electronics

MDPI

Article

A Knowledge Inference and Sharing-Based Open-Set Device Recognition Approach for Satellite-Terrestrial-Integrated IoT

Ying Yang * and Lidong Zhu

National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China
* Correspondence: yangying914@163.com

Abstract: Satellite-terrestrial-integrated internet of things (IoT) is an inevitable trend in future development, but open satellite link and massive IoT device access will bring serious security risks. However, most existing recognition models are unable to discover and reject malicious IoT devices since they lack the decision information of these unauthorized devices during training. To address this dilemma, this paper proposes a knowledge inference and sharing-based open-set recognition approach to protect satellite-terrestrial-integrated IoT. It proceeds in two steps. First, knowledge inference, where we construct ideal substitutes for unauthorized devices after reasonable inference on the training set, aims to compensate the model's missing decision information. Second, knowledge sharing, where we inherit the existing knowledge and modify the model's decision boundaries through model expansion and knowledge distillation, achieves accurate open-set recognition. Experiments on the ORACLE dataset demonstrated that our approach outperforms other state-of-the-art OSR methods in terms of accuracy and running time. In short, our approach has excellent performance while only slightly increasing computational complexity.

Keywords: satellite-terrestrial-integrated internet of things (IoT); IoT device recognition; open-set recognition; knowledge inference; model expansion

Citation: Yang, Y.; Zhu, L. A Knowledge Inference and Sharing-Based Open-Set Device Recognition Approach for Satellite–Terrestrial-Integrated IoT. *Electronics* **2023**, *12*, 1143. https://doi.org/10.3390/electronics12051143

Academic Editor: Qinghe Du

Received: 10 November 2022
Revised: 14 February 2023
Accepted: 20 February 2023
Published: 27 February 2023

1. Introduction

The rapid development of the internet of things (IoT) technologies has triggered an explosive growth of IoT device access. A report from Cisco showed that there will be around 500 billion IoT devices connected to the Internet by 2030 [1]. Obviously, satellite-terrestrial-integrated IoT is a trend in the future development of communication networks, which can provide global massive devices with low-cost access. However, maintaining its security is difficult due to open satellite links, massive connected devices, and complex IoT application environments [2]. The existence of malicious unauthorized devices, in particular, is a major hidden danger.

Each IoT device has unique hardware imperfection, which is caused by device-specific variations such as IQ imbalance, nonlinear distortion, and phase noise. These imperfections combine to form wireless device signatures, known as RF fingerprints, which serve as the basis for a recognition model to identify different device identities. An ideal recognition model should automatically extract fingerprint features of different devices and accurately recognize them. However, most models are mistaken unauthorized devices for authorized ones, since the training set used for model training has no information about unauthorized devices. To address this dilemma, this paper focuses on the open-set recognition (OSR) for IoT device in satellite-terrestrial-integrated IoT.

To date, many OSR approaches have been proposed to deal with unknown data recognition or outlier detection. Clearly, they can be used to solve our problem. OSR approaches can be divided into discriminative-based OSR and generative-based OSR. Openmax [3] is a popular discriminative-based OSR approaches in which Bendale et al.

replaced the Softmax layer in the neural network with the Openmax layer to correct test sample scores and set a distance threshold to detect outliers. Guo et al. [4] then combined center loss and the Openmax model to detect unauthorized devices. The above approaches have been demonstrated to successfully perform OSR tasks, but their performance is heavily dependent on the decision threshold, which requires a significant amount of computational resources to tune.

Differ from the discriminative-based OSR approaches, the generative-based OSR approaches transform this problem into a simpler $K + 1$ class closed-set classification problem, where K is the number of known classes (authorized devices). Based on this notion, Samer Hanna et al. utilized a set of known signals as substitutes to participate in model training. Then, the trained model created boundaries around known distributions to reject unknown signals [5]. Patrick Schlachter et al. split the known class data in the training set into typical and atypical subsets. The atypical subset was regarded as substitutes for unknown class data for model training to solve the OSR problem [6], whereas this simple replacement tends to increase additional open risk in the recognition model, since the distributions of known and unknown classes overlap. Recently, ref. [7] synthesized signals via a generation model to augment the training set of RF transmitters, this way has been shown to improve the classifier's recognition accuracy. However, the generation model cannot guarantee the quality of the synthetic samples while it consumes a lot of computational resources. Moreover, these synthetic samples need to be screened before being used to recognition model. This is not an easy way.

In this paper, a knowledge inference and sharing-based OSR approach is proposed to maintain the security of satellite–terrestrial-integrated IoT. Specifically, in the first step, we provide the lacking information of unauthorized devices to the recognition model by constructing synthetic substitutes after making reasonable inference on the training set. In the second step, we help the model inhert the learned knowledge and infer correct decision boundaries by model expansion and knowledge distillation. Therefore, our approach is able to both accurately identify authorized devices and effectively discover unauthorized malicious devices, as described in Section 3. Simulation results show that the recognition accuracy of our approach is better than that of the state-of-the-art OSR methods by 7.7%, while the running time is the least. The overall performance of our approach is verified to be superior to other four state-of-the-art OSR methods.

The rest of this paper is organized as follows. Section 2 introduces the related work. Section 3 presents the method framework based on the problem analysis and introduces the components of the model architecture in detail. The ablation experiments and performance simulations of our proposed approach on the public dataset ORACLE are presented in Section 4. Finally, Section 5 gives the conclusions.

2. Related Work

2.1. Open-Set Recognition

The researches that are closely related to the open-set recognition task are outlier detection [7,8], anomaly detection [9,10], or out-of-distribution detection [11]. These problems assumed that the training set cannot obtain any samples or information of unknown classes. As a result, many OSR methods [3,12,13] proposed to first train a perfect closed-set model on the trainning set, and then search for an optimal decision threshold based on the validation set, and finally use the trained model for open-set data recognition. Similar to our basic idea, some other works [14–16] trained one or more closed-set models with the virtual examples created during model training, oftentimes sacrificing the recognition performance on the known classes. However, most of them do not consider to alleviate this performance degradation phenomenon of open-set models. Motivated by the previous work of Li et al. [17], we found that model architecture expansion and fine-tuning training were the main causes of this problem. In our approach, knowledge distillation [18] is introduced to improve the model's recognition performance for known classes. It corrects the model decision boundaries by transferring the knowledge learned from a pre-trained

closed-set model to the open-set model. In this paper, we show that the performance of our approach is significantly better than other state-of-the-art OSR methods.

2.2. Knowledge Distillation

Knowledge distillation is a transfer learning method, which is first proposed by Hinton et al. in [18]. Its purpose is to transfer the knowledge learned in the teacher network (complex architecture but high accuracy) to the student network (compact architecture but easy to deploy) and help the student network converge faster. In brief, the knowledge distillation loss (KD loss) is an improved cross-entropy loss function (see Equation (7)), and it encourages the student network to produce similar responses to the teacher network by modeling the output of the original network when adapting to different tasks. Therefore, the KD loss is widely used to generate networks that approximate the original network but have different structures. After that, we note that Li et al. introduced KD loss in the related research of incremental learning [17], which effectively alleviates the sequelae caused by the change of model architecture, that is, the updated model forgets the knowledge learned on the old class data. Inspired by this, our approach uses KD loss for knowledge sharing between the original closed-set model and the expanded model. This is proved to help our recognition model learn and correct decision boundaries between authorized and unauthorized devices in the open-set recognition task.

3. Our Approach

In this section, we first propose the system model for open-set device recognition. Then, we introduce the problem analysis of wireless IoT device recognition under open-set scenarios. Finally, we describe the model architecture and implementation process of our approach.

3.1. System Model

For the application of satellite-terrestrial-integrated internet of things, we propose a simple system model for open-set IoT device recognition, as shown in Figure 1. In the system model, it is assumed that the ground receiver performs open-set recognition on the signals of all the received IoT devices in advance to determine whether there are malicious unauthorized devices in the current system. When the satellite moves into the coverage area of the ground receiver, the receiver transmits the IoT device recognition results in the area back to the satellite, providing the basis for the satellite to receive the securely authorized signals.

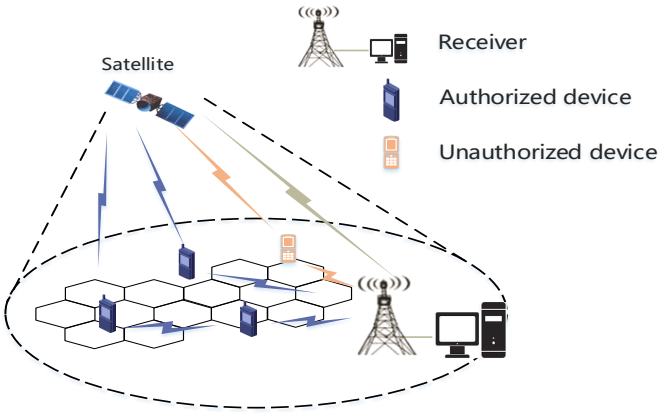


Figure 1. A simple diagram of the system model of open-set IoT device recognition for satellite-terrestrial-integrated internet of things.

3.2. Problem Analysis

In this paper, we assume that the original signal dataset of authorized devices is a set $D_a = \{(r_i(t), l_i)\}_{i=1}^{n}$ with K authorized classes and n signal samples, where its label

$l_i \in \{1, \ldots, K\}$. Similarly, the signal dataset of unauthorized devices is a set $D_u = \{r_i(t)\}_{i=n+1}^{m}$ without labels, its class number and sample number are unknown. According to [19–21], the original signal sequence $r(t)$ of a wireless IoT device is formalized as follows:

$$r(t) = s(t) * c(t) + n(t) \tag{1}$$

where, $s(t)$ is the transmitted time series signal, $c(t)$ is the impulse response of the transmission channel, $n(t)$ is the Additive White Gaussian Noise (AWGN), and $r(t)$ represents the split IQ signal sample of a wireless IoT device.

The open-set IoT device recognition task, similar to the traditional closed-set classification task, can be viewed as a $K + 1$ class decision problem, where K is the number of authorized devices and all unauthorized devices correspond to the class $K + 1$. Most signal recognition models cannot deal with the OSR problem since they lack decision information of unauthorized classes. Our approch is proposed to solve the open-set recognition problem of wireless IoT device. It provides the model's missing information of unauthorized devices to improve the recognition performance by constructing virtual knowledge as substitutes for unauthorized devices. Then, the basic recognition model is expended by adding an output neuron for unauthorized devices to dynamically learn the decision boundaries. Third, these decision boundaries are modified by using knowledge distillation, which can reduce the interference caused by model expansion and virtual knowledge.

3.3. Model Architecture

As shown in Figure 2, the model architectire of our approach consists of three parts: a virtual knowledge inference module, a feature extraction module, and a knowledge sharing module. Each component is described in detail below.

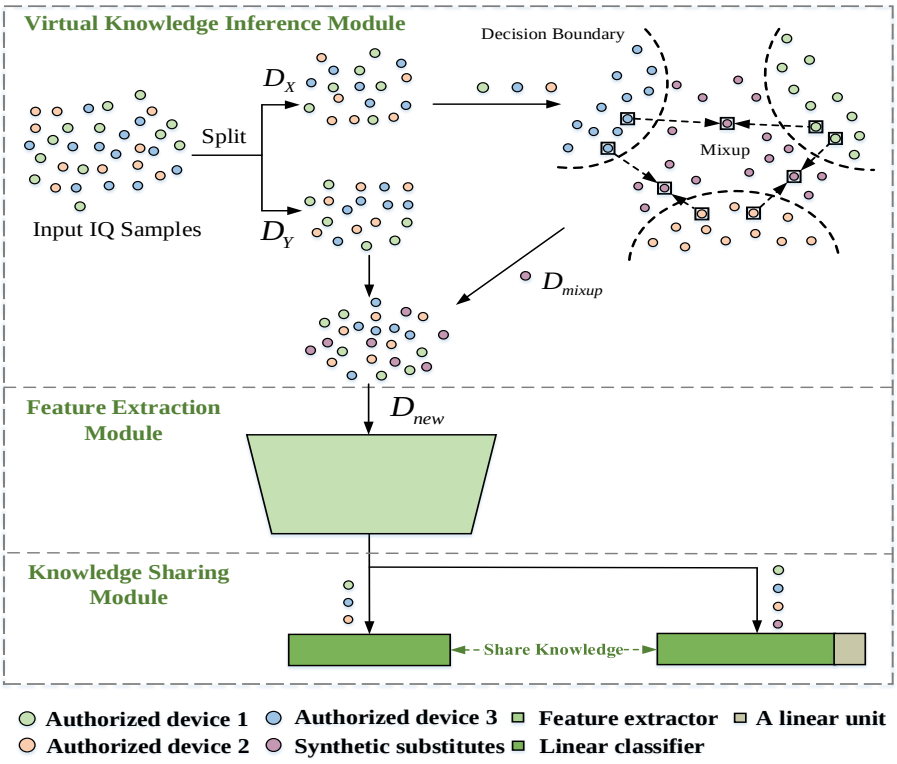


Figure 2. The schematic diagram of the knowledge inference and sharing-based open-set device recognition approach.

3.3.1. Virtual Knowledge Inference Module

It aims to use virtual knowledge to construct substitutes for unauthorized devices to offer the model's lack of decision information. Follow [16], these substitutes should have two main characteristics: i.e., their distribution seems novel, and the generation process should be fast. Despite the GAN-based sample generative methods [22,23] can generate such data, training them is difficult. To this end, we make a reasonable knowledge inference on the raw signals of authorized devices and construct the ideal substitutes for unauthorized ones by using mixup operations [24]. Mixup is a simple data augmentation method without consuming additional computing resources. In this module, we select two signal samples of different wireless IoT devices and mix them up in the original signal space.

$$\begin{cases} \tilde{r}_i = \alpha r_i + (1-\alpha) r_j \\ \tilde{l}_i = \alpha l_i + (1-\alpha) l_j \end{cases}, \alpha \sim Beta(\beta, \beta) \tag{2}$$

where, (r_i, l_i) and (r_j, l_j) are two signal samples from different authorized devices, $\tilde{r}_i$ is the synthetic substitute created by inferring the knowledge of two signals from different authorized devices, $l_i \neq l_j$. α is a mixup parameter, $\alpha \in [0, 1]$, and its value obeys the *Beta* distribution, $\beta = 0.2$.

These synthetic substitutes frequently occupy the low-confidence regions of the feature space where real unauthorized classes located. As a result, they are similar to but different from the signal samples in the training set, and they meet the requirements proposed by [16]. In this section, these substitutes are used to augment the subset of the original training set D_a, and their labels are forced to be a constant $K + 1$, where K is the number of authorized devices. In Algorithm 1, we provide the detailed pseudo-code of the virtual knowledge inference alogrithm.

Algorithm 1 Virtual Knowledge Inference

Input: training set $D_a = \{(r_i, l_i)\}_{i=1}^{n}$, and $l_i \in \{1, \ldots, K\}$;
Output: new training set $D_{new} = \{(r_i^*, l_i^*)\}_{i=1}^{n}$, and $l_i^* \in \{1, \ldots, K+1\}$;
1: $D_X = \{(r_i, l_i)\}_{i=1}^{n/2}, D_Y = \{(r_i, l_i)\}_{i=n/2}^{n}$;
2: **for** $i = 1: n/2$ **do**
3: $\quad \tilde{r}_i = \alpha \cdot r_i + (1-\alpha) \cdot r_j, l_i \neq l_j, \alpha \sim Beta(\beta, \beta)$;
4: $\quad \tilde{l}_i = K + 1$;
5: **end for**
6: $D_{mixup} = \{(\tilde{r}_i, \tilde{l}_i)\}_{i=1}^{n/2}$;
7: $D_{new} = \{D_{mixup} \cup D_Y\}_{shuffle}$.

The Algorithm 1 includes three steps. In the first step, a minibatch training set D_a contains the authorized IoT device signals are split into two subsets D_X and D_Y, each has half samples, see line 1. The second step performs virtual knowledge inference on the subset D_X, we can obtain a synthetic substitute set D_{mixup} by adopting the mixup operation, and its corresponding label is set to $K + 1$, see from line 2 to line 6. In the third step, the minibatch subset D_Y is augmented by adding the D_{mixup} and then shuffled, see line 7. The new training set D_{new} can provide the model's missing decision information of unauthorized IoT devices to improve the recognition performance.

3.3.2. Feature Extraction Module

Its task is to map the augmented training set D_{new} in original space into a compact RF fingerprint feature set. These fingerprint features provide discriminative information to the subsequent knowledge sharing module, they are critical in determining the model performance, and even outperforming human-engineered features [25,26].

Generally, feature extraction gets latent features for the input data through a pre-trained deep CNN, and the extracted features are the activation vectors of one layer (the last layer) or multiple layers of the given data. In this paper, considering the input data

form of the signal differs greatly from that of an image, the feature extraction network we used is primarily for fingerprint feature extraction of IoT device signals. The deep CNN model proposed in [19] (see Table 1) inspired the basic network architecture of our feature extraction module, which consists of two convolutional layers and two fully connected layers. This model architecture has been used in many applications and achieved excellent results. For example, Malte Schmidt et al. [27] used this CNN model to identify 15 classes of wireless interference in the 2.4 GHZ ISM frequency band. When the SNR > −5 dB, its recognition accuracy reaches 95%; Furthermore, Merima Kulin et al. [28] used this CNN model to identify wireless signals in spectrum monitoring tasks. When SNR > 5 dB, the recognition accuracy reaches more than 98%.

Table 1. The network parameters of the CNN model [19] and our model.

Layer	Number of Filters	Filter	Stride	Activation Function	Other Parameters	Output
Conv1	256	(1, 3)	(1, 1)	ReLu	Batch Normalization, Padding = (0, 0)	(N, 256, 2, 126)
Conv2	80	(2, 3)	(1, 1)	ReLu	Padding = (0, 0)	(N, 80, 2, 124)
Layer	**Number of Units**	**Bias**		**Activation Function**	**Other Parameters**	**Output**
FC1	256	True		ReLu	dropout = 0.6	(N, 256)
FC2 (CNN [19])	K	True		Softmax	-	(N, K)
FC2 (Ours)	$K+1$	True		Softmax	-	(N, $K+1$)

In our feature extraction module, the time-domain IQ signals of the model input are first passed through 256 and 80 filters of convolutional layers to extract latent feature maps from various channels. At the end of each convolutional layer, a batch normalization and ReLu activate function is added to improve the stability and nonlinearity of the output features. These feature maps are then compressed into a one-dimensional feature vector before being fed into two fully connected layers of 256 neurons and $K+1$ neurons to generate the RF fingerprint features for signal label prediction, where K is the number of authorized classes. More details are shown in Table 1 and Figure 3.

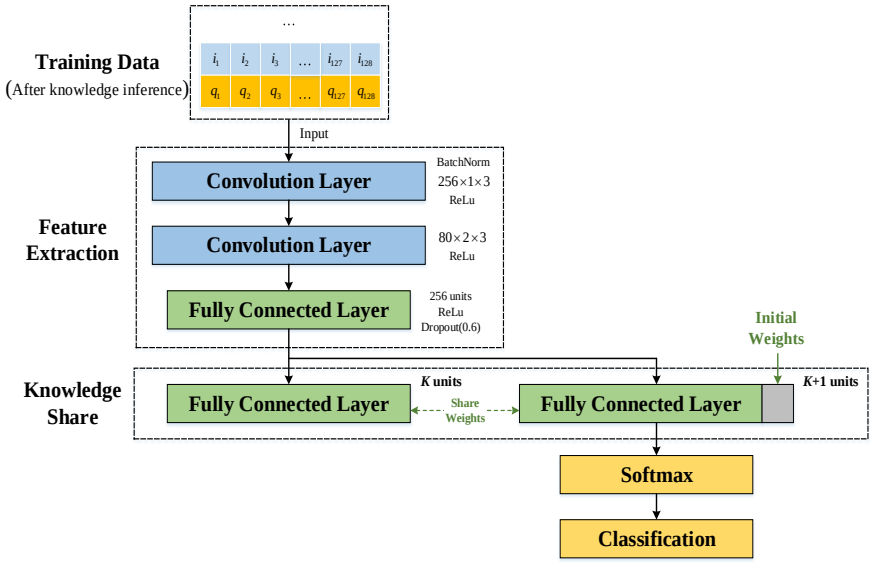


Figure 3. The model structure of the knowledge inference and sharing-based open-set device recognition approach.

We hope that the extracted fingerprint features have the characteristics of short intra-class distances and long inter-class distances. Since the more compact the latent space of fingerprint features of authorized devices, the more space reserved for that of unauthorized devices, which helps to improve the model performance for identifying unauthorized

devices. Many works based on metric learning can assist us to obtain features with the above desired compact attributes. For example, Wen et al. [29] proposed center loss function which is a penalty on the distance between latent feature vector and the class center, and pushed the same class of feature and its class centers together. This way avoids the complicated sample pair construction process. Similar work include constrained center loss [30] and II-loss [31]. These methods enhance the decision boundary constraint for feature space by adding a penalty term to the loss function, and to compress the intra-class distribution of authorized classes. In this paper, the center loss is used to improve the objective function of feature extraction module, and its definition is provided in [29].

$$L_{center}(\theta, \theta_K; r(t)) = \frac{1}{2n} \sum_{i=1}^{n} ||f_{\theta_K}(\varphi_\theta(r_i(t))) - c_{l_i}||_2^2 \tag{3}$$

where, $f_{\theta_K}(\cdot)$ is map function of the K-class classifier with the parameter θ_K, $\varphi_\theta(\cdot)$ is the map function of the feature extraction module, and θ is the model parameters. $r_i(t)$ is the i-th original signal in the new training set D_{new}, $f_{\theta_K}(\varphi_\theta(r_i(t)))$ represents the corresponding output feature vector without passing through the softmax layer, c_{l_i} is the class center of the class to which label l_i belongs, and n is the number of signals.

Therefore, the optimization function used to train this feature extraction module has two components: softmax loss and center loss. The former is intended to quantify the degree of deviation between the feature extraction network's predicted values and the ground truth. The latter is used to tighten the intra-class features. In this module, its training purpose is to minimize this optimization function.

$$L_{ext}(\theta, \theta_K; r(t)) = L_{soft}(\theta, \theta_K; r(t)) + \eta L_{center}(\theta, \theta_K; r(t)) \tag{4}$$

where, θ and θ_K are the model parameters of the feature extraction module and the K-class linear classifier, respectively. Furthermore, η is the penalty parameters of the center loss function.

3.3.3. Knowledge Sharing Module

It aims to share the knowledge learned from a pre-trained K class model with the expanded model via knowledge distillation technology, so as to correct decision boundaries and achieve open-set recognition. In this module, the K shared output units and the new adding output unit assign each input fingerprint feature $K + 1$ category probability scores.

Specifically, most closed-set recognition models use only K output units to predict K authorized classes and all unknown unauthorized classes, which will inevitably lead to misjudgment. Their output layers lack a unit for predicting the probability score of unauthorized classes. Therefore, this paper shares the existing K output units and expands the recognition model with an additional output unit to output the model's prediction scores for RF fingerprint features of unauthorized devices. The model parameters are then fine-tuned for the open-set recognition of IoT devices.

$$f_{\theta_{K+1}}(z_i) = [f_{\theta_K}(z_i), f_{\theta*}(z_i)], z_i = \varphi_\theta(r_i(t)) \tag{5}$$

where $\theta*$ and θ_K are the model parameters corresponding to the additional output unit and the K shared output units in the extended model $f_{\theta_{K+1}}(\cdot)$ with parameter θ_{K+1}, $\theta_{K+1} = [\theta_K, \theta*]$, and z_i represents the fingerprint feature generated from the i-th input signal $r_i(t)$ passes through the feature extraction module $\varphi_\theta(\cdot)$.

Model fine-tune is a transfer learning method that modifies the pre-trained model parameters to train it for a new task. According to the simulation results, the fine-tuned model often outperforms feature extraction [32,33] or networks learned from random initializations [34]. In this paper, our approach fine-tunes both the feature extractor parameters (θ) and the output parameters (θ_{K+1}), enabling the recognition model to better distinguish between authorized and unauthorized devices. However, the research by Li et al. [17] informed us that training for fine-tuning after the model architecture is expanded causes

the model to gradually forget what it has learnt, i.e., the model's performance in identifying authorized devices degrades. We use the knowledge distillation loss (KD loss) to correct the model decision boundaries, which can transfer the knowledge learned by the pre-trained closed-set model with K output units to our expanded model with the K shared output units and a new adding output unit, thereby alleviating the catastrophic forgetting phenomenon. In summary, the overall optimization of our open-set recognition model framework considers the following objective function.

$$L(\theta, \theta_{K+1}; r(t)) = L_{soft}(\theta, \theta_{K+1}; r(t)) + \mu L_{KD}(\theta, \theta_K, \theta_{K+1}; r(t)) \tag{6}$$

where θ, θ_K, and θ_{K+1} are the model parameters of the feature extractor, the K shared output units, and the $K+1$ output units consists of θ_K and a new adding unit $\theta*$, respectively, and μ is the penalty parameters of the KD loss function.

The KD loss [18] is aims to make the output probability of each authorized signal close to the output probability recorded by the pre-trained closed-set model, which is a modified cross-entropy loss with the addition of weights corresponding to small probability values.

$$L_{KD} = -\frac{1}{K}\sum_{i=1}^{K} q_i^* \cdot \log p_i^* \tag{7}$$

and the q_i^* and p_i^* are the modified versions of probabilities,

$$q_i^* = \frac{(q_i/T)}{\sum_j q_j/T}, p_i^* = \frac{(p_i/T)}{\sum_j p_j/T} \tag{8}$$

where K is the number of authorized devices in the training set, the q_i and p_i represent the output probabilities of the pre-trained close-set model and the first K output probabilities of our expanded model, T is the temperature coefficient, and we set $T = 2$, this is in line with the author's suggestion in [18].

The knowledge sharing module of our approach is suitable for solving the open-set recognition problem of IoT devices for the following two reasons. First, it reserves a special output unit for unauthorized classes, allowing the model to learn the decision boundary between authorized and unauthorized classes adaptively without setting a judgment threshold. Second, it introduces KD loss to address the expanded model's issue of forgetting the knowledge learned from authorized classes. The subsequent experimental results show that our recognition framework is effective.

4. Experiments and Results

In this paper, we propose a knowledge inference and sharing-based OSR approach to solve the IoT device recognition problem of satellite-terrestrial-integrate IoT. It should perform well in the following scenario: given a fixed number of authorized devices, the recognition model can accurately identify authorized device signals and effectively detect unauthorized device signals. In this section, we need to verify the rationality of knowledge inference and knowledge sharing in solving the OSR problem for IoT devices. As a result, we first show the feature similarity between real unauthorized device signals and synthetic substitutes generated by the virtual knowledge inference module. Then, we demonstrate the performance improvement of the above two modules by ablation study. Furthermore, we evaluate that whether our approach has superior open-set recognition ability. Two experiments are designed to compare our approach and other four state-of-the-art OSR methods in terms of recognition performance and runtime. All simulation experiments use the ORACLE dataset [35]. The following describes the implementation process and the analysis of experimental results.

4.1. Dataset and Evaluation Metric

4.1.1. Dataset

In this paper, all experiments are carried on the ORACLE dataset [35] which is a large WiFi signal dataset for recognizing the bit-similar wireless IoT devices. In order to improve the identifiability of different devices, two forms of controlled impairments are added to the received complex IQ signal samples: I/Q imbalance and DC offset. The receiver SDRs capture WiFi signals from 16 bit-similar USRP X310 radios with a center frequency of 2.45 GHz at 5 MS/s sampling rate. Each transmitter collects more than 20 million complex IQ signal samples. We utilize a window with length 128 to segment the collected complex IQ samples into multiple subsequences to enhance the translational invariance of features. Each sample is used to come each complex value is represented as 2 real values for storage, so the data input dimension of the recognition model is 2*128, which has the same signal format as the public RML2016.10a dataset [19].

In this paper, we take the first 2000 subsequences of each IQ sample as the signal dataset samples to construct four subsets: the training subset d_{train}, the validation subset d_{valid1}, the validation subset d_{valid2} and the test subset d_{test}, with the proportions of 70%, 10%, 10%, and 10%. The subset d_{train} is used to build the training set for model pre-training and open-set fine-tuning, the subset d_{valid1} is used to build the validation set for model pre-training, and the subset d_{valid2} and d_{test} are used to build the validation set and test set for open-set model evaluation. Specifically, for an open-set device recognition problem with three authorized devices and one unauthorized device, we need a training set and a validation set to pre-train the K class close-set model (K = 3), where both sets are composed of the training subset d_{train} and the validation subset d_{valid1} of the three authorized classes, respectively. Then, we use the training set again to fine-tune our expanded model. Finally, we adopt an open validation set or a test set to evaluate our model, where both sets are composed of the validation subsets d_{valid2} and test subsets d_{test} of the three authorized classes and the one unauthorized class, respectively.

4.1.2. Evaluation Metric

The recognition accuracy is used as an important metric to evaluate different OSR methods. In closed-set scenarios, recognition accuracy is defined as the proportion of the number of correctly predicted samples to the total number of all samples. Further, the extension of recognition accuracy to open-set scenarios should consider the unknown class (the unauthorized device), and the OSR accuracy (ACC) can be written as follow [36]:

$$ACC = \frac{\sum_{i=1}^{K+1}(TP_i + TN_i) + TU}{\sum_{i=1}^{K}(TP_i + TN_i + FP_i + FN_i) + (TU + FU)} \tag{9}$$

where, K is the number of authorized devices in the training set. TP and TN represent the true positive and the true negative, FP and FN represent the false positive and false negative, TU and FU represent the true unknown and false unknown.

Moreover, the accuracy on known samples (AKS) is the proportion of the correctly classified number to the total number in authorized class samples, and the accuracy on unknown samples (AUS) is the proportion of the correctly classified number to the total number in unauthorized class samples in [13,37]. These two metrics are introduced to evaluate the model's recognition performance for authorized and unauthorized devices, respectively.

$$AKS = \frac{\sum_{i=0}^{K-1}(TP_i + TN_i)}{\sum_{i=0}^{K-1}(TP_i + TN_i + FP_i + FN_i)} \tag{10}$$

$$AUS = \frac{TU}{TU + FU} \tag{11}$$

In addition, the F1-score is presented by Sokolova and Lapalme in [38]. It represents a harmonic mean of precision P and recall R and often appears in related literatures as a performance evaluation metric of open-set recognition models. The definition is as follows.

$$F1 - score = 2 \times \frac{P \times R}{P + R} \tag{12}$$

where, $P = \frac{\sum_{i=0}^{K-1} TP_i}{\sum_{i=0}^{K-1} (TP_i + FP_i)}$, $R = \frac{\sum_{i=0}^{K-1} TP_i}{\sum_{i=0}^{K-1} (TP_i + FN_i)}$ in [36].

The open-set recognition performance of our approach is evaluated by calculating the above four parameters in later experiments: the average accuracy of known samples (AKS), the average accuracy of unknown samples (AUS), the average OSR accuracy (ACC), and the average F1-score [37]. AKS and AUS, respectively, represent the proportion of the correctly classified number to the total number in known class samples and in unknown class samples, which are used to evaluate the model's ability to recognize the authorized classes and the ability to discover the unauthorized classes. ACC shows the comprehensive recognition performance of the OSR method. F1-score represents a harmonic mean of precision and recall, which is the most important parameter for evaluating the overall performance of open-set recognition methods.

4.2. Implementation Details

Our approach's training process is divided into four stages to achieve stable results: (1) closed-set model pre-training, (2) synthetic substitutes construction based on existing knowledge inference, (3) training set augmentation and model architecture expansion, and (4) model open-set fine-tuning based on knowledge sharing. More specifically, in the first stage, the closed-set model (includes θ and θ_K) is pre-trained on the training set consisting of signals from K authorized devices. We do for 350 epochs utilizing the Adam optimizer with a learning rate of 0.001, the size of each minibatch is set to 64, and the penalty coefficient of center loss is 1.0. In the second stage, the virtual knowledge is constructed as substitutes for unauthorized device signals after making reasonable inferences on the training set, which can compensate for the model's missing information of unauthorized classes. In the third stage, these synthetic substitutes are used to augment the training set, and the model architecture is expanded by sharing K output units and adding an additional unit ($\theta_{K+1} = [\theta_K, \theta*]$). Finally, the expanded model is trained on the new training set for model fine-tuning and knowledge sharing in order to achieve IoT device recognition. In this stage, we set the batch_size is 64 and do for 600 epochs and the Adam optimizer is used with a learning rate of 0.001, then, saving optimal model parameters. In addition, we use the coefficient $\mu = 0.1$ of the KD loss to correct model decision boundaries, as shown in Table 2.

Table 2. The coefficient μ selection of the knowledge distillation loss.

μ	0.0	0.05	0.1	0.5
ACC	83.75%	88.00%	89.75%	86.50%

4.3. Ablation Study

In this paper, our approach makes two efforts to enhance the recognition performance of the model. One is knowledge inference, which constructs substitutes for unauthorized device signals after inferring on the training set, providing the model with the missing decision information. The second is knowledge sharing, which expands the model by reserving an output unit for unauthorized classes and introduces knowledge distillation for decision boundary correction, so that the model inherits learned knowledge and discovers

new knowledge. In the following, two experiments are performed to demonstrate the contribution of the above two improvements to the overall performance improvement. The first one shows the similarity between the constructed synthetic substitute and the real unauthorized device signals, as shown in Figure 4. The second one compares the change in model recognition performance by adding the synthetic substitutes and the KD loss function, respectively, as shown in Figure 5 and Table 3.

In the following two experiments, we set the first three devices in the ORACLE WiFi signal dataset as authorized classes D_a, and the fourth and fifth devices as unauthorized classes D_u. The dataset is set as follows: firstly, we get subset d_{train} and subset d_{valid1} from each of the authorized classes D_a to form the training set and valication set, and pre-train the three class closed-set model in advance. Secondly, we use the training set for model open-set fine-tuning. Finally, we get the subset d_{valid2} from each of the authorized classes D_a the subset d_{test} from each of the unauthorized classes D_u to make up the valication set and the test set for performance evaluation of our model. Other details are set as described in Sections 4.1 and 4.2.

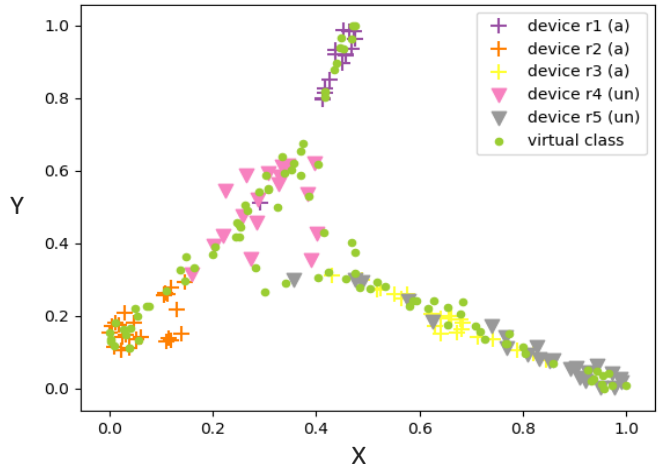
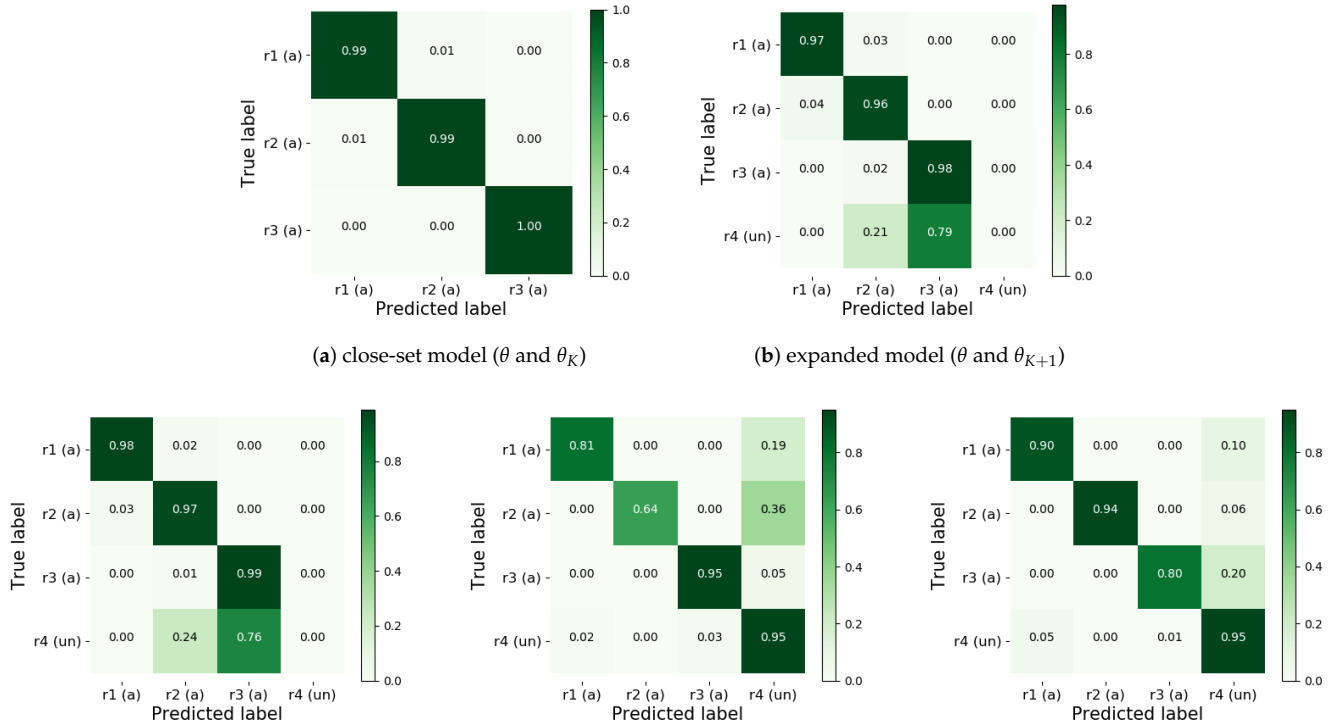


Figure 4. Comparison of constructed virtual substitutes with real unauthorized device signals. The plus sign, triangle and circle represent the extracted features of the authorized class (a), unauthorized class (un) and virtual class, respectively.

Most existing models are unable to solve the OSR problem since they lack the decision information of unauthorized devices. As a result, we propose the knowledge inference module to compensate for the lack of information. This module constructs virtual substitutes for unauthorized devices after making reasonable inference on the original training set. In the well-trained neural network, the feature representations of unauthorized classes are located in the low-confidence region near decision boundaries [16], so that of constructed substitutes should also appear in these feature space. In this section, we use the feature extraction module to map the original signals of authorized devices, unauthorized devices and constructed virtual classes into latent features, and then apply the t-SNE algorithm [39] to reduce the dimension of these features to two dimensions.

In Figure 4, we show the latent feature distribution of virtual substitutes and real unauthorized device signals. These simulation results show that the constructed virtual substitutes appear in the target region where unauthorized device features are located, which matches our expectations. Furthermore, these virtual substitutes are generated in a simple manner that requires no additional computational or training effort. It proves that these virtual class data are ideal substitutes for unauthorized device signals, and our approach aims to use them to pre-occupy the feature space where the unauthorized classes may appear.



(**a**) close-set model (θ and θ_K)

(**b**) expanded model (θ and θ_{K+1})

(**c**) our approach without synthetic substitutes

(**d**) our approach without KD loss

(**e**) our approach

Figure 5. Contribution analysis of different modules to the model performance improvement. r1, r2 and r3 represent authorized devices, and r4 represents all unauthorized devices.

Table 3. Contribution analysis of different modules to the model performance improvement.

Module	AKS	AUS	ACC
close-set model	99.33%	-	-
expanded model	97.00%	0.00%	72.75%
our approach without synthetic substitutes	98.00%	0.00%	73.50%
our approach without KD loss	80.00%	95.00%	83.75%
our approach	88.00%	95.00%	89.75%

In addition, the model expansion of our approach is realized by sharing the K linear output units of the pre-trained closed-set model and adding an additional output unit for unauthorized classes. Then, we hope to sovle the OSR problem of IoT devices by fine-tuning the expanded model on the augumented the original training set. However, the obtained results (as shown in Figure 5a,b) are not consistent with our expectations. After model fine-tuning, the expanded model (includes θ and θ_{K+1}) forgets the knowledge learned from the original training set, resulting in the performance degradation of the model on the authorization class (the value of AKS decreased from 99.33% to 97.00% as shown in Table 3). The reason is that the latent feature distribution of authorized classes has changed, and the original decision boundary is no longer optimal.

In this paper, we construct substitutes for unauthorized devices after inferring on the training set, providing the model with the missing decision information. Furthermore, drawing inspiration from Li et al. [17], we introduce KD loss to alleviate the forgetting phenomenon by modifying the model's decision boundary. The simulation results of the ablation study are shown in Figure 5 and Table 3.

Two aspects of information are shown in the confusion matrix in Figure 5b,c. First, the addition of the KD loss function improves the model's average accuracy for authorized devices (AKS) by 1%. Second, only relying on KD loss without synthetic substitutes, our model cannot identify unauthorized devices since lacking the decision information about these unauthorized classes. Furthermore, the results show in Figure 5c,e prove that the substitutes we constructed is useful, which improves recognition performance of the extended model by sharing the learned knowledge of the closed-set model. In addition, Figure 5d,e show the effect of adding KD loss on our approach's recognition accuracy. It can be seen that the KD loss in our approach not only rarely affects the model's ability to discover unauthorized devices, but also improves the accuracy of authorized devices by 8% (the average accuracy of authorized devices (AKS) increased from 80.00% to 88.00% as shown in Table 3). This indicates that the KD loss coordinates the identification and discovery capabilities of the model by correcting the decision boundary, and achieves an improvement in model recognition performance. Our approach is able to effectively discover unauthorized devices while improving the model forgetting on authorized ones. However, in contrast to our approach, most open-set models ignore the coordination between known and unknown classes, and they sacrifice the performance of known classes for the better performance of unknown classes.

4.4. Performance Comparison

The goal of open-set recognition is to effectively discover unauthorized device signals while recognizing authorized device signals. Therefore, experiments should demonstrate the ability of the proposed method to meet the above requirement. In this section, two experiments are contructed to compare the performance between our approach and other four state-of-the-art OSR methods in terms of recognition accuracy and running time. Softmax and Openmax [3] are a typical type of OSR methods that identify unknown classes by setting decision thresholds, and DC_LSTM [4] is a derivative of Openmax applied in the signal recognition field. DML (Deep Manifold Learning) [40] is another type of OSR methods, which maps the unauthorized class signals to the learned authorized class manifold representations, and uses a clustering model DBSCAN to distinguish unauthorized devices and authorized devices. It can be used to achieve open-set recognition of IoT devices, but the device number (or category number) need to be known in advance.

In this section, we randomly select K authorized devices and one unauthorized device in the ORACLE dataset for experiments with K = 3, 4, 5, respectively. The training set, valication set, and test set are set up similarly to Section 4.1. Each experiment is repeated 15 times, the value of mean and variance are taken in Tables 4 and 5.

Table 4. Comparison of the average accuracy of different state-of-the-art open-set recognition methods.

OSR Method	3 Authorized Devices	4 Authorized Devices	5 Authorized Devices
Softmax	73.55% (±0.84%)	68.58% (±0.72%)	61.03% (±0.31%)
Openmax	82.13% (±5.87%)	73.46% (±5.56%)	69.07% (±5.49%)
DC_LSTM	83.59% (±3.72%)	73.36% (±2.89%)	68.38% (±0.65%)
DML	85.73% (±0.60%)	74.56% (±0.30%)	70.03% (±0.13%)
Our Approach	93.50% (±0.06%)	87.70% (±0.20%)	83.25% (±0.04%)

Table 5. Comparison of the recognition performance of our approach in different conditions.

Authorized Classes	AKS	AUS	ACC	F1-Score
K = 3	93.67% (±0.16%)	92.88% (±0.31%)	93.50% (±0.06%)	0.96 (±0.0002)
K = 4	90.13% (±0.38%)	78.00% (±0.50%)	87.70% (±0.20%)	0.94 (±0.0012)
K = 5	89.90% (±0.45%)	50.00% (±2.00%)	83.25% (±0.04%)	0.91 (±0.0003)

Table 4 gives the test accuracy of our approach and the other four state-of-the-art OSR methods. It can be found that our approach outperforms other OSR methods in different open-set scenarios, although when the authorized device number K = 3, the test accuracy is improved by about 7.7% on average compared to the suboptimal DML method. Experimental results demonstrate that our approach is effective. Its effectiveness stems from the fact that our approach not only utilizes the knowledge inference module to construct ideal substitutes for unauthorized devices, but also uses the knowledge sharing module to correct the model's decision boundaries. In contrast to other four OSR methods, our approach considers balancing the recognition performance of the model for authorized and unauthorized classes.

Table 5 shows the recognition performance of our approach through a variety of evaluation metrics. Here, we conducted three OSR experiments when the number of authorized classes K is set to 3, 4, and 5. From Table 5, we can draw the following two conclusions. First, given a fixed number of authorized devices, the model's accuracy on different unauthorized devices (AUS) is stable. Second, when the number of authorized devices changes, the model's accuracy on unauthorized devices (AUS) decrease with the crease of authorized device numbers. The major reason for this is that as the number of authorized devices grows, the source of synthetic substitutes becomes more complex, and thus the interference caused by these substitutes to the authorized devices in the feature space also increases.

Here, we discuss the computational complexity of our approach. As we all know that time complexity and space complexity are two important evaluation indexes of computational complexity [41,42]. Time complexity is generally represented by the number of floating-point operations (FLOPs), which can be understood as the amount of computation and is the approximate estimation of the computing speed of the model. The multiply–adds (MAdds) index serves a similar purpose. Space complexity refers to how many parameters (Params) the model contains, which can be understood as the size of the model. As shown in Table 6, we provide the complexity evaluation results when the number of authorized classes K = 3, 4, 5. Table 6 shows that the value of the total Params, total FLOPs, and the total MAdds does not change much as the number of authorized classes increases, which indicates that our approach does not require many additional computing resources and model memory.

Table 6. Comparison of the complexity index of our approach in different conditions.

Authorized Classes	Total Params	Total FLOPs	Total MAdds
K = 3	2,664,790	18,120,832	36,017,852
K = 4	2,665,047	18,121,088	36,018,363
K = 5	2,665,304	18,121,344	36,018,874

In addition, running time is an important factor to evaluate the complexity of OSR methods. The definition is the total time spent on one epoch model training and a corresponding test. We compared the running time spent by five OSR methods for the recognition model training on the ORACLE dataset. The running time results, as shown in Figure 6, confirmed that our approach outperforms other four OSR methods. Combined with the results shown in Table 4, our approach provides a significant performance advantage over than other four OSR methods. Therefore, we suggest that the OSR method proposed in this paper be used for wireless device recognition in open-set scenarios.

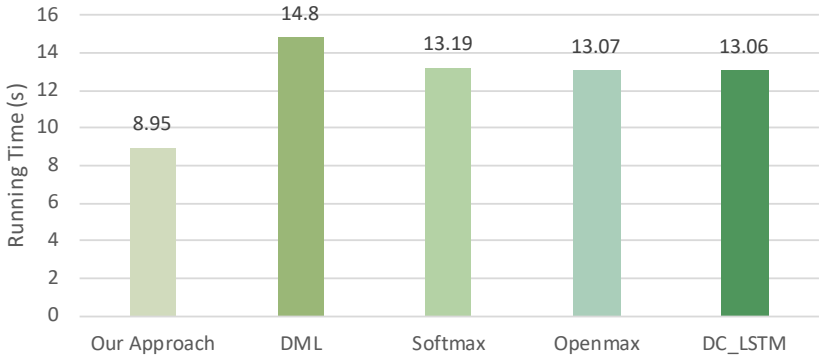


Figure 6. Comparison of running time of the five open-set recognition methods on the ORACLE dataset.

5. Conclusions

In this paper, we propose a knowledge inference and sharing-based open-set device recognition approach for in satellite-terrestrial-integrated IoT which has open satellite link and vast IoT device access. However, most existing models cannot handle the OSR problem due to their lack of decision information for unauthorized devices. Therefore, our approach first performs knowledge inference on the original training set, that is, constructs virtual data as substitutes for unauthorized devices to provide additional decision information to help model recognition. Then, we augment the training set and expand the model architecture, i.e., adds these substitutes into training set, and reserves an output dimension for the unauthorized device for adaptive learning the decision boundary between authorized and unauthorized classes. Moreover, considering the catastrophic forgetting phenomenon caused by knowledge inference and model expansion, we propose a knowledge sharing module that introduces the KD loss to alleviate this problem. In contrast to most OSR studies, our approch considers how to better balance the model's ability of recognizing authorized classes while discovering unauthorized classes. However, they focus on maintaining the model's recognition ability or enhancing the model's discovery ability, but ignore the coordination between the two. The experimental results on the ORACLE dataset show that our approach outperforms other four state-of-the-art OSR approaches in both recognition accuracy and running time. In the future, we will consider conducting open-set recognition experiments on real signal dataset that are closer to the real world, and carry out more detailed studies on different communication channel requirements.

Author Contributions: Conceptualization, Y.Y. and L.Z.; methodology, Y.Y. and L.Z.; software, Y.Y.; validation, Y.Y.; formal analysis, Y.Y.; investigation, Y.Y.; resources, Y.Y.; data curation, Y.Y.; writing—original draft preparation, Y.Y. and L.Z.; writing—review and editing, Y.Y. and L.Z.; visualization, Y.Y. and L.Z.; funding acquisition, L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: Natural Science Foundation of China Project No. 61871422, Natural Science Foundation of Sichuan Province No. 2023NSFSC1422, and Central Universities of Southwest Minzu University No. ZYN2022032.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study. Written informed consent has been obtained from the patients to publish this paper.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
OSR	Open-set Recognition
IQ	In-phase and Quadrature
RF	Radio Frequency
KD	Knowledge Distillation
ACC	Open-set Recognition Accuracy
AKS	The Accuracy on Known Samples
AUS	The Accuracy on Unknown Samples
TP	The True Positive
TN	The True Negative
FP	The False Positive
FN	The False Negative
DML	Deep Manifold Learning
DC_LSTM	Dual Channel LSTM

References

1. Shahid, A.; Fontaine, J.; Camelo, M.; Haxhibeqiri, J.; Saelens, M.; Khan, Z.; Moerman, I.; De Poorter, E. A convolutional neural network approach for classification of lpwan technologies: Sigfox, lora and ieee 802.15. 4g. In Proceedings of the 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 10–13 June 2019; pp. 1–8.
2. Jia, M.; Zhang, X.; Sun, J.; Gu, X.; Guo, Q. Intelligent resource management for satellite and terrestrial spectrum shared networking toward B5G. *IEEE Wirel. Commun.* **2020**, *27*, 54–61. [CrossRef]
3. Bendale, A.; Boult, T.E. Towards Open Set Deep Networks. In Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 27–30 June 2016; pp. 1563–1572. [CrossRef]
4. Guo, Y.; Jiang, H.; Wu, J.; Zhou, J. Open set modulation recognition based on dual-channel lstm model. *arXiv* **2020**, arXiv:2002.12037.
5. Hanna, S.; Karunaratne, S.; Cabric, D. Open Set Wireless Transmitter Authorization: Deep Learning Approaches and Dataset Considerations. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 59–72. [CrossRef]
6. Schlachter, P.; Liao, Y.; Yang, B. Open-set recognition using intra-class splitting. In Proceedings of the 2019 27th European signal processing conference (EUSIPCO), A Coruna, Spain, 2–6 September 2019; pp. 1–5. [CrossRef]
7. Karunaratne, S.; Hanna, S.; Cabric, D. Open set RF fingerprinting using generative outlier augmentation. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–7. [CrossRef]
8. Pidhorskyi, S.; Almohsen, R.; Doretto, G. Generative Probabilistic Novelty Detection with Adversarial Autoencoders. In Proceedings of the Advances in Neural Information Processing Systems, Montreal, QC, Canada, 3–8 December 2018; Volume 31, pp. 6822–6833.
9. Liu, S.; Chen, Y.; Trappe, W.; Greenstein, L.J. ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks. In Proceedings of the IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 675–683. [CrossRef]
10. Rajendran, S.; Lenders, V.; Meert, W.; Pollin, S. Crowdsourced Wireless Spectrum Anomaly Detection. *IEEE Trans. Cogn. Commun. Netw.* **2020**, *6*, 694–703. [CrossRef]
11. Mundt, M.; Pliushch, I.; Majumder, S.; Ramesh, V. Open Set Recognition Through Deep Neural Network Uncertainty: Does Out-of-Distribution Detection Require Generative Classifiers? In Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW), Seoul, Republic of Korea, 27–28 October 2019; pp. 753–757. [CrossRef]
12. Jain, L.P.; Scheirer, W.J.; Boult, T.E. Multi-class open set recognition using probability of inclusion. In Proceedings of the European Conference on Computer Vision, Zurich, Switzerland, 5–12 September 2014; pp. 393–409.
13. Mendes Júnior, P.R.; Souza, R.M.; Werneck, R.D.; Stein, B.V.; Pazinato, D.V.; Almeida, W.R.; Penatti, O.A.; Torres, R.D.; Rocha, A. Nearest neighbors distance ratio open-set classifier. *Mach. Learn.* **2017**, *106*, 359–386. [CrossRef]
14. Chen, G.; Peng, P.; Wang, X.; Tian, Y. Adversarial Reciprocal Points Learning for Open Set Recognition. *IEEE Trans. Pattern Anal. Mach. Intell.* **2022**, *44*, 8065–8081. [CrossRef]
15. Xu, Y.; Qin, X.; Xu, X.; Chen, J. Open-set interference signal recognition using boundary samples: A hybrid approach. In Proceedings of the 2020 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 21–23 October 2020; pp. 269–274.
16. Zhou, D.W.; Ye, H.J.; Zhan, D.C. Learning Placeholders for Open-Set Recognition. In Proceedings of the 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA, 20–25 June 2021; pp. 4399–4408.
17. Li, Z.; Hoiem, D. Learning without Forgetting. *IEEE Trans. Pattern Anal. Mach. Intell.* **2018**, *40*, 2935–2947. [CrossRef]
18. Hinton, G.; Vinyals, O.; Dean, J. Distilling the Knowledge in a Neural Network. *Comput. Sci.* **2015**, *14*, 38–39.

19. O'Shea, T.J.; Corgan, J.; Clancy, T.C. Convolutional radio modulation recognition networks. In Proceedings of the International Conference on Engineering Applications of Neural Networks, Aberdeen, UK, 2–5 September 2016; pp. 213–226.
20. Rajendran, S.; Meert, W.; Giustiniano, D.; Lenders, V.; Pollin, S. Deep Learning Models for Wireless Signal Classification With Distributed Low-Cost Spectrum Sensors. *IEEE Trans. Cogn. Commun. Netw.* **2018**, *4*, 433–445. [CrossRef]
21. Sun, J.; Jia, M.; Guo, Q.; Gu, X.; Gao, Y. Power Distribution Based Beamspace Channel Estimation for mmWave Massive MIMO System With Lens Antenna Array. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 10695–10708. [CrossRef]
22. Neal, L.; Olson, M.; Fern, X.; Wong, W.K.; Li, F. Open set learning with counterfactual images. In Proceedings of the Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, 8–14 September 2018; pp. 613–628.
23. Cao, C.; Cao, Z.; Cui, Z. LDGAN: A Synthetic Aperture Radar Image Generation Method for Automatic Target Recognition. *IEEE Trans. Geosci. Remote Sens.* **2020**, *58*, 3495–3508. [CrossRef]
24. Zhang, H.; Cisse, M.; Dauphin, Y.N.; Lopez-Paz, D. mixup: Beyond Empirical Risk Minimization. In Proceedings of the International Conference on Learning Representations (ICLR), Vancouver, BC, Canada, 30 April–3 May 2018; pp. 1–13.
25. Donahue, J.; Jia, Y.; Vinyals, O.; Hoffman, J.; Zhang, N.; Tzeng, E.; Darrell, T. Decaf: A deep convolutional activation feature for generic visual recognition. In Proceedings of the International Conference on Machine Learning, Beijing, China, 21–26 June 2014; pp. 647–655.
26. Jia, M.; Gao, Z.; Guo, Q.; Lin, Y.; Gu, X. Sparse Feature Learning for Correlation Filter Tracking Toward 5G-Enabled Tactile Internet. *IEEE Trans. Ind. Inform.* **2020**, *16*, 1904–1913. [CrossRef]
27. Schmidt, M.; Block, D.; Meier, U. Wireless interference identification with convolutional neural networks. In Proceedings of the 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), Emden, Germany, 24–26 July 2017; pp. 180–185. [CrossRef]
28. Kulin, M.; Kazaz, T.; Moerman, I.; De Poorter, E. End-to-End Learning From Spectrum Data: A Deep Learning Approach for Wireless Signal Identification in Spectrum Monitoring Applications. *IEEE Access* **2018**, *6*, 18484–18501. [CrossRef]
29. Wen, Y.; Zhang, K.; Li, Z.; Qiao, Y. A Discriminative Feature Learning Approach for Deep Face Recognition. In Proceedings of the Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, 11–14 October 2016; pp. 499–515.
30. Shi, Z.; Wang, H.; Leung, C.S. Constrained Center Loss for Convolutional Neural Networks. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *34*, 1080–1088. [CrossRef] [PubMed]
31. Hassen, M.; Chan, P.K. Learning a Neural-network-based Representation for Open Set Recognition. In Proceedings of the 2020 SIAM International Conference on Data Mining, Cincinnati, OH, USA, 7–9 May 2020; pp. 154–162.
32. Russakovsky, O.; Deng, J.; Su, H.; Krause, J.; Satheesh, S.; Ma, S.; Huang, Z.; Karpathy, A.; Khosla, A.; Bernstein, M.; et al. Imagenet large scale visual recognition challenge. *Int. J. Comput. Vis.* **2015**, *115*, 211–252. [CrossRef]
33. Azizpour, H.; Razavian, A.S.; Sullivan, J.; Maki, A.; Carlsson, S. Factors of transferability for a generic convnet representation. *IEEE Trans. Pattern Anal. Mach. Intell.* **2015**, *38*, 1790–1802. [CrossRef] [PubMed]
34. Yosinski, J.; Clune, J.; Bengio, Y.; Lipson, H. How transferable are features in deep neural networks? In Proceedings of the 27th International Conference on Neural Information Processing Systems-Volume 2, Kuching, Malaysia, 3–6 November 2014; pp. 3320–3328.
35. Sankhe, K.; Belgiovine, M.; Zhou, F.; Riyaz, S.; Ioannidis, S.; Chowdhury, K. ORACLE: Optimized Radio Classification through Convolutional NeuraL Networks. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 370–378. [CrossRef]
36. Geng, C.; Huang, S.j.; Chen, S. Recent advances in open set recognition: A survey. *IEEE Trans. Pattern Anal. Mach. Intell.* **2020**, *43*, 3614–3631. [CrossRef]
37. Dong, Y.; Jiang, X.; Zhou, H.; Lin, Y.; Shi, Q. SR2CNN: Zero-Shot Learning for Signal Recognition. *IEEE Trans. Signal Process.* **2021**, *69*, 2316–2329. [CrossRef]
38. Sokolova, M.; Lapalme, G. A systematic analysis of performance measures for classification tasks. *Inf. Process. Manag.* **2009**, *45*, 427–437. [CrossRef]
39. Van der Maaten, L.; Hinton, G. Visualizing Data using t-SNE. *J. Mach. Learn. Res.* **2008**, *9*, 2579–2605.
40. Stankowicz, J.; Kuzdeba, S. Unsupervised Emitter Clustering through Deep Manifold Learning. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Vegas, NV, USA, 27–30 January 2021; pp. 732–737. [CrossRef]
41. Guan, X.; Yang, Y.; Li, J.; Zhu, X.; Song, J.; Shen, H.T. On the Imaginary Wings: Text-Assisted Complex-Valued Fusion Network for Fine-Grained Visual Classification. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, 1–10. [CrossRef] [PubMed]
42. Chen, S.; Xie, E.; Chongjian, G.; Chen, R.; Liang, D.; Luo, P. CycleMLP: A MLP-like Architecture for Dense Prediction. In Proceedings of the International Conference on Learning Representations (ICLR), Virtual Event, 25–29 April 2022.