Physical Layer Anonymous Precoding Design: From the Perspective of Anonymity Entropy

Zhongxiang Wei, *Member, IEEE,* Christos Masouros, *Senior Member, IEEE,* Ping Wang, *Member, IEEE,* Xu Zhu, *Senior Member, IEEE,* Jingjing Wang, *Senior Member, IEEE,* and Athina P. Petropulu, *Fellow, IEEE*

***Abstract*—In the era of e-Health, privacy protection has become imperative in applications that carry personal and sensitive data. Departing from the data-perturbation based privacy-preserving techniques that reduce the fidelity of the disclosed data, in this paper we investigate anonymous communications, which mask the identity of the data sender while providing high data reliability. Focusing on the physical (PHY) layer, we first explore the break of privacy through a statistical attribute based sender detection (SD) from the receiver. Compared to the existing literature, this enables a much enhanced SD performance, especially when the users are equipped with different numbers of antennas. To counteract the advanced SD approach above, we formulate explicit anonymity constraints for the design of the anonymous precoder, which mask the sender's PHY attributes that can be exploited by SD, while at the same time preserving the reliability of the data. Then, anonymity entropy-oriented precoders are proposed for different antenna configurations at the users, which adaptively construct a maximum number of aliases while obeying users' signal-to-noise-ratio requirements for data accuracy. Simulation results demonstrate that the proposed anonymous precoders provide the highest level of anonymity entropy over the benchmarks, while achieving reasonable symbol error rate for the communication signal.**

***Index Terms*—Anonymous Communications, Statistical Attribute based Sender Detection, Anonymity Entropy oriented Precoding, Homogeneous and Heterogeneous Antennas Configurations, Physical Layer**

I. Introduction

The COVID-19 pandemic continues to take its toll across the world, bringing upheaval to societies and economies around the globe. Coordinated mechanisms across health sectors have been anticipated to support the response to the outbreak, and e-Health has been prompted as one of the most promising approaches to address this challenge. Promising e-Health applications include edge-based crowd monitoring and contact tracing, and reporting patients' physiological signals, such as heart rate and temperature, to a local access point (AP) for medical diagnosis and modelling. Most of the devices used, at some point, convey information in a wireless fashion. However, the broadcast nature of wireless communications poses a threat to the confidential and personal nature of the e-Health information, for which high levels of security and privacy are required [1] [2]. Information security in wireless communications has been extensively studied from higher layers to the physical (PHY) layer [3]-[9]. Here, we are concerned with privacy-oriented design. Considering the distributed and autonomous nature of edge AP nodes, private information can easily leak to a legitimate but curious AP receiver during e-Health applications. For example, while users need to expose their identities (ID)s to a local AP for trajectory/position monitoring and contact tracing, at other times they may need to send private signals to the AP for communications. During those times, in conventional privacy-agnostic communication systems, the local AP can easily correlate and link the received data to the specific sender's ID. By inferring private information from the sender, the AP could potentially misuse that information for cyber-fraud, or to launch other malicious attacks. Privacy leakage also occurs when users share their physiological signals to an AP for statistical modelling, diagnosis, recording or high-level detection of anomalies.

In general, security- and privacy-oriented research on attack models, protection methodologies and performance metrics, are different. In particular, 1) *the attack models of security and privacy intrusion are different*. From the point of view of security, an illegitimate adversary aims to eavesdrop the signal of other communication parties, and decipher the embedded data [1]. In contrast, in the context of privacy, an adversary may be the legitimate receiver of the data, but out of curiosity wants to infer the sender's non-shared data [2], or the sender's ID [10] from the received data. 2) Accordingly, *the protection mechanisms against security and privacy intrusions are different*. Secrecy designs enable confidential communications among the legitimate parities, while ensuring that the signal is not decodable at external adversaries. In contrast, the design principle for privacy protection is to guarantee the communication quality towards a legitimate receiver for utility, while minimizing the receiver's ability to infer the data's owner. 3) *Performance metrics of measuring security and privacy are different*. When measuring privacy leakage, the widely studied approaches include differential privacy, maximal leakage [11] [12], anonymity entropy, detection error rate (DER) [13], among others.

Zhongxiang Wei and Ping Wang are with the College of Electronic and Information Engineering, Tongji University, Shanghai, China. Email: z_wei@tongji.edu.cn, and pwang@mail.tongji.edu.cn.

Christos Masouros is with the Department of Electronic and Electrical Engineering at the University College London, London, UK. Email: c.masouros@ucl.ac.uk.

Xu Zhu is with the School of Electronic and Information Engineering, Harbin Institute of Technology, Shenzhen, China. Email: xuzhu@stu.hit.edu.cn.

Jingjing Wang is with Department of Electronic Engineering, Beihang University, Peking, China. Email: drwangjj@buaa.edu.cn.

Athina P. Petropulu is with the Department of Electrical and Computer Engineering, Rutgers University, NJ, USA. Email: athinap@rutgers.edu.

Corresponding authors: Ping Wang and Xu Zhu.

A. Related Work

As in this paper we focus on privacy protection, we next introduce the relevant privacy literature and discuss how they relate to e-Health applications. There are two approaches for privacy protection, namely perturbing the released data, or concealing the users' identities during the communication to avoid unwanted inference. The former approach generally exploits a randomizing mechanism, e.g., a noisy channel, to perturb the data while guaranteeing a moderate level of utility to be obtainable from the disclosed data [2] [11] [12] [14]-[16]. Nevertheless, those methods inevitably reduce the data fidelity. In e-Health scenarios, the fidelity of data is critical, which makes the data perturbation mechanism less desirable [10]. In this case, anonymous communication that provides a high level of data accuracy towards a receiver while guaranteeing senders' anonymity, plays an important role in the family of privacy design.

At the upper layers of networks, a curious receiver may extract the associated user ID during the authentication and encryption process, or exploit the characteristics of data traffic to trace the data sender. Accordingly, the anonymity-preserving techniques that reside at the upper layers can be classified into anonymous authentication, anonymous encryption and anonymous routing. The design principle of the anonymous authentication and encryption is to avoid using the users' real IDs for the authentication and encryption processes [17]-[20]. However, as the users only share their "pseudo accounts" for authentication and encryption, the AP may be unable to perform certain e-Health tasks, such as crowd monitoring and contact tracing. Another way for the AP to extract the users' IDs is to analyze the data traffic at the network layer, for example, use probabilistic packet-marking and log analysis. To counteract network layer detection, anonymous routing [21] [22] and its variants [23] attempt to conceal the user as well as the routing paths by using a number of proxy servers, where the extended routing length increases the difficulty of re-constructing the routing path. Nevertheless, the anonymous routing designs increase the end-to-end latency significantly, which may be a problem in certain e-Health applications.

While the above anonymous authentication, encryption and routing designs are employed at the upper layers of networks, the PHY also contains critical information that can be used to extract the senders' identities. For example, when an anonymously authenticated/encrypted sender transmits a signal to the AP, the received signal is always coupled with the sender's unique propagation channel. Hence, the recipient can analyze the signalling patterns of the received signal to unmask the data sender [10]. To this end, the work in [24] was the first to investigate sender detection (SD) and corresponding countermeasures at the PHY layer, where the detector exploits the characteristics of the received signal for unmasking the sender. Then, anonymous precoders were designed to scramble the receiver's detection while guaranteeing a reasonable signal-to-noise-ratio (SNR) performance for communications. In particular, the PHY anonymous techniques allow users to share their IDs with the local AP for monitoring and contact tracing, while counteracting the effect of the sender's unique propagation environment. By manipulating the transmitted signalling pattern, the received signal by the AP has no information related to the real sender's propagation channel. As a result, a curious AP can only know all the users' IDs in the vicinity for monitoring and contact tracing, but cannot find a way to associate the received signal to the real sender's ID. Indeed, the detector in [24] is built on the empirical assumption that a re-constructed signal (as will be detailed later) always has the smallest Euclidean distance to the actual received signal. As such, the optimality regarding the SD performance in [24] is not clear and may not be guaranteed. Especially in a practical scenario in which the users are equipped with different numbers of antennas, the DER of the SD design may approach 1, implying that the SD design in [24] fails to identify the real sender. In that case, regarding the anonymous precoders of [24], although they scramble the receiver's detection at low/moderate transmit-SNR regions, they do not prevent the AP from achieving a low DER given a high SNR. Thus, in the case of users having different numbers of antennas, the AP can correctly reveal the identity of the real sender, and the anonymous precoders fail to provide a high level of anonymity at high transmit-SNR regions.

B. Our Contributions

In this paper, we present a first attempt to exploit PHY SD and anonymous precoding designs for a heterogeneous antenna configuration. Our contributions are summarized as follows.

1) Focusing on a practical scenario where the users are equipped with different numbers of antennas, we first investigate the PHY SD design at the edge receiver. We propose a so-called statistical attribute (SA) based SD, which exhibits a much lower DER over the detector of [24] at all SNR regions, especially when the real sender is equipped with a small number of transmit-antennas. Interestingly, it is found that the SA detector reduces to the detector of [24], when the number of antennas of the real sender is no smaller than that of other users.
2) To counteract the enhanced detection ability at the receiver side, we first formulate the mathematical conditions of the PHY anonymity for the precoder design. Considering the homogeneous antenna (HA) and heterogeneous antennas (HeA) configurations, the conditions of the PHY anonymity are always achieved by manipulating the transmitted signalling pattern. Explicitly, the conditions help mask the real sender's channel characteristics, so that the users appear as equally likely senders from the perspective of the receiver.
3) Accordingly, anonymous precoders are proposed for the HA and HeA configurations, respectively. With their dedicated aliases selection algorithms, the proposed anonymous precoders adaptively construct a maximum number of users as equally probable senders to inhibit the receiver's SD. Hence, a higher level of anonymity is obtained than the benchmark anonymous precoder [24] without violating the subscribed receive-quality requirements. Importantly, the edge receiver is unable

to identify the real sender even at high transmit-SNR regions.

C. Paper Organization and Notations

Starting from introducing the system model and performance metrics of anonymity in Section-II, the SD strategy is first discussed in Section III. Then, anonymous precoding designs are proposed in Section IV. Simulation results are demonstrated in Section V, and a conclusion is given in the final section.

Matrices and vectors are represented by boldface capital and lower case letters, respectively. $|\cdot|$ denotes the absolute value of a complex number or the cardinality of a set. $||\cdot||$ denotes the Euclidean norm. $(\cdot)^T$, $(\cdot)^H$, Tr$(\cdot)$ and Rank$(\cdot)$ denote the transpose, Hermitian transpose, trace and Rank of a matrix. $\boldsymbol{A} \succeq 0$ means $\boldsymbol{A}$ is a positive semi-definite matrix. $\boldsymbol{I}_n$ means an n-by-n identity matrix. $\mathcal{N}\{\cdot\}$ denotes Gaussian distribution and $\mathcal{CN}\{\cdot\}$ denotes complex Gaussian distribution. $\mathbb{E}(\cdot)$ and $\mathbb{V}(\cdot)$ denote the expectation and variance of a random variable.

II. System Model and Performance Metrics of Anonymity

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

A. System Model

As depicted in Fig. 1, we consider an uplink multiuser multiple-input and multiple-output (MIMO) transmission, consisting of K users and an edge AP. Active users can expose their IDs with the local AP for e-Health monitoring and contact tracing, as well as for communication authentication, resource scheduling, and encryption. Time-division-multiple-access based communication access control can be performed among the users without notifying the AP, in either a contested or non-contested manner [24]. Hence, by applying the anonymous precoders as will be introduced in Section IV, though the edge AP can have knowledge of all the users' IDs in its cell, the AP cannot correctly relate the received data to a specific user ID. As a result, sender anonymity can still be guaranteed. For some statistics-based applications of e-Health, such as an edge AP collecting health related data aimed for statistical monitoring, modelling, diagnosis, recording or high-level detection of anomalies, both ID and data can be made anonymous. The active users can also apply the existing anonymous authentication/encryption to generate pseudo accounts for authentication, resource scheduling, encryption, etc [18] [19] [20]. In this case, the PHY anonymous technique can be seen an enhanced protection layer for the existing anonymous authentication and encryption designs, providing a "from-top-to-bottom" anonymity protection for users at all layers of networks[1].

[1]Such an anonymous demand can be found in many communication scenarios. For example, when reporting traffic and roadway information in vehicle-to-infrastructure communications, a vehicle makes his ID anonymous towards a road-side AP to avoid privacy leakage [19].

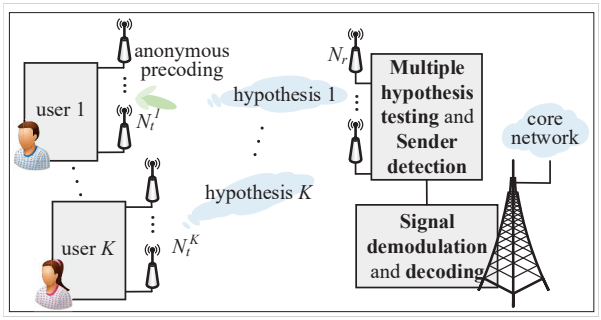

Fig. 1. Illustration of system model, where K users transmit signal to the receiver under anonymity requirement.

It is important to note that the philosophy of the anonymous precoder is to manipulate the transmitted signalling pattern for eliminating the characteristics of the sender's propagation channel, while providing high communication performance for the accuracy of the disclosed data. Since it does not require help from external proxies, nor does it rely on complex networking or dedicated data re-routing protocols, the anonymous precoding technique is readily compatible for the existing upper layer communication protocols and architectures. Channel estimation is performed during a training phase, as that in generic MIMO systems. Explicitly, by analyzing the pilot from the active users, the AP then feeds the channel state information (CSI) back to the users for use of precoding design.

Denote $\mathbb{K}$ as the user set that consists of all the potential users ($|\mathbb{K}| = K$). Denote N_t^k as the number of transmit-antennas of the k-th user, $\forall k \in \mathbb{K}$, N_r as the number of receive-antennas of the AP, where we have $N_r > N_t^k$ in a typical uplink scenario. Define $\boldsymbol{H}_k \in \mathbb{C}^{N_r \times N_t^k}$ as the MIMO channel between the user k and AP, $\boldsymbol{F}_k$ as the precoding matrix, and $\boldsymbol{s}_k$ as the symbol to be transmitted by the k-th user, $\forall k \in K$. Without loss of generality, assume that the k-th user is the real sender. The received signal at the AP is written as

$$\boldsymbol{r} = \boldsymbol{H}_k \boldsymbol{F}_k \boldsymbol{s}_k + \boldsymbol{z}, \tag{1}$$

where $\boldsymbol{z} \sim \mathcal{CN}(\boldsymbol{0}, \sigma^2 \boldsymbol{I}_{N_r})$ denotes the circularly symmetric complex Gaussian (CSCG) noise.

At the PHY layer, the AP exploits the received signal and the inherent characteristics of the wireless channels to disclose the identity of the sender [24]. The SD can be formulated as a multiple hypotheses testing (MHT) problem

$$\boldsymbol{R} = \begin{cases} \mathcal{H}_0: & \boldsymbol{z}, \\ \mathcal{H}_1: & \boldsymbol{H}_1 \boldsymbol{F}_1 \boldsymbol{s}_1 + \boldsymbol{z}, \\ \vdots & \\ \mathcal{H}_K: & \boldsymbol{H}_K \boldsymbol{F}_K \boldsymbol{s}_K + \boldsymbol{z}, \end{cases} \tag{2}$$

where the hypothesis $\mathcal{H}_0$ means that there was no signal transmission and only noise appears at the AP, while hypothesis $\mathcal{H}_k$ means there is a signal coming from the k-th user. The aim of the SD (denote as $\mathcal{D}$) at the AP is to correctly identify the real

sender. On the other hand, a favorable anonymous precoder at the user side is to manipulate the transmitted signalling for hiding the sender's characteristics and also guarantee a reasonable reception quality for the disclosed data.

B. Performance Metrics of Anonymity

In this work, anonymity entropy and DER are used as anonymous metrics [25] [26]. In fact, since the concept of the entropy exactly measures the uncertainty and randomness of a system, a larger value of entropy contains more possibilities. It essentially denotes that the AP node is not able to reveal which user is the real sender. Provided that the user k is the real sender, the AP may leverage a specific SD strategy and guess that each user i has a probability $p(\mathcal{H}_i;\mathcal{H}_k)$ of being the sender. Then the anonymity entropy [25] [26] is calculated as

$$\mathcal{A} = -\sum_{i\in\mathbb{K}} p(\mathcal{H}_i;\mathcal{H}_k)\log_2 p(\mathcal{H}_i;\mathcal{H}_k), \tag{3}$$

where the maximum anonymity entropy $\mathcal{A}_{\max} = \log_2(K)$ is achieved when $p(\mathcal{H}_i;\mathcal{H}_k) = \frac{1}{K}, \forall i \in \mathbb{K}$, i.e., all the users in $\mathbb{K}$ being equally likely senders. On the other hand, DER is another intuitive metric for measuring anonymity. Denote $N_{\rm mis}$ as the numbers of the blocks that their origin is mis-detected, and $N_{\rm tot}$ as the total number of received blocks. Then DER is calculated as DER = $\frac{N_{\rm mis}}{N_{\rm tot}}$.

In the following, we will first introduce the SD design for the AP. Subsequently, the countermeasures at the user sides are proposed for HA and HeA configurations, followed by their complexity analysis.

III. Sender Detection Strategy

To handle the MHT problem in (2), the presence of the signal is first detected, and the AP turns to detect the origin of the signal only when $\mathcal{H}_0$ is decided as a false hypothesis. The detection of $\mathcal{H}_0$ leads to the classic energy detection [27] [28] [29], where the test statistic is compared against a threshold β, i.e.,

$$\mathcal{X}(\boldsymbol{r}) = \frac{||\boldsymbol{r}||^2}{N_r} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1\sim\mathcal{H}_K}{\gtrless}} \beta, \tag{4}$$

where the value of β can be set based on the Neyman-Pearson criterion. Since it is not the focus of this paper, we refer readers to [30] for details. Once $\mathcal{H}_0$ is determined as a false hypothesis, the AP turns to detect the correct event from the hypotheses $\mathcal{H}_1$ to $\mathcal{H}_K$.

A. Least Euclidean Distance based SD

Let us briefly describe the work of [24], where a least-Euclidean distance based detector (referred to as L-ED hereafter) was proposed. As shown in (1), the characteristic of the received signal is closely coupled to the channel of the real sender. Suppose that the AP utilizes the correct propagation channel to obtain the maximum likelihood estimation (MLE) version of the transmitted signal. Then, the re-constructed signal equals

$$\hat{\boldsymbol{r}}_k = \boldsymbol{H}_k\boldsymbol{H}_k^{\dagger}\boldsymbol{r} = \boldsymbol{H}_k\boldsymbol{F}_k\boldsymbol{s}_k + \boldsymbol{H}_k\boldsymbol{H}_k^{\dagger}\boldsymbol{z}, \tag{5}$$

where $\boldsymbol{H}_k^{\dagger} = (\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H$. Then, the Euclidean distance between the re-constructed signal $\hat{\boldsymbol{r}}_k$ and the actual signal $\boldsymbol{r}$ is calculated as

$$d_k = ||\boldsymbol{r} - \hat{\boldsymbol{r}}_k||^2 = ||(\boldsymbol{H}_k\boldsymbol{H}_k^{\dagger} - \boldsymbol{I}_{N_r})\boldsymbol{z}||^2. \tag{6}$$

Note that $\boldsymbol{H}_k\boldsymbol{H}_k^{\dagger} - \boldsymbol{I}_r = \boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H - \boldsymbol{I}_r \neq \boldsymbol{0}$ when $N_r > N_t^k$. While if the AP uses the i-th user's channel, $i \neq k$ and $i \in \mathbb{K}$, to re-construct the transmitted signal, i.e., $\hat{\boldsymbol{r}}_i = \boldsymbol{H}_i\boldsymbol{H}_i^{\dagger}\boldsymbol{r}$, the Euclidean distance between the actual signal $\boldsymbol{r}$ and $\hat{\boldsymbol{r}}_i$ is calculated as

$$d_i = ||\boldsymbol{r} - \hat{\boldsymbol{r}}_i||^2 = ||(\boldsymbol{H}_i\boldsymbol{H}_i^{\dagger} - \boldsymbol{I}_{N_r})\boldsymbol{H}_k\boldsymbol{F}\boldsymbol{s} + (\boldsymbol{H}_i\boldsymbol{H}_i^{\dagger} - \boldsymbol{I}_{N_r})\boldsymbol{z}||^2. \tag{7}$$

The Euclidean distance in (6) only contains a colored-noise term, while the Euclidean distance in (7) is also related to the transmitted signal. On comparing the Euclidean distance results in (6) and (7), there is high probability that the value of (7) is larger than that of (6). Hence, the L-ED detector in [24] lets the AP re-construct a series of signals based on different users' channels, and calculates their Euclidean distances to the actual received signal. Finally, the AP considers the one having the smallest Euclidean distance as the real sender, written as

$$\mathcal{D}_{\rm L-ED} = \min_{k\in\mathbb{K}}\{||\boldsymbol{r} - \boldsymbol{H}_1\boldsymbol{H}_1^{\dagger}\boldsymbol{r}||^2, ..., ||\boldsymbol{r} - \boldsymbol{H}_K\boldsymbol{H}_K^{\dagger}\boldsymbol{r}||^2\}. \tag{8}$$

In fact, the expected value in (6) depends on the instantaneous channel realization and noise, which in some cases may have a large value than that of (7). More importantly, the L-ED detector relies on the assumption that all the users have HA configuration. However, when the users are equipped with different numbers of antennas, the DER performance of the L-ED detector significantly deteriorates. Especially, when the real sender is equipped with a small number of transmit-antennas, its DER approaches 1 in the transmit-SNR regions below 5 dB, as shown in Fig. 2.

B. The Statistical Attribute-based SD

Revisiting (6), the noise-related term is coupled with the real sender's channel $\boldsymbol{H}_k$. For simplicity, define $\boldsymbol{\Psi}_k = \boldsymbol{H}_k\boldsymbol{H}_k^{\dagger} - \boldsymbol{I}_{N_r}$. We now introduce Proposition 1 to show the statistical attributes of the result in (6).

Proposition 1: If the AP uses the correct sender's propagation channel for testing, the expectation and variance of the test result $||\boldsymbol{\Psi}_k\boldsymbol{z}||^2$ are calculated as

$$\mathbb{E}\{||\boldsymbol{\Psi}_k\boldsymbol{z}||^2\} = \sigma^2{\rm tr}\big(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\big), \tag{9}$$

and

$$\mathbb{V}\{||\boldsymbol{\Psi}_k\boldsymbol{z}||^2\} = \sigma^4{\rm tr}\big(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\big). \tag{10}$$

■

This article has been accepted for publication in IEEE Journal on Selected Areas in Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2022.3211556

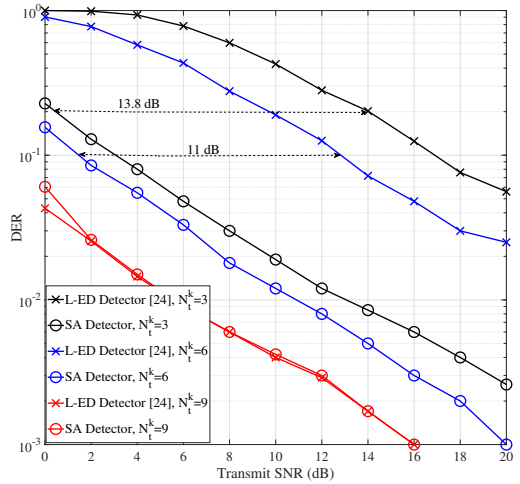

Fig. 2. DER performance of the L-ED [24] and the proposed SA detectors. $N_r = 10$. The real sender user k is equipped with $N_t^k = 3, 6, 9$ transmit-antennas, while other users are equipped with different numbers of transmit antenna ranging from 1 to 9. The diversity-based MMSE is used as precoder.

Proof: Please refer to APPENDIX A. □

Proposition 1 reveals the expectation and variance of the Euclidean distance if the AP selects the correct channel for testing, while it may still be difficult to obtain an accurate probability density function (pdf) of the test result. Though the pdf of such a quadratic form in (6) has been analyzed by [31] [32], the asymptotic expression which often involves complex integration hinders its application in our SD design. Instead, leveraging the central limit theory, we further introduce Proposition 2 to obtain a tackable but tight pdf expression of the test result in (6).

Proposition 2: In practice, the multi-user access and the AP's SD are operated at the block level. Assume that a block consists of M symbols. The block-level received signal is written as $[\boldsymbol{r}^{(1)}, ..., \boldsymbol{r}^{(M)}] = \boldsymbol{H}_k \boldsymbol{F}[\boldsymbol{s}^{(1)}, ..., \boldsymbol{s}^{(M)}] + [\boldsymbol{z}^{(1)}, ..., \boldsymbol{z}^{(M)}]$, where $[\boldsymbol{s}^{(1)}, ..., \boldsymbol{s}^{(M)}] \in \mathbb{C}^{N_r \times M}$ and $[\boldsymbol{z}^{(1)}, ..., \boldsymbol{z}^{(M)}] \in \mathbb{C}^{N_r \times M}$, with the superscripts denoting the symbol index. Hence, the term $||\boldsymbol{\Psi}_k \boldsymbol{z}||^2$ can be equivalently regarded as a combination of $N_r M$ test samples, approximately following Gaussian distribution based on central limit theory. ■

According to Propositions 1 and 2, we know that when $\mathcal{H}_k$ is true, the test result of (6) follows Gaussian distribution with known values of expectation and variance, written as

$$d_k \sim \mathcal{N}\big(M\sigma^2 \mathrm{tr}(\boldsymbol{\Psi}_k^H \boldsymbol{\Psi}_k), M\sigma^4 \mathrm{tr}(\boldsymbol{\Psi}_k^H \boldsymbol{\Psi}_k \boldsymbol{\Psi}_k^H \boldsymbol{\Psi}_k)\big). \quad (11)$$

Now, we are able to write the pdf expression of the test result in (12), but the impact of antenna configuration is still not clear. Hence, we introduce Proposition 3 to further simplify the pdf expression above.

Proposition 3: If the AP selects the real sender for testing, the expectation and variance in (12) are independent from the sender's channel realization $\boldsymbol{H}_k$, but are jointly decided by the antenna configurations of the sender and AP, given as $\mathcal{N}\big(M\sigma^2(N_r - N_t^k), M\sigma^4(N_r - N_t^k)\big)$. ■

Proof: Please refer to APPENDIX B. □

Now, leveraging the concept of generalized likelihood ratio test (GLRT), the SA detector is formulated as

$$\begin{aligned} P(d_1; \mathcal{H}_1) = & \\ & \frac{1}{\sigma^2\sqrt{2\pi M(N_r - N_t^1)}} \exp\Big(-\frac{\big(d_1 - M\sigma^2(N_r - N_t^1)\big)^2}{2M\sigma^4(N_r - N_t^1)}\Big), \\ & \vdots \\ P(d_K; \mathcal{H}_K) = & \\ & \frac{1}{\sigma^2\sqrt{2\pi M(N_r - N_t^K)}} \exp\Big(-\frac{\big(d_K - M\sigma^2(N_r - N_t^K)\big)^2}{2M\sigma^4(N_r - N_t^K)}\Big), \end{aligned} \quad (13)$$

where the hypothesis with the largest likelihood function value will be clarified as the real sender, as summarized in Algorithm 1.

Algorithm 1 SA Detection Design

Input: CSI, and transmit/receive-antenna configurations.
1: Re-construct signals with different CSI values, i.e., $\hat{\boldsymbol{r}}_i = \boldsymbol{H}_k \boldsymbol{H}_k^{\dagger} \boldsymbol{r}$, $\forall i \in \mathbb{K}$.
2: Calculate the Euclidean distance between the actual received signal $\boldsymbol{r}$ and different reconstructed signals $\hat{\boldsymbol{r}}_i$, i.e., $d_i = ||\boldsymbol{r} - \hat{\boldsymbol{r}}_i||^2$, $\forall i \in \mathbb{K}$.
3: Substitute d_i, $\forall i \in \mathbb{K}$, into the likelihood functions in (13), and calculate the corresponding likelihood function values.
4: Claim the user associated with the largest likelihood function value as the real sender.
Output: Testing result of the MHT problem.

The enhanced detection ability of SA detector is demonstrated in Fig. 2, where its DER performance is significantly improved over the L-ED detector. Especially when the real sender is equipped with a small or moderate number of antennas, i.e., $N_t^k = 3$ and 6, the proposed SA detector achieves more than 11 dB transmit-SNR gain over the L-ED detector for achieving the same DER performance. It is because when the AP selects the i-th user that has more antennas than the real sender for testing, its Euclidean distance has a high probability of being smaller than that of the real sender k, as suggested by Proposition 3. Hence, simply determining the user having the smallest Euclidean distance by the L-ED is not always accurate.

On the other hand, in the cases that no user has more antennas than the real sender (including the case that all the users have the same number of antennas), the SA detector interestingly shows the same DER performance to the L-ED detector (the red lines in Fig. 2). It is because when no user has more antennas than the real sender, i.e., $N_t^i \leq N_t^k = 9$ in the example above, the statistical distribution of the test result of the real sender is given as $\mathcal{N}(M\sigma^2(N_r - N_t^k), M\sigma^4(N_r - N_t^k))$, which has the smallest expectation and variance due to the small value of $N_r - N_t^k$. As a result, the user leading to the smallest Euclidean distance generally returns the largest likelihood function value, and the SA detector reduces to the L-ED detector.

Finally, we calculate the complexities of the proposed SA detector. Its complexity is dominated by the pseudo-inverse

$$P(d_k;\mathcal{H}_k)=\frac{1}{\sigma^2\sqrt{2\pi M\mathrm{tr}\big(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\big)}}\exp\Big(-\frac{\big(d_k-M\sigma^2\mathrm{tr}(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k)\big)^2}{2M\sigma^4\mathrm{tr}\big(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\big)}\Big), \tag{12}$$

operation of MIMO channel [33]. The overall complexity is approximated by

$$C_{\mathrm{SA}}=\sum_{k\in\mathbb{K}}(16N_r^2N_t^k+24N_r(N_t^k)^2+29(N_t^k)^3+8N_rN_t^k+8N_r). \tag{14}$$

As can be seen, the complexity increases linearly with the number of users K, and is quadratic with respect to (w.r.t) the number of receive-antennas N_r. Though the complexity is sensitive to the number of transmit-antennas, it still remains at a low level as the users generally are not equipped with massive antennas at uplink.

IV. Anonymous Precoding Design

To counteract the AP's enhanced detection ability, in this section, we devise anonymous precoding techniques for the users. The aim is to mask the sender's PHY characteristics while guaranteeing a reasonable reception performance at the AP for data accuracy. In [24], we have proposed an so-called constructive-interference anonymous (CIA) precoder to maximize the receive-SNR for communication signal subject to an anonymous constraint to scramble the AP's DER performance. Nevertheless, it may not lead to an optimal entropy performance in particular at high transmit-SNR regions, where the AP is able to correctly reveal the real sender with a probability as high as 60%. In this paper, we instead aim to leverage the anonymity entropy as our design objective, and attempt to provide a high level of anonymity at all SNRs regions.

The anonymous precoder needs to strike a balance between the anonymity and communication quality. This is because if the identity of the sender is concealed, the AP fails to know the exact channel that the signal comes from. As a result, the AP needs to leverage a channel-independent equalizer for signal combining, and without loss of generality, we let the AP apply an equal-gain combiner. For diversity MIMO design, since N_t^k transmit-antennas send the same symbols, the precoding matrix $\boldsymbol{F}_k$ can be equivalently reduced to a vector $\boldsymbol{f}_k$, while the symbol vector $\boldsymbol{s}_k$ reduces to a scalar s_k. Then, the post-combiner signal is given as $\mathbf{1}^T\boldsymbol{r}$, where $\mathbf{1}\in\mathbb{C}^{1\times N_r}$ denotes a vector having all-1 entries. Based on (1), the SNR of the post-combined signal is calculated as

$$\Gamma_k=\frac{||\mathbf{1}^T\boldsymbol{H}_k\boldsymbol{f}_ks_k||^2}{||\boldsymbol{z}||^2}. \tag{15}$$

Aiming at maximizing the system anonymity entropy subject to a subscribed receive-quality requirement, the diversity MIMO based anonymous precoder is formulated as

$$\begin{aligned}&P1:\max_{\boldsymbol{f}_k}\mathbb{E}\{-\sum_{i=1}^{K}p(\mathcal{H}_i,\mathcal{H}_k)\log_2p(\mathcal{H}_i,\mathcal{H}_k)\},\\&\text{s.t. (C1)}:\frac{||\mathbf{1}^T\boldsymbol{H}_k\boldsymbol{f}_ks_k||^2}{||\boldsymbol{z}||^2}\geq\bar{\Gamma}_k,\\&\quad\text{(C2)}:||\boldsymbol{f}_ks_k||^2\leq p_{\max},\end{aligned} \tag{16}$$

where (C1) guarantees the subscribed receive-quality requirement $\bar{\Gamma}_k$, while (C2) confines the power budget $p_{\max}$. Evidently, the difficulty of solving P1 lies in relating the value of anonymity entropy in the objective with the precoding variable $\boldsymbol{f}_k$. From the perspective of anonymity entropy, one needs to make each probability $p(\mathcal{H}_i,\mathcal{H}_k)$, $\forall i\in\mathbb{K}$, as close as possible. It is equivalent to making the likelihood functions in (13) indistinguishable from the perspective of the AP. In the following, we present anonymous precoder designs for HA and HeA configurations.

A. Anonymous Precoder Design in HA Configuration

Revisiting (13), the likelihood functions in (13) are only decided by the value of d_i, $\forall i\in\mathbb{K}$, in the HA configuration. Hence, the i-th user is treated as a likely sender if and only if $\mathbb{E}\{d_i\}=\mathbb{E}\{d_k\}$ holds, which suggests that

$$\mathbb{E}\{(\boldsymbol{H_i}\boldsymbol{H_i}^\dagger-\boldsymbol{I}_{N_r})\boldsymbol{H_k}\boldsymbol{f}_ks_k+(\boldsymbol{H_i}\boldsymbol{H_i}^\dagger-\boldsymbol{H_k}\boldsymbol{H_k}^\dagger)\boldsymbol{z}\}=\mathbf{0}, \tag{17}$$

which can be arranged to $\mathbb{E}\{(\boldsymbol{H_i}\boldsymbol{H_i}^\dagger-\boldsymbol{I}_{N_r})\boldsymbol{H_k}\boldsymbol{f}_ks_k\}+\mathbb{E}\{(\boldsymbol{H_i}\boldsymbol{H_i}^\dagger-\boldsymbol{H_k}\boldsymbol{H_k}^\dagger)\boldsymbol{n}\}=\mathbf{0}$. Since we have $\mathbb{E}\{(\boldsymbol{H_i}\boldsymbol{H_i}^\dagger-\boldsymbol{H_k}\boldsymbol{H_k}^\dagger)\boldsymbol{z}\}=\mathbf{0}$, (17) can be reduced to

$$(\boldsymbol{H_i}\boldsymbol{H_i}^\dagger-\boldsymbol{I}_{N_r})\boldsymbol{H_k}\boldsymbol{f}_ks_k=\mathbf{0}, \tag{18}$$

which denotes that the i-th user becomes an alias to scramble the AP's SD. (18) can be also explained based on Proposition 3. That is, when (18) holds, the Euclidean distances calculated based on the k-th and i-th users' channels both follow a Gaussian distribution with identical expectation and variance, and thus it is difficult for the AP to distinguish between those two users. Essentially, (18) inherently links the precoder $\boldsymbol{f}_k$ to the value of the anonymity entropy, as summarized in Lemma 1.

Lemma 1: Assume that there are N users in a set $\mathbb{N}$ ($|\mathbb{N}|=N$ and $\mathbb{N}\subseteq\{\mathbb{K}/k\}$) and any user in the set is able to make (18) hold. Then the value of the anonymity entropy is proportional to $\log(|\mathbb{N}|+1)$. ■

Proof: A set of equalities $(\boldsymbol{H}_i\boldsymbol{H}_i^\dagger-\boldsymbol{I}_{N_r})\boldsymbol{H}_k\boldsymbol{f}_ks_k=\mathbf{0}$ implies that $\mathbb{E}\{d_i\}=\mathbb{E}\{d_k\}$, $\forall i\in\mathbb{N}$, and thus the likelihood function values for the different users get close. As a result, the users in $\mathbb{N}$ become indistinguishable and will be considered as likely senders from the perspective of the AP, i.e., $\mathbb{E}\{p(\mathcal{H}_i,\mathcal{H}_k)\}=\mathbb{E}\{p(\mathcal{H}_k,\mathcal{H}_k)\}\simeq\frac{1}{|\mathbb{N}|+1}$, $\forall i\in\mathbb{N}$, where the system anonymity entropy is strictly proportional to

$$\sum_{\mathbb{N}\cup k}\frac{1}{|\mathbb{N}|+1}\log_2(|\mathbb{N}|+1)=\log(|\mathbb{N}|+1). \tag{19}$$

□

Under the provision of Lemma 1, P1 can re-formulated as

$$\begin{aligned} &P2:\max_{\boldsymbol{f}_k}\log(|\mathbb{N}|+1),\\ &\text{s.t. (C1)}:\frac{||\mathbf{1}^T\boldsymbol{H}_k\boldsymbol{f}_k s_k||^2}{||\boldsymbol{z}||^2}\geq\bar{\Gamma}_k,\ \text{(C2)}:||\boldsymbol{f}_k s_k||^2\leq p_{\max},\\ &\quad\text{(C3)}:(\boldsymbol{H}_i\boldsymbol{H}_i^{\dagger}-\boldsymbol{I}_{N_r})\boldsymbol{H}_k\boldsymbol{f}_k s_k=\mathbf{0},\forall i\in\mathbb{N}. \end{aligned} \tag{20}$$

where $\mathbb{N}\subseteq\mathbb{K}'=\{\mathbb{K}/k\}$. That is, maximizing anonymity entropy is equivalent to maximizing the cardinality of the alias sender set $\mathbb{N}$ in (C3). The optimization P2 belongs the class of non-convex second-order cone programming (SOCP). Defining $\boldsymbol{W}_k=\boldsymbol{f}_k\boldsymbol{f}_k^H$ and $\boldsymbol{h}_k=\mathbf{1}^T\boldsymbol{H}_k$, P2 can be further written as

$$\begin{aligned} &P3:\max_{\boldsymbol{W}_k}\log(|\mathbb{N}|+1),\\ &\text{s.t. (C1)}:\mathrm{tr}(\boldsymbol{h}_k\boldsymbol{W}_k\boldsymbol{h}_k^H)\geq\bar{\Gamma}_k N_r\sigma^2,\ \text{(C2)}:\mathrm{tr}(\boldsymbol{W}_k)\leq p_{\max},\\ &\quad\text{(C3)}:\mathrm{tr}((\boldsymbol{H_i}\boldsymbol{H_i}^{\dagger}-\boldsymbol{I}_{N_r})\cdot\\ &\qquad\qquad\boldsymbol{H_k}\boldsymbol{W}_k\boldsymbol{H_k}^H(\boldsymbol{H_i}\boldsymbol{H_i}^{\dagger}-\boldsymbol{I}_{N_r})^H)=0,\forall i\in\mathbb{N},\\ &\quad\text{(C4)}:\boldsymbol{W}_k\succeq\mathbf{0},\ \text{(C5)}:\mathrm{Rank}(\boldsymbol{W}_k)=1. \end{aligned} \tag{21}$$

P3 is a standard semi-definite-programming (SDP) problem after dropping the rank constraint in (C5), and can be handled by commercial solvers. In particular, if the obtained optimal solution $\boldsymbol{W}_k$ is of rank 1, a tight semi-definite relaxation (SDR) is guaranteed and $\boldsymbol{f}_k$ can be simply obtained from the principal eigen-vector of $\boldsymbol{W}_k$, where we have the following Proposition 4.

Proposition 4: Under the condition of independently distributed MIMO channels, the optimal solution of P3 satisfies $\mathrm{Rank}(\boldsymbol{W}_k^*)=1$, with probability one. ■

Proof: Please refer to APPENDIX C. □

Note that the tightness of the SDR has been proven by Propositions 4, and the anonymity and subscribed receive-quality requirement can always be guaranteed by decomposing the matrix $\boldsymbol{W}_k^*=\boldsymbol{f}_k^*\boldsymbol{f}_k^{*H}$. However, the matrix decomposition procedure may cause phase ambiguity towards the received signal, thus impairing the demodulation performance at the AP side. In particular, since the AP may not be able to declare a correct channel for designing its equalizer, the conventional receiver phase equalization is inapplicable in anonymous communications. Since the post-combined signal $\boldsymbol{h}_k\boldsymbol{f}_k^*s_k$ should have the same phase to that of the desired symbol s_k, a transmit-side equalization can be designed as $\boldsymbol{f}_k^{\dagger}=\boldsymbol{f}_k^*e^{-j\phi_k}$, where ϕ_k is the angle of the complex scalar $\boldsymbol{h}_k\boldsymbol{f}_k^*$. It is easy to verify that aided by the transmit-side equalization, the received signal $\boldsymbol{h}_k\boldsymbol{f}_k^{\dagger}s_k=\boldsymbol{h}_k\boldsymbol{f}_k^*e^{-j\phi_k}s_k$ eliminates the phase ambiguity without violating the receive-quality requirement and anonymity constraint.

Evidently, there is a fundamental tradeoff between the anonymity and communication performance. Accommodating more aliases in (C3) leads to a higher level of anonymity entropy and DER. Due to the power budget constraint, however, introducing an arbitrary number of aliases in (C3) may violate the receive-quality requirement in (C1), which requires a careful tradeoff between the anonymity entropy and receive-performance. In fact, if a candidate alias i has a high level of channel correlation to the real sender k, (C3) can hold easily and the precoder also has a high level of design degrees-of-freedom (DoF)s. This indicates that the preference of aliases selection can be made based on the channel correlation to the real sender's channel, as briefly discussed in Algorithm 2.

Algorithm 2 Alias Selection Algorithm for HA Precoder

Input: CSI of the users in $\mathbb{K}$.
1: Initialize the candidate set $\mathbb{K}'=\{\mathbb{K}/k\}$.
2: Measure the channel correlation between a candidate alias and the real sender, i.e., $||\boldsymbol{H}_i-\boldsymbol{H}_k||_{\mathrm{F}}$, $\forall i\in\mathbb{K}'$.
3: Rearrange the candidate aliases in a descent order from perspective of the channel correlation.
Output: The candidate alias set $\mathbb{K}'$.

Now, we are able to devise the HA precoder. Based on the subscribed receive-quality requirement as well as the instantaneous channel realization, we target at maximizing system anonymity entropy, where the aliases are adaptively constructed by examining the feasibility of P3. Afterwards, eigenvalue decomposition and transmit-side equalization are applied to obtain the optimal anonymous precoder. The whole algorithm is briefly summarized in Algorithm 3.

Algorithm 3 The HA Precoder Algorithm

Input: CSI, power budget $p_{\max}$, SNR threshold requirement $\bar{\Gamma}_k$.
1: Call Algorithm 2 to arrange the candidate aliases set $\mathbb{K}'$.
2: Initialize search region for the alias selection, i.e., left bound $b_l=1$, right bound $b_r=|\mathbb{K}'|$ and middle point $b_m=\lfloor\frac{1+|\mathbb{K}'|}{2}\rfloor$.
3: **while** $|b_r-b_l|>1$ **do**
4: Select the first b_m users from the set $\mathbb{K}'$ as aliases, and examine the feasibility of P3.
5: **if** P3 has feasible solution **then**
6: $b_l=b_m$
7: **else**
8: $b_r=b_m$
9: **end if**
10: Update $b_m=\lfloor\frac{b_l+b_r}{2}\rfloor$.
11: **end while**
12: Do eigenvalue decomposition of $\boldsymbol{W}_k^*$ and obtain optimal $\boldsymbol{f}_k^*$, and do transmit-side equalization $\boldsymbol{f}_k^{\dagger}=\boldsymbol{f}_k^*e^{-j\phi_k}$.
Output: Optimal anonymous precoding design $\boldsymbol{f}_k^{\dagger}$.

B. Anonymous Precoder Design in HeA Configuration

In this subsection, we further consider a challenging case for the HeA configuration, where only ensuring the equality in (18) may not be able to guarantee sender anonymity. Revisiting (13), one needs to design precoder such that under event $\mathcal{H}_k$, the value of the likelihood function $P(d_i;\mathcal{H}_i)$ approaches that of $P(d_k;\mathcal{H}_k)$, and the following equality should be satisfied

$$\begin{aligned} &-\ln\big(\sigma^2\sqrt{2\pi M(N_r-N_t^i)}\big)-\frac{(d_i-M\sigma^2(N_r-N_t^i))^2}{2M\sigma^4(N_r-N_t^i)}=\\ &-\ln\big(\sigma^2\sqrt{2\pi M(N_r-N_t^k)}\big)-\frac{(d_k-M\sigma^2(N_r-N_t^k))^2}{2M\sigma^4(N_r-N_t^k)}, \end{aligned} \tag{22}$$

which is equivalently reduced to

$$\frac{(d_i - M\sigma^2(N_r - N_t^i))^2}{2M\sigma^4(N_r - N_t^i)} - \frac{1}{2}\big(\frac{d_k - M\sigma^2(N_r - N_t^k)}{\sqrt{M\sigma^4(N_r - N_t^k)}}\big)^2 = \frac{1}{2}\ln(\frac{N_r - N_t^k}{N_r - N_t^i}). \tag{23}$$

Since we know $d_k \sim \mathcal{N}\big(M\sigma^2(N_r - N_t^k), M\sigma^4(N_r - N_t^k)\big)$, the second term $\big(\frac{d_k - M\sigma^2(N_r - N_t^k)}{\sqrt{M\sigma^4(N_r - N_t^k)}}\big)^2$ in (23) is in fact a quadratic form of a standard Gaussian distributed variable, following Chi-square distribution with DoF factor 1. Let $\tau = \big(\frac{d_k - M\sigma^2(N_r - N_t^k)}{\sqrt{M\sigma^4(N_r - N_t^k)}}\big)^2$. For the Chi-square distributed variable τ, its expectation equals its DoF factor, i.e., $\mathbb{E}\{\tau\} = 1$. Hence, (23) is rearranged to

$$\mathbb{E}\{\frac{d_i - M\sigma^2(N_r - N_t^i))^2}{2M\sigma^4(N_r - N_t^i)}\} = \frac{1}{2} + \frac{1}{2}\ln(\frac{N_r - N_t^k}{N_r - N_t^i}), \tag{24}$$

which further yields

$$\mathbb{E}\{\big(d_i - M\sigma^2(N_r - N_t^i)\big)^2\} = M\sigma^4(N_r - N_t^i)(1 + \ln(\frac{N_r - N_t^k}{N_r - N_t^i})). \tag{25}$$

To handle (25), we first show the statistical distribution of d_i in the following Proposition 5. For the sake of clarity, let $\boldsymbol{\Psi}_i = \boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r}$ and $\boldsymbol{p} = \boldsymbol{\Psi}_i\boldsymbol{H}_k\boldsymbol{f}_k s_k$.

Proposition 5: When event $\mathcal{H}_k$ is true while the AP uses the i-th user's channel for testing, the expectation and variance of d_i are written as $\mathbb{E}\{d_i\} = M\sigma^2(N_r - N_t^i) + M\boldsymbol{p}^H\boldsymbol{p}$, and $\mathbb{V}\{d_i\} = M\sigma^4(N_r - N_t^i) + 2M\sigma^2\boldsymbol{p}^H\boldsymbol{p}$. ■

Proof: Please refer to Appendix D. □

Leveraging the results of Proposition 5, it is easy to obtain that $\mathbb{E}\{d_i - M\sigma^2(N_r - N_t^i)\} = M\boldsymbol{p}^H\boldsymbol{p}$, and $\mathbb{V}\{d_i - M\sigma^2(N_r - N_t^i)\} = \mathbb{V}\{d_i\} = M\sigma^4(N_r - N_t^i) + 2M\sigma^2\boldsymbol{p}^H\boldsymbol{p}$. Based on the fact that $(\mathbb{E}\{d_i - M\sigma^2(N_r - N_t^i)\})^2 = \mathbb{E}\{(d_i - M\sigma^2(N_r - N_t^i))^2\} - \mathbb{V}\{d_i - M\sigma^2(N_r - N_t^i)\}$, (25) can be reformulated as

$$(M\boldsymbol{p}^H\boldsymbol{p})^2 = M\sigma^4(N_r - N_t^i)(\ln(\frac{N_r - N_t^k}{N_r - N_t^i})) - 2M\sigma^2\boldsymbol{p}^H\boldsymbol{p}. \tag{26}$$

Solving the quadratic equation above w.r.t $\boldsymbol{p}^H\boldsymbol{p}$, we obtain

$$\boldsymbol{p}^H\boldsymbol{p} = \frac{-\sigma^2 + \sqrt{\sigma^4 + M\sigma^4\ln(\frac{N_r - N_t^k}{N_r - N_t^i})(N_r - N_t^i)}}{M}, \tag{27}$$

where for the sake of feasibility, one needs to ensure

$$\ln(\frac{N_r - N_t^k}{N_r - N_t^i}) \geq 0 \Rightarrow N_t^i \geq N_t^k. \tag{28}$$

Evidently, (28) suggests if the antennas number of the i-th user is no less than that of the real sender k, the i-th user can be selected as an alias under the constraint in (27). While for the users having less antennas than the real sender, it is difficult to let the expectation of their maximum likelihood functions value equal that of the real sender. As a result, the anonymous constraint can be relaxed to $\boldsymbol{p}^H\boldsymbol{p} = 0$ for the users having more antennas than the sender, which also makes these users' likelihood function value be non-zero and thus improves the system anonymity entropy. Finally, substituting $\boldsymbol{p} = \boldsymbol{\Psi}_i\boldsymbol{H}_k\boldsymbol{f}_k s_k$ into (27) yields a more general form of the anonymous constraint in the HeAC configuration as

$$||\boldsymbol{\Psi}_i\boldsymbol{H}_k\boldsymbol{f}_k s_k||^2 = \max\{0, \frac{-\sigma^2 + \sqrt{\sigma^4 + M\sigma^4\ln(\frac{N_r - N_t^k}{N_r - N_t^i})(N_r - N_t^i)}}{M}\}, \tag{29}$$

Now, we are ready to formulate the HeA precoder. Starting from P1, the value of system anonymity entropy is directly related to the numbers of aliases that satisfies (29), where now the question is how to select aliases in the HeA scenario. In this context, we first propose an alias selection algorithm, as summarized in Algorithm 4.

Algorithm 4 Alias Selection Algorithm for HeA Precoder

Input: The number of the transmit-antennas N_t^i, $\forall i \in \mathbb{K}$.
1: Initialize the set $\mathbb{K}^\dagger = \{\mathbb{K}/k\}$.
2: Rearrange the users in a descend order, from the perspective of the numbers of transmit-antennas.
Output: The candidate aliases set $\mathbb{K}^\dagger$.

Following the alias selection algorithm, we are able to formulate the anonymity-entropy oriented precoder design as

$$\begin{aligned} P4: &\max_{\boldsymbol{f}_k} \log(|\mathbb{N}| + 1), \\ \text{s.t. } &(\text{C6}): \frac{||\mathbf{1}^T\boldsymbol{H}_k\boldsymbol{f}_k s_k||^2}{||\boldsymbol{z}||^2} \geq \bar{\Gamma}_k,\ (\text{C7}): ||\boldsymbol{f}_k s_k||^2 \leq p_{\max}, \\ &(\text{C8}): ||\boldsymbol{\Psi}_i\boldsymbol{H}_k\boldsymbol{f}_k s_k||^2 = \max\{0, \frac{-\sigma^2 + \sqrt{\sigma^4 + M\sigma^4\ln(\frac{N_r - N_t^k}{N_r - N_t^i})(N_r - N_t^i)}}{M}\}, \forall i \in \mathbb{N}, \end{aligned} \tag{30}$$

where we have $\mathbb{N} \subseteq \mathbb{K}^\dagger$. Again, defining $\boldsymbol{W}_k = \boldsymbol{f}_k\boldsymbol{f}_k^H$, P4 is further written as

$$\begin{aligned} P5: &\max_{\boldsymbol{W}_k} \log(|\mathbb{N}| + 1), \\ \text{s.t. } &(\text{C6}): \mathrm{tr}(\boldsymbol{h}_k\boldsymbol{W}_k\boldsymbol{h}_k^H) \geq \bar{\Gamma}_k N_r\sigma^2,\ (\text{C7}): \mathrm{tr}(\boldsymbol{W}_k) \leq p_{\max}, \\ &(\text{C8}): \mathrm{tr}(\boldsymbol{\Psi}_i\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{H}_k^H\boldsymbol{\Psi}_i^H) = \max\{0, \frac{-\sigma^2 + \sqrt{\sigma^4 + M\sigma^4\ln(\frac{N_r - N_t^k}{N_r - N_t^i})(N_r - N_t^i)}}{M}\}, \forall i \in \mathbb{N}, \\ &(\text{C9}): \boldsymbol{W}_k \succeq \mathbf{0},\ (\text{C10}): \mathrm{Rank}(\boldsymbol{W}_k) = 1. \end{aligned} \tag{31}$$

This is an SDP problem after dropping the rank constraint in (C10). The obtained optimal $\boldsymbol{W}_k^*$ is of rank 1, where the proof is similar to that in Proposition 4. Also, introducing an arbitrary number of aliases in (C8) may violate the SNR requirement in (C6) due to the power budget constraint. Hence, one is able to adaptively select alias from the set $\mathbb{K}^\dagger$ while examining the feasibility of P5. The whole algorithm of the HeA precoder is summarized in Algorithm 5.

Algorithm 5 The HeA Precoder Algorithm

Input: CSI, power budget $p_{\max}$, and receive-SNR requirement $\bar{\Gamma}_k$.
1: Call Algorithm 4 to obtain the candidate aliases set $\mathbb{K}^{\dagger}$.
2: **repeat**
3: Exam the feasibility of P5, and adaptively update the number of the aliases, as the steps 3∼11 in Algorithm 3.
4: **until** Convergence
5: Do eigenvalue decomposition of $\boldsymbol{W}_k^*$ to obtain optimal $\boldsymbol{f}_k^*$, and do transmit-side equalization $\boldsymbol{f}_k^{\dagger} = \boldsymbol{f}_k^* e^{-j\phi_k}$.
Output: Optimal precoding design $\boldsymbol{f}_k^{\dagger}$.

C. Complexity Analysis and Possible Extension of the Anonymous Precoders

Now we analyze the complexity of the proposed anonymous precoders. It is known that with a convergence factor ϵ_1, the number of iterations by the bisection-based search is upper-bounder by $\log_2(\frac{b_r - b_l}{\epsilon_1})$, where b_r and b_l denote the right and left bounds of the search region. For the proposed HA precoder in Algorithm 3, the convergence factor ϵ_1 is in fact an integer that denotes the number of users. b_r and b_l equal to 1 and $K-1$, respectively. Hence, the number of iterations is strictly bounded by $\log_2(K-2)$. For each iteration, P3 is solved subject to 1 linear matrix inequality (LMI) constraint (trace) with size 1 in (C1), 1 LMI constraint (trace) with size 1 in (C2), $|\mathbb{N}|$ LMI constraints (trace) with size 1 in (C3), as well as 1 LMI constraint with size N_t^k in constraint (C4). Since P3 is a standard SDP problem, it can be readily solved by the well-known interior-point method (IPM) [34] [37] [38]. Hence, the per-iteration computational complexity is calculated as

$$C_{\text{ite}}^{\text{HA}} = \ln\frac{1}{\epsilon_2}\sqrt{\underbrace{2+|\mathbb{N}|+N_t^k}_{C_{\text{bar}}}}\cdot \Big(\underbrace{n(2+|\mathbb{N}|+(N_t^k)^3)+n^2(2+|\mathbb{N}|+(N_t^k)^2)}_{C_{\text{form}}}+\underbrace{n^3}_{C_{\text{factor}}}\Big), \tag{32}$$

where $n = \mathcal{O}((N_t^k)^2)$ and ϵ_2 denotes the convergence factor of solving a convex optimization problem. In fact, the term C_{bar} in (32) denotes the so-called barrier parameter, measuring the geometric complexity of the conic constraints of the optimization problem P3. C_{form} and C_{factor} represent the complexities of forming and factorization of a $n \times n$ matrix, which is built to guide the search direction of the IPM [34] [37] [38]. As can be seen, the complexity is majorly decided by the cardinality of the set $\mathbb{N}$ and the number of the transmit-antenna N_t^k. Since the users generally are not equipped with massive antennas, the complexity in (32) is comparable to that of the classic SDP-based precoders [37]. On the other hand, the complexity analysis of HeA precoder equals that of the HA precoder, which thus is omitted due to the page limit.

Remark 1: A possible extension of this work would be anonymous communication design for multi-cell coordination scenarios. As the coordinated APs are connected via a backhaul link, they can share the received signal for joint signal processing. Due to the enhanced reception diversity, this multi-cell coordination mechanism enables a better communication performance, but also makes it easier to detect an anonymous user. Acting as a distributed MIMO system, the coordinated APs can share their received signal and merge them into a higher dimension matrix. Hence, the proposed sender detection in Section-III and anonymous precoding in Section-IV are still applicable. Also, there might be other coordination scheme. For example, the APs can apply the proposed sender detection algorithm locally, and only share their hard decision with others. As a countermeasure, the user can still apply the proposed anonymous precoding design to eliminate its PHY characteristics towards the multiple APs. In general, this hard decision-based coordination requires low overhead than the coordinated-multiple-point design above, and similar philosophy of the cooperative detection can be found in cognitive radios [39]. □

V. Simulation Results

We present the Monte-Carlo simulation results in this section. Without loss of generality, the power budget is normalized to $p_{\max} = 1$ Watt. Quadrature phase shift keying (QPSK) is adopted as modulation scheme and the transmitted symbol is randomly generated. Rayleigh block fading MIMO channel is considered. The energy detection threshold in is set to as $\beta = 0.001$. The following precoders are selected as benchmark algorithms: 1) Minimum mean-square error (MMSE) precoder [35], 2) Constructive interference (CI) precoder, which is designed by exploiting the geometry of the signal modulation [36], 3) CI-based anonymous precoder (CIA) precoder, which addresses anonymity by suppressing the value of the Euclidean distance between the actual received signal and the re-constructed signal [24]. Since MMSE and CI belong to the family of anonymity-agnostic precoders, they are used for benchmarking the symbol error rate (SER) performance of the proposed HA and HeA precoders. CIA is an anonymity-preserving design, which can be used for evaluating the anonymity performance of the HA and HeA precoders.

In Fig. 3(a), the system anonymity entropy of different precoders is demonstrated in the homogeneous antennas configuration[2]. It can be seen that the proposed HA precoder demonstrates the highest level of anonymity entropy, which achieves up to 100% enhancement over the CIA anonymous precoder. In particular, the anonymity entropy by the proposed HA precoder increases with transmit-SNRs, while the anonymity entropy by other comparison algorithms shows opposite trends. It is because with a higher value of SNR, the HA precoder is able to adaptively construct more users as equally probable senders and make them indistinguishable from the perspective of the AP, thereby leading to a better anonymity entropy performance. As comparisons, for the MMSE and CI precoders that are designed for optimizing communication performance without the consideration of anonymity (where they have same precoding structure with the combiner at the AP side [36]), the AP can leverage the proposed SA detector

[2]Since the value of the $p(\mathcal{H}_i;\mathcal{H}_k)$ is directly related to the likelihood function values in the GLRT problem [30], per realization value of $p(\mathcal{H}_i;\mathcal{H}_k)$ is equivalently replaced by the ratio of the likelihood function values, i.e., $p(\mathcal{H}_i;\mathcal{H}_k) = \frac{P(d_i;\mathcal{H}_i)}{\sum_{i\in\mathbb{K}} P(d_i;\mathcal{H}_i)}$, $\forall i \in \mathbb{K}$. Finally, per realization anonymity value is calculated as $\mathcal{A} = -\sum_{k\in\mathbb{K}} p(\mathcal{H}_i;\mathcal{H}_k)\log p(\mathcal{H}_i;\mathcal{H}_k)$.

This article has been accepted for publication in IEEE Journal on Selected Areas in Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2022.3211556

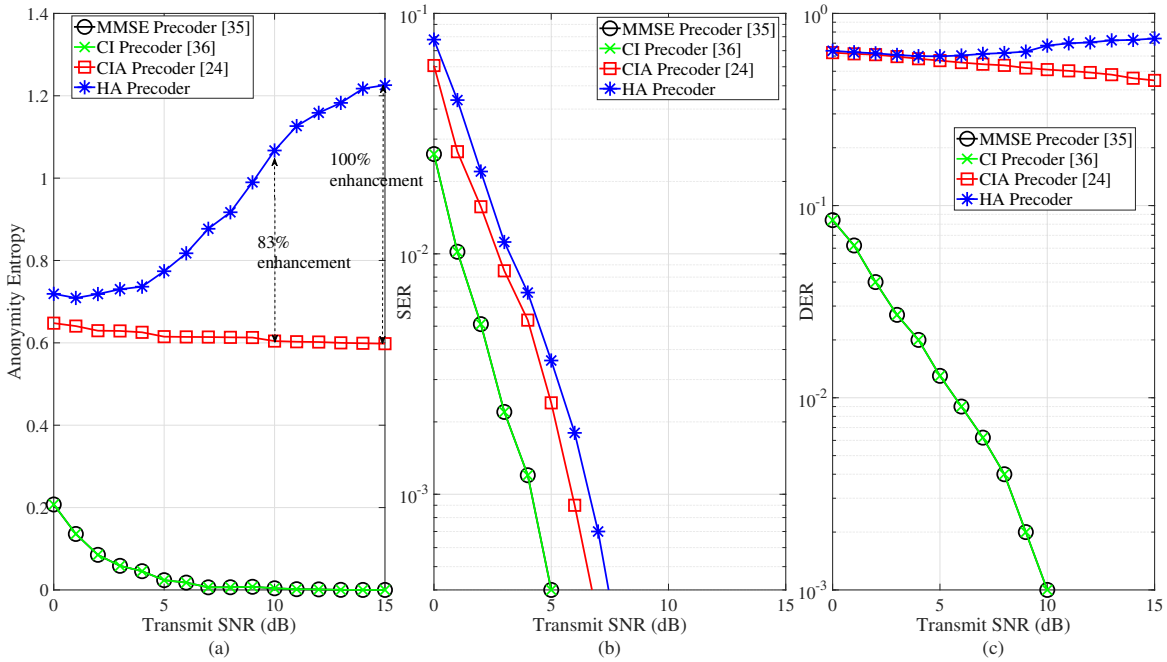

Fig. 3. The impact of the transmit-SNRs on the system anonymity entropy, SER and DER performance in the HA configuration. $N_r = 10$, and $N_t^i = 8, \forall i \in \mathbb{K}$. $\bar{\Gamma}_k = 10$ dB.

to correctly unmask the signal sender, and thus the anonymity entropy gradually decreases and finally approaches 0 at 7 dB SNR.

In Fig. 3(b), the SER performance under different precoders is presented. Since the MMSE and CI precoders aim to optimize receive-performance without anonymous constraint, the high DoFs at the sender side endorse a better SER performance than other anonymous precoders. Although the DoF of the HA precoder is reduced due to the anonymous constraint, it is able to guarantee the subscribed SNR requirement and thus obtains a close SER to the anonymity-agnostic precoders. Hence, the proposed HA precoder indeed maximizes the system anonymity entropy and meanwhile guarantees a high level of communication quality.

In Fig. 3(c), the DER performance at the AP side is illustrated. It can be seen that the proposed HA precoder significantly scrambles the DER performance of the AP, where the AP' DER is as high as 80% even at high SNR regions. It is because the proposed HA precoder manipulates the transmitted signal beampattern for masking the characteristics of the real sender, where the AP is difficult to detect the real sender. As a comparison, though the CIA precoder is able to inhibit the AP's detection at low/moderate SNR regions, the AP is able to correctly reveal the signal sender with 60% probability at high SNR regions. Also, since the MMSE and CI precoders fail to address sender's anonymity, the AP can almost perfectly detect the real sender.

In Fig. 4, the anonymity entropy, SER and DER performance under the HeA configuration are demonstrated. It is observed that the proposed HeA precoder outperforms the CIA precoder in terms of anonymity entropy, SER and DER performance. It is because the HeA precoder constructs aliases based on the users' transmit-antenna configuration, and the dedicated anonymous constraint for the HeA scenario makes the DoF of the HeA precoder less constrained. In comparison, the CIA selects alias randomly, and when a user having distinct number of antenna with the real sender is constructed as a alias, the DoF of the CIA precoder is significantly constrained, leading to a reduced anonymity and communication performance. As a result, the proposed HeA precoder obtains up to 120% anonymity entropy enhancement, and shows 2 dB SNR gain over the CIA precoder for achieving the same SER performance. Also, based on the anonymous constraint that is designed for the HeA configuration, the HeA precoder lets the the maximum likelihood function value of the aliases approach that of the real sender, even they are equipped with different numbers of antennas. Hence, it is observed in Fig. 4(c) that the HeA precoder scrambles the AP's DER to 80%-90% at all SNR regions, while the CIA can only demonstrates around 20%-30% DER.

In Fig. 5, the tradeoff between communication quality and anonymity performance is demonstrated. With a loose receive-SNR requirement, more aliases can be accommodated in the anonymous constraint to inhibit the AP's detection. As a result, both the proposed HA and HeA precoders are able to achieve better anonymity entropy performance in Fig. 5(a). As caparisons, the CI precoder [36], CIA precoder [24] and MMSE precoder [35] are designated based on the transmission power budget, but are not related to the AP's receive-SNR requirement. Hence, when the transmit-SNR is fixed at 15 dB, the anonymity entropy of the three benchmarks remains unchanged. In Fig. 5(b), the SER performance is demonstrated.

This article has been accepted for publication in IEEE Journal on Selected Areas in Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2022.3211556

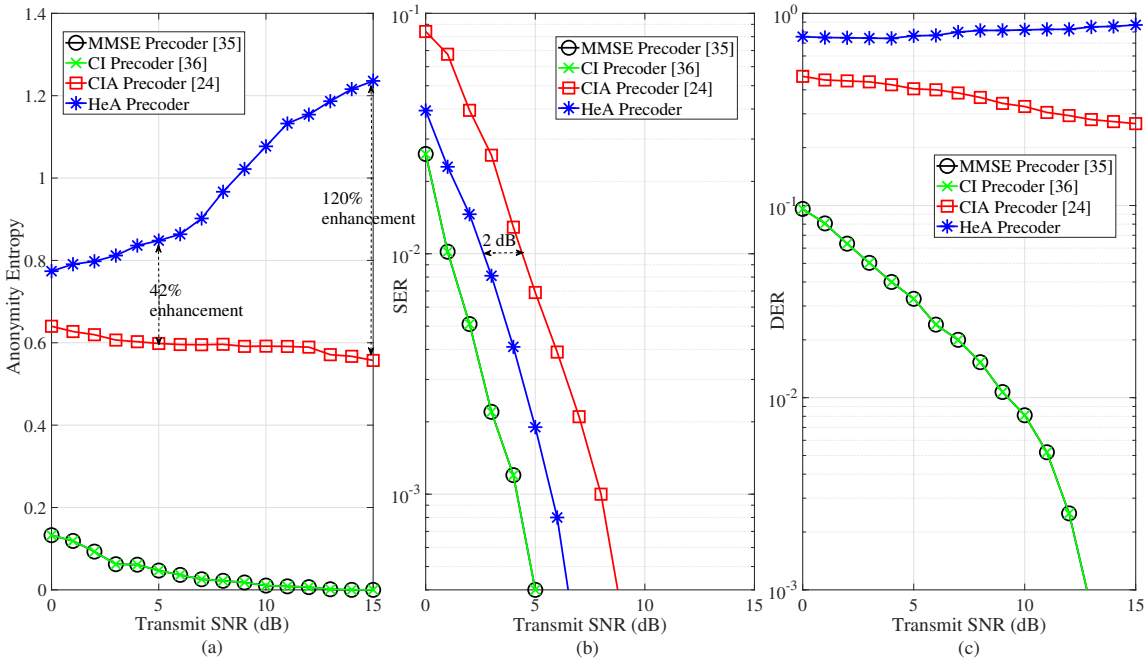

Fig. 4. The impact of the transmit-SNRs on the system anonymity entropy, SER and DER performance in the HeA configuration. $N_r = 10$, $N_t^k = 8$, $N_t^i = 1 \sim 9, \forall i \neq k$. $\bar{\Gamma}_k = 10$ dB.

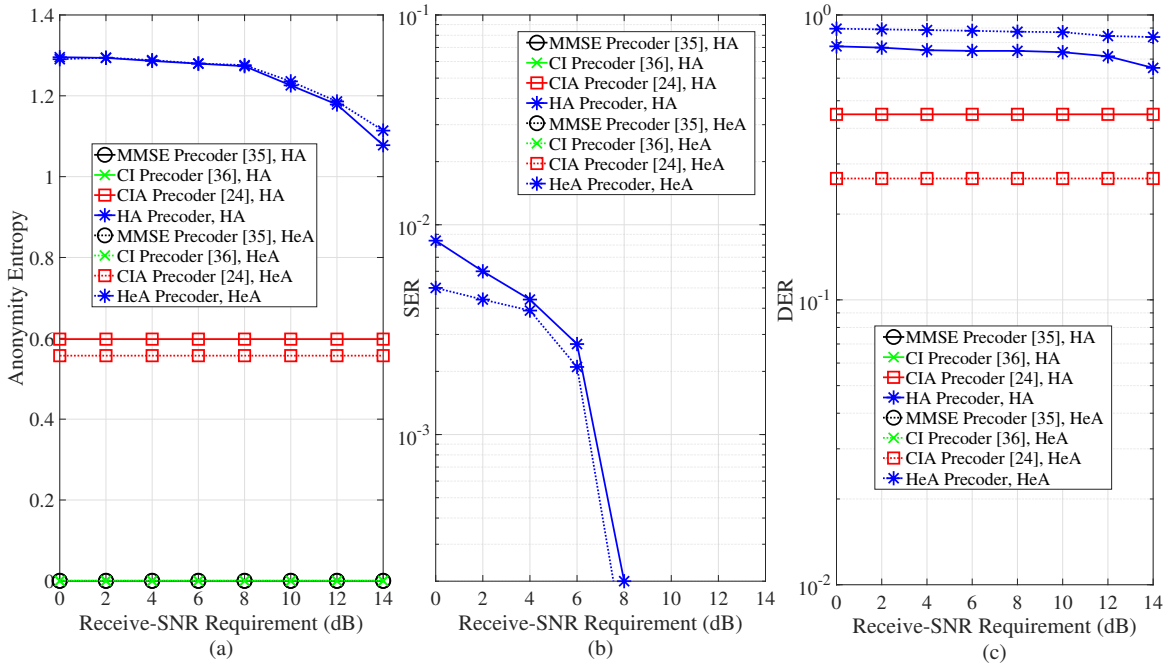

Fig. 5. The impact of the SNR requirement on the anonymity entropy, SER and DER for the HA and HeA configurations. Transmit SNR is fixed at 15 dB. $N_r = 10$. In the HeA configuration, $N_t^k = 8$, $N_t^i = 1 \sim 9, \forall i \neq k$, while in the HA configuration, $N_t^i = 8, \forall i \in \mathbb{K}$.

This article has been accepted for publication in IEEE Journal on Selected Areas in Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2022.3211556

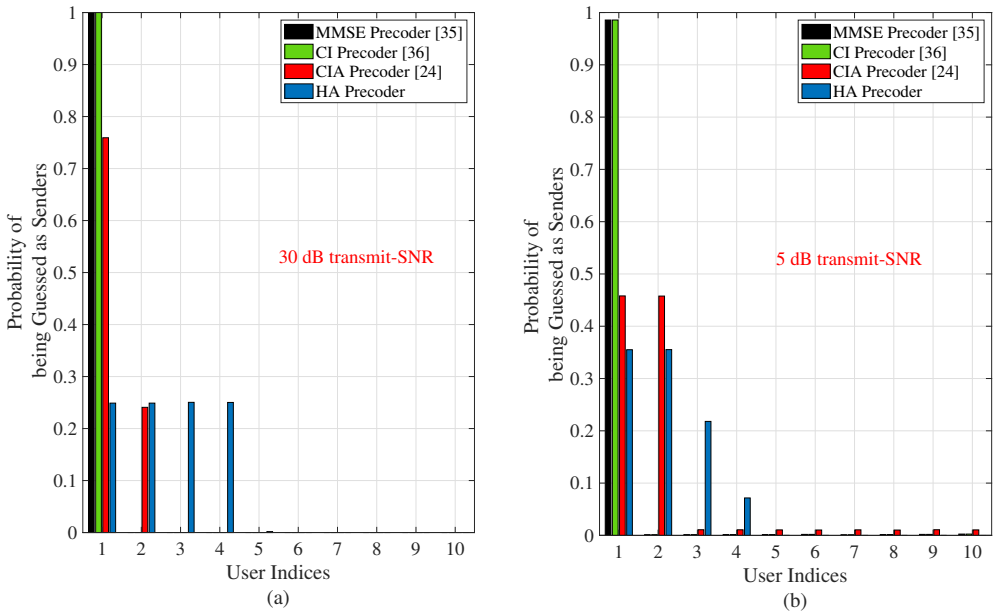

Fig. 6. The probability of being guessed as senders is demonstrated, from the perspective of the AP-side. $N_r = 10$, and $N_t^i = 8, \forall i \in \mathbb{K}$. HA configuration is considered for illustration purpose.

As the SER of the three benchmarks remains 0 at 15 dB transmit-SNR, it is not visible in Fig. 5(b). Also, it is observed that the HeA precoder generally outperforms the HA precoder. This is because the anonymous constraint of the HeA precoder is in fact a relaxed version of that of the HA precoder, and thus the enhanced DoF in precoder design improves its SER performance. The DER performance is demonstrated in Fig. 5(c), where the HA and HeA precoders significantly scramble the AP's DER performance. By contrast, since the AP can perfectly identify the real sender when the CI and MMSE precoder are applied at the user-side, the DER of these two anonymity-agnostic precoders remains 0, which is again not visible in Fig. 5(c).

In Fig. 6, the probability of being guessed as senders are demonstrated, from the perspective of the AP-side. For illustration purpose, we let the first user transmit signals to the AP, while aliases are selected starting from the second user. It can be seen that with a higher level of transmit-SNR, i.e., 30 dB in Fig. 6(a), more aliases more be generated by the proposed HA precoder. Hence, the users 1$\sim$4 are all equally probable senders from the perspective of the AP. With 5 dB transmit-SNR in Fig. 6(b), the capability of constructing aliases is reduced under the receive-side quality requirement, where the users 3 and 4 may not always be accommodated as aliases. Hence, the AP considers that the users 1$\sim$2 are more likely to be the senders, while users 3$\sim$4 are less suspicious. As a result, the anonymity entropy in Fig. 6(b) is smaller than that in Fig. 6(a). In fact, this also shows the fundamental tradeoff between the communication performance and anonymity. As comparisons, the MMSE and CI precoders cannot provide anonymity, where the AP can correctly guess the real sender with a probability approaching 1. The CIA precoder also fails to provide anonymity at high transmit-SNR regions. It is important to note that, in Fig. 6 we demonstrate the per-user average probability of being guessed as real senders. Hence, the entropy calculated based on the average probability in Fig. 6 is higher than the entropy results in Fig. 3.

VI. CONCLUSIONS

In this paper, the PHY SD and anonymous precoder designs have been investigated for the HA and HeA scenarios, respectively. By exploiting the statistical distribution of the Euclidean distances involved in the SD, we have shown that the mean and variance of the Euclidean distances involved in the SD are independent from the users' instantaneous channels realizations, and are decided by the antenna configurations. Based on that finding, we have proposed a SA detector for the edge AP. The proposed detector achieves more than 11 dB SNR gain over the L-ED detector for the same DER performance, and thus poses a new challenge for countermeasure at the users side. Accordingly, we have proposed the HA and HeA precoders based on maximizing the anonymity entropy, subject to the AP's subscribed receive-SNR requirement. The proposed anonymous precoders significantly scramble the AP's SD at all transmit-SNR regions, obtaining 40%-120% anonymity entropy enhancement over other anonymous precoders. Meanwhile, a high level of SER performance is maintained by the proposed anonymous precoders, achieving 10^{-3} level SER at around 6-7 dB transmit-SNRs.

ACKNOWLEDGEMENT

Z. Wei would like to acknowledge the financial support of the Natural Science Foundation of China (NSFC) under Grant

62101384, as well as of the Chongqing Key Laboratory of Mobile Communication Technology under Grant cqupt-mct-202101. C. Masouros would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council under Grant EP/R007934/1 and EP/S028455/1. P. Wang would like to acknowledge the financial support of the Science and Technology Commission of Shanghai Municipality under Grant 21511102400. Xu Zhu would like to acknowledge the financial support of the NSFC under Grant 62171161, the Natural Science Foundation of Guangdong Province under Grant 2021A1515011832, the Shenzhen Key Laboratory under Grant ZDSYS20210623091808025, as well as the Shenzhen Science and Technology Program under Grant JCYJ20210324133009027/KQTD20190929172545139. J. Wang would like to acknowledge the financial support of the Young Elite Scientist Sponsorship Program by CAST under Grant 2020QNRC001. A. P. Petropulu would like to acknowledge the financial support of the Army Research Office under Grant W911NF2110071.

APPENDIX A
PROOF OF PROPOSITION 1

Since $||\boldsymbol{\Psi}_k\boldsymbol{z}||^2 = \boldsymbol{z}^H\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{z}$, we first write the eigenvalue decomposition of $\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k$ as

$$\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k = \boldsymbol{Q}^H\boldsymbol{\Lambda}\boldsymbol{Q}, \tag{33}$$

where $\boldsymbol{\Lambda} = \mathrm{diag}(\lambda_1, ..., \lambda_{N_r})$ is a diagonal matrix, and the elements on its diagonal are the corresponding eigen-values. Let $\bar{\boldsymbol{z}} = \boldsymbol{Q}\boldsymbol{z}$. Since $\boldsymbol{z}$ is an independent identical distributed (i.i.d) Gaussian variable, $\bar{\boldsymbol{z}}$ is also an i.i.d Gaussian variable, where its entries are written as $\bar{\boldsymbol{z}} = [\bar{z}_1, ..., \bar{z}_{N_r}]$. Hence, $\boldsymbol{z}^H\boldsymbol{Q}^H\boldsymbol{\Lambda}\boldsymbol{Q}\boldsymbol{z} = \bar{\boldsymbol{z}}^H\boldsymbol{\Lambda}\bar{\boldsymbol{z}} = \lambda_1\bar{z}_1^2 + ... + \lambda_{N_r}\bar{z}_{N_r}^2$ is a linear combination of N_r i.i.d random variables. Hence, we have the expectation value

$$\begin{aligned}\mathbb{E}\{\boldsymbol{z}^H\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{z}\} &= \mathbb{E}\{\boldsymbol{z}^H\boldsymbol{Q}^H\boldsymbol{\Lambda}\boldsymbol{Q}\boldsymbol{z}\}\\ &= (\lambda_1 + ... + \lambda_{N_r})\sigma^2 = \sigma^2\mathrm{tr}(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k).\end{aligned} \tag{34}$$

On the other hand, we use the moment generating function (MGF) to calculate the variance. Let $\boldsymbol{C}(t) = \boldsymbol{I}_{N_r} - 2t\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Sigma}$, where $\boldsymbol{\Sigma} = \sigma^2\boldsymbol{I}_{N_r}$. Since $\mathbb{E}\{\boldsymbol{z}\} = \boldsymbol{0}$, the MGF of $\boldsymbol{z}^H\boldsymbol{\Psi}^H\boldsymbol{\Psi}\boldsymbol{z}$ is written as $M_{\boldsymbol{z}^H\boldsymbol{\Psi}^H\boldsymbol{\Psi}\boldsymbol{z}}(t) = |\boldsymbol{C}|^{-\frac{1}{2}}$. We further let

$$k(t) = \ln(M_{\boldsymbol{z}^H\boldsymbol{\Psi}^H\boldsymbol{\Psi}\boldsymbol{z}}(t)) = -\frac{1}{2}\ln|\boldsymbol{C}|, \tag{35}$$

where its second-order derivative is calculated as

$$k^{''}(t) = \frac{1}{2}\frac{1}{|\boldsymbol{C}|^2}[\frac{\boldsymbol{d}|\boldsymbol{C}|}{\boldsymbol{d}t}]^2 - \frac{1}{2}\frac{1}{|\boldsymbol{C}|}\frac{\boldsymbol{d}^2|\boldsymbol{C}|}{\boldsymbol{d}t^2}. \tag{36}$$

Denote the eigen-value of $\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Sigma}$ as $\rho_n, n = 1, 2, ..., N_r$. Substituting the value of $|\boldsymbol{C}||_{t=0}$, $\frac{\mathrm{d}|\boldsymbol{C}|}{\mathrm{d}t}|_{t=0}$ and $\frac{\mathrm{d}^2|\boldsymbol{C}|}{\mathrm{d}t^2}|_{t=0}$ into $k^{''}(t)$, we have $k^{''}(0) = \mathrm{tr}(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Sigma})^2 - 2\sum_{n\neq n'}\rho_n\rho_{n'}$. Since we have $\mathrm{tr}(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Sigma})^2 = \mathrm{tr}(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Sigma}\boldsymbol{\Sigma}^H\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k) + 2\sum_{n\neq n'}\rho_n\rho_{n'}$ [31], it yields

$$k^{''}(0) = \mathrm{tr}\big(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Sigma}\boldsymbol{\Sigma}^H\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\big) = \sigma^4\mathrm{tr}\big(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\big). \tag{37}$$

APPENDIX B
PROOF OF PROPOSITION 3

Substituting $\boldsymbol{\Psi}_k = \boldsymbol{H}_k\boldsymbol{H}_k^\dagger - \boldsymbol{I}_{N_r}$ into trace operator in (12) yields

$$\begin{aligned}&\mathrm{tr}(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k) = \mathrm{tr}\big((\boldsymbol{H}_k\boldsymbol{H}_k^\dagger - \boldsymbol{I}_{N_r})^H(\boldsymbol{H}_k\boldsymbol{H}_k^\dagger - \boldsymbol{I}_{N_r})\big)\\ &= \mathrm{tr}\big((\boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H - \boldsymbol{I}_{N_r})^H\cdot\\ &\qquad(\boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H - \boldsymbol{I}_{N_r})\big)\\ &= \mathrm{tr}\big(\boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H\boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H -\\ &\qquad\boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H - \boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H + \boldsymbol{I}_{N_r}\big),\end{aligned} \tag{38}$$

which is equivalent to

$$\begin{aligned}&\mathrm{tr}\big(\boldsymbol{I}_{N_r} - \boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k^H\big)\big)\\ &= \mathrm{tr}(\boldsymbol{I}_{N_r}) - \mathrm{tr}(\boldsymbol{H}_k^H\boldsymbol{H}_k(\boldsymbol{H}_k^H\boldsymbol{H}_k)^{-1}) = \mathrm{tr}(\boldsymbol{I}_{N_r}) - \mathrm{tr}(\boldsymbol{I}_{N_t^k})\\ &= N_r - N_t^k.\end{aligned} \tag{39}$$

In a similar fashion, it can be found that $\mathrm{tr}\big(\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\boldsymbol{\Psi}_k^H\boldsymbol{\Psi}_k\big) = N_r - N_t^k$. Substituting the values above into (12) yields the conclusion of Proposition 3.

APPENDIX C
PROOF OF PROPOSITION 4

Dropping the rank-1 constraint, the optimization problem in P3 is jointly convex w.r.t the variables and satisfies the Slater's constraint condition. With the strong duality, solving the dual problem is equivalent to solving the primal problem. We write the Lagrangian function of P3 as

$$\begin{aligned}\mathcal{L} = &-\log(|\mathbb{N}| + 1) - \mathrm{tr}(\boldsymbol{P}\boldsymbol{W}_k) +\\ &\mu\mathrm{tr}((\boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r})\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{H}_k^H(\boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r})^H) +\\ &\lambda(\bar{\Gamma}||\boldsymbol{z}||^2 - \mathrm{tr}(\boldsymbol{h}_k\boldsymbol{W}_k\boldsymbol{h}_k^H)) + \delta(p_{\max} - \mathrm{tr}(\boldsymbol{W}_k))\end{aligned} \tag{40}$$

where μ, λ and δ are the Lagrangian multipliers associated with constraints, while matrix $\boldsymbol{P} \in \mathbb{C}^{N_t^k\times N_t^k}$ is a Lagrangian multiplier matrix for the positive semi-definite constraint. We reveal the structure of the optimal matrix $\boldsymbol{W}_k^*$ by investigating the Karush-Kuhn-Tucker (KKT) conditions, which includes the dual constants, complementary slackness, and the gradient of Lagrangian function w.r.t $\boldsymbol{W}_k$ equals to 0:

$$\begin{cases}\mu^* \geq 0, \delta^* \geq 0, \boldsymbol{P}^* \succeq \boldsymbol{0},\\ \boldsymbol{P}^*\boldsymbol{W}_k^* \succeq \boldsymbol{0},\\ \frac{\partial\mathcal{L}}{\partial\boldsymbol{W}_k}|_{\boldsymbol{W}_k^*} = -\boldsymbol{P}^* + \mu^*\boldsymbol{\Upsilon} - \lambda^*\boldsymbol{h}_k\boldsymbol{h}_k^H - \delta^*\boldsymbol{I}_{N_t^k} = 0,\end{cases} \tag{41}$$

where $\boldsymbol{\Upsilon} = \boldsymbol{H}_k^T(\boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r})^T(\boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r})^*\boldsymbol{H}_k^*$. It further yields $\boldsymbol{P}^* = \mu^*\boldsymbol{\Upsilon} - \lambda^*\boldsymbol{h}_k\boldsymbol{h}_k^H - \delta^*\boldsymbol{I}_{N_t^k}$. It is straightforward that in order to meet the reception SNR requirement, it holds that $\mathrm{Rank}(\boldsymbol{W}_k^*) \geq 1$ and $\boldsymbol{W}_k^* \neq \boldsymbol{0}$. Hence, the complementary slackness $\boldsymbol{P}^*\boldsymbol{W}_k^* = \boldsymbol{0}$ indicates $\mathrm{Rank}(\boldsymbol{P}^*) \leq N_t^k - 1$. If $\mathrm{Rank}(\boldsymbol{P}^*) = N_t^k - 1$, the optimal matrix $\boldsymbol{W}_k^*$ must be a rank-one constraint. Hence, we first show by contradiction that $\mu^*\boldsymbol{\Upsilon} - \delta^*\boldsymbol{I}_{N_t^k}$ is a positive-definite matrix with probability one under the condition stated in the Proposition.

With the optimal dual variables $\mu^*, \delta^*, \lambda^*$, and $\boldsymbol{P}^*$, the dual problem is given as $\min_{\boldsymbol{W}_k}\mathcal{L}(\boldsymbol{W}_k, \mu^*, \delta^*, \lambda^*\boldsymbol{P}^*)$. Suppose

$\mu^*\boldsymbol{\Upsilon} - \delta^*\boldsymbol{I}_{N_t^k}$ is not positive definite, where we choose $\boldsymbol{W}_k = \beta\boldsymbol{f}\boldsymbol{f}^H$ as one of the optimal solution of the dual problem, where $\beta > 0$ is a scaling factor and $\boldsymbol{f}$ is the eigenvector corresponding to a non-positive eigenvalue $\alpha < 0$, i.e., $(\mu^*\boldsymbol{\Upsilon} - \delta^*\boldsymbol{I}_{N_t^k})\boldsymbol{f} = \alpha\boldsymbol{f}$. Substituting $\boldsymbol{W}_k = \beta\boldsymbol{f}\boldsymbol{f}^H$ and $(\mu^*\boldsymbol{\Upsilon} - \delta^*\boldsymbol{I}_{N_t^k})\boldsymbol{f} = \alpha\boldsymbol{f}$ into the dual problem yields

$$\mathrm{tr}(\alpha\beta\boldsymbol{f}\boldsymbol{f}^H) - \beta\mathrm{tr}\big((\boldsymbol{P}^* + \lambda^*\boldsymbol{h}_k\boldsymbol{h}_k^H)\boldsymbol{f}\boldsymbol{f}^H\big) \tag{42}$$

where the first term is not positive. For the second term, since $\boldsymbol{H}_k$ is an i.i.d channel matrix, the equivalent post-combiner channel $\boldsymbol{h}_k = \boldsymbol{1}^T\boldsymbol{H}_k$ is also an i.i.d vector. Based on $\boldsymbol{P}^* \succeq \boldsymbol{0}$, the term $\beta\mathrm{tr}\big((\boldsymbol{P}^* + \lambda^*\boldsymbol{h}_k\boldsymbol{h}_k^H)\boldsymbol{f}\boldsymbol{f}^H\big) \to -\infty$ by setting $\beta \to \infty$ where the dual optimal value becomes unbounded. However, the optimal value of the primal problem P3 is non-negative, and the strong duality cannot hold, leading to a contradiction. Hence, $\mu^*\boldsymbol{\Upsilon} - \delta^*\boldsymbol{I}_{N_t^k}$ is a positive-definite matrix with probability one, and it has $\mathrm{Rank}(\mu^*\boldsymbol{\Upsilon} - \delta^*\boldsymbol{I}_{N_t^k}) = N_t^k$. Based on the sub-additivity property of rank operator, we have

$$\begin{aligned}&\mathrm{Rank}(\boldsymbol{P}^*) + \mathrm{Rank}(\lambda^*\boldsymbol{h}_k\boldsymbol{h}_k^H) \geq \\ &\mathrm{Rank}(\boldsymbol{P}^* + \lambda^*\boldsymbol{h}_k\boldsymbol{h}_k^H) = \mathrm{Rank}(\mu^*\boldsymbol{\Upsilon} - \delta^*\boldsymbol{I}_{N_t^k}) = N_t^k,\end{aligned} \tag{43}$$

which indicates $\mathrm{Rank}(\boldsymbol{P}^*) = N_t^k - 1$. Hence, $\mathrm{Rank}(\boldsymbol{W}_k^*) = 1$ holds with probability one.

Appendix D
Proof of Proposition 5

The value of d_i is calculated as $d_i = ||\boldsymbol{r} - \hat{\boldsymbol{r}}_i||^2 = ||(\boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r})\boldsymbol{H}_k\boldsymbol{f}_k s_k + (\boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r})\boldsymbol{z}||^2$ as shown in (7). For simplicity, let $\boldsymbol{\Psi}_i = \boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r}$ and $\boldsymbol{p} = \boldsymbol{\Psi}_i\boldsymbol{H}_k\boldsymbol{f}_k s_k$, and we have $d_i = ||\boldsymbol{p} + \boldsymbol{\Psi}_i\boldsymbol{z}||^2$. Since $\boldsymbol{p} + \boldsymbol{\Psi}_i\boldsymbol{z} \sim \mathcal{N}(\boldsymbol{p}, \sigma^2\boldsymbol{\Psi}_i\boldsymbol{\Psi}_i^H)$, we have

$$\begin{aligned}\mathbb{E}\{d_i\} &= \mathbb{E}\{\mathrm{tr}((\boldsymbol{p} + \boldsymbol{\Psi}_i\boldsymbol{z})(\boldsymbol{p} + \boldsymbol{\Psi}_i\boldsymbol{z})^H)\} \\ &= \mathrm{tr}(\mathbb{E}\{(\boldsymbol{p} + \boldsymbol{\Psi}_i\boldsymbol{z})(\boldsymbol{p} + \boldsymbol{\Psi}_i\boldsymbol{z})^H\}) = \mathrm{tr}(\sigma^2\boldsymbol{\Psi}_i^H\boldsymbol{\Psi}_i + \boldsymbol{p}\boldsymbol{p}^H) \\ &= \sigma^2(N_r - N_t^i) + \boldsymbol{p}^H\boldsymbol{p}.\end{aligned} \tag{44}$$

On the other hand, its variance is given as

$$\begin{aligned}\mathbb{V}\{d_i\} &= \mathrm{tr}(\sigma^4\boldsymbol{\Psi}_i\boldsymbol{\Psi}_i^H\boldsymbol{\Psi}_i\boldsymbol{\Psi}_i^H) + 2\sigma^2\boldsymbol{p}^H\boldsymbol{\Psi}_i^H\boldsymbol{\Psi}_i\boldsymbol{p} \\ &= \sigma^4(N_r - N_t^i) + 2\sigma^2\boldsymbol{p}^H\boldsymbol{\Psi}_i^H\boldsymbol{\Psi}_i\boldsymbol{p} \\ &= \sigma^4(N_r - N_t^i) + 2\sigma^2\boldsymbol{p}^H\boldsymbol{p},\end{aligned} \tag{45}$$

In case of block-level of multi-user access and detection, the expectation and variance can be further re-written as

$$\mathbb{E}\{d_i\} = M\sigma^2(N_r - N_t^i) + M\boldsymbol{p}^H\boldsymbol{p}, \tag{46}$$

and

$$\mathbb{V}\{d_i\} = M\sigma^4(N_r - N_t^i) + 2M\sigma^2\boldsymbol{p}^H\boldsymbol{p}. \tag{47}$$

References

[1] Z. Wei, C. Masouros, F. Liu, S. Chatzinotas, and B. Ottersten, "Energy- and cost-efficient physical layer security in the era of IoT: the role of interference," *IEEE Commun. Mag.*, vol. 58, issue. 4, pp. 81-87, Apr. 2020.

[2] M. Bloch *et al.,* "An overview of information-theoretic security and privacy: metrics, limits and applications," *IEEE J. Sel. Inf. Theory*, vol. 2, no. 1, pp. 1-22, Mar. 2021.

[3] K. Emura, A. Kanaoka, SA. Ohta, K. Omote, and T. Takahashi, "Secure and anonymous communication technique: formal model and its prototype implementation," *IEEE Trans. Emerging Topics Comput.,* vol. 4, no. 1, pp. 88-101, Mar. 2016.

[4] M. S. Herfeh, A. Chorti and H. V. Poor, "Physical layer security: authentication, integrity and confidentiality," Chapter in *Physical Layer Security*, Switzerland: Springer Nature, to appear.

[5] L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Sig. Proc.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[6] 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.

[7] D. Wang, P. Ren, and J. Cheng, "Cooperative secure communication in two-hop buffer-aided networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 972-985, Mar. 2018.

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

[9] C. Jian *et al.,* "Underwater covert communications relying on bargaining game theory," in *Porc. IEEE GLOBECOM'21*, Virtual, May 2021.

[10] Z. Wei, C. Masouros, H. V. Poor, A. P. Petropulu, and L. Hanzo, "Physical layer anonymous precoding: the path to privacy-preserving communications," to appear in IEEE Wireless Commun.

[11] M. Diaz, H. Wang, F. P. Calmon, and L. Sankar, "On the robustness of information -theoretic privacy measures and mechanisms," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 1949-1978, Apr. 2020.

[12] J. Liao, O. Kosut, L. Sankar, and F. P. Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 8043-8066, Dec. 2019.

[13] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," *in Proc. Privacy Enhancing Technologies Workshop'02,* San Francisco, USA, Apr. 2002.

[14] C. Dwork, "Differential privacy," *in Proc. Int. Colloquium Automata Lang. Program.*, Venice, Italy, Jul. 2006.

[15] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Estimation efficiency under privacy constrains," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1512-1534, Mar. 2019.

[16] I. Issa, A. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1625-1657, Mar. 2020.

[17] D. Chaum and E. van Heyst, "Group signatures," in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 1991, London, UK, pp. 257–265.

[18] 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.

[19] K. Emura and T. Hayashi, "Road to vehicle communications with time-dependent anonymity, a lightweight construction and its experimental results," *IEEE Trans. Veh. Tech.*, vol. 67, no. 2, pp. 1582-1597, Feb. 2018.

[20] J. Liu, Z. Zhang, X. Chen, and K. Kwak, "Certificateless remote anonymous authentication schemes for wireless body-area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332-343, Feb. 2014,

[21] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proc. IEEE INFOCOM,* Miami, USA, 2005.

[22] K. Sakai, M. T. Sun, W. S. Ku, and J. Wu, "On anonymous routing in delay tolerant networks," *IEEE Trans. Mobile Comput.,* vol. 18, no. 12, pp. 2926-2940, Dec. 2019.

[23] J. Kong and X. Hong, "Anodr: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in *Proc. ACM MobiHoc,* Annapolis, USA, 2003.

[24] Z. Wei, F. Liu, and C. Masouros, "Fundamentals of physical layer anonymous communications: sender detection and anonymous precoding," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 64-79, Jan. 2022.

[25] C. Chou, D. Wei, C. J, Kuo, 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.

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

[27] Y. C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput trade-off for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

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

[29] E. Axell, G. Leus, E. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio," *IEEE Sig. Proc. Mag.*, vol. 57, no. 6, pp. 101-116, May 2012.

[30] S. M. Kay, Fundamental of statistical signal processing-Vol. 1: estimation theory, in Englewood Cliffs, NJ, U.S.A., Prentice Hall, 1993.

[31] R. A. Horn and C. R. Johnson, Matrix analysis, Cambridge University Press; 2nd edition, Oct. 2012.

[32] T. Y. Al-Naffouri *et al.,* "On the distribution of indefinite quadratic forms in Gaussian random variables," *IEEE Trans. Commun.,* vol. 64, no. 1, pp. 153-165, Jan. 2016.

[33] M. Arakawa, Computational workloads for commonly used signal processing kernels, project report ESC-TR-2006-071, MIT, U.S.A., 2006.

[34] 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.

[35] 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.

[36] A. Li and C. Masouros, "Interference exploitation precoding made practical: optimal closed-form solution for PSK modulations," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7661-7676, Sept. 2018.

[37] K. Wang, A. M. C. So, T. H. Chang, W. K. Ma, and C. Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: tractable approximations by conic optimization," *IEEE Trans. Sig. Proc.*, vol. 62, no. 21, pp. 5690-5605, Nov. 2014.

[38] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge, U.K.:Cambridge Univ. Press, 2004.

[39] W. Zhang, R. K. Mallik, and K. B. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5761-5766, Dec. 2009.

Zhongxiang Wei (S'15–M'17) received the Ph.D. degree in Electrical and Electronics Engineering from the University of Liverpool, Liverpool, U.K., in 2017. From March 2016 to March 2017, he was with the Institution for Infocomm Research, Agency for Science, Technology and Research, Singapore, as a Research Assistant. From March 2018 to March 2021, he was with the Department of Electrical and Electronics Engineering, University College London, as a research associate. He is currently an associate professor in the College of Electronic and Information Engineering, Tongji University, China. He has authored and co-authored more than 60 research papers published on top-tier journals and international conferences.

His research interests include anonymous communications, constructive interference designs, and millimeter-wave communications. He has acted as a Session/Track Chair or TPC member of various international flagship conferences, such as IEEE ICC, GLOBECOM, and ICASSP. He was a recipient of Shanghai Leading Talent Program (Young Scientist) in 2021, an Exemplary Reviewer of the IEEE TWC in 2016, the Outstanding Self-Financed Students Abroad in 2018, and the A*STAR Research Attachment Programme (ARAP) in 2016.

Christos Masouros (SMIEEE, MIET) received the Diploma degree in Electrical and Computer Engineering from the University of Patras, Greece, in 2004, and MSc by research and PhD in Electrical and Electronic Engineering from the University of Manchester, UK in 2006 and 2009 respectively. In 2008 he was a research intern at Philips Research Labs, UK. Between 2009-2010 he was a Research Associate in the University of Manchester and between 2010-2012 a Research Fellow in Queen's University Belfast. In 2012 he joined University College London as a Lecturer. He has held a Royal Academy of Engineering Research Fellowship between 2011-2016.

Since 2019 he is a Full Professor of Signal Processing and Wireless Communications in the Information and Communications Engineering research group, Dept. Electrical and Electronic Engineering, University College London. His research interests lie in the field of wireless communications and signal processing with particular focus on Green Communications, Large Scale Antenna Systems, Integrated Sensing and Communications, interference mitigation techniques for MIMO and multicarrier communications. He was the recipient of the Best Paper Awards in the IEEE GlobeCom 2015 and IEEE WCNC 2019 conferences, and has been recognized as an Exemplary Editor for the IEEE Communications Letters, and as an Exemplary Reviewer for the IEEE Transactions on Communications. He is an Editor for IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, the IEEE Open Journal of Signal Processing, and Editor-at-Large for IEEE Open Journal of the Communications Society. He has been an Associate Editor for IEEE Communications Letters, and a Guest Editor for a number of IEEE Journal on Selected Topics in Signal Processing issues. He is a founding member and Vice-Chair of the IEEE Emerging Technology Initiative on Integrated Sensing and Communications, Vice Chair of the IEEE Special Interest Group on Integrated Sensing and Communications, and Chair of the IEEE Special Interest Group on Energy Harvesting.

Ping Wang Ping Wang (M'20) received the Ph.D. degree in computer science from Shanghai Jiaotong University, Shanghai, China, in 2007. He is an associate professor of information and Communication engineering with Tongji University.

His main research interests are in routing algorithms, resource allocation of wireless networks (especially for VANETs) and multi-sensor information fusion. He also focuses on developing prototype systems for connected intelligent vehicles and building test bed for connected intelligent vehicles based on MEC. He has published over 120 scientific papers and 3 books. He has applied 1 international patent and over 20 national patents, and submitted 7 standardization drafts in the field of intelligent connected vehicles.

Xu Zhu (S'02-M'03-SM'12) received the B.Eng. degree (Hons.) in Electronics and Information Engineering from the Huazhong University of Science and Technology, Wuhan, China, in 1999, and the Ph.D. degree in Electrical and Electronic Engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2003. She has been a Reader of the Department of Electrical Engineering and Electronics, the University of Liverpool, Liverpool, U.K. She is also with the Harbin Institute of Technology, Shenzhen, China.

She has more than 200 peer-reviewed publications on communications and signal processing. She has served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and a Guest Editor for several international journals such as Electronics. She has acted as a Chair for various international conferences, such as the Vice-Chair of the 2006 and 2008 ICARN International Workshops, the Program Chair of ICSAI 2012, the Symposium Co-Chair of the IEEE ICC 2016, ICC 2019 and Globecom 2021, and the Publicity Chair of the IEEE IUCC 2016. She was the recipient of the Best Paper Award of the IEEE Globecom 2019. Her research interests include MIMO, channel estimation and equalization, ultra reliable low latency communication, resource allocation, cooperative communications.

Jingjing Wang (S'14-M'19-SM'21) received his B.S. degree in Electronic Information Engineering from Dalian University of Technology, Liaoning, China in 2014 and the Ph.D. degree in Information and Communication Engineering from Tsinghua University, Beijing, China in 2019, both with the highest honors. From 2017 to 2018, he visited the Next Generation Wireless Group chaired by Prof. Lajos Hanzo, University of Southampton, UK. Dr. Wang is currently an associate professor at School of Cyber Science and Technology, Beihang University.

His research interests include AI enhanced next-generation wireless networks, swarm intelligence and confrontation. He has published over 100 IEEE Journal/Conference papers. Dr. Wang was a recipient of the Best Journal Paper Award of IEEE ComSoc Technical Committee on Green Communications and Computing in 2018, the Best Paper Award of IEEE ICC and IWCMC in 2019.

Athina P. Petropulu (Fellow, IEEE) is a Distinguished Professor with the Electrical and Computer Engineering (ECE) Department, Rutgers, was the Chair of the Department during 2010–2016. Prior to joining Rutgers she was a Professor of ECE with Drexel University from 1992 to 2010. She held a Visiting Scholar appointments with SUPELEC, Universite' Paris Sud, Princeton University, and the University of Southern California.

Her research interests include the area of statistical signal processing, wireless communications, signal processing in networking, physical layer security, and radar signal processing. Her research was funded by various government industry sponsors including the National Science Foundation (NSF), the Office of Naval research, the U.S. Army, the National Institute of Health, the Whitaker Foundation, Lockheed Martin and Raytheon. Dr. Petropulu is the American Association for the Advancement of Science (AAAS), and was the recipient of the 1995 Presidential Faculty Fellow Award given by NSF and the White House. She is 2022 President of the IEEE Signal Processing Society (SPS) and 2020 President-Elect of IEEE SPS. She was the Editor-in-Chief of the IEEE TRANSACTIONS ON SIGNAL PROCESSING from 2009 to 2011 and IEEE Signal Processing Society Vice President-Conferences from 2006 to 2008. She was the General Chair of 2020 and 2021 IEEE SPS PROGRESS Workshops, General Co-Chair of the 2018 IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), and Genera Chair of the 2005 International Conference on Acoustics Speech and Signal Processing (ICASSP-05). She was Distinguished Lecturer for the Signal Processing Society for 2017-2018, and is currently a Distinguished Lecturer for the IEEE Aerospace and Electronics Systems Society. She was the recipient of the 2005 IEEE Signal Processing Magazine Best Paper Award, the 2012 IEEE Signal Processing Society Meritorious Service Award, is coauthor (with B. Li) of the 2020 IEEE Signal Processing Society Young Author Best Paper Award and co-recipient (with B. Li) of the 2021 Barry Carlton Best Paper Award by IEEE Aerospace and Electronic Systems Society.