High-performance Power Allocation Strategies for Secure Spatial Modulation

Feng Shu, Xiaoyu Liu, Guiyang Xia, Tingzhen Xu, Jun Li, and Jiangzhou Wang, Fellow, IEEE

Abstract—Optimal power allocation (PA) strategies can make a significant rate improvement in secure spatial modulation (SM). Due to the lack of secrecy rate (SR) closed-form expression in secure SM networks, it is hard to optimize the PA factor. In this paper, two PA strategies are proposed: gradient descent (GD), and maximum product of signal-to-interference-plus-noise ratio (SINR) and artificial-noise-to-signal-plus-noise ratio (ANSNR)(Max-P-SINR-ANSNR). The former is an iterative method and the latter is a closed-form solution. Compared to the former, the latter is of low-complexity. Simulation results show that the proposed two PA methods can approximately achieve the same SR performance as exhaustive search method and perform far better than three fixed PA ones. With extremely low complexity, the SR performance of the proposed Max-P-SINR-ANSNR performs slightly better and worse than that of the proposed GD in the low to medium, and high signal-to-noise ratio regions, respectively.

Index Terms—Spatial modulation, secure, secrecy rate, power allocation, and product

I. INTRODUCTION

In multiple-input-multiple-output (MIMO) systems, spatial modulation (SM) [1] was proposed as the third method to strike a good balance between spatial multiplexing and diversities while Bell Laboratories Layer Space-Time (BLAST) in [2] and space time coding (STC) in [3] were the first two ways. Unlike BLAST and STC, SM exploits both indices of activated antenna and modulation symbols to transmit information, which can increase the spectral efficiency and reduce the complexity and cost of multiple-antenna schemes without deteriorating the end-to-end system performance and still guaranteeing good data rates [4]. Compared to BLAST and STC, SM has a higher energy-efficiency due to the use of less active RF chains. Moreover, the information-theoretic in space modulation techniques (SMTs) is deduced in [5]. It is demonstrated that SMTs can achieve higher rate gains over the conventional MIMO systems. Recently, a new spatial modulation technique for MIMO systems, spatial lattice modulation, was proposed in [6], which jointly exploited spatial, in-phase, and quadrature dimensions to carry information bits and it achieved a high spectral efficiency.

This work was supported in part by the National Natural Science Foundation of China (Nos. 61771244, 61472190, 61501238, 61801453, 61702258, and 61271230).

Feng Shu, Xiaoyu Liu, Guiyang Xia, Tingzhen Xu, and Jun Li are with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, 210094, CHINA. (Email: shufen0101@163.com).

Feng Shu is also with the School of Computer and information at Fujian Agriculture and Forestry University, Fuzhou, 350002, China.

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.

How to enable SM to transmit confidential messages securely is an attractive and significantly important problem [7]–[9]. In [10], the authors analyzed the secrecy rate (SR) of SM for multiple-antenna destination and eavesdropper receivers. Instead of typical requirements for eavesdropper channel information, they investigated the security performance through joint signal and interference transmissions. Furthermore, the authors in [11] proposed and investigated a full-duplex receiver assisted secure spatial modulation scheme. It enhances the security performance through the interference sent by the full duplex legitimate receiver. In [9], the authors proposed two novel transmit antenna selection methods: leakage and maximum SR, and one generalized Euclidean distance-optimized antenna selection method for secure SM networks.

In a secure directional modulation system [12], power allocation (PA) between confidential message and artificial noise (AN) was shown to have an about 60 percent improvement on SR performance. Similarly, PA is also crucial for secure SM with the aid of AN. In [13], the optimal PA factor between signal and interference transmission was given by exhaustive search (ES) for precoding-aided spatial modulation. However, the computational complexity of ES is very high for a very small search step-size. Therefore, a low-complexity PA method is preferred for practical applications. By focusing on PA strategies in secure SM, our main contributions in this paper are as follows:

1) To reduce the computational complexity, using an approximate SR expression to the actual SR, we establish the optimization problem of maximizing SR over PA factor given AN projection matrix. A gradient descent (GD) algorithm is adopted to address this problem. The proposed GD converges to the locally optimal point. However, it is not guaranteed to converge the globally optimal point and may approach the optimal point by increasing the number of random initializations. Additionally, it is also an iterative method, and depend heavily on its termination condition.

2) To address the above iterative convergence problem of the proposed GD, a novel method, called maximizing the product of signal-to-interference-plus-noise ratio (SINR) and artificial-noise-to-signal-plus-noise ratio (ANSNR)(Max-P-SINR-ANSNR), is proposed to provide a closed-form expression. This significantly reduces the complexity of GD. Simulation results show that the proposed Max-P-SINR-ANSNR can achieve a SR performance close to that of optimal ES. This makes it become a promising practical PA strategy.
Thus, the proposed Max-P-SINR-ANSNR method can achieve a high SR performance, with an extremely low-complexity, which shows a slight SR performance loss over the optimal ES.

The remainder is organized as follows. Section II describes system model of secure SM system and express the average SR. In Section III, two PA strategies are proposed for secure SM and their computational complexities are also analyzed. We present our simulation results in Section IV. Finally, we draw conclusions in Section V.

II. SYSTEM MODEL

![Block diagram of secure SM](image)

Fig. 1 sketches a secure SM system with $N_a$ transmit antennas (TAs) at transmitter (Alice). In particular, in this setting, $N_r$ and $N_e$ receive antennas (RAs) are employed at desired receiver (Bob) and eavesdropping receiver (Eve), respectively. And confidential information will be intercepted by Eve. Additionally, the size of signal constellation $M$ is $M$. For a SM system, the number of the active transmit antennas should be a power of 2. Thus, $N_t$ active antennas are chosen from $N_a$, where $N_t$ is equal to $2^{\lceil \log_2 N_a \rceil}$. As a result, $\log_2 N_t + \log_2 M$ bits can be transmitted per channel use, where $\log_2 N_t$ bits are used to select one active antenna and the remaining $\log_2 M$ bits are used to form a constellation symbol. Similar to the secure SM model in [9], the transmit signal with the help of AN can be represented by

$$s = \sqrt{\beta} Pe_b b_j + \sqrt{(1-\beta)PT_{AN}} n.$$  

(1)

where $\beta \in [0, 1]$ is the PA factor, $P$ denotes the total transmit power constraint and $T_{AN} \in \mathbb{C}^{N_t \times N_r}$ is the AN projection matrix. $e_i$ is the $i$-th column of identity matrix $I_{N_t}$, implying that the $i$-th antenna is chosen to transmit symbol $b_j$, where $b_j, j \in \{1, 2, \ldots, M\}$ is the $j$-th input symbol from the $M$-ary signal constellation. In addition, $n \in \mathbb{C}^{N_t \times 1}$ is the AN vector. The receive signals at the desired and eavesdropping receivers are

$$y_B = \sqrt{\beta} H S e_b b_j + \sqrt{(1-\beta)PHST_{AN} n + n_B},$$  

(2)

$$y_E = \sqrt{\beta} G S e_b b_j + \sqrt{(1-\beta)PGST_{AN} n + n_E},$$  

(3)

where $H \in \mathbb{C}^{N_r \times N_a}$ and $G \in \mathbb{C}^{N_e \times N_a}$ are the channel gain matrices from Alice to Bob and to Eve, with each elements of $H$ and $G$ obeying the Gaussian distribution with zero mean and unit variance. $S \in \mathbb{R}^{N_a \times N_t}$ is the transmit antennas selection matrix constituted by the specifically selected $N_t$ columns of $I_{N_a}$, which is determined by the leakage-based method in [8]. Additionally, $n_B \in \mathbb{C}^{N_r \times 1}$ and $n_E \in \mathbb{C}^{N_e \times 1}$ are the complex Gaussian noises at Bob and Eve with $n_B \sim \mathcal{CN}(0, \sigma_B^2 I_{N_r})$ and $n_E \sim \mathcal{CN}(0, \sigma_E^2 I_{N_e})$, respectively. For a specific channel realization, the mutual information of Bob and Eve are as follows

$$I_g(x; y'_B) = \log_2 N_t M - N_t^2 \sum_{i=1}^{N_t} \sum_{j=1}^{N_t} \exp\left(-f_{g, i,j} + \|n'_E\|^2\right)$$

(4)

where $x = e_b b_j$, and $y'_B = W_B^{-1/2} y_g$. $g$ stands for B (Bob) or E (Eve). $f_{g, i,j} = \|\sqrt{\beta} H \cdot T_{AN} \cdot e_c b_j + n_B\|^2$, and $f_{g, m,k} = \|\sqrt{\beta} G \cdot T_{AN} \cdot e_c b_j + n_E\|^2$, where $H_s = HS, G_s = GS, n_B = W_B^{-1/2} (\sqrt{(1-\beta)PT_{AN} n + n_B})$, and $n_E = W_E^{-1/2} (\sqrt{(1-\beta)PGST_{AN} n + n_E})$. Here, $d_{ij} = x_i - x_j$, $d_{mk} = x_m - x_k$, $x_i, x_j, x_m$ and $x_k$ is one of possible transmit vectors in the set of combining antenna and all possible symbols. Here, $W_B(W_B$ or $W_E)$ is the corresponding covariance matrix of interference plus noise of Bob or Eve, where $W_B = (1-\beta)PC_g + \sigma_B^2 I_{N_t}$, with $C_B = H \cdot T_{AN} \cdot e_c b_j$ and $C_E = G \cdot T_{AN} \cdot e_c b_j$, respectively. According to [10], we know that pre-multiplying $y_B$ and $y_E$ by $W_B^{-1/2}$ and $W_E^{-1/2}$ is to whiten a colored noise plus AN into a white noise, and does not change the mutual information. In other words, $I(x; y_g) = I(x; y'_B)$. Finally, the average SR is given as

$$R_s = E_{H,G} [I(x; y_B) - I(x; y_E)]^+.$$  

(5)

where $[a]^+ = \max(a, 0)$ and $R_s = I(x; y_B) - I(x; y_E)$ is the instantaneous SR for a specific channel realization. Here, we assume that the ideal knowledge of $H$ and $G$ are available at the transmitter per channel use, in the case the eavesdropper is a participating user in a wiretap network [4]. The optimization problem can be casted as

$$\max R_s \quad \text{subject to } 0 < \beta < 1.$$  

(6)

III. TWO PROPOSED PA STRATEGIES

A. Proposed GD method

Due to the expression of SR lacks closed-form, it is hard for us to design a valid method to optimize PA factor effectively. Although ES in [13] can be employed to search out the optimal PA factor, the high complexity restricts its application.
for secure SM systems. With that in mind, the cut-off rate with closed-form for traditional MIMO systems in [14] can be extended to the secure SM systems, which is an efficient metric to optimize the PA factor below, and given by

$$R_s^B = I_0^B - I_0^E,$$  

(7)

where $I_0^B$ is the cut-off rate for Bob,

$$I_0^B = 2\log_2 N_t M - \sum_{i=1}^{N_t} \sum_{j=1}^{M} \log_2 \left( 1 + \frac{-\beta P d_{ij}^H H_s^H W^{-1} H_s d_{ij}}{4} \right),$$  

(8)

which can be derived similarly to Appendix A in [14] with a slight modification. Similarly, the cut-off rate $I_0^E$ is given by

$$I_0^E = 2\log_2 N_t M - \sum_{m=1}^{N_t} \sum_{k=1}^{M} \log_2 \left( 1 + \frac{-\beta P d_{mk}^H G_s^H W^{-1} G_s d_{mk}}{4} \right).$$  

(9)

Substituting (8) and (9) into (7), the optimization problem can be converted into

$$\max R_s^B \text{ subject to } 0 \leq \beta \leq 1,$$  

(10)

where $R_s^B = \log_2 \kappa_B(\beta) - \log_2 \kappa_B(1)$,

$$\kappa_B(\beta) = \sum_{i=1}^{N_t} \sum_{j=1}^{M} \exp \left( -\beta P d_{ij}^H H_s^H \omega_B(\beta) H_s d_{ij} \right),$$  

(11)

$$\kappa_B(\beta) = \sum_{m=1}^{N_t} \sum_{k=1}^{M} \exp \left( -\beta P d_{mk}^H G_s^H \omega_E(\beta) G_s d_{mk} \right),$$  

(12)

and $\omega_B(\beta) = W^{-1} H_s$ and $\omega_E(\beta) = W^{-1} G_s$. It is seen that the optimization problem (10) is non-convex because the terms $\log_2 \kappa_B(\beta)$ and $\log_2 \kappa_B(1)$ of the objective function are non-concave. To maximize $R_s^B$, GD method can be employed to directly optimize the PA factor, and the gradient of $R_s^B$ is derived as

$$\nabla_\beta R_s^B = \frac{P}{\ln^2 \kappa_B} \sum_{i=1}^{N_t} \sum_{j=1}^{M} \chi_B \cdot \exp \left( -\beta P d_{ij}^H H_s^H \omega_B(\beta) H_s d_{ij} \right),$$  

(13)

where

$$\chi_B = 0.25 \left\{ d_{ij}^H H_s^H \omega_B(\beta) H_s d_{ij} + \beta P d_{ij}^H H_s^H C_B \omega_B(\beta) H_s d_{ij} \right\},$$  

(14)

$$\chi_E = 0.25 \left\{ d_{mk}^H G_s^H \omega_E(\beta) G_s d_{mk} + \beta P d_{mk}^H G_s^H C_E \omega_E(\beta) G_s d_{mk} \right\},$$  

(15)

where the second terms of the right-hand side in (14) and (15) hold based on the fact that $\nabla (X^{-1}) = -X^{-1} \nabla (X) X^{-1}$, where $\nabla (\cdot)$ denotes the gradient operation. So as to get a better PA factor, we can repeat the algorithm with different initial values and find out the best $\beta$ that have the highest SR. Moreover, it is guaranteed that the best solution of GD method converges to the global optimal solution as the number of initial randomizations tends to be large.

B. Proposed Max-P-SINR-ANSNR method

In order to avoid the iterative process for obtaining PA factor, a closed-form solution may be preferred. Now, AN is viewed as the useful signal of Eve. The SINR at Eve is defined as ANSNR. If the product of SINR at Bob and ANSNR at Eve is maximized, it is guaranteed that at least one of SINR at Bob and ANSNR at Eve or both is high. This will accordingly improve SR. From the definition of SINR, the SINR of Bob and ANSNR of Eve are defined as

$$\text{SINR}_B(\beta) = \frac{1}{N_r} \beta P tr(H_s H_s^H) \left( 1 - \beta \right) P tr(C_B) + N_r \sigma_n^2,$$  

(16)

and

$$\text{ANSNR}_E(\beta) = \frac{(1 - \beta) P tr(G_s G_s^H) + N_r \sigma_e^2}{N_r \beta P tr(G_s G_s^H) + N_r \sigma_e^2},$$  

(17)

respectively. Observing the above two definitions, as $\beta$ varies from 0 to 1, SINR$_B$ increases and ANSNR$_E$ decreases. Thus, they are two conflicting cost functions. If we multiply SINR$_B$ and ANSNR$_E$, their product will form a maximum value at some point in the interval [0, 1] due to their rational property. Their product is defined as follows

$$f(\beta) = \text{SINR}_B \times \text{ANSNR}_E = \frac{a_b a_e \beta (1 - \beta)}{|(1 - \beta) b_b + c_b (\beta b_e + c_e)|},$$  

(18)

where $a_b = \frac{1}{N_r} P tr(H_s H_s^H)$, $a_e = P tr(C_E)$, $b_b = P tr(C_B)$, $c_b = N_r \sigma_n^2$, $b_e = \frac{1}{N_r} P tr(G_s G_s^H)$ and $c_e = N_r \sigma_e^2$. Therefore, the corresponding optimization problem is established as

$$\max \beta f(\beta) \text{ subject to } 0 \leq \beta \leq 1,$$  

(19)

which gives the derivative of cost function $f(\beta)$ as

$$f'(\beta) = \frac{d f(\beta)}{d \beta} = \frac{-a_b a_e (a \beta^2 + 2b \beta - b)}{|(b_b (1 - \beta) + c_b (\beta b_e + c_e))^2|} = 0,$$  

(20)

where $a = c_b b_e - c_e b_b$, and $b = c_b b_e + c_e c_b$. The above equation generates the two candidate solutions to (19)

$$\beta_1 = \frac{-b - \sqrt{b^2 + 2ab}}{a}, \quad \beta_2 = \frac{-b + \sqrt{b^2 + 2ab}}{a}.$$

(21)

Considering the constraint $0 \leq \beta \leq 1$ of (19), we have the set of all four potential solutions as follows

$$S = \{ \beta_1, \beta_2, \beta_3 = 0, \beta_4 = 1 \}.$$  

(22)

It is clear that $\beta_1 = 0$ means that no power is allocated to the useful signal, namely no mutual information is sent. In other words, SR equals zero. Since $a$ is positive, we can infer $\beta_1 < 0$. It is impossible because $\beta$ belongs to the interval [0, 1]. $\beta_1$ and $\beta_3$ should be removed from set $S$. Since the denominator of (20) is positive, it is clear that $f'(\beta)$ is negative.
when $\beta > \beta_2$ and $f'(\beta)$ is positive when $\beta < \beta_2$. Therefore, $\beta_2$ is a local maximum point and $\beta_4$ is a local minimum point.

Finally, we conclude that the optimal solution to (19) is

$$\beta_2 = \frac{-b + \sqrt{b^2 + 4ab}}{2a}. \quad (23)$$

Below, we present a direct simple proof to show the fact that maximizing the product in (18) can reach a high SR. For SINR$_B(\beta)$ and ANSNR$_E(\beta)$, $N_t$$\sigma_B^2$ and $N_e$$\sigma_B^2$ are fixed when the power of noise is given. In order to obtain a high SR, the average powers of the two useful receive signals $\sqrt{\beta_1}$$\mathbf{H}_{(i)}n$ and $\sqrt{1-\beta_1}$$\mathbf{H}_{ST}n$ for Bob and Eve in (2) and (3) should be as large as possible while the average powers of the two noise signals $\sqrt{1-\beta_1}$$\mathbf{H}_{ST}n$ and $\sqrt{1-\beta_1}$$\mathbf{H}_{ST}n$ in (2) and (3) should be as small as possible in (18). The former implies that the product of numerators of SINR$_B(\beta)$ and ANSNR$_E(\beta)$ should be as large as possible. The latter means that the corresponding product of their denominators should be as small as possible. Naturally, we can make an conclusion that maximizing the product of SINR$_B(\beta)$ and ANSNR$_E(\beta)$ can achieve a high SR performance.

### IV. Simulation and Numerical Results

To evaluate the SR performance of the two proposed PA strategies, system parameters are set as follows: $N_t = 4$, $N_r = 2$, $N_e = 2$, and quadrature phase shift keying (QPSK) modulation. At the same time, for the convenience of simulation, it is assumed that the total transmit power $P = N_t$ and the noise variances are identical, i.e., $\sigma_B^2 = \sigma_E^2$.

![Comparison of average SR versus SNR for different PA strategies](image)

**Fig. 2.** Comparison of average SR versus SNR for different PA strategies with $N_t = 4$, $N_r = 2$, and $N_e = 2$.

Fig. 2 demonstrates the average SR versus SNR for different PA strategies, where optimal ES method is used as a performance upper bound. It can be clearly seen from Fig. 2 that the performance of the proposed GD and Max-P-SINR-ANSNR are closer to the optimal security performance in the low and medium SNR regions. However, the former is slightly worse than the latter in the high SNR region. In all SNR regions, the proposed two methods exceed three fixed PA strategies in terms of SR. This confirms that optimal PA can improve the SR performance.

**Fig. 3 plots the cumulative distribution function (CDF) of SR for different PA strategies with SNR=10dB.** It can be seen that the CDF curves of the proposed Max-P-SINR-ANSNR and GD are up to the right of those of three fixed PAs. This means that they perform better than three fixed PA strategies. Therefore, the proposed two PA methods have substantial SR performance gains over fixed PAs.

**Fig. 4 illustrates the curves of the bit error rate (BER) versus SNR of the proposed Max-P-SINR-ANSNR and GD for Bob and Eve.** It can be seen that Eve has a high BER more than 25% with the help of AN and PA. The BER performances
of the proposed Max-P-SINR-ANSNR and GD at Bob are in between those of ES and three fixed PA schemes. In summary, the proposed Max-P-SINR-ANSNR and GD can strike good balances between SR and BER.

V. CONCLUSION

In this paper, we have made an investigation on PA strategies for the secure SM systems. Here, we proposed two PA strategies: GD and Max-P-SINR-ANSNR. The former is iterative and the latter is closed-form. In other words, the latter is of low-complexity. Simulation results showed that the proposed GD and Max-P-SINR-ANSNR methods nearly achieve the optimal SR performance achieved by ES. The former is better than the latter in the high SNR region, and worse than the latter in the low to medium regions in terms of SR performance.

REFERENCES