Hao *et al. EURASIP Journal on Wireless Communications and Networking* (2019) 2019:64
https://doi.org/10.1186/s13638-019-1369-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Amplify-and-forward relay identification using joint Tx/Rx I/Q imbalance-based device fingerprinting

Peng Hao, Xianbin Wang* and Aydin Behnad

Abstract

Relay identification is necessary in many cooperative communication applications such as detecting the presence of malicious relays for communication security, selecting the intended relays for signal forwarding, and tracing a specific relay. However, this identification task becomes extremely challenging for amplify-and-forward (AF) relaying systems since AF relays usually have no capability of adopting traditional identification methods implemented above the physical layer. This paper proposes a physical-layer AF relay identification scheme based on the exploitation of the device-specific in-phase and quadrature-phase imbalance (IQI) feature. Given that IQI estimation is mandatory in most present receivers for compensation, it is cost-effective to make use of these estimation results for fingerprinting AF relays. A generalized likelihood ratio test-based fingerprint differentiation technique is adopted to detect the minor difference between two range-limited IQI fingerprints. Using this differentiation technique, a whitelist-based identification algorithm consisting of fingerprint registration, update, and identification is proposed. Furthermore, the optimal training signals that lead to the maximal detection probability are derived for the typical quadrature amplitude modulation and phase-shift keying modulation schemes. The simulation results validate our derivations and confirm that the proposed method can accurately identify AF relays.

Keywords: Amplify-and-forward, Device fingerprint, GLRT, Relay identification, Tx/Rx I/Q imbalance, Optimal signal

1 Introduction

Relaying technique is a promising part of 5G and beyond cellular networks since it works toward broadening the communications coverage area, improving the communication reliability, and increasing the throughput of the network. In an ideal scenario, the identity of an intermediate relay is inessential for the destination device as long as the relay can provide satisfactory quality of service without any malicious behavior. However, identifying relay nodes is of great importance in practice. Signal relaying can potentially introduce new communication security threats, such as the ghost-and-leech attack [1], the man-in-the-middle attack [2], and the denial of service attack [3]. Some relay selection schemes require pre-classifying relays into trusted or untrusted groups for cooperation [4–6]. In these cases, relay identification is necessary either to detect the malicious relay nodes or to classify those intended relays. In addition, the applications of relay identification can be extended to wireless device localization and tracking [7, 8].

Although a cross-layer decode-and-forward relay identification was investigated in [8], this method cannot be applied to amplify-and-forward (AF) relay identification since AF nodes only work in the physical layer without any content modifications to the forwarded signals. This implies that all existing upper-layer identification methods are not applicable to the case of AF relaying, thus resulting in the need to fingerprint AF relays in the physical layer. It has been reported that a wireless transmitter can be identified by its unique hardware imperfections [9, 10]. At the transmitter side, all transmitted signals are inevitably affected by the device-specific RF front-end impairments. At the receiver side, both channel and RF

*Correspondence: xianbin.wang@uwo.ca
Department of Electrical and Computer Engineering, University of Western Ontario, London N6A 5B9, Ontario, Canada

imperfection estimations are usually mandatory for signal reception, and thus it is cost-effective to use these estimation results for wireless transmitter identification.

1.1 Related work

As a typical RF imperfection, transmitting (Tx) IQI has been studied for fingerprinting wireless transmitters [11–13]. The authors of [11] studied Tx IQI measurements of a large group of transmitters and concluded that IQI can uniquely represent the identity of a wireless transmitter. In [12], IQI fingerprinting was experimentally validated in the scenario of multiple 802.11n multiple-input multiple-output transmitters. The authors of [13] proposed a distance test (DT) method in which the Euclid distance between two Tx IQI fingerprints is used for device differentiation.

However, most current methods, including [11–13], are not suitable for AF relay identification. Unlike the regular transmitters, an AF must receive signals before the signal retransmission process. Given this fact, both receiving (Rx) and Tx IQI need to be taken into account in fingerprinting AF relays [14, 15]. The authors of [16, 17] proposed a varying fingerprint (VF) comprising both channel gain component and Tx/Rx IQI parameter component, where only the IQI parameter is useful for relay identification. However, the performance of using VF is inadequate in the case of small IQI values. In practice, the manufacturing market requires that the hardware-level imperfections (e.g., IQI parameter) must be small and within a limited range [18–20]. Due to the inevitable channel variation and estimation noise, the uniqueness, stability, and distinguishability of such small IQI parameters are remarkably weakened, thereby leading to degraded identification accuracy. To address these problems, an enhanced AF relay fingerprinting approach and high accuracy fingerprint differentiation technique with optimal performance design are urgently necessary.

1.2 Our methods and contributions

This paper proposes an accurate AF relay identification method using physical-layer IQI-based fingerprinting without the aid of any upper-layer identification technique. We consider small IQI values in a dual-hop AF relaying system in which the source node transmits signals to the destination node via an AF relay. Based on existing Rx/Tx IQI estimation results, we propose an improved AF relay fingerprint without channel gains interleaving compared to the VF fingerprinting method. This new fingerprint is used in our whitelist-based fingerprint registration and identification algorithms for relay identification. Moreover, we propose a generalized likelihood ratio test (GLRT)-based fingerprint differentiation technique and optimal signal designs to further improve the fingerprint identification accuracy under small IQI values. The main contributions of this paper are summarized as follows.

- We propose a new fingerprint of AF relay and analyze its dynamic range and features in order to reveal the main technical challenges in relay identification small IQI values. These general analysis results can also be useful in other IQI-related AF relaying performance studies.
- An accurate GLRT-based AF relay identification algorithm is proposed. The numerical results demonstrate that the introduced identification algorithm outperforms other identification methods [13, 17] in terms of distinguishing delicate IQI fingerprint differences, even with fewer symbols.
- Optimal and suboptimal training signals for quadrature amplitude modulation (QAM) and phase-shift keying (PSK) modulations are designed to maximize the capability of detecting an intended AF relay.

The remainder of this paper is organized as follows. Section 2 introduces the system model of our IQI-based AF relay identification. In Section 3, the features of IQI fingerprint are analyzed. A GLRT-based fingerprint differentiation technique is presented in Section 4. In Section 5, the fingerprint registration, identification, and update algorithms are described. In Section 6, the optimal and suboptimal signal designs are presented. Section 7 presents the numerical results and discussions. Finally, this paper is concluded in Section 8.

Notations: $(\cdot)^*$, $\mathbb{E}[\cdot]$, $|\cdot|$, $(\cdot)^T$, and $(\cdot)^H$ denote conjugate, expectation, absolute value, transpose, and conjugate transpose operations, respectively. Bold lowercase and uppercase letters represent vectors and matrices, respectively. For vector $\mathbf{a}$, we use a_k to show its kth element. $\mathbf{I}$ denotes the identity matrix. $\det(\mathbf{A})$ is the determinant of matrix $\mathbf{A}$. $\Re\{x\}$ and $\Im\{x\}$ denote the real part and imaginary part of x, respectively.

2 System model

This section mainly describes the system model for the AF relay's IQI fingerprint, the dual-hop AF relaying system, and the whitelist-based AF relay identification scheme. Finally, the objective of this study is presented.

2.1 IQI fingerprint model for AF relay

In an AF relay, all signal processing is accomplished in the physical layer. Specifically, the in-band received signal is down-converted, amplified, up-converted, and finally forwarded toward the destination node [14, 21]. We thus model the AF relay as the cascade of an Rx component, an amplifier, and a Tx component, as shown in Fig. 1. We consider the asymmetric IQI model [15, 22] in which

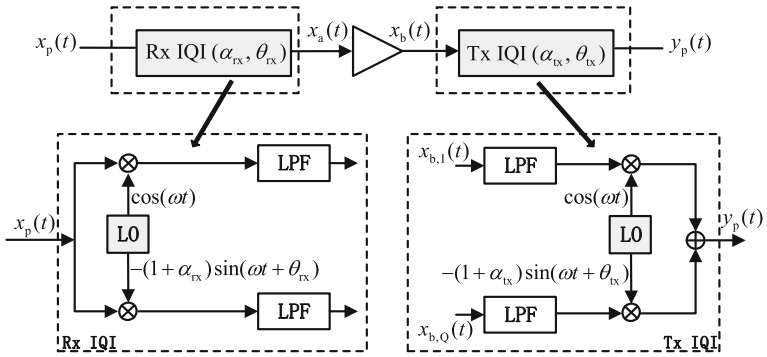

Fig. 1 Tx/Rx IQI model of the AF relay

the signal is affected by the Rx/Tx gain imbalance α_{rx}/α_{tx} and the Rx/Tx phase-shift imbalance θ_{rx}/θ_{tx}. Since the frequency-dependent IQI plays a minor role compared to the dominant effect caused by the frequency-independent IQI [23], the former is not considered in this model. After the imperfect RF front-end, the passband signal $y_p(t) = \Re\left\{y(t)e^{j\omega t}\right\}$ is forwarded to the destination, where $y(t)$ denotes the baseband equivalent signal as

$$y(t) = g_1 x(t) + g_2 x^*(t) \tag{1}$$

where

$$g_1 \triangleq a\left(\mu_{tx}\mu_{rx} + \nu_{tx}\nu_{rx}^*\right) \tag{2}$$

$$g_2 \triangleq a\left(\mu_{tx}\nu_{rx} + \nu_{tx}\mu_{rx}^*\right) \tag{3}$$

and $\mu_{rx} = \frac{1}{2}\left[1 + (1+\alpha_{rx})e^{-j\theta_{rx}}\right]$, $\nu_{rx} = \frac{1}{2}\left[1 - (1+\alpha_{rx})e^{j\theta_{rx}}\right] = 1 - \mu_{rx}^*$, $\mu_{tx} = \frac{1}{2}\left[1 + (1+\alpha_{tx})e^{j\theta_{tx}}\right]$ and $\nu_{tx} = \frac{1}{2}\left[1 - (1+\alpha_{tx})e^{j\theta_{tx}}\right] = 1 - \mu_{tx}$. Also, $x(t)$ is the baseband signal of the input $x_p(t) = \Re\left\{x(t)e^{j\omega t}\right\}$.

In this paper, g_1 and g_2 are the joint Tx/Rx IQI parameters and play the role of fingerprinting AF relays. Since IQI is a stable hardware feature, it can be steady in a time scale much longer than an identification session [24]. Hence, we consider that g_1 and g_2 are constants in the identification procedure. In addition, all of the following analyses are considered in the baseband domain.

2.2 System model for dual-hop AF relaying

We consider a dual-hop AF relay system consisting of a source node (S), an AF relay node (R), and a destination node (D). It is assumed that S, R, and D are equipped with a single antenna and operate in half-duplex mode. Thus, S first transmits the signal to R in the first phase, and then, R re-transmits the amplified signal to D in the second phase. It is considered that D can only receive signals via R. The two individual channels S–R and R–D experience independent block fading so that the instantaneous complex channel gains h_{SR} and h_{RD} are independent and fixed for a block [25–29]. n_{SR} and n_{RD} represent the receiving noises at R and D, which are circularly symmetric complex Gaussian (CSCG) random variables as $n_{SR} \sim CN\left(0, \sigma_1^2\right)$ and $n_{RD} \sim CN\left(0, \sigma_2^2\right)$.

As shown in Fig. 2, D is able to identify R through analyzing g_1 and g_2, which are extracted from the received signals. To avoid additional implementation costs, our identification method makes use of the channel and IQI estimation results, where such estimations are usually mandatory in most present receivers (i.e., D). Thus, we assume that D has the knowledge of h_{SR} and h_{RD} before performing the proposed identification method. Similar to [15], we consider the IQI-free S and D and focus on the IQI caused by the AF relays since it plays the important role of fingerprinting AF relays. Given that the IQI estimation is usually carried out using training signals, we consider the training signals in our identification method.

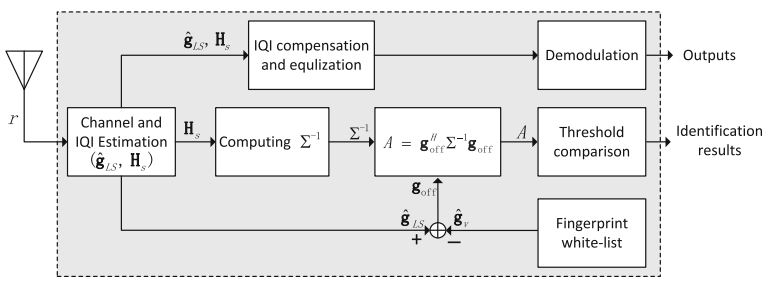

Fig. 2 Block diagram of the whitelist-based identification procedure at destination

In the S–R phase, an $N \times 1$ training symbol block $\mathbf{s}$ is transmitted from S to relay R. The kth received symbol at R can be represented as

$$x_k = s_k h_{\mathrm{SR}} + n_{\mathrm{SR}_k} \tag{4}$$

where s_k is the k-th transmitted symbol and has the average power $P = \mathbb{E}\left[s_k^* s_k\right]$, $k = 1, 2, \cdots, N$. In the R–D phase, using (1) and (4), the received Tx/Rx IQI distorted signal at D is

$$r_k = g_1 h_{\mathrm{SR}} h_{\mathrm{RD}} s_k + g_2 h_{\mathrm{SR}}^* h_{\mathrm{RD}} s_k^* + n_k \tag{5}$$

where $n_k = g_1 h_{\mathrm{RD}} n_{\mathrm{SR}k} + g_2 h_{\mathrm{RD}} n_{\mathrm{SR}k}^* + n_{\mathrm{RD}k}$. Let $\mathbf{H}_s = [\mathbf{s} \quad \mathbf{s}^*]\,\mathrm{diag}\left(h_{\mathrm{SR}} h_{\mathrm{RD}}, h_{\mathrm{SR}}^* h_{\mathrm{RD}}\right)$ and $\mathbf{g} = [g_1 \quad g_2]^T$, the observed block is

$$\mathbf{r} = \mathbf{H}_s \mathbf{g} + \mathbf{n} \tag{6}$$

The LS estimator, as a typical IQI estimator [19, 23], is then employed to estimate the IQI vector $\mathbf{g}$, which can be given by

$$\hat{\mathbf{g}}_{\mathrm{LS}} = \left(\mathbf{H}_s^H \mathbf{H}_s\right)^{-1} \mathbf{H}_s^H \mathbf{r} = \mathbf{g} + \left(\mathbf{H}_s^H \mathbf{H}_s\right)^{-1} \mathbf{H}_s^H \mathbf{n} \tag{7}$$

where the estimation error is $\mathbf{n}_g = \left(\mathbf{H}_s^H \mathbf{H}_s\right)^{-1} \mathbf{H}_s^H \mathbf{n}$. It is noteworthy that the Bayesian estimator is not suitable for our study since $\mathbf{g}$ is an unknown constant instead of a random variable.

2.3 Whitelist-based AF relay identification

Fig. 2 illustrates our whitelist-based AF relay identification based on the IQI estimation results [30]. We first whitelist the valid IQI fingerprints using the proposed fingerprint registration. After that, once a new relay tries to communicate with the destination node, the relay identification can be accomplished by comparing this new relay's fingerprint with the pre-registered fingerprints.

Our objective is to achieve accurate AF relay identification even with small IQI values through analyzing $\mathbf{g}$.

3 Device fingerprinting analysis

In this section, we analyze the important fingerprint (i.e., g_1 and g_2) to reveal the technical challenges in accurately identifying AF relays with small IQI values.

3.1 Fingerprint range analysis

Applying Euler's formula to (2) and (3), we get

$$\begin{aligned} g_1 = {} & \frac{a}{2}\left(1 + (1+\alpha_{\mathrm{tx}})(1+\alpha_{\mathrm{rx}})\cos(\theta_{\mathrm{tx}} - \theta_{\mathrm{rx}})\right) \\ & + j\frac{a}{2}(1+\alpha_{\mathrm{tx}})(1+\alpha_{\mathrm{rx}})\sin(\theta_{\mathrm{tx}} - \theta_{\mathrm{rx}}) \end{aligned} \tag{8}$$

$$\begin{aligned} g_2 = {} & \frac{a}{2}\left(1 - (1+\alpha_{\mathrm{tx}})(1+\alpha_{\mathrm{rx}})\cos(\theta_{\mathrm{tx}} + \theta_{\mathrm{rx}})\right) \\ & - j\frac{a}{2}(1+\alpha_{\mathrm{tx}})(1+\alpha_{\mathrm{rx}})\sin(\theta_{\mathrm{tx}} + \theta_{\mathrm{rx}}) \end{aligned} \tag{9}$$

Without the loss of generality, the ranges of amplitude and phase-shift imbalances are assumed to be $|\theta_{\mathrm{tx}}| \leqslant \theta_{m1}, |\theta_{\mathrm{rx}}| \leqslant \theta_{m2}, |\alpha_{\mathrm{tx}}| \leqslant \alpha_{m1}$, and $|\alpha_{\mathrm{rx}}| \leqslant \alpha_{m2}$. The ranges of $\Re\{g_1\}$, $\Im\{g_1\}$, $\Re\{g_2\}$ and $\Im\{g_2\}$ can be derived as

$$\begin{aligned} \frac{a}{2} + \frac{a}{2}\alpha_{\min}\cos\theta_{\max} \leqslant {} & \Re\{g_1\} \leqslant \frac{a}{2} + \frac{a}{2}\alpha_{\max}, \\ -\frac{a}{2}\alpha_{\max}\sin\theta_{\max} \leqslant {} & \Im\{g_1\} \leqslant \frac{a}{2}\alpha_{\max}\sin\theta_{\max}, \\ \frac{a}{2} - \frac{a}{2}\alpha_{\max} \leqslant {} & \Re\{g_2\} \leqslant \frac{a}{2} - \frac{a}{2}\alpha_{\min}\cos\theta_{\max}, \\ -\frac{a}{2}\alpha_{\max}\sin\theta_{\max} \leqslant {} & \Im\{g_2\} \leqslant \frac{a}{2}\alpha_{\max}\sin\theta_{\max} \end{aligned} \tag{10}$$

where $\alpha_{\min} = (1-\alpha_{m1})(1-\alpha_{m2})$, $\alpha_{\max} = (1+\alpha_{m1})(1+\alpha_{m2})$, and $\theta_{\max} = \theta_{m1} + \theta_{m2}$. To see the individual effect of amplitude imbalance and phase-shift imbalance on g_1 and g_2, we can set $\alpha_{\min} = \alpha_{\max} = 1$ to remove the amplitude imbalance, while set $\theta_{\max} = 0$ to remove the phase shift imbalance in (10). It is notable that we consider $a = 1$ in g_1 and g_2 in this study. For the cases $a \neq 1$, we can use g_1/a and g_2/a to replace g_1 and g_2 in our analysis.

As reported in [31], the realistic IQI can result in an image rejection ratio down to 20-40 dB, which is equivalent to $|\theta_{\mathrm{rx/tx}}| \leqslant 14.4212°$, $|\alpha_{\mathrm{rx/tx}}| \leqslant 0.22$. This is consistent with the IQI values used in [13, 19, 32]. Therefore, we reasonably define $(5° < \theta_{m1}, \theta_{m2} < 14.5°, 0.05 < \alpha_{m1}, \alpha_{m2} < 0.22)$ as the large IQI case, define $(0 < \theta_{m1}, \theta_{m2} < 5°, 0 < \alpha_{m1}, \alpha_{m2} < 0.05)$ as the small IQI case in our study, and give the numerical ranges of $\Re\{g_1\}$, $\Im\{g_1\}$, $\Re\{g_2\}$, and $\Im\{g_2\}$ in Table 1.

3.2 Signal-to-IQI-distortion ratio analysis

To mathematically represent the relative amount of g_1 and g_2, the signal-to-IQI-distortion ratio (defined in [18]) of our system is given by

$$\gamma = \frac{|g_1|^2}{|g_2|^2} = \frac{1 + \kappa^2 + 2\kappa\cos(\theta_{\mathrm{tx}} - \theta_{\mathrm{rx}})}{1 + \kappa^2 - 2\kappa\cos(\theta_{\mathrm{tx}} + \theta_{\mathrm{rx}})} \tag{11}$$

where $\kappa = (1+\alpha_{\mathrm{tx}})(1+\alpha_{\mathrm{rx}})$. The range of γ is further derived as

$$\gamma \in \left[1 + \frac{4}{\frac{\max(A_m, B_m)}{\cos\theta_{m1}\cos\theta_{m2}} + 2\tan\theta_{m1}\tan\theta_{m2} - 2}, \infty\right) \tag{12}$$

Table 1 The ranges of $\Re\{g_1\}, \Im\{g_1\}, \Re\{g_2\}$, and $\Im\{g_2\}$

IQI parameters	$\Re\{g_1\}$	$\Im\{g_1\}$	$\Re\{g_2\}$	$\Im\{g_2\}$
$\theta_{m1} = \theta_{m2} = 10°, \alpha_{m1} = \alpha_{m2} = 0.2$	[0.8007, 1.22]	[− 0.2463, 0.2463]	[− 0.22, 0.1993]	[− 0.2463, 0.2463]
$\theta_{m1} = \theta_{m2} = 5°, \alpha_{m1} = \alpha_{m2} = 0.05$	[0.9444, 1.0513]	[− 0.0957, 0.0957]	[− 0.0513, 0.0556]	[− 0.0957, 0.0957]

where $A_m = (1+\alpha_{m1})(1+\alpha_{m2}) + \frac{1}{(1+\alpha_{m1})(1+\alpha_{m2})}$, $B_m = (1-\alpha_{m1})(1-\alpha_{m2}) + \frac{1}{(1-\alpha_{m1})(1-\alpha_{m2})}$. The infinity in (12) denotes the IQI-free case.

Proof See Appendix 1. □

3.3 Challenges of identifying small and range-limited fingerprints

Substituting the large IQI and small IQI in (12), we obtain $10\log_{10}(\gamma) \in [\,11.142\ \text{dB}, \infty)$ and $[\,14.854\ \text{dB}, \infty)$, respectively, which implies that g_2 is always much less than g_1. Table 1 and the numerical result of (12) indicate that the ranges of $\Re\{g_1\}, \Im\{g_1\}, \Re\{g_2\}$, and $\Im\{g_2\}$ are extremely limited in small IQI case, which holds that $\Re\{g_1\} \approx 1$, and $\Im\{g_1\}, \Re\{g_2\}, \Im\{g_2\} \approx 0$ [18–20, 33, 34]. Therefore, the accurate detection of the differences between such range-limited IQI fingerprints $\mathbf{g}$ in the presence of estimation error term (i.e., $\mathbf{n}_g$) becomes further difficult.

In the following, we propose GLRT-based fingerprint differentiation technique and optimal signal designs to handle this challenging AF relay identification.

4 Generalized likelihood ratio test-based fingerprint differentiation

In this section, GLRT is applied to decide whether a fingerprint belongs to a pre-registered AF relay or not.

We assume that $\hat{\mathbf{g}}_\nu = \mathbf{g}_\nu + \mathbf{n}_\nu$ is one of the pre-registered valid fingerprints, where $\mathbf{g}_\nu$ denotes the actual value of this IQI fingerprint, and $\mathbf{n}_\nu$ denotes the estimation error. Since hardware-level IQI fingerprints are stable, the amount of $\mathbf{n}_\nu$ can be significantly reduced based on enough samples in the fingerprint registration phase, such as by using equal-gain combining, maximal-ratio combining, or selection combining techniques [16]. The fingerprint comparison between $\hat{\mathbf{g}}_{\text{LS}}$ and $\hat{\mathbf{g}}_\nu$ is

$$\mathbf{g}_{\text{off}} = \hat{\mathbf{g}}_{\text{LS}} - \hat{\mathbf{g}}_\nu = \Delta\mathbf{g} + \mathbf{n}_g - \mathbf{n}_\nu \tag{13}$$

where $\Delta\mathbf{g} = \mathbf{g} - \mathbf{g}_\nu$.

A binary hypothesis testing can be modeled by

$$\begin{cases} \mathcal{H}_0 : \Delta\mathbf{g} = \mathbf{0} \\ \mathcal{H}_1 : \Delta\mathbf{g} \neq \mathbf{0} \end{cases} \tag{14}$$

where hypothesis $\mathcal{H}_0$ means that the two compared fingerprints belong to the same AF relay, implying that $\mathbf{g} = \mathbf{g}_\nu$. Otherwise, hypothesis $\mathcal{H}_1$ is accepted.

According to Appendix 2, the elements of $\mathbf{n}$ can be modeled as CSCG variables. Therefore, their linear combination $\mathbf{n}_g$ is CSCG as well. The mean vector and covariance matrix of $\mathbf{g}_{\text{off}}$ can be given by

$$\begin{aligned} \mathbb{E}[\,\mathbf{g}_{\text{off}}] &= \mathbb{E}\left[\Delta\mathbf{g}\right] + \left(\mathbf{H}_s^H\mathbf{H}_s\right)^{-1}\mathbf{H}_s^H\mathbb{E}[\,\mathbf{n}] + \mathbb{E}\left[\mathbf{n}_\nu\right] \\ &= \Delta\mathbf{g} \end{aligned} \tag{15}$$

$$\begin{aligned} \mathbf{\Sigma} &= \mathbb{E}\left[(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})^H\right] \\ &= \mathbb{E}\left[\mathbf{n}_g\mathbf{n}_g^H\right] - \mathbb{E}\left[\mathbf{n}_g\mathbf{n}_\nu^H\right] - \mathbb{E}\left[\mathbf{n}_\nu\mathbf{n}_g^H\right] + \mathbb{E}\left[\mathbf{n}_\nu\mathbf{n}_\nu^H\right] \\ &= \mathbf{\Sigma}_g + \mathbf{\Sigma}_\nu \end{aligned} \tag{16}$$

where

$$\begin{aligned} \mathbf{\Sigma}_g = &\frac{\sigma^2}{|h_{\text{SR}}h_{\text{RD}}|^4\left(\sum_{i=1}^N\sum_{j=1}^N|s_i|^2|s_j|^2 - \left|\sum_{i=1}^N s_i\right|^2\right)} \\ &\times\begin{bmatrix} R_1 & R_2 \\ R_3 & R_4 \end{bmatrix} \end{aligned} \tag{17}$$

where σ^2 is the variance of n_g, and

$$R_1 = R_4 = |h_{\text{SR}}h_{\text{RD}}|^2\sum_{i=1}^N|s_i|^2, \tag{18a}$$

$$R_2 = R_3^* = -\left(h_{\text{SR}}^*\right)^2|h_{\text{RD}}|^2\sum_{i=1}^N s_i^{*2}. \tag{18b}$$

In (16), $\mathbb{E}\left[\mathbf{n}_g\mathbf{n}_\nu^H\right] = \mathbb{E}\left[\mathbf{n}_g\right]\mathbb{E}\left[\mathbf{n}_\nu^H\right] = 0$ and $\mathbb{E}\left[\mathbf{n}_\nu\mathbf{n}_g^H\right] = \mathbb{E}[\,\mathbf{n}_\nu]\,\mathbb{E}\left[\mathbf{n}_g^H\right] = 0$ since $\mathbf{n}_g$ and $\mathbf{n}_\nu$ are independent variables. The expression of $\mathbf{\Sigma}_\nu$ depends on the specific processing in the fingerprint registration phase. Taking equal-gain combining as an example, $\mathbf{n}_\nu = \frac{1}{Z}\sum_i^Z\mathbf{n}_{\nu,i}$, where $\mathbf{n}_{\nu,i}$ denotes the ith estimation error. Similar to $\mathbf{n}_g$, $\mathbf{n}_{\nu,i}$ are independent and identically distributed circularly symmetric complex Gaussian variables. Given $\mathbb{E}\left[\mathbf{n}_{\nu,i}\mathbf{n}_{\nu,j}^H\right] = 0, i \neq j$, $\mathbf{\Sigma}_\nu$ can be given by

$$\mathbf{\Sigma}_\nu = \frac{1}{Z^2}(\mathbf{\Sigma}_{\nu,1} + \mathbf{\Sigma}_{\nu,2} + \cdots + \mathbf{\Sigma}_{\nu,Z}) \tag{19}$$

where each $\mathbf{\Sigma}_{\nu,i} = \mathbb{E}[\,\mathbf{n}_{\nu,i}\mathbf{n}_{\nu,i}^H]$. Consequently, we can get $\mathbf{g}_{\text{off}} \sim CN(\Delta\mathbf{g}, \mathbf{\Sigma})$. Given that $\mathbf{g}_{\text{off}}$ is a zero-mean and non-zero mean complex normal vector under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, the likelihood functions of $\mathbf{g}_{\text{off}}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ can be given by [35]

$$p(\mathbf{g}_{\text{off}}|\mathcal{H}_0) = \frac{1}{\pi^2|\det(\mathbf{\Sigma})|}\exp\left(-\mathbf{g}_{\text{off}}^H\mathbf{\Sigma}^{-1}\mathbf{g}_{\text{off}}\right) \tag{20}$$

$$\begin{aligned} p(\mathbf{g}_{\text{off}}|\mathcal{H}_1) = &\frac{1}{\pi^2|\det(\mathbf{\Sigma})|} \\ &\times\exp\left(-(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})^H\mathbf{\Sigma}^{-1}(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})\right) \end{aligned} \tag{21}$$

where $\Delta\mathbf{g} \neq \mathbf{0}$ in Eq. (21).

Due to the presence of noise in (13), $\Delta\mathbf{g}$ is not directly available. We apply the GLRT ([36], eq. 6.12) to determine $\mathcal{H}_0/\mathcal{H}_1$ as

$$GL(\mathbf{g}_{\text{off}}) = \frac{\max_{\Delta\mathbf{g}} p(\mathbf{g}_{\text{off}}|\mathcal{H}_1)}{p(\mathbf{g}_{\text{off}}|\mathcal{H}_0)} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \eta. \tag{22}$$

where η is a real positive number. According to (21), the numerator of (22) is maximized when the exponential argument $(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})^H \mathbf{\Sigma}^{-1}(\mathbf{g}_{\text{off}} - \Delta\mathbf{g})$ is minimized. Since $\mathbf{\Sigma}$ and $\mathbf{\Sigma}^{-1}$ are positive definite matrices, we have $\mathbf{x}^H\mathbf{\Sigma}^{-1}\mathbf{x} \geqslant 0$ for any $\mathbf{x}$ and the equality holds if and only if $\mathbf{x} = 0$ ([37], Definition 1-(i)). Hence, $\Delta\mathbf{g} = \mathbf{g}_{\text{off}}$ maximizes the numerator of (22), and produces the logarithmic GLRT as

$$A = \mathbf{g}_{\text{off}}^H \mathbf{\Sigma}^{-1} \mathbf{g}_{\text{off}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} T. \tag{23}$$

If A is larger than the threshold T, hypothesis $\mathcal{H}_1$ is supported. Otherwise, $\mathcal{H}_0$ is supported. We use Neyman-Pearson lemma [36, Theorem 3.1] to determine the best T with a given false alarm probability by solving the following equation

$$P_{\text{FA}}(T) = \Pr(A > T|\mathcal{H}_0) = \int_T^\infty p_A(x|\mathcal{H}_0)dx \tag{24}$$

where $p_A(\cdot|\mathcal{H}_0)$ denotes the probability density function (PDF) of A under $\mathcal{H}_0$, and P_{FA} is the false alarm probability. Appendix 3 shows that the PDFs of A under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are

$$p_A(x|\mathcal{H}_0) = xe^{-x}, \quad x \geqslant 0 \tag{25}$$

$$p_A(x|\mathcal{H}_1) = \sqrt{\frac{2x}{\beta}}\, e^{-\frac{2x+\beta}{2}} I_1(\sqrt{2\beta x}), \quad x \geqslant 0, \tag{26}$$

where $I_1(\cdot)$ is the first order modified Bessel function of the first kind ([38], eq. 9.6.19). The parameter β in (26) is defined as

$$\beta = 2\left(\lambda_1|b_1|^2 + \lambda_2|b_2|^2\right) \tag{27}$$

where λ_1 and λ_2 are the eigenvalues of $\mathbf{\Sigma}^{-1}$, b_1 and b_2 are the elements of $\mathbf{b}$ that can be given by

$$\mathbf{b} = \mathbf{Q}\Delta\mathbf{g} \tag{28}$$

where $\mathbf{Q}$ is a 2×2 matrix whose i-th column is the eigenvector of $\mathbf{\Sigma}^{-1}$ corresponding to λ_i, $i = 1, 2$, and satisfies $\mathbf{Q}\mathbf{Q}^H = \mathbf{I}$. Substituting (25) into (24), P_{FA} can be obtained as

$$P_{\text{FA}}(T) = (T+1)e^{-T} \tag{29}$$

and T for a given false alarm rate can be calculated by solving (29).

Finally, the detection probability for this fingerprint comparison can be derived as

$$\begin{aligned} P_{\text{D}}(T) &= \Pr(A > T|\mathcal{H}_1) \\ &= \int_T^\infty \sqrt{\frac{2x}{\beta}}\, e^{-\frac{2x+\beta}{2}} I_1\left(\sqrt{2\beta x}\right) dx \\ &= Q_2\left(\sqrt{\frac{2\Delta\mathbf{g}^H\mathbf{C}\Delta\mathbf{g}}{(C_1+\epsilon_1)^2 - |C_2+\epsilon_2|^2}}, \sqrt{2T}\right), \end{aligned} \tag{30}$$

where $\mathbf{C} = \begin{bmatrix} C_1+\epsilon_1 & C_2+\epsilon_2 \\ C_3+\epsilon_3 & C_4+\epsilon_4 \end{bmatrix}$, $Q_m(\cdot,\cdot)$ represents the m-th order Marcum Q-function ([39], eq. 4.59), and

$$C_1 = C_4 = \frac{\gamma_1}{|h_{\text{SR}}h_{\text{RD}}|^2\left(\gamma_1^2 - |\gamma_2|^2\right)} \tag{31a}$$

$$C_2 = C_3^* = \frac{h_{\text{SR}}^*\gamma_2^*}{|h_{\text{SR}}|^2|h_{\text{RD}}|^4\left(\gamma_1^2 - |\gamma_2|^2\right)} \tag{31b}$$

where $\gamma_1 = \frac{\sum_{i=1}^N |s_i|^2}{\sigma^2}$, $\gamma_2 = \frac{\sum_{i=1}^N s_i^2}{\sigma^2}$. Based on our fingerprint registration process (see Algorithm 1), $\mathbf{\Sigma}_v = \begin{bmatrix} \epsilon_4 & -\epsilon_2 \\ -\epsilon_3 & \epsilon_1 \end{bmatrix}$ and $\epsilon_1 = \epsilon_4$, $\epsilon_2 = \epsilon_3^*$.

In most practical cases, it can be observed from (19) that the effect of $\mathbf{\Sigma}_v$ in $\mathbf{\Sigma}$ can nearly vanish when large Z is used, which means $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 \approx 0$. Hence, P_{D} can be further simplified as

$$P_{\text{D}} = Q_2\left(\sqrt{2\Delta\mathbf{g}^H\mathbf{D}\Delta\mathbf{g}}, \sqrt{2T}\right) \tag{32}$$

where $\mathbf{D} = \begin{bmatrix} |h_{\text{SR}}h_{\text{RD}}|^2\gamma_1 & h_{\text{SR}}^{*2}|h_{\text{RD}}|^2\gamma_2^* \\ h_{\text{SR}}^2|h_{\text{RD}}|^2\gamma_2 & |h_{\text{SR}}h_{\text{RD}}|^2\gamma_1 \end{bmatrix}$. By using (32) instead of (30), we are able to quickly calculate the instantaneous detection probability for every fingerprint comparison, which may enable the timely adjustment of T in (23) for ensuring the desired detection performance.

In summary, using the GLRT presented in (22) and (23), two fingerprints can be differentiated with the detection probability derived in (30) given a given false alarm rate. In practical implementation, the detection probability can be quickly computed using (32) instead of (30).

5 Whitelist-based AF relay identification algorithm

Based on our above derived results, this section presents the AF relay identification algorithm consisting of the fingerprint registration, update, and identification.

5.1 Fingerprint registration

We consider that a new relay, R_{AF}, joins in the network. The fingerprint of R_{AF} (i.e., $\hat{\mathbf{g}}_{v,U}$) needs to be extracted and stored in the whitelist.

As shown in Algorithm 1, the average of the Z estimated IQI fingerprint is used to improve the accuracy of the registered fingerprint. Then, $\hat{\mathbf{g}}_{v,U}$ is registered as the U-th valid fingerprint in the whitelist.

Algorithm 1 Fingerprint registration algorithm

1: **for** $i \leftarrow 1$ to Z **do**
2: S sends **s** to D via R_{AF}
3: Extract $\hat{\mathbf{g}}_{\mathrm{LS},i}$ of R_{AF} using (7).
4: **end for**
5: Calculate the average value by $\hat{\mathbf{g}}_{v,U} = \frac{\sum_{i=1}^{Z} \hat{\mathbf{g}}_{\mathrm{LS},i}}{Z}$
6: Add $\hat{\mathbf{g}}_{v,U}$ into the whitelist $\mathbf{G}_{\mathrm{v}} = \left[\hat{\mathbf{g}}_{v,1}\, \hat{\mathbf{g}}_{v,2} \cdots \hat{\mathbf{g}}_{v,U-1}\right]$

5.2 Fingerprint identification and update

If this R_{AF} is not claimed as a newly joined relay, the fingerprint identification algorithm should be executed to verify its identity. In some practical applications, such as an authentication application, R_{AF} may actively claim its identity, which can be indexed to one of the valid fingerprints in the whitelist. In this case, we only need to compare the estimated fingerprint of R_{AF} (i.e., $\hat{\mathbf{g}}_{\mathrm{LS}}$) with the claimed fingerprint. Without the loss of generality, we assume that R_{AF} does not claim its identity. As presented in Algorithm 2, the proposed GLRT-based differentiation is performed to compare R_{AF}'s $\hat{\mathbf{g}}_{\mathrm{LS}}$ with all U pre-recorded $\mathbf{G}_{\mathrm{v}}$ one-by-one, which leads to three possible cases:

Case #1 ($l = 0$)**:** R_{AF} is not identified as any candidate in the whitelist, implying all U GLRT claim $\mathcal{H}_1$.

Case #2 ($l = 1$)**:** R_{AF} is identified as one candidate, implying that only one GLRT claims $\mathcal{H}_0$.

Case #3 ($l > 1$)**:** There are a number of l candidates that have the similar fingerprints to R_{AF}.

To handle Case #3, we use the maximum likelihood (ML) technique and choose the relay with its A_j closest to 1 as the final decision, since that $A = 1$ can lead to the ML in (25). If R_{AF} is not identified, *alarm* is set to 1 to give an alarm. Otherwise, the R_{AF}'s identity is obtained in *ID*.

In addition, although stable in the time scales of hours and days, the hardware fingerprint may slowly change over time, and thus, it may have the chance to affect the identification performance. In fact, it is practically impossible to model and predict the random minor changes of our fingerprint in a short time duration. As reported in [24], it may take up to 30 days to observe the distinguishable hardware changes, which is usually unnecessary to be taken into account in our short time identification. In our case, it is more efficient to consider the fingerprint update by taking the advantage of every signal reception since our IQI fingerprint can be extracted from any relayed signals. As shown in line 22 of Algorithm 2, after identifying R_{AF}, Algorithm 1 can be optionally used to update the R_{AF}'s fingerprint in the whitelist. Moreover, the fingerprint registration can be periodically executed if needed, for example, after receiving a certain number of signals.

Algorithm 2 Fingerprint identification and update algorithm

1: Initialization: $l \leftarrow 0$, $d_{\min} \leftarrow 0$, $k \leftarrow 0$ and $idx \leftarrow \{0\}$.
2: Extract $\hat{\mathbf{g}}_{\mathrm{LS}}$ of R_{AF} using (7).
3: Calculate $\mathbf{\Sigma}$ for R_{AF} using (16).
4: **for** $i \leftarrow 1$ to U **do** *%U GLRT exams*
5: Compare $\hat{\mathbf{g}}_{\mathrm{LS}}$ with $\hat{\mathbf{g}}_{v,i}$ in $\mathbf{G}_{\mathrm{v}}$ to obtain $\mathbf{g}_{\mathrm{off}}$ using (13).
6: Calculate $A_i = \mathbf{g}_{\mathrm{off}}^H \mathbf{\Sigma}^{-1} \mathbf{g}_{\mathrm{off}}$.
7: Set a required P_{FA} in (29) and calculate T.
8: Compare A_i with T to determine the true hypothesis using (23).
9: **if** $\mathcal{H}_0$ is claimed **then**
10: $l \leftarrow l + 1$, $idx_l \leftarrow i$
11: **end if**
12: **end for**
13: **if** $l = 0$ **then** *%Case #1*
14: $alarm \leftarrow 1$ *%give an alarm*
15: **else if** $l = 1$ **then** *%Case #2*
16: $k \leftarrow idx_1, ID \leftarrow \hat{\mathbf{g}}_{v,k}, alarm \leftarrow 0$
17: **else** *%Case #3*
18: Find j that satisfies $min(|A_j - 1|), j = 1, \cdots, l$
19: $k \leftarrow idx_j, ID \leftarrow \hat{\mathbf{g}}_{v,k}, alarm \leftarrow 0$
20: **end if**
21: **if** $alarm = 0$ **then** *% update fingerprint*
22: Algorithm 1 can be optionally executed for updating $\hat{\mathbf{g}}_{v,k}$ in $\mathbf{G}_{\mathrm{v}}$
23: **end if**

6 Optimal signal design for maximizing identification performance

Unlike the easily programmable upper-layer identities (e.g., medium access control address) or fast varying channel-based characteristics, IQI is fixed on the hardware level for a relatively long period. Therefore, once the presence of a relay's IQI fingerprint is detected, this fingerprint can be used as pre-knowledge associated with this relay for a period. This enables us to design the best signal for intentionally detecting this relay again with a maximized detection probability in the future, which is useful in many practical applications. Taking authentication as an example, we assume that a malicious AF relay R' is detected by an authentication, and its fingerprint is thereby stored. In practice, this R' can repeatedly attempt to impersonate other legitimate relays through changing its upper-layer identity. Given the stability of IQI, the already stored fingerprint of R' can be used as known in Eq. (13) to obtain $\mathbf{g}_{\mathrm{off}}$ and the pre-knowledge of $\Delta\mathbf{g}$ can be obtained as well according to our previous GLRT analysis.

With this pre-knowledge, we are able to derive the optimal s_i to intentionally maximize the detection probability for the future authentication of R'.

We first assume that the $\Delta\mathbf{g}$ associated with an intended AF relay is known. In (30), the two arguments of P_{D} are β and T, where the value of T is to hold a fixed false alarm, thus implying P_{D} can only be maximized by adjusting β in practice. According to [40], P_{D} is a strictly increasing function with respect to β. Thus, maximizing P_{D} is equivalent to maximizing $\beta = 2\Delta\mathbf{g}^H(\mathbf{\Sigma}_g + \mathbf{\Sigma}_v)^{-1}\Delta\mathbf{g} > 0$ through adjusting s_i. However, the mathematical expression of $\mathbf{\Sigma}_v$ is unavailable in general as it is only dependent on the specific sample processing method of the past fingerprint registration phase. Hence, the adjustment of s_i cannot affect $\mathbf{\Sigma}_v$. In practice, $\mathbf{\Sigma}_v$ always approaches a null matrix with the proper diversity-combining techniques and enough samples, as discussed in Eq. (32). Also, using Lemma 1 below, we get $\Delta\mathbf{g}^H\mathbf{\Sigma}_g^{-1}\Delta\mathbf{g} \geqslant \Delta\mathbf{g}^H(\mathbf{\Sigma}_g + \mathbf{\Sigma}_v)^{-1}\Delta\mathbf{g}$, where the equality holds if and only if $\mathbf{\Sigma}_v = \mathbf{0}$. Therefore, we practically consider Eq. (32) with $\mathbf{\Sigma}_v = \mathbf{0}$ in the maximization of β.

Lemma 1 *Given two $N \times N$ positive definite Hermitian matrices* $\mathbf{U}$ *and* $\mathbf{V}$*, and a $N \times 1$ complex vector* $\mathbf{x}$*, the following inequality holds*

$$\mathbf{x}^H\mathbf{U}^{-1}\mathbf{x} > \mathbf{x}^H(\mathbf{U}+\mathbf{V})^{-1}\mathbf{x}$$

Proof See Appendix 4. □

Using (16), (27), (28), and setting $\mathbf{\Lambda} = \mathrm{diag}(\lambda_1, \lambda_2)$, we can get

$$J = \frac{1}{2}\sigma^2\beta = \left(|h_1\Delta g_1|^2 + |h_2\Delta g_2|^2\right)\sum_{i=1}^{N}|s_i|^2 + 2\Re\left\{h_2^*\Delta g_2^* h_1\Delta g_1\sum_{i=1}^{N}s_i^2\right\} \tag{33}$$

where $h_1 = h_{\mathrm{SR}}h_{\mathrm{RD}}$ and $h_2 = h_{\mathrm{SR}}^* h_{\mathrm{RD}}$. It can be observed that maximizing β is also equivalent to maximizing J for a given σ^2. Since s_i is subject to the specific constellation patterns, QAM and PSK as two basic modulation schemes are considered in deriving the optimal s_i.

6.1 QAM modulation case

In QAM modulation, the signal can be represented as $s_i = a_i + jb_i$. Let $l = |h_1\Delta g_1|^2 + |h_2\Delta g_2|^2$, $c = \Re\left\{h_2^*\Delta g_2^* h_1\Delta g_1\right\}$, and $d = \Im\left\{h_2^*\Delta g_2^* h_1\Delta g_1\right\}$, then J can be expressed as

$$J = \sum_{i=1}^{N}J_i = (l+2c)\sum_{i=1}^{N}a_i^2 + (l-2c)\sum_{i=1}^{N}b_i^2 - 4d\sum_{i=1}^{N}a_ib_i \tag{34}$$

where J_i is defined as

$$J_i = (l+2c)a_i^2 + (l-2c)b_i^2 - 4da_ib_i. \tag{35}$$

Since s_i are independent, we are able to separately design s_i to maximize J_i, which leads to the maximal J. The rule of optimal signal design under QAM modulations is summarized in Proposition 1.

Proposition 1 *If $d < 0$, the optimal s_i is the point at the angles of the rectangular constellation in the first and third quadrants of the I/Q coordinate plane.*

If $d > 0$, the optimal s_i is the point at the angles of the rectangular constellation in the second and fourth quadrants of the I/Q coordinate plane.

If $d = 0$, the optimal s_i is the point at any angle of the rectangular constellation of the I/Q coordinate plane.

Proof See Appendix 5. □

In our optimal design, the value of the optimal symbol only has two options when $d > 0$ or $d < 0$. This may occasionally result in a singular matrix $\mathbf{H}_s^H\mathbf{H}_s$ that makes the matrix inversion difficult, e.g., the calculation of $\mathbf{\Sigma}^{-1}$. For practical implementation purpose, we give a more robust suboptimal signal design as follows:

If $d > 0$ or $d < 0$, the suboptimal signals are the two constellation points that are the closest to the optimal signal.

Figure 3a shows the optimal symbols (red) and suboptimal symbols (green) in a 64-QAM constellation. It is noteworthy that the optimal and suboptimal symbols are not required to be located in the same quadrant. For instance, if $d < 0$, an optimal symbol has been chosen from the first quadrant, while the suboptimal symbol can be either in the first or the third quadrant.

6.2 PSK modulation case

For a general M-PSK modulation, the constellation diagram is a circle such that the signal can be represented by $s_i = A_s e^{j\theta_i}$, where A_s denotes the constant signal amplitude and θ_i denotes the phase-shift. The rule of optimal signal design for PSK is proposed in Proposition 2.

Proposition 2 *The optimal s_i should satisfy $\theta_i = \frac{-\phi}{2}$ or $\theta_i = \frac{-\phi}{2} + \pi$, where*

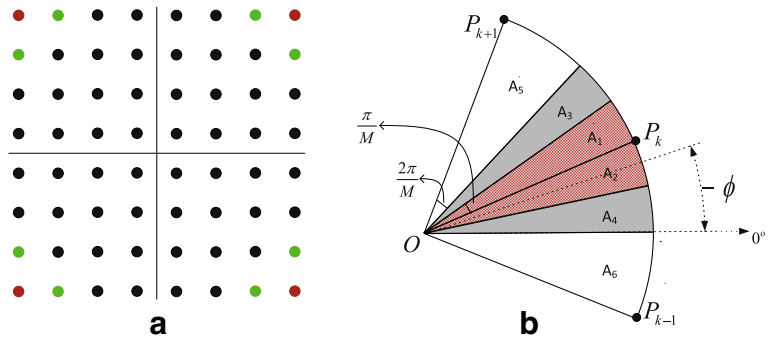

Fig. 3 The optimal and suboptimal signals for **a** QAM and **b** PSK

$$\begin{aligned}\phi &= \angle(h_2^*\Delta g_2^* h_1 \Delta g_1)\\ &= \arctan\left(\frac{\Im\{h_2^*\Delta g_2^* h_1\Delta g_1\}}{\Re\{h_2^*\Delta g_2^* h_1\Delta g_1\}}\right) \in (-\pi,\pi]. \end{aligned} \tag{36}$$

Proof See Appendix 6. □

Since ϕ can be any degree, whereas the values of θ_i are subject to the specific PSK constellation diagram, we need to choose the M-PSK symbol having the closest angle to θ_i as the optimal s_i in practice.

Similarly, we also propose a suboptimal design to solve the problem of a singular matrix, $\mathbf{H}_s^H\mathbf{H}_s$. Since the degree of derived $-\phi$ is twice that of θ_i, we first create a $\frac{M}{2}$-PSK constellation. As shown in Fig. 3b, P_k denotes the square of the kth constellation point of M-PSK, i.e., $P_k = s_k^2 = A_s^2 e^{j2\theta_k}$. As shown in this newly defined $\frac{M}{2}$-PSK constellation, the phase shift between two neighboring points (e.g., P_k and P_{k-1}) is $\frac{4\pi}{M}$. The phase shift for areas A_1, A_2, A_3, and A_4 are $\frac{\pi}{M}$, and the phase shift for A_5 and A_6 are $\frac{2\pi}{M}$. Without the loss of generality, it is assumed that $-\phi$ is closer to P_k than P_{k-1} and P_{k+1}, which means that it falls in one of the sectors of A_1, A_2 (red sectors), A_3, or A_4 (gray sectors). Herein, we take a combination of two signals (s_i, s_{i+1}) into account to approach the desired phase $-\phi$ and accordingly present the rules of suboptimal approach as follows:

1 If $-\phi$ falls in A_1 or A_2, we set $s_i = s_{k+n}, s_{i+1} = s_{k-n}, n = 0, 1, 2\cdots$.
2 If $-\phi$ falls in A_3, we set $s_i = s_{k+n}, s_{i+1} = s_{k+1-n}$.
3 If $-\phi$ falls in A_4, we set $s_i = s_{k+n}, s_{i+1} = s_{k-1-n}$.

In practical implementation, Proposition 1/2 can be first considered to design the optimal QAM/PSK signals. Then, a portion of them can be flexibly replaced by applying the suboptimal approaches.

7 Numerical results

In this section, numerical results are presented to validate our derivations and evaluate the performance of the proposed IQI-based AF relay identification method.

We consider $a = 1$, $Z = 500$, 16-QAM, and 16-PSK modulations. Rayleigh fading model is used to generate $h_{SR} \sim CN(0,2)$ and $h_{RD} \sim CN(0,2)$, unless otherwise noted. SNR=$10\log_{10}(\frac{P}{\sigma^2})$ is defined as used in [14, 41, 42], where $P = 10$. To evaluate the identification performance under the challenging small IQI condition, the amplitude imbalance and phase-shift imbalance are randomly chosen within $[-0.05, 0.05]$ and $[-5°, 5°]$. As an example of the contrast, to achieve satisfactory identification performance, the method proposed in [13] requires large IQI values $[-0.3, 0.3]$ and $[-15°, 15°]$, which is rarely the case in practice. All simulation results are based on the average of 10^5 independent realizations of our system.

7.1 Numerical results for IQI device fingerprint

The dynamic range of the IQI device fingerprints and the parameter γ derived in Section 3 are first evaluated. Figure 4 shows the real and imaginary values of g_1 and g_2 vs. α, where $\alpha = (1+\alpha_{rx})(1+\alpha_{tx})$. The Rx and Tx IQIs are set as $\theta_{rx} = 5°$, $\theta_{tx} = 1°$, and α varies between 0.81 and 1.21. The curves between two vertical lines confirm that $\Re\{g_1\} \approx 1$, and $\Im\{g_1\}, \Re\{g_2\}, \Im\{g_2\} \approx 0$ under the small IQI values since $\sin(\theta_{tx} - \theta_{rx})$, $\sin(\theta_{tx} + \theta_{rx})$, and $1 - (1+\alpha_{tx})(1+\alpha_{rx})\cos(\theta_{tx} + \theta_{rx})$ approximate zero in (8) and (9). In addition, these 4 simulated parameters' ranges also validate our analytical results derived in (10).

Figure 5 depicts $10\log_{10}\gamma$ in terms of α. The figure shows that the peak values of all four simulated $10\log_{10}\gamma$ appear at $\alpha = 1$, which is the case of the absence of phase-shift imbalance. It is shown that the black curve ($\theta_{rx} = \theta_{tx} = 0°$) can go to infinity when $\alpha = 1$, thus confirming the result of the infinity case in Eq. (12). We then substitute $\alpha = 0.64 - 1.44$ in (12) to calculate the lower limit of $10\log_{10}\gamma$. As expected, the calculated analytical results (11.9032 dB, 12.5637 dB, 12.8595 dB, and 13.1708 dB) can match the simulated results.

The above numerical results confirm our IQI fingerprint derivations in Eq. (8)–(12).

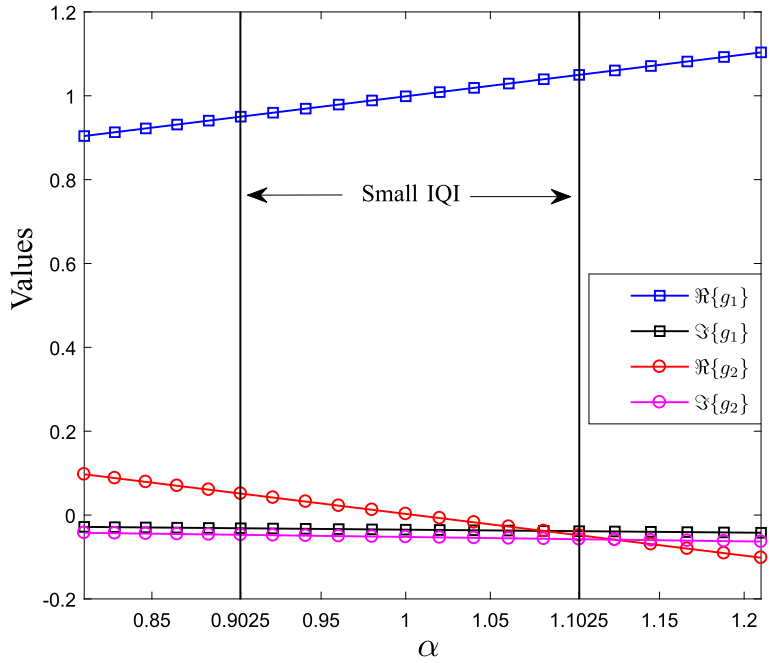

Fig. 4 $\Re\{g_1\}, \Im\{g_1\}, \Re\{g_2\}$, and $\Im\{g_2\}$ vs. α under $\theta_{rx} = 5°, \theta_{tx} = 1°$

7.2 Performance evaluation of proposed AF relay identification

In Fig. 6, the detection probability P_D in terms of the false alarm probability P_{FA} is shown. It can be seen that the analytical P_D calculated by Eq. (30) is well confirmed by the simulation results. Threshold T, which is calculated by solving (29), decreases with P_{FA} varying from 10^{-3} to 1.

In Fig. 7, P_D for different instantaneous channel gains h_{SR} and h_{RD} is evaluated. We set a fixed T for holding $P_{FA} = 5\%$, and randomly choose a fixed fingerprint offset $\Delta\mathbf{g} = [0.0306 + j0.0669 \quad -0.0186 - j0.0712]^T$, fixed $\mathbf{s}$ and noise variance $\sigma^2 = 0.1$ to ensure constant γ_1 and γ_2. We consider $h_{SR} \sim CN(0, w_{SR})$ and $h_{RD} \sim CN(0, w_{RD})$ to respectively generate h_{SR} and h_{RD}, where $w_{RD} = ww_{SR}$,

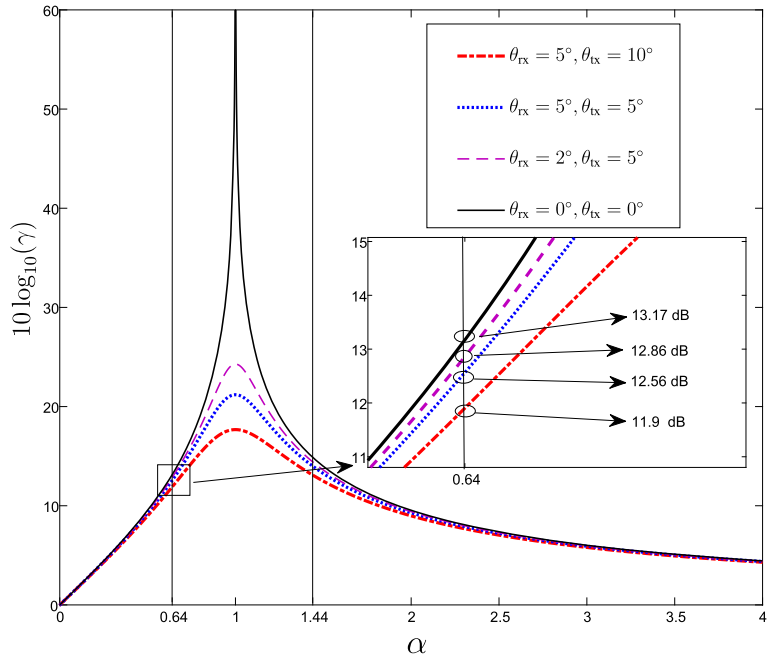

Fig. 5 The range of $10\log_{10}(\gamma)$ vs. α under different θ_{rx} and θ_{tx}

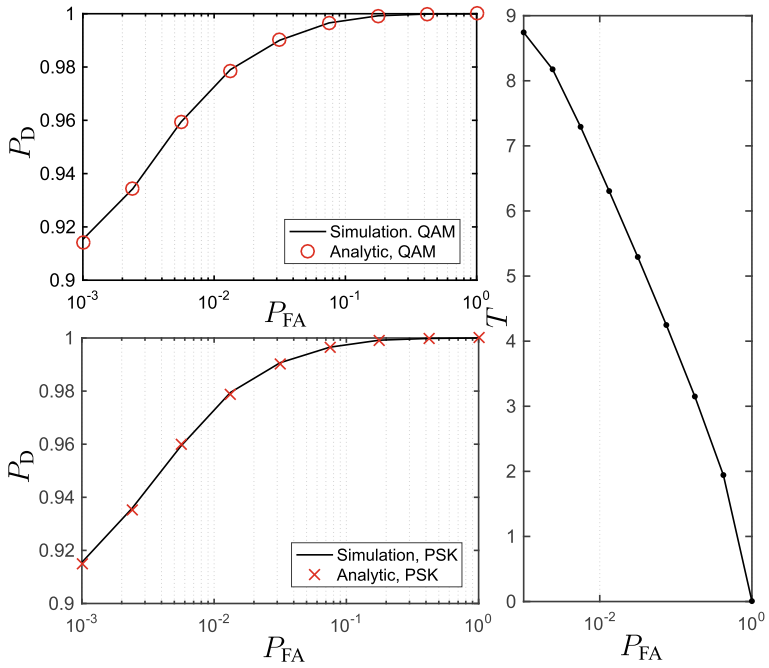

Fig. 6 Analytical and simulated P_D vs. P_{FA} and corresponding T. The current AF relay $(\alpha_{rx}, \theta_{rx}, \alpha_{tx}, \theta_{tx}) = (-0.03, 5°, 0.05, 4°)$, the pre-registered AF relay $(\alpha_{rx}, \theta_{rx}, \alpha_{tx}, \theta_{tx}) = (0.02, 5°, -0.05, -4°)$, $\sigma^2 = 0.1, N = 14$

and show P_D vs w_{SR} with different w. The fingerprint estimation can become more precise under good channel condition, thus improving the accuracy of the fingerprint differentiation. As expected, P_D increases with the growth of w_{SR} and w_{RD}.

In Fig. 8, P_D using the optimal signal described in Propositions 1 and 2 is compared with the suboptimal and non-optimal signals. We substitute the optimal signal derived by Propositions 1 and 2 into (30) to obtain the analytically maximal P_D, and call it the upper bound. The

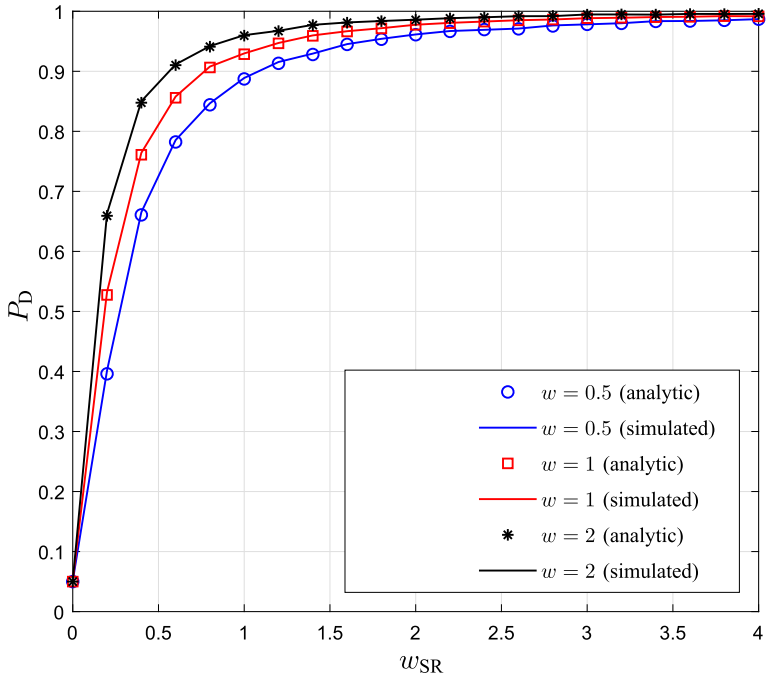

Fig. 7 P_D performance for different source-relay-destination channels

non-optimal signals are randomly chosen symbols. The results show that our suboptimal methods have a detection probability loss of only 2.59% and 1.68% on average in QAM and PSK, respectively, compared to the optimal methods. On the other hand, our suboptimal methods also show on average a 34.54% and 23.43% higher P_{D} than the non-optimal cases. Therefore, the suboptimal solution is capable of significantly improving the identification performance in the small IQI condition, and furthermore it can be more robust than the optimal solution.

At last, the performance of the identification algorithm is evaluated. Specifically, the algorithm can either choose the correct identity from the four pre-registered candidates for the relay under test or give a timely alarm if the relay is not identified. The aforementioned DT [13] and VF methods [17] are simulated and compared. The correct identification rate (CIR) is defined as the ratio of the number of correct identity claims and correct alarms to the total number of identification attempts. Figure 9 shows the CIR performance vs. SNR. Since the estimation error $\mathbf{n}_g$ is reducing with the increase of SNR, the detection accuracy and CIR go higher. It can also be seen that our method is superior to the VF and DT schemes in all simulated cases. Compared to VF, our fingerprint removes most effects of the channel variation, and thus, the uniqueness and stability of our fingerprint are improved. Regarding DT, the distance between different fingerprints $\mathbf{g}$ is usually too short to differentiate due to the limited range of IQI, as discussed in Section 3. Meanwhile, in our method, the proposed GLRT-based differentiation and optimal signal designs can significantly improve the accuracy in differentiating minor $\Delta\mathbf{g}$. Additionally, our identification can achieve better performance but use fewer training symbols. For instance, it can be seen that the CIR of our method with $N = 32$ and $P_{\mathrm{FA}} = 1\%$ is even higher than VF with $N = 512$ and $P_{\mathrm{FA}} = 1\%$, which also implies lower Tx power consumption by using our method.

8 Conclusion

A physical-layer AF relay identification scheme was proposed to accurately identify relays based on the examination of their unique IQIs. Since IQI estimation and compensation are usually mandatory in most present wireless receivers, we direct use the LS estimation results to generate the IQI fingerprint of an AF relay node. Comprehensive analyses including the features of this IQI fingerprint, the probabilities of detection and false alarm in differentiating between two relays with small IQI values, and whitelist-based relay identification algorithms were presented. In addition, we proposed optimal and suboptimal training signal designs for the purpose of maximizing the detection probability. The simulation results validated our analytical results and showed that the proposed identification method could accurately identify AF relays even under the small IQI condition.

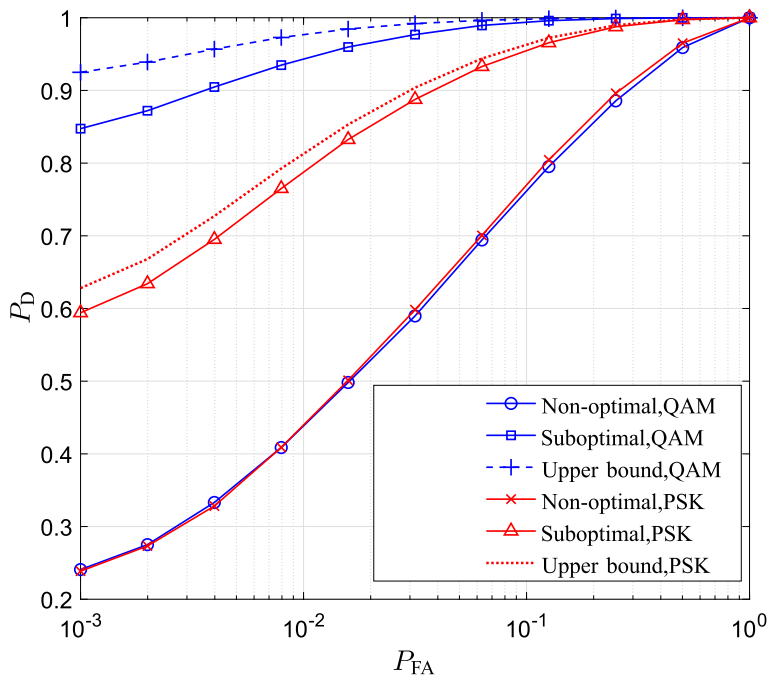

Fig. 8 Detection probabilities comparison between suboptimal and non-optimal signal design and the corresponding upper bounds. The two compared relays have $(\alpha_{\mathrm{rx}}, \theta_{\mathrm{rx}}, \alpha_{\mathrm{tx}}, \theta_{\mathrm{tx}}) = (-0.03, 3°, 0.03, 3°)$, $(\alpha_{\mathrm{rx}}, \theta_{\mathrm{rx}}, \alpha_{\mathrm{tx}}, \theta_{\mathrm{tx}}) = (0.02, 5°, -0.05, -4°)$, SNR=16 dB, $N = 14$

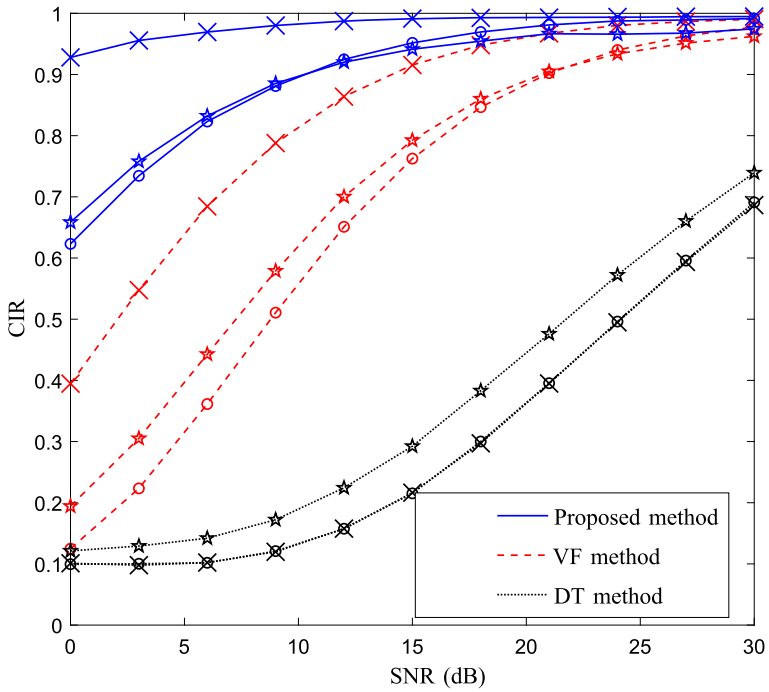

Fig. 9 CIR comparisons between proposed methods and VF- and DT-based methods. The cross marker denotes $N = 512$ and $P_{\text{FA}} = 1\%$, the star marker denotes $N = 32$ and $P_{\text{FA}} = 5\%$, and the circle marker denotes $N = 32$ and $P_{\text{FA}} = 1\%$

Appendix 1: Proof for the range of γ in Eq. (12)

From (11), it is found that the ideal IQI-free condition, i.e., $\theta_{m1} = \theta_{m2} = 0, \alpha_{m1} = \alpha_{m2} = 0$, can result in a zero denominator and a real positive numerator. In this case, γ is positive infinity.

We then summarize the derivations for the minimum value of γ as an optimization problem, which is given by

$$\arg\min_{\alpha,\theta_{\text{tx}},\theta_{\text{rx}}} \left(\frac{1+\alpha^2+2\alpha\cos(\theta_{\text{tx}}-\theta_{\text{rx}})}{1+\alpha^2-2\alpha\cos(\theta_{\text{tx}}+\theta_{\text{rx}})} \right), \tag{37a}$$

$$\text{s.t.} \quad \alpha = (1+\alpha_{\text{tx}})(1+\alpha_{\text{rx}}),$$
$$|\theta_{\text{tx}}| \leqslant \theta_{m1}, |\theta_{\text{rx}}| \leqslant \theta_{m2},$$
$$|\alpha_{\text{tx}}| \leqslant \alpha_{m1}, |\alpha_{\text{rx}}| \leqslant \alpha_{m2}. \tag{37b}$$

Using the constraints in (37b), the range of α can be determined as

$$(1-\alpha_{m1})(1-\alpha_{m2}) \leqslant \alpha \leqslant (1+\alpha_{m1})(1+\alpha_{m2}). \tag{38}$$

Using the addition and subtraction theorems of trigonometric functions, (37a) can be simplified as

$$\begin{aligned} &\frac{1+\alpha^2+2\alpha\cos(\theta_{\text{tx}}-\theta_{\text{rx}})}{1+\alpha^2-2\alpha\cos(\theta_{\text{tx}}+\theta_{\text{rx}})} \\ =&1+\frac{4}{\left(\alpha+\frac{1}{\alpha}\right)(\cos\theta_{\text{tx}}\cos\theta_{\text{rx}})^{-1}+2\tan\theta_{\text{tx}}\tan\theta_{\text{rx}}-2}. \end{aligned} \tag{39}$$

Note that both the numerator and denominator are divided by $\alpha\cos\theta_{\text{tx}}\cos\theta_{\text{rx}}$ in deriving (39). This is reasonable as the practical amplitude mismatch and phase mismatch are small enough to ensure $\alpha > 0$ and $\cos\theta_{\text{tx}}\cos\theta_{\text{rx}} > 0$. According to the inequality of arithmetic and geometric means [43], we can obtain

$$2 = 2\sqrt{\alpha\cdot\frac{1}{\alpha}} \leqslant \alpha+\frac{1}{\alpha} \leqslant \max(A_m, B_m) \tag{40}$$

where $A_m = (1+\alpha_{m1})(1+\alpha_{m2}) + \frac{1}{(1+\alpha_{m1})(1+\alpha_{m2})}$, $B_m = (1-\alpha_{m1})(1-\alpha_{m2}) + \frac{1}{(1-\alpha_{m1})(1-\alpha_{m2})}$. It is notable that the monotonicity of $\alpha+\frac{1}{\alpha}$ is considered in (40) to find its upper bound. Further, we can also refer to the monotonicity of cosine and tangent, and get

$$\cos\theta_{m1}\cos\theta_{m2} \leqslant \cos\theta_{\text{tx}}\cos\theta_{\text{rx}} \leqslant 1, \tag{41}$$

$$-\tan\theta_{m1}\tan\theta_{m2} \leqslant \tan\theta_{\text{tx}}\tan\theta_{\text{rx}} \leqslant \tan\theta_{m1}\tan\theta_{m2}. \tag{42}$$

Based on (40)-(42), the lower bound of (39) can be calculated as

$$\begin{aligned} &1+\frac{4}{\left(\alpha+\frac{1}{\alpha}\right)(\cos\theta_{\text{tx}}\cos\theta_{\text{rx}})^{-1}+2\tan\theta_{\text{tx}}\tan\theta_{\text{rx}}-2} \\ \geqslant&1+\frac{4}{\frac{\max(A_m,B_m)}{\cos\theta_{m1}\cos\theta_{m2}}+2\tan\theta_{m1}\tan\theta_{m2}-2}. \end{aligned} \tag{43}$$

Consequently, the range of γ can be obtained as shown in (12).

Appendix 2: Analysis for the PDF of n

We first define $\mathbf{n} = \mathbf{n}' + \mathbf{n}_{\mathrm{RD}}$, where the k-th element of $\mathbf{n}'$ is $n'_k = g_1 h_{\mathrm{RD}} n_{\mathrm{SR}k} + g_2 h_{\mathrm{RD}} n^*_{\mathrm{SR}k}$. Generally, $\mathbf{n}'$ is an improper complex Gaussian vector as it depends on both of $\mathbf{n}_{\mathrm{SR}}$ and $\mathbf{n}^*_{\mathrm{SR}}$, and the PDF of $\mathbf{n}'$ is [44, 45]

$$p(\mathbf{n}') = \frac{1}{\pi^N |\det(\mathbf{R})|^{\frac{1}{2}}} \exp\left(-\frac{1}{2}\mathbf{n}_t^H \mathbf{R}^{-1} \mathbf{n}_t\right) \tag{44}$$

where $\mathbf{n}_t = \left[\mathbf{n}'^T \ \mathbf{n}'^H\right]^T$, and $\mathbf{R}$ is a covariance matrix of $\mathbf{n}_t$ given by $\mathbf{R} = \mathbb{E}\left[\mathbf{n}_t \mathbf{n}_t^H\right]$.

However, in the case of IQI caused n'_k, the conjugate term $g_2 h_{\mathrm{RD}} n^*_{\mathrm{SR}k}$ nearly vanishes since $g_2 \approx 0$. Substituting $\Re\{g_1\} \approx 1$, and $\Im\{g_1\}, \Re\{g_2\}, \Im\{g_2\} \approx 0$ [18–20, 33, 34] in n'_k, we can get $\Re\left\{n'_k\right\}, \Im\left\{n'_k\right\} \sim N\left(0, \left(a_1^2 + a_2^2\right)\frac{\sigma_1^2}{2}\right)$, where $a_1 = \Re\{g_1 h_{\mathrm{RD}}\}, a_2 = \Im\{g_1 h_{\mathrm{RD}}\}$. Also, since $\mathbb{E}[\Re\{n_{\mathrm{SR}k}\}\Im\{n_{\mathrm{SR}k}\}] = \mathbb{E}[\Re\{n_{\mathrm{SR}k}\}]\,\mathbb{E}[\Im\{n_{\mathrm{SR}k}\}] = 0$ and $\mathbb{E}[\Re\{n_{\mathrm{SR}k}\}^2] = \mathbb{E}[\Im\{n_{\mathrm{SR}k}\}^2] = \frac{\sigma_1^2}{2}$, we can get $\mathbb{E}[\Re\{n'\}\Im\{n'\}] \approx a_1 a_2 \left(\mathbb{E}\left[\Re\{n_{\mathrm{SR}k}\}^2\right] - \mathbb{E}\left[\Im\{n_{\mathrm{SR}k}\}^2\right]\right) = 0$. Given that $n_{\mathrm{RD}k}$ is circularly symmetric complex Gaussian random variable, $n_k = n'_k + n_{\mathrm{RD}k}$ can be modeled as a circularly symmetric complex Gaussian variable since its real and imaginary parts are independent and identically distributed Gaussian.

Appendix 3: Derivations for PDFs in Eqs. (25) and (26)

This appendix derives the PDFs of A under $\mathcal{H}_0$ in (25) and $\mathcal{H}_1$ in (26).

The eigendecomposition of matrix $\mathbf{\Sigma}^{-1}$ is

$$\mathbf{\Sigma}^{-1} = \mathbf{Q}^H \mathbf{\Lambda} \mathbf{Q} \tag{45}$$

where $\mathbf{\Lambda} = \mathrm{diag}(\lambda_1, \lambda_2)$ with its elements $\lambda_i > 0, i = 1, 2$ denoting the ith eigenvalue of $\mathbf{\Sigma}^{-1}$; $\mathbf{Q}$ is a 2×2 matrix whose ith column is the eigenvector of $\mathbf{\Sigma}^{-1}$ corresponding to λ_i. Substituting (45) in metric A, we can obtain

$$A = \mathbf{g}_{\mathrm{off}}^H \mathbf{\Sigma}^{-1} \mathbf{g}_{\mathrm{off}} = \mathbf{d}^H \mathbf{\Lambda} \mathbf{d} = \lambda_1 |d_1|^2 + \lambda_2 |d_2|^2 \tag{46}$$

where $\mathbf{d} = \mathbf{Q}\mathbf{g}_{\mathrm{off}} = [d_1, d_2]^T$. Given (13) (16) (28) and the orthogonal matrix $\mathbf{Q}$, the covariance matrix of $\mathbf{d}$ can be computed as

$$\begin{aligned}\mathrm{cov}(\mathbf{d}) &= \mathbb{E}[(\mathbf{d} - \mathbf{b})(\mathbf{d} - \mathbf{b})^H] = \mathrm{diag}\left(\frac{1}{\lambda_1}, \frac{1}{\lambda_2}\right) \\ &= \begin{bmatrix} \mathrm{cov}(d_1) & \mathrm{cov}(d_1, d_2) \\ \mathrm{cov}(d_2, d_1) & \mathrm{cov}(d_2) \end{bmatrix}.\end{aligned} \tag{47}$$

Since $\mathrm{cov}(d_1, d_2) = \mathrm{cov}(d_2, d_1) = 0$, d_1, d_2 are two independent random variables. Also, we can obtain $d_1 \sim CN\left(b_1, \frac{1}{\lambda_1}\right), d_2 \sim CN\left(b_2, \frac{1}{\lambda_2}\right)$, where $\mathbf{b} = \mathbf{Q}\Delta\mathbf{g}$ as defined in (28). Since $b_i = 0$ under $\mathcal{H}_0$ and $b_i \neq 0$ under $\mathcal{H}_1$, A follows scaled central/non-central chi-squared distributions under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. Using (46), we define $K = 2A$ as

$$K = k_1^2 + k_2^2 + k_3^2 + k_4^2 \tag{48}$$

where k_1, k_2, k_3 and k_4 are normalized, and defined by $k_1 = \sqrt{2\lambda_1}\Re\{d_1\}, k_2 = \sqrt{2\lambda_1}\Im\{d_1\}, k_3 = \sqrt{2\lambda_2}\Re\{d_2\}$, $k_4 = \sqrt{2\lambda_2}\Im\{d_2\}$.

In this case, the PDF of K under $\mathcal{H}_0$ is a central chi-squared PDF with 4 degrees of freedom as [38]

$$p_K(x|\mathcal{H}_0) = \frac{1}{4} x e^{-\frac{x}{2}}, x > 0. \tag{49}$$

While under $\mathcal{H}_1$, K follows the standard non-central chi-squared distribution with 4 degrees of freedom and non-centrality β_1 and its PDF can be given by

$$p_K(x|\mathcal{H}_1) = \frac{1}{2}\sqrt{\frac{x}{\beta_1}} e^{-\frac{x+\beta_1}{2}} I_1\left(\sqrt{x\beta_1}\right), x > 0 \tag{50}$$

where the non-centrality is defined as

$$\begin{aligned}\beta_1 = &\left(\sqrt{2\lambda_1}\Re\{b_1\}\right)^2 + \left(\sqrt{2\lambda_1}\Im\{b_1\}\right)^2 \\ &+ \left(\sqrt{2\lambda_2}\Re\{b_2\}\right)^2 + \left(\sqrt{2\lambda_2}\Im\{b_2\}\right)^2.\end{aligned} \tag{51}$$

It can be seen that $\beta_1 = \beta$, where β is defined in (27).

Finally, we are able to obtain the PDF of A under $\mathcal{H}_0$ and $\mathcal{H}_1$ by first replacing x with $2x$ in (49) and (50) and then multiplying the two PDFs by 2, which produces (25) and (26), respectively.

Appendix 4: Proof for Lemma 1

Since $\mathbf{U}$ and $\mathbf{V}$ are positive definite Hermitian matrices, $\mathbf{U}$ and $\mathbf{V}$ are invertible, and $(\mathbf{U} + \mathbf{V})$ is invertible Hermitian matrix as well. Using Woodbury matrix identity, we get

$$(\mathbf{U} + \mathbf{V})^{-1} = \mathbf{U}^{-1} - \mathbf{U}^{-1}\left(\mathbf{U}^{-1} + \mathbf{V}^{-1}\right)^{-1}\mathbf{U}^{-1}, \tag{52}$$

and thus

$$\begin{aligned}&\mathbf{x}^H \mathbf{U}^{-1}\mathbf{x} - \mathbf{x}^H (\mathbf{U} + \mathbf{V})^{-1}\mathbf{x} \\ &= \mathbf{x}^H \mathbf{U}^{-1}\left(\mathbf{U}^{-1} + \mathbf{V}^{-1}\right)^{-1}\mathbf{U}^{-1}\mathbf{x}\end{aligned} \tag{53}$$

Since $\mathbf{U}^{-1}\left(\mathbf{U}^{-1} + \mathbf{V}^{-1}\right)^{-1}\mathbf{U}^{-1}$ is positive definite, we can obtain $\mathbf{x}^H \mathbf{U}^{-1}\left(\mathbf{U}^{-1} + \mathbf{V}^{-1}\right)^{-1}\mathbf{U}^{-1}\mathbf{x} > 0$. Therefore, $\mathbf{x}^H \mathbf{U}^{-1}\mathbf{x} > \mathbf{x}^H (\mathbf{U} + \mathbf{V})^{-1}\mathbf{x}$.

Appendix 5: Proof for Proposition 1

According to (35), we can do some manipulations and express J_i as a summation of two quadratic components, which is given by

$$J_i = (l+2c)\left(a_i - \frac{2d}{l+2c}b_i\right)^2 + \frac{l^2-4c^2-4d^2}{l+2c}b_i^2. \tag{54}$$

We set $h_1\Delta g_1 = c_1 + jd_1$ and $h_2\Delta g_2 = c_2 + jd_2$. Given that $l = |h_1\Delta g_1|^2 + |h_2\Delta g_2|^2$, $c = \Re\{h_2^*\Delta g_2^* h_1\Delta g_1\}$, and $d = \Im\left\{h_2^*\Delta g_2^* h_1\Delta g_1\right\}$, the l, c and d can be expressed as $l = c_1^2+c_2^2+d_1^2+d_2^2, c = c_1c_2+d_1d_2$ and $d = d_1c_2 - d_2c_1$.

Hence, the representation of coefficient $l+2c$ is

$$l + 2c = (c_1+c_2)^2 + (d_1+d_2)^2 > 0 \tag{55}$$

and the second coefficient is

$$\frac{l^2-4c^2-4d^2}{l+2c} = \frac{\left(c_1^2+d_1^2-c_2^2-d_2^2\right)^2}{(c_1+c_2)^2+(d_1+d_2)^2} > 0. \tag{56}$$

Eqs. (55) and (56) show that the coefficients of the two quadratic components are positive. Therefore, the maximum value of J_i can be achieved only if the maximum values of $\left(a_i - \frac{2d}{l+2c}b_i\right)^2$ and b_i^2 can be simultaneously achieved. Given that $l + 2c > 0$, it can be seen that the values of $\left(a_i - \frac{2d}{l+2c}b_i\right)^2$ and b_i^2 depend upon the sign of d and the maximum modulus of a_i, b_i. Without loss of generality, we assume the maximum values of $|a_i|$ and $|b_i|$ are $a_{\max} > 0$ and $b_{\max} > 0$, respectively, under the current QAM modulation. For the square constellation case, $a_{\max} = b_{\max}$.

If $d = 0$, (54) reduces to

$$J_i = (l+2c)a_i^2 + \frac{l^2-4c^2-4d^2}{l+2c}b_i^2. \tag{57}$$

In this case, J_i can be maximized when $|a_i| = a_{\max}$ and $|b_i| = b_{\max}$, which implies the four angles of the constellation diagram.

If $d < 0$, it results in $-\frac{2d}{l+2c} > 0$. Thus, the quadratic components $\left(a_i - \frac{2d}{l+2c}b_i\right)^2$ and b_i^2 can be maximized when $a_i = a_{\max}, b_i = b_{\max}$ or $a_i = -a_{\max}, b_i = -b_{\max}$, which corresponds to the angles of constellation diagram in the first and third quadrants.

If $d > 0$, then $-\frac{2d}{l+2c} < 0$. In this case, a_i and b_i are required to have opposite signs and satisfy $a_i = a_{\max}$, $b_i = -b_{\max}$ or $a_i = -a_{\max}, b_i = b_{\max}$, which corresponds to the angles of constellation diagram in the second and fourth quadrants.

Appendix 6: Proof for Proposition 2

As per Eq. (33), it can be seen that $\sum_{i=1}^N |s_i|^2$ in the first item $\left(|h_1\Delta g_1|^2 + |h_2\Delta g_2|^2\right)\sum_{i=1}^N |s_i|^2$ is fixed in PSK and thereby it is not adjustable. Hence, the maximization of J depends upon whether or not the second item $2R = 2\Re\left\{h_2^*\Delta g_2^* h_1\Delta g_1 \sum_{i=1}^N s_i^2\right\}$ can be maximized through adjusting s_i. First, we apply Euler's formula and set

$$h_2^*\Delta g_2^* h_1\Delta g_1 = Ge^{j\phi} \tag{58}$$

where ϕ is defined as

$$\phi = \arctan\left(\frac{\Im\{h_2^*\Delta g_2^* h_1\Delta g_1\}}{\Re\{h_2^*\Delta g_2^* h_1\Delta g_1\}}\right) \in (-\pi, \pi].$$

According to (58) and $s_i = A_s e^{j\theta_i}$, we can obtain

$$R = \Re\left\{Ge^{j\phi}\sum_{i=1}^N A_s^2 e^{j2\theta_i}\right\} = A_s^2 G\sum_{i=1}^N \cos(2\theta_i + \phi). \tag{59}$$

Since θ_i is independent, we can separately adjust θ_i to maximize all R_i, where R_i is defined as

$$R_i = A_s^2 G\cos(2\theta_i + \phi). \tag{60}$$

As a result, R can be maximized because $R = \sum_{i=1}^N R_i$. Considering the $(-\pi, \pi]$ range limit of θ_i and ϕ, R_i can achieve its maximum value when $\theta_i = \frac{-\phi}{2}$ or $\theta_i = \frac{-\phi}{2} + \pi$.

Abbreviations

AF: Amplify-and-forward; CSCG: Circularly symmetric complex Gaussian; DT: Distance test; GLRT: Generalized likelihood ratio test; IQI: In-phase and quadrature-phase imbalance; ML: Maximum likelihood; PDF: Probability density function; PSK: Phase-shift keying; QAM: Quadrature amplitude modulation; Rx: Receiving; SNR: Signal-to-noise ratio; Tx: Transmitting; VF: Varying fingerprint

Authors' contributions

All authors read and approved the final manuscript.

Authors' information

Peng Hao (phao5@uwo.ca), Xianbin Wang (xianbin.wang@uwo.ca), and Aydin Behnad (abehnad@uwo.ca) are with the Department of Electrical and Computer Engineering, Western University, N6A 5B9 London, Ontario, CA.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 12 February 2018 Accepted: 6 February 2019
Published online: 14 March 2019

References

1. T. Halevi, H. Li, D. Ma, N. Saxena, J. Voris, T. Xiang, Context-aware defenses to RFID unauthorized reading and relay attacks. IEEE Trans. Emerg. Top. Comput. **1**(2), 307–318 (2013)
2. L. Wang, A. M. Wyglinski, Detection of man-in-the-middle attacks using physical layer wireless security techniques. Wirel. Commun. Mob. Comput. **16**(4), 408–426 (2016)
3. Y. Mao, M. Wu, in *2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, Toulouse*. Security Issues in Cooperative Communications: Tracing Adversarial Relays, (2006), pp. 69–72. https://doi.org/10.1109/ICASSP.2006.1660907
4. F. R. Yu, H. Tang, S. Bu, D. Zheng, Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks. EURASIP J. Wirel. Commun. Networking. **2013**(1), 188 (2013)

5. W. Wang, K. C. Teh, K. H. Li, Relay selection for secure successive af relaying networks with untrusted nodes. IEEE Trans. Inf. Forensic Secur. **11**(11), 2466–2476 (2016)
6. L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
7. J. Zhou, J. Shi, X. Qu, Landmark placement for wireless localization in rectangular-shaped industrial facilities. IEEE Trans. Veh. Technol. **59**(6), 3081–3090 (2010)
8. Y. Mao, M. Wu, Tracing malicious relays in cooperative wireless communications. IEEE Trans. Inf. Forensic Secur. **2**(2), 198–212 (2007)
9. K. Zeng, K. Govindan, P. Mohapatra, Non-cryptographic authentication and identification in wireless networks. IEEE Wirel. Commun. **17**(5), 56–62 (2010)
10. A. C. Polak, S. Dolatshahi, D. L. Goeckel, Identifying wireless users via transmitter imperfections. IEEE J. Sel. Areas Commun. **29**(7), 1469–1479 (2011)
11. M. Pospíšil, R. Marsalek, J. Pomenkova, in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), London*. Wireless device authentication through transmitter imperfections–measurement and classification, (2013), pp. 497–501. https://doi.org/10.1109/PIMRC.2013.6666187
12. Y. Shi, M. A. Jensen, Improved radiometric identification of wireless devices using MIMO transmission. IEEE Trans. Inf. Forensic Secur. **6**(4), 1346–1354 (2011)
13. H. Li, X. Wang, Y. Zou, in *2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA*. Exploiting transmitter I/Q imbalance for estimating the number of active users, (2013), pp. 3318–3322. https://doi.org/10.1109/GLOCOM.2013.6831584
14. M. Mokhtar, A. Gomaa, N. Al-Dhahir, OFDM AF relaying under I/Q imbalance: Performance analysis and baseband compensation. IEEE Trans. Commun. **61**(4), 1304–1313 (2013)
15. J. Li, M. Matthaiou, T. Svensson, I/Q imbalance in AF dual-hop relaying: Performance analysis in Nakagami-*m* fading. IEEE Trans. Commun. **62**(3), 836–847 (2014)
16. X. Wang, P. Hao, L. Hanzo, Physical-layer authentication for wireless security enhancement: Current challenges and future development. IEEE Commun. Mag. **54**(6), 152–158 (2016)
17. P. Hao, X. Wang, A. Behnad, in *2014 IEEE Global Communications Conference, Austin, TX*. Relay authentication by exploiting I/Q imbalance in amplify-and-forward system, (2014), pp. 613–618. https://doi.org/10.1109/GLOCOM.2014.7036875
18. F. Horlin, A. Bourdoux, *Digital Compensation for Analog Front-Ends*. (Wiley, Chichester, 2008)
19. W. Hou, M. Jiang, Enhanced joint channel and IQ imbalance parameter estimation for mobile communications. IEEE Commun. Lett. **17**(7), 1392–1395 (2013)
20. A. Tarighat, A.H. Sayed, Joint compensation of transmitter and receiver impairments in OFDM systems. IEEE Trans. Wirel. Commun. **6**(1), 240–247 (2007)
21. P. Murphy, A. Sabharwal, B. Aazhang, On building a cooperative communication system: Testbed implementation and first results. EURASIP J. Wirel. Commun. Netw. **2009**(1), 71–79 (2009)
22. G. J. González, F. H. Gregorio, J. E. Cousseau, T. Riihonen, R. Wichman, Full-duplex amplify-and-forward relays with optimized transmission power under imperfect transceiver electronics. EURASIP J. Wirel. Commun. Netw. **2017**(1), 76 (2017)
23. K. Y. Sung, C. Chao, Estimation and compensation of I/Q imbalance in OFDM direct-conversion receivers. IEEE J. Sel. Top. Signal Process. **3**(3), 438–453 (2009)
24. R. L. Filler, J. R. Vig, Long-term aging of oscillators. IEEE Trans. Ultrason. Ferroelectr. Freq. Control. **40**(4), 387–394 (1993)
25. P. L. Yu, J. S. Baras, B. M. Sadleru, Physical-layer authentication. IEEE Trans. Inf. Forensic Secur. **3**(1), 38–51 (2008)
26. A. G. i Fàbregas, G. Caire, Coded modulation in the block-fading channel: coding theorems and code construction. IEEE Trans. Inf. Theory. **52**(1), 91–114 (2006)
27. G. Verma, P. Yu, B. M. Sadler, Physical layer authentication via fingerprint embedding using software-defined radios. IEEE Access. **3**, 81–88 (2015)
28. F. Gao, R. Zhang, Y.-C. Liang, Optimal channel estimation and training design for two-way relay networks. IEEE Trans. Commun. **57**(10), 3024–3033 (2009)
29. J. Li, M. Matthaiou, T. Svensson, I/Q imbalance in two-way AF relaying. IEEE Trans. Commun. **62**(7), 2271–2285 (2014)
30. Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: Challenges and opportunities. IEEE Commun. Surveys Tuts. **18**(1), 94–104 (2016)
31. A. A. Boulogeorgos, V. M. Kapinas, R. Schober, G. K. Karagiannidis, I/Q-imbalance self-interference coordination. IEEE Trans. Wirel. Commun. **15**(6), 4157–4170 (2016)
32. Y. H. Chung, S. M. Phoong, Channel estimation in the presence of transmitter and receiver I/Q mismatches for OFDM systems. IEEE Trans. Wirel. Commun. **8**(9), 4476–4479 (2009)
33. A. Tarighat, R. Bagheri, A. H. Sayed, Compensation schemes and performance analysis of IQ imbalances in OFDM receivers. IEEE Trans. Signal Process. **53**(8), 3257–3268 (2005)
34. Y.-H. Chung, S.-M. Phoong, Joint estimation of I/Q imbalance, CFO and channel response for MIMO OFDM systems. IEEE Trans. Commun. **58**(5), 1485–1492 (2010)
35. S. M. Kenneth, *Complex stochastic processes: an introduction to theory and application*. (Addison-Wesley Pub. Co., NY, 1974)
36. S. M. Kay, *Fundamentals of statistical signal processing, Volume II: Detection Theory*. (Prentice Hall, NJ, 1998)
37. J. Bowers, *Matrices and Quadratic Forms, Chapter 13*. (Arnold, UK, 2000)
38. M. Abramowitz, I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. (Dover Publications, Washington, 1970)
39. M. K. Simon, M.-S. Alouini, *Digital communication over fading channels: a unified approach to performance analysis*. (Wiley, New York, 2005)
40. Y. Sun, A. Baricz, S. D. Zhou, On the monotonicity, log-concavity, and tight bounds of the generalized Marcum and Nuttall Q-functions. IEEE Trans. Inf. Theory. **56**(3), 1166–1186 (2010)
41. O. Ozdemir, R. Hamila, N. Al-Dhahir, I/Q imbalance in multiple beamforming OFDM transceivers: SINR analysis and digital baseband compensation. IEEE Trans. Commun. **61**(5), 1914–1925 (2013)
42. A. Gomaa, M. Mokhtar, N. Al-Dhahir, in *2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA*. Amplify-and-forward relaying under I/Q imbalance, (2012), pp. 4671–4676. https://doi.org/10.1109/GLOCOM.2012.6503856
43. A. L. Peressini, F. E. Sullivan, J. J. J. Uhl, *The mathematics of nonlinear programming*. (Springer, New York, 1988)
44. A. ElSamadouny, A. Gomaa, N. Al-Dhahir, A blind likelihood-based approach for OFDM spectrum sensing in the presence of I/Q imbalance. IEEE Trans. Commun. **62**(5), 1418–1430 (2014)
45. B. Picinbono, Second-order complex random vectors and normal distributions. IEEE Trans. Signal Process. **44**(10), 2637–2640 (1996)