

Precoding Strategy Based on SLR for Secure Communication in MUME Wiretap Systems

Kun Xie and Wen Chen,

Department of Electronic Engineering, Shanghai Jiao Tong University, China 200240

Email: {xiekunuestc;wenchen}@sjtu.edu.cn

Abstract—Secure communication in the Multi-user and Multi-eavesdropper (MUME) scenario is considered in this paper. It has been shown that secrecy can be improved when the transmitter simultaneously transmits information signal to the legitimate receivers and artificial noise to confuse the eavesdroppers. Several processing schemes have been proposed to limit the co-channel interference (CCI). The conventional method and the ZF beamforming method are simple but of little ideal performance. While the block diagonalization (BD) method is of ideal performance but too complex. In this paper, we propose a new alternative approach based on maximizing the signal-to-leakage ratio (SLR). Simulations demonstrate that the proposed SLR method can achieve compromise between the secrecy performance and complexity.

Index Terms—MUME, artificial noise, block diagonalization, ZF beam-forming, SLR, secrecy capacity

I. INTRODUCTION

Because of the broadcast nature of the wireless communications, security is a fundamental problem in wireless communications. A passive eavesdropper in an unknown location wiretapping the information of the transmitted signal is supposed without risk of being detected. Traditionally, secure communications are achieved by using cryptographic technologies such as encryption. On the other hand, studies from an information-theoretic viewpoint have found conditions for reliable secure communication without using secret keys. In the early works on information theoretic security, Wyner introduced the wiretap channel model in which the eavesdropper's channel is defined to be a degraded version of the legitimate receiver's channel [1]. It has shown that a non-zero secrecy capacity can be obtained only if the eavesdropper's channel is of lower quality than that of the legitimate receivers. Csiszar and Korner extended this problem to a general nondegraded channel condition in which a common message is transmitted to both receivers and a confidential message to only one of them [2]. In order to achieve secure communication, even when the receiver's channel is worse than the eavesdropper's channel, various physical-layer techniques were proposed. One of the most common techniques is the use of artificial noise to confuse the eavesdropper.

When multiple antennas are equipped at the transmitter, it is possible to simultaneously transmit both the information-bearing signal and artificial noise to achieve secrecy in a fading environment [3]–[7]. The artificial noise is radiated randomly to mask the transmission of the information signal to the legitimate receiver. In the design of secure communication

based on multi-antenna technique with artificial noise, the transmit power allocation between the information signal and the artificial noise is an important issue, which has not been investigated in [3], [4], [5]. A suboptimal power allocation strategy was considered in [6], which aims to meet an ideal signal-to-interference-and-noise ratio (SINR) at the intended receiver to satisfy a quality of service requirement. The secure communication with artificial noise was also discussed in [7], in which the closed-form expression and the optimal power allocation was obtained.

All the previous papers focus on the single-user system. However, most practical communication systems have more than one user. In addition, the eavesdroppers may not appear alone, which means that they may choose to cooperate or not. This is the so-called Multi-user and Multi-eavesdropper (MUME) system, which was seldom investigated before. The secrecy capacity of MUME system is different to that of single-user system, which must make sure any legitimate user will not be wiretapped. The authors in [8], [9] put forward the MUME model and give us the rough definition of the secrecy capacity of MUME. The authors in [9] discussed the realization of the secrecy capacity of multiple users and multiple eavesdroppers with artificial noise separately. However, the transmission power allocation between the information signal and the artificial noise has not been investigated. The authors [10] discussed two ZF beamforming strategies for secrecy in multiuser MIMO wiretap channels, in which SNR and BER at receivers and eavesdroppers are analyzed. However only single data stream transmission case was considered.

In order to limit the co-channel interference (CCI) from other users and mask the information-bearing signal simultaneously, there are two practical linear transmission techniques: (i) the conventional method discussed in [3], [5], which conducts a singular value decomposition (SVD) on each user's channel matrix to get a maximum channel gain for their own message; (ii) the ZF beamforming method [10] and its promotion—the block diagonalization (BD) method [11], [12], in which all the information is transmitted in the null space of all other receivers' channels. The conventional method and ZF beamforming method are simple, but of little ideal performance. While the BD method is of ideal performance but too complex.

In view of the strong and weak points of the previous schemes, we propose an alternative approach, which is based on the signal-to-leakage-ratio (SLR) [13]. When single data stream transmission is required, it offers compromise between

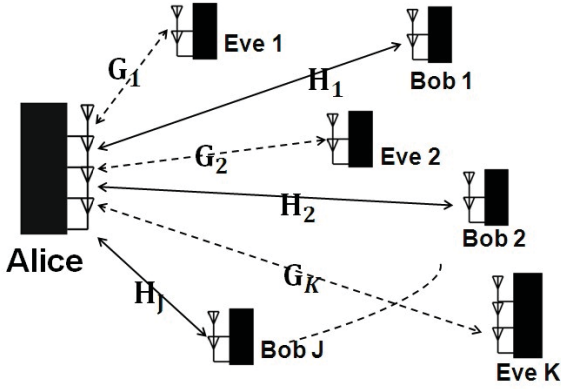


Fig. 1: The MUME-MIMO wiretap system model.

the secrecy capacity and complexity. Moreover, we analyze the optimal power allocation in MUME scenario: not only the power ratio between the information signal and the artificial noise but also that between the signals for different legitimate users. The maximum secrecy capacity can be obtained when the power is allocated according to these optimal power ratios.

In this paper, $E(\bullet)$ denotes expectation, $(\bullet)^H$ denotes the Hermitian transpose, and \mathbf{I} is an identity matrix. $E(\cdot)$ denotes the expectation of a random or vector, $I(\cdot, \cdot)$ denotes mutual information, and $\|\cdot\|$ denotes the square norm of a vector. $[x]^+ = \max\{0, x\}$. $\text{tr}(\cdot)$ is the trace of a matrix and $(\cdot)^H$ is Hermitian transpose of a matrix.

II. SYSTEM MODEL

In this paper, we consider the MUME wiretap model as shown in Fig. 1, in which there is one transmitter named Alice, J legitimate users (Bobs) and K eavesdroppers (Eves). All of the terminals may be equipped with multiple antennas. N_{Bj} antennas are equipped at the j th Bob, N_{Ek} antennas at the k th Eve, and N_A antennas at Alice. Perfect channel state information (CSI) of Bob is assumed at Alice but the CSI of Eve is unavailable at Alice for their passive feature.

Let the transmit signal $\mathbf{X} = \sum_{j=1}^J \mathbf{U}_j + \mathbf{V}$, where \mathbf{U}_j is the information bearing signal vector for Bob j , and \mathbf{V} is the artificial noise signal vector to interference Eves. Let \mathbf{H}_j be the full-rank $N_{Bj} \times N_A$ channel matrix between Alice and the Bob j , and \mathbf{G}_k be the full-rank $N_{Ek} \times N_A$ channel matrix between Alice and the Eve k . Assume that the channel matrix \mathbf{H}_j and \mathbf{G}_k are block-fading, whose entries are complex Gaussian variables with zero-mean and unit-variance. Then the received signals at Bobs and Eves are respectively,

$$\begin{aligned} \text{Bob } j: \quad \mathbf{Y}_j &= \mathbf{H}_j \mathbf{X} + \mathbf{N}_j^B, \quad \text{for } j = 1, \dots, J, \\ \text{Eve } k: \quad \mathbf{Z}_k &= \mathbf{G}_k \mathbf{X} + \mathbf{N}_k^E, \quad \text{for } k = 1, \dots, K, \end{aligned} \quad (1)$$

where \mathbf{N}_j^B , and \mathbf{N}_k^E are respectively the additive white Gaussian noise vectors at Bob j and Eve k , which covariance $E[\mathbf{N}_j^B \mathbf{N}_j^{B^H}] = \sigma_{Bj}^2 \mathbf{I}$, and $E[\mathbf{N}_k^E \mathbf{N}_k^{E^H}] = \sigma_{Ek}^2 \mathbf{I}$. We also assume that the channel matrices \mathbf{H}_j , $j = 1, 2, \dots, J$, are

available only at Alice, e.g., either through reverse channel estimation in time-division-duplex (TDD) or feedback in frequency-division-duplex (FDD), while the channel \mathbf{G}_k , $k = 1, 2, \dots, K$, are assumed unavailable at Alice due to the passive nature of eavesdroppers.

Our objective is to transmit different secret message to the corresponding Bobs. We try to reduce the interference from the others, and make sure that Eves can not wiretap any communication between Alice and Bobs. Let C_j^B denote the capacity between Alice and Bob j , and C_k^E denote the capacity between Alice and Eve k . Then

$$\begin{aligned} C_j^B &= \max[I(X; Y_j)], \quad \text{for } j = 1, \dots, J, \\ C_k^E &= \max[I(X; Z_k)], \quad \text{for } k = 1, \dots, K. \end{aligned} \quad (2)$$

In the sequel, the secrecy capacity of the pair (j, k) for Bob j and Eve k can be denoted by [14]

$$C_{jk} = [C_j^B - C_k^E]^+. \quad (3)$$

The secure capacity of MUME Wire-tap system is determined neither by the best transmission pair nor the total capacity gap between Bobs and Eves, but by the poorest performance transmission pair. Then the secrecy of MUME wire-tap channel is given by $C_s = \min_{j,k} \{C_{jk}\}$.

III. PRECODER IN MUME-MIMO NETWORK BASED ON SLR

At Alice, the data is processed before transmission, which refers to as transmission preprocessing, and then is launched into the MIMO channel. Let \mathbf{W}_j be an $N_{Bj} \times d_j$ linear precoder, \mathbf{u}_j be a $d_j \times 1$ arbitrary data symbol vector for user j , and d_j be the number of parallel data symbols transmitted simultaneously for Bob j [16]. Let \mathbf{V} be the artificial noise signal vector to jam Eves, \mathbf{W} be the transmission preprocessing matrix, and \mathbf{v} be the arbitrary data symbol vector for the artificial noise. Then the transmission signal is

$$\mathbf{X} = \sum_{\ell=1}^J \mathbf{U}_\ell + \mathbf{V} = \sum_{\ell=1}^J \mathbf{W}_\ell \mathbf{u}_\ell + \mathbf{W} \mathbf{v}. \quad (4)$$

Then the received signal at Bobs and Eves are respectively

$$\begin{aligned} \mathbf{Y}_j &= \mathbf{H}_j \sum_{\ell=1}^J \mathbf{W}_\ell \mathbf{u}_\ell + \mathbf{H}_j \mathbf{W} \mathbf{v} + \mathbf{N}_j^B, \quad j = 1, \dots, J, \\ \mathbf{Z}_k &= \mathbf{G}_k \sum_{\ell=1}^J \mathbf{W}_\ell \mathbf{u}_\ell + \mathbf{G}_k \mathbf{W} \mathbf{v} + \mathbf{N}_k^E, \quad k = 1, \dots, K. \end{aligned} \quad (5)$$

The emphasis of this paper is to design the precoders \mathbf{W} and \mathbf{W}_ℓ for $\ell = 1, 2, \dots, J$. Here, we propose a new approach, which is based on maximizing the signal-to-leakage ratio (SLR). It uses the SLR as the measure instead of SINR when designing the precoders to avoid the optimization problem with multiple unknown variables and can therefore reduce the computational complexity. In this paper, a single data stream is sent to Bob when $d_j = 1$, $\forall j$, and multiple data streams are sent when $d_j > 1$, $\forall j$. Only a maximum of N_{Bj} streams can be transmitted simultaneously for user j , else the message

will not be decoded, which however is seldom studied in the MUME model. Criterion of judging the design is whether the secrecy capacity is sufficiently good under the given power constraints, which will be discussed in detail with the design of transmission processing matrix in the following part.

A. Design of Precoder Based on SLR in MUME system

In MUME scenarios, several co-channel Bobs with multiple antennas aiming to communicate with Alice in the same frequency or time slots. In this case, it is necessary to design transmission scheme able to suppress the CCI at Bobs. Before our discussion, we first introduce the concept signal-to-leakage ratio (SLR), which was first proposed in [13]. The SLR is the ratio of the average received power S of the message for the targeted user over the average leaked power L of the corresponding message to other co-channel users, i.e., the useful signal detected by other users. The SLR denotes the efficiency of power utilization, which can be given by $SLR = S/R$. Based on the transmission method introduced in [5], we first select the J nonzero precoding matrices, $\mathbf{W}_1, \mathbf{W}_2, \dots, \mathbf{W}_J$, for the J users, and then form an $N_A \times N_A$ matrix $\mathbf{W} = [\mathbf{W}_1 \mathbf{W}_2 \dots \mathbf{W}_J \mathbf{W}]$.

Conventionally the receiver estimates its message \mathbf{u}_j from the received signal \mathbf{Y}_j according to a classical single-user maximum-likelihood detection scheme. Then the capacity for user j can be characterized by the output SINR. Using this SINR expression for $j = 1, 2, \dots, J$, as an optimization criterion to determine $\{\mathbf{W}_j, j = 1, 2, \dots, J\}$ results in a complex optimization problem with J variables [17].

Let us reconsider (5) again. The power of the desired message \mathbf{u}_j received at Bob j is $\|\mathbf{H}_j \mathbf{W}_j \mathbf{u}_j\|^2$. At the same time, the power of the interference caused by the user j ($j \neq i$) received at the user i is given by $\|\mathbf{H}_i \mathbf{W}_j \mathbf{u}_j\|^2$. We define it as the leakage from the user j to the user i . Then the total power leaked from the user j to all other $J - 1$ users can be written as $\sum_{i=1, i \neq j}^J \|\mathbf{H}_i \mathbf{W}_j \mathbf{u}_j\|^2$. Then we can obtain the SLR for user j as

$$SLR_j = \frac{E\|\mathbf{H}_j \mathbf{W}_j \mathbf{u}_j\|^2}{\sum_{i=1, i \neq j}^J E\|\mathbf{H}_i \mathbf{W}_j \mathbf{u}_j\|^2} = \frac{P_j \text{tr}(\mathbf{W}_j^H \mathbf{H}_j^H \mathbf{H}_j \mathbf{W}_j)}{\sum_{i=1, i \neq j}^J \text{tr}(\mathbf{W}_j^H \mathbf{H}_i^H \mathbf{H}_i \mathbf{W}_j)}, \quad (6)$$

where P_j is the power allocated to signal \mathbf{u}_j . Therefore we need to solve a distributed optimization problem as follows.

Problem Statement: Given a fixed transmit power for each user's message, we need to design the precoders $\mathbf{W}_j, j = 1, 2, \dots, J$, such that the SLR is maximized for every user:

$$\mathbf{W}_j = \arg \max SLR_j = \arg \max \frac{\text{tr}(\mathbf{W}_j^H \mathbf{H}_j^H \mathbf{H}_j \mathbf{W}_j)}{\text{tr}(\mathbf{W}_j^H \tilde{\mathbf{H}}_j^H \tilde{\mathbf{H}}_j \mathbf{W}_j)}, \quad (7)$$

Subject to $\text{tr}(\mathbf{W}_j^H \mathbf{W}_j) = 1, j = 1, 2, \dots, J$,

where $\tilde{\mathbf{H}}_j = [\mathbf{H}_1^T, \mathbf{H}_2^T, \dots, \mathbf{H}_{(j-1)}^T, \mathbf{H}_{(j+1)}^T, \dots, \mathbf{H}_J^T]^T$.

To solve (7), we refer to the Rayleigh-Ritz quotient result [18],

$$\frac{\text{tr}(\mathbf{W}_j^H \mathbf{H}_j^H \mathbf{H}_j \mathbf{W}_j)}{\text{tr}(\mathbf{W}_j^H \tilde{\mathbf{H}}_j^H \tilde{\mathbf{H}}_j \mathbf{W}_j)} \leq \lambda_{\max}(\mathbf{H}_j^H \mathbf{H}_j, \tilde{\mathbf{H}}_j^H \tilde{\mathbf{H}}_j), \quad (8)$$

where λ_{\max} is the largest generalized eigenvalue¹ of the matrix pair $\mathbf{H}_j^H \mathbf{H}_j$ and $\tilde{\mathbf{H}}_j^H \tilde{\mathbf{H}}_j$. Equality occurs if \mathbf{W}_j is proportional to a generalized eigenvector corresponding to the largest generalized eigenvalue, written compactly as

$$\mathbf{W}_j \propto \max \text{gen-eigenvector} (\mathbf{H}_j^H \mathbf{H}_j, \tilde{\mathbf{H}}_j^H \tilde{\mathbf{H}}_j). \quad (9)$$

Compare this solution to the conventional beamforming solution [3],[5]

$$\mathbf{W}_j \propto \max \text{eigenvector} (\mathbf{H}_j^H \mathbf{H}_j). \quad (10)$$

In the conventional method, we can see that (10) only uses the channel information of user j , while (9) in the SLR method is obtained based on all users' channel information. Therefore the SLR method can be expected to obtain better performance compared to the conventional one. It is worthy of noting that the equations (9) is just for the single data streams cases ($d_j = 1$). When ($d_j \neq 1$), formula (9) will be rewritten as

$$\mathbf{W}_j \propto \max d_j \text{ gen-eigenvectors} (\mathbf{H}_j^H \mathbf{H}_j, \tilde{\mathbf{H}}_j^H \tilde{\mathbf{H}}_j), \quad (11)$$

and the power will be allocated among the d_j generalized eigenvectors corresponding to the largest d_j generalized eigenvalues of matrix pair $(\mathbf{H}_j^H \mathbf{H}_j, \tilde{\mathbf{H}}_j^H \tilde{\mathbf{H}}_j)$. However, whether the increase of parallel data streams will gives us more room for improvement is still an open problem and subject to further study.

Since the CSI of all receivers (except for the eavesdroppers) is available at the transmitter, in order to guarantee that it does not impact the desired receivers, the artificial noise is often mapped into the subspace orthogonal to the effective downlink co-channel matrix $\tilde{\mathbf{H}}$ [3],[5], where

$$\tilde{\mathbf{H}} = [\mathbf{H}_1^T, \mathbf{H}_2^T, \dots, \mathbf{H}_J^T]^T. \quad (12)$$

Then we can get $\mathbf{W} = \ker(\tilde{\mathbf{H}})$, i.e., the kernel of $\tilde{\mathbf{H}}$. Note that the precoding matrix \mathbf{W} should also be a nonzero matrix. To guarantee the existence of a nonzero power of artificial noise, a sufficient condition is that the number of the transmit antennas is larger than the rank of matrix $\tilde{\mathbf{H}}$. Because the practical channel matrix is usually assumed to be full-rank, N_A must satisfies $N_A > \sum_{i=1}^J N_{Bj}$.

B. The Secrecy Capacity of SLR Method for MUME-MIMO Systems

The $N_A \times 1$ transmitted symbol vector at Alice is given by (5) as

$$\mathbf{X} = \sum_{j=1}^J \mathbf{U}_j + \mathbf{V} = \sum_{j=1}^J \mathbf{W}_j \mathbf{u}_j + \mathbf{W} \mathbf{v},$$

¹If there is a scalar λ and a non-zero vector \mathbf{u} such that $\mathbf{A}\mathbf{u} = \lambda\mathbf{B}\mathbf{u}$, then λ is called a generalized eigenvalue of the matrix pair \mathbf{A} and \mathbf{B} , and \mathbf{u} is called a generalized eigenvector corresponding to the eigenvalue λ .

where \mathbf{u}_j is a $d_j \times 1$ data vector, whose variance is $\sigma_{u_j}^2$, and the complex Gaussian random elements of \mathbf{v} are i.i.d whose variance is σ_v^2 .

Assume that Alice has a total amount of transmit power budget P . Due to the normalization of the noise variance at Bob, we can also refer to P as the transmission SNR. One important design parameter in this paper is the power ratio, denoted by ρ_j ($0 < \rho_j < 1$), allocated for the user j 's information transmission. We define the power fraction for transmitting artificial noise as α ($0 < \alpha < 1$), which leads to

$$\begin{aligned} \mathbf{Q}_j &= E(\mathbf{u}_j \mathbf{u}_j^H), \quad \text{tr}(\mathbf{Q}_j) = P_j = \rho_j P, \\ \mathbf{Q}_v &= E(\mathbf{v} \mathbf{v}^H), \quad \text{tr}(\mathbf{Q}_v) = \alpha P, \\ P &\geq \sum_{j=1}^J \rho_j P + \alpha P = \sum_{j=1}^J d_j \sigma_{u_j}^2 + (N_A - \sum_{j=1}^J N_{Bj}) \sigma_v^2, \end{aligned} \quad (13)$$

in which, we have the following relationships:

$$\begin{aligned} \alpha &= 1 - \rho = 1 - \sum_{j=1}^J \rho_j, \\ N_A &\geq \sum_{i=1}^J B_{Bj} + 1, \\ \sigma_{u_j}^2 &= \frac{P_j}{d_j} = \frac{\rho_j P}{d_j}, \\ \sigma_v^2 &= \frac{(1 - \rho)P}{N_A - \sum_{j=1}^J B_{Bj}} = \frac{(1 - \sum_{j=1}^J \rho_j)P}{N_A - \sum_{j=1}^J N_{Bj}}. \end{aligned} \quad (14)$$

In order to analyze the secrecy capacity more concisely, the equation (5) can be rewritten as:

$$\begin{aligned} \mathbf{Y}_j &= \mathbf{H}_j \sum_{i=1}^J \mathbf{W}_i \mathbf{u}_i + \mathbf{H}_j \mathbf{W} \mathbf{v} + \mathbf{N}_j^B \\ &= \mathbf{H}_j \mathbf{W}_j \mathbf{u}_j + \mathbf{H}_j \sum_{i \neq j} \mathbf{W}_i \mathbf{u}_i + \mathbf{H}_j \mathbf{W} \mathbf{v} + \mathbf{N}_j^B \\ &= \hat{\mathbf{H}}_{jj} \mathbf{u}_j + \sum_{i \neq j} \hat{\mathbf{H}}_{ji} \mathbf{u}_i + \hat{\mathbf{H}}_j \mathbf{v} + \mathbf{N}_j^B, \\ \mathbf{Z}_k &= \mathbf{G}_k \sum_{l=1}^K \mathbf{W}_l \mathbf{u}_l + \mathbf{G}_k \mathbf{W} \mathbf{v} + \mathbf{N}_k^E \\ &= \mathbf{G}_k \mathbf{W}_j \mathbf{u}_j + \mathbf{G}_k \sum_{l \neq j} \mathbf{W}_l \mathbf{u}_l + \mathbf{G}_k \mathbf{W} \mathbf{v} + \mathbf{N}_k^E \\ &= \hat{\mathbf{G}}_{kj} \mathbf{u}_j + \sum_{l \neq j} \hat{\mathbf{G}}_{kl} \mathbf{u}_l + \hat{\mathbf{G}}_k \mathbf{v} + \mathbf{N}_k^E, \end{aligned} \quad (15)$$

where we have defined

$$\hat{\mathbf{H}}_{ji} \triangleq \mathbf{H}_j \mathbf{W}_i, \quad \hat{\mathbf{H}}_j \triangleq \mathbf{H}_j \mathbf{W}, \quad (16)$$

$$\hat{\mathbf{G}}_{kl} \triangleq \mathbf{G}_k \mathbf{W}_l, \quad \hat{\mathbf{G}}_k \triangleq \mathbf{G}_k \mathbf{W}, \quad (17)$$

for $j, i, l = 1, 2, \dots, J$, $k = 1, 2, \dots, K$.

The secrecy capacity is the maximum transmission rate at which the intended receiver can decode the data with arbitrarily small error, which is bounded by the difference in the capacity between Alice and Bob and that between Alice

and Eve [2]. As in [5], we can normalize the distance of each Bob or user to make the variance of the entries of \mathbf{H}_j equal to unity without loss of generality, and the noise vector \mathbf{N}_j^B be of unit variance. Then the capacity between Alice and Bob j is

$$\begin{aligned} C_j^B &= E_{\tilde{\mathbf{H}}} \left\{ \log_2 \left| \mathbf{I} + \sigma_{u_j}^2 \hat{\mathbf{H}}_{jj} \hat{\mathbf{H}}_{jj}^H \left(\mathbf{I} + \sum_{i=1, i \neq j}^J \sigma_{u_i}^2 \hat{\mathbf{H}}_{ji} \hat{\mathbf{H}}_{ji}^H \right)^{-1} \right| \right\} \\ &= E_{\tilde{\mathbf{H}}} \left\{ \log_2 \left| \mathbf{I} + \frac{\rho_j P}{d_j} \hat{\mathbf{H}}_{jj} \hat{\mathbf{H}}_{jj}^H \left(\mathbf{I} + \sum_{i=1, i \neq j}^J \frac{\rho_i P}{d_i} \hat{\mathbf{H}}_{ji} \hat{\mathbf{H}}_{ji}^H \right)^{-1} \right| \right\}, \end{aligned} \quad (18)$$

where we used the fact $\hat{\mathbf{H}}_j = 0$.

Next, we study the capacity between Alice and the multiple colluding or non-concluding Eves. When multiple Eves allocated at different place, the noise at each Eve may be certainly different also. In addition, the receiver noise levels at Eves may not be known by Alice or Bobs. To guarantee secure communication, it is therefore reasonable to consider the worst-case scenario where the noises at Eves are arbitrarily small. Note that this approach was also taken in [3] and [5]. In this case, the noiseless eavesdropper assumption gives a upper bound on the capacity between Alice's message for the user j and the eavesdropper k as

$$\begin{aligned} C_{kj}^E &= E_{\tilde{\mathbf{H}}, \mathbf{G}_k} \left\{ \log_2 \left| \mathbf{I} + \sigma_{u_j}^2 \hat{\mathbf{G}}_{kj} \hat{\mathbf{G}}_{kj}^H \right. \right. \\ &\quad \left. \left(\sum_{l=1, l \neq j}^J \sigma_{u_l}^2 \hat{\mathbf{G}}_{kl} \hat{\mathbf{G}}_{kl}^H + \sigma_v^2 \hat{\mathbf{G}}_k \hat{\mathbf{G}}_k^H \right)^{-1} \right| \right\} \\ &= E_{\tilde{\mathbf{H}}, \mathbf{G}_k} \left\{ \log_2 \left| \mathbf{I} + \frac{\rho_j P}{d_j} \hat{\mathbf{G}}_{kj} \hat{\mathbf{G}}_{kj}^H \right. \right. \\ &\quad \left. \left(\sum_{l=1, l \neq j}^J \frac{\rho_l P}{d_l} \hat{\mathbf{G}}_{kl} \hat{\mathbf{G}}_{kl}^H + \frac{\alpha P}{N_A - \sum_{i=1}^J N_{Bi}} \hat{\mathbf{G}}_k \hat{\mathbf{G}}_k^H \right)^{-1} \right| \right\}. \end{aligned} \quad (19)$$

After deriving the expressions of C_j^B and C_{kj}^E , a lower bound on the ergodic secrecy capacity can now be obtained as $C_{jk} = [C_j^B - C_{kj}^E]^+$, and the secrecy capacity for the whole system is determined by the minimum secrecy in $\{C_{jk}\}$, i.e., $C_s = \min_{1 \leq j \leq J, 1 \leq k \leq K} \{C_{jk}\}$. As we have discussed, for the MUME-MIMO system, the lower bound of ergodic secrecy capacity is given by

$$\begin{aligned} C_s &= \max_{j,k} \min_{j,k} \left[E_{\tilde{\mathbf{H}}, \mathbf{G}_k} \left\{ \log_2 \left| \mathbf{I} + \frac{\rho_j P}{d_j} \hat{\mathbf{H}}_{jj} \hat{\mathbf{H}}_{jj}^H \right. \right. \right. \\ &\quad \left. \left(\mathbf{I} + \sum_{i=1, i \neq j}^J \frac{\rho_i P}{d_i} \hat{\mathbf{H}}_{ji} \hat{\mathbf{H}}_{ji}^H \right)^{-1} \right| \right\} \\ &\quad - E_{\tilde{\mathbf{H}}, \mathbf{G}_k} \left\{ \log_2 \left| \mathbf{I} + \frac{\rho_j P}{d_j} \hat{\mathbf{G}}_{kj} \hat{\mathbf{G}}_{kj}^H \right. \right. \\ &\quad \left. \left(\sum_{l=1, l \neq j}^J \frac{\rho_l P}{d_l} \hat{\mathbf{G}}_{kl} \hat{\mathbf{G}}_{kl}^H + \frac{\alpha P}{N_A - \sum_{i=1}^J N_{Bi}} \hat{\mathbf{G}}_k \hat{\mathbf{G}}_k^H \right)^{-1} \right| \right\} \right]^+. \end{aligned} \quad (20)$$

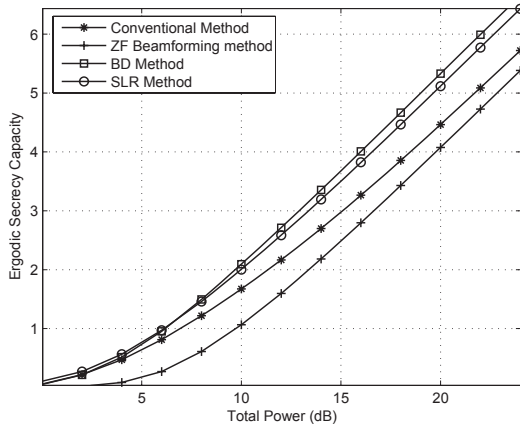


Fig. 2: The secrecy capacity for the four methods when $d_j = 1$, $N_A = 10$, $N_{Bj} = 3$, $N_{Ek} = 4$.

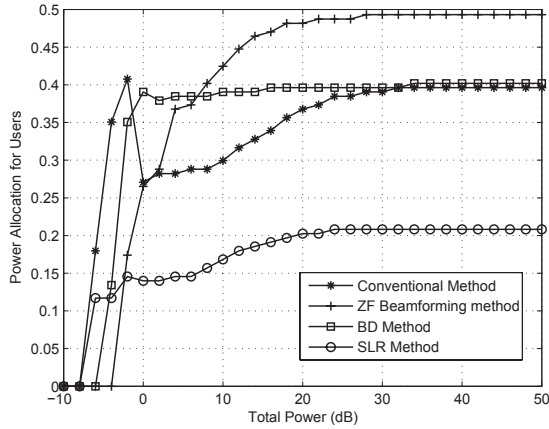


Fig. 3: The information power ratio for the four methods when $d_j = 1$, $N_A = 10$, $N_{Bj} = 3$, $N_{Ek} = 4$.

IV. SIMULATION RESULTS

In this section, we will present some simulation results to show the achieved secrecy capacity. In all simulations, the channel matrices are assumed to be composed of independent, zero-mean Gaussian random variables with unit variance. All displayed results are based on an average of 1000 independent trials. The background noise power is the same for all Bobs with a variance \mathbf{I} . To guarantee the secure communication, it is therefore reasonable to consider the worst-case scenario where the noises variance at Eves are arbitrarily small (approaching zero). The desired rate for Bobs and Eves will be measured by ergodic capacity rather than the outage capacity.

Fig. 2 and Fig. 3 exhibits the comparison of secrecy capacity and information power ratio for information signal among the 4 methods. From Fig. 2, we can see that the SLR method performs a little worse than the BD method but still much better than the conventional method and the ZF beamforming method. However the SLR method are obviously

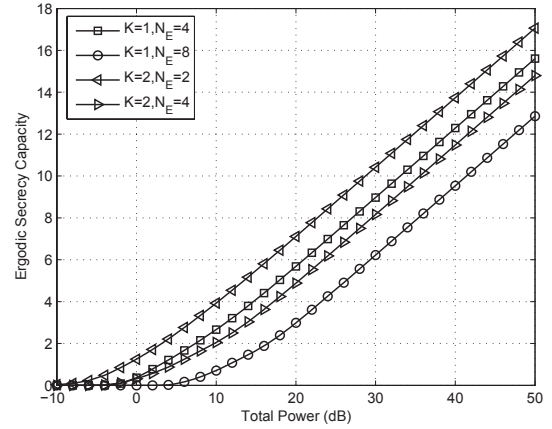


Fig. 4: The secrecy capacity of SLR for Eves' colluding ($K = 1$) and non-colluding ($K = 2$) scenarios when $N_A = 10$, $N_{Bj} = 3$.

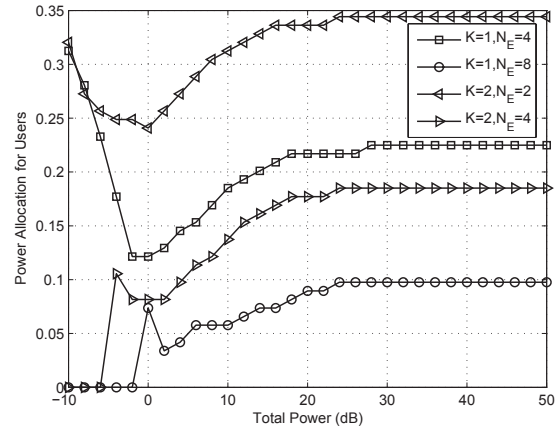


Fig. 5: The information power ratio of SLR for Eves' colluding ($K = 1$) and non-colluding ($K = 2$) scenarios when $N_A = 10$, $N_{Bj} = 3$.

of less complexity than the BD method. Therefore it offer a compromise between the secrecy capacity and complexity. Fig. 3 demonstrates that both SLR method has less power efficiency than the other three ones. However the criterion for a good scheme is the secrecy capacity obtained under the same given power constraints. Therefore the relatively low power efficiency can not be seen as a shortcoming.

Fig. 4 and Fig. 5 show the comparison of secrecy capacity and information power ratio of SLR for the Eves' colluding and non-colluding scenarios. If the Eves choose to wiretap the message jointly, we may think they are colluding, else non-colluding. As shown in Fig. 4, it will be more difficult to achieve secure communication if the Eves choose to cooperate, which is as we expected. We are interested in whether we need to allocate more power to transmit information signal or artificial noise when the Eves choose to cooperate. Fig. 5

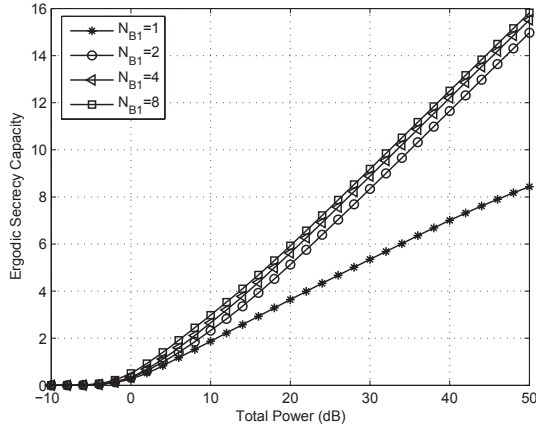


Fig. 6: The secrecy capacity for different N_{B1} of Bob1's antenna when $N_A = 10$, $N_{B2} = 2$, $N_{Ek} = 4$.

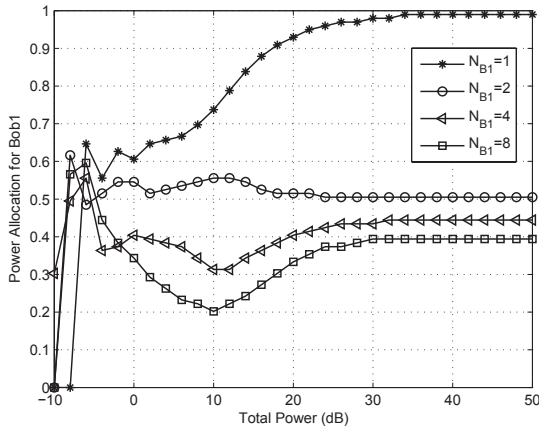


Fig. 7: The power ratio of Bob1 for different N_{B1} of Bob1's antenna when $N_A = 10$, $N_{B2} = 2$, $N_{Ek} = 4$.

shows that more power needs to be allocated to artificial noise if Eves choose to cooperate and the same as the case that there are more Eves.

Fig. 6 and Fig. 7 show the secrecy capacity and power ratio for Bob1 for different antenna number N_{B1} of Bob1, where 2 Bobs and 3 Eves are considered. We wish to study how the power is allocated between the two Bobs when their antennas are different. Fig. 6 illustrates that the secrecy capacity is mainly determined by the user with the least antennas, and the improvement is not notable when the antennas of the other Bob increase. Fig. 7 shows that the more antennas a user has, the less power need to be allocated. The power should be averagely distributed among Bobs, when the channel condition and the number of antennas are the same.

V. CONCLUSIONS

This paper proposes the precoding strategy based on the SLR method for providing secure communication at the physical layer in MUME-MIMO wiretap channels combined with

artificial noise. We also derive the secrecy capacity of the SLR method. Simulations show that the SLR offers compromise between the secrecy capacity and complexity compared to the existing methods. Besides, we find that more power should be allocated to artificial noise instead of information signal when the eavesdroppers' condition is better, and less power should be allocated to a user when it has more antennas.

ACKNOWLEDGEMENT

This work is supported by the National 973 Project #2012CB316106, by NSF China #60972031 and #61161130529, by the National 973 Project #2009CB824904.

REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
- [2] I. Csiszr and J. K?rner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, May 1978.
- [3] R. Negi and S. Goel, "Secret communications using artificial noise," in *Proc. IEEE VTC*, Dallas, TX, Sep. 2005, pp. 1906-1910.
- [4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.
- [5] X. Zhou and M. R. McKay, "Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831- 3842, Oct. 2010.
- [6] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Taipei, Taiwan, Apr. 2009, pp. 2437-2440.
- [7] X. Zhou, M. R. McKay, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Trans. Vehicular Technology*, vol. 59, no. 8, 2010.
- [8] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.
- [9] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," in *Proc. 45th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, USA, 2007.
- [10] A. Mukherjee and A. Swindlehurst, "Utility of Beamforming Strategies for Secrecy in Multiuser MIMO Wiretap Channels," in *Proc. 47th Allerton Conf. on Communication, Control and Computing*, October, 2009.
- [11] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461471, Feb. 2004.
- [12] Q. Spencer and A. Swindlehurst, "A hybrid approach to spatial multiplexing in multi-user MIMO downlinks," *EURASIP Journ. Wireless Commun. and Network*, pp. 236-247, Dec. 2004.
- [13] A. Tarighat, M. Sadek, and A. H. Sayed, "A multi user beamforming scheme for downlink MIMO channels based on maximizing signal-toleakage ratios," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 3, Philadelphia, PA, 2005, pp. 1129C 1132.
- [14] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE ISIT*, Toronto, ON, Canada, Jul. 2008, pp. 524-528.
- [15] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in *Proc. IEEE ITW*, Porto, Portugal, May 2008, pp. 164-168.
- [16] D. Gesbert, M. Kountouris, R. W. Heath Jr, C.-B. Chae, and T. Salzer, "Shifting the MIMO paradigm: From single user to multiuser communications," *IEEE Sig. Proc. Mag.*, vol. 24, pp. 36C46, Oct. 2007.
- [17] M. Schubert and H. Boche, "Solution of the multiuser downlink beamforming problem with individual SINR constraints," *IEEE Transactions on Vehicular Technology*, vol. 53, no. 1, pp. 18-28, Jan. 2004.
- [18] G. Golub and C. Van Loan, *Matrix Computations*, The Johns Hopkins University Press, third edition, 1996.