Physical Layer Anonymous Communications

Zhongxiang Wei, Fan Liu, and Christos Masouros
Department of Electronic and Electrical Engineering, *University College London*, London, UK
{zhongxiang.wei, fan.liu, c.masouros}@ucl.ac.uk

***Abstract*—In the era of the big data, anonymity is recognized as an important attribute in privacy-preserving communications. The existing anonymous authentication, encryption, routing and protocols are applied at higher layers of networks, and ignore the fact that physical layer (PHY) also contains privacy-critical information, such as the signalling patterns and the inherent characteristics of channel fading. These can be used to identify traffic patterns and reveal users' identities, inflicting an unprecedented vulnerability to potential anonymity-violating behavior. Hence, privacy threats start from the acquisition of data, which necessitates complementary privacy solutions that reside at PHY. In this paper, we introduce the concept of PHY anonymity, and reveal the fact that the receiver is able to unmask the sender's identity by only analysing the PHY information. We first propose a novel sender detection strategy at the receiver, and then we develop a corresponding anonymous precoding design to address sender's anonymity while guaranteeing high receive signal-to-interference-plus-noise ratio (SINR) for communications. Simulation verifies that the proposed anonymous precoder is able to preserve anonymity and simultaneously guarantee high receive performance for communication purpose, opening a new dimension on anonymous designs at PHY.**

***Index Terms*—Anonymous Communications, Physical Layer, Sender Detection, Anonymous Precoding**

I. Introduction

In the era of cloud computing, storage and communications, the misuse of confidential data has attracted much attention in both commercial and military applications. Due to the inherent broadcast nature of wireless communications, threats arise from two main aspects, namely security and privacy. The aim of security is to prevent the confidential signal from being eavesdropped by potential adversaries. There has been extensive research on cryptography/authentication [1], covert communication [2], multiple-input and multiple-output (MIMO) beamforming plus artificial noise design, and cooperative jamming [3], from upper layer to physical layer (PHY) of networks. These extensive works enable confidential communications among the legitimate parities, while ensuring the signal is not breakable and decodable at adversaries. Differently, the aim of privacy is to guarantee the communication quality of the legitimate users, and meanwhile to conceal the identities of communication parties or the specific users' participation during the communications, also defined as anonymous communications [4]. A typical example of anonymous communications comes from remote healthcare applications, where patients wish to anonymously access online medical services by only sharing bio-information, whereas all the rest private information and the users' identity must be kept unknown. In summary, privacy-preserving techniques have become imperative, where the communication parties should only be able to process the data without the knowledge of other participants' identities.

There are three categories of anonymity, namely sender anonymity, receiver anonymity and bi-directional anonymity. The sender anonymity denotes that the receiver cannot trace sender's identity; receiver anonymity denotes that sender can contact receiver without knowing its identity; while the bi-directional anonymity means that both the sender and receiver communicate without knowing each other's identities [5]. To this end, researchers have unveiled various ways to enhance anonymity at the high layer of network, such as authentication and routing protocols. The general design principle is to apply anonymous authentication [6], mutual authentication [7], distributed authentication [8], or multiple times authentication/encryption [9] to conceal the participants' identity. On the other hand, a great deal of effort has been invested in designing anonymous routing for the Internet and the ad-hoc networks [10], which preserves the privacy of end hosts as well as routing paths by a number of cooperative nodes.

Nevertheless, there are still outstanding issues by the aforementioned anonymous techniques. i) Since the existing anonymous, mutual, distributed, or multiple times authentication/encryption techniques are generally based on public-key cryptosystems, they may be restrictive in many emerging scenarios of 5G-beyond networks due to the high computational requirement and latency, where the cooperation among the entities is required for both ring and group signature [6]. ii) The existing anonymous routing protocols are only applicable for large-scale networks. More importantly, none of the users could be off-line during the underlying process, and the cooperative participants should be fully honest, which is vulnerable to the internal malicious member attacks that can easily break the anonymity. iii) The existing anonymous techniques and associated protocols are employed at the upper layer of networks, assuming PHY provides a privacy-preserving link. In fact, the long-ignored PHY also contains information that can be used to extract the nodes' identities. When an anonymously authenticated/encrypted sender transmits signal via its wireless channel, the recipient can analyze the signalling patterns based on the characteristics of channel fading, and then is able to unmask the origin of the received signal. Thus, privacy threats start from the acquisition of data, which necessitates complementary privacy techniques that reside at PHY.

Motivated by the aforementioned open challenges, in this

paper, we present a first attempt to exploit the PHY sender detection design and its counterpart anonymous precoding technique. Our contributions are summarized as follows.

1) It is the first work to reveal that the PHY information, i.e., the signalling patterns and the inherent characteristics of wireless channel fading, can be judiciously analyzed to unmask the sender's identity and this incurs an unprecedented vulnerability by the anonymity-violating behavior at the receiver.
2) We first propose a low-complexity multiple hypothesis testing (MHT)-based sender detector, which exploits only the PHY information to break the sender's anonymity. Subsequently, we are motivated to develop a novel interference-suppression based anonymous (ISA) precoder against the sender detection scheme, which maximizes the per-antenna signal-to-interference-plus-noise ratio (SINR) for communications while simultaneously addressing anonymity by manipulating the patterns of the received signal. It is also proven that the applied semi-definite-relaxation (SDR) operation is tight and the optimality of the precoder is always maintained.
3) It is revealed that sender anonymity is achieved at the cost of reduced receive diversity, and hence the conventional receive equalizer that relies on the deterministic channel information becomes inapplicable. To this end, a novel transmit phase equalization scheme is dedicatedly proposed for removing the phase ambiguity without loss of anonymity or SINR performance.

Notations: $||\cdot||$ denotes the Euclidean norm. $\boldsymbol{A}^T$, $\boldsymbol{A}^H$, Tr($\boldsymbol{A}$), and Rank($\boldsymbol{A}$) denote the transpose, Hermitian transpose, trace and rank of matrix $\boldsymbol{A}$. $\boldsymbol{A} \succeq 0$ denotes a positive semi-definite matrix. $\boldsymbol{I}_n$ means an n-by-n identity matrix.

II. System Model and Anonymity Metrics

In this section, the system model and anonymity performance metric are presented in subsections II-A and II-B, respectively.

A. System Model

We consider an uplink multiuser MIMO system, and in particular a sender anonymity scenario, where users anonymously transmit data to an access point (AP) without leaking their identities. Assume the user set $\mathbb{K}$ consists of K users, and there is one user communicating (denote $\mathbb{S}$ as the sender) with the receiver at each time slot in a time-division-multiple-access (TDMA) fashion. The receiver is equipped with N_r antennas, while each user is equipped with N_t transmit antennas. Define $\boldsymbol{H}_k \in \mathbb{C}^{N_r \times N_t}$ as the MIMO channel between the user k and receiver, $\boldsymbol{W}_k$ as the precoding matrix, and $\boldsymbol{s}_k$ as the intended symbol vector. The received signal at the receiver is written as

$$\boldsymbol{y} = \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{s}_k + \boldsymbol{n}, \tag{1}$$

where $\boldsymbol{n} \in \mathbb{C}^{N_r \times 1}$ denotes the circularly symmetric complex Gaussian (CSCG) noise at the receiver, and its r-th element follows $[\boldsymbol{n}]_r \sim \mathcal{CN}(0, \sigma^2)$, $\forall r \in N_r$.

B. Performance Metric of Anonymity

Higher layer anonymity is typically quantified by an entropy based metric [11]. Considering the set $\mathbb{K}$, the receiver decides/assigns each user k in $\mathbb{K}$ a probability p_k of being the sender $\mathbb{S}$ based on its sender detection strategy. Hence, the anonymity entropy can be calculated as

$$H(\mathbb{K}) = -\sum_{k \in \mathbb{K}} p_k \log_2 p_k. \tag{2}$$

Evidently, the maximum anonymity entropy $H_{max}(\mathbb{K})$ is achieved when $p_k = \frac{1}{K}, \forall k \in \mathbb{K}$, i.e., the users are equally suspicious, with the maximal anonymity entropy $H_{max}(\mathbb{K}) = \log_2(K)$. Hence, the sender detection and sender's anonymity-preserving strategies are motivated by the following Remark.

Remark 1: As suggested by (2), the sender detection (denoted as $\mathcal{D}$) for the receiver is to correctly identify the real sender k with a high probability p_k of being the sender, i.e.,

$$\mathcal{D}^* = \max_{k \in \mathbb{K}} \{p_k | \mathbb{S} : k\}, \tag{3}$$

On the other hand, a favorable anonymity-preserving design at senders is to deteriorate the sender detection's performance, and guarantee a high receive quality for communications. □

III. Sender Detection Strategy

We first study the sender detection schemes at the receiver, where the receiver only analyzes the PHY information, i.e., the received signal and the inherent characteristics of the wireless channels to disclose identity of the sender. Hence, under the TDMA premise, the sender detection can be formulated as an MHT problem, given by

$$\mathbb{Y} = \begin{cases} \mathcal{H}_0: & \boldsymbol{n}, \\ \mathcal{H}_1: & \boldsymbol{H}_1 \boldsymbol{W}_1 \boldsymbol{s}_1 + \boldsymbol{n}, \\ \quad \vdots & \\ \mathcal{H}_K: & \boldsymbol{H}_K \boldsymbol{W}_K \boldsymbol{s}_K + \boldsymbol{n}, \end{cases} \tag{4}$$

where the hypothesis $\mathcal{H}_0$ means no data is transmitted from the user set $\mathbb{K}$ and only noise appears at the receiver. In comparison, hypothesis $\mathcal{H}_k$ denotes there is signal coming from the k-th sender. Apparently, to handle the MHT problem, the receiver can first detect the hypotheses $\mathcal{H}_0$, and the receiver only turns to detect the origin of the signal (the hypothesis $\mathcal{H}_1$ to $\mathcal{H}_K$) when $\mathcal{H}_0$ is decided as a false hypothesis. The detection of $\mathcal{H}_0$ leads to a classic energy detection that has been extensively researched in cognitive radios [12] [13], which is briefly discussed for the sake of completeness. Based on the received signal, the test statistic for energy detector is given by

$$\mathcal{T}(\boldsymbol{y}) = \frac{1}{N_r} \sum_{n=1}^{N_r} ||\boldsymbol{y}(n)||^2 = \frac{||\boldsymbol{y}||^2}{N_r}, \tag{5}$$

where $\boldsymbol{y}$ denotes the received signal vector and $\boldsymbol{y}(n)$ represents the signal on the n-th antenna. Under hypothesis $\mathcal{H}_0$, the test statistic $\mathcal{T}(\boldsymbol{y})$ is a Chi-square distributed variable with $2N_r$

degrees of freedom (DoF) [12]. Define the probability of a false alarm, under hypothesis $\mathcal{H}_0$, as the probability of the receiver falsely declaring the presence of an incoming signal. Assume the detection threshold β, the probability of false alarm of $\mathcal{H}_0$ is then given by

$$P_f(\beta|\mathcal{H}_0) = \Pr(\mathcal{T}(\boldsymbol{y}) > \beta|\mathcal{H}_0) = \int_{\beta}^{\infty} \psi_{(2N_r)}(x)\ \mathrm{d}x, \quad (6)$$

where $\psi_{(2N_r)}(x)$ denotes the probability density function (pdf) of a Chi-square distributed variable with $2N_r$ DoF. Note that there is a number of advanced energy detection schemes, such as eigenvalue [13] and feature-based detection [14]. Since energy detection has been extensively researched and is not our main contribution, we refer readers to [13] [14] for details. Once the receiver has sensed the presence of an incoming signal, it turns to detect the origin of the signal, and we have the following Remark for the detector's design.

Remark 2: The detection of the senders' identities is equivalent to the identification of the propagation channel $\boldsymbol{H}_k$ from the received signal, where the receiver is able to utilize the characteristics of the MIMO channel (which is also the unique PHY identity of the k-th user) to disclose the real sender. □

Starting from the fact that the norm of $\boldsymbol{H}_k^H\boldsymbol{H}_k$ is more likely to be larger than the norm of $\boldsymbol{H}_{k'}^H\boldsymbol{H}_k$, $\forall k' \neq k$, it is safe to conclude that with a high probability it holds that $||\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{s}_k||^2 \geq ||\boldsymbol{H}_{k'}^H\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{s}_k||^2$. Since the term $\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{s}_k$ denotes the received signal excluding noise, it is intuitive to multiply the received signal $\boldsymbol{y}$ with different $\boldsymbol{H}_k^H$ and calculate the norm of $\boldsymbol{H}_k^H\boldsymbol{y}$, $\forall k \in \mathbb{K}$. If the signal indeed comes from the channel $\boldsymbol{H}_k$, the resulting norm should be the largest among all the candidates. Finally, we reach a so-called MHT-based sender detector as

$$\mathcal{D}_{MHT}^{*} = \max_{k\in\mathbb{K}}\{||\boldsymbol{H}_1^H\boldsymbol{y}||^2, ..., ||\boldsymbol{H}_K^H\boldsymbol{y}||^2\}, \quad (7)$$

IV. Anonymous Precoding Design

In this section, on the contrary we investigate anonymous precoder at the sender end, which judiciously manipulates the pattern of the received signal to inhibit the receiver's detection. Problem formulation, optimization and transmit phase equalisation designs are presented in subsection IV-A, B, and C.

A. Problem Formulation for Anonymous Precoder Design

Since the aim of sender anonymity is to guarantee high receive quality for communications and meanwhile to conceal the senders' identities, a reasonable anonymous precoder needs to strike a good trade-off between these two metrics. Hence, we have Proposition 1 for the anonymous precoding design.

Proposition 1: Implementing sender anonymity conflicts with the design of receive equalizer, and thus anonymity is achieved at the cost of reduced receive diversity. □

Proposition 1 can be proved by a counter example. If the sender's anonymity is maintained and the identity of the sender is concealed, the receiver fails to know the exact channel that the signal comes from, further indicating that correct equalizer would be impossible. On the other hand, if the receive performance can be enhanced by channel equalizer at the receiver, no anonymity is achieved as the correct equalizer is essentially built on the deterministic knowledge of the sender's channel. In fact, proposition 1 essentially indicates that we need to treat each receive antenna as an individual receiver and impose per-antenna SINR constraint for multiplexing streams.

Without loss of generality, assume the k-th user as the sender at uplink. Denote $\boldsymbol{q}_i \in \mathbb{C}^{N_t\times 1}$ as the i-th column of the precoding matrix $\boldsymbol{W}_k$ (i.e., $\boldsymbol{W}_k = [\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]$), which corresponds to the precoder for the symbol s_i. Denote $\boldsymbol{h}_i \in \mathbb{C}^{1\times N_t}$ as the channel between the i-th receive antenna and sender (i.e., $\boldsymbol{H}_k = [\boldsymbol{h}_1^T, ..., \boldsymbol{h}_{N_r}^T]^T$). To scramble the sender detection at the receiver, the anonymous precoder should suppress the norm of $\boldsymbol{H}_k^H\boldsymbol{y}$ small enough to address the norm test. Since the exact value of receive noise is unknown at the sender, we alternatively suppress the norm of $\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{W}_k$, which has the same effect to manipulating the norm of $\boldsymbol{H}_k^H\boldsymbol{y}$ and guarantees the real sender hiding in the user sets $\mathbb{K}$. Now, we present the problem formulation, which maximizes the minimal per-antenna SINR Γ under the power and anonymity constraints, such as

$$\begin{aligned} P1: &\max_{[\boldsymbol{q}_1,...,\boldsymbol{q}_{N_r}]}\ \Gamma, \\ \text{s.t. } (C1): &\frac{||\boldsymbol{h}_i\boldsymbol{q}_i||^2}{\sigma^2 + \sum_{i'=1,i'\neq i}^{N_r}||\boldsymbol{h}_i\boldsymbol{q}_{i'}||^2} \geq \Gamma, \forall i \in N_r, \\ (C2): &\sum_{i=1}^{N_r}||\boldsymbol{q}_i||^2 \leq p_{max}, \\ (C3): &||\boldsymbol{H}_k^H\boldsymbol{H}_k[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]||^2 \leq \epsilon, \end{aligned} \quad (8)$$

where (C1) denotes that the per-antenna SINR should be higher than the lower-bound Γ. It is also observed that each receive antenna is impaired by inter-antenna interference, which acts as multi-user interference in multiple-input and single-output systems. (C2) guarantees the transmission power lower than the budget p_{max}. (C3) suppresses the norm to be lower than a threshold ϵ to scramble the sender detector at the receiver.

B. Optimization Design for Anonymous Precoder Design

The optimization problem P1 is a non-convex second-order cone programming (SOCP), where the coupling of the objective Γ and inter-antenna interference in (C1) makes the optimization intractable. However, it is straightforward to show that the constraint (C2) will be achieved with equality at the optimum. Otherwise, we can simply increase the transmission power to further improve the value of Γ, thus contradicting optimality. Hence, we begin with the dual power minimization problem as

$$\begin{aligned} P1(a): \min\ \ &f_{\Gamma^{(j)}}([\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]) \triangleq \sum_{i=1}^{N_r}||\boldsymbol{q}_i||^2 \\ \text{s.t. } (C4): &\frac{||\boldsymbol{h}_i\boldsymbol{q}_i||^2}{\sigma^2 + \sum_{i'=1,i'\neq i}^{N_r}||\boldsymbol{h}_i\boldsymbol{q}_{i'}||^2} \geq \Gamma^{(j)}, \forall i \in N_r, \\ (C5): &||\boldsymbol{H}_k^H\boldsymbol{H}_k[\boldsymbol{q}_1, ..., \boldsymbol{q}_{N_r}]||^2 \leq \epsilon, \end{aligned} \quad (9)$$

where $\Gamma^{(j)}$ serves as the pre-set per-antenna minimum SINR requirement and superscript j denotes the index of iteration as

detailed later. Let $f^*_{\Gamma^{(j)}}$ represent the consumed power of P1(a) with the minimum SINR requirement $\Gamma^{(j)}$. In fact, solving P1 with (C2) upper bounded by $f^*_{\Gamma^{(j)}}$ yields an optimal objective value of $\Gamma^{(j)}$. Furthermore, the optimal objective values of problems P1(a) and P1 are strictly monotonic increasing. Therefore, considering $\Gamma^{(j)}$ as a variable of optimization, the optimal solution of P1 can be obtained by alternatively solving P1(a) for a given $\Gamma^{(j)}$ and searching over different $\Gamma^{(j)}$. Since P1(a) is still a non-convex SOCP problem, we define $\boldsymbol{Q}_i = \boldsymbol{q}_i\boldsymbol{q}_i^H \in \mathbb{C}^{N_t\times N_t}, \forall i \in N_r$, and transform P1(a) into a semi-definite programming (SDP) as

$$
\begin{aligned}
P1(b): \ & \min \sum_{i=1}^{N_r} \mathrm{Tr}(\boldsymbol{Q}_i) \\
\text{s.t. } & (\tilde{C}4): \mathrm{Tr}(\boldsymbol{h}_i\boldsymbol{Q}_i\boldsymbol{h}_i^H) - \\
& \qquad \Gamma^{(j)}(\sigma^2 + \sum_{i'=1,i'\neq i}^{N_r} \mathrm{Tr}(\boldsymbol{h}_i\boldsymbol{Q}_{i'}\boldsymbol{h}_i^H)) \geq 0, \forall i \in N_r, \quad (10) \\
& (\tilde{C}5): \mathrm{Tr}(\boldsymbol{H}_k^H\boldsymbol{H}_k(\sum_{i=1}^{N_r}\boldsymbol{Q}_i)\boldsymbol{H}_k\boldsymbol{H}_k^H) \leq \epsilon, \\
& (C6): \boldsymbol{Q}_i \succeq \boldsymbol{0}, \forall i \in N_r, (C7): \mathrm{Rank}(\boldsymbol{Q}_i) = 1, \forall i \in N_r,
\end{aligned}
$$

where ($\tilde{C}4$) and ($\tilde{C}5$) are the linear matrix inequalities (LMI)s transformed from (C4) and (C5). Constraints (C6) and (C7) are the SDR of $\boldsymbol{Q}_i = \boldsymbol{q}_i\boldsymbol{q}_i^H$, $\forall i \in N_r$. Neglecting the rank-one constraint in (C7), P1(b) becomes a standard SDP and can be readily solved by optimization solvers. Hence, the procedure starts with an initial value of $\Gamma^{(j)}$, and we solve P1(b) to obtain $\boldsymbol{Q}_i^*$, $\forall i \in N_r$. If the consumed power, i.e., $\sum_{i=1}^{N_r}\mathrm{Tr}(\boldsymbol{Q}_i)$, is smaller than the budget p_{max}, we can increase the value of $\Gamma^{(j)}$, otherwise decrease the value of $\Gamma^{(j)}$. The iteration is operated until convergence. Obviously, if the obtained optimal solution $\boldsymbol{Q}_i^*$ is of rank 1, then SDR is tight and the optimal beamformer $\boldsymbol{q}_i^*$ can be simply obtained by the eigenvalue decomposition (the principal eigen-vector of $\boldsymbol{Q}_i^*$). Regarding the rank of the optimal solution, we have the following Proposition.

Proposition 2: Under the condition of independently distributed MIMO channels, the optimal solution of P1(b) satisfies $\mathrm{Rank}(\boldsymbol{Q}_i) = 1, \forall i \in N_r$, with probability one. □

Proof: The transformed problem P1(b) is jointly convex with respect to the variables and satisfies the Slater's conditions (without (C7)). Hence, strong duality holds and solving the dual problem is equivalent to solving the primal problem. We first write the Lagrangian function of the primal problem as

$$
\begin{aligned}
\mathcal{L} = & \sum_{i=1}^{N_r}\mathrm{Tr}(\boldsymbol{Q}_i) + \mu(\mathrm{Tr}(\boldsymbol{\Pi}\sum_{i=1}^{N_r}\boldsymbol{Q}_i) - \epsilon) - \sum_{i=1}^{N_r}\boldsymbol{P}_i\boldsymbol{Q}_i \\
& \sum_{i=1}^{N_r}\lambda_i\big(\Gamma^{(j)}\sigma^2 + \Gamma^{(j)}\sum_{i'\neq i, i'=1}^{N_r}\mathrm{Tr}(\boldsymbol{G}_i\boldsymbol{Q}_{i'}) - \mathrm{Tr}(\boldsymbol{G}_i\boldsymbol{Q}_i)\big),
\end{aligned} \quad (11)
$$

where $\boldsymbol{\Pi} = \boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{H}_k^H\boldsymbol{H}_k$ and $\boldsymbol{G}_i = \boldsymbol{h}_i^H\boldsymbol{h}_i$ for brevity. μ and λ_i are the Lagrange multipliers for the constraints ($\tilde{C}5$) and ($\tilde{C}4$), respectively, while matrix $\boldsymbol{P}_i \in \mathbb{C}^{N_t\times N_t}$ is the Lagrange multiplier matrix for the positive semi-definite constraint (C6). Hence, the dual problem for P1(b) in (10) is written as $\max_{\mu\geq 0,\lambda_i\geq 0,\boldsymbol{P}_i\succeq\boldsymbol{0}}\min_{\boldsymbol{Q}_i}\mathcal{L}(\mu,\lambda_i,\boldsymbol{P}_i,\boldsymbol{Q}_i)$. We now reveal the structure of the optimal $\boldsymbol{Q}_i$ by studying the Karush-Kuhn-Tucker (KKT) conditions, including the dual constraints: $\mu^* \geq 0, \lambda_i^* \geq 0, \boldsymbol{P}_i^* \succeq \boldsymbol{0}, \forall i \in N_r$; and complementary slackness: $\boldsymbol{P}_i^*\boldsymbol{Q}_i^* \succeq \boldsymbol{0}, \forall i \in N_r$; and the gradient of Lagrange function with respect to $\boldsymbol{Q}_i$ vanishing to 0: $\frac{\partial\mathcal{L}}{\partial\boldsymbol{Q}_i}|_{\boldsymbol{Q}_i^*} = 0$:

$$
\frac{\partial\mathcal{L}}{\partial\boldsymbol{Q}_i}|_{\boldsymbol{Q}_i^*} = \boldsymbol{R}_i^* - \boldsymbol{P}_i - \lambda_i^*\boldsymbol{G}_i = 0, \forall i \in N_r, \quad (12)
$$

where $\boldsymbol{R}_i^* = \boldsymbol{I}_{N_t} + \Gamma^{(j)}\sum_{i'\neq i}^{N_r}\lambda_{i'}^*\boldsymbol{G}_{i'} + \mu^*\boldsymbol{\Pi}$. It further yields $\boldsymbol{P}_i^* = \boldsymbol{R}_i^* - \lambda_i^*\boldsymbol{G}_i$. Indeed, it can be verified that in order to meet the per-antenna SINR constraints, it must hold that $\mathrm{rank}(\boldsymbol{Q}_i^*) \geq 1$ with $\boldsymbol{Q}_i^* \neq \boldsymbol{0}$. Hence, the complementary slackness $\boldsymbol{P}_i\boldsymbol{Q}_i = \boldsymbol{0}$ indicates $\mathrm{Rank}(\boldsymbol{P}_i^*) \leq N_t - 1$.

If $\mathrm{Rank}(\boldsymbol{P}_i^*) = N_t - 1$, then the optimal beamforming matrix $\boldsymbol{Q}_i^*$ must be a rank-one matrix. In order to further reveal the structure of $\boldsymbol{P}_i^*$, we first show by contradiction that $\boldsymbol{R}_i^*$ is a positive-definite matrix with probability one under the condition stated in the Proposition 2. For a given set of optimal dual variables, i.e., $\mu^*, \lambda_i^*, \boldsymbol{P}_i^*$, the dual problem can be written as $\min_{\boldsymbol{Q}_i}\mathcal{L}(\boldsymbol{Q}_i, \mu^*, \lambda_i^*, \boldsymbol{P}_i^*)$. Suppose $\boldsymbol{R}_i^*$ is not positive-definite. In this case, we can choose $\boldsymbol{Q}_i = \beta\boldsymbol{r}_i\boldsymbol{r}_i^H$ as one of the optimal solution of the dual problem, where $\beta > 0$ is a scaling parameter and $\boldsymbol{r}_i$ is the eigenvector corresponding to a non-positive eigenvalue $\rho_i < 0$ of $\boldsymbol{R}_i^*$, i.e., $\boldsymbol{R}_i^*\boldsymbol{r}_i = \rho_i\boldsymbol{r}_i$. With $\boldsymbol{Q}_i = \beta\boldsymbol{r}_i\boldsymbol{r}_i^H$ and $\boldsymbol{R}_i^*\boldsymbol{r}_i = \rho_i\boldsymbol{r}_i$, we have

$$
\sum_{i=1}^{N_r}\mathrm{Tr}(\beta\boldsymbol{r}_i\boldsymbol{r}_i^H) - \rho\sum_{i=1}^{N_r}\mathrm{Tr}(\boldsymbol{r}_i\boldsymbol{r}_i^H(\boldsymbol{P}_i^* + \lambda_i\boldsymbol{G}_i)) \quad (13)
$$

It is observed that the first term in (13) is not positive. For the second term, since the channel vector $\boldsymbol{h}_i$ is statistically independent, and based on $\boldsymbol{P}_i^* \succeq \boldsymbol{0}$, we have the second term $\rho\sum_{i=1}^{N_r}\mathrm{Tr}(\boldsymbol{r}_i\boldsymbol{r}_i^H(\boldsymbol{P}_i^* + \lambda_i\boldsymbol{G}_i))$ is greater than 0. Setting $\rho \to \infty$, we have the term $-\rho\sum_{i=1}^{N_r}\mathrm{Tr}(\boldsymbol{r}_i\boldsymbol{r}_i^H(\boldsymbol{P}_i^* + \lambda_i\boldsymbol{G}_i)) \to -\infty$. In this case, the dual optimal value becomes unbounded from below. However, the optimal value of the primal problem (10) is non-negative. Thus, strong duality cannot hold which leads to a contradiction. Therefore, $\boldsymbol{R}_i^*$ is a positive-definite matrix with probability one, i.e., $\mathrm{Rank}(\boldsymbol{R}_i^*) = N_t$. Based on the sub-additivity property of the rank operation, we have

$$
\begin{aligned}
\mathrm{Rank}(\boldsymbol{P}_i^*) + \mathrm{Rank}(\lambda_i\boldsymbol{G}_i) &\geq \mathrm{Rank}(\boldsymbol{P}_i^* + \lambda_i\boldsymbol{G}_i) \\
&= \mathrm{Rank}(\boldsymbol{R}_i^*) \Rightarrow \mathrm{Rank}(\boldsymbol{P}_i^*) = N_t - 1.
\end{aligned} \quad (14)
$$

Based on (14), we obtain that $\mathrm{Rank}(\boldsymbol{P}_i^*) = N_t - 1$. Thus, $\mathrm{Rank}(\boldsymbol{Q}_i^*) = 1$ holds with probability one. ■

C. Transmit Phase Equalizer for Eliminating Phase Ambiguity

Now, the tightness of SDR operation in P1(b) has been confirmed by Propositions 2, and the optimal precoder $\boldsymbol{q}_i^*$ can be obtained by the matrix decomposition. Nevertheless, while the receive SINR and sender's anonymity can always be guaranteed after decomposition, the received signal propagating through the channel may have phase ambiguity, which impairs

the de-modulation at the receiver. Conventionally, receive phase equalisation is adopted to align phase of the received signal with the desired symbol. However, since the sender's identity is concealed by the anonymous precoder and the receiver may not be able to declare the correct channel, the conventional receive phase equalization is disabled in anonymous communications. Hence, we further propose a dedicated transmit phase equalization for removing phase ambiguity at the receiver.

Proposition 3: With the optimal precoder $\boldsymbol{q}_i^*$ for the symbol s_i, the desired signal at the i-th receive antenna is calculated as $\boldsymbol{h}_i\boldsymbol{q}_i^* s_i$, which should have the same phase to the desired symbol s_i. Write $\boldsymbol{h}_i\boldsymbol{q}_i^* = |\boldsymbol{h}_i\boldsymbol{q}_i^*|e^{j\varphi_i}$, where φ_i denotes the angle of the complex number $\boldsymbol{h}_i\boldsymbol{q}_i^*$. Hence, the transmit phase equalization is calculated as $\boldsymbol{q}_i^* = \boldsymbol{q}_i^* e^{-j\varphi_i}$, which makes the desired signal $\boldsymbol{h}_i\boldsymbol{q}_i^* s_i$ have exactly same phase to the desired symbol s_i to avoid phase ambiguity without violating anonymity and per-antenna SINR performance. □

Proof: Recalling (C4), the power of the desired signal remains unchanged after the equalization such as $||\boldsymbol{h}_i\boldsymbol{q}_i^* e^{-j\varphi_i}||^2 = ||\boldsymbol{h}_i\boldsymbol{q}_i^*||^2$. Also based on the trigonometry property of norm operation, the power of the overall inter-antenna interference after equalization $||\sum_{i'=1,i'\neq i}^{N_r} \boldsymbol{h}_i\boldsymbol{q}_{i'}^* e^{-j\varphi_{i'}}||^2$ is upper bounded by $\sum_{i'=1,i'\neq i}^{N_r} ||\boldsymbol{h}_i\boldsymbol{q}_{i'}^* e^{-j\varphi_{i'}}||^2 = \sum_{i'=1,i'\neq i}^{N_r} ||\boldsymbol{h}_i\boldsymbol{q}_{i'}^*||^2$, denoting the obtained optimal per-antenna SINR remained unchanged. On the other hand, the sender's anonymity is also maintained after transmit phase equalization, as phase rotation of $\boldsymbol{q}_i$ has no impact on the trace of $\boldsymbol{Q}_i, \forall i \in N_r$. ■

Evidently, the proposed transmit phase equalization only requires the knowledge of the channel information and the symbols to be transmitted. Now we are able to devise the whole algorithm, as summarized in Algorithm 1. We first solve P1(b) to obtain the optimal matrix $\boldsymbol{Q}_i^*$, and $\boldsymbol{q}_i^*$ is immediately obtained, $\forall i \in N_r$. Afterwards, transmit phase equalization is applied onto $[\boldsymbol{q}_1^*, ..., \boldsymbol{q}_{N_r}^*]$ for eliminating receiver's phase ambiguity without violating SINR and anonymity performance.

Algorithm 1 The Algorithm of ISA Precoder Design

Input: MIMO channel $\boldsymbol{H}_k$, power budget p_{max}, symbol vector $\boldsymbol{s}_k$, initial left bound Γ_l, right bound Γ_r, anonymity threshold ϵ, and tolerance τ.

Initialize $\Gamma^{(j)} = (\Gamma_l + \Gamma_r)/2$.
while $|\Gamma_r - \Gamma_l| \geq \tau$ **do**
  Solve P1(b) with $\Gamma^{(j)}$. Let $f^*_{\Gamma^{(j)}} = \sum_{i=1}^{N_r} \mathrm{Tr}(\boldsymbol{Q}_i)$
  Calculate the power reward factor $R = p_{max} - f^*_{\Gamma^{(j)}}$.
  if $R \geq 0$ **then**
    Update $\Gamma_l = \Gamma^{(j)}$.
  else
    Update $\Gamma_r = \Gamma^{(j)}$.
  end if
  Update the iteration index $j = j + 1$; Update $\Gamma^{(j)} = \frac{\Gamma_l + \Gamma_r}{2}$.
end while
Decompose $\boldsymbol{Q}_i^*$ to obtain the $\boldsymbol{q}_i^*$, $\forall i \in N_r$. Do transmit phase equalization to avoid phase ambiguity, based on Proposition 3.

Output: Optimal precoding design $[\boldsymbol{q}_1^*, ..., \boldsymbol{q}_{N_r}^*]$.

V. Complexity Analysis for the Sender Detection and Anonymous Precoder

Now we calculate the complexities of the proposed detector and anonymous precoder [3]. The sender detector multiplies the received signal with different $\boldsymbol{H}_k^H$ and calculates the norm of $\boldsymbol{H}_k^H\boldsymbol{y}$ in sequence. Hence, its overall complexity of the MHT-based detector is given as $K(8N_tN_r+8N_t)$. On the other hand, for the anonymous precoder, it first iteratively solves P1(b) to obtain the optimal SDR matrices $\boldsymbol{Q}_i$, $\forall i \in N_r$. Since P1(b) subjects to N_r LMI constraints (trace) in ($\tilde{C}4$) with size 1, 1 LMI constraint (trace) in ($\tilde{C}5$) with size 1, N_r LMI constraints in (C6) with size N_t (and (C7) is removed by SDR operation), the complexity for iteratively optimizing P1(b) is given as $l_i\sqrt{N_r+1+N_rN_t}\ln(\frac{1}{\tau})\big(n_1(N_r+1+N_rN_t^3)+n_1^2(N_r+1+N_rN_t^2)+n_1^3\big)$, where l_i denotes the number of iterations for convergence and will be further demonstrated in simulations. τ represents the tolerance of accuracy [3]. Afterwards, eigenvalue decomposition for $\boldsymbol{Q}_i$ is computed for obtaining $\boldsymbol{q}_i$ with complexity $23N_t^3$, followed by transmit phase equalization with complexity $8N_t$. Hence, the overall complexity of the ISA precoder is given as $l_i\sqrt{N_r+1+N_rN_t}\ln(\frac{1}{\tau})\big(n_1(Nr+1+N_rN_t^3)+n_1^2(N_r+1+N_rN_t^2)+n_1^3\big)+N_r(23N_t^3+8N_t)$.

VI. Simulation Results

We now present the Monte-Carlo simulations. Without loss of generality, power budget is set to as $p_{max} = 1$ Watt. QPSK is adopted as modulation scheme and the transmitted symbol vector is randomly generated. Assume that each block consists of 50 symbols. There are $K = 5$ potential senders, and the sender in each time slot (block) is randomly selected. Rayleigh block-fading channel is adopted. The antenna configuration is set to as $N_r = N_t = 10$. The energy detection threshold in (6) is set to as $\beta = 10^{-2}$. The following classic precoders are selected as benchmarks: 1) Singular value decomposition (SVD) precoder [15], where its precoder and equaliser are obtained by the SVD of channel matrix. In particular, the receiver first detects the origin of the received signal and then calculates its equaliser based on the declared hypothesis. 2) Minimum-mean-squared-error (MMSE) precoder [16]. For fair comparison, the dissipated power at the sender side is normalized to p_{max} for all the precoders, i.e., $||\boldsymbol{W}\boldsymbol{s}||^2 = p_{max}$.

In Fig. 1(a), the receiver's detection error rate (DER) performance is demonstrated. First, with the reduced detrimental impact of noise at higher SNR regime, the accuracy of the sender detector of the receiver is improved (except MMSE) and hence the receiver's detection becomes more accurate. Nevertheless, it is observed that the ISA precoder achieves a strong anonymity, where the DER is maintained at up to 0.7 even with high receive SNR. It also proves that the anonymity is guaranteed after the SDR and transmit phase equalization. In comparison, the SVD precoder demonstrates the worst anonymity, where the receiver is able to unmask the real sender with below 10^{-2} DER at 10 dB. By the MMSE precoder, the receiver's DER demonstrates a U-shape. It is because the detection is significantly impaired by the receive noise at low

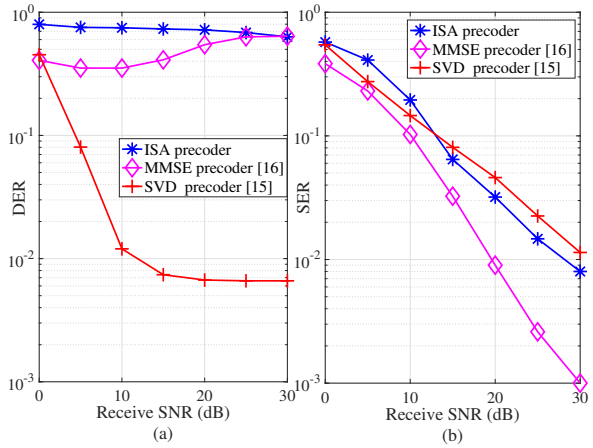

Fig. 1. The impact of receive SNR on the DER and SER by different precoders, where anonymity threshold $\epsilon = 20$.

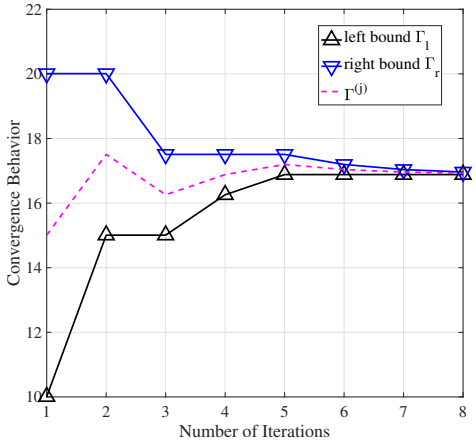

Fig. 2. The convergence behavior on finding $\Gamma^{(j)}$ by P1(b), where $\epsilon = 20$.

SNR regime. While at high SNR regime, the MMSE precoder approaches to zero-forcing (ZF) precoder and thus the received signal tends to be $\boldsymbol{y} = \boldsymbol{s}_k + \boldsymbol{n}$, where the sender's channel information is removed. As a result, the DER by the MMSE precoder is occasionally maintained at high receive SNR. On the other hand, the symbol error rate (SER) [17] performance is demonstrated in Fig. 1(b). For the ISA precoder, although its DoF of the precoder is constrained by the anonymity constraint, it still demonstrates a close SER to the SVD precoder at 0-12 dB SNR regimes, and outperforms the SVD precoder with above 12 dB SNR. Hence, the proposed anonymous precoder indeed strikes a good trade-off between guaranteeing high communication quality and addressing sender's anonymity.

Fig. 2 shows the convergence behavior by the ISA precoder, where initial $\Gamma_r = 20$, $\Gamma_l = 0$, and tolerance $\tau = 0.1$. Since bisection search is adopted for updating the intermediate $\Gamma^{(j)}$ in Algorithm 1, at most $\ln(\frac{\Gamma_r - \Gamma_l}{\tau})$ iterations is required for convergence. As seen, the algorithm converges to a stationary point with around 6-7 iterations, confirming its low complexity.

VII. CONCLUSIONS

In this paper, we have proposed the concept of PHY anonymity, and revealed that by only analysing PHY information, the receiver is able to unmask the senders' identities. Then, we have proposed a low-complexity MHT-based detector for the receiver, which utilizes the signalling patterns and the inherent characteristics of channel fading to break the senders' anonymity. Subsequently, it has been motivated to propose an anonymous precoder to guarantee the senders' anonymity while maximizing per-antenna SINR performance, assisted by a novel transmit phase equaliser dedicated for eliminating the possible phase ambiguity in anonymous communications. Compared to the benchmarks, simulation results have confirmed that the proposed anonymous precoder is able to inhibit the anonymity-violating behavior at the receiver with high DER, and simultaneously provide high per-antenna SINR for communications with low SER performance.

REFERENCES

[1] J. Zhang, R. Woods, and T. Duong, "Efficient key generation by exploiting randomness from channel of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578-2588, Jun. 2016.

[2] J. Hu, *et al.,* "Covert communication achieved by a greedy relay in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766-4779, Jul. 2018.

[3] Z. Wei and C. Masouros, "Device-centric distributed antenna transmission: secure precoding and antenna selection with interference exploitation," *IEEE Internet Things J.,* vol. 7, no. 3, pp. 192-203, Mar. 2020.

[4] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," *in Workshop PET'02,* San Francisco, USA, Apr. 2002.

[5] George Danezis, "Introducing anonymous communications properties, threat models, systems and attack," [Online] http://www0.cs.ucl.ac.uk/staff/G.Danezis/talks/AnonTalk.pdf, 2006.

[6] C. C. Chang, C. Y. Lee, and Y. C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," *Computer Commun.*, vol. 32, pp. 611–618, 2009.

[7] R. Lu *et al.,* "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Trans. Veh. Technol.,* vol. 58, no. 3, pp. 1454-1466, Mar. 2009.

[8] P. Gope *et al.*, "Anonymous communications for D2D-aided fog computing," *IEEE Consumer Electron. Maga.*, vol. 15, pp. 10-16, May 2019.

[9] B. Lian, G. Chen, M. Ma, and J. Li, "Periodic K-times anonymous authentication with efficient revocation of violator's credential," *IEEE Trans. Inf. Forensics Secur.,* vol. 10, no. 3, pp. 543-557, Mar. 2015.

[10] K. Sakai *et al.*, "On anonymous routing in delay tolerant networks," *IEEE Trans. Mobile Comput.,* vol. 18, no. 12, pp. 2926-2940, Dec. 2019.

[11] C. Chou, D. Wei, and K. Naik, "An efficient anonymous communication protocol for peer-to-peer applications over mobile Ad-hoc networks," *IEEE J. Sel. Areas Commun.,* vol. 25, no. 1, pp. 192-203, Jan. 2007.

[12] Y. C. Liang *et al.*, "Sensing-throughput trade-off for CR networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[13] Y. Zeng and Y. Liang, "Eigenvalue-based spectrum sensing for cognitive radio," *IEEE Trans. Commun.*, vol. 57, no. 6, pp. 1784-1793, Jun. 2009.

[14] M. Kosunen, V. Turunen, and J. Ryynanen, "Survey and analysis of cyclostationary signal detector implementations on FPGA," *IEEE J. Emerg. Sel. Topic Circuits Syst.*, vol. 3, no. 4, pp. 541-551, Dec. 2013.

[15] D. Tse and P. Viswanath, Fundamentals of Wireless Communications. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[16] C. B. Peel *et al.,* "A vector-perturbation technique for near-capacity multi-antenna multiuser communication—part I: channel inversion and regularization," *IEEE Trans. Wireless Commun.*, vol. 53, no. 1, pp. 195-202, Jan. 2005.

[17] Z. Wei, C. Masouros, K. Wong, and X. Kang, "Multi-cell interference exploitation: enhancing the power efficiency in cell coordination," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 547-562, Jan. 2020.