Communications in Information and Systems
Volume 20, Number 2, 117–129, 2020

An approach to physical layer security in MIMO wireless via vector perturbation precoding

Liutong Du*, Lihua Li*, and Arogyaswami J. Paulraj

In this paper, we investigate the application of vector perturbation (VP) precoding for physical layer security. We propose the notion of *practical secrecy leakage* to measure the performance of practical secrecy schemes which aims to maximize eavesdropper's error probability. We show that *practical secrecy leakage* can be avoided with modified VP scheme under specified restrictions of perturbation vector. A new sphere decoder is developed to satisfy these limitations with a cost of legitimate receiver's error performance. We show that the proposed scheme can avoid practical secrecy leakage although the number of receiver's antenna is small while obtaining a better performance at the legitimate receiver compared with artificial noise based schemes.

1. Introduction

Physical layer security has drawn a growing interest in recent years due to the wide use of wireless communications. *Artificial noise* (AN) scheme [1] proposed by Geol *et al.* as a promising scheme to increase secrecy rate has been well studied in theory and application [2]. The approach assumes the transmitter (Alice) aligns an artificial noise vector within the null space between itself and the legitimate receiver (Bob), thus only the performance of eavesdropper (Eve) is degraded. In [1], both secret signal and jamming signal are assumed to follow Gaussian distribution to ensure a non-zero secrecy rate and the number of Bob's antennas N_B is assumed strictly smaller than the number of Alice's antennas N_A to make sure a non-trivial null space exists, i.e., $N_B < N_A$. *Practical secrecy* (PS) scheme [3] is a AN-based techniques with finite alphabet (e.g., M-QAM) which aims at maximizing Eve's error probability P_E as a more practical measure instead of theoretical approaches of increasing secrecy rate. Although well studied, AN-based scheme is not optimal in many aspects. First, for Bob, $N_A - N_B$ spatial degrees of freedom

*This paper is supported by National Key Research and Development Plan under grant 2018YFE0205501.

is assigned to generate jamming signals to ensure only damage to Eve, thus not used for Bob. Second, Bob will suffer a rate penalty because some of the transmit power has to be diverted to generate artificial noise. The rate penalty is even higher when Eve's channel is not known accurately by Alice [4] or is highly correlated to Bob's channel. Third, but not least important, secrecy leakage may happen as not all points have closed decoding regions due to the use of finite alphabet in practical transmission schemes [5].

In this paper, we propose a vector perturbation (VP) precoding based practical secrecy transmission scheme, where the transmitter generate the perturbation vector with a 'secure' parameter τ_s instead of the standard parameter τ, the effect of perturbation vector can be perfectly removed as τ_s is known to the legitimate receiver in advance of transmission. As Eve has no information about τ_s, the residual part of perturbation vector after a modulo process with τ would function similarly as artificial noise in the AN scheme of degrading the received signal quality at eavesdropper. We further propose a new sphere decoder to guarantee practical secrecy while minimizing the unscaled transmit power. Compared with AN-based practical secrecy schemes in [3], the proposed scheme has several benefits as listed below:

1) As the interference term does not have to align within the null space of Bob's channel, N_B does not have to be smaller than N_A, which means the proposed schemes suffers less spatial DoF loss, and is more suitable for transmitters with small number of antennas compared with AN scheme.
2) As perturbation vector is selected to minimize effective transmit power whilst generating artificial noise vector would cost extra power other than data vector, proposed scheme outperforms AN in consideration with Bob's rate.
3) The secrecy leakage due to finite alphabet, especially with small N_B and low order modulation, would disappear within the proposed sphere decoder.

This paper is organized as follows: Section 2 presents system model and some lattice basics. VP based practical secure transmission scheme and the newly designed sphere decoder are given in Section 3. In Section 4, simulation results of the proposed scheme are given. Some concluding remarks are drawn in Section 5.

Notations In this paper, matrices and column vectors are denoted by upper and lowercase boldface letters, super scripts $\mathbf{A}^T$, $\mathbf{A}^{-1}$ and $\mathbf{A}^\dagger$ denote the transpose, the inverse and the pseudo-inverse of matrix $\mathbf{A}$ respectively. $\|\mathbf{x}\|$ denotes the Euclidean norm of vector $\mathbf{x}$. $\Re(c)$, $\Im(c)$ denotes the real and imaginary part of c. $X \to Y$ denotes that random variable X converges to random variable Y in distribution. $\mathrm{QR}(\cdot)$ denotes QR decomposition and $\oplus$ denotes the exclusive OR operation. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$ and $\mathbb{Z}[i]$ represent the real, complex, integer and complex integer numbers respectively.

2. System model and some preliminaries

2.1. System model

Consider secure communications over point to point MIMO channel. A three-terminal system is a typical research model, which includes a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve), equipped with N_A, N_B, and N_E antennas, respectively. The received signal vectors at Bob and Eve can be denoted as:

$$\mathbf{z} = \mathbf{H}\mathbf{x}{+}\mathbf{n}_B, \tag{1}$$

$$\mathbf{y} = \mathbf{G}\mathbf{x}{+}\mathbf{n}_E, \tag{2}$$

where $\mathbf{x} \in \mathbb{C}^{N_A \times 1}$ is the signal vector, $\mathbf{n}_B \in \mathbb{C}^{N_B \times 1}$ and $\mathbf{n}_E \in \mathbb{C}^{N_E \times 1}$ are the complex white Gaussian noise vectors with i.i.d entries $\sim \mathcal{N}_{\mathbb{C}}\left(0, \sigma_B^2\right)$ and $\mathcal{N}_{\mathbb{C}}\left(0, \sigma_E^2\right)$, respectively. $\mathbf{H} \in \mathbb{C}^{N_B \times N_A}$ and $\mathbf{G} \in \mathbb{C}^{N_E \times N_A}$ represent the complex channel matrices from Alice to Bob and Alice to Eve, respectively, For the performance analysis and numerical simulations, we will assume the entries to be i.i.d. circularly symmetric Gaussian random variables (Rayleigh distributed) $\sim \mathcal{N}_{\mathbb{C}}(0,1)$. In this paper, we assume Bob and Eve are not co-located thus $\mathbf{H}$ and $\mathbf{G}$ are mutually independent.

2.2. VP precoding

At each time instant, Alice transmits a secret data vector $\mathbf{u} \in \mathbb{C}^{N_B \times 1}$ whose elements are independent, uniformly distributed over the symbol alphabet $\mathcal{C}$ with normalized symbol power. In this paper we assume $\mathbf{u}$ is generated within uniform M-QAM modulation, which is widely applied in 4G and 5G systems, we have $\Re(\mathbf{u})$ and $\Im(\mathbf{u}) \in \mathcal{C}^{N_B}$, where $\mathcal{C}$ is generally defined as $\left\{\left(-\sqrt{M}+1\right)\frac{\Delta}{2}, \left(-\sqrt{M}+3\right)\frac{\Delta}{2} \ldots, \left(\sqrt{M}-1\right)\frac{\Delta}{2}\right\}$, Δ is the spacing between constellation points and is determined by the modulation order. In VP precoding, the secret data vector $\mathbf{u}$ is first perturbed by a scaled complex

Gaussian integer[1] vector $\mathbf{u}' = \tau\mathbf{l}$, where $\mathbf{l} \in \mathbb{G}^{N_B}$ is called as *perturbation vector*, the real-valued scale parameter τ is chosen such that $\mathcal{C} + \tau\mathbb{G}$ forms an extended symbol alphabet consisting of nonoverlapping copies of $\mathcal{C}$ (cf. [6])

$$\tau = 2\left(c_{\max} + \Delta/2\right), \tag{3}$$

where $c_{\max}$ is the absolute value of the constellation symbol(s) with largest magnitude. Perturbation vector $\mathbf{u}'$ is selected to minimize the unscaled transmit power as

$$\mathbf{u}' = \arg\min_{\hat{\mathbf{u}} \in \tau\mathbf{l}} \left\|\mathbf{P}\left(\mathbf{u} + \hat{\mathbf{u}}\right)\right\|^2, \tag{4}$$

where $\mathbf{P} = \mathbf{H}^{\dagger}$ is a zero-forcing form precoding matrix. The perturbation vector $\mathbf{u}'$ can be solved with *sphere decoder* [8], which comes up with a computational complexity that scales exponentially with N_B. It is preferable to apply complexity reduction techniques as in [9] when the scale of antenna arrays goes large. The transmit vector $\mathbf{x}$ can be formed as

$$\mathbf{x} = \frac{1}{\beta}\mathbf{P}\left(\mathbf{u} + \tau\mathbf{l}\right), \tag{5}$$

where $\beta = \sqrt{\frac{1}{P}\left\|\mathbf{P}\left(\mathbf{u} + \tau\mathbf{l}\right)\right\|^2}$ is the power scaling factor to fulfill the transmit power limit P, i.e., $E\left[\left\|\mathbf{x}\right\|^2\right] \leqslant P$. With (1), the received signal vector at Bob can be denoted as

$$\mathbf{z} = \frac{1}{\beta}\mathbf{HP}\left(\mathbf{u} + \tau\mathbf{l}\right) + \mathbf{n}_B. \tag{6}$$

Through this paper, we assume β is perfectly known at Bob and Eve, the affect of imperfect CSI and β has been well investigated in [7]. The received signal can be recovered with β as

$$\mathbf{z}' = \beta\mathbf{z} = \mathbf{HP}\left(\mathbf{u} + \tau\mathbf{l}\right) + \beta\mathbf{n}_B, \tag{7}$$

Bob then removes the effect of perturbation vector $\mathbf{u}'$ by performing a modulo operation $\hat{\mathbf{u}}_B = M_\tau\left(\mathbf{z}'\right)$. The modulo operator is defined as:

$$M_\tau(a) = a - \left\lfloor \frac{\Re(a)}{\tau} + \frac{1}{2} \right\rfloor \tau - j\left\lfloor \frac{\Im(a)}{\tau} + \frac{1}{2} \right\rfloor \tau \in \Omega, \tag{8}$$

[1] The set of Gaussian integers $\mathbb{G} = \mathbb{Z} + j\mathbb{Z}$ comprises all complex numbers with integer real and imaginary parts.

where the constellation region Ω is defined as:

$$\Omega = \left\{ c \in \mathbb{C} | -\frac{\tau}{2} \leqslant \Re(c) < \frac{\tau}{2}, -\frac{\tau}{2} \leqslant \Im(c) < \frac{\tau}{2} \right\}. \tag{9}$$

Then the data vector to be decoded after modulo process is only affected by a scaled noise as

$$\hat{\mathbf{u}}_B = \mathbf{u} + \beta \mathbf{n}_B. \tag{10}$$

2.3. Lattice basics and practical secrecy

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

$$\Lambda_{\mathbb{C}} = \{\mathbf{Bu} : \mathbf{u} \in \mathbb{Z}[i]^n\}, \tag{11}$$

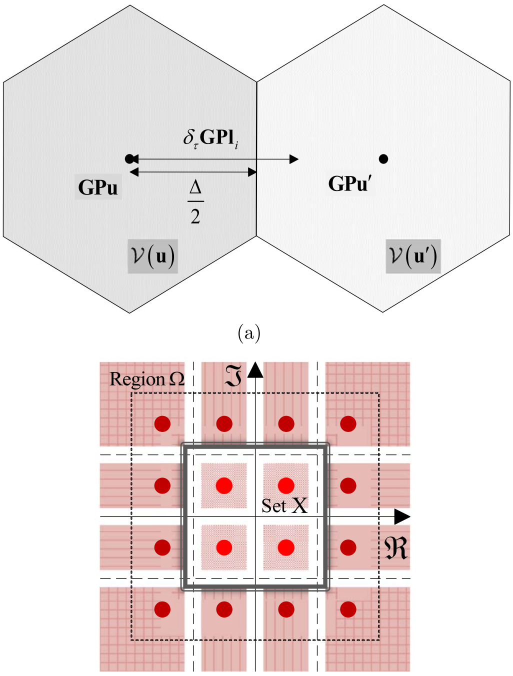
where the *basis* matrix $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$ is column linear independent.

The *Voronoi region* of a lattice point $\mathbf{x}_i$= $\mathbf{Bu}_i$, which gives the corresponding decoding region, is denoted by:

$$\mathcal{V}(\mathbf{x}_i \in \Lambda_{\mathbb{C}}) = \{\mathbf{y} \in \mathbb{C}^m : \|\mathbf{y} - \mathbf{x}_i\| \leq \|\mathbf{y} - \mathbf{x}_j\|, \forall \mathbf{x}_j \neq \mathbf{x}_i\}. \tag{12}$$

Instead of targeting a non-zero secrecy rate assuming an infinite-length wiretap code and Gaussian artificial noise [1], a more practical AN based scheme is proposed in [3] which makes use of finite alphabet(e.g. M-QAM) and has no requirement on the distribution of $\mathbf{v}$. *Practical secrecy* [3] is defined to measure the secrecy with Eve's error probability $P_E \triangleq \Pr(\hat{\mathbf{u}}_E \neq \mathbf{u})$: Practical secrecy is achieved if for any SNR_E, $P_E \to 1$ exponentially as $N_B \to \infty$. The SNR of Eve is defined as $SNR_E \triangleq P/\sigma_E^2$. Each secret data $\mathbf{u}$ with M-QAM alphabet can be seen as a lattice point, with minimum distance decoding, P_E only depends on whether $\hat{\mathbf{u}}_E \in \mathcal{V}(\mathbf{u})$ or not.

In [3], Liu *et al.* showed that practical secrecy can be guaranteed with specified power as $N_B \to \infty$, the authors then point out in [5] that a secrecy outage may happen due to the use of finite constellations, and the outage probability can be made arbitrarily small by considering either longer blocks of messages or larger constellation size. However in practical transmissions, secrecy leakage may happen as the receiver only has finite number of antennas due to many reasons e.g., cost and physical size, thus practical secrecy in



(a)

(b)

Figure 1: (a) Decoding region of lattice constructed by **GP**, (b) Decoding region of uniform 16-QAM modulation.

[3] may not able to describe the secrecy performance or due to small block and constellation size. In this paper, we define a notion *practical secrecy leakage* as the probability that Eve can correctly decode the secret data to measure the secrecy performance more clearly as:

$$P_L \triangleq \Pr\left(\hat{\mathbf{u}}_E = \mathbf{u}\right) = 1 - P_E. \tag{13}$$

3. Secure transmissions utilizing VP precoding and proposed Algorithm

In this section, we show the secure transmission scheme with VP precoding, the problem of finding optimal perturbation vector is reformed under demand for secrecy, then a novel designed sphere decoder is proposed to solve the resulting problem.

3.1. Secure transmission process and problem formulation

In secure VP transmission scheme, the transmitter generate the signal vector with a modified parameter τ_s as

$$\mathbf{x} = \frac{1}{\beta_s}\mathbf{P}\left(\mathbf{u} + \tau_s \mathbf{l}\right), \tag{14}$$

where an offset δ_τ is added to the standard τ in (3):

$$\tau_s = \tau + \delta_\tau . \tag{15}$$

As τ_s is assumed known to the legitimate receiver in advance of transmission, the estimated data at Bob with a modified modulo processor can be denoted as:

$$\hat{\mathbf{u}}_{B_s} = M_{\tau_s}(\mathbf{z'}_s) = \mathbf{u} + \beta_s \mathbf{n}_B . \tag{16}$$

Consider that Eve has the ability to know power scaling factor β_s and modulation order, then the standard scale factor τ can be calculated following (3) and is used in Eve's modulo process. The received signal vector at Eve recovered by β_s can be obtained with (2) as

$$\mathbf{y}' = \beta_s \mathbf{y} = \mathbf{GP}\left(\mathbf{u} + \tau_s \mathbf{l}\right) + \beta_s \mathbf{n}_E . \tag{17}$$

In this work, we consider the worst case to Alice and Bob, i.e., channel matrix $\mathbf{G}$ and $\mathbf{H}$ are assumed known to Eve and $\sigma_E^2 \to 0$. After the standard modulo process (8), the estimated signal can be denoted as:

$$\hat{\mathbf{u}}_E = M_\tau\left(\mathbf{y}'\right) = \mathbf{GPu} + M_\tau\left(\delta_\tau \mathbf{GPl}\right). \tag{18}$$

As shown in Fig. 1(a), consider the complex lattice constructed by $\mathbf{GP}$, as pointed out in [3], the decoding region of the target point $\mathbf{GPu}$ is its *Voronoi region* $\mathcal{V}(\mathbf{u})$. From (18), we can see that the decoding result is only determined by $\delta_\tau \mathbf{GPl}$, and more exactly by $M_\tau\left(\delta_\tau \mathbf{GPl}\right)$.

Remark 1: If the optimal perturbation vector $\mathbf{l} = \mathbf{0}$, with (18), then $P_L \triangleq \Pr\left(\hat{\mathbf{u}}_E = \mathbf{u}\right) = 1$ as Eve can decode the secret data correctly due to $\hat{\mathbf{u}}_E = \mathbf{GPu} \in \mathcal{V}(\mathbf{u})$.

We assume that $\mathbf{l} \neq \mathbf{0}$, as shown in Fig. 1(b), the interference term $\delta_\tau \mathbf{GPl}$ aligned to the lattice constructed by $\mathbf{GP}$, for the inner points which have closed decoding region, it is easy to make $\hat{\mathbf{u}}_E \notin \mathcal{V}(\mathbf{u})$ by selecting a proper δ_τ following an amplitude limit

$$\left\| M_\tau \left(\delta_\tau \mathbf{GPl} \right) \right\|^2 > \left(\frac{\Delta}{2} \right)^2 . \tag{19}$$

For the outer points at edge or corner of the constellation which compose the set X, to make sure that $\hat{\mathbf{u}}_E \notin \mathcal{V}(\mathbf{u})$, it is not enough that the interference term $\delta_\tau \mathbf{GPl}$ fulfills the amplitude limit as (19): $\hat{\mathbf{u}}_E$ may belong to the corresponding half open decoding region of the target point $\mathbf{GPu}$ if $\delta_\tau \mathbf{GPl}$ has the same sign as $\mathbf{u}$.

Remark 2: Even with $\mathbf{l} \neq \mathbf{0}$ and (19) fulfilled, secrecy leakage will also happen when the the symbol lies at the edge and $\delta_\tau \mathbf{GPl}$ has the same sign as $\mathbf{u}$.

To make sure that $P_L = 0$, i.e. $\hat{\mathbf{u}}_E \notin \mathcal{V}(\mathbf{u})$. At the transmitter side, the precoding progress has to fulfill both (19) and the direction limit: there exists at least one different sign between $\delta_\tau \mathbf{GPl}$ and the secret data $\mathbf{u}$ at corresponding position. Then the problem utilizing VP precoding to obtain both diversity gain and practical secrecy can be formulated as:

$$\begin{aligned} \mathbf{u'_s} &= \underset{\hat{\mathbf{u}} \in \tau_s \mathbf{l}}{\arg\min} \left\| \mathbf{P} \left(\mathbf{u} + \hat{\mathbf{u}} \right) \right\|^2 \\ & s.t.\ \mathbf{l} \neq \mathbf{0} \\ & \sum u_i \oplus l_i > 0, \forall\, u_i \in X. \end{aligned} \tag{20}$$

Note that problem (20) is also NP hard as [6], and an modified sphere decoder is proposed following [8], the corresponding algorithm is summarized as Algorithm 1.

4. Numerical results

In this section, the practical secrecy leakage of Eve and BER performance of Bob are compared over four schemes:VP precoding with standard sphere decoder, proposed sphere decoder and two AN based PS schemes in [3] are compared. As stated in Section 3, we assume $\sigma_E^2 \to 0$, thus the secrecy leakage of Eve is averaged over SNR of Bob.

Fig. 2 compares the secrecy leakage and BER performance of proposed sphere decoder and standard power-minimized sphere decoder [6] over varied δ_τ. The numerical results show that the secrecy leakage performance P_L of both schemes are divided by $\delta_\tau \in \Xi | \left\| M_\tau \left(\delta_\tau \right) \right\|^2 = \left(\frac{\Delta}{2} \right)^2$: when

Algorithm 1 Modified sphere decoder for secrecy

```
INPUT: $\tau_s, \mathbf{P}, \mathbf{u}$;
OUTPUT: $\mathbf{l}_p \in \mathbb{Z}^{2N_B}$;
Initialization:
$\mathbf{d} = [\Re(\mathbf{u}); \Im(\mathbf{u})]^T$, $\mathbf{u}_t = [\Re(-\mathbf{Pu}); \Im(-\mathbf{Pu})]^T$
$\mathbf{H}_t = [\Re(\tau_s \mathbf{P}), -\Im(\tau_s \mathbf{P}); \Im(\tau_s \mathbf{P}), \Re(\tau_s \mathbf{P})]^T$
$[\mathbf{Q}_t, \mathbf{R}_t] = QR(\mathbf{H}_t)$
$\mathbf{D} = diag(sign(diag(\mathbf{R}_t)))$, $\mathbf{G} = \mathbf{R}_t{}^T \mathbf{D}$
$\mathbf{r} = \mathbf{u}_t \mathbf{Q}_t \mathbf{D}$, $C = \infty$, $n = 2N_B$, $i = n + 1$
$g_s = n - 1$, $\lambda = \mathbf{g} = \mathbf{s} = \mathbf{0}^{(n+1)\times 1}$
LOOP
do {
  if $(i \neq 1)$ {
    $i = i - 1$
    $\mathbf{p}_i = \left(\mathbf{r}_i - \sum_{j=i+1}^{n} \mathbf{l}_j \mathbf{G}_{j,i}\right) \Big/ \mathbf{G}_{i,i}$
    $\mathbf{l}_i = round(\mathbf{p}_i)$
    $\mathbf{g}_i = \mathbf{g}_{i+1} + (\mathbf{l}_i == 0)$
    $\mathbf{s}_i = \mathbf{s}_{i+1} + (\mathbf{l}_i == 0) + (sign(\mathbf{l}_i) == sign(\mathbf{d}_i))$
    $y = (\mathbf{p}_i - \mathbf{l}_i)\mathbf{G}_{i,i}$
    $\Delta_i = sign(y)$
    $\lambda_i = \lambda_{i+1} + y^2$
  } else {
    $\mathbf{l}_p = \mathbf{l}$
    $C = \lambda_1$}}
  while$(\lambda_i < C \& \mathbf{g}_i < g_s \& \mathbf{s}_i < n)$
do {
  if $(i = n)$
    return $\mathbf{l}_p$ and exit
  else {
    $i = i + 1$
    $\mathbf{l}_i = \mathbf{l}_i + \Delta_i$
    $\Delta_i = -\Delta_i - sign(\Delta_i)$
    $y = (\mathbf{p}_i - \mathbf{l}_i)\mathbf{G}_{i,i}$
    $\mathbf{g}_i = \mathbf{g}_{i+1} + (\mathbf{l}_i == 0)$
    $\mathbf{s}_i = \mathbf{s}_{i+1} + (\mathbf{l}_i == 0) + (sign(\mathbf{l}_i) == sign(\mathbf{d}_i))$
    $\lambda_i = \lambda_{i+1} + y^2$} }
while$(\lambda_i \geq C \& \mathbf{g}_i < g_s \& \mathbf{s}_i < n)$
goto LOOP
```

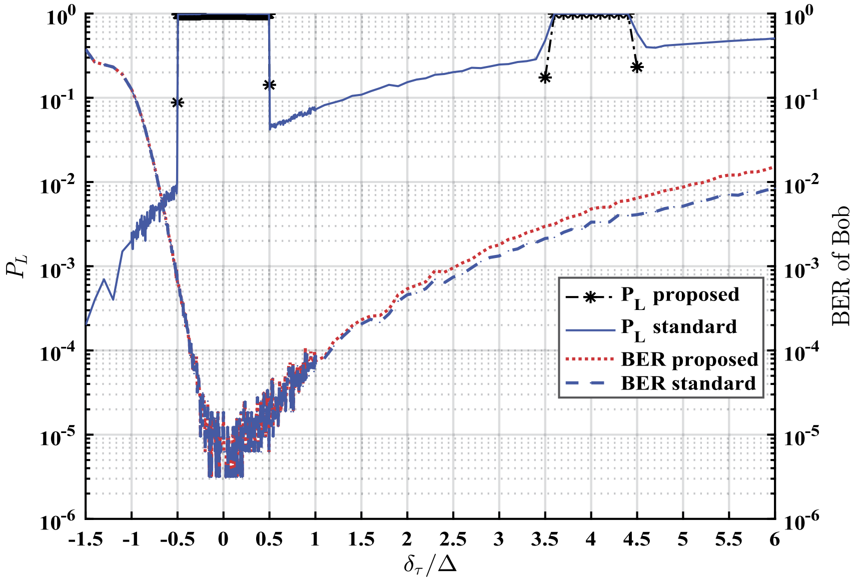


Figure 2: Performance of standard VP and proposed algorithm under varied δ_τ with 16-QAM modulation and $N_A = N_B = N_E = 8$ at $SNR_{Bob} = 25$ dB.

$\|M_\tau(\delta_\tau)\|^2 \leq \left(\frac{\Delta}{2}\right)^2$, both schemes meet a secrecy leakage with $P_L = 1$; when it turns to $\|M_\tau(\delta_\tau)\|^2 > \left(\frac{\Delta}{2}\right)^2$, standard VP scheme has a secrecy leakage increase with the growth of δ_τ due to the increase sparsity of $\mathbf{l}$ while there is no secrecy leakage of proposed scheme. The price of secrecy is the BER performance loss of legitimate user, first, a BER degradation is introduced by a non-zero δ_τ to keep $\|M_\tau(\delta_\tau)\|^2 > \left(\frac{\Delta}{2}\right)^2$ as indicated both in our simulations and other researches over VP, e.g., [6], a δ_τ around 0 always captures the best performance; second, as the proposed sphere decoder no longer aims at minimizing the unscaled transmit power, a trade-off between diversity and secrecy is made by force the 'optimal' perturbation vector in (4) follow (20) instead, as shown in Fig. 2 the performance gap between standard decoder and Alg. 1 increases with the growth of δ_τ and is negligible when δ_τ is small.

In Fig. 3, performance of VP based schemes and AN-based schemes in [3] are compared when $N_A = 6, N_B = N_E = 4$ with 16-QAM for 200000 independent channel realizations and δ_τ is set as 0.51Δ to fulfill (19). As part of transmit power is separated to artificial noise vector, VP based schemes can achieve a better diversity performance compared with AN based schemes, the proposed scheme meets a about 2 dB loss compared with standard de-

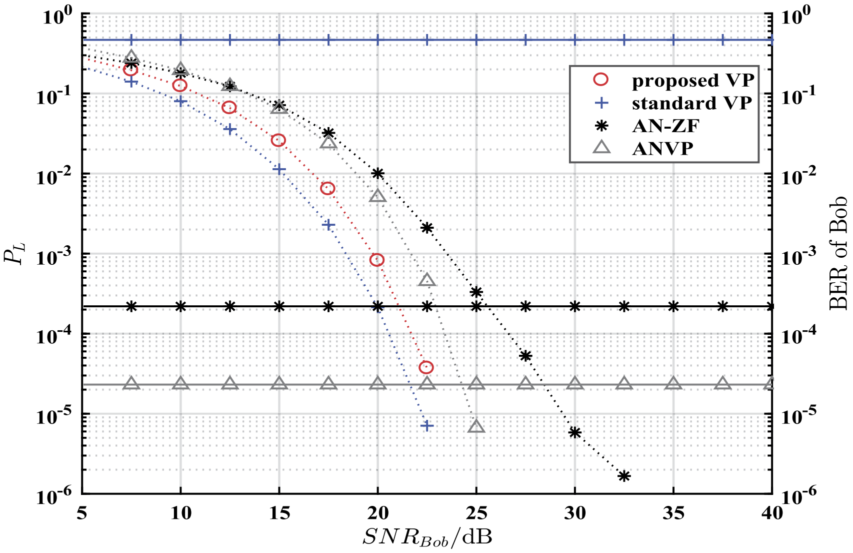


Figure 3: Performance of practical secrecy schemes based on standard and proposed VP precoding and AN scheme [3] (AN-ZF and AN-VP).

coder at 10^{-3}, and is 2 dB better than the AN based VP precoding scheme in [3]. When it comes to practical secrecy leakage, we can see that no leakage happens to the proposed scheme while standard decoder meets the biggest leakage mostly owing to the sparsity of $\mathbf{l}$. All these schemes suffers the leakage introduced by finite constellations [5] except the proposed decoder. It is clear that only the proposed scheme can avoid both practical secrecy leakage and power waste introduced by artificial noise vector even when the antenna numbers and the constellation is small.

5. Conclusion

In this paper, we investigate the application of VP precoding to avoid practical secrecy leakage for MIMO wiretap channel. Novel principles of selecting perturbation vector are given and new corresponding sphere decoder is developed. Simulation results show that the proposed scheme outperforms artificial noise based schemes in terms of BER performance at the legitimate receiver. At the same time, the proposed scheme can work well even when the transmitter is equipped with only few antennas and low order modulation scheme is applied, whilst the state-of-art AN based scheme would meet a secrecy leakage.

References

[1] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[2] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010. MR2798976

[3] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013. MR3367811

[4] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in: *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing – Proceedings*, pp. 2437–2440, 2009.

[5] S. Liu, Y. Hong, and E. Viterbo, "Unshared secret key cryptography," *IEEE Transactions on Wireless Communications*, vol. 13, no. 12, pp. 6670–6683, 2014.

[6] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication-part II: perturbation," *IEEE Transactions on Communications*, vol. 53, no. 3, pp. 537–544, 2005.

[7] L. Du, L. Li, P. Zhang, D. Miao, and Z. Liu, "Vector perturbation precoding under imperfect CSI and inaccurate power scaling factors," *IEEE Access*, vol. 7, pp. 89 162–89 171, 2019.

[8] A. Ghasemmehdi and E. Agrell, "Faster recursions in sphere decoding," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3530–3536, 2011. MR2817035

[9] Y. Ma, A. Yamani, N. Yi and R. Tafazolli, "Low-complexity MU-MIMO nonlinear precoding using degree-2 sparse vector perturbation," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 497–509, March 2016.

Liutong Du
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, 100876
China
E-mail address: liutongdu@bupt.edu.cn

Lihua Li
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, 100876
China
E-mail address: lilihua@bupt.edu.cn

Arogyaswami J. Paulraj
Department of Electrical Engineering
Stanford University
Stanford, CA 94305-9510
USA
E-mail address: apaulraj@stanford.edu

Received February 2, 2020