Trust Management Method of D2D Communication Based on RF Fingerprint Identification

Zhaoyue Zhang¹, Xinghao Guo² and Yun Lin²,∗

¹ College of Air Traffic Management, Civil Aviation University of China, Tianjin, P.R. China
² College of Information and Communication Engineering, Harbin Engineering University, Harbin, P.R.China

Corresponding author: Yun Lin (e-mail: linyun@hrbeu.edu.cn).

ABSTRACT With the rapid development and the increasing security threats of D2D communication, the D2D communication security has become more and more important. Device recognition is the foundation of communication security. Traditional device authentication is the cryptographic mechanism and the security protocol, which are not enough for the new security threat. RF fingerprint of wireless device have physical characteristics, which is difficult to clone. Therefore, it can be used for D2D device recognition. In this paper, a recognition algorithm of D2D device based on RF fingerprint is proposed. Firstly, Hilbert transform and principal component analysis (PCA) is used to generate the RF fingerprint of D2D device. Secondly, Support Vector Machine (SVM) is introduced and CV-SVM is used as the classifier. Finally, simulation results show that the recognition rate is more than 90% under SNR=5dB, which proves that proposed method is effective for D2D device recognition. Therefore, it can be used as the trust management of D2D communication.

INDEX TERMS D2D Communication, Trust Management, RF Fingerprint, Device Recognition

I. INTRODUCTION

As an emerging technology of wireless communication, D2D communication technology permits to establish a direct communication relationships among close-by wireless communication devices[1],[2]. Therefore, their data transmission does not need to traverse the core network. In particular, the distinctive advantages of D2D communication have attracted a large number of scholars and research institutions from different fields[3].

D2D communication is an indispensable technology of Internet of things (IoT). The open D2D communication environment enables some service providers to put their service programs at the edge of the communication network, which improves the service efficiency. But it is also because of the openness of D2D communication, the distributed structure and the lack of control system capabilities, which makes it vulnerable to be malicious attacks. Meanwhile, the growing number and variety of wireless devices in the Internet of things makes it more vulnerable to be intruded. Some traditional IoT security authentication algorithms can’t ensure information security in D2D communication environment. Most of the devices connected to the Internet of Things do not have enough computing ability, which is unable to apply complex encryption mechanisms and other security technologies[4]. In addition, because the access control of D2D communication is distributed, the traditional access strategy is not suitable for D2D communication network[5]. In reference [6], Ramirez introduced three key problems of user security and privacy: “ubiquitous data collection, the potential for unexpected use of consumer data and heightened consumer risks”, which not only reduces the user’s confidence in it, but also hinders the development of D2D communication[6].

In a D2D communication network, if both devices gain the trust of the other party, the devices can share resources and services on such basis. In the communication process, trust analysis between devices plays an important role in improving the efficiency and reliability of communication. Trust management in D2D communication helps improve communication reliability and security and it also plays a vital role in unified decision of different platforms in communication system. Trust can enhance users’ confidence
in D2D communication and reduce the risks and uncertainties in D2D communication[7]. Trust management can work with some authentication algorithms. Therefore, trust management is an emerging solution to D2D communication security issues. In the study of trust management, many scholars focus on wireless sensor networks[8]-[10], there are currently relatively few studies on access services in the D2D communication.

In recent years, RF fingerprint identification have been paid more and more attention by scholars and research institutions all over the world, which is proved to be effective in physical layer security of wireless communication. And the biggest advantage of RF fingerprints compared to other trust management methods is that they use the inherent hardware differences of the transmitter for identification, so this method cannot be completely copied. Considering some of the above reasons, in the paper, based on RF fingerprint identification, a trust management method of D2D communication is proposed. The rest of this paper is arranged as follows. The work related to RF fingerprint are shown in section II. The RF fingerprint identification model is proposed in section III. The trust management mechanism is designed in section IV. Simulation experiments and results analysis is shown in section V. The conclusion of the paper is summarized in section VI.

II. RESEARCH ON RF FINGERPRINT IDENTIFICATION

RF fingerprint is a kind of pattern technology, which is used to identify the individual wireless devices through the signal nuances producing by the difference of individual transmitter. Research on RF fingerprint first began in 1995. Until now, a large number of RF fingerprint technology had been proposed. In this section, a simple review of RF fingerprint extraction and identification is summarized[11]-[24].

There are two types of RF Fingerprint techniques: transient based and steady state based. Transient based RF fingerprint was firstly proposed in the early 90s and has been widely studied. In reference [11],[12], the turn-on transients at the FM discriminator circuit of 7 FM transmitters from 4 different manufacturers was extracted, the RF fingerprint of devices were composed of the wavelet spectra from signal transients. The experimental results showed the effectiveness of this method. Subsequently, a large number of related works about based on the transient signal appeared in the open literature. The transient based RF fingerprint in recent researches were mainly extracted from the instantaneous characteristic (amplitude, phase and frequency)[13],[14] and the time-frequency-distribution[15],[16].

Although the transient based method had shown very good performance, it still has several challenges[17]. That was mainly because the transient signal duration is too short to be obtained, which puts forward high requirements for signal acquisition equipment. Compared with the transient-based RF fingerprint, the steady-state-based method was more suitable for engineering implementation. The steady-state-based RF fingerprint method was firstly proposed in 2008, in reference [18], the spectrum of the preamble signal from the Universal Mobile Telecommunications System (UMTS) for the identification of eight identical transmitters was proposed, the approach performed very well-being able to achieve a classification rate 97% at 30dB SNR. Following this research, new method about steady-state-based RF fingerprint has been put forward continuously in recent years. Such as the distinctive signal properties of modulated signals[19],[20], the Power Spectral Density (PSD) of the preamble signals[21],[22], the RF-DNA Fingerprint[23],[24]. In recent years, deep learning method was used for signal recognition, which was also proved to be effective in device recognition[25],[26].

III. RF FINGERPRINT IDENTIFICATION MODEL

In this paper, the identification process of D2D communication is shown in Fig.1, which is including signal acquisition, RF fingerprint formation and classification methods. Firstly, Hilbert transform is used to analyze the signal feature. Secondly, principal component analysis (PCA) is used to reduce feature dimensionality and get the RF fingerprint. Finally, support vector machine is used as classifier based on cross-validation parameter selection.

A. Hilbert transform

In a communication system, it is often necessary to decompose a signal into orthogonal components, that is, to decompose into an in-phase component and a quadrature component. Hilbert transform has been widely used in the field of communication.

The Hilbert transform of function \( x(t) \) is defined as the convolution of \( x(t) \) with function \( h(t) = \frac{1}{\pi t} \), which can be expressed as follows:

\[
H \{ x(t) \} = x^h(t) = x(t) * h(t) = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{x(f)}{t-f} df
\]

(1)
Where: * is convolution operation; \( H[x(t)] \) and \( x'(t) \) is the Hilbert transform in time domain. And that in the frequency domain is expressed as follows:

\[
X^h(f) = X(f)H(f)
\]  

(2)

Since the Fourier transform of \( h(t) \) is expressed as follows:

\[
F[h(t)] = H(f) = -j\text{sgn}(f) = \begin{cases} 
1 & f > 0 \\
-1 & f < 0 
\end{cases}
\]  

(3)

Where, \( \text{sgn}(f) \) is a symbolic function.

B. Principal component analysis

PCA is data compression based on minimum mean square error criterion. Suppose, a training set with \( m \) samples is \( X = \{x_1, x_2, \ldots, x_m\} \), \( x_i \) is a \( n \)-dimensional vector. Meantime, a lower dimensional data set is \( Y = \{y_1, y_2, \ldots, y_m\} \), \( y_i \) is an one-dimensional vector.

The PCA processing steps are shown as follows:

1. Data preprocessing

The training sample is centralized, making its mean zero.

\[
\mu_x = \frac{1}{m}\sum_{i=1}^{m} x_i
\]  

(4)

\[
x_i' = x_i - \mu_x
\]  

(5)

The matrix after centralization is \( X' = \{x_1', x_2', \ldots, x_m'\} \)

(2)

2. Calculate the covariance matrix of the sample is express as follows:

\[
C_x = X'X'^T
\]  

(6)

3. The eigenvalues \( \lambda_1, \lambda_2, \ldots, \lambda_n \) and eigenvectors \( \{a_1, a_2, \ldots, a_n\} \) of the covariance matrix are express as follows:

\[
C_x. a = \lambda a
\]  

(7)

The feature values are arranged from large to small, and the feature vector corresponding to the first one eigenvalue of the covariance matrix is selected to form a new transformation matrix \( A \).

\[
A = \begin{bmatrix} 
\lambda_1 & 0 & \cdots & 0 \\
0 & \lambda_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \lambda_n 
\end{bmatrix}
\]  

(8)

\[
\sum_{i=1}^{l} \lambda_i \geq k
\]  

(9)

\[
\sum_{i=1}^{l} \lambda_i
\]  

(10)

\[
A = \{a_1, a_2, \ldots, a_l\}
\]

\( k \) represents the percentage of data after dimension reduction with the percentage of the original data set. If \( k=95\% \), it means the energy of the training sample on the first \( k \) axes accounts for 95% of the total energy. \( k \) can also be selected based on the input of the classifier.

4. Calculate the new sample matrix \( Y \) after dimensionality reduction.

The original centralization data \( Y = \{y_1, y_2, \ldots, y_m\} \) is multiplied by the transposed matrix of the feature vector, where each sample is one-dimension. The original training sample data is subtracted from its mean value to ensure that the training sample and the test sample are converted into the same sample space.

\[
Y = A^T \times X'
\]  

(11)

C. SVM based on cross-validation parameter selection

The support vector machine (SVM) theory was proposed by Vapnik to solve the pattern recognition problem, which had been improved by many scholars till now. The goal of the SVM algorithm is to construct a decision function which can be used to classify the test data as accurately as possible.

\[
\tilde{f}(x) = \text{sign}(\omega \cdot x + b)
\]  

(12)

Where sign is symbolic function. The most hyperplane solution needs to maximize \( 2/\|\omega\|^2 \). In other words, minimize \( \frac{1}{2}\|\omega\|^2 \). \( \omega \) is the normal vector, \( b \) is the displacement term. For the following secondary planning problem. It is the basic type of SVM.

\[
\min_{\omega,b} \frac{1}{2}\|\omega\|^2
\]  

(13)

s.t. \( \gamma_i (\omega \cdot x_i + b) \geq 1 \quad i = 1, 2, \ldots, l \)

Based on the basic model, in this paper, a cross-validation of radial basis kernel function parameters (C, V) is used to establish a SVM classifier based on cross-validation, which is called CV-SVM. Cross-validation uses the grid search method based on parameters C and V is essentially to try various combinations of parameter pairs (C, V), and then select the parameter with the highest cross-validation accuracy as the final parameter to train. It is found that searching for sequences with exponential growth on C and V have better parameters.
When the parameters C and V increase with the step size, the accuracy is displayed on the z-axis. It can be seen that when (C,V) takes different values, the classification accuracy is different. In the paper, the step size of the parameter (C,V) grid search is $2^{0.5}$. Traditional SVM is used to determine parameters based on the experience of users. As there are many parameters, parameter adjustment is a thorny problem for users. However, CV-SVM overcomes the problem of parameter selection, and it will directly give parameters with satisfactory performance.

IV. D2D COMMUNICATION SECURITY AUTHENTICATION BASED ON RF FINGERPRINT IDENTIFICATION

The complete D2D communication trust management process is shown in Fig.3, which includes three phases: database establishment phase, RF fingerprint extraction and identification phase, D2D device trust management phase. The three phases are described as follows.

A. Database Establishment Phase

During this period, all the legal D2D device is give a unique identity tag, and their RF fingerprints are extracted based on the proposed method in this paper. Then, a database is set up with the legal D2D device, identify tag and RF fingerprint.

B. RF Fingerprint Extraction and Identification Phase

After the database is established, all the legal D2D device can be certified. When a device signal is detected and received, the RF fingerprint is extracted, and the individual device is recognized. Finally, the device identity tag can be obtained.

C. D2D Device Trust Management Phase

In D2D device trust management phase, the legal devices will get the access permission and transmit the information between each other. The trust management method should be used to keep the security of D2D communication. The specific process is as follows:

**D2D Device Trust Management Algorithm**

**Data:** RF Fingerprint$_A$, IDT$_A$. RF Fingerprint data of legitimate devices stored in the background

**Result:** Second stage of authentication success or authentication failed

**Input:** RF Fingerprint$_A$, IDT$_A$

**for** $i=1:n$ (RF Fingerprint dimension of the device corresponding to IDT$_A$)

$$\text{mean}_RF\text{-Fingerprint}=\text{mean}(\text{IDT}_RF\text{-Fingerprint});$$

**end**

IDT$_{RF\text{-Fingerprint}}$: IDT$_A$ corresponds to the device's RF Fingerprint;

**mean**(x): mean function;

**for** $i=1:m$ (The number of training samples of the RF Fingerprint of the device corresponding to IDT$_A$)

$$\text{mean}_D=\text{mean}(\text{dis}(\text{IDT}_RF\text{-Fingerprint}, \text{mean}_RF\text{-Fingerprint}));$$

**end**

$\text{dis}(x,y)$: calculate the Euclidean distance of the vector $x$ and $y$;

**for** $i=1:m$

$$D=\text{mean}(\text{dis}(\text{RF Fingerprint}_A, \text{mean}_RF\text{-Fingerprint}));$$

**end**

if $\text{mean}_D*N>D$ ($N$ is the distance coefficient used to adjust the error probability of this method)

**Result:** Add trust to device A and start D2D communication;

else

**Result:** Cancel trust on device A and terminate the communication protocol;

**end**

V. SIMULATION AND ANALYSIS

In the simulation experiment, the data set is collected from ten wireless devices, which contains 500 samples. Each wireless device has 50 samples, and each sample has a feature dimension of 159,901. The ratio between training set and test set is 2:3, which means the training set has 200 samples and the test set has 300 samples. The acquisition device is a high performance Agilent oscilloscope. In the experiment, the influence of noise environment and channel environment on device information during the acquisition process is not considered.
Firstly, Hilbert transform is performed on the samples, the amplitude is extracted and the absolute value is calculated. Secondly, because the dimension of the data sample is too large, it is necessary to reduce the dimension. In this simulation, it is sampled at a ratio of 50:1 and the dimension reduces to 50 by using PCA method. Finally, CV-SVM is used as classifier. Two parameters \((C, V)\) of CV-SVM are selected between \(2^{-4}\) and \(2^{4}\) through cross-validation and grid search. Since parameters \((C, V)\) selected by cross-validation are different under each SNR, they are not listed here. In the simulation, Gaussian white noise is added to the data set. Fig.4 and Fig.5 show the recognition rate of the test set according to the RF Fingerprint recognition method mentioned in this paper.

![Signal recognition rate confusion matrix](image_url)

(d) SNR is 15 dB

**FIGURE 4.** Confusion Matrix of Ten Wireless Devices.

![Wireless Device Recognition Rate Under Different SNR.](image_url)

**FIGURE 5.** Wireless Device Recognition Rate Under Different SNR.

According to the Fig.4 and Fig.5, in low SNR, the recognition rate is always higher than 70%, but there are still many misjudgments. In Fig.4(a), it can be seen that the algorithm is not ideal for the classification performance of 10 wireless devices with a signal-to-noise ratio of 0 dB. Classification performance improved significantly in Fig.4(a), (b) and (c). However, with the increasing of SNR, the recognition rate of the proposed method is increasing steadily. When the SNR is 2 dB, the recognition rate is more than 80%; when the SNR is 5 dB, the recognition rate is more than 90%. Moreover, when the SNR is larger than 8 dB, the recognition rate is 100%. Therefore, the proposed method is effective for the security and trust management of D2D communication.

VI. CONCLUSION

For the trust management of D2D communication, in this paper, a wireless device authentication method is proposed based on RF fingerprint technology. The Hilbert transform and PCA method is used to generate the RF fingerprint, and CV-SVM is used to classify the wireless devices. Simulation results show that when SNR is higher than 8 dB, the recognition rate is 100%. Therefore, the proposed method is...
V. ACKNOWLEDGEMENT

The authors would like to thank the special funding project of Civil Aviation University of China for the basic scientific research services of the Central University (3122013z006) and Shandong province key project development plan (2016GGX101023).

REFERENCES


