Research on Consistency Enhancement of Wireless Channel Key Against RF Fingerprint

Mingming Zhang¹, Chao Xu²,a,*, Meng Li¹, Fei Xia¹ and Ran Zhao¹

¹State Grid Jiangsu Electric Power Co., Ltd. information & communication branch
²Jiangsu Electric Power Information Technology Co., Ltd.
a dayangxx@163.com

Abstract The development of the physical layer key extraction technology provides a new type of encryption mechanism that uses the reciprocity and time varying of wireless channels to generate keys. This encryption mechanism can achieve informational security. However, the wireless channels in the real environment are not completely reciprocal, which results in low consistency in generating the keys. In this paper, we study the influence of RF fingerprint on channel reciprocity, and propose a calibration matrix algorithm resist the RF fingerprint effect. Based on the RF fingerprinting model established previously, we propose two calibration methods from the perspective of RF gain and I/Q gain. The superiority of the two calibration methods is proved by the average system capacity and the linear quantification error rate. Next, we extend the calibration matrix algorithm of narrowband systems to wideband OFDM systems. The applicability of the calibration matrix algorithm in OFDM systems is proved by the linear quantification error rate of the uplink and downlink channels. In order to prove the reliability of the algorithm in the real environment, we use a USRP to collect multiple sets of measured data, and analyse the data through the calibration algorithm. The final result shows that this algorithm makes the uplink and downlink channel reciprocity compensated.

1. The principle of RF fingerprint
In wireless communication system, radio frequency fingerprint (RFF) is the inherent property of communication equipment [1-3]. It is mainly caused by the physical characteristics of integrated circuits. In the research of physical layer security, RF fingerprint has been used as the method of device authentication [4]. Therefore, the research of RF fingerprint has been paid more and more attention at home and abroad. But on the other hand, for a large number of key systems based on channel reciprocity, the existence of RF fingerprints leads to the reduction of reciprocity. RF fingerprint will offset the amplitude and phase of the received signal, and affect the consistency of the key. The main problem of this paper is how to resist the influence of RF fingerprint on key consistency.

Before solving this problem, we should first understand the principle and characteristics of RF fingerprint generation. The concept of RF fingerprint was first proposed by J. hall in 2003. At that time, this concept was proposed for ID authentication of Bluetooth devices. This paper will take the traditional digital communication system as an example to illustrate the principle of RF fingerprint generation. In the digital communication system in Figure 1, this part of the module is mainly digital to analog converter, filter, converter, power amplifier and transceiver antenna. The tolerance of these electronic components is the main source of RF fingerprint. Tolerance refers to the deviation between electronic components and other similar components in the process of production or use. Tolerance
can be divided into two categories: manufacturing tolerance and drift tolerance [5-6]. Among them, manufacturing tolerance refers to the internal difference of integrated circuit caused by different processing materials and processes during the manufacturing of electronic container parts. Manufacturing tolerance makes the hardware parameters of electronic devices have certain error with the standard value. This part of the error is usually one hundred grade or one thousand grade. The higher the accuracy is, the lower the manufacturing tolerance is. The drift tolerance refers to the difference in the use of electronic components due to different environments and different use times. These tolerances even make the signal gain of different devices of the same RF equipment of the same manufacturer different. These hardware tolerances are the same as human fingerprint, and they are different. Therefore, the probability of two transceiver having the same RF fingerprint is close to zero. It's like there are no two leaves in the world, so RF fingerprints can be used for device authentication.

Although there are many researches on RF fingerprint, it is not feasible to use today's mobile devices to achieve RF authentication. Considering the non-idealist of the RF device, the RF fingerprint deviation is a limiting factor that affects the key consistency of the communication system. Key consistency is based on channel reciprocity. In this paper, RF fingerprint is divided into two parts. One part is the RF gain part, which will affect the amplitude and gain of channel measurement. The other part is the I/Q imbalance, which will cause the phase difference and amplitude gain difference between the two I/Q channels.

Another reason for RF fingerprint distortion is the in-phase / quadrature (I / Q) imbalance of RF signal [7]. I / Q imbalance can also be represented by the unequal amplitude gain and the non-orthogonal phase of the two signals. This section still considers a 2 × 2 MIMO system:

\[
Y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & L_{2,2} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = HX + N
\]

Where \( y_i \) (\( i = 1, 2 \)) represents the complex signal received by the \( i \)th receiving antenna, \( x_i \) (\( i = 1, 2 \)) represents the complex signal sent by the \( i \)th transmitting antenna, and \( x_i \) (\( i = 1, 2 \)) represents the additive complex Gaussian noise of the \( i \)th antenna. \( h_{i,j} \) is the channel coefficient, where \( i \) is the \( i \)th transmitting antenna and \( j \) is the \( j \)th receiving antenna. In order to analyse the influence of I/Q imbalance, it is necessary to transform each element in equation (1) into a combination of real part and virtual part. After finishing, we can get the equivalent 4 × 4 channel model: matrix:
Where I and Q represent I and Q signals respectively, i.e. the real part and the imaginary part of the signal. In order to get the fingerprint influence model of MIMO system, the undistorted signal of single antenna should be analysed first. Without considering distortion, the transmitted signal can be expressed as:

\[
x(t) = \text{Re} \left[ (x_t + jx_Q) e^{jw_t} \right] = x_t \cos w_t - x_Q \sin w_t
\]  

(3)

If complex Gaussian noise is not considered, the two I / Q channels of the received signal can be expressed as:

\[
y_I = (x_t \cos w_t - x_Q \sin w_t) \times 2 \cos w_t = x_t + x_t \cos 2w_t - x_Q \sin 2w_t
\]

(4)

\[
y_Q = (x_t \cos w_t - x_Q \sin w_t) \times (-2 \sin w_t) = x_Q - x_t \sin 2w_t - x_Q \cos 2w_t
\]

(5)

This is the I/Q two-way receiving signal when RF fingerprint is not added. If the signal is assumed to be affected by the I/Q imbalance of RF fingerprint, the error parameter needs to be added. \( \varepsilon_T \) and \( \varphi_T \) are used to represent the amplitude error factor and phase error factor of the signal. After adding these influence factors, rewrite the formula:

\[
x_T'(t) = x_t (1 + \varepsilon_T) \cos w_t - x_Q \sin (w_t + \varphi_T)
\]

(6)

\[
y_I'(t) = (x_t (1 + \varepsilon_T) \cos w_t - x_Q \sin (w_t + \varepsilon_T)) \times 2 \cos w_t
\]

\[
= x_t (1 + \varepsilon_T) - x_Q \sin \varphi_T + x_t (1 + \varepsilon_T) \cos 2w_t - x_Q \sin (2w_t + \varphi_T)
\]

(7)

\[
y_Q'(t) = (x_t (1 + \varepsilon_T) \cos w_t - x_Q \sin (w_t + \varepsilon_T)) \times (-2 \sin w_t)
\]

\[
= x_Q \cos \varphi_T - x_t (1 + \varepsilon_T) \sin 2w_t - x_Q \cos (2w_t + \varphi_T)
\]

(8)

Equation (7) and equation (8) pass through the filter at the receiving end, and the left part is \( x_t (1 + \varepsilon_T) - x_Q \sin \varphi_T \) and \( x_Q \cos \varphi_T \) respectively. The impact of this I/Q imbalance at the sending end can be expressed by the following matrix:

\[
\begin{bmatrix}
x_I' \\
x_Q'
\end{bmatrix} = \begin{bmatrix}
1 + \varepsilon_T & -\sin \varphi_T \\
0 & \cos \varphi_T
\end{bmatrix} \begin{bmatrix}
x_I \\
x_Q
\end{bmatrix}
\]

(9)

Among them, \( a \) is a normalization factor to make the signal power not change due to the influence of I/Q imbalance. Here, the signal is divided into two I/Q channels to analyse their changes. This is only the distortion of the signal at the transmitter. It also needs to analyse the RF fingerprint factor at the receiver. Therefore, \( \varepsilon_R \) and \( \varphi_R \) are also used to represent the amplitude error factor and phase error factor of I/Q.

\[
y_I'' = (x_t \cos w_t - x_Q \sin w_t) \times 2 (1 + \varepsilon_R) \cos w_t
\]

\[
= x_t (1 + \varepsilon_T) + x_t (1 + \varepsilon_R) \cos 2w_t - x_Q (1 + \varepsilon_R) \sin 2w_t
\]

(10)
\[
y_Q'' = \left( x_I \cos w_c t - x_Q \sin w_c t \right) \times 2 \left( 1 + \varepsilon_V \right) \cos w_c t
\]
= \left[ -x_I \sin \varphi_R - x_Q \cos \varphi_R - x_I \sin \left( 2w_c t + \varphi_R \right) - x_Q \cos \left( 2w_c t + \varphi_R \right) \right] \tag{11}

After formula (10) and formula (11) pass through the receiver filter, the remaining parts are \( x_I \left( 1 + \varepsilon_R \right) \) and \(-x_I \sin \varphi_R + x_Q \cos \varphi_R \) respectively. The impact of this I/Q imbalance at the receiver can be expressed by the following matrix:

\[
\begin{bmatrix}
y_I \\
y_R
\end{bmatrix} = a' \begin{bmatrix}
1 + \varepsilon_T \\
-\sin \varphi_T \\
\cos \varphi_T
\end{bmatrix}
\begin{bmatrix}
y_I \\
y_Q
\end{bmatrix}
\tag{12}
\]

Where a’, as before, is the normalization factor. So far, the impact analysis of I/Q imbalance in the case of single antenna has been completed, and the case of single antenna can be extended to 2 × 2 MIMO system.

For 2 × 2 MIMO system. The model of transmit signal, receive signal and I/Q imbalance influence matrix can be established as follows:

\[
\begin{bmatrix}
x_1 \\
x_2
\end{bmatrix} = \begin{bmatrix}
x_{1I} + jx_{1Q} \\
x_{2I} + jx_{2Q}
\end{bmatrix},
X = \begin{bmatrix}
x_{1I} \\
x_{2I}
\end{bmatrix},
\begin{bmatrix}
y_1 \\
y_2
\end{bmatrix} = \begin{bmatrix}
y_{1I} + jy_{1Q} \\
y_{2I} + jy_{2Q}
\end{bmatrix},
Y = \begin{bmatrix}
y_{1I} \\
y_{1Q} \\
y_{2I} \\
y_{2Q}
\end{bmatrix}
\tag{13}
\]

\[
L_T = \begin{bmatrix}
a_{T1} \left( 1 + \varepsilon_T \right) & -a_{T1} \sin \varphi_{T1} & 0 & 0 \\
0 & a_{T1} \cos \varphi_{T1} & 0 & 0 \\
0 & 0 & a_{T2} \left( 1 + \varepsilon_T \right) & -a_{T2} \sin \varphi_{T2} \\
0 & 0 & 0 & a_{T2} \cos \varphi_{T2}
\end{bmatrix}
\tag{14}
\]

\[
L_R = \begin{bmatrix}
a_{R1} \left( 1 + \varepsilon_R \right) & 0 & 0 & 0 \\
-a_{R1} \sin \varphi_{R1} & a_{R1} \cos \varphi_{R1} & 0 & 0 \\
0 & 0 & a_{R2} \left( 1 + \varepsilon_R \right) & 0 \\
0 & 0 & 0 & a_{R2} \sin \varphi_{R2} \cos \varphi_{R2}
\end{bmatrix}
\tag{15}
\]

Where equation (13) are the transmission signal of two antennas at the transmitting end and the reception signal of two antennas at the receiving end. Equation (14) is the I/Q imbalance influence matrix of the transmitter, where 1 and 2 correspond to the normalization factors of the two transmit antennas. The amplitude and phase errors of \( \varepsilon_{T1}, \varepsilon_{T2}, \varphi_{T1}, \varphi_{T2} \) for I/Q imbalance. The corresponding equation (15) is the I/Q imbalance influence matrix of the receiver, in which the parameters correspond to equation (14) one by one. In TDD-MIMO system, we can get the RF fingerprint influence matrix corresponding to base station and mobile terminal, \( L_{BT}, L_{MT}, L_{BR}, L_{MR} \), in which \( L_{BT} \), \( L_{MT} \), and \( L_T \) form is the same, \( L_{BR}, L_{MR} \), and \( L_R \) form is the same. Similar to the processing method of RF gain, the uplink and downlink channel matrix under the influence of I/Q unbalanced RF fingerprint can be obtained:

\[
H_D = L_{MR} H L_{BT}, H_U = L_{BR} H^T L_{MT}
\tag{16}
\]

Where h is the channel matrix in equation (2). So far, the impact analysis caused by I/Q imbalance has been completed, and the calibration method will be obtained through this model later.
3. Principle of calibration matrix method for I/Q imbalance

In a single communication, relative to the fast time-varying channel, the influence factor of RF fingerprint is almost unchanged. In this section, the calibration matrix is still calculated before each communication. This calibration matrix will not be calculated in each subsequent communication, and the results of the first calculation will be used directly.

Because the RF fingerprint matrix of I/Q imbalance is no longer a diagonal matrix, in order to calibrate the reciprocity of the uplink and downlink channels, the calibrated uplink and downlink channels need to meet the following formula:

$$L_{MR}HL_{BR}K_D = \left(L_{BR}H^TL_{MT}K_U\right)^T = K_U^TL_{MT}^THL_{BR}^T$$

(17)

In the discussion of I/Q imbalance, \(H\) refers to the channel \(4 \times 4\) channel matrix in equation (9). From equation (17), we can further obtain:

$$HL_{BR}K_D \left(L_{BR}^T\right) = \left(L_{BR}\right)^{-1}K_U^TL_{MT}^TH$$

(18)

Therefore, the expression of calibration matrix \(K_D\) and \(K_U\) can be obtained:

$$K_D = \left(L_{BR}\right)^{-1}L_{BR}^T, \quad K_U = \left(L_{MT}\right)^{-1}L_{MR}^T$$

(19)

Because the influence matrix of RF fingerprint is no longer a diagonal matrix, so \(K_D\) and \(K_U\) are not diagonal matrices. From the above two formulas, we can get their matrix form as follows:

$$K_D = \begin{bmatrix}
    a_1 & b_1 & 0 & 0 \\
    0 & c_1 & 0 & 0 \\
    0 & 0 & a_2 & b_2 \\
    0 & 0 & 0 & c_2
\end{bmatrix}, \quad K_U = \begin{bmatrix}
    d_1 & e_1 & 0 & 0 \\
    0 & f_1 & 0 & 0 \\
    0 & 0 & d_2 & e_2 \\
    0 & 0 & 0 & f_2
\end{bmatrix}$$

(20)

The obtained calibration matrix shall meet the minimum result of the following formula:

$$\left\|H_DK_D - (H_UK_U)^T\right\|_F$$

(21)

After \(vec(\ldots)\) operation, you can get:

$$vec\left(H_DK_D - (H_UK_U)^T\right) = \left(I \otimes H\right)vec\left(K_D\right) - \left(H_UI\right)vec\left(K_U^T\right)$$

(22)

Where \(I\) is a \(4 \times 4\) unit matrix. Can get \(vec(K_D)\) and \(vec(K_U^T)\):

$$vec\left(K_D\right) = S_Dd_D, \quad vec\left(K_U^T\right) = S_Ud_U$$

(23)

Therefore, equation (22) can be rewritten as follows:

$$\left(I \otimes H_D\right)S_Dd_D - \left(H_U \otimes I\right)S_Ud_U = \left[I \otimes H_D\right]S_D - \left(H_U \otimes I\right)S_U \begin{bmatrix}d_D \\ d_U\end{bmatrix}$$

(24)

According to equation (24), a \(16 \times 12\) matrix \(W = \left[I \otimes H_D\right]S_D - \left(H_U \otimes I\right)S_U\). The value of calibration matrix can be obtained by solving this matrix.

4. Experimental Result

This experiment consists of two laptops connected with general radio peripheral N210. Through the GNU radio software on the notebook computer to set the parameters of both sides of the communication, two general radio peripherals can carry out data transmission. In the communication process, the modulation and demodulation operation is completed by computer software, while the high-speed processing such as frequency conversion is completed by the general radio peripheral. Write the same IP address to the two general radio peripherals, through which the computer can identify the radio peripherals and receive the communication data between them through the Ethernet port. Finally, the computer uses MATLAB to estimate the channel of the received data, and gets the experimental data needed in this paper.
Figure 2 is the comparison before and after using the calibration matrix algorithm for one group of data. The former shows the comparison of uplink and downlink channels before calibration. It can be seen that the modulus value of uplink channel is always greater than that of downlink channel, which is mainly affected by RF fingerprint, as well as some sudden interference and noise in wireless channel. The latter shows the comparison of the up and down channels after calibration. The two channels are basically overlapped, which shows that it has a good calibration ability for this set of RF fingerprints.

![Figure 2. Channel coefficient before and after calibration](image)

**Acknowledgement**

Project Name: Research and Application of Wireless Access Security Management Platform based on Device Fingerprint Technology

Project Source: Science and Technology Project of State Grid Jiangsu Electric Power Co., Ltd

**Reference**

[1] Raeesi O, Zou Y, Antti Tölli, et al. Closed-form Analysis of Channel Non-Reciprocity Due to Transceiver and Antenna Coupling Mismatches in Multi-user Massive MIMO Network[C]// IEEE GLOBECOM 2014 (Massive MIMO: From theory to practice workshop). IEEE, 2014.

[2] Li G, Sun C, Zhang J, Jorswieck E, Xiao B, Hu A. "Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities", Entropy. 2019; 21(5):497.

[3] Bourdoux A, Come B, Khaled N. Non-reciprocal transceivers in OFDM/SDMA systems: impact and mitigation[C]// Radio & Wireless Conference. IEEE, 2003.

[4] Guyue Li, Aiqun Hu, Yaning Zou, Linning Peng, Mikko Valkama, "A Novel Transform for Secret Key Generation in Time-varying TDD Channel under Hardware Fingerprint Deviation", in Proc.IEEE 82th Vehicular Technology Conference (VTC2015-Fall), Boston, Sep. 2015, pp.1-5.

[5] Honglin Y, Aiqun H. Fountainhead and uniqueness of RF fingerprint[J]. Journal of Southeast University(Natural Science Edition), 2009.

[6] Guyue Li, Jiabao Yu, Yuexiu Xing, and Aiqun Hu. Location-invariant physical layer identification approach for WiFi devices. IEEE Access, vol.7, no.1, pp.106973-106985, 2019.

[7] Liang Y, Li H, Li F, et al. Channel Compensation for Reciprocal TDD Massive MIMO-OFDM With IQ Imbalance[J]. IEEE Wireless Communications Letters, 2017, 6(6):778-781.