Collaborative Spectrum Sensing for Illegal Drone Detection: A Deep Learning-Based Image Classification Perspective

Huichao Chen[1], Zheng Wang[1,*], Linyuan Zhang[2]

[1] College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
[2] College of communications engineering, Army Engineering University, Nanjing 210007, China
* The corresponding author, email: z.wang@nuaa.edu.cn.

Abstract: Drones, also known as mini-unmanned aerial vehicles (UAVs), are enjoying great popularity in recent years due to their advantages of low cost, easy to pilot and small size, which also makes them hard to detect. They can provide real time situational awareness information by live videos or high definition pictures and pose serious threats to public security. In this article, we combine collaborative spectrum sensing with deep learning to effectively detect potential illegal drones with states of high uncertainty. First, we formulate the detection of potential illegal drones under illegitimate access and rogue power emission as a quaternary hypothesis test problem. Then, we propose an algorithm of image classification based on convolutional neural network which converts the cooperative spectrum sensing data at a sensing slot into one image. Furthermore, to exploit more information and improve the detection performance, we develop a trajectory classification algorithm which converts the flight process of the drones in consecutive multiple sensing slots into trajectory images. In addition, simulations are provided to verify the proposed methods' performance under various parameter configurations.

Keywords: illegal drones detection;deep learning; collaborative spectrum sensing

I. INTRODUCTION

During the past few years, mini-unmanned aerial vehicles, also known as drones, have widely applied in communications, surveillance, agriculture, photography, public services, and so on [1]-[3]. However, the wide proliferation of drones brings up the problem of keeping unauthorized drones away from private or sensitive areas, where they can bring a personal or public threat. Drones are physically small in size, which also make them hard to detect. A major threat from small UAVs is their use in direct physical attacks on people, property, and infrastructure and there have been reports of near accidents involving UAVs and aircraft around airports. Small UAVs may carry radioactive materials, explosives, or guns that may be used by malicious entities, to carry out targeted attacks on people and infrastructure. For instance, organized crime groups can use small UAVs to carry illegal information or material, such as smuggling drugs across national borders. Targeted physical attacks to a country

Received: Jun. 25, 2019
Revised: Nov. 9, 2019
Editor: Zan Li

This paper proposed a deep learning based method to detect potential illegal drones in the area of interest in real time.

critical infrastructure, such as its power grid, can enable follow-up cyber attacks [4]. Another major concern related to the use of drones is that of privacy. Drones are easy to carry a camera or recode device to capture information, and this can violate personal or public privacy. Thus, it is critical to detect drones in time.

To detect the drones, a variety of methods have been proposed: video detection, sound detection, radar detection, radiofrequency (RF) detection [5], etc. However, each approach has its merits and limitations.

Video-based detection techniques is based on the use of camera sensors to identify a moving object against the background of the sky [6]. They attempt to distinguish the automatic and mechanical movements of drones from the more natural behavior of birds. But these approaches usually fail in the case of gliding birds, and they do not work well in misty, foggy conditions and at night [5]. Camera sensors are also sensitive to light, and they can only detect objects only when the target is in line of sight.

Sound-based approaches consist of using acoustic sensors such as microphones to capture ambient sounds. The rationale behind this kind of technique is that UAVs usually produce a typical hissing high-frequency sound around 40 kHz due to their brushless direct current motors. The two main differentiators in prior work are the signal processing method and the type of acoustic sensor employed. However, they only work well in quiet environments, but it usually fails in urban or noisy areas.

Radar-based methods utilize the electromagnetic principle of backscattering. The traditional radar approach is useful for detecting large aircraft, but it generally does not work well with small-sized quad-copters. Indeed, using the radar cross-section (RCS) as a feature for drone identification is not quite suitable to detect small UAVs, which are objects providing a rather small RCS [7]. Combined with artificial intelligence technology, these methods can be improved by analyzing the motion characteristic in the signals [8]. Another non-trivial issue is that the radar transmitter may raise radiation health concerns.

RF-based method is another effective method to detect drones. It relies on the fact that drones communicate with the ground control station through RF transmissions. The most commonly employed frequency bands are around 2.4 and 5 GHz. Moreover, UAVs equipped with cameras usually transmit video to their control unit in a wireless manner. Remarkably, the strength of the received signal can be relatively high due to high probability of Line-of-Sight condition in the UAV communication networks, which can be regarded as one key advantage of RF-based method. Some of the problems such as clutters and direct-path interference that are present in passive radar systems are also avoided [9].

Also, there is a trend to combine various techniques for improving the drone detection performance. Some new technologies are emerging recently [10], [11]. In [12], Ding, et al propose a vision named Dragnet by tailoring the recently emerging cognitive Internet of Things framework for amateur drone surveillance where various active and passive surveillance devices (e.g., cameras, sensors, radars, and drones) or crowds of people serve as local fog computing platforms to sense the environment and locally warn about the presence of amateur drone, while a cloud center acts as a system orchestrator that integrates the data from various fog nodes, stores and analyzes these data, and makes global decision making on the presence of amateur drone as well as actions (e.g., jamming, capturing or destroy) on them.

In this article, we combine collaborative spectrum sensing with deep learning to effectively detect illegal drones. Our aim is to detect whether the channel is occupied, and if it is occupied, recognize whether the illegal drones exists. The contributions of this paper are summarized as follows:

- We first formulate the detection of potential illegal drones as a quaternary hypothesis test problem, where the states without

the illegal drones are modeled as simple hypotheses and the states with the illegal drones are modeled as composite ones due to the unknown characteristics about the illegal drones.

- We propose an algorithm of image classification based on convolutional neural network. Exactly, a cooperative spectrum sensing scheme is conducted to measure spectrum, and then we convert the sensing data at a sensing slot into one image for convolutional neural network. Then, the quaternary hypothesis test problem is transformed into a problem of image classification. In this article, the convolutional neural network VGGNet [13] and the lightweight network ShuffleNetV2 [14] are used.
- To improve the detection probability, we develop a trajectory classification algorithm by exploiting the motion characteristics of the drones. Specifically, we convert the flight process of the drones in consecutive multiple sensing slots into trajectory images, which can reduce the influence of noise, sensing errors and other factors.
- We present simulations to verify the detection performance of the proposed methods versus the number of sensors, transmit signal power of drones and the length of sensing time.

The rest of this paper is organized as follows. The system deployment is illustrated in Section II. VGGNet, ShuffleNetV2 and data conversion for convolutional neural network is illustrated in Section III. UAVs detection using deep learning are presented in Section IV. Simulations are described in Section V, followed by conclusion in Section VI.

II. System Model

In this article, we utilize underlying wireless sensing network to obtain spectrum utilization states in the area of interest. In the wireless sensing network, sensor nodes use the energy detection. At a sensing slot, sensors measure spectrum synchronously, and transmit the local observations to a fusion center (FC), at which the data is analyzed to detect illegal drones. The system deployment is shown in figure 1.

In this article, we assume the received signal power at a sensor is given by the following propagation model:

$$P_{ir} = P_t \times d_i^{\gamma}(mW), i = 1, \ldots, N, \quad (1)$$

where P_t denotes the transmit power of drones; d_i denotes the distance between the drones and the i-th sensor; γ denotes the path loss exponent; N denotes the number of sensors. In this article, the path loss exponent γ is 2.

One problem of using wireless sensing network to sense spectrum is that it relies on the radiation of signals transmitted by drones. Drones have to communicate with the ground controllers in navigation or imagery collection. Hence, RF based detection is an effective way to detect the threats of drone by exploiting drone wireless emissions.

In this article, we consider the case that an authorized drone is allowed to flying in a given area and use frequency band M_i from time T_1 to T_2. The activities of illegal drones include:

- When no drones are allowed to enter specific areas, unauthorized drones broke in

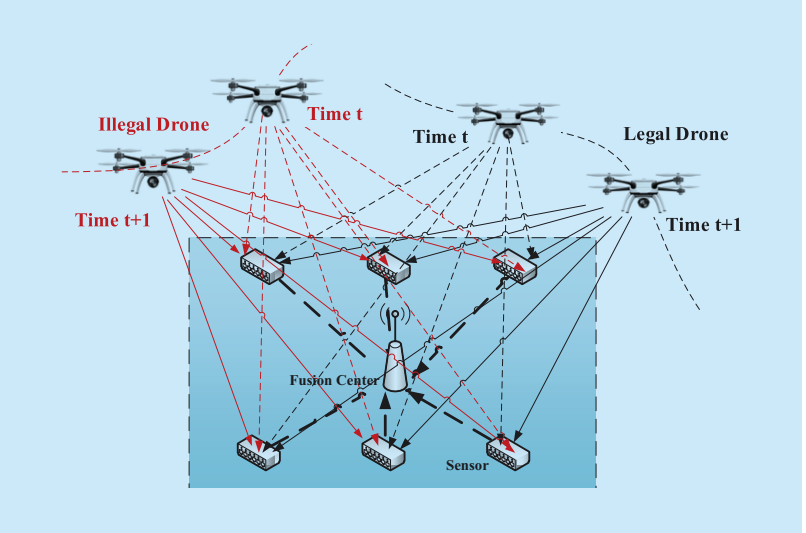

Fig. 1. *System model. It consists of wireless sensing networks, an illegal drone and a legal drone. The arrow lines between drones and sensors denote the received signal of sensors from drones. The red arrow lines represent the signal from illegal drones and the black arrow lines represent the signal from legal drones. In addition, solid arrow lines denote the signal at time t and dotted arrow lines denote the signal at time t+1.*

and communicate;

- In the case of authorized drones are flying and communicate in given areas, unauthorized drones intrude and interfere with authorized drones' normal communications.

The problem of detecting illegal drones is formulated as a quaternary hypothesis test [15]:

$$\begin{cases} H_0 : y_i(n,t) = n_i(n,t), \\ H_1 : y_i(n,t) = \sqrt{P_{\mathrm{si}}} s_i(n,t) + n_i(n,t), \\ H_2 : y_i(n,t) = \sqrt{P_{xi}} x_i(n,t) + n_i(n,t), \\ H_3 : y_i(n,t) = \sqrt{P_{\mathrm{si}}} s_i(n,t) + \sqrt{P_{xi}} x_i(n,t) + n_i(n,t), \end{cases} \tag{2}$$

where H_0 denotes the state that no drones fly and communicate, H_1 denotes the state that only the authorized drone exists, H_2 denotes the state that only unauthorized drone exists corresponding to the first case, H_3 denotes the state that the authorized drone and unauthorized drone co-exists corresponding to the second case, $y_i(n,t)$ is the n-th sample value of i-th sensor at the t-th sensing slot and $n = 1, \ldots, M$, M is the total sample number, $s_i(n,t)$ and $x_i(n,t)$ denote the signal transmitted by the legal drone and illegal drone, respectively, P_{si} and P_{xi} denote the received power of i-th sensor from legal drones and illegal drones, respectively, that are related with the transmit power and the path loss and invariable during the sample time. Here, $s_i(n,t)$ and $x_i(n,t)$ follow the independent and identically distribution (i.i.d.) with zero mean and unit variance [16]. In addition, $n_i(n,t)$ is modeled as i.i.d. Gaussian distribution with zero mean and variance σ_n^2 [17].

For each sensor, we consider energy detection as the means of signal detection. The test statistic for energy-based opportunity detection by each sensor is:

$$E_i(k) = \frac{1}{M} \sum_{n=1}^{M} [y_i(n,k)]^2. \tag{3}$$

According to the central limit theorem (CLT), when the sample number is sufficiently large (e.g., $M \gg 10$), $E_i(k)$ is approximated as a Gaussian random variable under both hypotheses H_0, H_1, H_2 and H_3 in the k-th sensing period [18], [19].

$$E_i(k) \sim \begin{cases} N(u_0, {\sigma_0}^2), & H_0 \\ N(u_1, {\sigma_1}^2), & H_1 \\ N(u_2, {\sigma_2}^2), & H_2 \\ N(u_3, {\sigma_3}^2), & H_3, \end{cases} \tag{4}$$

where

$$\begin{cases} u_0 = {\sigma_n}^2, \\ {\sigma_0}^2 = 2{\sigma_n}^4 / M, \\ u_1 = (1+\gamma_{1i}){\sigma_n}^2 = (1+\gamma_{1i})u_0, \\ {\sigma_1}^2 = 2(1+2\gamma_{1i}){\sigma_n}^4 / M = (1+2\gamma_{1i}){\sigma_0}^2, \\ u_2 = (1+\gamma_{2i}){\sigma_n}^2, \\ {\sigma_2}^2 = 2(1+2\gamma_{2i}){\sigma_n}^4 / M, \\ u_3 = (1+\gamma_{3i}){\sigma_n}^2, \\ {\sigma_3}^2 = 2(1+2\gamma_{3i}){\sigma_n}^4 / M, \end{cases}$$

$\gamma_{1i} = P_{is} / {\sigma_n}^2$, $\gamma_{2i} = P_{ix} / {\sigma_n}^2$, $\gamma_{3i} = (P_{is} + P_{ix}) / {\sigma_n}^2$ represent the received signal-to-noise ratio (SNR) of the i-th sensor under hypotheses H_1, H_2 and H_3, respectively.

One vital challenge is that illegal drones may act in an intermittent and fast-changing manner, which brings about much uncertainty for spectrum sensing. Moreover, the prior knowledge, such as the prior probabilities and the distribution of the probability density function of the received power from the illegal drones are hard to obtain, so the quaternary hypothesis test problem is hard to be solved. The traditional methods are mainly based on the classical statistical signal processing theory. In this article, we consider the spectrum sensing network composed of multiple sensors, and designs the related methods from the perspective of image.

III. Convolutional Neural Network and Data Conversion

In this section, we first present the background knowledge on VGGNet and ShuffleNetV2 and then we introduce two methods of data conversion for CNN according to the selection of the length of sensing time.

3.1 VGGNet and ShuffleNetV2

Convolutional neural networks, are a specialized kind of neural network for processing data that has a known, grid-like topology. Examples include time-series data, which can be thought of as a one-dimensional grid taking samples at regular time intervals, and image data, which can be thought of as a two-dimensional grid of pixels.

The VGGNet architecture was proposed in 2014 for the contest ImageNet Large Scale Visual Recognition Challenge (ILSVRC 2014) [13] of large-scale image classification. The main contribution is to increase the network depth using very small convolution filters. This model demonstrated that the depth of the network (16 or 19 layers) improves the classification performance significantly. VGGNet has a strong extensibility, strong ability of generalization and is widely used as trunk feature extraction network for various detection network frameworks such as Fast-RCNN, SSD. It has been widely used in image classification. It consists of thirteen convolutional layers and two fully connected layers with a 1000-way softmax layer as illustration in figure 2 and the activation function is rectified linear units (ReLUs): $f(x) = \max(0, x)$.

Besides accuracy, computation complexity is another important consideration. Under a limited computational budget, a series of light-weight networks are proposed for light-weight architecture design and better speed-accuracy tradeoff. Group convolution and depth-wise convolution are crucial in these works. To further reduce computational complexity, the ShuffleNetV2 proposes a new efficient architecture and uses a new operator called channel split. The main constituent unit of ShuffleNetV2 is shown in figure 3.

This paper studies the use of convolutional neural network in illegal drones detection. Specifically, given the data received by sensors in wireless sensing network, our task is to detect illegal drones combining with the working status of legal drones. As mentioned above, most existing convolutional neural network models, including VGGNet and ShuffleNetV2, are developed for image recognition/classification. However, in the data from energy sensor to be processed are not images but complex

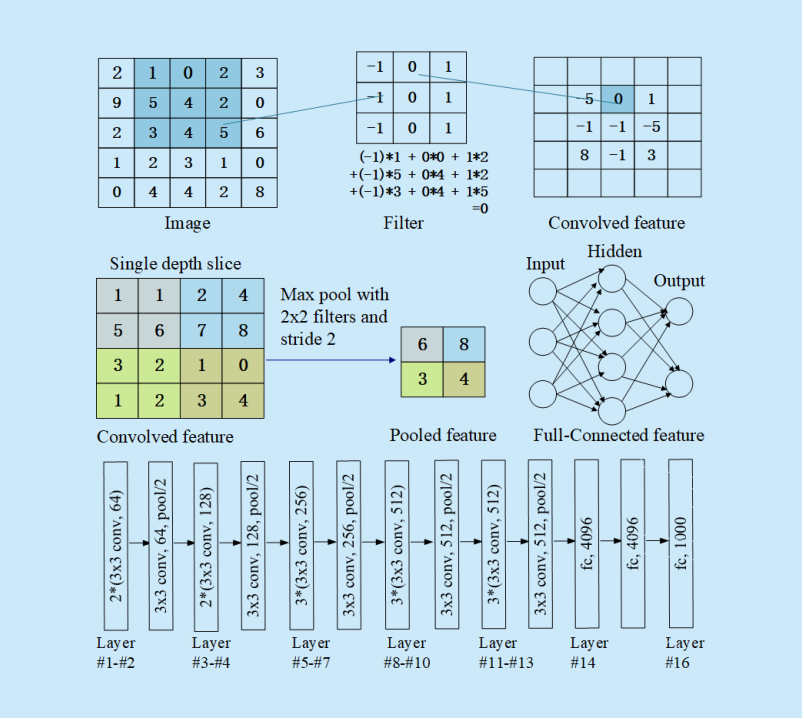

Fig. 2. *The VGG16Net architecture. It consists of 16 layers. Convolution layer extracts features automatically. Pooling layer reduces parameters and prevents overfitting.*

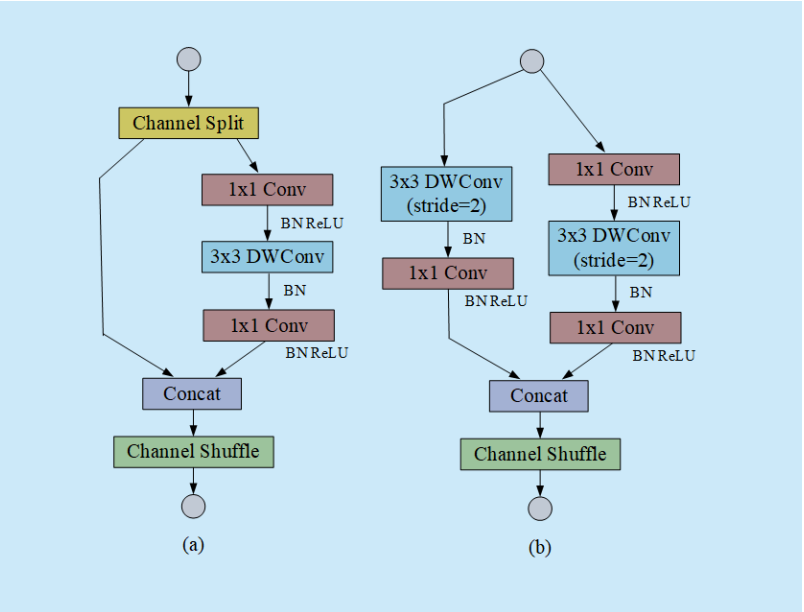

Fig. 3. *The main constituent unit of ShuffleNetV2. (a) is the basic unit; (b) is the unit for spatial down sampling. DWConv is depthwise convolution. GConv is group convolution.*

data samples. In order to utilize the existing deep learning models, we can convert energy sensor data into images. Since a data conversion process usually introduces information loss, our research and design aim to gain more information through studing the trajectory images of the drone.

3.2 Single slot sensing image

At every sensing slot, sensors measure spectrum synchronously, and transmit local observations to a fusion center. The fusion center converts the data into images according to the location of each sensor and the corresponding signal strength value. However, due to the different position of UAV in each sensing slot, the range of signal intensity value in fusion center is different, so each image shows relative brightness. Moreover, the more sensor nodes there are, the more information can be obtained, and the number of different sensor nodes in wireless sensing network corresponds to different resolution of the image. Thus, we study the influence of different sensor number N on classification performance, and mainly focus on the bad conditions of low-sensor nodes as illustrated in figure 4, where the single transmission power P_t is 100 mW, the noise power is 0.1 mW, the coordinates of the drone in one drone images is (600, 600, 50), then the signal power received by each sensors $P_r = P_t \times d^{-2}$ range from 1.46×10^{-4} mW to 3.68×10^{-4} mW, then the SNR of sensors in wireless sensing network rang from -69.27 dB to -10.01 dB approximately.

Then, the quaternary hypothesis test problem of equation (2) is transformed into a three-classification problem. Exactly, the problem is to detect the number of drones signal transmit sources n:

$$\begin{cases} H_0 : n = 0, no \ \ signal \ \ source, \\ H_1 : n = 1, singal \ \ drone \ \ source, \\ H_2 : n = 2, two \ \ drone \ \ source. \end{cases} \tag{5}$$

When we detect there exists one drone, it can be a legal drone or an illegal drone corresponding to the state H_1 and H_2 of equation (2). As for the traditional methods based on the classical statistical signal processing theory, it is especially difficult to distinguish them. In this article, we can obtain the working state of the legal drone based on the spectrum

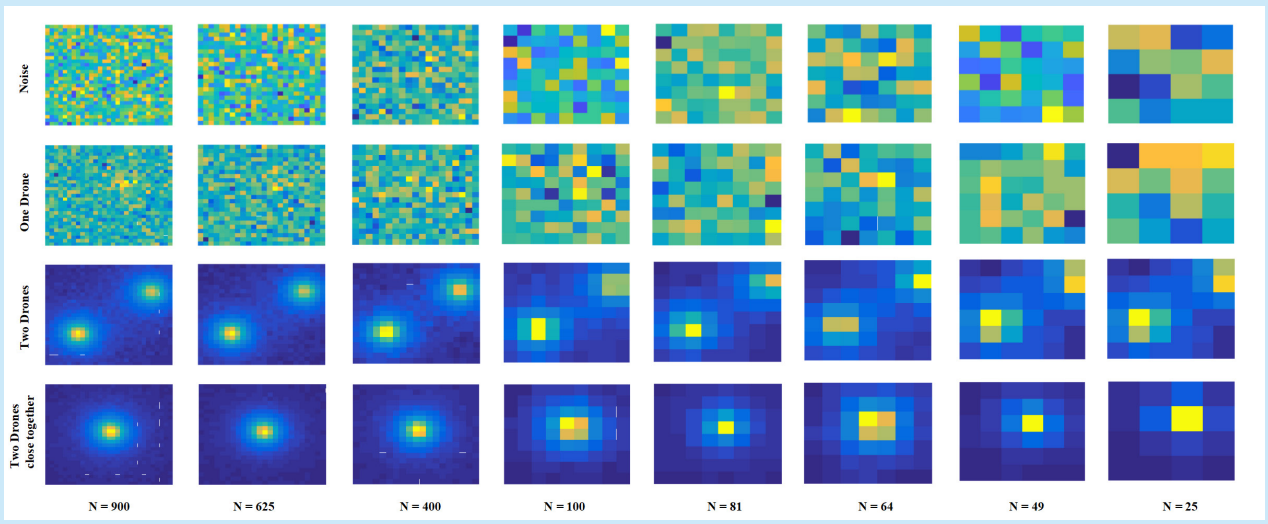

Fig. 4. *Four kinds of images of single slot sensing image under different sensor nodes. For each image, the noise power σ_n^2 is 0.1 mW; the coordinates of the drone in one drone images is (600, 600, 50), the signal transmission power P_t is 100 mW and the SNR of sensors in wireless sensing network rangs from -69.27 dB to -10.01 dB approximately; the coordinates of two drones are (800, 700, 80) and (250, 300, 70), the signal power are both 100 mW and the SNR of sensors in wireless sensing network rang from -56.88 dB to -16.16 dB approximately; the coordinates of two drones closed together are (500, 500, 60) and (480, 530, 80).*

resource management unit. If the authorized drone is working, then there exists no illegal drone, otherwise, there exists illegal drone.

As is shown in figure 4, under the influence of noise, the images in the case of only one drone looks like the same as noise, thus, it is hard to tell one drone from noise. Moreover, when two drones close together, it is not easy to tell if it's two drones.

3.3 Trajectory image of UAVs

Due to the influence of noise and sensor error, it is not reliable to detect UAVs based on a single sensing slot image. Generally, if the UAVs communicates, it will communicate for a period of time. Trajectory images of 5 continuous data collections is illustrated in figure 5 when the number of sensors N is 900. As we can see, by observing the trajectory images, the influence of noise is seems to be reduced, and for two drones close at one slot, detecting illegal drones will be easier by introducing trajectory image.

IV. UAVS Detection Using Convolutional Neural Network

4.1 VGGNet and ShuffleNetV2 configurations

Keras, a widely used deep learning framework, is utilized to build convolutional neural network-based models for drones detection. Due to its strong modularity with Python/MATLAB support, we are able to design and evaluate our models efficiently. For VGGNet, a built-in model, VGG16 provided within Keras interface are investigated. To accommodate our mission, we modify two layers in the network while keeping the rest fourteen layers unchanged. The number of output in layer 16 is changed from the default of 1000 to 3 which is matched to the number of detection categories investigated in our case. The number of neurons in the layer 16 is shrinked to 100, since the original 4096 neurons always lead to difficulty in convergence during our model training. ShuffleNetV2 is also programmed based on keras. In addition to the changes of model architecture, several parameters of solver configuration are also adjusted for a better classification performance as well as a higher training speed, such as learning rate is set 0.001 for training Single Slot Sensing Image and set 0.01 for training Trajectory Image. Moreover, the method early stop and automatic attenuation of learning rate are added to improve classification performance and prevent overfitting. Moreover, considering the tradeoff between available computing resources on graphics processing unit (GPU) and training efficiency, we use a mini-batch Adam with a batch size of 64 in the input layer.

4.2 Implementation

The VGGNet and ShuffleNetV2 are trained as follows: 1) the singals received from sensors are obtained from computer simulations and the sampling number M is 100; 2) each image is labeled according to the number of UAV;

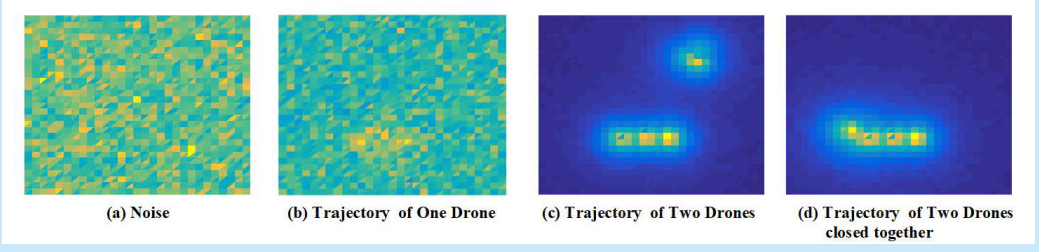

Fig. 5. *Four kinds of trajectory images. For each image, the noise power is 0.1 mW. For image of (b), (c) and (d), the signal transmission power P_t is 100 mW. For image of (b), the coordinates of drone is (300, 300, 50). For image of (c), the coordinates of drones are (300, 300, 50) and (700, 700, 70). For image of (d), the coordinates of drones are (300, 300, 50) and (300, 350, 70).*

3) 4000 per category are collected to form training sets; 4) both data sets are fed to deep learning networks for training with Keras; 5) after a maximum of 100 training iterations, the trained models can be obtained. In this paper, training is conducted on our computing server with a Nvidia GTX 1080 GPU.

After training, test sets consist of 2000 per category are fed to deep learning networks for calculation. Calculation result is a probability vector that indicates all possible categories and take the category with the highest probability as the result. Therefore, the detection probability is the classification accuracy of equation (5), i.e. $P_d = P(H_0 \mid H_0) + P(H_1 \mid H_1) + P(H_2 \mid H_2)$.

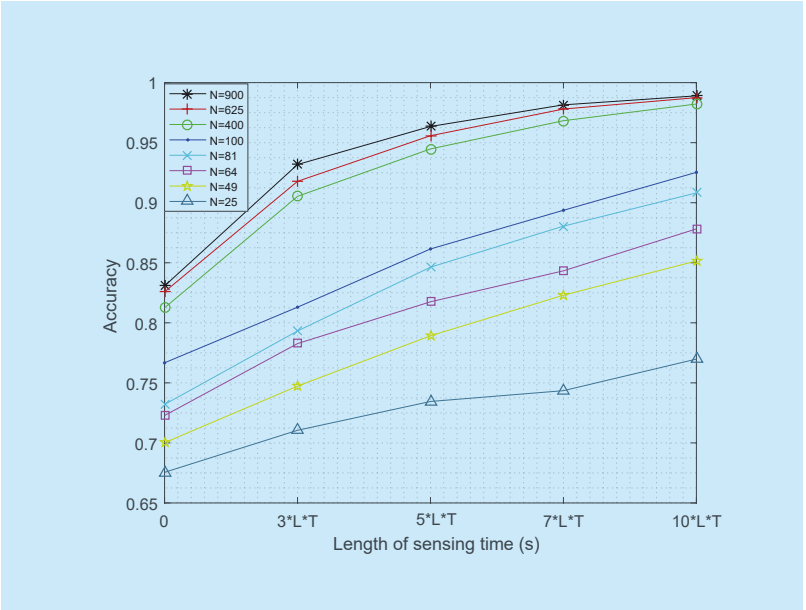

Fig. 6. *Impact of the length of sensing time on VGGNet accuracy at different sensor nodes N. Here, the noise power σ_n^2 is 0.1 mW, the sample number is M = 100, signal transmission power P_t = 100 mW.*

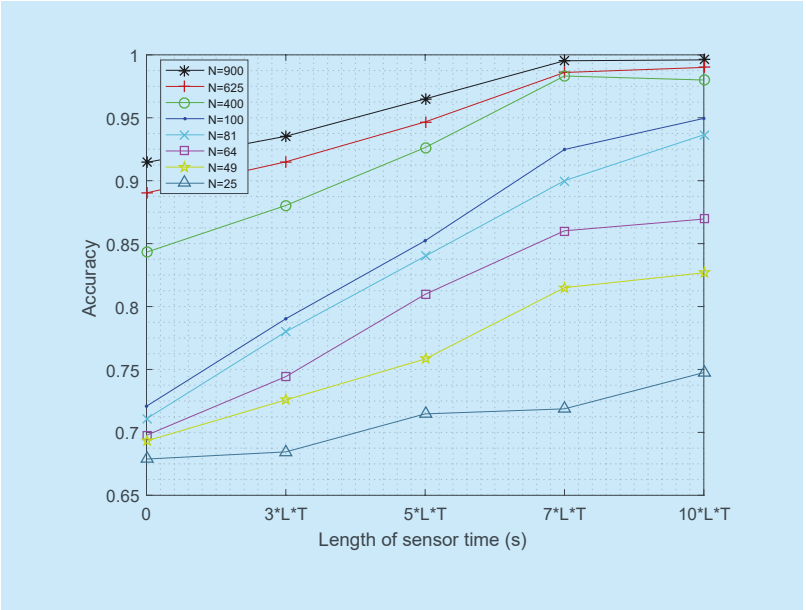

Fig. 7. *Impact of the length of sensing time on ShuffleNetV2 accuracy at different sensor nodes N. Here, the noise power σ_n^2 is 0.1 mW, the sample number is M = 100, signal transmission power P_t = 100 mW.*

V. Simulations

We consider the wireless sensing network is a 1000m×1000m square area, and the sensors are placed uniformly in it.

5.1 Effect of the length of sensing time

In Section III, we have discussed methods to convert observations into single slot sensing images and trajectory images. As mentioned earlier, we collect data per L sensor period. Here, we assume that the UAV moves in a straight line with a velocity of v along with a certain direction within L sensor period. If the move speed v is 100 m/s, and the sensor period T is 0.02s, then we set the L as 25. We present some simulation results to show the impact of different length of sensing time. In each case, we set the noise power σ_n^2 as 0.1 mW and set the transmission power of UAVs P_t as 100 mW. For each case, 12000 images are fed to VGGNet and ShuffleNetV2 for training, which results in a trained network. For each network, 6000 tests are implemented to evaluate its classification performance. Figure 6 records the test results of VGGNet and figure 7 records the test results of ShuffleNetV2. As shown in the figure, the classification accuracy increases with the increase of the length of sensing time. From figure 6 and figure 7, we can see that when the number of sensors is smaller than 400, VGGNet works better than ShuffleNetV2, but ShuffleNetV2 has less computational complexity than VGGNet. In the

actual process, we can choose different networks according to different requirements to trade off between accuracy and computational complexity.

5.2 Impact of the number of sensor nodes

As mentioned before, the more perceptive nodes in the wireless sensing network, the more information can be obtained and the number of different sensor nodes N corresponds to different resolution of the image. Thus, the number of sensor nodes in wireless sensing network is a key parameter. Figure 8 and figure 9 demonstrates the impact of the number of sensors on the classification accuracy of single sensor images and the number of sensors settings is show in Table I. The classification accuracy is evaluated based on 2000 tests per category. As shown in this figure, higher number of sensors incurs a better classification accuracy. From figure 8 and figure 9, we can see that when the number of sensors is smaller than 400, VGGNet works better than ShuffleNetV2 at different transmission power of UAVs. When the transmission power is 30 mW and the number of sensor nodes is smaller than 900, VGGNet works better than ShuffleNetV2. But ShuffleNetV2 has less computational complexity than VGGNet. In the actual process, we can choose different networks according to different requirements to trade off between accuracy and computational complexity.

5.3 Accuracy comparisons

For accuracy comparison between traditional feature extraction based method and VGGNet and ShuffleNetV2 at different transmission power of UAVs P_t of single sensor images, we also train and test based on the traditional image classification algorithms. The first benchmark is Histogram of Oriented Gradient (HOG) algorithm [20], which can well describe the features of local target area and is a common feature extraction method. Moreover, HOG combines with SVM have an excellent effect in pedestrian detection. Figure 10 shows the simulation results of comparison between VGGNet and HOG algorithms. Figure 11 shows the simulation results of comparison between ShuffleNetV2 and HOG algorithms. The second benchmark is Fuzzy Removing

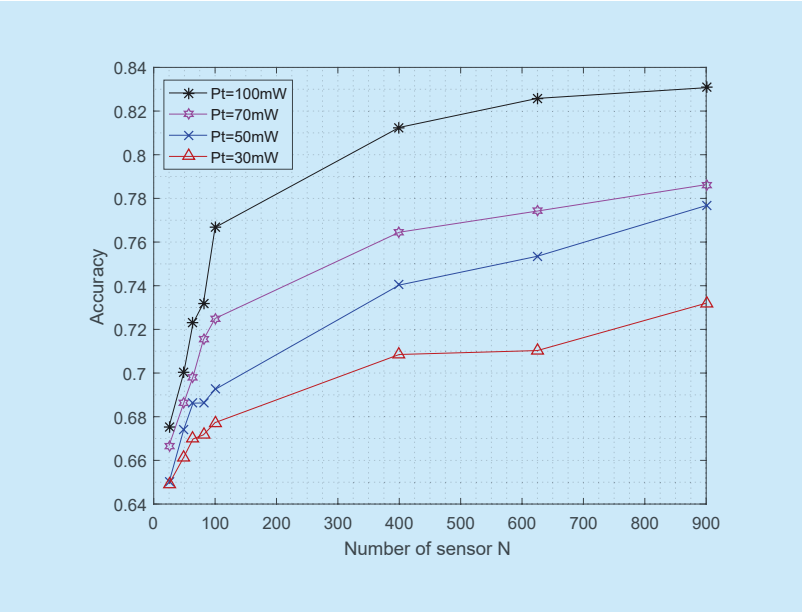

Fig. 8. *Impact of the number of sensors on VGGNet accuracy at different transmission power of UAVs P_t. Here, the noise power σ_n^2 is 0.1 mW, the sample number is M = 100.*

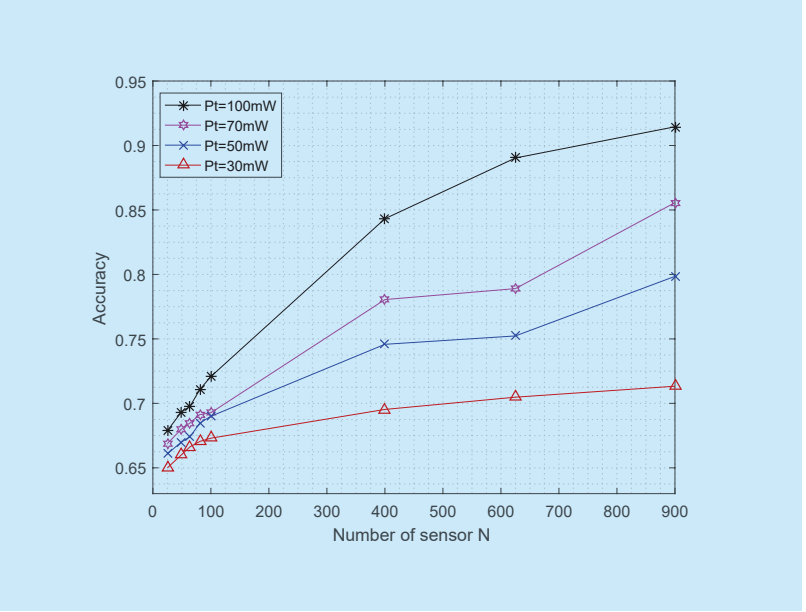

Fig. 9. *Impact of the number of sensors on ShuffleNetV2 accuracy at different transmission power of UAVs P_t. Here, the noise power σ_n^2 is 0.1 mW, the sample number is M = 100.*

Table I. *Number of sensors settings.*

Sensor density (m^{-2})	Number of snesors
2.5×10^{-5}	25
10^{-5}	49
2×10^{-5}	64
8.1×10^{-5}	81
10^{-4}	100
4×10^{-4}	400
6.25×10^{-4}	625
9×10^{-4}	900

Redundancy Restricted Boltzmann Machine (F3RBM) algorithm [21], which is proposed recently. The features extracted by F3RBM are imported into SVM to establish F3RBM-SVM model for fast and automatic classification. Since F3RBM algorithm is suitable for grayscale image, we convert our rgb image into grayscale image for comparative experiment. Figure 12 shows the simulation results of comparison between VGGNet and F3RBM algorithms based on grayscale image. Figure 13 shows the simulation results of comparison

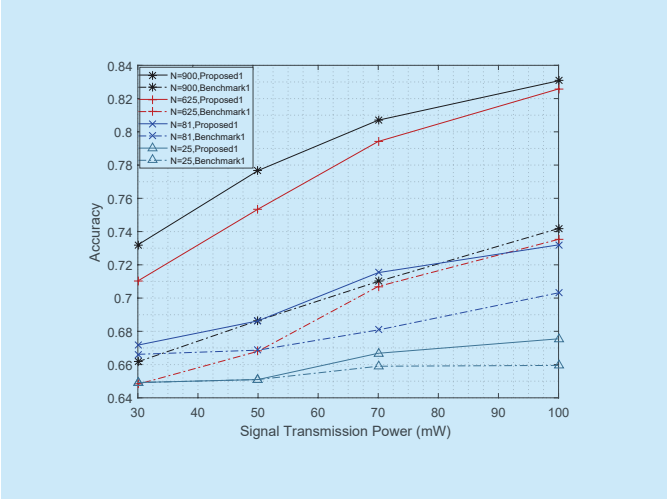

Fig. 10. *Accuracy comparisons between VGGNet and Hog algorithms at different transmission power of UAVs P_t. Here, the noise power σ_n^2 is 0.1 mW, the sample number is M = 100.*

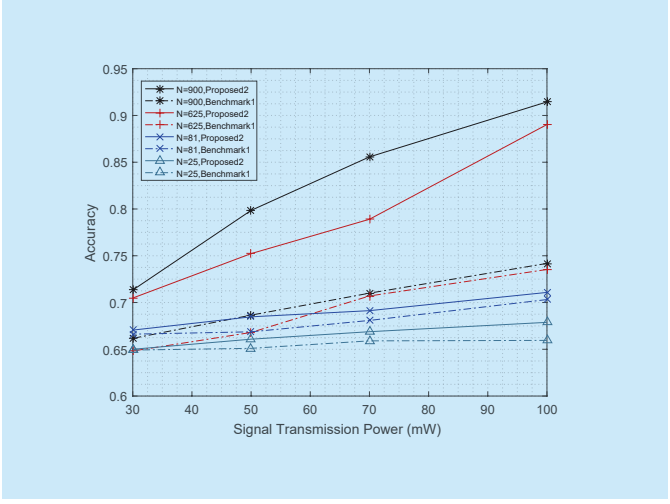

Fig. 11. *Accuracy comparisons between ShuffleNetV2 and Hog algorithms at different transmission power of UAVs P_t. Here, the noise power σ_n^2 is 0.1 mW, the sample number is M = 100.*

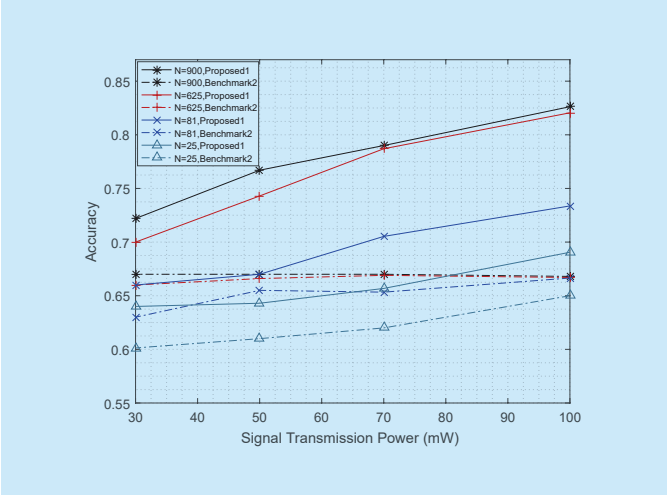

Fig. 12. *Accuracy comparisons between VGGNet and F3RBM algorithms at different transmission power of UAVs P_t. Here, the noise power σ_n^2 is 0.1 mW, the sample number is M = 100.*

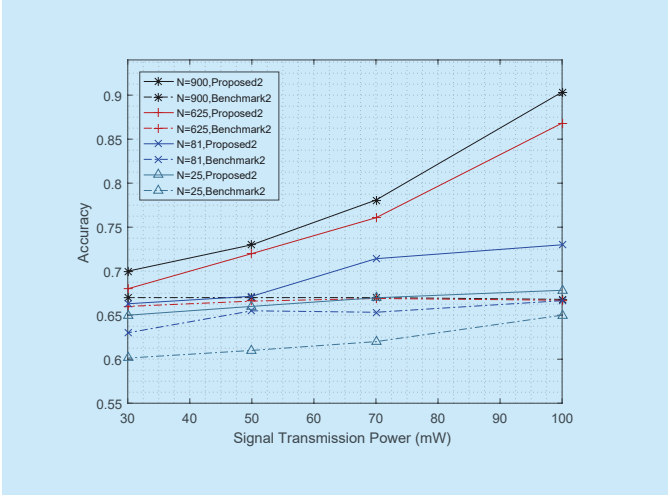

Fig. 13. *Accuracy comparisons between ShuffleNetV2 and F3RBM algorithms at different transmission power of UAVs P_t. Here, the noise power σ_n^2 is 0.1 mW, the sample number is M = 100.*

between ShuffleNetV2 and F3RBM algorithms based on grayscale image. As we can see, the classification performance of VGGNet and ShuffleNetV2 are both better than HOG combined with SVM and F3RBM-SVM at different number of sensor nodes and transmission power of UAVs.

VI. Conclusion

This paper proposed a deep learning based method to detect potential illegal drones in the area of interest in real time. We converted the data into single sensor slot images and trajectory images for deep learning. Simulation results show the effectiveness of this method even on the bad conditions of low-sensor nodes and low SNR environment. The simulation results verified the detection performances in terms of the number of sensors, signal transmitting power of drones and the length of sensing time. The remaining challenge is that when legal and illegal drones very close together, the network may misclassify. Further research will be conducted to investigate several issues including some more effective image data preprocessing to improve the detection of drones and the imperfect wireless channels as well as the resource constrain of Wireless sensing network. Moreover, the non-uniform distribution of sensor nodes will be taken into consideration.

Acknowledgement

This work is supported by the Foundation of Graduate Innovation Center in NUAA under Grant No. kfjj20190414, the open research fund of Key Laboratory of Dynamic Cognitive System of Electromagnetic Spectrum Space (Nanjing Univ. Aeronaut. Astronaut.), Ministry of Industry and Information Technology, Nanjing, 211106, China (No. KF20181913), National Natural Science Foundation of China (No. 61631020, No. 61871398, No. 61931011 and No. 61801216), the Natural Science Foundation for Distinguished Young Scholars of Jiangsu Province (No. BK20190030) and the Natural Science Foundation of Jiangsu Province (No. BK20180420).

References

[1] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 899–922, 2016.

[2] M. Liu, J. Yang, and G. Gui, "DSF-NOMA: UAV-assisted emergency communication technology in a heterogeneous Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5508–5519, June 2019.

[3] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV relaying-assisted secure transmission with caching," *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3140–3153, 2019.

[4] Li, An, and Wenjing Zhang. "Mobile jammer-aided secure UAV communications via trajectory design and power control." *China Communications* 15.8 (2018): 141-151.

[5] S. R. Ganti and Y. Kim, "Implementation of detection and tracking mechanism for small UAS," in *2016 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2016, pp. 1254–1260.

[6] M. A. Ma'sum, M. K. Arrofi, G. Jati, F. Arifin, M. N. Kurniawan, P. Mursanto, and W. Jatmiko, "Simulation of intelligent unmanned aerial vehicle (UAV) for military surveillance," in *2013 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*. IEEE, 2013, pp. 161–166.

[7] M. Ritchie, F. Fioranelli, H. Griffiths, and B. Torvik, "Micro-drone RCS analysis," in *2015 IEEE Radar Conference*. IEEE, 2015, pp. 452– 456.

[8] D. Schneider, "Can we detect small drones like the one that crashed at white house? yes, we can," *IEEE Spectrum*, 2015.

[9] P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han, and T. Vu, "Investigating cost-effective RF-based detection of drones," in *Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*. ACM, 2016, pp. 17–22.

[10] Q. Wu, G. Ding, Y. Xu, S. Feng, Z. Du, J. Wang, and K. Long, "Cognitive internet of things: a new paradigm beyond connection," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 129–143, 2014.

[11] Q. Wu, G. Ding, J. Wang, and Y.-D. Yao, "Spatial-temporal opportunity detection for spectrum-heterogeneous cognitive radio networks: Twodimensional sensing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 2, pp. 516–526, 2013.

[12] G. Ding, Q. Wu, L. Zhang, Y. Lin, T. A. Tsiftsis, and

Y.-D. Yao, "An amateur drone surveillance system based on the cognitive internet of things," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 29–35, 2018.

[13] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv*:1409.1556, 2014.

[14] N. Ma, X. Zhang, H.-T. Zheng, and J. Sun, "Shufflenet v2: Practical guidelines for efficient CNN architecture design," in *Proceedings of the European Conference on Computer Vision (ECCV)*, 2018, pp. 116–131.

[15] L. Zhang, G. Ding, Q. Wu, and Z. Han, "Spectrum sensing under spectrum misuse behaviors: A multi-hypothesis test perspective," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 993–1007, 2017.

[16] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, 2011.

[17] G. Ding, Q. Wu, Y. Yao, J. Wang, and Y. Chen, "Kernel-based learning for statistical signal processing in cognitive radio networks: Theoretical foundations, example applications, and future directions," *IEEE Signal Processing Magazine*, vol. 30, no. 4, pp. 126–136, July 2013.

[18] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[19] Hu, Linna, et al. "Optimal energy-efficient transmission for hybrid spectrum sharing in cooperative cognitive radio networks." *China Communications* 16.6 (2019): 150-161.

[20] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *international Conference on computer vision & Pattern Recognition (CVPR'05)*, vol. 1. IEEE Computer Society, 2005, pp. 886–893.

[21] X. Lü, L. Meng, C. Chen, and P. Wang, "Fuzzy removing redundancy restricted boltzmann machine: improving learning speed and classification accuracy," *IEEE Transactions on Fuzzy Systems*, 2019.

Biographies

Huichao Chen, received her B.S. degree in information engineering from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2018. Her research interests include cognitive information theory, cognitive radio, signal processing and wireless communications.

Zheng Wang, received the B.S. degree in electronic and information engineering from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2009, and the M.S. degree in communications from the Department of Electrical and Electronic Engineering, University of Manchester, Manchester, U.K., in 2010. He received the Ph.D degree in communication engineering from Imperial College London, UK, in 2015. From 2015 to 2016 he served as a Research Associate at Imperial College London, UK and from 2016 to 2017 he was an senior engineer with Radio Access Network R&D division, Huawei Technologies Co.. He is currently an Assistant Professor at the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China. His current research interests include lattice methods for wireless communications, cognitive radio and physical layer security.

Linyuan Zhang, received his B.S. degree (with honors) in electronic engineering from Inner Mongolia University, Hohhot, China, in 2012. He is currently pursuing his Ph.D. degree in communications and information system in College of Communications Engineering, Army Engineering University of PLA. His research interests are wireless security and statistical learning.