On the Closed-Form Detection Error Rate Analysis in Physical Layer Anonymous Communications

Yifan Cui, *Student Member, IEEE*, Zhongxiang Wei, *Member, IEEE*, Christos Masouros, *Senior Member, IEEE*, Xu Zhu, *Senior Member, IEEE*, and Hong Tang

***Abstract*—In recent years, physical layer (PHY) anonymous precoding has become imperative in applications that carry personal and sensitive data. While manipulating the signaling pattern of transmitted signals for obtaining high utility, the anonymous precoder also mask the sender's PHY characteristics for the purpose of sender anonymity. Nevertheless, the anonymity provided by anonymous precoding has only been numerically demonstrated, and there still lacks analytic result regarding the detection error rate (DER) performance. In this letter, we give the first attempt to show analytic DER result of generic precoders. The closed-form yet tight DER expressions are derived, as a function of the precoder employed at the sender, block length, propagation channel, and noise status. Some important properties are revealed. Finally, simulation results validate that the deviation between the closed-form and actual DER results is on the level of 0∼0.05. The proposed analytic DER results help easily quantify the anonymity performance of existing anonymity-agnostic and anonymous precoders.**

***Index Terms*—Closed-form DER, anonymous communications, physical layer, anonymous precoding.**

I. Introduction

In the era of the Internet of Things (IoT), provision of security and privacy is a pervasive issue. In general, purpose of data security is to prevent confidential communication from being exploited or attacked by external eavesdroppers. Authentication [1], cryptography [2], covert communication [3], securing beamforming and other methods [4] from the PHY to the upper layers of networks have been extensively studied for security. By contrast, the aim of privacy protection is to minimize the receiver's capability to infer the non-shared information, while guaranteeing the communication quality of the same receiver for utility [5]. For example, when receiving signal for utility in smart homes and telemedicine, a legitimate but curious receiver may also infer the user's non-shared data, such as users' political inclination, lifestyle and whereabouts. Hence, when communicating with service providers for utility, users wish to remain anonymous towards the receiver for avoiding potential cyberfraud, known as anonymous communications.

On the upper layers of networks, a bundle of anonymous protection strategies has been studied, including anonymous encryption [6], anonymous authentication [7], routing designs [8] and so on. These techniques conceal users' characteristics of the higher layers, such as their identities (ID)s or media access control (MAC)/Internet protocol (IP) addresses. As a further step, the work in [5] points out that the signaling pattern at the PHY can also be leveraged to unmask individuals. To be specific, when employing classic minimum mean squared error (MMSE), zero-forcing (ZF) [9], singular value decomposition (SVD) [10], power minimization (PM) [11] and other anonymity-agnostic precoders, the pattern of the received signal is coupled with the user's unique channel state information (CSI). Hence, the receiver can employ PHY sender detection algorithms, which will be detailed in Section II, to disclose the sender. As a countermeasure at the PHY, anonymous precoding is investigated [5], which is capable of concealing a sender's CSI from the transmitted signal, thereby scrambling the accuracy of sender detection at the receiver side [5].

Nevertheless, the provision of anonymity by the anonymous precoder has only been numerically proved. [5] was the first to show that, with an empirical anonymous constraint, the pattern of the transmitted signal can be controlled for the purpose of sender anonymity. [12] pointed out that a stricter value of anonymous constraint is able to better guarantee the anonymity, thus deteriorating the DER performance of the receiver. Despite of recent progress made, the analytic DER performance achieved by different precoders is still an open challenge. As a result, the anonymity performance gain of the anonymous precoder has not been quantified yet. This further hinders researcher from flexibly balancing the anonymity and communication performance. Motivated by this issue, in this paper, we attempt to present theoretical analysis of the DER performance. Our contributions are summarized as follows.

Exploiting the statistics of the received signal, we first demonstrate analytic DER performance of two classic PHY sender detection strategies, i.e., the maximum Frobenius norm (MFN) based and the maximum likelihood estimation (MLE) based detectors. The closed-form but tight DER expression is explicitly derived, as a function of the precoder employed at the sender, block length, propagation channel, and noise status. With the closed form DER expression at hand, we evaluate the DER of several classic block- and symbol-level anonymity-agnostic precoders, as well as anonymous precoders. Also, a

Yifan Cui and Zhongxiang Wei are with the College of Electronic and Information Engineering, Tongji University, Shanghai 200092, China (e-mail: 2230692, z_wei@tongji.edu.cn).

Christos Masouros is with the Department of Electronic and Electrical Engineering, University College London, London WC1E 6BT, U.K. (e-mail: c.masouros@ucl.ac.uk).

Xu Zhu is with the School of Electronic and Information Engineering, Harbin Institute of Technology, Shenzhen 518055, China (e-mail: xuzhu@stu.hit.edu.cn).

Hong Tang is with the School of Electronic and Information Engineering, Chongqing University of Posts and Telecommunication, Chongqing 400065, China (e-mail: tangh@cqupt.edu.cn).

series of important properties regarding the PHY anonymity has been revealed.

Notation: Matrices and vectors are represented by boldface capital and lower case letters, respectively. $\boldsymbol{I}_n$ denotes an n-by-n identity matrix. $[\boldsymbol{A}]_{mn}$ abstracts the element in row m and column n of a matrix. $\boldsymbol{A}^H$, $\mathrm{tr}(\boldsymbol{A})$ and $\|\boldsymbol{A}\|_F$ denote the Hermitian transpose, trace and Frobenius norm of a matrix. $\|\boldsymbol{x}\|_2$ denotes the 2-norm of a vector $\boldsymbol{x}$. $|\cdot|$ denotes absolute value of a complex number. $\mathcal{N}\{\cdot\}$ and $\mathcal{CN}\{\cdot\}$ represent Gaussian distribution and complex Gaussian distribution. $\Pr(a|b)$ denotes the conditional probability of a given b. $\mathbb{E}\{\cdot\}$ and $\mathbb{V}\{\cdot\}$ denote expectation and variance of a random variable. $\mathrm{cov}\{a,b\}$ denotes covariance of two random variables.

II. System Model and Sender Detection Strategies

In this section, system model and PHY sender detectors are introduced in subsections II-A and II-B.

A. System Model

Consider an uplink multiuser multiple-input and multiple-output (MIMO) transmission scenario, where a group of users $\mathbb{K}$ ($|\mathbb{K}| = K$) send signals to a base station (BS) under time-division-multiple-access. In particular, users remain anonymous during transmitting. Assume that each user is equipped with N_t transmit-antennas, while the BS is equipped with N_r receive-antennas. Define $\boldsymbol{H}_k \in \mathbb{C}^{N_r \times N_t}$ as the block-fading MIMO channel between the k-th user and the BS. As the sender detection is performed at the block level, assume that the block length is L. Define $\boldsymbol{W}_k \in \mathbb{C}^{N_t \times N_s}$ as the precoding matrix of the k-th user, and $\boldsymbol{S}_k \in \mathbb{C}^{N_s \times L}$ as the symbol matrix transmitted by the k-th user, where N_s denotes the number of symbols transmitted per slot depending on the specific multiplexing strategy. Denote $\boldsymbol{N} \in \mathbb{C}^{N_r \times L}$ as the circularly symmetric complex Gaussian (CSCG) noise with noise variance σ^2 and element as $[\boldsymbol{N}]_{mn} \sim \mathcal{CN}(0, \sigma^2)$. Without loss of generality, assume that the k-th user sends signal to the BS in the considered block, and the received signal at BS is written as

$$\boldsymbol{Y} = \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{S}_k + \boldsymbol{N}. \tag{1}$$

At PHY layer, the BS only analyzes the received signal and the inherent characteristics of the wireless channels to detect the sender. The sender detection can be formulated as a multiple hypotheses testing (MHT) problem

$$\boldsymbol{Y} = \begin{cases} \mathcal{H}_0 : \boldsymbol{N}, \\ \mathcal{H}_1 : \boldsymbol{H}_1 \boldsymbol{W}_1 \boldsymbol{S}_1 + \boldsymbol{N}, \\ \quad \vdots \\ \mathcal{H}_K : \boldsymbol{H}_K \boldsymbol{W}_K \boldsymbol{S}_K + \boldsymbol{N}, \end{cases} \tag{2}$$

where the hypothesis $\mathcal{H}_0$ denotes that only noise appears at the BS, while hypothesis $\mathcal{H}_k$ means a signal coming from the k-th user is received.

B. Sender Detection Strategies

In this subsection, the MFN and the MLE sender detection strategies are briefly discussed for the sake of completeness [5]. For handling the MHT problem in (2), the BS can first detect the presence of a signal, generally solved by classic energy detection [13]. The test statistic is given by $\Gamma(\boldsymbol{Y}) = \frac{\|\boldsymbol{Y}\|_F^2}{LN_r}$. On comparing $\Gamma(\boldsymbol{Y})$ against a detection threshold ε, the hypothesis $\mathcal{H}_0$ is clarified to be true when $\Gamma(\boldsymbol{Y}) < \varepsilon$, and to be false otherwise.

1) MFN Sender Detection: The philosophy of the MFN is to leverage the concept of match filter for sender detection. As the received signal propagates from $\boldsymbol{H}_k$, one can multiply the received signal with $\boldsymbol{H}_k^H$. Then, the resulted F-norm $G_k = \|\boldsymbol{H}_k^H \boldsymbol{Y}\|_F^2 = \|\boldsymbol{H}_k^H \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{S}_k + \boldsymbol{H}_k^H \boldsymbol{N}\|_F^2$ has a high probability to be higher than the norm $G_i = \|\boldsymbol{H}_i^H \boldsymbol{Y}\|_F^2$, calculated by a false hypothesis channel $\boldsymbol{H}_i$. Thus, the MFN sender detection is written as $\Psi_{\mathrm{MFN}} = \arg\max_{k \in \mathbb{K}} \{\|\boldsymbol{H}_1^H \boldsymbol{Y}\|_F^2, \ldots, \|\boldsymbol{H}_K^H \boldsymbol{Y}\|_F^2\}$.

2) MLE Sender Detection: The philosophy of the MLE detection is to estimate the transmitted signal with different users' channels, and then compute the Euclidean distance between the reconstructed and actual received signal. Explicitly, if the i-th ($i \neq k$) user's channel is used for estimation, a reconstructed signal is given as $\hat{\boldsymbol{Y}}_i = \boldsymbol{H}_i \boldsymbol{H}_i^\dagger \boldsymbol{Y} = \boldsymbol{H}_i \boldsymbol{H}_i^\dagger \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{S}_k + \boldsymbol{H}_i \boldsymbol{H}_i^\dagger \boldsymbol{N}$, where $\boldsymbol{H}_i^\dagger = (\boldsymbol{H}_i^H \boldsymbol{H}_i)^{-1} \boldsymbol{H}_i^H$. Then, the Euclidean distance between the reconstructed and actual received signal is calculated as $D_i = \|\boldsymbol{Y} - \hat{\boldsymbol{Y}}_i\|_F^2 = \|(\boldsymbol{H}_i \boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r}) \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{S}_k + (\boldsymbol{H}_i \boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r}) \boldsymbol{N}\|_F^2$, where $\boldsymbol{H}_k^\dagger = (\boldsymbol{H}_k^H \boldsymbol{H}_k)^{-1} \boldsymbol{H}_k^H$. In a similar vein, when the real sender k's channel is used for detection, the Euclidean distance is computed as $D_k = \|(\boldsymbol{H}_k \boldsymbol{H}_k^\dagger - \boldsymbol{I}_{N_r}) \boldsymbol{N}\|_F^2$. As D_k only contains a noise term, there is a high probability that $D_i > D_k$. Therefore, the MLE sender detection algorithm can be expressed as $\Psi_{\mathrm{MLE}} = \arg\min_{k \in \mathbb{K}} \{\|(\boldsymbol{H}_1 \boldsymbol{H}_1^\dagger - \boldsymbol{I}_{N_r}) \boldsymbol{Y}\|_F^2, \ldots, \|(\boldsymbol{H}_K \boldsymbol{H}_K^\dagger - \boldsymbol{I}_{N_r}) \boldsymbol{Y}\|_F^2\}$.

III. Analysis on Detection Error Rate Performance

In this section, the DER performance of the MFN and MLE detectors is quantified, and associated closed-form yet tight expression expressions are presented.

A. DER Analysis of MFN Detector

Exploiting the MHT problem (2), evidently, DER is the probability of under $\mathcal{H}_k$, the BS falsely declaring either that no signal is received, or that a signal is transmitted from a user other than the k-th user, written as

$$\zeta_{\mathrm{MFN}} = 1 - \Pr(\Gamma(\boldsymbol{Y}) \geq \varepsilon | \mathcal{H}_k) \prod_{i, i \neq k}^{K} \Pr(G_i \leq G_k | \mathcal{H}_k). \tag{3}$$

The term $\Pr(\Gamma(\boldsymbol{Y}) \geq \varepsilon | \mathcal{H}_k)$ represents the probability of under $\mathcal{H}_k$, the BS correctly identifies an incoming signal. The term $\prod_{i, i \neq k}^{K} \Pr(G_i \leq G_k | \mathcal{H}_k)$ represents the probability of the BS correctly identifies user k as the signal sender. For the energy detector, its test statistic $\Gamma(\boldsymbol{Y})$ follows chi-square distribution with $2N_rL$ degree of freedom (DoF) and non-centrality parameter $\frac{2\|\boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{S}_k\|_F^2}{\sigma^2}$ [13]. Hence, the term $\Pr(\Gamma(\boldsymbol{Y}) \geq \varepsilon | \mathcal{H}_k)$ is calculated as

$$\Pr(\Gamma(\boldsymbol{Y}) \geq \varepsilon | \mathcal{H}_k) = 1 - \Pr(\Gamma(\boldsymbol{Y}) < \varepsilon | \mathcal{H}_k) = 1 - \mathcal{C}\left(\tfrac{2N_r \varepsilon L}{\sigma^2}\right), \tag{4}$$

where $\mathcal{C}(\cdot)$ denotes the cumulative distribution function (cdf) of the non-central chi-square distributed variable $\Gamma(\boldsymbol{Y})$. In

$$\Pr(\gamma_i \geq 0|\mathcal{H}_k) = \frac{1}{2}\left(1+\mathrm{erf}\left(\frac{L\sigma^2\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H-\boldsymbol{H}_i\boldsymbol{H}_i^H)+\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{U}_k-\boldsymbol{U}_i^H\boldsymbol{U}_i)}{\sqrt{2L\sigma^4\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{H}_k^H+\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{H}_i^H)+4\sigma^2\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{U}_k+\boldsymbol{U}_i^H\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{U}_i)}}\right)\right). \tag{10}$$

$$\zeta_{MFN} = 1-\left(1-\mathcal{C}\left(\tfrac{2N_r\varepsilon L}{\sigma^2}\right)\right)\prod_{i,i\neq k}^{K}\frac{1}{2}\left(1+\mathrm{erf}\left(\frac{L\sigma^2\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H-\boldsymbol{H}_i\boldsymbol{H}_i^H)+\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{U}_k-\boldsymbol{U}_i^H\boldsymbol{U}_i)}{\sqrt{2L\sigma^4\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{H}_k^H+\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{H}_i^H)+4\sigma^2\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{U}_k+\boldsymbol{U}_i^H\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{U}_i)}}\right)\right). \tag{11}$$

$$\zeta_{MFN} = 1-\prod_{i,i\neq k}^{K}\frac{1}{2}\left(1+\mathrm{erf}\left(\frac{L\sigma^2\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H-\boldsymbol{H}_i\boldsymbol{H}_i^H)+\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{U}_k-\boldsymbol{U}_i^H\boldsymbol{U}_i)}{\sqrt{2L\sigma^4\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{H}_k^H+\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{H}_i^H)+4\sigma^2\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{U}_k+\boldsymbol{U}_i^H\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{U}_i)}}\right)\right). \tag{12}$$

order to calculate the term $\Pr(G_i \leq G_k|\mathcal{H}_k)$, we first need to investigate the statistics of G_k and G_i as summarized in Lemma 1.

Lemma 1: Define $\boldsymbol{U}_i = \boldsymbol{H}_i^H\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{S}_k$. The expectation and variance of G_i are given as

$$\mathbb{E}\{G_i\} = L\sigma^2\mathrm{tr}(\boldsymbol{H}_i\boldsymbol{H}_i^H) + \mathrm{tr}(\boldsymbol{U}_i^H\boldsymbol{U}_i), \tag{5}$$

and

$$\mathbb{V}\{G_i\} = L\sigma^4\mathrm{tr}(\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{H}_i^H) + 2\sigma^2\mathrm{tr}(\boldsymbol{U}_i^H\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{U}_i). \tag{6}$$

Proof of Lemma 1: please see Appendix. ■

The expectation and variance of G_k can be obtained in the same manner. Although the expectation and variance of G_i are given by Lemma 1, it is still difficult to obtain an exact probability density function (pdf) of G_i. The exact pdf of such a quadratic form was presented in [14]. However, it involves complex integration, which limits its application in our DER analysis. Fortunately, as G_i in fact contains the summation of N_rL samples, they can be approximated as Gaussian distributed variables.

Fig. 1 (a) shows that the value of G_i and G_k indeed approximately follow Gaussian distribution. More importantly, G_k and G_i show distinct expectations and variances, which thus can be used to distinguish the two statistics. Defining $\gamma_i = G_k - G_i$, its expectation and variance are

$$\begin{aligned}\mathbb{E}\{\gamma_i\} &= \mathbb{E}\{G_k\} - \mathbb{E}\{G_i\}\\ &= L\sigma^2\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H - \boldsymbol{H}_i\boldsymbol{H}_i^H) + \mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{U}_k - \boldsymbol{U}_i^H\boldsymbol{U}_i),\end{aligned} \tag{7}$$

and

$$\begin{aligned}\mathbb{V}\{\gamma_i\} &= \mathbb{V}\{G_k\} + \mathbb{V}\{G_i\} + \mathrm{cov}\{G_k, G_i\}\\ &= L\sigma^4\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{H}_k^H + \boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{H}_i^H)\\ &\quad + 2\sigma^2\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{H}_k^H\boldsymbol{H}_k\boldsymbol{U}_k + \boldsymbol{U}_i^H\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{U}_i),\end{aligned} \tag{8}$$

where the covariance term $\mathrm{cov}\{G_k, G_i\}$ is ignored because G_k and G_i are weakly correlated. Given that γ_i follows Gaussian distribution, we have

$$\begin{aligned}\Pr(G_i \leq G_k|\mathcal{H}_k) &= \Pr(\gamma_i \geq 0|\mathcal{H}_k)\\ &= \int_0^\infty f_{\gamma_i}(t)\mathrm{d}t = \frac{1}{2}\left(1+\mathrm{erf}\left(\frac{\mathbb{E}(\gamma_i)}{\sqrt{2\mathbb{V}(\gamma_i)}}\right)\right),\end{aligned} \tag{9}$$

where $f_{\gamma_i}(\cdot)$ denotes the pdf of the variable γ_i, and $\mathrm{erf}(\cdot)$ denotes the Gaussian error function. Substituting (7) and (8) into (9), $\Pr(\gamma_i \geq 0|\mathcal{H}_k)$ is rewritten as (10). Substituting (4) and (10) into (3) leads a tight closed-form DER expression of the MFN detector in (11), as shown at the top of this page.

As the term $\mathcal{C}\left(\frac{2N_r\varepsilon L}{\sigma^2}\right)$ approaches 0 when ε is a small value, the miss detection rate can be omitted. According to the Neyman-Pearson criterion, the probability of false alarm may be raised by the small valued ε. However, its effect ca be significantly reduced on account of the multiple antennas at the receiver. Ignoring the effect of miss detection, a tight expression of DER is given as (12), which is shown at the top of this page.

B. DER Analysis of MLE Detector

Recalling the MLE detection, its DER is expressed as

$$\zeta_{\mathrm{MLE}} = 1 - \Pr(\Gamma(\boldsymbol{Y}) \geq \varepsilon|\mathcal{H}_k)\prod_{i,i\neq k}^{K}\Pr(D_i \geq D_k|\mathcal{H}_k). \tag{13}$$

To calculate the term $\Pr(D_i \geq D_k|\mathcal{H}_k)$, we first investigate the distributions of D_k and D_i. For the sake of simplicity, denote $\boldsymbol{\Theta}_i = \boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r}$ and $\boldsymbol{V}_i = \boldsymbol{\Theta}_i\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{S}_k$. The expectation and variance of D_i are summarized in Lemma 2.

Lemma 2: The expectation and variance of D_i are given as

$$\mathbb{E}\{D_i\} = L\sigma^2\mathrm{tr}(\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H) + \mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i), \tag{14}$$

and

$$\mathbb{V}\{D_i\} = L\sigma^4\mathrm{tr}(\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H) + 2\sigma^2\boldsymbol{V}_i^H\boldsymbol{\Theta}_i^H\boldsymbol{\Theta}_i\boldsymbol{V}_i. \tag{15}$$

The proof of Lemma 2 is similar to that of Lemma 1, and thus is omitted due to page limit. ■

Similarly, the expectation and variance of D_k are calculated as

$$\mathbb{E}\{D_k\} = L\sigma^2\mathrm{tr}(\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H), \tag{16}$$

and

$$\mathbb{V}\{D_k\} = L\sigma^4\mathrm{tr}(\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H). \tag{17}$$

Again leveraging the central limit theorem, D_i and D_k are approximated to follow Gaussian distribution. Fig. 1 (b) demonstrates that, the approximated Gaussian variables indeed match the actual simulation results. Defining $\rho_i = G_k - G_i$, its expectation is

$$\begin{aligned}\mathbb{E}\{\rho_i\} &= \mathbb{E}\{D_k\} - \mathbb{E}\{D_i\}\\ &= L\sigma^2\mathrm{tr}(\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H - \boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H) - \mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i).\end{aligned} \tag{18}$$

Since it is easy to find that $\mathrm{tr}(\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H - \boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H) = 0$, (18) can be simplified into

$$\mathbb{E}\{\rho_i\} = -\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i). \tag{19}$$

The variance of ρ_i is

$$\begin{aligned}\mathbb{V}\{\rho_i\} &= \mathbb{V}\{D_k\} + \mathbb{V}\{D_i\} + \mathrm{cov}\{D_k, D_i\}\\ &= L\sigma^4\mathrm{tr}(\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H + \boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H)\\ &\quad + 2\sigma^2\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{\Theta}_i^H\boldsymbol{\Theta}_i\boldsymbol{V}_i),\end{aligned} \tag{20}$$

where the covariance term $\mathrm{cov}\{D_k, D_i\}$ is ignored because D_k and D_i are weakly correlated. With simple manipulations, it proves that $\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H = \boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H$ and $\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H = \boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H$. Thus, (20) can be simplified into

$$\mathbb{V}\{\rho_i\} = L\sigma^4\mathrm{tr}(\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H + \boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H) + 2\sigma^2\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i). \tag{21}$$

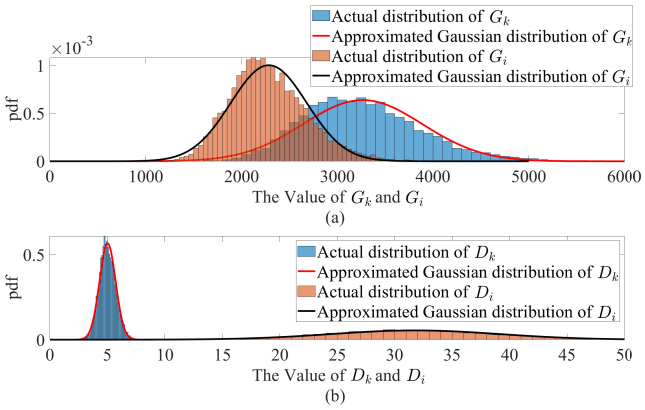

Fig. 1. The actual and approximated pdfs of the values of G_k, G_i, D_k and D_i. MMSE precoder is employed by the sender [9], SNR is set to 10 dB.

Since ρ_i follows Gaussian distribution, the value of $\Pr(\rho_i \leq 0|\mathcal{H}_k)$ can be calculated by the cdf of ρ_i as

$$\Pr(\rho_i \leq 0|\mathcal{H}_k) = \int_{-\infty}^{0} f_{\rho_i}(t)\mathrm{d}t \quad = \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{0-\mathbb{E}(\rho_i)}{\sqrt{2\mathbb{V}(\rho_i)}}\right)\right), \tag{22}$$

where $f_{\rho_i}(\cdot)$ denotes the pdf of ρ_i. Substituting (19) and (21) into (22), $\Pr(\rho_i \leq 0|\mathcal{H}_k)$ is rewritten as

$$\Pr(\rho_i \leq 0|\mathcal{H}_k) = \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i)}{\sqrt{2L\sigma^4\mathrm{tr}(\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H+\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H)+4\sigma^2\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i)}}\right)\right). \tag{23}$$

Substituting (4) and (23) into (13) leads to a tight expression of ζ_{MLE} as

$$\zeta_{\mathrm{MLE}} = 1 - \prod_{i,i\neq k}^{K} \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i)}{\sqrt{2L\sigma^4\mathrm{tr}(\boldsymbol{\Theta}_i\boldsymbol{\Theta}_i^H+\boldsymbol{\Theta}_k\boldsymbol{\Theta}_k^H)+4\sigma^2\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i)}}\right)\right). \tag{24}$$

With the closed-form DER, we are able to conclude a series important remarks below.

Remark 1: For classic anonymity-agnostic precoders, their design principles can be rate, user fairness, weighted signal to interference plus noise ratio (SINR) maximization, or power minimization. Since the value of $\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i)$ is typically a non-zero finite valued number, a small or moderate value of noise variance makes the value of the erf function in (24) approach 1, meaning that the receiver can correctly reveal the real sender. In a different manner, the anonymous precoder manipulates the signaling pattern to let the value of $\mathrm{tr}(\boldsymbol{V}_i^H\boldsymbol{V}_i)$ approach 0. As a result, the user j acts as an alias sender, and makes the receiver fail to distinguish the real sender k and alias j. The resulted DER equals to 0.5. Evidently, for achieving a better DER performance, one needs to add more anonymous constraints, and lets the associated value of $\mathrm{tr}(\boldsymbol{V}_j^H\boldsymbol{V}_j)$ approach 0.

Remark 2: As for the closed-form DER of MFN detector in (12), the value of the term $\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{U}_k - \boldsymbol{U}_i^H\boldsymbol{U}_i)$ is typically a non-zero finite valued number, when classic anonymity-agnostic precoders are employed. As the term $\mathrm{tr}(\boldsymbol{H}_k\boldsymbol{H}_k^H - \boldsymbol{H}_i\boldsymbol{H}_i^H)$ approaches 0, a small value of noise variance makes the value of the erf function in (12) approach 1, resulting to the DER of the MFN detector approaching 0. Hence, the principle of the anonymous precoder against the MFN detector is to manipulate the term $\mathrm{tr}(\boldsymbol{U}_k^H\boldsymbol{U}_k - \boldsymbol{U}_i^H\boldsymbol{U}_i)$, and makes it approach or even less than 0. As a result, the value of the erf function in (12) approaches or is less than 0, thus scrambling the DER performance.

Remark 3: With a large value of block length L, the value of DER is effectively reduced. A special case would be $L \to \infty$, it makes the erf function in (12) and (24) to approach 1, and thus both ζ_{MFN} and ζ_{MLE} approach 0. In other words, with more samples for sender detection, it becomes easier for both MFN and MLE detectors to identify the sender. A high level of signal-to-noise ratio (SNR) makes the value of the erf function in (12) and (24) approach 1, resulting in better DER performance of MFN and MLE detectors. The observation is intuitive, as the detection performance can be improved with a smaller value of noise.

Remark 4: As shown in subsection II-B , the principles of the MFN and MLE detectors are exploiting the difference of the users' CSI for sender detection. Hence, the DER performance is significantly dependent of the channel correlation among users. When two users' channels are strongly correctly, G_k and G_i (D_k and D_i) will have similar value of expectation and variance. It becomes difficult for the receiver to distinguish those two users.

Remark 5: The MLE detector identifies the sender by exploiting the difference in distributions of D_k and D_i. As shown in subsection II-B, D_i $(\forall i \neq k)$ involves the term $(\boldsymbol{H}_i\boldsymbol{H}_i^\dagger - \boldsymbol{I}_{N_r})\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{S}_k$ and colored noise, while D_k only contains a colored noise. This leads to a significant difference in their expectation and variance, as shown in Fig. 1 (b). However, for the MFN detector, both G_k and G_i contain the signal related term and colored noise, as shown in subsection II-B. As a result, the detection accuracy of MFN detector is inferior to that of the MLE detector.

IV. Simulation Results

To verify the tightness of the analytic analysis, Monte Carlo simulation is carried out. Quadrature phase shift keying (QPSK) is used in modulation. Assume that there are $K = 5$ users, and the communication user is randomly generated per slot. The energy detection threshold is $\varepsilon = 10^{-2}$, and the antenna configuration of the BS and the user is $N_r = 9$ and $N_t = 8$ respectively. We normalize the maximum power $p_{\max} = 1$ watt, while changing SNR by tuning the noise power. Assume that the block size $L = 50$. Consider Rayleigh block fading MIMO channel, we select the following classic precoders: 1) MMSE precoder [9], 2) SVD precoder [10], 3) PM precoder [11], 4) constructive interference (CI) precoder [15], 5) CI-based anonymous (CIA) precoder [5]. Note that CI and CIA precoders perform at symbol level, while others perform at block level. Also, the CIA is an anonymous precoder, which manipulates the transmitted signal for masking the real sender.

Fig. 2 (a) shows the closed-form and actual DER results of the MFN detector. It can be observed that the closed-form DER is close to the actual DER regardless of the employed precoders and SNR statuses. Typically, with a generic precoder,

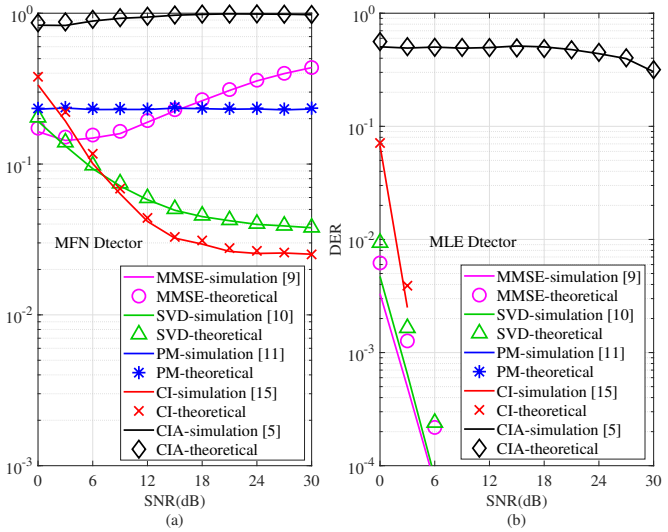

Fig. 2. The impact of receive SNR on the DER by different precoders. $N_t = 8$, $N_r = 9$. The SINR of each receive antenna of the PM precoder is set to 5 dB. The anonymous related thresholds of CIA (MFN) and CIA (MLE) precoder are set to 2 and 0.01.

the deviation between the closed-form and actual DER results are on the levels of 0∼0.05. Also, it proves that anonymous CIA precoder obtains better DER performance than other anonymity-agnostic precoders. It validates our analysis in Remark 1 that, by manipulating transmitted signaling pattern, the DER performance of sender detection can be scrambled.

Fig. 2 (b) shows the closed-form and actual DER results of the MLE detector. It can be seen that the closed-form DER is also close to the actual DER regardless of the employed precoders and SNR statuses. Analogous to the MFN detection, the deviation between the closed-form and actual DER results of the MLE detection are on the same levels of 0∼0.05. In addition, it shows that the detection accuracy of the MLE detector is better then that of the MFN detector, validating the analysis in Remark 1. Also, the anonymous CIA precoder obtains better DER performance against the MLE detector, effectively protecting user anonymity as we discussed in Remark 1.

V. Conclusion

In this letter, the DER performance of two classic PHY sender detectors has been theoretically analyzed, and their tight closed-form expressions have been derived. Based on the analytic DER result, we have theoretically built the relation between the instantaneous signaling pattern and the statistical DER performance for generic precoders applied at the sender side. In addition, a series of important properties have been presented, such as the impact of blocklength, noise status, and precoder on the DER performance. Finally, we have benchmarked the derived closed-form DER against actual simulation results, and the tightness of the derived closed-form results has been verified.

Appendix
Proof of Lemma 1

Denote $\boldsymbol{y}_{(j)}$, $\boldsymbol{u}_{i(j)}$ and $\boldsymbol{\mu}_{(j)}$ as the j-th column of $\boldsymbol{Y}$, $\boldsymbol{U}_i$ and $\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{S}_k$, respectively. We have that $G_i = \|\boldsymbol{H}_i^H\boldsymbol{Y}\|_F^2 = \sum_{j=1}^{L}\|\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\|_2^2$, where $\boldsymbol{y}_{(j)} \sim \mathcal{N}(\boldsymbol{\mu}_{(j)}, \boldsymbol{\Lambda})$ and $\boldsymbol{\Lambda} = \sigma^2\boldsymbol{I}_{N_r}$. Since each term $\|\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\|_2^2$ is quadratic with respect to $\boldsymbol{y}_{(j)}$, the expectation of $\|\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\|_2^2$ can be calculated as

$$\begin{aligned}&\mathbb{E}\{\|\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\|_2^2\} = \mathbb{E}\{\boldsymbol{y}_{(j)}^H\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\}\\ &= \mathbb{E}\{\mathrm{tr}(\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\boldsymbol{y}_{(j)}^H)\} = \mathrm{tr}(\boldsymbol{H}_i\boldsymbol{H}_i^H\mathbb{E}\{\boldsymbol{y}_{(j)}\boldsymbol{y}_{(j)}^H\})\\ &= \sigma^2\mathrm{tr}(\boldsymbol{H}_i\boldsymbol{H}_i^H) + \boldsymbol{u}_{i(j)}^H\boldsymbol{u}_{i(j)}.\end{aligned} \tag{25}$$

Now we use the moment generating function (MGF) to calculate the variance of $\|\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\|_2^2$. Let $\boldsymbol{D}(t) = \boldsymbol{I}_{N_r} - 2t\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{\Lambda}$, and the MGF of $\boldsymbol{y}_{(j)}^H\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}$ is written as $M(t)=|\boldsymbol{D}|^{-\frac{1}{2}}e^{-\frac{1}{2}[\boldsymbol{I}_{N_r}-\boldsymbol{D}^{-1}(t)]\boldsymbol{\Lambda}^{-1}\boldsymbol{\mu}_{(j)}}$. We further let $k(t) = \ln(M(t))$, and denote its second-order derivative as $k''(t)$. Substituting the value of $|\boldsymbol{D}|_{t=0}$, $\frac{\mathrm{d}|\boldsymbol{D}|}{\mathrm{d}t}|_{t=0}$, $\frac{\mathrm{d}^2|\boldsymbol{D}|}{\mathrm{d}t^2}|_{t=0}$, $\boldsymbol{D}|_{t=0}$, $\boldsymbol{D}^{-1}|_{t=0}$, $\frac{\mathrm{d}\boldsymbol{D}}{\mathrm{d}t}|_{t=0}$ and $\frac{\mathrm{d}^2\boldsymbol{D}}{\mathrm{d}t^2}|_{t=0}$ into $k''(t)$, we have

$$\begin{aligned}&\mathbb{V}\{\|\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\|_2^2\} = k''(0)\\ &= \sigma^4\mathrm{tr}(\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{H}_i^H) + 2\sigma^2\boldsymbol{u}_{i(j)}^H\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{u}_{i(j)}.\end{aligned} \tag{26}$$

Considering the block length L, the expectation and variance of G_i are

$$\mathbb{E}\{G_i\} = \sum_{j=1}^{L}\mathbb{E}\{\|\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\|_2^2\} = L\sigma^2\mathrm{tr}(\boldsymbol{H}_i\boldsymbol{H}_i^H) + \mathrm{tr}(\boldsymbol{U}_i^H\boldsymbol{U}_i), \tag{27}$$

and

$$\begin{aligned}\mathbb{V}\{G_i\} &= \sum_{j=1}^{L}\mathbb{V}\{\|\boldsymbol{H}_i^H\boldsymbol{y}_{(j)}\|_2^2\}\\ &= L\sigma^4\mathrm{tr}(\boldsymbol{H}_i\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{H}_i^H) + 2\sigma^2\mathrm{tr}(\boldsymbol{U}_i^H\boldsymbol{H}_i^H\boldsymbol{H}_i\boldsymbol{U}_i).\end{aligned} \tag{28}$$

References

[1] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Industr. Inform.*, vol. 16, no. 3, pp. 1984–1992, 2020.

[2] S. Tangade, S. S. Manvi, and P. Lorenz, "Trust management scheme based on hybrid cryptography for secure communications in vanets," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5232–5243, 2020.

[3] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7252–7267, 2018.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017.

[5] Z. Wei, F. Liu, C. Masouros, and H. V. Poor, "Fundamentals of physical layer anonymous communications: Sender detection and anonymous precoding," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 64–79, 2022.

[6] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 912–925, 2018.

[7] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, 2013.

[8] M. Sayad Haghighi and Z. Aziminejad, "Highly anonymous mobility-tolerant location-based onion routing for vanets," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2582–2590, 2020.

[9] A. Wiesel, Y. C. Eldar, and S. Shamai, "Zero-forcing precoding and generalized inverses," *IEEE Trans. Signal Process.*, vol. 56, no. 9, pp. 4409–4418, 2008.

[10] F. Sohrabi and W. Yu, "Hybrid digital and analog beamforming design for large-scale antenna arrays," *IEEE J. Sel. Top. Signal Process.*, vol. 10, no. 3, pp. 501–513, 2016.
[11] R. López-Valcarce and N. González-Prelcic, "Hybrid beamforming designs for frequency-selective mmwave mimo systems with per-rf chain or per-antenna power constraints," *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 5770–5784, 2022.
[12] Z. Wei, C. Masouros, P. Wang, X. Zhu, J. Wang, and A. P. Petropulu, "Physical layer anonymous precoding design: From the perspective of anonymity entropy," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 11, pp. 3224–3238, 2022.
[13] E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio : State-of-the-art and recent advances," *IEEE Trans. Signal Process.*, vol. 29, no. 3, pp. 101–116, 2012.
[14] T. Y. Al-Naffouri, M. Moinuddin, N. Ajeeb, B. Hassibi, and A. L. Moustakas, "On the distribution of indefinite quadratic forms in gaussian random variables," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 153–165, 2016.
[15] C. Masouros and G. Zheng, "Exploiting known interference as green signal power for downlink beamforming optimization," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3628–3640, 2015.