

Retraction

Retracted: Detection of Constellation-Modulated Wireless Covert Channel Based on Adjusted CNN Model

Security and Communication Networks

Received 26 December 2023; Accepted 26 December 2023; Published 29 December 2023

Copyright © 2023 Security and Communication Networks. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

- [1] S. Huang, W. Liu, G. Liu, Y. Dai, and H. Bai, "Detection of Constellation-Modulated Wireless Covert Channel Based on Adjusted CNN Model," *Security and Communication Networks*, vol. 2021, Article ID 5569745, 14 pages, 2021.

Research Article

Detection of Constellation-Modulated Wireless Covert Channel Based on Adjusted CNN Model

Shuhua Huang ¹, Weiwei Liu ¹, Guangjie Liu,² Yuewei Dai,² and Huiwen Bai ¹

¹Nanjing University of Science and Technology, Nanjing 210094, China

²Nanjing University of Information Science and Technology, Nanjing 210044, China

Correspondence should be addressed to Weiwei Liu; lwwnjust@njust.edu.cn

Received 1 February 2021; Revised 8 May 2021; Accepted 26 May 2021; Published 7 June 2021

Academic Editor: Chi-Hua Chen

Copyright © 2021 Shuhua Huang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the development of wireless communication technology, more and more information leakage is realized through a wireless covert channel, which brings great challenges to the security of wireless communication. Compared with the wireless covert channel on the upper layer, the wireless covert channel based on the physical layer (WCC-P) has better concealment and greater capacity. As the most widely used scheme of WCC-P, the wireless covert channel with the modulation of the constellation point (WCC-MC) has attracted more and more attention. In this paper, a deep learning scheme based on amplitude-phase characteristics is proposed to detect and classify the WCC-MC scheme. We first extract the amplitude and phase characteristic of error vector magnitude (EVM) and constellation points and then map the amplitude and phase characteristic to the grayscale image, respectively. Finally, the generated feature images are trained, detected, and classified with the adjusted convolution neural network. The experimental results show that the detection accuracy of our proposed scheme can reach 98.5%, and the classification accuracy can reach 81.7%.

1. Introduction

A covert channel is considered a technique for secretly transmitting information from a malicious entity to other entities. In the wireless covert channel communication model, there are one transmitter and one receiver. The transmitter sends a wireless signal embedded with hidden information to the receiver via the broadcast media. The receiver decodes the hidden information by the rule shared with the transmitter. Wireless covert channel (WCC) is more capable of realizing the purpose of covert communication because of its unique broadcasting characteristics. Although there have been recent research efforts on detecting covert timing channels over the Internet [1–5]. Research on the detection of WCC is currently relatively rare, mainly divided into two types, one is the detection for wireless covert channel based on upper layer protocol (WCC-U), and the other is for wireless covert channel based on the physical layer (WCC-P).

WCC-U scheme realizes the information leakage mainly through embedded secret information in the redundant position in the wireless protocol; this kind of covert channel can be detected through the analysis of upper layer protocol and firewall. The realization of the WCC-P covert channel is mainly through the modulation of the physical layer signal, such as modulation of the characteristic parameter (WCC-MP) [6, 7], the modification of Orthogonal Frequency Division Multiplexing symbols (WCC-MO) [8–11], and the modulation of the constellation point (WCC-MC) [12, 13]. The correlation of the time domain signal [14] is used to realize the effective detection of the WCC-MP signal [6]. WCC-MO scheme is constrained by Orthogonal Frequency Division Multiplexing (OFDM) structure and can be detected by numerical statistics [9]. There are little researches on WCC-MC detection due to the randomness of the physical layer (such as channel fading and receiver noise) making the WCC-MC scheme more difficult to crack. In [12], the concealment of the WCC-MC signal is measured by

using the characteristics of Kolmogorov–Smirnov (K-S) distance, Kullback–Leibler (K-L) Divergence, and regularity of the constellation point. However, there is no quantitative analysis of the detection accuracy, and no effective detection scheme for the WCC-MC signal is proposed. It is increasingly difficult to identify wireless covert channel hiding techniques used constellation modulation in this era of great advancement in technology.

With the development of wireless physical layer covert channels, secret information and even confidential information are at risk of leakage. When hiding information on upper layers, only a few changes are possible, and firewalls can easily detect most types of changes. In contrast, WCC-P schemes [15, 16] contain a high amount of noise and random signal variations. These make the wireless covert channel easier to implement, and this covert channel has a low probability of detection (LPD) [17–20]. This paper concerns the problem of detecting the WCC-MC covert channel, which is an important component of the WCC-P covert channel. Such detection scheme can be used to detect information leakage behavior caused by WCC-MC schemes.

The detection scheme based on deep learning has achieved good results in many fields. Convolutional Neural Network (CNN), as one of the representative algorithms of deep learning, is widely used in image processing problems. It excels in many aspects such as target recognition, speech recognition, and natural language processing. The CNN has the characteristics of local perception, weight-sharing, and subsampling, which can achieve higher performance at a lower cost. In deep learning, the convolutional neural network (CNN) [21] plays a leading role in dealing with problems related to vision. The modern structure of CNNs was firstly introduced in [22] and refined in [23, 24]. Researchers improved it and designed a multilayer artificial neural network LeNet-5, which has excellent applications for handwritten digit classification [25]. To the best of our knowledge, this model is not used before for the WCC-MC signal detection.

The purpose of this paper is to detect and classify WCC-MC signals. We convert the amplitude-phase characteristics of EVM signal and constellation points into the EVM grayscale feature image and constellation feature image. These feature images are used for deep learning model training and detection. Under different channel noise intensities, the adjusted convolutional neural network (CNN-T) is used to train and classify legitimate communication signals and WCC-MC communication signals with different embedding rates, based on the difference between the constellation diagrams of legitimate communication and covert communication. Dutta et al. [13] proposed a WCC-MC scheme with a dirty constellation (WCC-DC) that uses existing modulation schemes of OFDM. The covert messages are hidden within “dirty” constellations that mimic noise commonly imposed by hardware imperfections and channel conditions. In this paper, we use the proposed scheme for detecting and classifying WCC-DC communication signal, which is difficult to detect in the WCC-MC schemes, to verify the effectiveness of the scheme. This paper’s contributions can be summarized as follows:

- (1) A detection and classification scheme is proposed for WCC-MC signal based on deep learning, which uses the amplitude and phase characteristics of EVM and constellation points.
- (2) The amplitude-phase characteristics of EVM signal and constellation points will be converted into grayscale feature images. The input layer of the CNN-T network is adjusted to train and test the EVM feature image and the constellation feature image at the same time.
- (3) In this paper, the legitimate communication signal and covert signal are collected at the platform of software radio, and the proposed scheme is used to effectively detect and classify the WCC-MC signal.

The remainder of the paper is structured as follows. Section 2 introduces the background and related work for our work. Section 3 describes characteristic extraction, CNN design, and detection process. Section 4 shows the simulation and experiment results of applying our scheme and the advantages of our algorithm compared to other schemes. Section 5 concludes the paper and discusses directions for our future work.

2. Background and Related Work

This section first detailed introduces the WCC-DC covert channel to be detected in this paper. Then, we summarize the existing covert channel detection schemes.

2.1. Wireless Covert Channel with Dirty Constellation. Wireless covert channels are an existing technology used to hide and leak information through wireless networks [26]. Because the ubiquitous wireless devices and wireless communication signals make the wireless covert communication possible, the wireless covert channel attracts more and more attention. In the WCC-MC communication schemes, the secret message bit can be transmitted as the constellation error of legitimate signal to realize the transmission of secret information. Dutta et al. [13] used a more straightforward technique that uses existing modulation schemes of OFDM.

The information is hidden within “dirty” constellations that mimics noise commonly imposed by hardware imperfections and channel conditions. The hidden information is embedded in the covert subcarriers by modifying the position of the constellation points at the transmitter. For the uninformed user, the secret constellation points will be treated as random channel noise. Taking Quadrature Phase Shift Keying (QPSK) modulation as an example, the legitimate constellation modulation is shown in Figure 1(a).

For the covert subcarriers, the mapping sequence bits are checked after the hidden information is modulated by the QPSK constellation. The mapping sequence bits shared between the transmitter and receiver are used to select the appropriate mapping for covert and cover subcarriers. To embed the hidden information, the positions of the constellation points for the covert subcarriers are modified. Figure 2(b) corresponds to the upper right quadrant of the

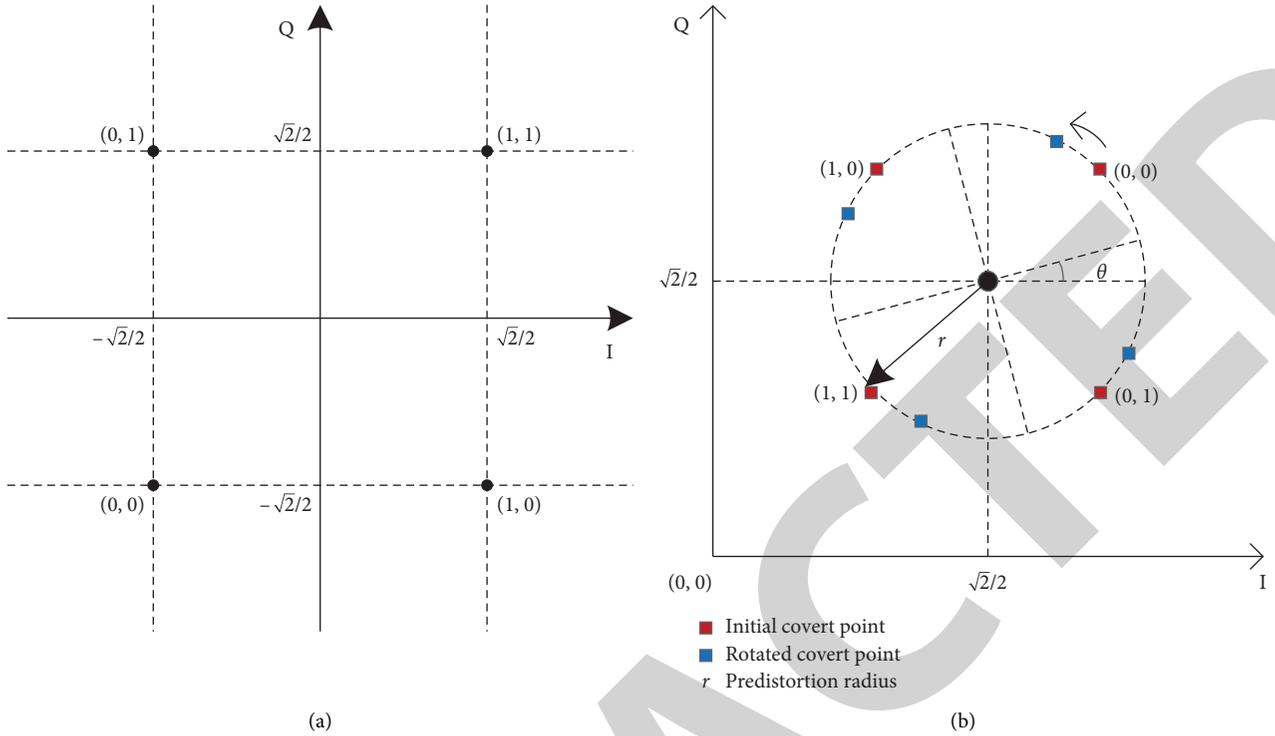


FIGURE 1: The constellation points of legitimate and WCC-DC signal. (a) Legitimate signal. (b) WCC-DC signal.

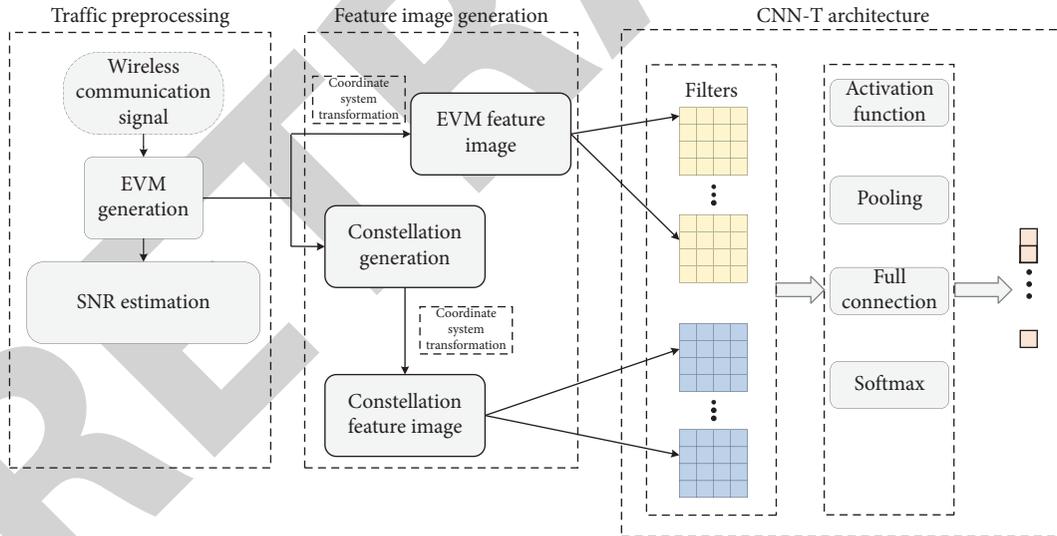


FIGURE 2: The WCC-MC signal detection framework architecture.

constellations of the QPSK constellation shown in Figure 2(a). Firstly, the constellation points are moved from the original position to the red dot according to the hidden information. As shown in Figure 2(b), the dispersion of covert constellation points is limited to a radius of θ , which is a distance equal to that of a 64 Quadrature Amplitude Modulation (64QAM) constellation. The red dot represents the initial covert constellation point and the constellation

points are modulated to the blue dot by rotating the axis. The rotation is performed with a monotonically increasing rotation angle θ ; the transmitter and receiver both start with $\theta = 0^\circ$ at the start of the packet and increment θ for each covert subcarrier.

For the cover subcarriers, the random noise (Meet Gaussian distribution in the in-phase and quadrature (I/Q) vectors) is added to the original constellation points. To

make the modulation points of the secret information closer to hardware imperfections and channel conditions and avoid sudden changes in the modulation characteristics.

2.2. Wireless Covert Channel Detection Approaches. The purpose of covert channel detection is to distinguish covert communication signals from legitimate communication signals. However, as far as we know, there is no special work to realize the detection of the WCC-MC signal. In the field of signal analysis, the difference between two signals can be measured in the frequency domain and time domain. Kolmogorov–Smirnov (K-S) test [12] and regularization test [2] in the wireless covert channel are proposed to measure the difference between covert and cover signals from the aspect of distribution characteristics. The correlation of the time domain signal [14] is used to realize the effective detection of the WCC-MP signal. The detection of the covert channel is realized mainly by studying the time sequence of communication signal arrival and the temporal correlation of signal. In [2], the author uses a flat metric of a standard deviation metric to determine the existence of a covert timing channel. On the other hand, the author uses entropy as a measure in [27] to detect covert timing channels. Entropy provides important evidence for the existence of patterns within the data, the presence of signals with high probability in covert channels.

In general, the detection of covert channels uses statistical tests to differentiate covert traffic from legitimate traffic. These include standard deviation, mean, entropy, regularity, and median. In the current literature, the support vector machine (SVM) [28, 29] has been viewed as an efficient and stable scheme for covert channel classification tasks. SVM attempts to separate different types of data by learning the best decision hyperplane which best separates training samples in the high-dimensional feature space (implemented with different kernel functions). Neural networks (NN), such as multilayer perceptron (MLP) [30, 31] neural networks, have already been investigated for the classification of remote sensing data.

3. Methodology

This section describes the details of the designed framework as well as the methods used aiming at detecting and classifying the WCC-MC signal.

3.1. Framework Architecture. The proposed framework is shown in Figure 2. We propose a three-stage approach to detect and classify the WCC-P signal based on the amplitude-phase feature images and adjusted CNN. The first block is traffic preprocessing, including the EVM generation and SNR estimate. Without further processing, the generated EVM data is fed to the next block for amplitude-phase feature image generation. During feature image generation, the EVM amplitude-phase feature image and constellation amplitude-phase feature image are generated with the EVM signal. Then these feature images will be subject to statistical computations which will be fed to the final block (deep

neural network) for training/testing purposes and eventually WCC-MC signal classification (detection). In the rest of this section, we describe in detail the process for WCC-MC detection.

3.2. WCC-MC Signal Detection Process. This process starts with the collection of a large number of data streams between the transmitter and receiver entities. Following the step, a flow set is created based on different channel noise intensity, which contains legitimate communication signals and covert communication signals under different embedding rates. Each flow is then divided into small subflows; each one has N constellation points. The constellation points are converted into EVM amplitude-phase feature image and adjusted constellation amplitude-phase feature image. Finally, the feature images are fed to the deep neural network which trains the model and tests the performance of that model.

3.3. Traffic Preprocessing. In this paper, we assume that the detector can demodulate the cover message. As shown in Figure 3, The EVM signal can be expressed as

$$\text{EVM} = R^I + j \cdot R^Q - (D^I + j \cdot D^Q) = E^I + j \cdot E^Q, \quad (1)$$

where $R^I + j \cdot R^Q$ is the received constellation points and $D^I + j \cdot D^Q$ is the QPSK demodulation result of the communication signal.

Besides, considering the received constellation points, there will be a small number of constellation points with large deviation; we will exclude these points in EVM statistics of constellation points. We select the circular region as shown in Figure 4, so that the constellation points that fall in the box account for 99% of the total constellation points and discard the other 1% possible error signals.

Due to the different signal-to-noise ratios (SNRs), the EVM signals received by the detector are significantly different, which leads to the amplitude-phase characteristic difference of the constellation points generated under different SNR conditions even for the legitimate communication signals. Therefore, we need to train the samples under different SNR conditions in the CNN training process. We can estimate the signal-to-noise ratio of EVM signal by the following equation:

$$\text{psnr} = \text{round} \left[10 * \lg \left(\frac{N}{\sum_{i=1}^N |EVM_i|^2} \right) \right], \quad (2)$$

where N is the number of EVM data. $\text{round}[\cdot]$ is the nearest integer function. A small error of SNR has little influence on the feature images. To facilitate statistics, we do a rounding operation when estimating SNR.

3.4. Gray Scale Image Generation. For the scheme of wireless covert communication based on constellation modulation, there is a difference between the amplitude-phase characteristic of covert communication and that of legitimate communication due to the regular change of constellation

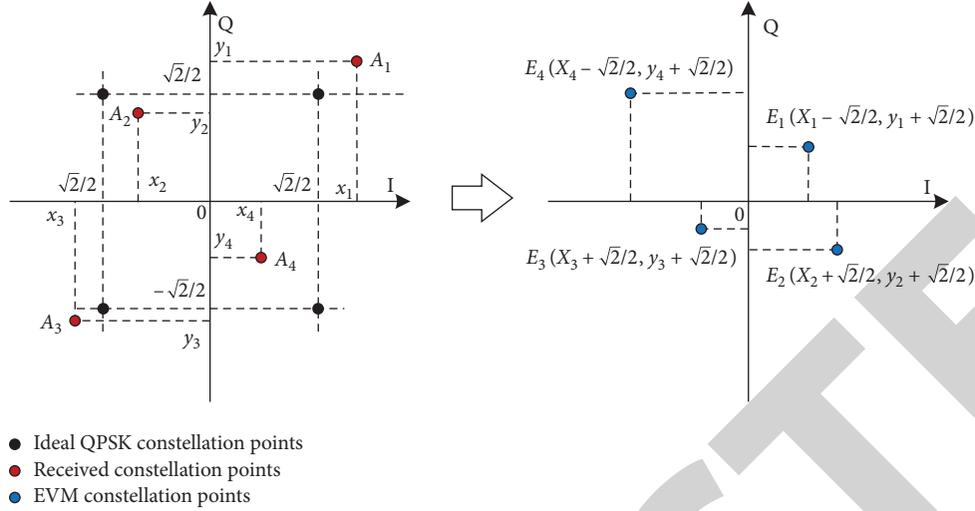


FIGURE 3: Schematic diagram of receiving constellation diagram converted to EVM constellation diagram.

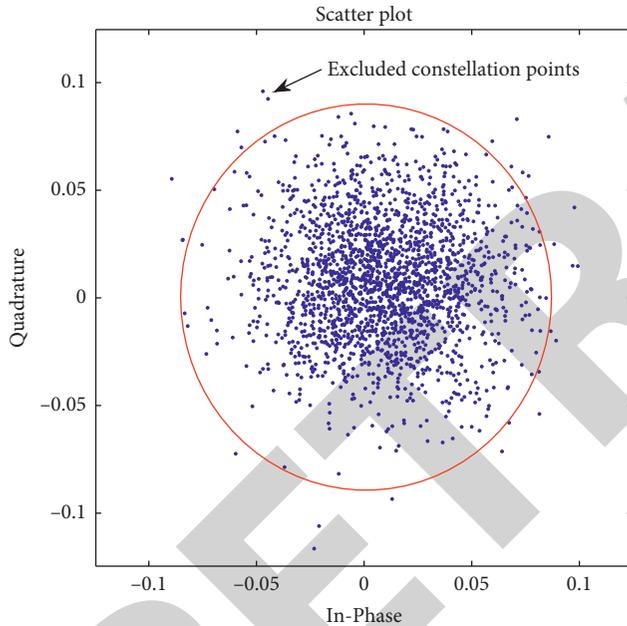


FIGURE 4: Selection of constellation points for EVM computing.

points in the process of modulation. For the WCC-MC scheme, the secret messages are embedded by moving the legitimate constellation points regularly, so that there are constellation points with certain distribution around the legitimate constellation points. In this paper, we use a certain distribution to implement WCC-MC detection through a deep learning network, although these distributions will be weakened in the process of wireless signal transmission. The difference between legitimate communication and WCC-MC communication is mainly reflected in the amplitude and phase of constellation points. To extract the distribution characteristics of the constellation diagram, we convert the received constellation diagram into the EVM constellation diagram and the adjusted constellation diagram to generate amplitude-phase feature images, respectively.

3.4.1. EVM Constellation Diagram Amplitude-Phase Characteristic Extraction. For the amplitude characteristics, the EVM signal can be defined as the difference between the actual observed constellation point and the ideal constellation point in the process of wireless communication. The dispersion degree of the EVM signal in the covert constellation is different from that in the legitimate constellation due to the movement of constellation points with the WCC-MC scheme. The amplitude and phase values of the EVM signal are extracted with

$$r_i = \sqrt{|\text{real}(\text{evm}_i)|^2 + |\text{imag}(\text{evm}_i)|^2}, \quad (3)$$

$$\varphi_i = \arctan\left(\frac{\text{imag}(\text{evm}_i)}{\text{real}(\text{evm}_i)}\right), \quad (4)$$

where $\text{real}(\cdot)$ represents the real value extractor; $\text{imag}(\cdot)$ represents the imaginary value extractor; r_i is the amplitude value of constellation point, and φ_i is the phase value of constellation point. We use the phase as abscissa and the amplitude as ordinate to establish a phase-amplitude coordinate system. As shown in Figure 5, the EVM constellation points in the rectangular coordinate system are transferred to the phase-amplitude coordinate system.

In this paper, QPSK modulation is taken as an example to extract EVM signal, which is the same as that of other modulation schemes. The phase-amplitude coordinate in the range is divided into 32×32 small areas, the size of each small area is $(\max(\Phi)/32) \times (\max(R)/32)$. The number of constellation coordinates in each region is counted and normalized to obtain a characteristic matrix N . $n_{ij} = (e_{ij}/\max(E)) \in N$ is the element of the characteristic matrix, where $i, j = 1, 2, \dots, 32$ and $e_{ij} \in E$ is the number of constellation points in the small area in row i and column j .

3.4.2. Adjusted Constellation Diagram Amplitude-Phase Characteristic Extraction. In this section, we analyze the amplitude and phase characteristics of the adjusted

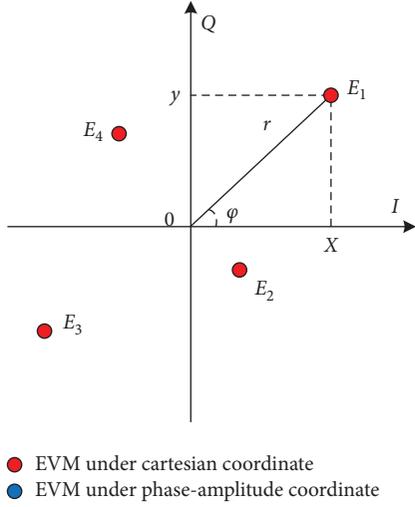


FIGURE 5: The amplitude and phase values extraction of EVM signal.

constellation points. As shown in Figure 6, we add a fixed signal $((\sqrt{2}/2) + j \cdot (\sqrt{2}/2))$ to the EVM signal; it is equivalent to transferring the received constellation diagram to the first quadrant. The amplitude and phase values of adjusted constellation points are extracted with

$$d_i = \sqrt{|\text{real}(\text{evm}_i) + \frac{\sqrt{2}}{2}|^2 + |\text{imag}(\text{evm}_i) + \frac{\sqrt{2}}{2}|^2}, \quad (5)$$

$$\theta_i = \arctan\left(\frac{\text{imag}(\text{evm}_i) + (\sqrt{2}/2)}{\text{real}(\text{evm}_i) + (\sqrt{2}/2)}\right). \quad (6)$$

Similar to the amplitude and phase values extraction of EVM signal, the adjusted constellation points in the rectangular coordinate system are transferred to the phase-amplitude coordinate system. The phase-amplitude coordinate in the range is divided into 32×32 small areas (the size of each small area is $(\max(\Theta)/32) \times (\max(D)/32)$) to get the normalized characteristic matrix M . $m_{ij} = (a_{ij}/\max(A))$ is the element of the characteristic matrix M , where $i, j = 1, 2, \dots, 32$ and $a_{ij} \in A$ is the number of constellation points in the small area in row i and column j .

3.4.3. Amplitude-Phase Feature Image Generation. As shown in Figure 7, the two different grayscale image samples formed by gray-scale mapping of the wireless signal of the physical layer are obtained, and the two grayscale images are used for training and testing of the network model.

To classify wireless signals using constellation characteristics, we transform the constellation characteristics into 32×32 pixel gray images according to the image format. We deal with each element in the characteristic matrix corresponding to a normalized gray pixel value in the image.

3.5. Detection and Classification with Adjusted CNN. CNN was originally used for image classification and recognition because its structure is very suitable for extracting

pixel-level characteristics from 2D images. Therefore, CNN can extract complex characteristics automatically by the convolution layer containing multiple filters. The CNN-T used in this paper is shown in Figure 8.

The input layer is the data front end of the whole neural network, that is, the image to be trained. The input layer images are processed to a size of 32×32 ; the preprocessed images are shown in Section 3.4 which includes the EVM feature image and adjusted constellation feature image. The number of each type of image in each input layer can be adjusted, and the adjustment parameter is called batch size. In our experiment, we set the batch size to 128; that is, 128 EVM feature image and 128 adjusted constellation feature image are input each time for training, mainly for two reasons: (1) the memory of the machine can be used reasonably; (2) the algorithm converges within the set number of iterations. Besides, the time complexity is optimal [32, 33].

The convolution layer is the local perception characteristic of the image, which is the characteristic perception of each part of the image, and then carries out a higher-level comprehensive operation to obtain the global information. The purpose of this operation, as shown in (7), is to reduce the calculation parameters of the model:

$$z_{(i,j)}^{l,t} = \begin{cases} \sum_{i=1}^m \sum_{j=1}^n x_{(i+p,j+q)}^t \odot k^l, & 1 \leq l \leq \frac{L}{2}, \\ \sum_{i=1}^m \sum_{j=1}^n y_{(i+p,j+q)}^t \odot k^l, & \frac{L}{2} < l \leq L, \end{cases} \quad (7)$$

where $t = 1, 2, \dots, T$, T represents the batch size; $l = 1, 2, \dots, L$, L represents the number of the filter; $z_{(i,j)}^{l,t}$ is the (i, j) element of the l -th feature map with the size of $m \times n$ for the t -th group feature maps; k^l is the convolution kernel coefficient of the l -th filter with the size of $p \times q$; x represents the grayscale value of the EVM feature image; and y represents the grayscale value of the adjusted constellation feature image.

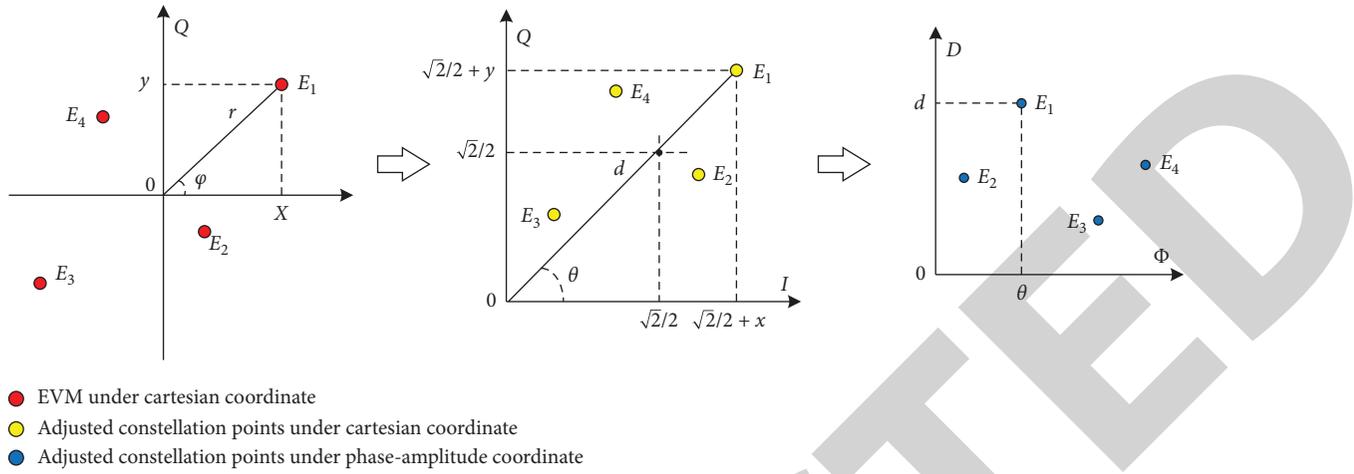


FIGURE 6: The amplitude and phase values extraction of adjusted constellation points.

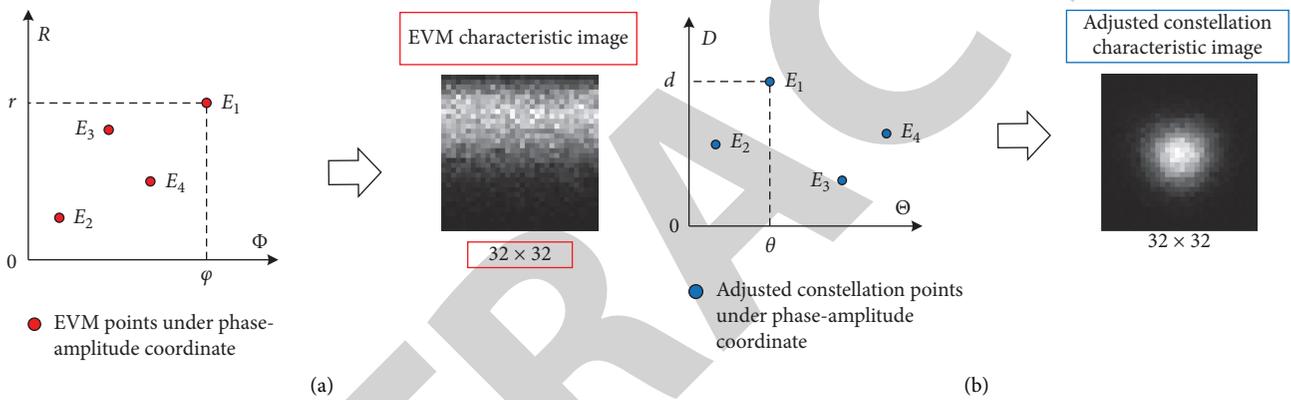


FIGURE 7: The amplitude and phase values extraction of adjusted constellation points.

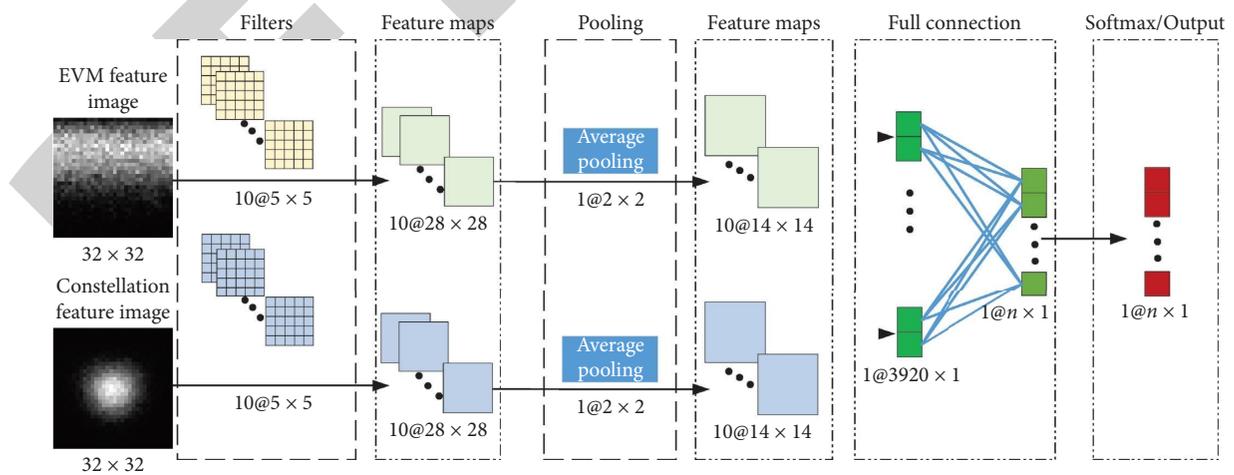


FIGURE 8: The architecture of the proposed CNN-T classifier.

The pooling layer is mainly used for feature dimension reduction, compressing the number of data and parameters, reducing overfitting, and improving the fault tolerance of the model. The algorithm is shown as

$$D_{(u,v)}^{l,t} = \begin{bmatrix} d_{((u-1)*g+1,(v-1)*h+1)}^{l,t} & \cdots & d_{((u-1)*g+1,v*h)}^{l,t} \\ \vdots & \ddots & \vdots \\ d_{(u*g,(v-1)*h+1)}^{l,t} & \cdots & d_{(u*g,v*h)}^{l,t} \end{bmatrix}, \quad (8)$$

$$p_{(u,v)}^{l,t} = \text{average}(D_{(u,v)}^{l,t}) \quad (9)$$

where $d^{l,t} = \sigma(z^{l,t})$ is the input of pooling layer, $p^{l,t}$ is the output, and $g \times h$ is the size of pooling size.

The full connection and softmax layer play the role of "Classifier" in the whole convolutional neural network. Each node of the full connection layer is connected with each node of the upper layer, which integrates the output characteristics of the previous layer. The algorithm for this step is

$$\begin{bmatrix} o_{(1,1)} & \cdots & o_{(1,T)} \\ \vdots & \ddots & \vdots \\ o_{(n,1)} & \cdots & o_{(n,T)} \end{bmatrix} = \begin{bmatrix} W_{11} & \cdots & W_{1m} \\ \vdots & \ddots & \vdots \\ W_{n1} & \cdots & W_{nm} \end{bmatrix} * \begin{bmatrix} h_{(1,1)} & \cdots & h_{(1,T)} \\ \vdots & \ddots & \vdots \\ h_{(m,1)} & \cdots & h_{(m,T)} \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}, \quad (10)$$

$$\begin{bmatrix} a_{(1,1)} & \cdots & a_{(1,T)} \\ \vdots & \ddots & \vdots \\ a_{(n,1)} & \cdots & a_{(n,T)} \end{bmatrix} = \begin{bmatrix} \frac{\exp(o_{(1,1)})}{\sum_{i=1}^n \exp(o_{(i,1)})} & \cdots & \frac{\exp(o_{(1,T)})}{\sum_{i=1}^n \exp(o_{(i,T)})} \\ \vdots & \ddots & \vdots \\ \frac{\exp(o_{(n,1)})}{\sum_{i=1}^n \exp(o_{(i,1)})} & \cdots & \frac{\exp(o_{(n,T)})}{\sum_{i=1}^n \exp(o_{(i,T)})} \end{bmatrix}, \quad (11)$$

where h is the input of the full connection layer, a is the output of the softmax layer and W and b represent the weight value and bias value.

The backpropagation algorithm [34] can be divided into two parts: error calculation and parameter gradient calculation. For the feature map generated by each layer, we calculate an error to show the difference between the result calculated by this layer and the correct result it should give. For the feature map generated by each layer, we calculate an error to show the difference between the result calculated by each layer and the desired result it should give. The errors of all layers are as follows:

$$\Delta S_{(p,q)} = a_{(p,q)} - y_{(p,q)}, \quad (12)$$

$$\Delta P_{(u,v)}^{l,t} = \text{resample}(W^T * \Delta S), \quad (13)$$

$$\Delta K_{(i,j)}^{l,t} = \text{upsample}(\Delta P) \odot \sigma'(z_{(i,j)}^{l,t}), \quad (14)$$

where ΔS is the error of softmax layer, ΔP is pooling layer, and ΔK is convolution layer.

The parameter gradients of all layers are as follows:

$$\text{Wd_grad} = \frac{1}{T} \Delta S * h^T, \quad (15)$$

$$\text{bd_grad} = \frac{1}{T} \sum_{q=1}^T \Delta S_{(p,q)}, \quad (16)$$

$$\text{Wc_grad}^l = \begin{cases} \frac{1}{T} \sum_{t=1}^T x \otimes \text{ROT180}(\Delta K_{(i,j)}^{l,t}), & 1 \leq l \leq \frac{L}{2}, \\ \frac{1}{T} \sum_{t=1}^T y \otimes \text{ROT180}(\Delta K_{(i,j)}^{l,t}), & \frac{L}{2} < l \leq L, \end{cases} \quad (17)$$

$$\text{bc_grad}^l = \frac{1}{T} \sum_{t=1}^T \sum_{i,j} \Delta K_{(i,j)}^{l,t}, \quad (18)$$

where Wd_grad and bd_grad are the gradients of weight and bias for full connection layer and Wc_grad and bc_grad are the gradients of weight and bias for convolution layer.

4. Experiment and Simulation

In this section, we validate the effectiveness of our proposed approach through a series of simulations and experiments. All trainable parameters in our CNN-T are initialized to random values between -0.05 and 0.05 . The effectiveness of the proposed scheme for detecting WCC-MC signals is verified by detecting and classifying WCC-DC (the classic scheme of WCC-MC) signals. The test in this paper is divided into two steps: WCC-DC signal detection and WCC-DC signal classification under different embedding rates and SNRs. The purpose of the detection test is to distinguish WCC-DC traffic from legitimate traffic. The classification

test is to classify WCC-DC signals with different embedding rates.

To evaluate the detection effectiveness of the proposed scheme, the following terms are used for determining the quality of the classification models:

- (1) True positive (TP), the number of WCC-DC samples correctly classified to the covert class
- (2) True negative (TN), the number of legitimate samples correctly classified to the legitimate class
- (3) False positive (FP), the number of legitimate samples wrongly classified to the covert class
- (4) False negative (FN), the number of WCC-DC samples wrongly classified to the legitimate class

Based on the aforementioned terms, the following most commonly used evaluation metrics are considered.

Accuracy estimates the ratio of the correctly recognized wireless communication samples to the entire test dataset:

$$\text{accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (19)$$

Precision estimates the ratio of the correctly identified WCC-DC samples to the total number of samples classified to covert class. It is denoted as

$$\text{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (20)$$

Recall estimates the ratio of the correctly identified WCC-DC samples to the number of all WCC-DC samples. It is denoted as

$$\text{recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (21)$$

F1-Score is the harmonic mean of Precision and Recall. It is denoted as

$$F_{1\text{-score}} = 2 \times \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}} \quad (22)$$

4.1. Simulation Analysis

4.1.1. Establishment of Simulation Database. Due to the influence of channel noise on the generated feature image, the accuracy of detection results will be affected. Therefore, we set up data samples under different SNRs. We can estimate the SNR with the EVM signal by (2).

As shown in Figure 9, for each SNR, we generate a positive sample set P_s (legitimate communication sample) and a negative sample set N_s (WCC-DC communication sample), where P_s is the set of positive samples when the SNR is s . $P_s = P_s^{\text{tr}} \cup P_s^{\text{te}}$, P_s^{tr} is the set of positive samples for training; P_s^{te} is the set of positive samples for test. N_s is the set of negative samples when the SNR is s . $N_s = N_s^{\text{tr}} \cup N_s^{\text{te}}$, N_s^{tr} is the negative sample set used for training; N_s^{te} is the set of negative samples for test. The training set with SNR of s is $TR_s = P_s^{\text{tr}} \cup N_s^{\text{tr}}$; the test set is $TE_s = P_s^{\text{te}} \cup N_s^{\text{te}}$.

4.1.2. Simulation Setup. We use MATLAB software to verify our proposed scheme, and the wireless communication is set on the 802.11a/g physical layer. There are 48 subcarriers in the symbols being transmitted. In the simulation experiment, the high throughput group (TGn) channel model and the Gaussian noise (AWGN) channel model were selected as the wireless channel model [21]. The TGn channel models B selected for the simulation experiment on the 802.11a/g PHY layer is universal, and the receivers of the transmitter and the informer remain static. Therefore, the Doppler shift of wireless communication can be ignored.

Different channel noise intensity will have a great impact on the characteristic picture, so in the simulation, we mainly study the influence of channel noise (SNR) on the detection and classification effect. Under each group of different SNRs, the simulation samples possessed include the following sets:

(1) *Samples of Covert Communication Signals.* 10000 sets of WCC-DC signal samples with the embedding rate of 10%; 10000 sets of WCC-DC signal samples with the embedding rate of 20%; 10000 sets of WCC-DC signal samples with the embedding rate of 30%.

(2) *Sample of Legitimate Communication Signal.* 10000 sets of legitimate communication samples with OFDM modulation.

Among the 10000 sets of samples of various types, 7000 sets of samples are used as training samples, and the remaining 3000 sets are used for detection and classification. Each sample contains 2080 constellation points.

4.1.3. Simulation Result. In the following chapters, simulation experiments are used to verify the detection and classification effects of the proposed scheme on WCC-DC communication signals under AWGN and TGn-B channels.

(1) *Detection Result under AWGN Channel.* To verify the effectiveness of the proposed scheme, we implement the detection of WCC-DC signals with different embedding rates in the AWGN channel model. As shown in Figure 10, it is apparent that the reliability of the proposed scheme is influenced by the SNR and the embedding rate. With the improvement of SNR, the proposed scheme has more accurate detection results and our scheme has a higher detection rate for WCC-DC signals with a higher embedding rate.

(2) *Detection Result under TGn-B Channel.* Similar to the simulation test in the AWGN channel, we detect the wireless communication signal under the TGn-B channel with the proposed scheme. Figure 11 shows the detection results of the proposed scheme for WCC-DC signals with different embedding rates under different SNRs. It is consistent with the simulation results in the AWGN channel, with the improvement of SNR and embedding rate, the proposed scheme can achieve a higher detection rate. However, the detection accuracy is lower than that in the AWGN channel due to the complexity of the TGn-B channel.

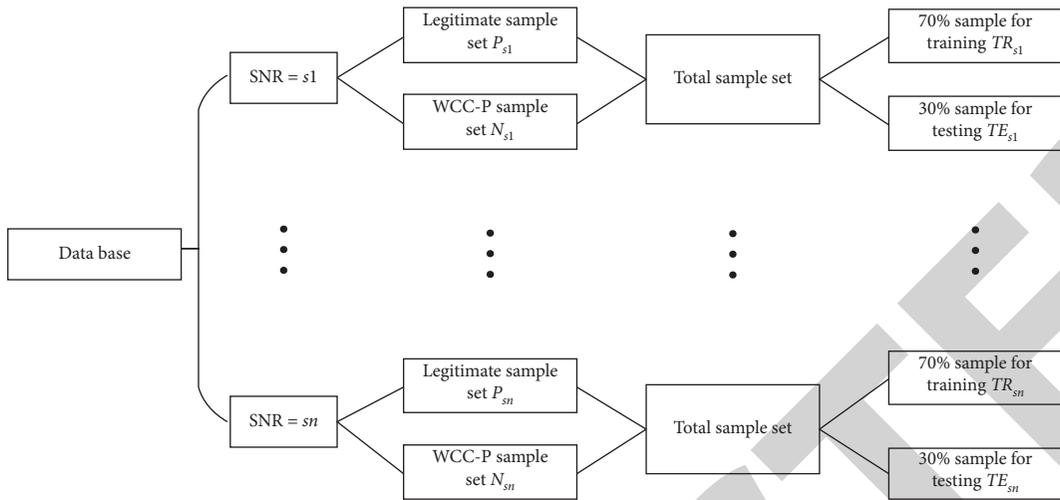


FIGURE 9: Establishment of the simulation database.

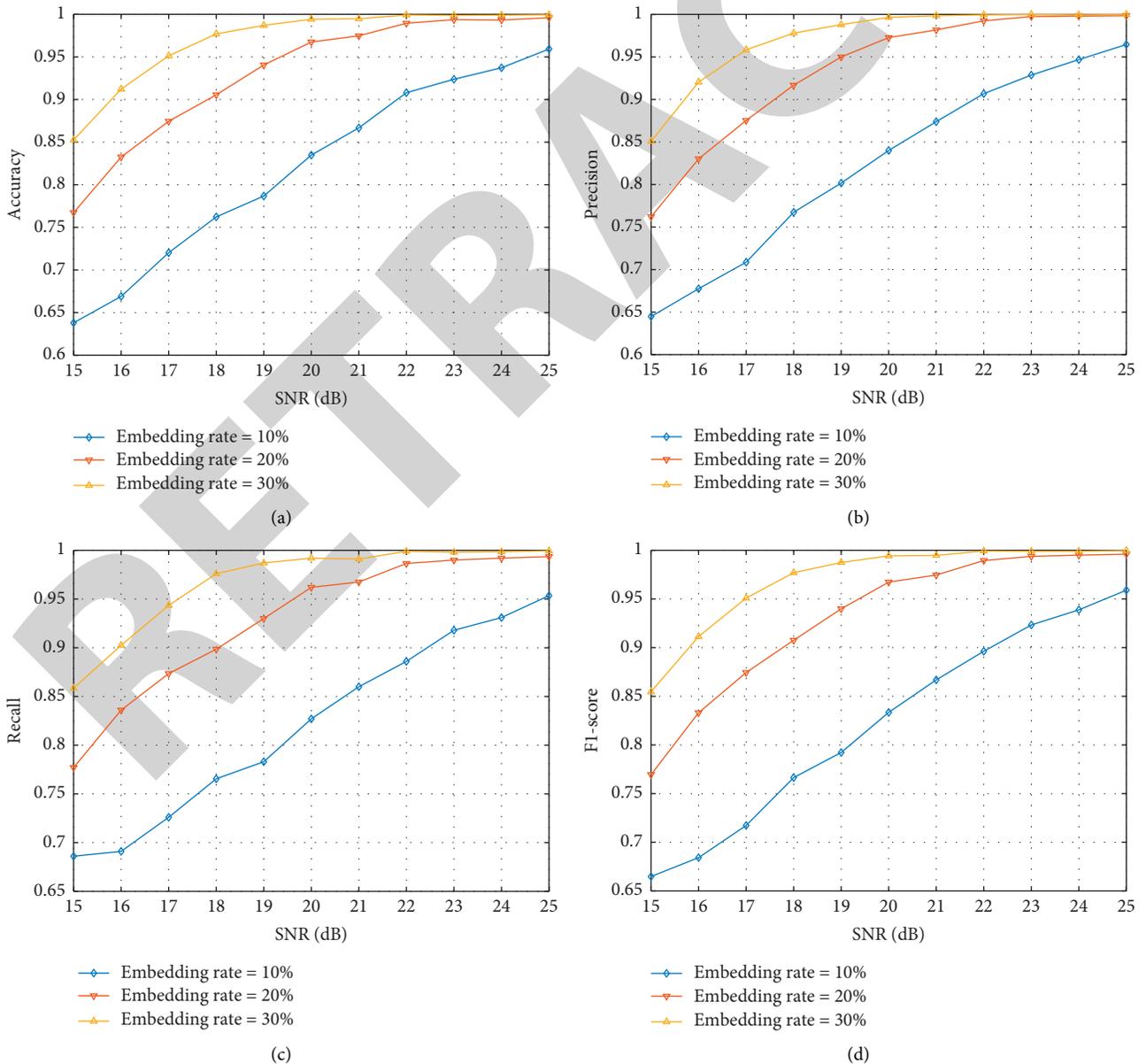


FIGURE 10: Detection result for the WCC-DC signal under AWGN channel: (a) Accuracy, (b) Precision, (c) Recall, and (d) F1-Score.

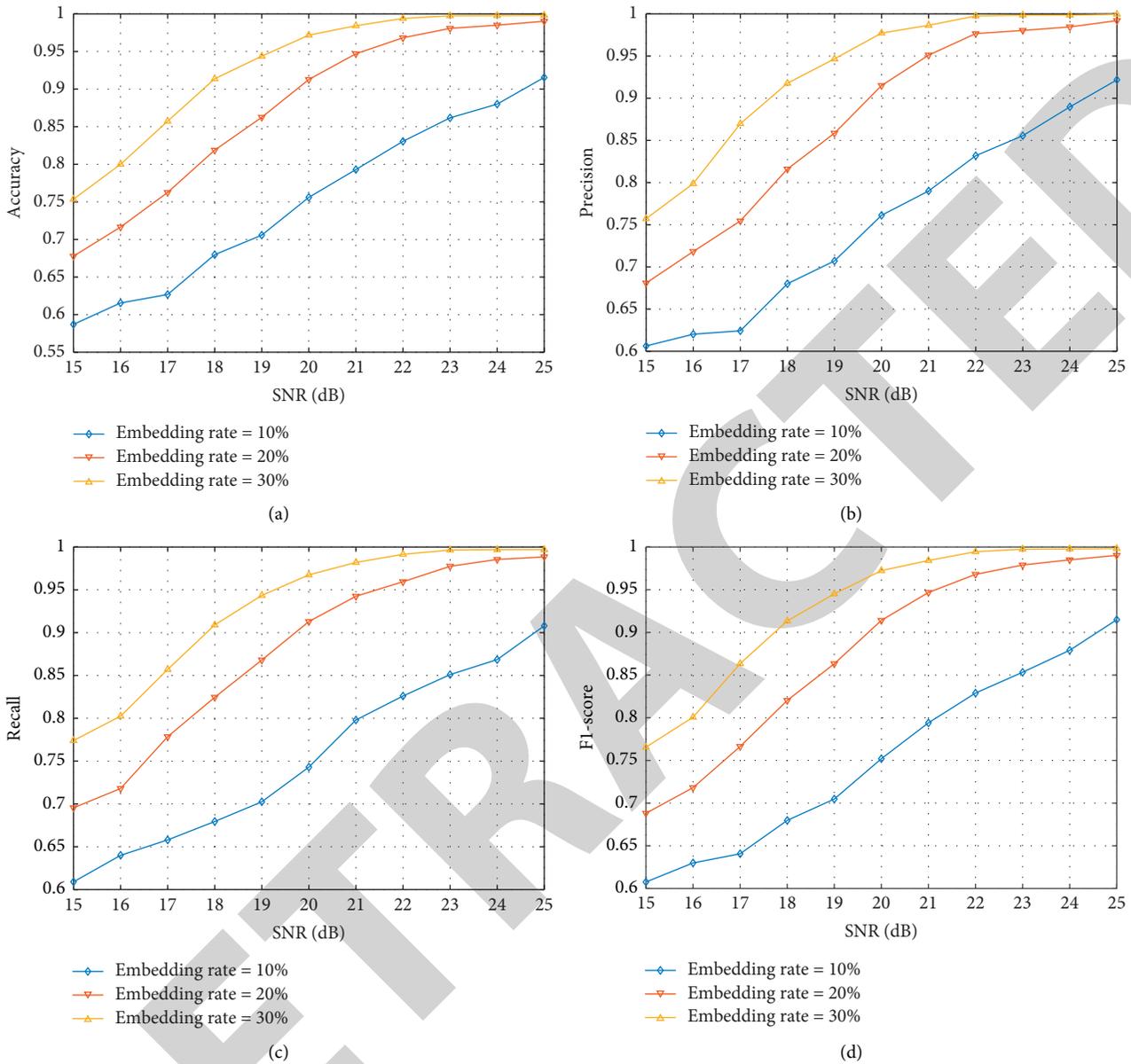


FIGURE 11: Detection result for the WCC-DC signal under TGn-B channel: (a) Accuracy, (b) Precision, (c) Recall, and (d) F1-Score.

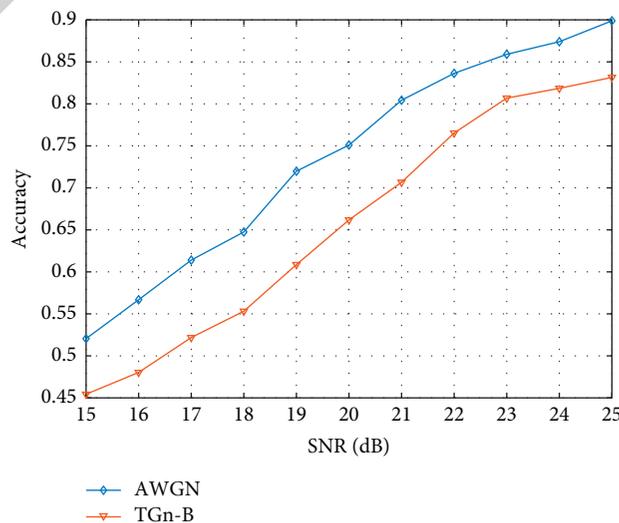


FIGURE 12: Classification result for the WCC-DC signal under AWGN and TGn-B channel.

(3) *Classification Result.* In this section, we use the proposed scheme to classify WCC-DC signals with different embedding rates. Figure 12 shows the classification results of the proposed scheme for WCC-DC signals under different channel models and SNRs. The horizontal axis denotes the SNR and the vertical axis denotes the corresponding classification accuracy. As shown in Figure 12, the classification accuracy of the proposed scheme can achieve 80% when SNR = 23 dB for both types of channel models.

4.2. Experiment Analysis

4.2.1. *Experimental Setup.* The experiment data set used in this paper is based on the Long-Term Evolution (LTE) communication system for physical layer wireless covert channel construction and wireless signal acquisition. The whole wireless communication system is divided into transmitting and receiving sides. Both sides use Universal Software Radio Peripheral (USRP) b210 as the LTE base station, and the two LTE workstations are connected to a PC, respectively. The PC is equipped with Linux Ubuntu 16.04 and the CPU processor is Intel Core i7. The operating frequency is 2.685 GHz, the bandwidth is 5 MHz, and the modulation mode is set to QPSK. The samples possessed include the following sets:

(1) *Samples of Covert Communication Signals.* 13000 sets of WCC-DC signal samples with the embedding rate of 10%, 13000 sets of WCC-DC signal samples with the embedding rate of 20%, and 13000 sets of WCC-DC signal samples with the embedding rate of 30%.

(2) *Sample of Legitimate Communication Signal.* 13000 sets of legitimate communication samples with OFDM modulation.

Among the 13000 sets of samples of various types, 10000 sets of samples are used as training samples, and the remaining 3000 sets are used for detection and classification. Each sample contains 2080 constellation points.

4.2.2. *Experimental Result.* In the following chapters, we use the data received by the radio platform to verify the detection and classification performance of the proposed scheme on WCC-DC communication signals.

(1) *Detection Result.* The detailed description of detection performance indexes of different detection schemes is shown in Table 1. CNN-T represents the proposed scheme in this paper; K-S-A-P represents the K-S test with the amplitude-phase characteristic; K-S-A represents the K-S test with the amplitude characteristic; K-S-P represents the K-S test with the phase characteristic. Label 0-1 represents the detection for the WCC-DC signal with the embedding rate of 10%. Label 0-2 is the detection for the WCC-DC signal with the embedding rate of 20%. Label 0-3 is the detection for the WCC-DC signal with the embedding rate of 30%. In the K-S test, we measured the K-S distance between the tested sample and the legitimate sample. Thus, if the test score is

TABLE 1: Detection performance of different detection schemes.

		Label 0-1	Label 0-2	Label 0-3
CNN-T	Accuracy	0.9859	0.9937	0.9968
	Precision	0.9898	0.9954	0.9969
	Recall	0.9820	0.9921	0.9968
	F1-score	0.9859	0.9937	0.9968
K-S-A-P	Accuracy	0.9453	0.9623	0.9877
	Precision	0.9532	0.9727	0.9900
	Recall	0.9367	0.9513	0.9853
	F1-score	0.9449	0.9619	0.9876
K-S-A	Accuracy	0.9400	0.9613	0.9867
	Precision	0.9496	0.9714	0.9899
	Recall	0.9293	0.9507	0.9833
	F1-score	0.9392	0.9609	0.9866
K-S-P	Accuracy	0.5250	0.5600	0.6837
	Precision	0.5328	0.5777	0.7033
	Recall	0.4067	0.4460	0.6353
	F1-score	0.4613	0.5034	0.6676

TABLE 2: Classification performance of different classification schemes.

	CNN-T	K-S-A-P	K-S-A	K-S-P
Label 1-2-3	0.81736	0.652	0.6489	0.4649

small, it indicates that the sample under test is close to legitimate behavior. However, if the sample does not fit well into the legitimate behavior, the test score will be large, indicating the possible presence of WCC-P communication signals.

As shown in Table 1, the proposed scheme (CNN-T) has the highest detection performance among all detection schemes. The detection accuracy for the WCC-DC signal with the 10% embedding rate is more than 98.5%, while the accuracy of the K-S test (K-S-A-P, K-S-A, K-S-P) can only reach 94.53%.

(2) *Classification Result.* In this section, we use the WCC-DC signals with different embedding rates received by the radio platform to verify the reliability of our proposed scheme for WCC-DC signal classification and compare it with other classification schemes. Label 1-2-3 represents the classification for the WCC-DC signal with the embedding rates of 10%, 20%, and 30%. As shown in Table 2, the proposed scheme has the best classification result, which has over 81.7% classification accuracy for Label 1-2-3. In contrast, the K-S test (K-S-A-P, K-S-A, K-S-P) has only 65.2% classification accuracy.

5. Conclusions

In this paper, we have proposed a detection scheme based on a convolutional neural network for the wireless covert channel with the modulation of the constellation points (WCC-MC). We use the difference of amplitude and phase characteristics between the WCC-MC scheme and legitimate communication constellation points to realize the detection and classification of the WCC-MC signal. By

extracting the amplitude and phase characteristics of the EVM signal and constellation points, we transform them into grayscale images and use the adjusted CNN network (CNN-T) to realize the detection and classification of the WCC-MC signal. Through simulation and radio experiments, we prove the effectiveness of the scheme for WCC-MC covert channel detection and classification. In the radio experiment, we get more than 98.5% detection accuracy rate for WCC-DC signal with the 10% embedding rate and more than 81.7% classification accuracy rate for WCC-DC with different embedding rates (10%, 20%, and 30%). Although the proposed scheme has been shown to be effective in detecting the WCC-MC communication signal, however, there are areas of our study that can be further improved. The problem of capturing radio signals, including the choice of listening frequencies and capturing radio signals by adding listening devices, is not described in our scheme. This problem will be studied in future work.

Data Availability

The .txt data used to support the findings of this study are included within the supplementary information files.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants U1836104 and 61702235 and in part by the Fundamental Research Funds for the Central Universities under Grant 30918012204.

Supplementary Materials

The supplementary information files contain the constellation points received by USRP for legitimate wireless communication and for WCC-DC schemes with embedding rates of 0.1, 0.2, and 0.3. (*Supplementary Materials*)

References

- [1] S. Cabuk, *Network Covert Channels: Design, Analysis, Detection, and Elimination*, Purdue University, West Lafayette, Indiana, 2006.
- [2] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels: design and detection," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pp. 178–187, Washington, DC, USA, October 2004.
- [3] G. Shah, A. Molina, and M. Blaze, "Keyboards and covert channels," in *Proceedings of the USENIX Security Symposium*, Vancouver, Canada, August 2006.
- [4] X. Luo, E. W. W. Chan, and R. K. C. Chang, *Cloak: A Ten-fold Way for Reliable Covert Communications*, 2007.
- [5] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based covert timing channels: automated modeling and evasion," in *Proceedings of the International Workshop on Recent Advances in Intrusion Detection*, pp. 211–230, Cambridge, MA, USA, September 2008.
- [6] Z. J. Xu, Y. Gong, K. Wang, W. D. Lu, and J. Y. Hua, "Covert digital communication systems based on joint normal distribution," *IET Communications*, vol. 11, no. 8, pp. 1282–1290, 2017.
- [7] M. E. Çek and F. Savaci, "Stable non-Gaussian noise parameter modulation in digital communication," *Electronics Letters*, vol. 45, pp. 1256–1257, 2009.
- [8] K. Szczypiorski and W. Mazurczyk, "Steganography in IEEE 802.11 OFDM symbols," *Security and Communication Networks*, vol. 9, no. 2, pp. 118–129, 2016.
- [9] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for WiFi systems," in *Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS)*, pp. 209–217, Florence, Italy, October 2015.
- [10] P. Praveenkumar, K. K. Thenmozhi, S. Vivekhanandan, J. B. B. Rayappan, and R. Amirtharajan, "Intersect embedding on OFDM channel—a stego perspective," in *Proceedings of the 2013 IEEE Conference on Information and Communication Technologies, ICT 2013*, Thuckalay, India, April 2013.
- [11] G. Shabsigh and V. S. Frost, "Covert communications in wideband OFDMA primary networks," in *Proceedings of the IEEE Globecom Workshops*, San Diego, CA, USA, December 2015.
- [12] P. Cao, W. Liu, G. Liu, X. Ji, J. Zhai, and Y. Dai, "A wireless covert channel based on constellation shaping modulation," *Security and Communication Networks*, vol. 2018, 2018.
- [13] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: covert communication through dirty constellations," in *Proceedings of the International Workshop on Information Hiding*, pp. 160–175, Berkeley, CA, USA, May 2012.
- [14] S. Huang, W. Liu, G. Liu, Y. Dai, and W. Tian, "Exploiting correlation characteristics to detect covert digital communication," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 14, pp. 3550–3566, 2020.
- [15] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, 2015.
- [16] N. Xie, C. Chen, and M. Zhong, "Security model of authentication at the physical layer and performance analysis over fading channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, p. 1, 2018.
- [17] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: opportunities and challenges," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 19–25, 2019.
- [18] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.
- [19] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206, 2017.
- [20] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.
- [21] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science*, vol. 313, no. 5786, pp. 504–507, 2006.
- [22] Y. LeCun, B. E. Boser, J. S. Denker et al., "Handwritten digit recognition with a back-propagation network," in *Advances in Neural Information Processing Systems* Morgan Kaufmann, Burlington, MA, USA, 1990.

- [23] D. C. Cireşan, U. Meier, J. Masci, L. M. Gambardella, and J. Schmidhuber, "Flexible, high performance convolutional neural networks for image classification," in *Proceedings of the Twenty-second International Joint Conference on Artificial Intelligence*, Barcelona, Spain, July 2011.
- [24] P. Y. Simard, D. Steinkraus, and J. C. Platt, "Best practices for convolutional neural networks applied to visual document analysis," in *Proceedings of the Seventh International Conference on Document Analysis and Recognition*, Edinburgh, UK, August 2003.
- [25] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.
- [26] C. Scott, *Network Covert Channels: Review of Current State and Analysis of Viability of the Use of x. 509 Certificates for Covert Communications*, Department of Mathematics-University of London, London, UK, 2008.
- [27] S. Gianvecchio and H. Wang, "An entropy-based approach to detecting covert timing channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, pp. 785–797, 2010.
- [28] T. Sohn, J. Seo, and J. Moon, "A study on the covert channel detection of TCP/IP header using support vector machine," *Information and Communications Security*, vol. 2839, pp. 313–324, 2003.
- [29] T. Sohn, J. Moon, S. Lee, D. H. Lee, and J. Lim, "Covert channel detection in the ICMP payload using support vector machine," *Computer and Information Sciences-ISCIS 2003*, vol. 286, pp. 828–835, 2003.
- [30] P. M. Atkinson and A. R. L. Tatnall, "Introduction neural networks in remote sensing," *International Journal of Remote Sensing*, vol. 18, no. 4, pp. 699–709, 1997.
- [31] L. Bruzzone and D. F. Prieto, "A technique for the selection of kernel-function parameters in RBF neural networks for classification of remote-sensing images," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 37, no. 2, pp. 1179–1184, 1999.
- [32] A. Langevin, D. Riopel, and K. E. Steckle, "Transfer batch sizing in flexible manufacturing systems," *Journal of Manufacturing Systems*, vol. 18, no. 2, pp. 140–151, 1999.
- [33] E. Veral, "Using production and transfer batches in flowshops under MRP control," *Journal of Operations Management*, vol. 12, no. 2, pp. 89–100, 1995.
- [34] M. A. Nielsen, *Neural Networks and Deep Learning*, Vol. 2018, Determination press, San Francisco, CA, USA, 2015.