Practical Secrecy using Artificial Noise

Shuiyin Liu, Yi Hong, and Emanuele Viterbo

***Abstract*—In this paper, we consider the use of artificial noise for secure communications. We propose the notion of *practical secrecy* as a new design criterion based on the behavior of the eavesdropper's error probability P_{E}, as the signal-to-noise ratio goes to infinity. We then show that the *practical secrecy* can be guaranteed by the randomly distributed artificial noise with specified power. We show that it is possible to achieve *practical secrecy* even when the eavesdropper can afford more antennas than the transmitter.**

***Index Terms*—Physical layer security, lattices, wiretap channel, artificial noise.**

I. Introduction

THE *broadcast* characteristic of wireless communication systems results in enormous challenges in securing transmitted data in the presence of eavesdroppers. The eavesdropper is commonly assumed to be passive and its location is unknown to the transmitter. In current wireless systems, secure communication mainly depends on the network layer cryptographic technologies. Information theoretic results show that it is possible to secure the data by employing physical layer strategy [1], when the intended receiver has a better channel than the eavesdropper. The secrecy capacity is thus defined to measure the difference between the capacities of the intended user and the eavesdropper [2].

A recently proposed physical layer security scheme makes use of artificial noise to degrade the eavesdropper's reception [3]. The intended user is unaffected, so that a non-zero secrecy rate is ensured. The approach assumes a Gaussian artificial noise and requires that the number of eavesdropper antennas N_{E} is strictly smaller than the number of transmitter antennas N_{A}. In this paper we tackle this problem. To overcome the restriction $N_{\mathrm{E}} < N_{\mathrm{A}}$, we aim at maximizing the eavesdropper's error probability, defined by P_{E}, rather than the secrecy rate. Hence, we define the notion of *practical secrecy* as $P_{\mathrm{E}} \to 1$ exponentially as the number of receiver antennas $N_{\mathrm{B}} \to \infty$, for any signal-to-noise ratio (SNR) at the eavesdropper. The proposed criterion is different from the *secrecy gain* introduced in [4], where $P_{\mathrm{E}} \to 0$ for high eavesdropper SNR. More importantly, we propose the *covering ratio* as a fundamental secrecy parameter which guarantees the convergence of P_{E} and characterizes the amount of the artificial noise required. Furthermore, we propose lattice precoding to improve performance over singular value decomposition (SVD) precoding used in [3].

The paper is organized as follows: Section II presents the transmission model and lattice basics. The SVD precoding and the lattice precoding are given in Section III. In Section IV, *practical secrecy* is addressed. Section V presents some simulation results. Some concluding remarks are drawn in Section VI. Proofs of the theorems are given in Appendix.

Notation: Matrices and column vectors are denoted by upper and lowercase boldface letters, and the transpose, inverse, pseudoinverse of a matrix $\mathbf{B}$ by $\mathbf{B}^T$, $\mathbf{B}^{-1}$, and $\mathbf{B}^{\dagger}$, respectively. $X \to Y$ denotes that random variable X converges to random variable Y in distribution. We use the standard asymptotic notation $f(x) = O(g(x))$, when $\limsup_{x\to\infty} |f(x)/g(x)| < \infty$. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$ and $\mathbb{Z}[i]$ represent the real, complex, integer and complex integer numbers, respectively.

II. System Model and Lattice Preliminary

We consider the multiple-input multiple-output (MIMO) wiretap channel using the *M*-QAM signalling. The precoding and decoding problems in this system can be easily modeled using lattices [5][6]. In what follows, the system model is introduced first, followed by some lattice preliminaries that are relevant to this paper.

A. System Model

Consider a MIMO wiretap system including three terminals: a transmitter Alice, an intended receiver Bob, and a passive eavesdropper Eve, which are equipped with N_{A}, N_{B} and N_{E} antennas, respectively. Bob and Eve receive

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n}_{\mathrm{B}}, \tag{1}$$

$$\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{n}_{\mathrm{E}}, \tag{2}$$

respectively, where $\mathbf{n}_{\mathrm{B}} \in \mathbb{C}^{N_{\mathrm{B}}\times 1}$ and $\mathbf{n}_{\mathrm{E}} \in \mathbb{C}^{N_{\mathrm{E}}\times 1}$ are the complex white Gaussian noise vectors with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{B}}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{E}}^2)$, respectively. Assuming Bob and Eve are not co-located, then the mutually independent matrices $\mathbf{H} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{A}}}$ and $\mathbf{G} \in \mathbb{C}^{N_{\mathrm{E}}\times N_{\mathrm{A}}}$ represent the channels from Alice to Bob and Alice to Eve, respectively, where the entries are assumed to be i.i.d. circularly symmetric Gaussian random variable $\sim \mathcal{N}_{\mathbb{C}}(0,\, 1)$.

We assume $N_{\mathrm{B}} < N_{\mathrm{A}}$, so that $\mathbf{H}$ has a non-trivial null space generated by the columns of the matrix $\mathbf{Z} = \mathrm{null}(\mathbf{H})$. Let $\mathbf{u}$ be the secret data vector. Using the artificial noise technique, Alice sends

$$\mathbf{x} = \mathbf{P}\mathbf{u} + \mathbf{Z}\mathbf{v}, \tag{3}$$

where $\mathbf{P}$ is the precoding matrix and $\mathbf{v}$ is the artificial noise generated by Alice. Considering uniform M-QAM signalling,

Manuscript received March 13, 2013. The associate editor coordinating the review of this letter and approving it for publication was W. Xu.

The authors are with the Department of Electrical and Computer Systems Engineering, Monash University, Melbourne VIC 3180, Australia (e-mail: {shuiyin.liu, yi.hong, emanuele.viterbo}@monash.edu).

This work was performed at the Monash Software Defined Telecommunications Lab. The authors were supported by the Monash Professional Fellowship, the 2013 Monash Faculty of Engineering Seed Funding Scheme, and the Australian Research Council Discovery grants (ARC DP130100336).

Digital Object Identifier 10.1109/LCOMM.2013.052013.130556

we have the secret data $\Re(\mathbf{u})$ and $\Im(\mathbf{u}) \in \mathcal{C}^{N_\mathrm{B}}$, where $\mathcal{C} = \{-\sqrt{M}+1,\ -\sqrt{M}+3\ \ldots, \sqrt{M}-1\}$. The total transmit power is constrained to P, i.e., $\mathrm{E}[||\mathbf{x}||^2] \leq P$.

Then, (1) and (2) can be rewritten as

$$\mathbf{z} = \mathbf{HPu} + \mathbf{n}_\mathrm{B} \quad (4)$$

$$\mathbf{y} = \mathbf{GPu} + \mathbf{GZv} + \mathbf{n}_\mathrm{E}. \quad (5)$$

We consider the worse case for Alice where Eve not only knows the channel matrices $\mathbf{H}$ and $\mathbf{G}$, but also knows the matrix $\mathbf{Z}$ and the precoding matrix $\mathbf{P}$. Alice is assumed to know only $\mathbf{H}$. The SNR of Eve is defined as $\mathrm{SNR}_\mathrm{E} \triangleq P/\sigma_\mathrm{E}^2$. From (4) and (5), through the interference term $\mathbf{GZv}$, we can see that $\mathbf{v}$ affects Eve, but not Bob.

B. Lattice Preliminary

An n-dimensional real *lattice* in an m-dimensional Euclidean space $\mathbb{R}^m$ ($n \leq m$) is the set of integer linear combinations of n independent vectors:

$$\Lambda_\mathbb{R} = \{\mathbf{Bu} : \mathbf{u} \in \mathbb{Z}^n\},$$

where $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$ is a *basis* of the lattice $\Lambda_\mathbb{R}$.

In the following, we introduce some lattice parameters which are related to this work.

A *shortest vector* of $\Lambda_\mathbb{R}$ is a non-zero vector in $\Lambda_\mathbb{R}$ with the smallest Euclidean norm. The length of the shortest vector is denoted by $\lambda_1(\mathbf{B})$.

The *Voronoi region* of a lattice point $\mathbf{x}_i$ is denoted by:

$$\mathcal{V}(\Lambda_\mathbb{R}) = \{\mathbf{y} \in \mathbb{R}^m : \|\mathbf{y} - \mathbf{x}_i\| \leq \|\mathbf{y} - \mathbf{x}_j\|, \forall\ \mathbf{x}_i \neq \mathbf{x}_j\}.$$

The determinant of $\Lambda_\mathbb{R}$, $\det(\Lambda_\mathbb{R}) \triangleq \sqrt{\det(\mathbf{B}^T\mathbf{B})}$, gives the n-dimensional volume of $\mathcal{V}(\Lambda_\mathbb{R})$.

In Fig. 1, we illustrate two important lattice parameters which are related to $\mathcal{V}(\Lambda_\mathbb{R})$:

1) the *effective radius* of $\Lambda_\mathbb{R}$, denoted by $r_\mathrm{eff}(\Lambda_\mathbb{R})$, is the radius of a sphere $\mathcal{S}_\mathrm{eff}(\Lambda_\mathbb{R})$ of volume $\det(\Lambda_\mathbb{R})$ [7]. For large n, it is approximately

$$r_\mathrm{eff}(\Lambda_\mathbb{R}) \approx \sqrt{n/(2\pi e)}\,\det(\Lambda_\mathbb{R})^{1/n};$$

2) the *covering radius* of $\Lambda_\mathbb{R}$, denoted by $r_\mathrm{cov}(\Lambda_\mathbb{R})$, is the radius of the smallest sphere centred at a lattice point which covers $\mathcal{V}(\Lambda_\mathbb{R})$.

In wireless communication, it is common to use complex number representation of signals. The real lattice definition can be extended to complex:

$$\Lambda_\mathbb{C} = \{\mathbf{B}_\mathbb{C}\mathbf{u}_\mathbb{C} : \mathbf{u}_\mathbb{C} \in \mathbb{Z}[i]^n\},$$

where $\mathbf{B}_\mathbb{C} \in \mathbb{C}^{m \times n}$ is a *basis* of the *complex lattice* $\Lambda_\mathbb{C}$. There is a simple way to represent n-dimensional complex lattices as $2n$-dimensional real lattices [8]. In this work, when we use the lattice parameters of $\Lambda_\mathbb{C}$ (e.g., $\mathcal{V}(\Lambda_\mathbb{C})$), we first convert $\Lambda_\mathbb{C}$ to the real equivalent $\Lambda_\mathbb{R}$, and then apply the corresponding definitions of $\Lambda_\mathbb{R}$.

From the lattice viewpoint, $\mathbf{GPu}$ in (5) can be described as a point of the lattice with a basis $\mathbf{GP}$. The detection of $\mathbf{u}$ fits in the lattice decoding scenario and can be solved by sphere decoding [9]. In this paper, we assume the worst-case for Alice and Bob, where Eve is able to perform maximum likelihood decoding (e.g., by sphere decoding) to estimate $\mathbf{u}$, even if the average complexity grows exponentially with the lattice dimension.

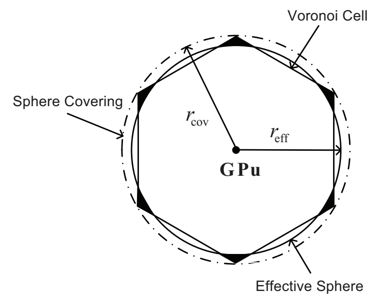

Fig. 1. Voronoi Cell, Effective Radius and Covering Radius.

III. Precoding for Secure Communication

In this Section, we analyze two different precoding schemes for the artificial noise strategy: SVD precoding and lattice precoding.

For the MIMO scenario, the original artificial noise stragegy [3] uses SVD precoding, where $\mathbf{H} = \mathbf{U\Lambda V}^T$, $\mathbf{V} = [\mathbf{V}_1, \mathbf{Z}]$ and $\mathbf{P} = \mathbf{V}_1$. Due to the orthogonality between $\mathbf{P}$ and $\mathbf{Z}$, from (3), the total transmission power is

$$||\mathbf{x}_\mathrm{SVD}||^2 = ||\mathbf{u}||^2 + ||\mathbf{v}_\mathrm{SVD}||^2. \quad (6)$$

Different from SVD precoding, lattice precoding [5] transmits

$$\mathbf{x}_\mathrm{LP} = \mathbf{H}^\dagger(\mathbf{u} - A\hat{\mathbf{w}}) + \mathbf{Zv}, \quad (7)$$

where $A = 2\sqrt{M}$ and

$$\hat{\mathbf{w}} = \arg \min_{\mathbf{w} \in \mathbb{Z}[i]^{N_\mathrm{B}}} \|\mathbf{H}^\dagger(\mathbf{u} - A\mathbf{w})\|^2. \quad (8)$$

Hence the corresponding transmission power is

$$||\mathbf{x}_\mathrm{LP}||^2 = ||\mathbf{H}^\dagger(\mathbf{u} - A\hat{\mathbf{w}})||^2 + ||\mathbf{v}_\mathrm{LP}||^2. \quad (9)$$

The search in (8) requires the use of sphere decoder. To speed up the search process, we apply the lattice reduction aided successive interference cancellation (LR-SIC) precoding [10], in which $\hat{\mathbf{w}}$ is approximated by Babai's nearest plane algorithm [11].

In the next Section, we will show that lattice precoding outperforms SVD precoding by requiring lower artificial noise power.

IV. Practical Secrecy

In this Section, we propose a new artificial noise strategy to overcome the limitation of $N_\mathrm{E} < N_\mathrm{A}$ and the assumption of Gaussian artificial noise in [3]. Instead of targeting a non-zero secrecy rate, the proposed scheme aims to maximize Eve's error probability $P_\mathrm{E} \triangleq \Pr(\hat{\mathbf{u}}_\mathrm{E} \neq \mathbf{u})$.

A. Practical Secrecy

Let $\hat{\mathbf{u}}_\mathrm{E}$ be the estimated secret message at Eve. We propose a new measure of secrecy in terms of P_E.

Definition 1: We say *practical secrecy* is achieved if for any SNR_E, $P_\mathrm{E} \to 1$ exponentially as $N_\mathrm{B} \to \infty$.

The traditional secrecy capacity criterion, is based on the assumption of a Gaussian input alphabet. On the contrary, *practical secrecy* is proposed for the practical communication systems, which make use of a finite alphabet (e.g., M-QAM).

To the best of the authors' knowledge, no scheme has been proposed in the literature to achieve *practical secrecy*. In the following, we will evaluate the relationship between *practical secrecy* and $\mathbf{v}$ under the assumption that Eve can perform maximum likelihood decoding.

B. Achieving Practical Secrecy

Consider the lattice $\Lambda_{\mathbb{C}}$ with a basis $\mathbf{GP}$. The decoding region of the target lattice point $\mathbf{GPu}$ is its associated $\mathcal{V}(\Lambda_{\mathbb{C}})$. Therefore, P_{E} is determined by whether $\mathbf{y}$ in (5) belongs to $\mathcal{V}(\Lambda_{\mathbb{C}})$ or not. Let $\tilde{\mathbf{n}}_{\mathrm{E}} = \mathbf{GZv} + \mathbf{n}_{\mathrm{E}}$ be Eve's generalized noise term. For a given $\mathbf{v}$, the entries of $\tilde{\mathbf{n}}_{\mathrm{E}}$ are i.i.d. random variables $\sim \mathcal{N}_{\mathbb{C}}(0, \tilde{\sigma}_{\mathrm{E}}^2)$ with $\tilde{\sigma}_{\mathrm{E}}^2 = ||\mathbf{v}||^2 + \sigma_{\mathrm{E}}^2$. A salient feature is that Eve's channel noise $\mathbf{n}_{\mathrm{E}}$ can help Alice to save on the artificial noise power. In this work, we consider the worst-case scenario, i.e., $\sigma_{\mathrm{E}}^2 \to 0$, so that P_{E} only depends on $\mathbf{GZv}$ and is independent of $\mathrm{SNR}_{\mathrm{E}}$.

As shown in Fig. 1, if the interference term $||\mathbf{GZv}|| \geq r_{\mathrm{cov}}(\Lambda_{\mathbb{C}})$, then $\mathbf{y} \notin \mathcal{V}(\Lambda_{\mathbb{C}})$, so that $P_{\mathrm{E}} = 1$. If

$$\frac{r_{\mathrm{cov}}(\Lambda_{\mathbb{C}})}{r_{\mathrm{eff}}(\Lambda_{\mathbb{C}})} \geq \frac{||\mathbf{GZv}||}{r_{\mathrm{eff}}(\Lambda_{\mathbb{C}})} > 1, \tag{10}$$

there are two cases: $P_{\mathrm{E}} = 1$ when $\mathbf{y} \in \bar{\mathcal{S}}_{\mathrm{eff}}(\Lambda_{\mathbb{C}}) - \mathcal{V}(\Lambda_{\mathbb{C}})$ and $P_{\mathrm{E}} = 0$ when $\mathbf{y} \in \mathcal{V}(\Lambda_{\mathbb{C}}) - \mathcal{S}_{\mathrm{eff}}(\Lambda_{\mathbb{C}})$ (the shaded corners), where $\bar{\mathcal{S}}_{\mathrm{eff}}(\Lambda_{\mathbb{C}})$ is the complement of $\mathcal{S}_{\mathrm{eff}}(\Lambda_{\mathbb{C}})$. As $||\mathbf{GZv}||$ approaches $r_{\mathrm{cov}}(\Lambda_{\mathbb{C}})$, the shaded corners will disappear. In other words, Eve has a higher error floor as $||\mathbf{GZv}||$ increases from $r_{\mathrm{eff}}(\Lambda_{\mathbb{C}})$ to $r_{\mathrm{cov}}(\Lambda_{\mathbb{C}})$. Note that the idea is directly applicable to lattice precoding, where the target lattice point $\mathbf{GPu}$ is simply replaced by the lattice point $\mathbf{GH}^{\dagger}(\mathbf{u}-A\hat{\mathbf{w}})$. The secret data therefore becomes $\mathbf{u}-A\hat{\mathbf{w}}$.

Inspired by (10), we now introduce a new secrecy parameter related to P_{E}.

Definition 2: The *covering ratio* is defined as

$$c_{\mathrm{R}} \triangleq \frac{||\mathbf{GZv}||}{r_{\mathrm{eff}}(\Lambda_{\mathbb{C}})}. \tag{11}$$

The c_{R} and P_{E} are related by the following theorem.

Theorem 1: For $c_{\mathrm{R}} \geq \pi e$ and $N_{\mathrm{B}} \to \infty$, $P_{\mathrm{E}} = 1$ for any value of $\mathrm{SNR}_{\mathrm{E}}$.

Proof: See Appendix A. ■

To apply Theorem 1, we need to find the sufficient condition of $c_{\mathrm{R}} \geq \pi e$. Since c_{R} is a random variable depending on the random channel matrix $\mathbf{G}$, the problem then reduces to finding the sufficient condition on $\Pr\{c_{\mathrm{R}} < \beta\} \to 0$ for some $\beta > 0$.

Theorem 2: For $N_{\mathrm{B}} \to \infty$, let $||\mathbf{v}|| = \beta e/\Phi$, where

$$\Phi_{\mathrm{LP}} = \left[\frac{(N_{\mathrm{E}} - N_{\mathrm{B}})!}{(N_{\mathrm{A}} - N_{\mathrm{B}})!} \cdot \frac{N_{\mathrm{A}}!}{N_{\mathrm{E}}!}\right]^{\frac{1}{2N_{\mathrm{B}}}} \quad \text{for lattice precoding} \tag{12}$$

$$\Phi_{\mathrm{SVD}} = \left[\frac{(N_{\mathrm{E}} - N_{\mathrm{B}})!}{N_{\mathrm{E}}!}\right]^{\frac{1}{2N_{\mathrm{B}}}} \quad \text{for SVD precoding} \tag{13}$$

then

$$\Pr\{c_{\mathrm{R}} < \beta\} \leq O\left(e^{-\min(N_{\mathrm{B}}^2/\log(N_{\mathrm{B}}),\, N_{\mathrm{E}})}\right). \tag{14}$$

Proof: See Appendix B. ■

From Theorem 1 with $\beta = \pi e$ and 2, the convergence behavior of $\Pr\{c_{\mathrm{R}} < \pi e\}$ implies $P_{\mathrm{E}} \to 1$ exponentially as $N_{\mathrm{B}} \to \infty$.

Remark 1: Practical secrecy is achieved when $||\mathbf{v}|| \geq \pi e^2/\Phi$, where Φ is given in (12) and (13), depending on precoders.

Remark 2: Since $\Phi_{\mathrm{SVD}} < \Phi_{\mathrm{LP}}$, $||\mathbf{v}_{\mathrm{SVD}}|| > ||\mathbf{v}_{\mathrm{LP}}||$.

As shown above, *practical secrecy* is only related to $||\mathbf{v}||$. However, if $\mathbf{v}$ is an integer vector, the term $\tilde{\mathbf{x}} = \mathbf{GPu} + \mathbf{GZv}$ in (5) can be viewed as a lattice point of $\tilde{\Lambda}_{\mathbb{C}}$ with a basis $[\mathbf{GP}, \mathbf{GZ}]$, so that Eve may be able to recover $\tilde{\mathbf{x}}$ by using sphere decoding. To avoid this, we generate a continuous random vector $\mathbf{v}$, so that $\tilde{\mathbf{x}}$ can never be a lattice point of $\tilde{\Lambda}_{\mathbb{C}}$, hence can not be detected.

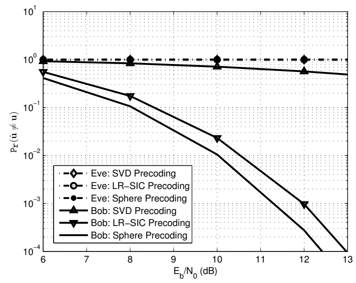

Fig. 2. $\Pr(\hat{\mathbf{u}} \neq \mathbf{u})$ vs. Bob's average SNR per bit for the uncoded MIMO system with $N_{\mathrm{A}} = 10$, $N_{\mathrm{B}} = 9$, $N_{\mathrm{E}} = 20$, 64-QAM and $\mathrm{SNR}_{\mathrm{E}} \to \infty$.

Since *practical secrecy* requires that P_{E} approaches 1 exponentially, it implies that even for small values of N_{B} the P_{E} is very close to 1. The simulation in the following section shows that our analysis is applicable to a real system with finite numbers of antennas, even with $N_{\mathrm{E}} > N_{\mathrm{A}}$.

V. Simulation Results

This section examines the performance of the proposed artificial noise scheme in the most favorable case for Eve, i.e., $\mathrm{SNR}_{\mathrm{E}} \to \infty$. We construct $\mathbf{v}$ in two steps: 1) generating a vector with $N_{\mathrm{A}} - N_{\mathrm{B}}$ uniformly distributed random variables; 2) normalizing the length of the random vector to $\beta e/\Phi$.

Fig. 2 shows the error performances at Bob and Eve for an uncoded system using 64-QAM with $N_{\mathrm{A}} = 10$, $N_{\mathrm{B}} = 9$ and $N_{\mathrm{E}} = 20$. Reference [3] argued that the non-zero secrecy rate can not be guaranteed when $N_{\mathrm{A}} < N_{\mathrm{E}}$. Nevertheless, our *practical secrecy* criterion provides the opportunity to protect $\mathbf{u}$ in these scenarios. With $\beta = 1$, the result in Fig. 2 shows $P_{\mathrm{E}} = 1$, even when $N_{\mathrm{A}} - N_{\mathrm{B}} = 1$. We find that $\beta = 1$ is already good enough in practice. $\Pr(c_{\mathrm{R}} < \beta)$ is shown to decay very fast. Observe that the performance of lattice precoding is considerably better than that of SVD precoding.

VI. Conclusions

In this paper, we have shown how the artificial noise can force Eve's received signal to settle around the borders of the decision region, so that the *practical secrecy* can be achieved. Of particular interest is that even if only one degree of freedom is used for artificial noise ($N_{\mathrm{A}} - N_{\mathrm{B}} = 1$) and Eve has unlimited resources ($N_{\mathrm{E}} > N_{\mathrm{A}}$), the data can still be protected. The connection between secrecy capacity and *practical secrecy*, as well as the effect of finite N_{B}, will be investigated in the future work.

Acknowledgment

The authors would like to thank Professor Terence Tao for his constructive comments and pointing out the references.

Appendix

A. Proof of Theorem 1

Let $\mathbf{B} = \mathbf{GP}$. We recall the fact [12]:

$$r_{\mathrm{cov}}(\mathbf{B}) \leq \frac{N_{\mathrm{B}}}{\lambda_1((\mathbf{B}^{\dagger})^T)}. \tag{15}$$

It is known that for a random lattice basis $\mathbf{B}$ and $N_{\rm B} \to \infty$, $\lambda_1((\mathbf{B}^\dagger)^T)$ converges to [13]

$$\sqrt{N_{\rm B}/(\pi e)} \left|\det((\mathbf{B}^\dagger)^T)\right|^{1/N_{\rm B}}. \quad (16)$$

Consequently, the right hand side of (15) tends towards

$$\frac{\sqrt{\pi e N_{\rm B}}}{\left|\det((\mathbf{B}^\dagger)^T)\right|^{1/N_{\rm B}}} = \pi e r_{\rm eff}(\mathbf{B}). \quad (17)$$

If $c_{\rm R} > \pi e$, using (11), we have $||\mathbf{GZv}|| > r_{\rm cov}(\mathbf{B})$, which means $\mathbf{y} \notin \mathcal{V}(\Lambda_{\mathbb{C}})$, so that $P_{\rm E} = 1$. ■

B. Proof of Theorem 2

1) Lattice precoding: Performing the QR decomposition yields $\mathbf{H}^T = \mathbf{Q}_{\rm H}\mathbf{R}_{\rm H}$, where $\mathbf{Q}_{\rm H}$ has orthogonal columns and $\mathbf{R}_{\rm H}$ is an upper triangular matrix with nonnegative diagonal elements. We have

$$c_{\rm R} = \frac{||\mathbf{GZv}|| \det(\mathbf{R}_{\rm H})^{1/N_{\rm B}}}{\sqrt{\frac{N_{\rm B}}{\pi e}} \left|\det(\mathbf{GQ}_{\rm H})\right|^{1/N_{\rm B}}}. \quad (18)$$

We recall the facts that $\mathbf{Q}_{\rm H}$ is independent of $\mathbf{R}_{\rm H}$ [14], and $\mathbf{GZ}$ and $\mathbf{GQ}_{\rm H}$ are mutually independent Gaussian random matrices [15]. Consequently, $||\mathbf{GZv}||$, $\det(\mathbf{GQ}_{\rm H})^{1/N_{\rm B}}$ and $\det(\mathbf{R}_{\rm H})^{1/N_{\rm B}}$ are mutually independent random variable. It is easy to verify that $\frac{\sqrt{2}}{||\mathbf{v}||}||\mathbf{GZv}||$ is a $\mathcal{X}$ distributed random variable with $2N_{\rm E}$ degrees of freedom, i.e.,

$$\frac{\sqrt{2}}{||\mathbf{v}||}||\mathbf{GZv}|| \to \mathcal{X}(2N_{\rm E}). \quad (19)$$

According to [16] , for $N_{\rm B} \to \infty$, we have

$$\frac{\log|\det(\mathbf{R}_{\rm H})| - 1/2\log\frac{N_{\rm A}!}{(N_{\rm A}-N_{\rm B})!} + 1/4\log(N_{\rm B})}{1/2\sqrt{\log(N_{\rm B})}} \to \mathcal{N}(0,1). \quad (20)$$

Multiplying the numerator and denominator in (20) by $1/N_{\rm B}$, we obtain

$$\det(\mathbf{R}_{\rm H})^{1/N_{\rm B}} \to e^{\mathcal{N}(0,\frac{1}{4}N_{\rm B}^{-2}\log(N_{\rm B}))}\left[\frac{N_{\rm A}!}{N_{\rm B}^{1/2}(N_{\rm A}-N_{\rm B})!}\right]^{\frac{1}{2N_{\rm B}}}. \quad (21)$$

Similarly, since $\mathbf{GQ}_{\rm H}$ is a Gaussian random matrix, for $N_{\rm B} \to \infty$, we have

$$\det(\mathbf{GQ}_{\rm H})^{1/N_{\rm B}} \to e^{\mathcal{N}(0,\frac{1}{4}N_{\rm B}^{-2}\log(N_{\rm B}))}\left[\frac{N_{\rm E}!}{N_{\rm B}^{1/2}(N_{\rm E}-N_{\rm B})!}\right]^{\frac{1}{2N_{\rm B}}}. \quad (22)$$

According to (19), (21) and (22), the right hand side of (18) converges to the product of two random variables $f_{\mathcal{X}} \cdot f_{\mathcal{N}}$, where

$$\begin{aligned} f_{\mathcal{X}} &= \frac{||\mathbf{v}||}{\sqrt{2N_{\rm B}}}\Phi_{\rm LP}\mathcal{X}(2N_{\rm E}), \\ f_{\mathcal{N}} &= \sqrt{\pi e}\exp(\mathcal{N}(0,\frac{1}{2}N_{\rm B}^{-2}\log(N_{\rm B}))), \end{aligned} \quad (23)$$

with $\Phi_{\rm LP}$ given in (12). Now we compute the probability of $f_{\mathcal{X}} \cdot f_{\mathcal{N}} \le \beta$. We have

$$\Pr\{f_{\mathcal{X}} \cdot f_{\mathcal{N}} \le \beta\} \le \Pr\{f_{\mathcal{X}} \le \beta\} + \Pr\{f_{\mathcal{N}} \le 1\}. \quad (24)$$

We first compute the probability of $f_{\mathcal{N}} \le 1$:

$$\Pr\{f_{\mathcal{N}} \le 1\} = \Pr\left\{\mathcal{N}(0,\frac{1}{2}N_{\rm B}^{-2}\log(N_{\rm B})) \le -\frac{1}{2}\log\pi e\right\}$$

$$\le 1/2\exp\left(-\frac{N_{\rm B}^2\log^2\pi e}{4\log(N_{\rm B})}\right) \le O\left(e^{-N_{\rm B}^2/\log(N_{\rm B})}\right). \quad (25)$$

Then, we compute the probability of $f_{\mathcal{X}} \le \beta$:

$$\Pr\{f_{\mathcal{X}} \le \beta\} = \Pr\left\{\mathcal{X}^2(2N_{\rm E}) \le \frac{2\beta^2 N_{\rm B}}{||\mathbf{v}||^2\Phi_{\rm LP}^2}\right\}. \quad (26)$$

Let $||\mathbf{v}|| = \frac{\beta e}{\Phi_{\rm LP}}$. Since $\frac{2\beta^2 N_{\rm B}}{||\mathbf{v}||^2\Phi_{\rm LP}^2} = \frac{2N_{\rm B}}{e^2} < 2N_{\rm E}$, we have

$$\Pr\left\{\mathcal{X}^2(2N_{\rm E}) \le \frac{2N_{\rm B}}{e^2}\right\} \le (\gamma e^{1-\gamma})^{N_{\rm E}}, \quad (27)$$

where $\gamma = \frac{N_{\rm B}}{e^2 N_{\rm E}}$. It is easy to show that

$$\Pr\left\{\mathcal{X}^2(2N_{\rm E}) \le \frac{2N_{\rm B}}{e^2}\right\} \le \left[\frac{e^2 N_{\rm E}}{e^{1-\gamma}N_{\rm B}}\right]^{-N_{\rm E}} \le O(e^{-N_{\rm E}}). \quad (28)$$

Therefore, with $||\mathbf{v}|| = \frac{\beta e}{\Phi_{\rm LP}}$

$$\begin{aligned} \Pr\{c_{\rm R} &< \beta\} = \Pr\{f_{\mathcal{X}} \cdot f_{\mathcal{N}} < \beta\} \\ &\le O\left(e^{-\min(N_{\rm B}^2/\log(N_{\rm B}),\, N_{\rm E})}\right). \end{aligned} \quad (29)$$

2) SVD precoding: The proof is similar to the above. ■

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] S. K. L.-Y. Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[3] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[4] J.-C. Belfiore, F. Oggier, and P. Solé, "Lattice codes for the Gaussian wiretap channel," in *Proc. 2011 International Workshop on Coding and Cryptography*.

[5] B. M. Hochwald, C. B. Peel, and A. L. Swindlehurst, "A vector perturbation technique for near-capacity multiantenna multiuser communications—part II: perturbation," *IEEE Trans. Commun.*, vol. 53, pp. 537–544, Mar. 2005.

[6] W. H. Mow, "Maximum likelihood sequence estimation from the lattice viewpoint," *IEEE Trans. Inf. Theory*, vol. 40, pp. 1591–1600, Sep. 1994.

[7] R. Zamir, "Lattices are everywhere," in *Proc. 2009 Information Theory and Applications Workshop*, pp. 392–421.

[8] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*, 2nd ed. Springer-Verlag, 1993.

[9] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1639–1642, Jul. 1999.

[10] C. Windpassinger, R. Fischer, and J. B. Huber, "Lattice-reduction-aided broadcast precoding," *IEEE Trans. Commun.*, vol. 52, pp. 2057–2060, Dec. 2004.

[11] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.

[12] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers," *Math. Ann.*, vol. 296, pp. 625–635, 1993.

[13] M. Ajtai, "Random lattices and a conjectured 0 - 1 law about their polynomial time computable properties," in *Proc. 2002 IEEE Symposium on Foundations of Computer Science*.

[14] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*. Now Publishers Inc., 2004.

[15] E. Lukacs and E. P. King, "A property of the normal distribution," *Ann. Math. Statist.*, vol. 25, no. 2, pp. 389–394, 1954.

[16] T. Tao and V. Vu, "A central limit theorem for the determinant of a Wigner matrix," *Advances in Mathematics*, vol. 231, pp. 74–101, Sep. 2012.