An Anti-eavesdropping Strategy for Precoding-aided Spatial Modulation with Rough CSI of Eavesdropper

Guiyang Xia, Yan Lin, Feng Shu, Yongpeng Wu, Jiangzhou Wang

***Abstract*—In this paper, an anti-eavesdropping strategy is proposed for secure precoding-aided spatial modulation networks, under the assumption that the rough channel state information of eavesdropper can be obtained at the transmitter. Traditionally, artificial noise (AN) can be always projected into the null-space of the legitimate channel, however it may lead to some security loss since this strategy dispenses with a holistic consideration for secure transmission. To reduce the computational complexity of our optimization problem, we derive a closed-form expression that is a lower bound of the approximate rate over the illegitimate channel. Then a concave maximization problem is formulated for optimizing the covariance matrix of AN. Simulation results show that our proposed scheme achieves almost the same secrecy rate (SR) performance as the method of directly maximizing the approximate SR, and harvests significant SR gains compared with the traditional null-space projection benchmark.**

***Index Terms*—Spatial modulation, precoding-aided, artificial noise, secure transmission, finite-alphabet inputs.**

I. Introduction

As one of emerging multiple-input-multiple-out (MIMO) techniques, spatial modulation (SM) [1] has been proposed to reduce the radio frequency chains and evade the inter-channel interference. Recently, SM has exhibited its capabilities of achieving a high energy efficiency [2] and being easily implemented. Owing to these advantages, the SM-based network has attracted tremendous attention from academia [3]–[7]. As a specific counterpart of SM, precoding-aided SM (PSM) exploits the indices of receive antennas (RAs) to increase the spectral efficiency by concentrating the transmit signals onto one of the RAs in single channel used. As such, PSM attains the benefits of the low detection complexity [8] and obtains the opportunity to achieve physical layer security (PLS) [9] via its precoder.

However, secure transmission for PSM networks cannot be merely ensured by the dedicated precoder, since the secrecy performance will be seriously degraded in the face of having a high-quality channel of eavesdropper (Eve). As a powerful technique for reinforcing security, artificial noise (AN) can be invoked to the transmission for safeguarding the confidential message to be intercepted. For Gaussian inputs, plenty of secrecy enhancement schemes of designing AN were studied in prior researches [10]–[12]. To combat with a multiple-antenna Eve, both the power minimization problem and the secrecy rate (SR) maximization problem were comprehensively studied in [13]. Moreover, a cooperative jammer assisted scheme was investigated in [14] for further enhancing the secrecy performance. In [15], the authors elaborately proposed a Stackelberg game model to tackle a rate maximization problem for a multi-casting network, in which the transmitter and the jammers are the follower and the leaders, respectively. However, it is particularly worth mentioning that the assumption of Gaussian inputs as signaling is mismatched with the contemporary advanced wireless system, since finite-alphabet inputs are typically adopted as the signaling in practice, such as amplitude phase modulation (APM) symbols. Unfortunately, the SR expression for finite-alphabet inputs cannot be expressed in a closed form, which thus leads to a tricky optimization of the AN.

Recently, the security problem of PSM networks for practical finite-alphabet inputs were also drawn attention. In [16], the precoder was optimized by maximizing the power received at Bob whilst minimizing the signal power received at Eve, under the assumption that the perfect channel state information (CSI) was available at the transmitter (Alice). To combat with a passive Eve, a time-varying interference based scheme was proposed in [17], where the interference signals were also projected into the null-space of the legitimate channel. Furthermore, a scrambling matrix was designed for a multi-user PSM network in [18] to impose a fast varying effect on the signal precoding matrices at Eve, which aimed for degrading Eve's blind detection. More elaborately, upon assuming that the imperfect CSI of Eve's channel can be obtained at the transmitter, the authors in [19] investigated an AN generated scheme for maximizing the secrecy performance of a secure SM network. However, this strategy only aimed to combat with the Eve who has a single RA. As a result, the security might be seriously threatened when confronted with a multiple-antenna Eve. In addition, as the null-space dimensionality of the legitimate channel is zero, a dual optimization strategy was proposed in [20] for optimizing the beamformer of AN to achieve a secure transmission. Nevertheless, this strategy is unable to guarantee that there is no duality gap, since the optimization problem is non-convex.

As above mentioned, the prior researches [16]–[18] for SM-based systems, generally, improved the security by projecting

Guiyang Xia, Yan Lin and Feng Shu are with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, 210094, CHINA. Email: xiaguiyang@njust.edu.cn; yanlin@njust.edu.cn; shufeng@njust.edu.cn;

Yongpeng Wu is with the Shanghai Key Laboratory of Navigation and Location-Based Services, Shanghai Jiao Tong University, Minhang 200240, CHINA. Email: yongpeng.wu2016@gmail.com;

Jiangzhou Wang is with the School of Engineering and Digital Arts, University of Kent, Canterbury CT2 7NT, U.K. Email: j.z.wang@kent.ac.uk.

the AN into the null-space of the legitimate channel, which results in the interference signals only jeopardizing Eve's decoding but without affecting that of the desired receiver (Bob). The main reason that the null-space projection (NSP) scheme is frequently adopted because of its analytical structure and easy implement. Notably, the conventional NSP scheme dispenses with a comprehensive consideration of a secure transmission, because the AN is only designed from the perspective of the legitimate receiver. This implies that the NSP strategy lacks of taking overall system configurations into account, such as the characterises of both the channels and the phases of the finite-alphabet. Therefore, the NSP scheme may result in some secrecy performance loss especially in the case that partial CSI of Eve's channel can be obtained at the transmitter.

To the best of our knowledge, the NSP scheme is usually adopted to improve the SR performance for PSM networks, regardless of Eve's location. Therefore, it is imperative to conceive an efficient method that fully exploits system parameters for enhancing the security, especially when some beneficial information related to Eve's channel is obtained at Alice. To this end, this work assumes that a rough CSI of Eve's channel can be available at the transmitter, which corresponds to the scenario that Eve is an idle/irregular user of the secure system [21] [22]. Then, a PLS scheme is proposed for reinforcing the security of the PSM network. Specifically, considering the fact that the SR expression is in non-closed form and non-convexity, a novel lower bound of the approximate SR in a closed-form expression is derived. Then, a convex optimization problem of the AN covariance matrix (ANCM) is established for maximizing the SR. Finally, simulation result verifies the efficiency of our proposed algorithm in terms of the SR performance attained.

II. System Model

Consider a secure PSM-assisted MIMO communication system over Rayleigh fading channels with N_t transmit antennas (TAs) at Alice, N_r and N_e RAs at Bob and at Eve, respectively. According to the principle of the PSM systems, $N_t > N_r$ and $N_r = 2^{k_0}$ are satisfied. Notably, an advantage of the PSM system is that extra k_0 bits can be conveyed by activating one of Bob's RAs, and simultaneously, a M-ary APM symbol is received in each channel used. As a result, there are $\log_2 M + k_0$ bits that can be totally decoded at Bob. Specifically, a PSM symbol can be expressed as $\mathbf{s}_i^j = \mathbf{e}_i b_j$, where $\mathbf{e}_i$ refers to the i-th column of $\mathbf{I}_{N_r}$, indicating the i-th ($i = 1, \cdots, N_r$) RA is activated. Moreover, $b_j \in \{b_1, \cdots, b_M\}$ is the j-th modulation symbol of a M-ary APM constellation, which is normalized to $\mathbb{E}[|b_j|] = 1$. To combat with eavesdropping, a PSM signal associated with AN is given by

$$\boldsymbol{x} = \sqrt{P_1}\mathbf{P}\mathbf{s}_i^j + \sqrt{P_2}\mathbf{T}\mathbf{n}, \tag{1}$$

where $P = P_1 + P_2$ is the total power constraint. Here, $\mathbf{P} \in \mathbb{C}^{N_t \times N_r}$ is the precoder of the confidential signal and $\mathbf{T} \in \mathbb{C}^{N_t \times N_t}$ is the beamformer of AN $\mathbf{n} \in \mathbb{C}^{N_t \times 1}$ with $\mathrm{tr}\left(\mathbf{T}\mathbf{T}^H\right) = 1$. Then, the coexisting received signals at Bob and Eve are

$$\boldsymbol{y}_B = \mathbf{H}\boldsymbol{x} + \mathbf{n}_B, \tag{2}$$

$$\boldsymbol{y}_E = \mathbf{G}\boldsymbol{x} + \mathbf{n}_E, \tag{3}$$

where $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$ and $\mathbf{G} \in \mathbb{C}^{N_e \times N_t}$ are the channel matrices corresponding to the Bob's and the Eve's, respectively. In particular, $\mathbf{P}$ is the zero-forcing precoder that ensures one of Bob's antennas being activated, which is given by $\mathbf{P} = \alpha\mathbf{H}^H\left(\mathbf{H}\mathbf{H}^H\right)^{-1}$ and here α is the normalization factor. In this work, we pay attention on a PLS scheme under a scenario that the perfect CSI of Bob's channel is available while a rough CSI of Eve's channel is obtained at Alice. It should be noted that, our studied case considers that Eve is not a regular user, thus the regular message cannot be received from the Alice. Therefore, Alice has only an imprecise estimation of Eve's channel. Particularly, the statistical property of Eve's channel estimation error can be obtained with the aid of the outdated information, which also might be acquired by a sophisticated guess [21]. As a result, an estimation model of Eve's channel should be carefully taken into consideration. Explicitly, the Eve's channel is modeled as

$$\mathbf{G} = \tilde{\mathbf{G}} + \Delta\mathbf{G}, \tag{4}$$

where $\tilde{\mathbf{G}}$ and $\Delta\mathbf{G} \in \mathcal{CN}(\mathbf{0}, \sigma_e^2\mathbf{I}_{N_e \times N_t})$ are the estimated channel and its corresponding estimation error, respectively. In addition, $\mathbf{n}_B$ and $\mathbf{n}_E$ are the independent complex Gaussian noises at Bob and at Eve, which follow $\mathcal{CN}(\mathbf{0}, \sigma_B^2\mathbf{I})$ and $\mathcal{CN}(\mathbf{0}, \sigma_E^2\mathbf{I})$, respectively. Moreover, we assume that $\mathbf{H}$, $\tilde{\mathbf{G}}$, $\Delta\mathbf{G}$, $\mathbf{n}_B$ and $\mathbf{n}_E$ are independent.

III. Proposed Beamformer Design Scheme

A. Proposed algorithm for maximizing the SR

As a result of the prohibitive computational complexity (CC), we circumvent this difficulty by avoiding the mean operation over a large number of noise or channel samples. With the aid of the result in [20], an alternative to the approximate mutual information (AMI) over the legitimate channel can be expressed as

$$R_B(\mathbf{Q}) = \log_2 \sum_{i=1}^{N_r M} \sum_{j=1}^{N_r M} \exp\left(-0.25 P_1 \mathbf{d}_{ij}^H \mathbf{W}_B^{-1} \mathbf{d}_{ij}\right), \tag{5}$$

where $\mathbf{d}_{ij} = \boldsymbol{x}_i - \boldsymbol{x}_j$ and $\boldsymbol{x}_{\{\cdot\}}$ is one of the possible legitimate transmit symbols. Moreover, $\mathbf{W}_B = P_2\mathbf{H}\mathbf{Q}\mathbf{H}^H + \sigma_B^2\mathbf{I}$ and $\mathbf{Q} = \mathbb{E}\left\{\mathbf{T}\mathbf{T}^H\right\}$ is the ANCM with $\mathrm{tr}(\mathbf{Q}) = 1$. It should be noticed that $R_B(\mathbf{Q})$ is a concise form, since the derived AMI of [20] for Bob is $\log_2 2N_rM - R_B(\mathbf{Q})$. Similarly, when a rough CSI of Eve's channel is available at Alice, such a concise AMI over the illegitimate channel can be reduced to the following form:

$$R_E(\mathbf{Q}) = \mathbb{E}_{\Delta\mathbf{G}} \log_2 \sum_{m=1}^{N_r M} \sum_{k=1}^{N_r M} \exp$$
$$\left(-0.25 P_1 \mathbf{d}_{mk}^H \mathbf{P}^H (\tilde{\mathbf{G}} + \Delta\mathbf{G})^H \mathbf{W}_E^{-1} (\tilde{\mathbf{G}} + \Delta\mathbf{G}) \mathbf{P} \mathbf{d}_{mk}\right), \tag{6}$$

where $\mathbf{W}_E = P_2(\tilde{\mathbf{G}} + \Delta\mathbf{G})\mathbf{Q}(\tilde{\mathbf{G}} + \Delta\mathbf{G})^H + \sigma_E^2\mathbf{I}$. By using $R_E(\mathbf{Q})$ and $R_B(\mathbf{Q})$ as our alternatives, the original optimization problem of maximizing the SR is reduced to maximize the

difference between $R_E(\mathbf{Q})$ and $R_B(\mathbf{Q})$, termed as maximizing approximate SR (Max-ASR) optimization algorithm, which avoids averaging over a large number of noise samples. In particular, its effectiveness has been demonstrated in [5]. However, $R_E(\mathbf{Q})$ is still lack of a closed-form expression, which imposes a challenge when designing an effective method for optimizing the beamformer of AN. For this reason, a gradient ascent (GA) algorithm can be utilized for solving the problem. Unfortunately, such a strategy will result in a high CC since sufficient channel samples are generally required to be averaged for accurately evaluating the target and its gradient. Moreover, considering that the solution of the GA-based algorithm is easy to trap in a local optimum, hence it also requires us to repeat the algorithm with different initializations for approaching the optimal solution. In order to circumvent these barriers, firstly, a closed-form expression which is also a lower bound of $R_E(\mathbf{Q})$ is derived, and then a concave problem of the ANCM is formulated. By employing Jensen's inequality, we have

$$R_E(\mathbf{Q}) \geq \log_2 \sum_{m=1}^{N_tM} \sum_{k=1}^{N_tM} \exp\left(-0.25P_1 \times \mathbb{E}_{\Delta\mathbf{G}} \mathbf{d}_{mk}^H \mathbf{P}^H (\tilde{\mathbf{G}} + \Delta\mathbf{G})^H \mathbf{W}_E^{-1} (\tilde{\mathbf{G}} + \Delta\mathbf{G}) \mathbf{P} \mathbf{d}_{mk}\right). \quad (7)$$

In particular, we restrict $\mathbf{Q} \succ 0$ to simplify our optimization problem for ensuring that $\mathbf{Q}$ is invertible, thus obtaining a suboptimal solution. By means of the property of the pseudo-inverse, $(\mathbf{AB})^\dagger = \mathbf{B}^\dagger \mathbf{A}^\dagger$ holds when $\mathbf{A}$ and $\mathbf{B}$ have full column rank and full row rank, respectively [23]. Then we have

$$\mathbf{d}_{mk}^H \mathbf{P}^H (\tilde{\mathbf{G}} + \Delta\mathbf{G})^H \mathbf{W}_E^{-1} (\tilde{\mathbf{G}} + \Delta\mathbf{G}) \mathbf{P} \mathbf{d}_{mk} = \mathbf{d}_{mk}^H \mathbf{P}^H \boldsymbol{\Upsilon}^H \left(P_2 \mathbf{Q} + \sigma_E^2 \boldsymbol{\Lambda}^\dagger\right)^{-1} \boldsymbol{\Upsilon} \mathbf{P} \mathbf{d}_{mk}, \quad (8)$$

where $\boldsymbol{\Upsilon} = (\tilde{\mathbf{G}} + \Delta\mathbf{G})^\dagger (\tilde{\mathbf{G}} + \Delta\mathbf{G})$, and $\boldsymbol{\Lambda} = (\tilde{\mathbf{G}} + \Delta\mathbf{G})^H (\tilde{\mathbf{G}} + \Delta\mathbf{G})$ is not full-rank, hence only pseudo-inverse exists. It is generally intractable for handling (8), therefore we generalize the property of $\left(\mathbf{C} + \mathbf{D}^{-1}\right)^{-1} = \mathbf{C}^{-1} - \mathbf{C}^{-1}\left(\mathbf{D} + \mathbf{C}^{-1}\right)^{-1}\mathbf{C}^{-1}$ to the case of pseudo-inverse by sacrificing some of the accuracy, where both $\mathbf{C}$ and $\mathbf{D}$ are square matrices. Then the term in expression (8) can be rewritten as

$$\left(P_2 \mathbf{Q} + \sigma_E^2 \boldsymbol{\Lambda}^\dagger\right)^{-1} \simeq \frac{1}{P_2}\left[\mathbf{Q}^{-1} - \mathbf{Q}^{-1}\left(\varpi \boldsymbol{\Lambda} + \mathbf{Q}^{-1}\right)^{-1} \mathbf{Q}^{-1}\right], \quad (9)$$

where $\varpi = P_2/\sigma_E^2$. As such, inequality (7) can be further lower bounded as

$$R_E(\mathbf{Q}) \geq \log_2 \sum_{m=1}^{N_rM} \sum_{k=1}^{N_rM} \exp\left\{\frac{-P_1 N_e}{2P_2} \mathbf{d}_{mk}^H \mathbf{P}^H \times \left[\mathbf{Q}^{-1} - \mathbf{Q}^{-1}\left(\varpi \mathbb{E}_{\Delta\mathbf{G}} \boldsymbol{\Lambda} + \mathbf{Q}^{-1}\right)^{-1} \mathbf{Q}^{-1}\right] \mathbf{P} \mathbf{d}_{mk}\right\}. \quad (10)$$

Note that $\Delta\mathbf{G}^H \Delta\mathbf{G} \in \mathbb{C}^{N_t \times N_t}$ is a Hermitian matrix, which obeys the Wishart distribution with N_t degrees of freedom [24]. As a result, we have $\mathbb{E}(\Delta\mathbf{G}^H \Delta\mathbf{G}) = \sigma_e^2 N_r \mathbf{I}_{N_t}$, and

$$\bar{\boldsymbol{\Lambda}} = \mathbb{E}_{\Delta\mathbf{G}} \boldsymbol{\Lambda} = \tilde{\mathbf{G}}^H \tilde{\mathbf{G}} + \sigma_e^2 N_e \mathbf{I}_{N_t}. \quad (11)$$

As a further step, a closed-form expression, that is also a lower bound of R_E, can be derived as

$$R_E(\mathbf{Q}) \geq R_E^c(\mathbf{Q}) = \log_2 \sum_{m=1}^{N_rM} \sum_{k=1}^{N_rM} \exp\left(-0.5P_1 N_e \mathbf{d}_{mk}^H \mathbf{P}^H \left(P_2 \mathbf{Q} + \mathbf{E}\right)^{-1} \mathbf{P} \mathbf{d}_{mk}\right), \quad (12)$$

where $\mathbf{E} = \sigma_E^2 \bar{\boldsymbol{\Lambda}}^{-1}$. Therefore, the optimization problem of the Max-ASR can be further reduced to

$$\begin{aligned} \max \ & R_s^a(\mathbf{Q}) = R_E^c(\mathbf{Q}) - R_B(\mathbf{Q}) \\ s.t. \ & \mathrm{tr}(\mathbf{Q}) = 1, \ \mathbf{Q} \succ 0. \end{aligned} \quad (13)$$

Now the optimization target of $R_s^a(\mathbf{Q})$ has a closed form. However, problem (13) is non-concave since both $R_E^c(\mathbf{Q})$ and $R_B(\mathbf{Q})$ do not have any convexities. Specifically, $R_E^c(\mathbf{Q})$ is the combination of $-0.5P_1 N_e \mathbf{d}_{mk}^H \mathbf{P}^H \left(P_2 \mathbf{Q} + \mathbf{E}\right)^{-1} \mathbf{P} \mathbf{d}_{mk}$ (concave, $\mathbf{Q} \succ 0$) and $\log \sum \exp(\cdot)$ (only has convexity-preserving), hence it is non-convex. Moreover, $R_B(\mathbf{Q})$ has a similar nature. As a result, $R_s^a(\mathbf{Q})$, which is a difference between a pair of non-convex functions, is thus non-concave. In order to address this difficulty, we aim for transforming problem (13) into a concave maximization problem in the following part. For this purpose, two slack variables, $\boldsymbol{\Upsilon}_B \in \mathbb{C}^{N_r \times N_r}$ and $\boldsymbol{\Upsilon}_E \in \mathbb{C}^{N_e \times N_e}$, are invoked to reformulate problem (13) as follows

$$\begin{aligned} \max \ & f_E(\boldsymbol{\Upsilon}_E)/f_B(\boldsymbol{\Upsilon}_B) && (14a) \\ s.t. \ & \boldsymbol{\Upsilon}_E \succeq \mathbf{P}^H \left(P_2 \mathbf{Q} + \mathbf{E}\right)^{-1} \mathbf{P}, && (14b) \\ & \boldsymbol{\Upsilon}_B \preceq \mathbf{W}_B^{-1}(\mathbf{Q}), && (14c) \\ & \mathrm{tr}(\mathbf{Q}) = 1, \ \mathbf{Q} \succ 0, && (14d) \end{aligned}$$

where

$$f_E(\boldsymbol{\Upsilon}_E) = \sum_{m=1}^{N_rM} \sum_{k=1}^{N_rM} \exp\left(-0.5P_1 N_e \mathbf{d}_{mk}^H \boldsymbol{\Upsilon}_E \mathbf{d}_{mk}\right), \quad (15)$$

$$f_B(\boldsymbol{\Upsilon}_B) = \sum_{i=1}^{N_rM} \sum_{j=1}^{N_rM} \exp\left(-0.25P_1 \mathbf{d}_{ij}^H \boldsymbol{\Upsilon}_B \mathbf{d}_{ij}\right). \quad (16)$$

The main benefit of invoking $\boldsymbol{\Upsilon}_B$ and $\boldsymbol{\Upsilon}_E$ is that $R_s^a(\mathbf{Q})$ is transformed into a ratio of convex function, i.e., $f_E(\boldsymbol{\Upsilon}_E)/f_B(\boldsymbol{\Upsilon}_B)$. Correspondingly, (14b) and (14c) should be added to ensure that the modified optimization problem is equivalent to problem (13). It can be noted that (14a) is a fractional programming function, which is non-concave. Moreover, (14c) is also non-convex with respect to $\mathbf{Q}$. To this end, we can expand $f_E(\boldsymbol{\Upsilon}_E)$ at a feasible point $\boldsymbol{\Upsilon}_{E,0}$, and then formulating a lower bound with the aid of its convexity, which is given by

$$f_E(\boldsymbol{\Upsilon}_E) \geq f_E^o(\boldsymbol{\Upsilon}_E) = f_E(\boldsymbol{\Upsilon}_{E,0}) + \nabla_{\boldsymbol{\Upsilon}_{E,0}} f_E(\boldsymbol{\Upsilon}_E)\left(\boldsymbol{\Upsilon}_E - \boldsymbol{\Upsilon}_{E,0}\right), \quad (17)$$

where $f_E(\boldsymbol{\Upsilon}_{E,0})$ is a constant that depends on $\boldsymbol{\Upsilon}_{E,0}$, and its gradient is given by

$$\nabla_{\boldsymbol{\Upsilon}_{E,0}} f_E(\boldsymbol{\Upsilon}_E) = -0.5P_1 N_e \times \sum_{m=1}^{N_rM} \sum_{k=1}^{N_rM} \mathbf{d}_{mk} \mathbf{d}_{mk}^H \exp\left(-0.5P_1 N_e \mathbf{d}_{mk}^H \boldsymbol{\Upsilon}_E \mathbf{d}_{mk}\right). \quad (18)$$

Herein, $f_E^o(\boldsymbol{\Upsilon}_E)$ is a linear function with respect to $\boldsymbol{\Upsilon}_E$. For (14c), we have

$$\begin{aligned}\mathbf{W}_B^{-1}(\mathbf{Q}) &\succeq \mathbf{W}_B^o(\mathbf{Q}) \\ &= \mathbf{W}_{B,\mathbf{Q}_0}^{-1} - P_2\mathbf{W}_{B,\mathbf{Q}_0}^{-1}\mathbf{H}\left(\mathbf{Q}-\mathbf{Q}_0\right)\mathbf{H}^H\mathbf{W}_{B,\mathbf{Q}_0}^{-1}, \end{aligned} \quad (19)$$

where $\mathbf{W}_{B,\mathbf{Q}_0}^{-1}$ is the matrix at the feasible point $\mathbf{Q}_0$. Equation (19) holds based on the fact that $\mathbf{W}_B^{-1}(\mathbf{Q})$ is convex of $\mathbf{Q}$ and the property of matrix inverse, given by

$$\begin{aligned}\nabla_{\mathbf{Q}}\mathbf{W}_B^{-1}(\mathbf{Q}) &= \nabla_{\mathbf{Q}}\left(P_2\mathbf{H}\mathbf{Q}\mathbf{H}^H + \sigma_B^2\mathbf{I}_{N_r}\right)^{-1} \\ &= -P_2\mathbf{W}_B^{-1}(\mathbf{Q})\mathbf{H}\nabla\mathbf{Q}\mathbf{H}^H\mathbf{W}_B^{-1}. \end{aligned} \quad (20)$$

Consequently, problem (14) can be transformed as follows:

$$\begin{aligned} \max\ & f_E^o(\boldsymbol{\Upsilon}_E) - \lambda f_B(\boldsymbol{\Upsilon}_B) && (21a)\\ s.t.\ & \boldsymbol{\Upsilon}_E \succeq \mathbf{P}^H\left(P_2\mathbf{Q}+\mathbf{E}\right)^{-1}\mathbf{P}, && (21b)\\ & \boldsymbol{\Upsilon}_B \preceq \mathbf{W}_B^o(\mathbf{Q}), && (21c)\\ & \mathsf{tr}(\mathbf{Q}) = 1,\ \mathbf{Q}\succ 0, && (21d)\end{aligned}$$

where λ is an auxiliary variable, iteratively updated by

$$\lambda[n+1] = f_E(\boldsymbol{\Upsilon}_{E,n})/f_B(\boldsymbol{\Upsilon}_B), \quad (22)$$

where n is the iteration index. The convergence can be guaranteed by alternatively updating λ using (22) and solving it for $\mathbf{Q}$ with the aid of (21), since λ is nondecreasing after each iteration. The details are shown in Algorithm 1, in which ϵ is the convergence tolerance.

Algorithm 1 Proposed Algorithm for Solving Problem (13).

Initialize: Given feasible points, λ_0, $\boldsymbol{\Upsilon}_{E,0}$ and $\mathbf{Q}_0$, and set iterative counter n=0.

repeat

1. Solve problem (21) with λ_0, $\boldsymbol{\Upsilon}_{E,0}$ and $\mathbf{Q}_0$, and obtain the current optimal solutions $\boldsymbol{\Upsilon}_E^*$ and $\mathbf{Q}^*$; n=n+1.
2. Update $\boldsymbol{\Upsilon}_{E,n}$=$\boldsymbol{\Upsilon}_E^*$, $\mathbf{Q}_n$=$\mathbf{Q}^*$ and $\lambda_n = \frac{f_E(\boldsymbol{\Upsilon}_{E,n})}{f_B(\boldsymbol{\Upsilon}_B)}$.

until $|f_E(\boldsymbol{\Upsilon}_{E,n}) - \lambda_n f_B(\boldsymbol{\Upsilon}_B)| \le \epsilon$ is satisfied.

return $\mathbf{Q}$=$\mathbf{Q}_n$.

B. Complexity analysis

The CCs of the Max-ASR method and our proposed algorithm are compared in this subsection, where the number of floating-operations (Flops) is evaluated. In terms of the Max-ASR method, its CC is related to: ASR, its gradient and the number of iterations. Particularly, the CC of computing the inverse of a square matrix is approximately as the cube of its size. Therefore, the CC of the Max-ASR scheme becomes $\mathcal{O}_{\text{Max-ASR}} = D_1(\mathcal{C}_{\text{ASR}} + \mathcal{C}_{\text{G-ASR}})$, where D_1 is the number of iterations in the GA-based algorithm, $\mathcal{C}_{\text{ASR}} = N_{\text{samp}}N_r^2M^2(4N_eN_t+4N_rN_t^2+2N_e^2+N_r^3)+N_r^2M^2(2N_r^2+2N_r)$, and $\mathcal{C}_{\text{G-ASR}} \approx 2N_{\text{samp}}N_r^2M^2(N_rN_t^2+N_r^3)$. By comparison, the CC of our proposed algorithm can be approximately expressed as $\mathcal{O}_{\text{Max-CSR}} \approx D_2(n(N_t+N_r)^{3.5}+2N_r^4M^2)$, where n and D_2 are the decision variable and the corresponding number of iterations, respectively. Hence, it can be readily observed that the CC of our proposed algorithm is much lower than that of the Max-ASR method due to $N_{\text{samp}} \gg N_t > N_r$.

IV. Simulation Results and Discussion

In what follows, numerical simulations are shown to evaluate the SR performance for our proposed AN design strategy, where the NSP method [16], and the method which directly maximizes the ASR, i.e., $\max_{\mathbf{Q}=\mathbf{T}\mathbf{T}^H} R_E(\mathbf{Q}) - R_B(\mathbf{Q})$, are introduced as the performance benchmarks. Specifically, the Max-ASR scheme exploits GA strategy to find the best $\mathbf{T}$ for maximizing $R_E(\mathbf{Q}) - R_B(\mathbf{Q})$. Moreover, considering the fact that the solution of the Max-ASR method easily traps into a local maxima, we repeat the Max-ASR algorithm with 5 different initializations and then choose the solution with the highest ASR as our anticipated result. In addition, the iterative termination condition is set as $\epsilon = 0.001$, and the total power is constrained by $P = N_r$. Moreover, the noise levels at Bob and at Eve are assumed to be identical, i.e., $\sigma_B^2 = \sigma_E^2$. The ergodic SR is obtained by averaging over 500 random channel realizations.

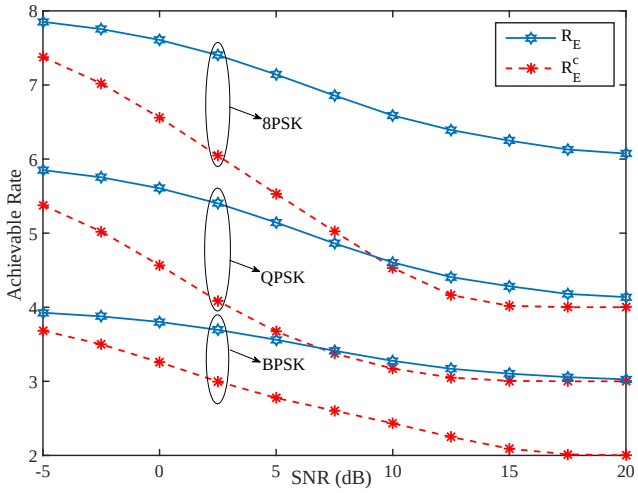

Fig. 1. Comparison of $R_E(\mathbf{Q})$ and $R_E^c(\mathbf{Q})$, where $N_r = 2, N_e = 2$ and $N_t = 6$.

Fig. 1 compares the non-closed form $R_E(\mathbf{Q})$ and our derived closed term $R_E^c(\mathbf{Q})$ for three typical modulation types (BPSK, QPSK, 8PSK), when $\sigma_e^2 = 0.1$. It can be observed that both $R_E(\mathbf{Q})$ and $R_E^c(\mathbf{Q})$ increase upon increasing the modulation size, but $R_E^c(\mathbf{Q})$ is consistently lower than $R_E(\mathbf{Q})$ for each modulation type in the whole SNR region. In particular, we note that the CPU time (Intel Core-i5-7400, 3.0 GHz) of evaluating R_E is about 2.503086s while that of evaluating $R_E^c(\mathbf{Q})$ is only about 0.005006s, when the modulation type is 8PSK and the number of the experimental channel samples ($\mathbb{E}_{\Delta\mathbf{G}}$) is 800. This implies that a significant computational amounts can be saved by employing $R_E^c(\mathbf{Q})$ as an alternative of $R_E(\mathbf{Q})$.

Fig. 2 shows the achievable SR versus SNR for three different estimation errors of Eve's channel ($\sigma_e^2 = 0.1, 0.25, 0.5$). We observe that the SR performance of our proposed scheme is better than that of the existing NSP method, even as $\sigma_e^2 = 0.5$. This is mainly owing to the fact that for the NSP method, the projection matrix is merely created based on the legitimate channel, which just aims for avoiding Bob's decoding, but regardless of the characteristic of Eve's channel

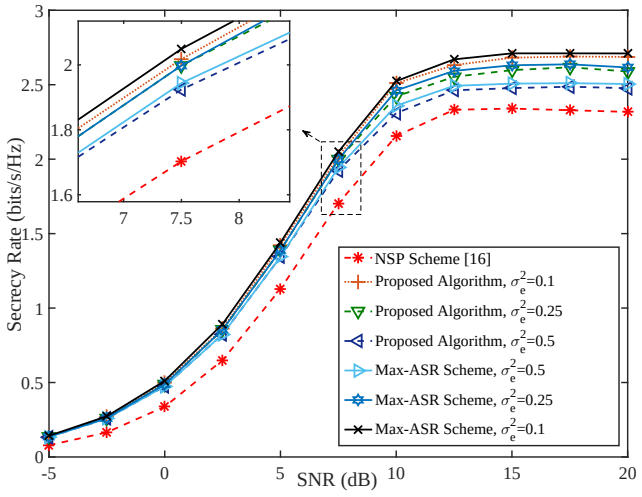

Fig. 2. Achievable SR versus SNR for $\sigma_e^2 = 0.1, 0.25, 0.5$, where $N_t = 6, N_r = N_e = 2$, and the modulation type is QPSK.

or the modulation type. In other words, the NSP method dispenses with a holistic consideration of secure transmission, albeit it is simple. Moreover, it can be observed from Fig. 2 that, for any of the three typical estimation errors, our proposed algorithm consistently performs close to the high-complexity Max-ASR scheme in terms of the SR performance attained, yet avoids the cumbersome expectation operation over $\Delta\mathbf{G}$. This result verifies the efficiency of our proposed algorithm. On the other hand, we note that the SR gap among the cases with the different estimation error can be negligible when SNR is lower than 7.5dB. The reason behind this trend is that the most influential factor is the precoder $\mathbf{P}$ in the low-SNR region. Upon increasing the SNR, such a factor turns to be $\mathbf{Q}$, which also illustrates why the SR gaps become apparent. In summary, our proposed algorithm harvests a obvious SR gain compared with the NSP scheme, and enjoys almost the same SR performance as the high-complexity Max-ASR scheme.

V. Conclusion

This work studied an AN-based strategy for enhancing the security of PSM networks. To circumvent the expectation operation over a large number of channel samples, a loose bound of the ASR in a closed form was derived for reducing CC when optimizing ANCM. Based upon this bound, a near-optimal iterative solution was proposed for the simplified Max-SR optimization problem. Our simulation results showed that the proposed scheme obtains a significant SR improvement compared with the existing NSP method, albeit in the case of a relatively large estimation error of Eve's channel. Additionally, the efficiency of our proposed algorithm was verified upon comparing with the Max-ASR scheme in terms of the SR performance attained. Our work will focus on tackling the SR maximization problem in the presence of both imperfect CSIs of Bob's channel and Eve's channel.

References

[1] R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2228–2241, Jul. 2008.

[2] M. Di Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, "Spatial modulation for generalized MIMO: Challenges, opportunities, and implementation," *Proc. IEEE*, vol. 102, no. 1, pp. 56–103, Jan. 2014.

[3] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Spatial modulation: optimal detection and performance analysis," *IEEE Commun. Lett.*, vol. 12, no. 8, pp. 545–547, Aug. 2008.

[4] R. Zhang, L. L. Yang, and L. Hanzo, "Error probability and capacity analysis of generalised pre-coding aided spatial modulation," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 364–375, Jan. 2015.

[5] G. Xia, F. Shu, Y. Zhang, J. Wang, S. ten Brink, and J. Speidel, "Antenna selection method of maximizing secrecy rate for green secure spatial modulation," *IEEE Trans. Green Commun. and Netw.*, vol. 3, no. 2, pp. 288–301, Jun. 2019.

[6] Z. Huang, Z. Gao, and L. Sun, "Anti-eavesdropping scheme based on quadrature spatial modulation," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 532–535, Mar. 2017.

[7] F. Shu, Z. Wang, R. Chen, Y. Wu, and J. Wang, "Two high-performance schemes of transmit antenna selection for secure spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8969–8973, Sep. 2018.

[8] R. Zhang, L. Yang, and L. Hanzo, "Generalised pre-coding aided spatial modulation," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5434–5443, Nov. 2013.

[9] Y. Lin, R. Zhang, L. Yang, and L. Hanzo, "Secure user-centric clustering for energy efficient ultra-dense networks: Design and optimization," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1609–1621, Jul. 2018.

[10] Y. Tang, J. Xiong, D. Ma, and X. Zhang, "Robust artificial noise aided transmit design for MISO wiretap channels with channel uncertainty," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2096–2099, Nov. 2013.

[11] P. Lin, S. Lai, S. Lin, and H. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Area. Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[12] Z. Zhu, Z. Chu, N. Wang, S. Huang, Z. Wang, and I. Lee, "Beamforming and power splitting designs for AN-aided secure multi-user MIMO SWIPT systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2861–2874, Dec. 2017.

[13] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[14] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[15] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1417–1432, Dec. 2016.

[16] F. Wu, R. Zhang, L. L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[17] Y. Chen, L. Wang, Z. Zhao, M. Ma, and B. Jiao, "Secure multiuser MIMO downlink transmission via precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1116–1119, Jun. 2016.

[18] F. Wu, L. L. Yang, W. Wang, and Z. Kong, "Secret precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1544–1547, Sep. 2015.

[19] G. Xia, Y. Lin, T. Liu, F. Shu, and L. Hanzo, "Transmit antenna selection and beamformer design for secure spatial modulation with rough CSI of Eve," 2019. [Online]. Available: https://arxiv.org/abs/1905.10088.

[20] S. R. Aghdam and T. M. Duman, "Joint precoder and artificial noise design for MIMO wiretap channels with finite-alphabet inputs based on the cut-off rate," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3913–3923, Jun. 2017.

[21] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[22] Y. Wu, J. B. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3614–3628, Aug. 2017.

[23] K. Petersen and M. Pedersen, *The Matrix Cookbook*. Technical University of Denmark (DTU), 2006.

[24] M. Matthaiou, M. R. Mckay, P. J. Smith, and J. A. Nossek, "On the condition number distribution of complex Wishart matrices," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1705–1717, Jun. 2010.