fault Tolerance Mechanism: In this part, we aim to further verify the fault tolerance mechanism of MHAFFN. Considering a real IIoT scenario, sensor damage is a common issue. Another advantage of MH-SEI technology is its higher fault tolerance. If M out of N sensors are damaged, MH-SEI technology is able to achieve accurate and efficient identification result through the signals from $(N-M)$ sensors. Compared to traditional SEI technology using single data source, it is obvious that the MHAFFN proposed in this paper has its inherent fault-tolerant mechanism. Therefore, we use random AWGN signal to cover a certain proportion of data from a receiver to simulate this specific scene. Assuming the length of AWGN signal is Len_a and the original signal length is Len_s, the mask ratio can be defined as follow,

$$MaskRatio(\%) = Len_a / Len_s \times 100\%. \tag{11}$$

As is shown in Fig. 8, the x-axis is the mask ratio, which represents the proportion of the original signal being covered. The y-axis represents the recognition accuracy of different algorithms in this experiment. The larger the mask ratio, the longer time it takes for the sensor to be damaged or down. The solid red lines represent the performance curve of the proposed MHAFFN, while the cyan and green dashed lines represent the performance of the AFFCNN and CNN, respectively. Fig. 8a, 8b, and 8c represent the damage or downtime of receiver 1, receiver 2, and receiver 3, respectively. The experimental results exhibit that the proposed MHAFFN can maintain stable identification performance even in the event of one receiver outage. Therefore, from the curve analysis in the figure, we conclude that the proposed MHAFFN has a better fault-tolerant mechanism than traditional SEI methods.

TABLE IV

COMPUTATIONAL COMPLEXITY AND STORAGE OVERHEAD OF THE PROPOSED MHAFFN AND BENCHMARKS

	FLOPs	$T_{train}(s)$	$T_{test}(s)$	Parameters
MHAFFN	4.908G	3085.855	1.487	298.702M
AFFCNN-R1	1.525G	4234.312	1.744	379.420M
AFFCNN-R2	6.275G	4764.008	1.807	356.909M
AFFCNN-R3	3.102G	2385.876	1.087	155.582M
CNN-R1	1.524G	881.423	1.255	24.732M
CNN-R2	2.416G	882.032	0.706	33.291M
CNN-R3	1.189G	517.312	0.437	12.45M

D. Complexity Analysis

This section aims to further analyze the computational and storage overhead of the proposed MHAFFN. For a DL based algorithm solution, its computational complexity and parameter storage overhead determine whether the scheme can be applied in real world. The main computational cost of the proposed MHAFFN network is concentrated in the convolutional layer, and the parameter storage cost is concentrated in the fully connected layer. During analysis and calculation, the computational complexity and parameter count of the proposed MHAFFN and its corresponding benchmark algorithm are shown in Table IV. The experimental results in Tab. IV were obtained by training 200 epochs, with batch-size of 32. The floating point operations (FLOPs) refer to the number of floating-point operations, which can be understood as a unit that describes the total amount of computation. The T_{train} and T_{test} represent the training time and testing time recoded automatically. The parameters denotes the storage overhead in hard disk. From the analysis of the numerical results, it is not difficult to conclude that the proposed MHAFFN is a relatively complex algorithm compared with benchmarks. Correspondingly, MHAFFN exhibits better recognition performance and robustness. Considering that MHAFFN can provide better utilization of multi-source heterogeneous data and achieve better performance, we believe that such computational overhead is acceptable and necessary.

VI. Conclusion

In this paper, we investigated the MH-SEI method, which is a common issue in the real world. We designed MHAFFN as MH-SEI technology, which consists of a multi-channel RFF feature extraction module, an RFF fusion module based on attention mechanism, and an automatic classifier. To validate the proposed MH-SEI method, we built a multisource heterogeneous receiving platform based on a laboratory environment. The experimental results exhibited that the proposed MHAFFN achieved excellent identification performance in perfect environments. Even with the presence of noise interference, MHAFFN could still maintain its performance advantage. Finally, we explored whether the proposed MHAFFN can still work stably in real-world scenarios where sensor damage occurs, and the answer is yes. The experimental results demonstrated excellent fault tolerance mechanism of MHAFFN, which is a major advantage compared to traditional SEI methods. The proposed MH-SEI method is applicable to IIoT, digital twins, vehicle-to-everything and other scenarios. And we aims at further ensuring the security of high-tech life in society.

References

[1] 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.

[2] P. Zhang et al., "Real-time malicious traffic detection with online isolation forest over SD-WAN," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2076–2090, 2023.

[3] E. Bout, V. Loscri, and A. Gallais, "Evolution of IoT security: The era of smart attacks," *IEEE Internet Things Mag.*, vol. 5, no. 1, pp. 108–113, Mar. 2022.

[4] E. Bout, V. Loscri, and A. Gallais, "How machine learning changes the nature of cyberattacks on IoT networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 248–279, 1st Quart., 2022.

[5] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE J. Radio Freq. Identificat.*, vol. 4, no. 3, pp. 222–233, Sep. 2020.

[6] T. Jian et al., "Deep learning for RF fingerprinting: A massive experimental study," *IEEE Internet Things Mag.*, vol. 3, no. 1, pp. 50–57, Mar. 2020.

[7] S. U. Rehman, K. W. Sowerby, S. Alam, and I. Ardekani, "Portability of an RF fingerprint of a wireless transmitter," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 151–156.

[8] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, "Towards scalable and channel-robust radio frequency fingerprint identification for LoRa," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 774–787, 2022.

[9] Y. Wang, J. Wang, W. Zhang, J. Yang, and G. Gui, "Deep learning-based cooperative automatic modulation classification method for MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4575–4579, Apr. 2020.

[10] Y. Wang et al., "Distributed learning for automatic modulation classification in edge devices," *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2177–2181, Dec. 2020.

[11] Y. Tu, Y. Lin, C. Hou, and S. Mao, "Complex-valued networks for automatic modulation classification," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 10085–10089, Sep. 2020.

[12] Y. Yang, F. Gao, C. Xing, J. An, and A. Alkhateeb, "Deep multimodal learning: Merging sensory data for massive MIMO channel prediction," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 7, pp. 1885–1898, Jul. 2021.

[13] J. Guo, C.-K. Wen, and S. Jin, "Deep learning-based CSI feedback for beamforming in single- and multi-cell massive MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 7, pp. 1872–1884, Jul. 2021.

[14] H. Huang, Y. Peng, J. Yang, W. Xia, and G. Gui, "Fast beamforming design via deep learning," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1065–1069, Jan. 2020.

[15] R. Zhao et al., "A novel intrusion detection method based on lightweight neural network for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9960–9972, Jun. 2022.

[16] L. Liu, G. Han, Z. Xu, J. Jiang, L. Shu, and M. Martínez-García, "Boundary tracking of continuous objects based on binary tree structured SVM for industrial wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 3, pp. 849–861, Mar. 2022.

[17] L. Liu, G. Han, Z. Xu, L. Shu, M. Martínez-García, and B. Peng, "Predictive boundary tracking based on motion behavior learning for continuous objects in industrial wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 9, pp. 3239–3249, Sep. 2022.

[18] J. Ning et al., "Malware traffic classification using domain adaptation and ladder network for secure industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17058–17069, Sep. 2022.

[19] G. Gui, F. Liu, J. Sun, J. Yang, Z. Zhou, and D. Zhao, "Flight delay prediction based on aviation big data and machine learning," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 140–150, Jan. 2020.

[20] Z. Gao, Y. Gao, S. Wang, D. Li, and Y. Xu, "CRISLoc: Reconstructable CSI fingerprinting for indoor smartphone localization," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3422–3437, Mar. 2021.

[21] Y. Lin, Y. Tu, Z. Dou, L. Chen, and S. Mao, "Contour stella image and deep learning for signal recognition in the physical layer," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 1, pp. 34–46, Mar. 2021.

[22] P. Yin, L. Peng, J. Zhang, M. Liu, H. Fu, and A. Hu, "LTE device identification based on RF fingerprint with multi-channel convolutional neural network," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

[23] H. Li, Y. Liao, W. Wang, J. Hui, J. Liu, and X. Liu, "A novel time-domain graph tensor attention network for specific emitter identification," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–14, 2023.

[24] Y. Peng et al., "Supervised contrastive learning for RFF identification with limited samples," *IEEE Internet Things J.*, vol. 10, no. 19, pp. 17293–17306, Oct. 2023.

[25] Z. Yao et al., "Few-shot specific emitter identification using asymmetric masked auto-encoder," *IEEE Commun. Lett.*, vol. 27, no. 10, pp. 2657–2661, Oct. 2023.

[26] Y. Zhang, C. Jiang, B. Yue, J. Wan, and M. Guizani, "Information fusion for edge intelligence: A survey," *Inf. Fusion*, vol. 81, pp. 171–186, May 2022.

[27] W. Lu, C. Tao, H. Li, J. Qi, and Y. Li, "A unified deep learning framework for urban functional zone extraction based on multi-source heterogeneous data," *Remote Sens. Environ.*, vol. 270, Mar. 2022, Art. no. 112830.

[28] X. Wang, D. Bo, C. Shi, S. Fan, Y. Ye, and P. S. Yu, "A survey on heterogeneous graph embedding: Methods, techniques, applications and sources," *IEEE Trans. Big Data*, vol. 9, no. 2, pp. 415–436, Apr. 2023.

[29] G. Han, Z. Xu, H. Zhu, Y. Ge, and J. Peng, "A two-stage model based on a complex-valued separate residual network for cross-domain IIoT devices identification," *IEEE Trans. Ind. Informat.*, early access, Jul. 26, 2023, doi: 10.1109/TII.2023.3296871.

[30] P. Deng, S. Hong, J. Qi, L. Wang, and H. Sun, "A lightweight transformer-based approach of specific emitter identification for the automatic identification system," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2303–2317, 2023.

[31] M. Hua et al., "Specific emitter identification using adaptive signal feature embedded knowledge graph," *IEEE Internet Things J.*, early access, Aug. 1, 2023, doi: 10.1109/JIOT.2023.3300689.

[32] Z. Xu, G. Han, L. Liu, H. Zhu, and J. Peng, "A lightweight specific emitter identification model for IIoT devices based on adaptive broad learning," *IEEE Trans. Ind. Informat.*, vol. 19, no. 5, pp. 7066–7075, May 2023.

[33] Y. Zhang, Y. Peng, J. Sun, G. Gui, Y. Lin, and S. Mao, "GPU-free specific emitter identification using signal feature embedded broad learning," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 13028–13039, Jul. 2023.

[34] J. E. Engelen and H. Hoos, "A survey on semi-supervised learning," *Mach. Learn.*, vol. 109, pp. 373–440, Feb. 2020.

[35] X. Yang, Z. Song, I. King, and Z. Xu, "A survey on deep semi-supervised learning," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 9, pp. 8934–8954, Sep. 2023.

[36] Z. Wu, F. Wang, and B. He, "Specific emitter identification via contrastive learning," *IEEE Commun. Lett.*, vol. 27, no. 4, pp. 1160–1164, Apr. 2023.

[37] X. Fu et al., "Semi-supervised specific emitter identification method using metric-adversarial training," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10778–10789, Jun. 2023.

[38] C. Liu et al., "Overcoming data limitations: A few-shot specific emitter identification method using self-supervised learning and adversarial augmentation," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 500–513, 2024.

[39] K. Tan, W. Yan, L. Zhang, Q. Ling, and C. Xu, "Semi-supervised specific emitter identification based on bispectrum feature extraction CGAN in multiple communication scenarios," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 1, pp. 292–310, Feb. 2023.

[40] Z.-H. Zhou, "Open-environment machine learning," *Nat. Sci. Rev.*, vol. 9, no. 8, pp. 1–11, Aug. 2022.

[41] A. Gupta, S. Narayan, K. J. Joseph, S. Khan, F. S. Khan, and M. Shah, "OW-DETR: Open-world detection transformer," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 9225–9234.

[42] T. G. Dietterich and A. Guyer, "The familiarity hypothesis: Explaining the behavior of deep open set methods," *Pattern Recognit.*, vol. 132, Dec. 2022, Art. no. 108931.

[43] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, and J. Yu, "A robust radio-frequency fingerprint extraction scheme for practical device recognition," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11276–11289, Jul. 2021.

[44] Y. Dong, X. Jiang, H. Zhou, Y. Lin, and Q. Shi, "SR2CNN: Zero-shot learning for signal recognition," *IEEE Trans. Signal Process.*, vol. 69, pp. 2316–2329, 2021.

[45] R. Xie et al., "A generalizable model-and-data driven approach for open-set RFF authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4435–4450, 2021.

[46] W. Wang and M. Zhang, "Tensor deep learning model for heterogeneous data fusion in Internet of Things," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 4, no. 1, pp. 32–41, Feb. 2020.

[47] T. Gao, H. Chen, and W. Chen, "Adaptive heterogeneous support tensor machine: An extended STM for object recognition using an arbitrary combination of multisource heterogeneous remote sensing data," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, 2022, Art. no. 3113784.

[48] H. Lang, G. Yang, C. Li, and J. Xu, "Multisource heterogeneous transfer learning via feature augmentation for ship classification in SAR imagery," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, 2022, Art. no. 3178703.

[49] J. Wang, Y. Zhang, L. Wang, Y. Hu, X. Piao, and B. Yin, "Multitask hypergraph convolutional networks: A heterogeneous traffic prediction framework," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18557–18567, Oct. 2022.

[50] S. Fang, C. Zhang, S. Xiang, and C. Pan, "AutoMSNet: Multi-source spatio-temporal network via automatic neural architecture search for traffic flow prediction," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 2827–2841, Mar. 2023.

[51] Y. Dai, F. Gieseke, S. Oehmcke, Y. Wu, and K. Barnard, "Attentional feature fusion," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Jan. 2021, pp. 3559–3568.

[52] S. Zhang et al., "A real-world radio frequency signal dataset based on LTE system and variable channels," 2022, *arXiv:2205.12577*.

Yibin Zhang (Graduate Student Member, IEEE) received the B.S. degree in communication engineering from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2020, where he is currently pursuing the Ph.D. degree. His research interests include specific emitter identification, the Industrial Internet of Things, broad learning, deep learning, and the corresponding application in wireless communications.

Qianyun Zhang (Member, IEEE) received the B.Sc. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2014, and the Ph.D. degree from the Queen Mary University of London, U.K., in 2018. She is currently an Associate Professor with the School of Cyber Science and Technology, Beihang University, Beijing. Her current research interest includes wireless network security, intelligent sensing, and recognition.

Haitao Zhao (Senior Member, IEEE) received the M.S. and Ph.D. degrees (Hons.) in signal and information processing from the Nanjing University of Posts and Telecommunications (NJUPT), Nanjing, China, in 2008 and 2011, respectively. He is currently a Professor with NJUPT. His research interests include wireless multimedia modeling, capacity prediction, and wireless network coding.

Yun Lin (Senior Member, IEEE) received the B.S. degree in electrical engineering from Dalian Maritime University, Dalian, China, in 2003, the M.S. degree in communication and information systems from the Harbin Institute of Technology, Harbin, China, in 2005, and the Ph.D. degree in communication and information systems from Harbin Engineering University, Harbin, in 2010. From 2014 to 2015, he was a Research Scholar with Wright State University, Dayton, OH, USA. He is currently a Full Professor with the College of Information and Communication Engineering, Harbin Engineering University. He has authored or coauthored more than 200 international peer-reviewed journal/conference papers, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, TR, INFOCOM, GLOBECOM, ICC, VTC, and ICNC. His current research interests include machine learning and data analytics over wireless networks, signal processing and analysis, cognitive radio and software-defined radio, artificial intelligence, and pattern recognition.

Guan Gui (Fellow, IEEE) received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2012.

From 2009 to 2014, he joined Tohoku University as a Research Assistant and a Post-Doctoral Research Fellow. From 2014 to 2015, he was an Assistant Professor with Akita Prefectural University, Akita, Japan. Since 2015, he has been a Professor with the Nanjing University of Posts and Telecommunications, Nanjing, China. He has published more than 200 IEEE journals/conference papers. His recent research interests include intelligence sensing and recognition, intelligent signal processing, and physical layer security.

Dr. Gui contributions to intelligent signal analysis and wireless resource optimization have earned him the title of fellow of the IEEE, IET, and AAIA. He was a recipient of several Best Paper Awards, such as ICC 2017, ICC 2014, and VTC 2014-Spring. He received the IEEE Communications Society Heinrich Hertz Award in 2021, top 2% scientists of the world by Stanford University from 2021 to 2023, the Clarivate Analytics Highly Cited Researcher in Cross-Field from 2021 to 2023, the Highly Cited Chinese Researchers by Elsevier from 2020 to 2023, a member and Global Activities Contributions Award in 2018, the Top Editor Award of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2019, the Outstanding Journal Service Award of *KSII Transactions on Internet and Information System* in 2020, the Exemplary Reviewer Award of IEEE COMMUNICATIONS LETTERS in 2017, the 2012 Japan Society for Promotion of Science (JSPS) Postdoctoral Fellowships for Foreign Researchers, and the 2018 Japan Society for Promotion of Science (JSPS) International Fellowships for Overseas Researchers. He was also selected as the Jiangsu Specially-Appointed Professor in 2016, the Jiangsu High-Level Innovation and Entrepreneurial Talent in 2016, and the Jiangsu Six Top Talent in 2018. Since 2022, he has been a Distinguished Lecturer of the IEEE Vehicular Technology Society. He is serving or served on the editorial boards of several journals, including IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *IEICE Transactions on Communications*, *Physical Communication*, *Wireless Networks*, IEEE ACCESS, *Journal of Circuits, Systems and Computers*, *Security and Communication Networks*, *IEICE Communications Express*, and *KSII Transactions on Internet and Information Systems*, and *Journal on Communications*. In addition, he served as the IEEE VTS Ad Hoc Committee Member in AI Wireless; the Executive Chair of IEEE ICCT 2023; the Workshop Chair of LANTINCOM2023; the TPC Chair of PRAI 2022, ICGIP 2022, PHM 2021, and WiMob 2020; the Executive Chair of VTC 2021-Fall; the Vice Chair of WCNC 2021; the Symposium Chair of WCSP 2021; the General Co-Chair of Mobimedia 2020; the Track Chairs of EuCNC 2021 and 2022, and VTC 2020 Spring; the Award Chair of PIMRC 2019; and a TPC Member of many IEEE international conferences, such as GLOBECOM, ICC, WCNC, PIRMC, VTC, and SPAWC.

Hikmet Sari (Life Fellow, IEEE) received the Engineering, Diploma, and Ph.D. degrees from ENST, Paris, France, and the Habilitation degree from the University of Paris—XI. From 1980 to 2002, he held various research and management positions at Philips Research Laboratories, SAT, Alcatel, Pacific Broadband Communications, and Juniper Networks. From 2003 to 2016, he was a Professor and the Head of the Telecommunications Department, Suplec, and the Chief Scientist at Sequans Communications. He is currently a Professor with the Nanjing University of Posts and Telecommunications (NJUPT). He was a member of the IEEE Fellow Evaluation Committee from 2002 to 2007 and the IEEE Awards Committee from 2005 to 2007. He was a recipient of the Andre Blondel Medal in 1995, the Edwin H. Armstrong Achievement Award in 2003, the Harold Sobol Award in 2012, as well as election to the Academia Europaea (Academy of Europe), and the Science Academy of Turkey in 2012. He was the Chair of the Communication Theory Symposium of ICC 2002; the Technical Program Chair of ICC 2004 and EuCNC 2015; the Vice General Chair of ICC 2006; the General Chair of PIMRC 2010, WCNC 2012, and ICUWB 2014; an Executive Chair of WCNC 2014 and ICC 2017; the General Co-Chair of IEEE BlackSeaCom 2015, ATC 2016, ATC 2018, and PIMRC 2019; and an Executive Co-Chair of ICC 2016. He also chaired the Globecom and the ICC Technical Content (GITC) Committee from 2010 to 2011. He was the Communications Society (ComSoc) Vice President for Conferences from 2014 to 2015, the Director for Conference Operations of ComSoc from 2018 to 2019, and the Vice President for Conferences of the IEEE France Section from 2017 to 2019. He is currently serving as a General Chair for WCNC 2021 and an Executive Co-Chair for GLOBECOM 2023. He served as the Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS from 1987 to 1991; an Associate Editor for the IEEE COMMUNICATIONS LETTERS from 1999 to 2002; and a Guest Editor for several special issues of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, *European Transactions on Telecommunications* (ETT), and other journals. He served as a Distinguished Lecturer for ComSoc from 2001 to 2006.