

Received March 14, 2021, accepted March 31, 2021, date of publication April 6, 2021, date of current version April 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3071352

Differential Contour Stellar-Based Radio Frequency Fingerprint Identification for Internet of Things

JINGCHAO LI¹, YULONG YING², CHUNLEI JI¹, AND BIN ZHANG³, (Member, IEEE)

¹School of Electronic and Information, Shanghai Dianji University, Shanghai 201306, China

²School of Energy and Mechanical Engineering, Shanghai University of Electric Power, Shanghai 200090, China

³Department of Mechanical Engineering, Kanagawa University, Yokohama 221-8624, Japan

Corresponding author: Yulong Ying (yingyulong060313@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 62076160, Grant 51806135, and Grant 61603239.

ABSTRACT Data attacks from illegal access devices of the Internet of Things will cause serious interference and threats to the entire network. It is difficult to ensure the security of the communication system only by relying on traditional application layer password authentication methods. Therefore, it is of great significance to design an effective physical layer authentication system based on radio frequency fingerprints. Regarding the issue above, this paper proposes a novel physical layer authentication method for Internet of Things based on differential contour stellar. Through the test of identification and authentication of 20 WiFi network card devices from same manufacturer, same type and same batch, the recognition accuracy rate can reach 98.6% by the proposed method. The proposed method can improve the effect of radio frequency fingerprint identification from three aspects: i. The differential processing can effectively reduce the negative influence of phase rotation caused by carrier frequency offset and Doppler effects; ii. The color processing can effectively reduce the negative influence of random noise caused by channel noise; iii. It is suitable for processing large-scale networks and the massive data they bring.

INDEX TERMS Differential contour stellar, radio frequency fingerprint, physical layer authentication, fine portrait, deep convolutional neural network.

I. INTRODUCTION

Information security is the key to building a reliable and robust Internet of Things (IoT). With the continuous emergence of information security problems brought about by wireless communication networks, how to accurately identify and authenticate IoT objects and prevent user identity impersonation and device cloning is the primary problem to be solved by the application of IoT. The traditional authentication mechanism is implemented at the application layer, using cryptographic algorithms to generate numerical results that are difficult for third parties to counterfeit, but this mechanism has risks such as protocol security vulnerabilities and key leakage. The terminal equipment of the perception layer of the Internet of Things has the characteristics of diversification, intelligence, complexity and a large number.

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaochun Cheng.

Although the traditional authentication mechanism can guarantee information security to a certain extent, it is not suitable for processing large-scale networks and the massive data they bring, and it is difficult to meet the information security requirements of the Internet of Things. Therefore, research on a low error rate, high efficiency, and low cost individual identification method for communication radiation sources is the key to ensuring the stable operation of the Internet of Things.

Physical layer authentication is one of the core technologies to ensure the security of wireless communication. Its basic principle is to combine the space-time specificity of the transceiver channel and the transmitted signal to verify the physical characteristics of the communicating parties, thereby realizing identity authentication at the physical layer. Compared with the authentication technology at the application layer, it can effectively resist imitation attacks. It has the advantages of fast authentication speed, low complexity, good

compatibility, and no need to consider the implementation of various protocols. Nowadays, the research on the physical layer security authentication technology is still in its infancy and the abundant physical layer resources have not been fully utilized, and there is still a lot of research space.

Radio frequency fingerprint identification is a non-password authentication method based on the physical layer hardware of the device. It does not need to consume additional computing resources or embed additional hardware. And it is a very potential technique to establish a low-cost, simpler and safer identification and authentication system [1]. The existing radio frequency fingerprint identification technology can be divided into channel-based fingerprint identification technology and transmission signal-based fingerprint identification technology according to the use of physical layer resources. The channel-based fingerprint identification technology aims to use the unique location information of the device as the identity detection indicator for different users in different scenarios, and is usually applied to indoor positioning of IoT devices [2]. Common channel characteristics include radio signal strength (RSS), channel state information (CSI) and channel frequency response (CFR) [3], [4]. The fingerprint identification technology based on the transmission signal is divided into the fingerprint identification technology based on the transient signal and the fingerprint identification technology based on the steady signal. The fingerprint identification based on the transient signal is a process of extracting radio frequency fingerprint from a section of transient signal sent at the moment the device is turned on/off [5]. The transient signal does not contain any data information, only reflects the hardware characteristics of the transmitter, and is independent. RF fingerprints are initially extracted from transient signals. Due to the short duration of the transient signal, it is difficult to capture, and it is more sensitive to the detection and location of mutation points, which limits its application in the actual environment [6]. The steady-state signal is the signal when the transmitter is in a stable working state. It has a long duration and is easier to obtain. It can be completed with a cheap receiver. However, the radio frequency fingerprints present in the steady-state signal are more difficult to extract [7], [8]. According to the different feature extraction methods, it can be divided into fingerprint identification methods based on waveform domain and fingerprint identification methods based on modulation domain. The fingerprint recognition method based on the waveform domain uses the time-domain waveform characteristics of the signal to directly recognize the signal. It can also perform various domain transformations on the signal before extracting its characteristics, such as Fourier transform, wavelet transform, Hilbert–Huang transform [9], Synchrosqueezing transform [10], improved fractal box dimension [11], etc. The transform domain method attempts to transform the time domain signal to other domains to maximize individual differences, but the features extracted by the transform domain method will vary with the changes in the transmitted data. In order to avoid the feature extraction

method from being affected by the transmission data of the signal, radio frequency fingerprint extraction methods based on steady-state signals mostly use the preamble sequence repeatedly appearing in the signal. Electromagnetic signals are affected by factors such as transmitter carrier frequency offset, power amplifier nonlinearity, quadrature modulator imbalance and DC offset, and their differences are directly manifested in the modulation domain of the signal. This makes it possible to construct the radio frequency fingerprint identification of the transmitter in the modulation domain. At present, quadrature modulation has been widely used in communication signals, and the modulation domain features involved include carrier frequency offset, modulation offset, I/Q offset, constellation trace figure [12], differential constellation trace figure [13], etc. and their combinations. The modulation domain method takes I/Q signal samples as the basic processing unit, and uses the signal structure forced by the modulation scheme to make the specific attributes of the transmitter easier to identify. Knox *et al.* used the Ettus Labs USRP1 software radio platform as the receiving device (sampling frequency of 4MHz) for the classification problem of the SiLabs IEEE 802.15.4 2.4GHz RF device, and collected and demodulated signals from 5 same type RF devices from same manufacturer. The phase information of the baseband signal was extracted as a radio frequency fingerprint. The experimental results show that the classification performance of the RF fingerprint changes due to temperature difference and channel distance difference. The shorter the channel distance, the higher the recognition accuracy. When three different channel distances (i.e., short distance, medium distance, and long distance) were used, the average classification accuracy was 99.6%, 95.3%, and 81.9%, respectively [14]. Carbino *et al.* proposed a radio frequency fingerprint identification method based on constellation based-distinct native attribute (CB-DNA). The fingerprint of the device is extracted from the unintentional cable radiation of the Ethernet card to enhance the traditional MAC-based ID verification to reduce unauthorized network intrusion [15], [16]. In terms of feature engineering-based methods, the feature extraction methods have changed from using single-domain features to using multi-domain features, and shifting from methods based mainly on the waveform domain to methods based on the modulation domain. The classifier is designed to improve the generalization ability as the research goal, minimize the manually set parameters, and perform global optimization parameter settings.

In the identification and authentication stage, according to the type of classifier, classifiers for radio frequency fingerprint identification can be divided into traditional machine learning classifiers and deep learning classifiers. Classifier design is one of the key processing steps after extracting radio frequency fingerprints using feature engineering methods. At present, there are a large number of mature classifiers available, such as k-nearest neighbor, support vector machine, neural network, gray relation algorithm, extreme learning machine and other methods. Related research shows

that it is best to combine feature selection, feature dimensionality reduction, and classifier design together, so that correlation analysis can be performed better, and radio frequency fingerprint features that are more conducive to classification can be obtained [17]. In addition, by integrating multiple classifiers through strategies, better classification performance can be obtained than a single classifier. This is the idea of ensemble learning classifiers. Deep learning methods have been successfully applied in the fields of image recognition, speech recognition, and autonomous driving. Scholars have continued to introduce deep learning methods into the field of radio frequency fingerprint identification to solve the difficulties of feature extraction, and feature selection in RFF recognition [18], [19]. Ding *et al.* proposed a SEI method based on deep learning. This method selects the steady-state part of the signal, and first uses bispectral transformation to extract features, then uses supervised dimensionality reduction method to significantly reduce the bispectrum dimensions, and finally uses convolutional neural network to use the compressed bispectrum to identify specific transmitters [20]. Zhao *et al.* used a transfer learning method based on rejection sampling to update weights, and combined the weights with rejection sampling to construct a training set. The model trained by this method is less affected by time-varying and channel environments [21]. Merchant *et al.* developed a framework for training convolutional neural networks directly using time-domain complex baseband error signals and successfully identified 7 ZigBee devices [18]. This method does not need to specifically use the preamble sequence or the signal segment that reappears at a fixed position, and the extracted radio frequency fingerprint feature has nothing to do with the content carried by the signal to be identified. In 2018, Chatterjee *et al.* proposed the concept of RF-PUF [22]. This method uses only the waveform of the data portion and does not require a preamble sequence. It is a framework based on deep neural networks. It uses 50 hidden layer neurons to detect features such as local oscillator offset and I/Q imbalance. Simulation results show that under different channel conditions, the recognition rate of 10,000 transmitters is as high as 99%. In 2019, Yu *et al.* proposed a multi-sampling convolutional neural network (MSCNN) and developed an adaptive ROI selection algorithm based on SNR [23]. USRP was used as the receiver and 54 CC2530 devices were used as recognition targets. The feasibility and reliability of the method in line of sight (LOS) and non line of sight (NLOS) scenarios were tested. The results show that the algorithm is robust under LOS and NLOS, and the classification accuracy is as high as 97% in the LOS environment with an SNR of 30dB. In the same year, Yu *et al.* also proposed a deep learning RFF recognition model based on denoising autoencoder (DAE) [24]. Compared with traditional CNN, under the additive white Gaussian noise channel, the recognition accuracy can be improved by 14% to 23.5% when the SNR is -10 dB to 5 dB. Even if the SNR is 10dB, the recognition accuracy is as high as 97.5%. In addition, the deep sparse capsule network can also be used for signal

classification [25]. Compared with CNN, it not only has good classification performance, but also can automatically obtain hierarchical feature representations. Deep learning methods provide new ideas and techniques for radio frequency fingerprint identification. However, the current fingerprint recognition technology based on deep learning mainly directly uses baseband data as training data, trying to let the algorithm find fingerprint features by itself, and has achieved certain results. However, due to its “black box” characteristics, it is best to combine it with feature engineering methods to enhance the interpretability of deep learning models and improve the understanding of the mechanism of radio frequency fingerprint identification.

In this paper, the inherent and essential unintentional modulation information carried by the electromagnetic wave signal emitted by the terminal device of the Internet of Things is used as the identifiable fingerprint feature of the device. Through the effective feature extraction method of the differential contour stellar, a fine portrait database of the fingerprint features of the devices is constructed, and the one-dimensional radio frequency signal feature set is converted into a two-dimensional image data set. And a deep convolutional neural network is used to identify the extracted fine portrait of the RF fingerprint, which can achieve reliable identification and authentication of the physical layer terminal devices of the Internet of Things. And the main contribution of the paper is as follows:

- a. A differential contour stellar based RF fingerprint extraction method is proposed and can be used as a fine portrait of the transmitter’s RF fingerprint by using transmission data segment of the steady-state signal.
- b. Deep convolutional neural network based RF Fingerprint identification scheme using differential contour stellar (DSC-CNN) is proposed.
- c. Based on the measured signals of 20 WiFi network card devices from the same manufacturer, same type and same batch, the validity and reliability of the method proposed in the paper are tested.
- d. Compared with the contour stellar [22], the differential contour stellar has better robustness as RF fingerprint. Even if the carrier frequency deviation and phase deviation of the receiver are not estimated and compensated, a reliable RF fingerprint of the communication radiation source (transmitter) can be obtained.

The remainder of this paper is organized as follows. In Section II, the typical constellation method and the proposed method are described. The application and analysis are presented in Section III, and test results of the proposed method are also presented in Section III, followed by the conclusions in Section IV.

II. METHODOLOGY

A. TYPICAL CONSTELLATION METHOD

Due to the deviation between the actual value and the nominal value of the electronic component, even if the transmitters composed of the same batch of electronic components still

have differences, it is also called transmitter imperfection, which is the physical basis of RFF, as shown in fig.1.

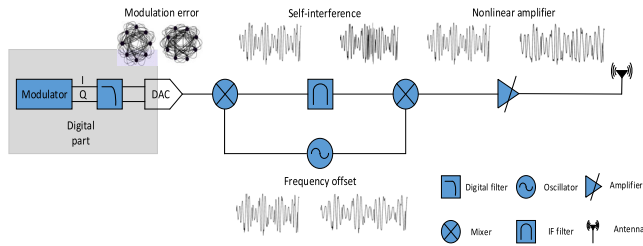


FIGURE 1. Software radio universal digital transmitter.

Even if it is device from the same manufacturer, same type and same batch, due to the tolerance effect of electronic components, the actual hardware parameters of some internal components such as oscillator (existence of frequency offset and phase noise), modulator (existence of modulation error) and power amplifier (existence of non-linear distortion) and so on, will also vary. The RF signal is modulated by modulating the current at the excitation source before transmission, and the information to be transmitted is added to the signal. In this process, the intentional modulation information transmitted is included, and the unintentional modulation information of the characteristics of the radiation source is also included [26]. Radio frequency fingerprint is an essential feature of the physical layer of a wireless communication device, and it is difficult to be tampered with. Just as different people have different fingerprints, different radio frequency fingerprints of different communication devices can be used for wireless device identification and access authentication. After these information-carrying electromagnetic waves start from the excitation source and propagate step by step, although the characteristics of the electromagnetic field at the excitation source are retained, they are also constantly affected by the transmission medium.

The constellation diagram is a vector diagram obtained by drawing the endpoints of the modulation signal under a specific base vector projection on the two-dimensional coordinates with I and Q as the horizontal and vertical axes. Each vector endpoint (also called a symbol point) can express two basic information of the amplitude and phase of the signal relative to the carrier at a certain moment, and its projection on the two coordinate axes is the two baseband signals at the current moment. The number of symbol points of the digital modulation signal is limited, and all symbol points are represented in the same vector diagram to form a constellation diagram, as shown in fig.2.

Fig. 2 shows examples of transitions in the I/Q complex plane corresponding to QPSK, BPSK, and OQPSK. It can be seen that different modulation waveforms present different transition patterns in the I/Q complex plane. For example, the transitions between (1,0) and (-1, 0) are unique to BPSK but do not appear in QPSK, which has a substantially different constellation. It can constitute a unique signature of the RF baseband signal that can eventually be learned by the CNN's

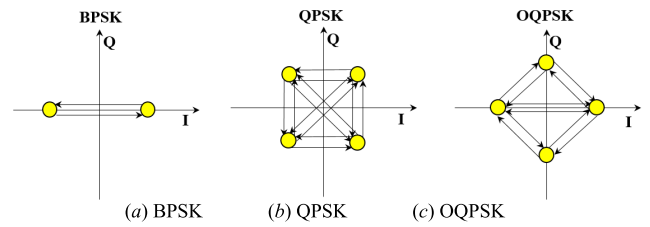


FIGURE 2. Transitions in the I/Q complex plane corresponding to (a) BPSK, (b) QPSK, and (c) OQPSK, where the arrows indicate the symbol transition traces.

filters. At present, quadrature modulation has been extensively applied in communication signals, and the radio frequency fingerprint features in the modulation domain, such as constellation trace figure [12], [13], and constellation based contour stellar [27], have been typically proposed by scholars to represent radio frequency fingerprints. And a constellation figure of radio frequency baseband I/Q signals of a wifi network card device can be shown in fig.3.

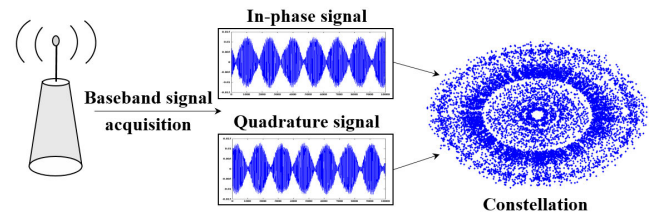


FIGURE 3. A constellation diagram of RF baseband signal from a WiFi network card device.

Since the constellation diagram corresponds to the amplitude and phase of the RF baseband signal, the shape of the array can also be used to analyze amplitude imbalance, quadrature error, correlated interference, phase/amplitude noise, phase error, modulation error ratio, etc.

B. THE PROPOSED METHOD

Assume that the radio frequency signal emitted by the communication radiation source (transmitter) is as follows:

$$S(t) = X(t) e^{-j2\pi f_c^t t} \quad (1)$$

where $X(t)$ is the transmitter baseband signal; f_c^t is the transmitter carrier frequency.

Assuming that the RF circuit of the transmitter is ideal and the channel is also ideal, the RF signal received by the receiver is as follows:

$$R(t) = S(t) \quad (2)$$

The receiver down-converts the RF signal to obtain the baseband signal as follows:

$$Y(t) = R(t) e^{j(2\pi f_c^r t + \varphi)} \quad (3)$$

where f_c^r is the receiver carrier frequency; φ is the received signal phase offset.

when $f_c^t \neq f_c^r$, the receiver down-converts the RF signal to obtain the baseband signal as follows:

$$Y(t) = X(t) e^{j(2\pi\theta t + \varphi)} \tag{4}$$

where $\theta = f_c^r - f_c^t$.

Since the demodulated signal contains residual frequency deviation θ , each sampling point of the baseband signal has a phase rotation factor $e^{j2\pi\theta t}$. The phase rotation factor $e^{j2\pi\theta t}$ varies with the position t of the sampling point, which usually leads to poor robustness and stability of the extracted constellation features, as shown in fig.4.

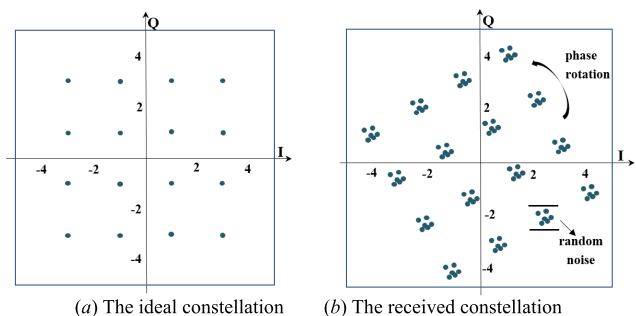


FIGURE 4. Transitions in the I/Q complex plane corresponding to 16-QAM: (a) The ideal constellation; (b) The received constellation which is affected by random channel noise, carrier frequency offset and Doppler effect, etc.

In most coherent demodulation communication systems, the estimated frequency deviation $\hat{\theta}$ and phase deviation $\hat{\varphi}$ can be obtained by estimating the frequency deviation and phase deviation. The receiver uses the estimated results to compensate the received signal for frequency deviation $\hat{\theta}$ and phase deviation $\hat{\varphi}$, thereby obtaining a stable constellation. In the radio frequency fingerprint extraction method based on constellation, the purpose of the receiver is not to demodulate each received signal symbol correctly. Therefore, the received I and Q baseband signals can be differentially processed according to a certain interval n to obtain a stable constellation diagram as follows:

$$\begin{aligned} D(t) &= Y(t) \cdot Y^*(t+n) \\ &= X(t) e^{j(2\pi\theta t + \varphi)} \cdot X(t+n) e^{-j(2\pi\theta(t+n) + \varphi)} \\ &= X(t) \cdot X(t+n) e^{-j2\pi\theta n} \end{aligned} \tag{5}$$

where Y^* takes the conjugate value.

Although the differentially processed signal $D(t)$ still contains a phase rotation factor $e^{-j2\pi\theta n}$, the phase rotation factor $e^{-j2\pi\theta n}$ is a constant value and will not change with the change of the sampling point position. Therefore, after differential processing, a stable constellation can be obtained even if the carrier frequency deviation $\tilde{\theta}$ and phase deviation $\tilde{\varphi}$ of the receiver are not estimated and compensated, as show in fig.5.

Here the new RF baseband signal after differential processing is as follows:

$$D(t) = (x_1 \cdot x_2 + y_1 \cdot y_2) + j(y_1 \cdot x_2 - x_1 \cdot y_2)$$

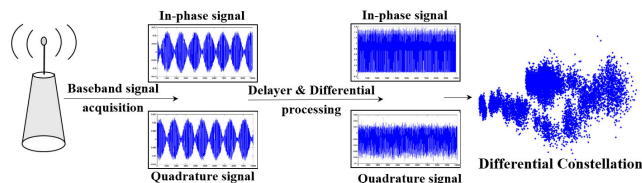


FIGURE 5. Visualize the new In-phase signal and Quadrature signal after differential processing as a differential constellation.

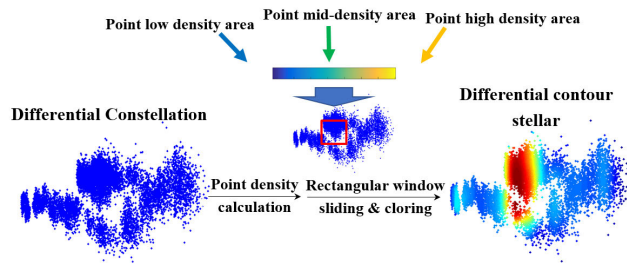


FIGURE 6. The transition from differential constellation to differential contour stellar.

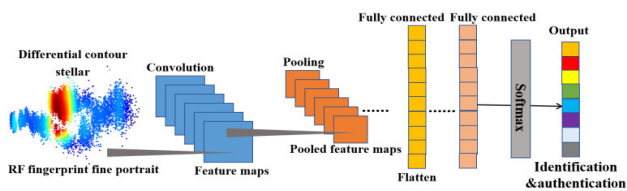


FIGURE 7. Deep convolutional neural network-based RF fingerprint identification scheme using differential contour stellar (DSC-CNN).

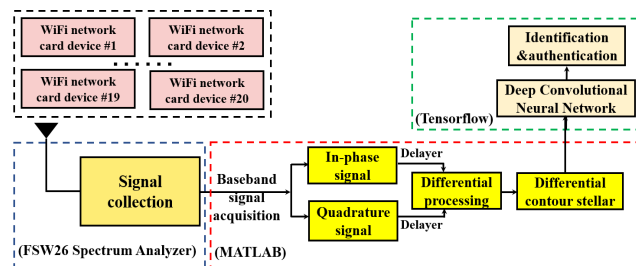


FIGURE 8. Experimental test scheme.

where $x_1 = I(t)$; $y_1 = Q(t)$; $x_2 = I(t+n)$; $y_2 = Q(t+n)$. And the time interval n is 1.

Therefore, the subsequent feature extraction of the contour stellar based on the differential constellation can be performed. According to the different point density of the two-dimensional differential constellation diagram, the distribution of different colors is given to different areas, and the one-dimensional signal is converted into a two-dimensional color image (like an ultra-high-definition X-ray film), which can describe the subtle characteristics of the signal more comprehensively, as seen fig.6.

As shown in fig.6, when sliding the density window function on the differential constellation, the density window

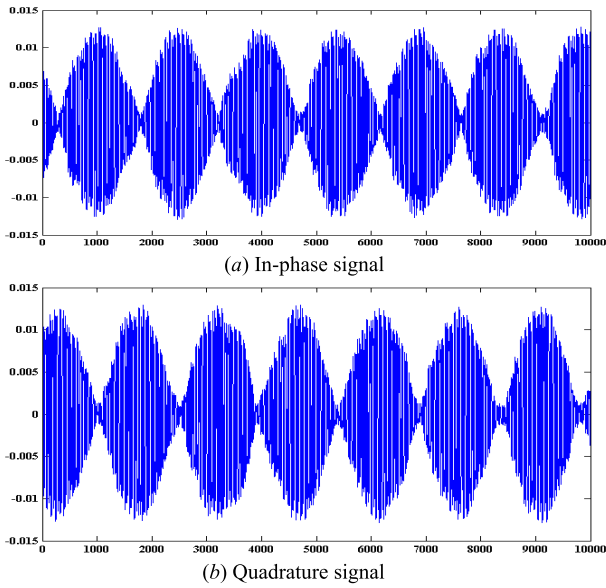


FIGURE 9. One new sample for one WiFi network card device.

TABLE 1. The deep convolutional neural network structure.

Layer	Output shape
Input	227x227x3
Conv	55x 55x96
MaxPooling	27x 27x96
BatchNormalization	27x 27x96
Conv	27x 27x256
MaxPooling	13x 13x256
BatchNormalization	13x 13x256
Conv	13x 13x384
Conv	13x 13x384
Conv	13x 13x256
MaxPooling	6x 6x256
BatchNormalization	6x 6x256
Flatten	9216
FC/Relu	4096
FC/Relu	4096
FC/Softmax	20

function will calculate how many points are in the window. Different calculation results mean different densities, and different colors will be used to mark different densities. Yellow indicates a relatively high density area of sampling points, green indicates a relatively medium density area of sampling points, and blue indicates a low density area of sampling points. By calculating the point density on the differential constellation, and then coloring by sliding the rectangular window function (density window), the colored differential contour stellar of the RF baseband signal can be obtained as a fine portrait of the transmitter’s RF fingerprint.

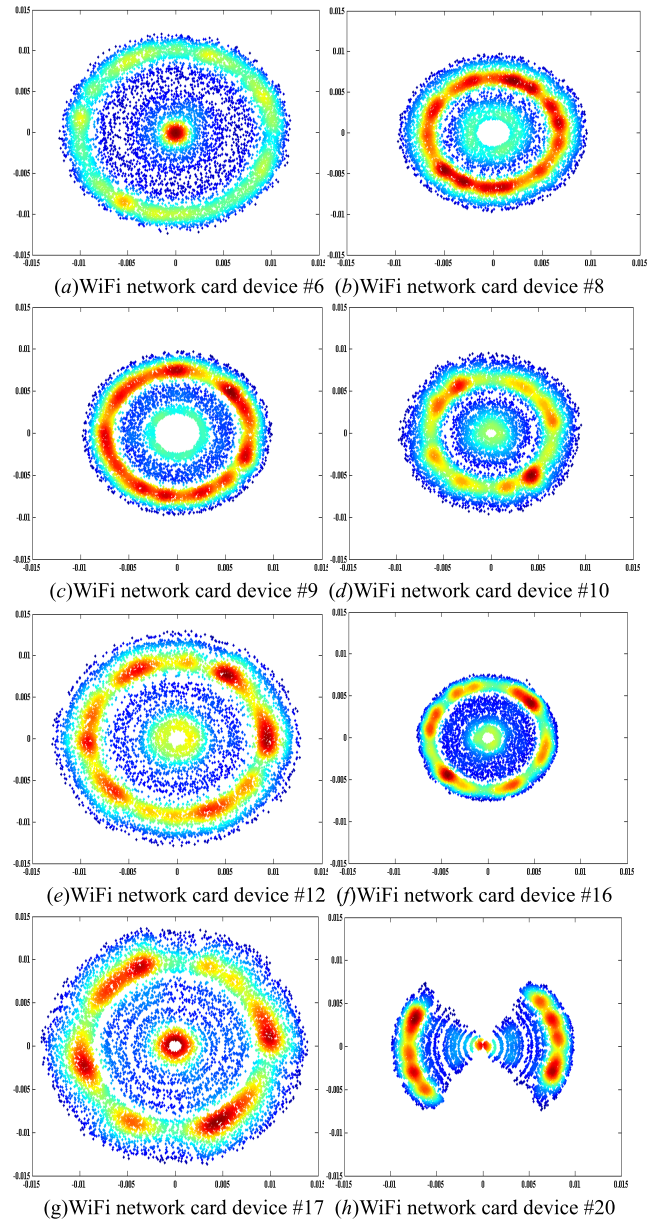


FIGURE 10. An example of the transition from constellation to contour stellar for the WiFi network card devices.

Finally, a deep convolutional neural network can be used to identify the extracted fine portrait of the RF fingerprint, which can achieve reliable identification and authentication of the physical layer of the Internet of Things, as seen fig.7.

Mathematically speaking, the method (DSC-CNN) proposed in this paper can improve the effect of physical layer authentication from three aspects: i. The differential processing can effectively reduce the negative influence of phase rotation caused by carrier frequency offset and Doppler effect; ii. The color processing can effectively reduce the negative influence of random noise caused by channel noise; iii. It is suitable for processing large-scale networks and the massive data they bring.

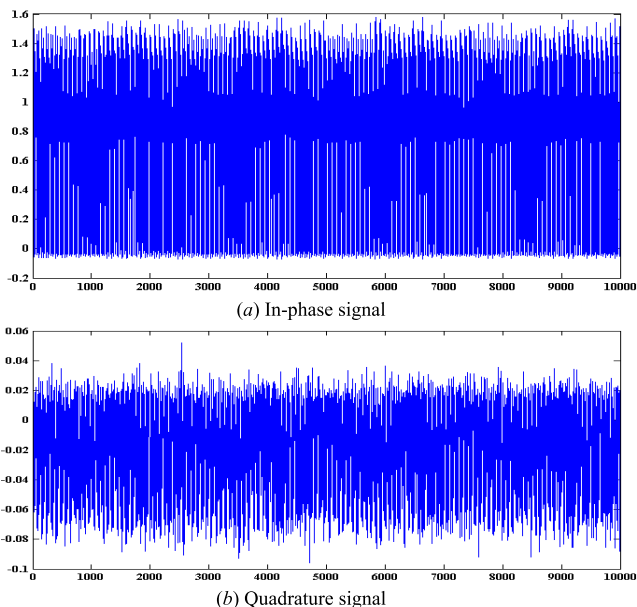


FIGURE 11. An example of differential processing on the In-phase signal and Quadrature signal after delayer to form a new In-phase signal and Quadrature signal.

III. EXPERIMENT AND ANALYSIS

A. EXPERIMENT INTRODUCTION

The specific implementation case takes as an example the identification of 20 WiFi network card devices from the same manufacturer, same type and same batch, as shown in fig.8.

Among them, the radio frequency baseband signal acquisition equipment adopts FSW26 spectrum analyzer. The collection environment is a laboratory in line of sight (LOS) scenario. Collect 50 samples per device; The signal acquisition bandwidth is 80MHz, and each acquisition is 1.75ms, that is, 140,000 points per sample (take a single channel as an example). The effective data transmission section excluding the channel noise section is 80,000 points (all are steady-state signals). And then slice the effective data transmission section, and take 10,000 points as a new sample, and there are a total of 8,000 samples for these 20 WiFi network card devices. And one new sample for one WiFi network card device is seen in fig.9.

B. APPLICATION AND ANALYSIS

After generating a differential contour stellar for each new sample, randomly selects 320 samples for each device to be used for the training of the deep convolutional neural network, and the remaining 80 samples are tested for recognition.

In order to illustrate the effectiveness of the method proposed in this paper, compare it with the radio frequency fingerprint extraction method of the contour stellar [27], [28], and the deep convolutional neural network structure is unified as shown in Table 1, which is improved on the basis of AlexNet.

An example of the transition from constellation to contour stellar for the WiFi network card devices is shown in fig.10.

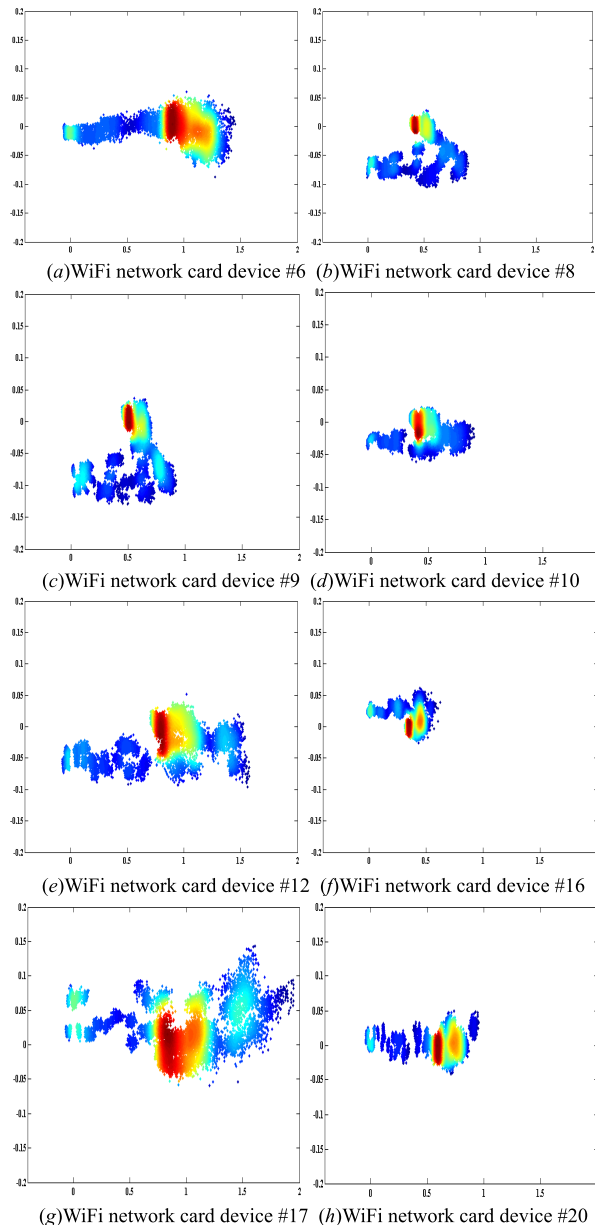


FIGURE 12. An example of the transition from differential constellation to differential contour stellar for the WiFi network card devices.

Note: the x -axis is the In-phase signal and the y -axis is the Quadrature signal. Various modulation waveforms always present various transition patterns in the I/Q complex plane, and therefore the constellation figures can represent a distinctive signature of the radio frequency baseband I/Q signals.

An example of differential processing on the In-phase signal and Quadrature signal after delayer to form a new In-phase signal and Quadrature signal is shown in fig.11.

An example of the transition from differential constellation to differential contour stellar for the WiFi network card devices is shown in fig.12.

We can see that, from fig.10 and fig.12, the differential contour stellar for each WiFi network card device is quite different from contour stellar. Finally, through the recognition and authentication of the deep convolutional neural network,

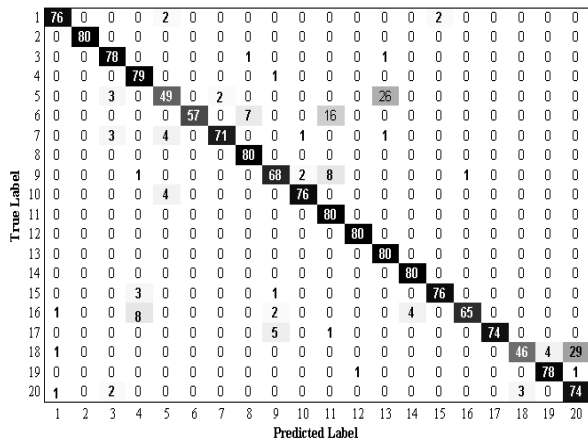


FIGURE 13. The recognition results of the individual communication radiation source based on the contour stellar.

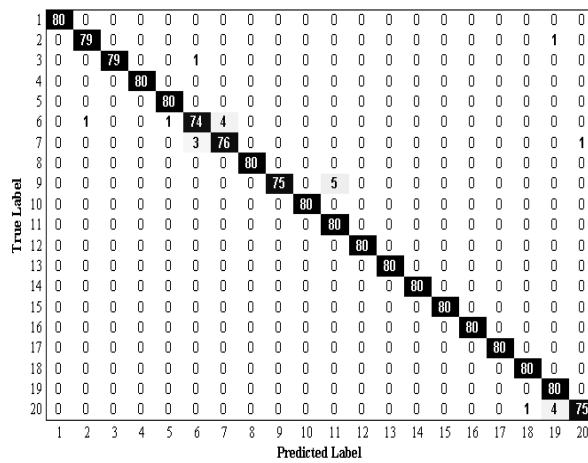


FIGURE 14. The recognition results of the individual communication radiation source based on the differential contour stellar.

the recognition results of the individual communication radiation source based on the contour stellar and the recognition results based on the method proposed in this paper are obtained respectively, as shown in fig.13 and fig.14.

From fig.13, we can see, the overall recognition success rate of a total of 1600 test samples from 20 WiFi network card devices is 90.4%. And a total of 6 devices are fully recognized correctly. And there are 5 devices with a recognition rate of below 87.5%, which are device#5, device#6, device#9, device#16, and device#18, and the recognition rate of device#18 is the lowest, only 57.5%.

From fig.14, we can see, the overall recognition success rate of a total of 1600 test samples from 20 WiFi network card devices reaches 98.6%. And a total of 14 devices are fully recognized correctly. The recognition rate of device#6 is the lowest, still as high as 92.5%. As the differential contour stellar can effectively reduce the negative effects of phase rotation and random noise, compared with the contour stellar [27], the differential contour stellar has better robustness as RF fingerprint. Even if the carrier frequency deviation and phase deviation of the receiver are not estimated and compensated, a reliable RF fingerprint of the communication

radiation source (transmitter) can be obtained by the proposed method.

IV. CONCLUSION

This paper proposes a novel physical layer authentication method for Internet of Things based on differential contour stellar. First, collect the radio frequency baseband signal through the receiver, and collect the In-phase signal and Quadrature signal; Then carry out differential processing on the In-phase signal and Quadrature signal after delay to form a new In-phase signal and Quadrature signal; Then visualize the new In-phase signal and Quadrature signal as a differential constellation; And next, by calculating the point density on the differential constellation, and then coloring by sliding the rectangular window function (density window), the colored differential contour stellar of each segment of the RF baseband signal is obtained as a fine portrait of the transmitter’s RF fingerprint; Finally, a deep convolutional neural network is used to identify the extracted fine portrait of the RF fingerprint, which can achieve reliable identification and authentication of the physical layer of the Internet of Things. Through the test of identification and authentication of 20 WiFi network card devices from the same manufacturer, same type and same batch, some meaningful conclusions can be obtained as follows:

- (1) The differential contour stellar can be used as a fine portrait of the transmitter’s RF fingerprint, extracted from the transmission data segment of the steady-state signal.
- (2) Compared with the contour stellar, the differential contour stellar has better robustness as RF fingerprint. Even if the carrier frequency deviation and phase deviation of the receiver are not estimated and compensated, a reliable RF fingerprint of the communication radiation source can be obtained.
- (3) Deep convolutional neural network based RF Fingerprint identification scheme using differential contour stellar (DSC-CNN) can achieve reliable identification and authentication of the physical layer of the Internet of Things.

In the future work, experimental case studies will be conducted for more wifi network card devices from same batch, same type, and same manufacturer, at mixed scenarios of line-of-sight (LOS) scene and non-line-of-sight (NOS) scene to further test the robustness of the proposed approach. And the deep convolutional neural network structure can be further improved.

ACKNOWLEDGMENT

This research is supported by the National Natural Science Foundation of China (No. 62076160, No.51806135 and 61603239).

REFERENCES

[1] T. Zheng, Z. Sun, and K. Ren, “FID: Function modeling-based data-independent and channel-robust physical-layer identification,” 2019, arXiv:1901.05914. [Online]. Available: http://arxiv.org/abs/1901.05914

[2] Y. Shu, Y. Huang, J. Zhang, P. Coue, P. Cheng, J. Chen, and K. G. Shin, “Gradient-based fingerprinting for indoor localization and tracking,” *IEEE Trans. Ind. Electron.*, vol. 63, no. 4, pp. 2424–2433, Apr. 2016.

- [3] W. K. Zegeye, S. B. Amsalu, Y. Astatke, and F. Moazzami, "WiFi RSS fingerprinting indoor localization for mobile devices," in *Proc. IEEE 7th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2016, pp. 1–6.
- [4] K. Lin, M. Chen, J. Deng, M. M. Hassan, and G. Fortino, "Enhanced fingerprinting and trajectory prediction for IoT localization in smart buildings," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1294–1307, Jul. 2016.
- [5] J. Li, D. Bi, Y. Ying, K. Wei, and B. Zhang, "An improved algorithm for extracting subtle features of radiation source individual signals," *Electronics*, vol. 8, no. 2, pp. 1–11, Feb. 2019, doi: [10.3390/electronics8020246](https://doi.org/10.3390/electronics8020246).
- [6] H. Han, J. Li, and X. Chen, "The individual identification method of wireless device based on a robust dimensionality reduction model of hybrid feature information," *Mobile Netw. Appl.*, vol. 23, no. 4, pp. 709–716, Aug. 2018.
- [7] J.-C. Li, Y.-B. Li, S. Kidera, and T. Kirimoto, "A robust signal recognition method for communication system under time-varying SNR environment," *IEICE Trans. Inf. Syst.*, vol. 96, no. 12, pp. 2814–2819, 2013.
- [8] J. Li, "A novel recognition algorithm based on holder coefficient theory and interval gray relation classifier," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 11, pp. 4573–4584, 2015.
- [9] Y. Yuan, Z. Huang, H. Wu, and X. Wang, "Specific emitter identification based on Hilbert–Huang transform-based time–frequency–energy distribution features," *IET Commun.*, vol. 8, no. 13, pp. 2404–2412, Sep. 2014.
- [10] G. Baldini, R. Giuliani, and G. Steri, "Physical layer authentication and identification of wireless devices using the synchrosqueezing transform," *Appl. Sci.*, vol. 8, no. 11, p. 2167, Nov. 2018.
- [11] X. Chen, J. Li, H. Han, and Y. Ying, "Improving the signal subtle feature extraction performance based on dual improved fractal box dimension eigenvectors," *Roy. Soc. Open Sci.*, vol. 5, no. 5, May 2018, Art. no. 180087.
- [12] Y. Jiang, L. Peng, A. Hu, S. Wang, Y. Huang, and L. Zhang, "Physical layer identification of LoRa devices using constellation trace figure," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 223, Dec. 2019, doi: [10.1186/s13638-019-1542-x](https://doi.org/10.1186/s13638-019-1542-x).
- [13] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep learning based RF fingerprint identification using differential constellation trace figure," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1091–1095, Jan. 2020, doi: [10.1109/TVT.2019.2950670](https://doi.org/10.1109/TVT.2019.2950670).
- [14] D. A. Knox and T. Kunz, "Wireless fingerprints inside a wireless sensor network," *ACM Trans. Sensor Netw.*, vol. 11, no. 2, pp. 1–30, Mar. 2015.
- [15] T. J. Carbino, M. A. Temple, and T. J. Bihl, "Ethernet card discrimination using unintentional cable emissions and constellation-based fingerprinting," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2015, pp. 369–373.
- [16] T. J. Carbino, M. A. Temple, and J. Lopez, "Conditional constellation based-distinct native attribute (CB-DNA) fingerprinting for network device authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.
- [17] J. Li, "A new robust signal recognition approach based on holder cloud features under varying SNR environment," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 12, pp. 4934–4949, 2015.
- [18] K. Merchant, S. Revay, G. Stantchev, and B. Noursain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 160–167, Feb. 2018.
- [19] C. Zhao, M. Shi, Z. Cai, and C. Chen, "Research on the open-categorical classification of the Internet-of-Things based on generative adversarial networks," *Appl. Sci.*, vol. 8, no. 12, p. 2351, Nov. 2018.
- [20] L. Ding, S. Wang, F. Wang, and W. Zhang, "Specific emitter identification via convolutional neural networks," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2591–2594, Dec. 2018.
- [21] C. Zhao, Z. Cai, M. Huang, M. Shi, X. Du, and M. Guizani, "The identification of secular variation in IoT based on transfer learning," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Mar. 2018, pp. 878–882.
- [22] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using *in-situ* machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.
- [23] J. Yu, A. Hu, G. Li, and L. Peng, "A robust RF fingerprinting approach using multisampling convolutional neural network," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6786–6799, Aug. 2019.
- [24] J. Yu, A. Hu, F. Zhou, Y. Xing, Y. Yu, G. Li, and L. Peng, "Radio frequency fingerprint identification based on denoising autoencoders," 2019, *arXiv:1907.08809*. [Online]. Available: <http://arxiv.org/abs/1907.08809>
- [25] M. Liu, G. Liao, Z. Yang, H. Song, and F. Gong, "Electromagnetic signal classification based on deep sparse capsule networks," *IEEE Access*, vol. 7, pp. 83974–83983, 2019.
- [26] J. Li, Y. Ying, and C. Ji, "Study on radio frequency signal gene characteristics from the perspective of fractal theory," *IEEE Access*, vol. 7, pp. 124268–124282, 2019, doi: [10.1109/ACCESS.2019.2938791](https://doi.org/10.1109/ACCESS.2019.2938791).
- [27] Y. Tu, Y. Lin, J. Wang, and J. U. Kim, "Semi-supervised learning with Generative Adversarial Networks on digital modulation classification," *CMC-Comput. Mater. Continua*, vol. 55, no. 2, pp. 243–254, May 2018, doi: [10.3970/cm.c.2018.01755](https://doi.org/10.3970/cm.c.2018.01755).
- [28] S. Wang, H. Jiang, X. Fang, Y. Ying, J. Li, and B. Zhang, "Radio frequency fingerprint identification based on deep complex residual network," *IEEE Access*, vol. 8, pp. 204417–204424, 2020, doi: [10.1109/ACCESS.2020.3037206](https://doi.org/10.1109/ACCESS.2020.3037206).



JINGCHAO LI received the B.S. degree in electrical information engineering from Harbin Engineering University (HEU), in 2010, the M.S. degree from HEU, and the Ph.D. degree from the Faculty of Communication and Information System, HEU, in June 2014. From 2012 to 2013, she was with the University of Electro-Communication (UEC), Japan, as an Exchanged Student. From April 2014 to June 2014, she was with Western New England University, USA, as a Visiting Scholar. She is currently an Assistant Professor with Shanghai Dianji University. Her research interest includes communication signals recognition, which conclude feature extraction and classifier design. She has published over 40 articles on these topics.



YULONG YING received the B.S. degree in power and energy engineering, the M.S. degree in power machinery and engineering, and the Ph.D. degree in marine engine engineering from Harbin Engineering University, Harbin, China, in 2010, 2013, and 2016, respectively. From 2013 to 2016, he was an Engineer and a Researcher with Shanghai Electric Shanghai Electric Gas Turbine Company Ltd. He is currently an Assistant Professor with the School of Energy and Mechanical Engineering, Shanghai University of Electric Power, Shanghai, China. His research interests include thermodynamics, control systems, signal feature extraction, and pattern recognition, machine learning, and power machine fault diagnosis and prognosis. He has published over 50 research articles on these topics.



CHUNLEI JI is currently a Professor with Shanghai Dianji University, where he is the Leader of the Computer Science and Technology discipline. His research interests include cloud computing and big data technology, software development, and measurement technology.



BIN ZHANG (Member, IEEE) received the B.E. degree in automation from Harbin Engineering University (HEU), China, in 2011, and the M.E. and Ph.D. degrees in mechanical engineering and intelligent systems from the University of Electro-Communications (UEC), Japan, in 2013 and 2017, respectively. From April 2017 to March 2018, he worked as an Engineer with Nissan Motor Company Ltd., Japan. He is currently an Assistant Professor with the Department of Mechanical Engineering, Kanagawa University (KU). His research interests include intelligent robotics, human–robot interaction, signal processing, and artificial intelligence.