

# Interference Exploitation for Secure Communications: Error Rate and Secrecy Analysis

Abdelhamid Salem and Christos Masouros  
Department of Electronic and Electrical Engineering,  
University College London, London, UK  
emails: {a.salem, c.masouros}@ucl.ac.uk

**Abstract**—Interference exploitation has recently been shown to provide significant security benefits in multiuser communication systems. In this technique, the known interference is designed to be constructive to the legitimate users and disruptive to the malicious receivers. Accordingly, this paper analyzes the secrecy performance of constructive interference (CI) precoding technique in multi-user multiple-input single-output (MU-MISO) systems with phase-shift-keying (PSK) signals and in the presence of multiple passive eavesdroppers. The secrecy performance of CI technique is comprehensively investigated in terms of symbol error probability (SEP), and secrecy sum-rate. Firstly, new and exact analytical expressions for the average SEP of the legitimate users and the eavesdroppers are derived. Departing from classical Gaussian rate analysis, we employ finite constellation rate expressions to investigate the secrecy sum-rate. In this regard, closed-form analytical expression of the ergodic secrecy sum-rate is obtained. Then, based on the new secrecy sum-rate expression we revisit adaptive modulation (AM) scheme with the aim to enhance the secrecy performance. The numerical results in this work demonstrate that, the interference exploitation technique achieves a significant performance gain over the interference suppression schemes. Furthermore, the proposed AM scheme provides significant improvement in terms of the secrecy sum-rate.

**Index Terms**—Physical layer security, constructive interference, MU-MISO.

## I. INTRODUCTION

Multi-user multiple-input single-output (MU-MISO) communication systems play important roles in achieving high spectral efficiency, reliability, and energy efficiency [1]. In MU-MISO systems, it is necessary to perform pre-processing at the base station (BS) to reduce the interferences and achieve the high spectral efficiency promised by implementing multiple-antennas at the BS. Among various techniques, constructive interference (CI) exploitation precoding scheme has received significant research interest in the past few years. The CI precoding exploits the well-known interferences to improve the performance of MU-MISO communication systems [2], [3]. The interference is considered to be constructive if it moves the received symbol deeper in the constructive region of the desired symbol. Therefore, with the knowledge of the channel state information (CSI) and the users' signals at the network access points, the precoder can be designed to make all the inherent multi-user interferences constructive to the

received symbols. The CI exploitation technique has been extensively investigated over the past few years. This line of research was presented in [2], where the CI exploitation has been proposed for down-link multiple input multiple-output (MIMO) systems. The results in [2] showed that the CI precoding can enhance the signal to interference-plus-noise ratio (SINR) significantly, and thus improve the system performance. The authors in [3] presented transmit beamforming techniques for MU-MISO systems by exploiting the well-known interference. Furthermore, closed-form formula for the CI precoding has been derived in [4]. Based on this precoding expression, the performance analysis of the CI precoding in MU-MISO systems has been investigated in [5]–[9]. Very recently, the concept of CI has been proposed to provide secure communication in MU-MISO systems. In [10] the interference exploitation scheme has been used to design different artificial noise (AN) precoders. In [11], secure precoder for wireless information and power transfer has been proposed based on the concept of CI exploitation techniques.

Accordingly, this paper analyzes the secrecy performance of CI precoding scheme in MU-MISO systems under PSK signals and in the presence of multiple passive eavesdroppers. Particularly, the inherent multi-user interference is exploited to secure the down-link transmission in MU-MISO systems. The secrecy performance of interference exploitation technique is analyzed in terms of symbol error probability (SEP), and secrecy sum-rate. The challenge here is that, as CI is modulation dependent, traditional approaches based on the assumption of Gaussian signaling do not apply. Thus, we employ finite constellation analysis in this work. In this context, new and explicit analytical expressions have been derived for SEP, and ergodic secrecy sum-rate. In addition, from the secrecy sum-rate analysis in this paper, it has been shown that the secrecy rate of the communication systems with finite alphabet signals tends to zero in high SNR regime. In order to tackle this issue and improve the secrecy performance, adaptive modulation (AM) technique has been implemented and investigated. The results in this paper show that, the interference exploitation technique yields superior performance over the conventional interference suppression techniques in terms of SEP and secrecy sum-rate.

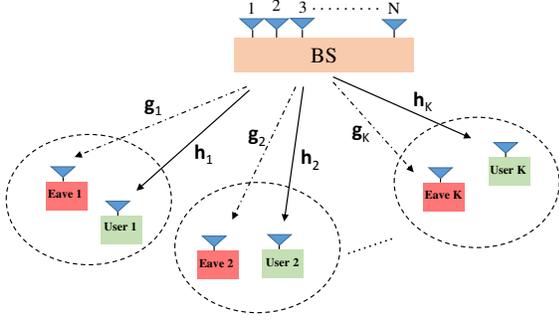


Figure 1: MU-MISO down-link with  $N$  antennas BS, single-antenna user-eavesdropper pairs.

## II. SYSTEM MODEL

Consider a wireless MU-MISO system with a BS and  $K$  user-eavesdropper pairs as illustrated in Fig. 1. The BS is equipped with  $N$  antennas, while each user and eavesdropper equipped with single antenna. The BS transmits  $K$  confidential messages to the users, and each eavesdropper tries to wiretap the user in the same pair, as in [12]. This scenario can occur in many practical applications, such as in the applications where the user-pairing technique is implemented and the BS transmits confidential messages to only one user in each pair. The down-link  $K \times N$  channel matrix from the BS to the legitimate users is presented by  $\mathbf{H}$ , which is modeled as  $\mathbf{H} = \mathbf{D}^{1/2} \tilde{\mathbf{H}}$ , where the  $K \times N$  matrix  $\tilde{\mathbf{H}}$  models the small-scale fading coefficients from the BS to the legitimate users which are modeled as independent, circularly symmetric complex Gaussian random variables with mean zero and variance one, and  $\mathbf{D}$  is a  $K \times K$  diagonal matrix in which  $[\mathbf{D}]_{kk} = \varpi_k = d_k^{-m}$  where  $d_k$  denotes the distance from the BS to the  $k^{\text{th}}$  user and  $m$  denotes the path-loss exponent. On the other side, the  $K \times N$  channel matrix from the BS to the eavesdroppers is  $\mathbf{G}$ , which is modeled as  $\mathbf{G} = \mathcal{D}^{1/2} \tilde{\mathbf{G}}$  where the  $K \times N$  matrix  $\tilde{\mathbf{G}}$  models the small-scale fading coefficients from the BS to the eavesdroppers which are also modeled as independent, circularly symmetric complex Gaussian random variables with mean zero and variance one and  $\mathcal{D}$  is a  $K \times K$  diagonal matrix where  $[\mathcal{D}]_{kk} = \omega_k = \vartheta_k^{-m}$ ,  $\vartheta_k$  is the distance from the BS to the  $k^{\text{th}}$  eavesdropper. It is assumed that the BS knows the legitimate CSI, but it knows only the statistics of the eavesdroppers' channels. The received signals at the  $k^{\text{th}}$  user and the  $k^{\text{th}}$  eavesdropper in the considered system can be written, respectively, as

$$y_{d,k} = \sqrt{P} \mathbf{h}_{d,k} \mathbf{W} \mathbf{s} + n_{d,k} \quad (1)$$

$$y_{e,k} = \sqrt{P} \mathbf{g}_k \mathbf{W} \mathbf{s} + n_{e,k} \quad (2)$$

where  $\mathbf{s} = [s_1, s_2, \dots, s_K]^H$  is the PSK-modulated signal vector,  $\mathbf{W}$  denotes the precoding matrix,  $P$  is the BS

transmission power,  $\mathbf{h}_k$  is the channel from the BS to user  $k$ ,  $\mathbf{g}_k$  is the channel from the BS to eavesdropper  $k$ ,  $n_{d,k}$  and  $n_{e,k}$  are the additive white Gaussian noises (AWGNs) at the  $k^{\text{th}}$  legitimate user,  $n_{d,k} \sim \mathcal{CN}(0, \sigma_{d,k}^2)$ , and the  $k^{\text{th}}$  eavesdropper,  $n_{e,k} \sim \mathcal{CN}(0, \sigma_{e,k}^2)$ , respectively. The CI precoding matrix with PSK signaling can be expressed as [4]

$$\mathbf{W} = \frac{1}{K} \beta \mathbf{H}^H (\mathbf{H} \mathbf{H}^H)^{-1} \text{diag} \{ \mathbf{V}^{-1} \mathbf{u} \} \mathbf{s} \mathbf{s}^H, \quad (3)$$

where  $\beta = \frac{1}{\sqrt{\mathbf{u}^H \mathbf{V}^{-1} \mathbf{u}}}$  is the power scaling factor,  $\mathbf{V} = \text{diag} (\mathbf{s}^H) (\mathbf{H} \mathbf{H}^H)^{-1} \text{diag} (\mathbf{s})$  and  $\mathbf{1}^T \mathbf{u} = 1$ .

## III. ANALYSIS OF SYMBOL ERROR PROBABILITY

Secure transmission schemes can be achieved based on constraining the SEPs of the legitimate users and the eavesdroppers to predefined threshold values. This leads to the concept of the, security gap, which is simply the difference between the SEPs of the legitimate users and the eavesdroppers [13]. Consequently, in this section we analyze the average SEP of both the  $k^{\text{th}}$  user and the  $k^{\text{th}}$  eavesdropper as follows.

### A. SEP of The Legitimate Users

In CI precoding the resulting interference contributes to the user's signal power, thus the received SNR at the  $k^{\text{th}}$  user using CI precoding can be written as

$$\gamma_{d,k} = \frac{|\sqrt{P} \mathbf{h}_{d,k} \mathbf{W} \mathbf{s}|^2}{\sigma_{d,k}^2} \quad (4)$$

Substituting (3) into (4) we can get

$$\gamma_{d,k} = \frac{\left| \frac{\sqrt{P} \beta}{K} \mathbf{b} \Sigma \mathbf{c} \frac{\mathbf{b} \mathbf{A} \mathbf{c}}{\mathbf{b} \Sigma \mathbf{c}} s_k \right|^2}{\sigma_{d,k}^2} = \alpha_k |\Psi|^2 \quad (5)$$

where  $\mathbf{b} = \mathbf{a}_k (\text{diag} (\mathbf{s}^H))$ ,  $\mathbf{c} = (\text{diag} (\mathbf{s})) \mathbf{u}$ ,  $\mathbf{a}_k$  is a  $1 \times K$  vector the  $k^{\text{th}}$  element of this vector is one, and all the other elements are zeros,  $\alpha_k = \frac{|\frac{\sqrt{P} \beta}{K} \mathbf{b} \Sigma \mathbf{c}|^2}{\sigma_k^2}$  and  $\Psi = \frac{\mathbf{b} \mathbf{A} \mathbf{c}}{\mathbf{b} \Sigma \mathbf{c}}$ . For simplicity but without loss of generality,  $\beta$  has been designed to constrain the long-term transmit power, thus it can be expressed as  $\beta = \frac{1}{\sqrt{\mathbf{u}^H \text{diag} (\mathbf{s}^H)^{-1} N \Sigma (\text{diag} (\mathbf{s}))^{-1} \mathbf{u}}}$ , where  $\Sigma = \mathbf{D}$  [5], [14]. It was shown that, the distribution of  $\Psi$  can be approximated to Gamma distribution,  $\Psi \sim \Gamma(\nu, \theta)$  [5], [14]. Thus, the received SNR,  $\gamma_{d,k}$ , can be approximated to General Gamma distribution  $\Gamma(\rho, \varrho, \kappa)$  with  $\rho = \frac{1}{2}$ ,  $\varrho = \frac{\nu}{2}$  and  $\kappa = \theta^2$ . Therefore, the probability density function (PDF) of the received SNR,  $\gamma_{d,k}$  can be written as

$f_{\gamma_{d,k}}(\gamma) = \left( \frac{(\frac{\rho}{\kappa \varrho}) \gamma^{\rho-1} e^{-\frac{\gamma}{\kappa}}}{\Gamma(\frac{\rho}{\varrho})} \right)$  [14]. Now, the average SEP

of the  $k^{\text{th}}$  legitimate user with  $M$ -PSK can be calculated by [15, (5.67)]

$$SP_k = \frac{1}{\pi} \int_0^{\frac{\pi(M-1)}{M}} \mathcal{M}_{\gamma_{d,k}} \left( -\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\Phi} \right) d\Phi \quad (6)$$

where  $\mathcal{M}_{\gamma_{d,k}}(z)$  is the the moment-generating function (MGF) of the received SNR. Using the PDF expression, the MGF of the received SNR,  $\gamma_{d,k}$ , can be derived as

$$\mathcal{M}_{\gamma_k}(z) = \int_0^{\infty} e^{-z\gamma} \left( \frac{\left(\frac{\rho}{\kappa^\rho}\right) \gamma^{\rho-1} e^{-\left(\frac{\gamma}{\kappa}\right)^\rho}}{\Gamma\left(\frac{\rho}{\rho}\right)} \right) d\gamma \quad (7)$$

The MGF can be written using Gaussian Quadrature rules as,

$$\mathcal{M}_{\gamma_k}(z) = \sum_{i=1}^n \frac{H_i}{z\alpha_k} \left( \frac{\left(\frac{\rho}{\kappa^\rho}\right) \left(\frac{\gamma_i}{zP\zeta_k}\right)^{\rho-1} e^{-\left(\frac{\gamma_i}{\kappa z P \zeta_k}\right)^\rho}}{\Gamma\left(\frac{\rho}{\rho}\right)} \right) \quad (8)$$

where  $\gamma_i$  and  $H_i$  are the  $i^{\text{th}}$  zero and the weighting factor of the Laguerre polynomials, respectively [16]. Substituting (8) into (6), we can get

$$SP_k = \frac{1}{\pi} \sum_{i=1}^n \int_0^{\frac{\pi(M-1)}{M}} \frac{H_i \left(\frac{\rho}{\kappa^\rho}\right) \left(\frac{\gamma_i}{zP\zeta_k}\right)^{\rho-1} e^{-\left(\frac{\gamma_i}{\kappa z P \zeta_k}\right)^\rho}}{z\alpha_k \Gamma\left(\frac{\rho}{\rho}\right)} d\Phi \quad (9)$$

where  $z = \frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\Phi}$ .

### B. SEP of The Eavesdroppers

Here exact and approximate expressions for the average SEP of the  $k^{\text{th}}$  eavesdropper are derived. After substituting (3) into (2) and collecting terms, the SINR at the  $k^{\text{th}}$  eavesdropper can be expressed as

$$\gamma_{e,k} = \frac{\left| \frac{\sqrt{P}\beta}{K} \mathbf{g}_k [\mathbf{H}^H]_k u_k \right|^2}{\sum_{r=1, r \neq k}^K \left| \frac{\sqrt{P}\beta}{K} \mathbf{g}_k [\mathbf{H}^H]_r u_r \right|^2 + \sigma_{e,k}^2} \quad (10)$$

The SINR expression in (10) can also be written as

$$\gamma_{e,k} = \frac{\frac{|\mathbf{g}_k [\mathbf{H}^H]_k u_k|^2}{\|\mathbf{g}_k\|^2}}{\sum_{r=1, r \neq k}^K \frac{|\mathbf{g}_k [\mathbf{H}^H]_r u_r|^2}{\|\mathbf{g}_k\|^2} + \frac{\delta_k}{\|\mathbf{g}_k\|^2}} \quad (11)$$

where  $\delta_k = \frac{K^2 \sigma_{e,k}^2}{P\beta^2}$ . It was shown that,  $\frac{|\mathbf{g}_k [\mathbf{H}^H]_r u_r|^2}{\|\mathbf{g}_k\|^2}$  and  $\frac{|\mathbf{g}_k [\mathbf{H}^H]_k u_k|^2}{\|\mathbf{g}_k\|^2}$  are independent and have exponential distributions, while  $\frac{\delta_k}{\|\mathbf{g}_k\|^2}$  has inverse Gamma distribution. Therefore, the CDF of  $\gamma_{e,k}$  can be obtained as

$$F_{\gamma_{e,k}}(\bar{\gamma}) = \Pr\left(\frac{X}{Y+Z} < \bar{\gamma}\right) \quad (12)$$

where  $X = \frac{|\mathbf{g}_k [\mathbf{H}^H]_k u_k|^2}{\|\mathbf{g}_k\|^2}$ ,  $Y = \sum_{r=1, r \neq k}^K \frac{|\mathbf{g}_k [\mathbf{H}^H]_r u_r|^2}{\|\mathbf{g}_k\|^2}$  and  $Z = \frac{\delta_k}{\|\mathbf{g}_k\|^2}$ . Since  $X$  has exponential distribution with parameter  $\lambda_x$ , the conditional distribution can be expressed as  $F_{\gamma_{e,k}}(\bar{\gamma}|Y, Z) = 1 - e^{-\lambda_x(\bar{\gamma}Y + \bar{\gamma}Z)}$ . In addition,  $Y$  has Gamma distribution,  $Y \sim \Gamma(\kappa_e, \tilde{\beta})$ , with shape parameter  $\kappa_e = K - 1$  and inverse scale parameter  $\tilde{\beta}$ . Thus, the CDF conditioning on  $Z$  can be found as  $F_{\gamma_{e,k}}(\bar{\gamma}|Z) = 1 - \tilde{\beta}^{\kappa_e} e^{-\tilde{\beta}\bar{\gamma}Z} \left(\tilde{\beta} + \bar{\gamma}\lambda_x\right)^{-\kappa_e}$ . Finally, since  $Z$  has inverse Gamma distribution with shape parameter  $\nu$ , the CDF of  $\gamma_{e,k}$  can be found as

$$F_{\gamma_{e,k}}(\bar{\gamma}) = 1 -$$

$$\frac{2\tilde{\beta}^{\kappa_e} \delta_j^{\frac{\nu}{2}} (\lambda_x \bar{\gamma})^{\frac{\nu}{2}} \left(\tilde{\beta} + \lambda_x \bar{\gamma}\right)^{-\kappa_e} \mathbf{J}\left[\nu, 2\sqrt{\delta_j \lambda_x \bar{\gamma}}\right]}{\Gamma(\nu)} \quad (13)$$

where  $\mathbf{J}[\cdot]$  is the Besselk function. Now, the average SEP of the  $j^{\text{th}}$  eavesdropper with  $M$ -PSK can be expressed as [15, (5.67)]

$$SP_{e,k} = \frac{1}{\pi} \int_0^{\frac{\pi(M-1)}{M}} \mathcal{M}_{\gamma_{e,k}} \left( -\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\Phi} \right) d\Phi \quad (14)$$

Using integration by parts, the MGF,  $\mathcal{M}_{\gamma_{e,k}}(z)$ , can be derived as

$$\mathcal{M}_{\gamma_{e,k}}(z) = 1 - z \int_0^{\infty} e^{-z\bar{\gamma}} (1 - F_{\gamma_{e,k}}(\bar{\gamma})) d\bar{\gamma} \quad (15)$$

which can be found as

$$\mathcal{M}_{\gamma_{e,k}}(z) = 1 - \sum_{i=1}^n \frac{2H_i \tilde{\beta}^{\kappa_e} \delta_j^{\frac{\nu}{2}} \left(\frac{\lambda_x \bar{\gamma}_i}{z}\right)^{\frac{\nu}{2}} \left(\tilde{\beta} + \frac{\lambda_x \bar{\gamma}_i}{z}\right)^{-\kappa_e} \mathbf{J}\left[\nu, 2\sqrt{\frac{\delta_j \lambda_x \bar{\gamma}_i}{z}}\right]}{\Gamma(\nu)} \quad (16)$$

where  $\bar{\gamma}_i$  and  $H_i$  are the  $i^{\text{th}}$  zero and the weighting factor of the Laguerre polynomials, respectively [16]. Substituting (16) into (14), we can obtain the exact SEP of the eavesdropper as in (17), shown at the top of next page.

## IV. ANALYSIS OF SECRECY SUM-RATE

The secrecy rate can be defined as the maximum difference between the mutual information of the legitimate user and eavesdropper channels. Accordingly, the ergodic secrecy sum-rate can be calculated by [17]

$$\bar{R}_s = \sum_{k=1}^K [\bar{R}_{d,k} - \bar{R}_{e,k}]^+ \quad (18)$$

$$SP_{e,k} = \frac{1}{\pi} \int_0^{\frac{\pi(M-1)}{M}} \left( 1 - \sum_{i=1}^n \mathbf{H}_i \frac{2\tilde{\beta}^{\kappa_e} \delta_j^{\frac{\nu}{2}} \left(\frac{\lambda_x \tilde{\gamma}_i}{z}\right)^{\frac{\nu}{2}} \left(\tilde{\beta} + \frac{\lambda_x \tilde{\gamma}_i}{z}\right)^{-\kappa_e} \mathbf{J} \left[ v, 2\sqrt{\frac{\delta_j \lambda_x \tilde{\gamma}_i}{z}} \right]}{\Gamma(v)} \right) d\Phi \quad (17)$$

where  $[l]^+ = \max(0, l)$ ,  $\bar{R}_{d_k} = \mathcal{E}(R_{d_k})$ ,  $R_{d_k}$  is the rate of the  $k^{\text{th}}$  user,  $\bar{R}_{e_k} = \mathcal{E}(R_{e_k})$ ,  $R_{e_k}$  is the rate of the  $k^{\text{th}}$  eavesdropper. Therefore, to evaluate the ergodic secrecy sum-rate we need to derive the ergodic rates at user  $k$  and eavesdropper  $k$ , which are considered in the following subsections.

#### A. Ergodic Sum-Rate of the Legitimate Users

Following the principles of CI, very accurate approximation of the ergodic rate of user  $k$  using CI precoding technique can be calculated by [5], [18],

$$\mathcal{E}\{R_{d_k}\} = \log_2 M - \frac{1}{M^N} \sum_{m=1}^{M^N} \mathcal{E}_{\mathbf{h}} \log_2 \underbrace{\sum_{i=1}^{M^N} e^{-\frac{|\sqrt{P}\mathbf{h}_{d,k}[\mathbf{W}]_k s_{m,i}|^2}{2\sigma_{d,k}^2}}}_{\psi} \quad (19)$$

where  $s_{m,i} = s_m - s_i$ ,  $s_m$  and  $s_i$  are symbols taken from the  $M$  signal constellation. Substituting (3) into (19), we can write the ergodic rate as

$$\mathcal{E}\{R_{d_k}\} = \log_2 M - \frac{1}{M^N} \sum_{m=1}^{M^N} \mathcal{E}_{\mathbf{h}} \log_2 \underbrace{\sum_{i=1}^{M^N} e^{-\frac{|\sqrt{P}\beta \mathbf{b}\mathbf{F}\mathbf{u}s_{m,i}|^2}{2\sigma_{d,k}^2}}}_{\psi} \quad (20)$$

where  $\mathbf{F} = \mathbf{V}^{-1}$  and  $\mathbf{b} = \mathbf{a}_k$ . To derive the ergodic rate, we need to obtain the average of the term  $\psi$  in (20). Invoking Jensen inequality,  $\psi$ , can be written as

$$\psi \leq \log_2 \sum_{i=1}^{M^N} \mathcal{E}_{\mathbf{h}} \left\{ e^{-\frac{|\sqrt{P}\beta \mathbf{b}\mathbf{F}\mathbf{u}s_{m,i}|^2}{2\sigma_{d,k}^2}} \right\}. \quad (21)$$

Now, the average over the channel can be derived as,  $\psi = \log_2 \sum_{i=1}^{M^N} \mathcal{E}_{\mathbf{h}} \left\{ e^{-\frac{|cY s_{m,i}|^2}{2\sigma_{d,k}^2}} \right\}$ , where  $c = \frac{\sqrt{P}\beta \mathbf{b}\mathbf{F}\mathbf{u}}{K}$  and  $Y = \frac{\mathbf{b}\mathbf{F}\mathbf{u}}{\mathbf{b}\Sigma\mathbf{u}}$ . The distribution of  $Y$  can be approximated to Gamma distribution,  $Y \sim \Gamma(\nu, \theta)$  [14]. Therefore, the average can be calculated by

$$\psi = \log_2 \sum_{i=1}^{M^N} \int_0^{\infty} e^{-\frac{|cY s_{m,i}|^2}{2\sigma_{d,k}^2}} \frac{e^{-Ky} (Ky)^{N-K} K}{(N-K)!} dy, \quad (22)$$

which can be obtained as in (23), where  ${}_1F_1$  is the Hypergeometric function.

#### B. Ergodic Rate of Eavesdropper $k$

Similarly, following the principles of CI, very accurate approximation of the average rate for the  $k^{\text{th}}$  eavesdropper with PSK signals can be written as in (24) [5], where  $\mathbf{B}$  is the matrix  $\mathbf{H}^{\mathbf{H}}$  without vector  $k$ , and  $\mathbf{s}_{m,i}$  is a vector contains all the users' signals except user  $k$  signal. By invoking Jensen inequality, the first term in (24),  $\varphi$ , can be expressed by

$$\varphi \leq \log_2 \sum_{i=1}^{M^N} \mathcal{E}_{\mathbf{g},n} \left\{ e^{-\frac{|\frac{\sqrt{P}\beta}{K} \mathbf{g}_k \mathbf{H}^{\mathbf{H}} \tilde{\mathbf{s}}_{m,i+n_{e,k}}|^2}{\sigma_{e,k}^2}} \right\} \quad (25)$$

Since  $n_{e,j}$  has Gaussian distribution, applying the integrals of exponential function in [16], the average over the noise can be obtained as

$$\mathcal{E}_n \left\{ e^{-\frac{|\frac{\sqrt{P}\beta}{K} \mathbf{g}_k \mathbf{H}^{\mathbf{H}} \tilde{\mathbf{s}}_{m,i+n_{e,k}}|^2}{\sigma_{e,k}^2}} \right\} \approx \frac{1}{2} e^{-\frac{P\beta^2 |\mathbf{g}_k \mathbf{H}^{\mathbf{H}} \tilde{\mathbf{s}}_{m,i}|^2}{2K^2 \sigma_{e,k}^2}}. \quad (26)$$

Now to derive the average over the channel  $\mathbf{g}$  we need firstly to find the distribution of  $\Omega = |\mathbf{g}_k \mathbf{H}^{\mathbf{H}} \tilde{\mathbf{s}}_{m,i}|^2$ . The CDF of  $\Omega$  can be obtained as

$$F_{\Omega}(\tilde{\gamma}) = \Pr \left( \underbrace{\frac{|\mathbf{g}_k \mathbf{H}^{\mathbf{H}} \tilde{\mathbf{s}}_{m,i}|^2}{\|\mathbf{g}_k\|^2}}_v < \frac{\tilde{\gamma}}{\|\mathbf{g}_k\|^2} \right) \quad (27)$$

It is shown that  $v$  has exponential distribution with CDF,  $F_v(v) = 1 - e^{-\frac{v}{\lambda_v}}$  where  $\lambda_v = \|\tilde{\mathbf{s}}_{m,i}\|^2$ . Let  $Z = \frac{1}{\|\mathbf{g}_k\|^2}$ , now by conditioning on  $Z$  we can find,  $\Pr(v < Z\tilde{\gamma}) = \int_0^{\infty} (1 - e^{-\frac{Z\tilde{\gamma}}{\lambda_v}}) f_Z(z) dz$ . Since  $Z$  has inverse Gamma distribution with PDF given by  $f_Z(z) = \frac{(\frac{1}{z})^{v+1} \delta^v e^{-\frac{\delta}{z}}}{\Gamma(v)}$ , where  $\delta$  is the scale parameter and  $v$  is the shape parameter which is equal to  $N$ , the CDF can be found as

$$F_{\Omega}(\tilde{\gamma}) = 1 - \frac{2\delta^{\frac{\nu}{2}} \left(\frac{\tilde{\gamma}}{\lambda_v}\right)^{\frac{\nu}{2}} \mathbf{J} \left[ v, 2\sqrt{\frac{\delta\tilde{\gamma}}{\lambda_v}} \right]}{\Gamma(v)} \quad (28)$$

Finally, the PDF can be obtained as in (29). Consequently, the average of (26) over the channel can be found as

$$\mathcal{E}_{\mathbf{g}} \left\{ e^{-\frac{P\beta^2 \Omega}{2K^2 \sigma_{e,k}^2}} \right\} = \int_0^{\infty} \left( \frac{1}{2} e^{-\frac{P\beta^2 \tilde{\gamma}}{2K^2 \sigma_{e,k}^2}} \right) f_{\Omega}(\tilde{\gamma}) d\tilde{\gamma} \quad (30)$$

$$\begin{aligned} \psi = \log_2 \sum_{i=1}^{M^N} & \left( \left( \frac{2^{\left(\frac{1}{2}(N-K-1)\right)} K^{(N-K+1)} |s_{m,i}|^{-2+K-N}}{(N-K)!} \right) \left( \left( \frac{c^2}{\sigma_{d,k}^2} \right)^{\frac{1}{2}(K-N-1)} \right) \right) \\ & \times \left( (c^2 |s_{m,i}|) \Gamma \left( \frac{1}{2} (N-K+1) \right) {}_1F_1 \left( \frac{1}{2} (N-K+1), \frac{1}{2}, \frac{K^2 \sigma_{d,k}^2}{2c^2 |s_{m,i}|^2} \right) \right. \\ & \left. - \sqrt{2} K c \sigma_{d,k}^2 \Gamma \left( \frac{1}{2} (N-K+2) \right) {}_1F_1 \left( \frac{1}{2} (N-K+2), \frac{3}{2}, \frac{K^2 \sigma_{d,k}^2}{2c^2 |s_{m,i}|^2} \right) \right). \end{aligned} \quad (23)$$

$$\mathcal{E} \{R_{e_k}\} = \log_2 M - \frac{1}{M^N} \sum_{m=1}^{M^N} \underbrace{\mathcal{E}_{g,n} \log_2 \sum_{i=1}^{M^N} e^{-\frac{|\frac{\sqrt{P}\beta}{K} \mathbf{g}_k \mathbf{H} \mathbf{H}^H \mathbf{s}_{m,i+n_{e,k}}|^2}{\sigma_{e,k}^2}}}_{\varphi} + \frac{1}{M^{N-1}} \sum_{m=1}^{M^{N-1}} \underbrace{\mathcal{E}_{g,n} \log_2 \sum_{i=1}^{M^{N-1}} e^{-\frac{|\frac{\sqrt{P}\beta}{K} \mathbf{g}_k \mathbf{B} \mathbf{s}_{m,i+n_{e,k}}|^2}{\sigma_{e,k}^2}}}_{\psi}, \quad (24)$$

$$f_{\Omega}(\tilde{\gamma}) = -\frac{\delta^{\frac{v}{2}+\frac{1}{2}} \left( \frac{\tilde{\gamma}}{\lambda_v} \right)^{\frac{v}{2}-\frac{1}{2}} \left( \mathbf{J} \left[ v-1, 2\sqrt{\frac{\delta\tilde{\gamma}}{\lambda_v}} \right] + \mathbf{J} \left[ v+1, 2\sqrt{\frac{\delta\tilde{\gamma}}{\lambda_v}} \right] \right)}{\lambda_v \Gamma(v)} - \frac{\delta^{\frac{v}{2}} \left( \frac{\tilde{\gamma}}{\lambda_v} \right)^{\frac{v}{2}-1} v \mathbf{J} \left[ v, 2\sqrt{\frac{\delta\tilde{\gamma}}{\lambda_v}} \right]}{\lambda_v \Gamma(v)} \quad (29)$$

$$\begin{aligned} \varphi = \log_2 \sum_{i=1}^{M^N} \sum_{\epsilon=0}^n \frac{H_{\epsilon}}{4\sigma_{e,k}^2} & \left( -\frac{\delta^{\frac{v}{2}+\frac{1}{2}} \left( \frac{P\beta^2 \tilde{\gamma}_{\epsilon}}{\lambda_v 2K^2 \sigma_{e,k}^2} \right)^{\frac{v}{2}-\frac{1}{2}} \left( \mathbf{J} \left[ v-1, 2\sqrt{\frac{P\beta^2 \delta \tilde{\gamma}_{\epsilon}}{2K^2 \sigma_{e,k}^2 \lambda_v}} \right] + \mathbf{J} \left[ v+1, 2\sqrt{\frac{P\beta^2 \delta \tilde{\gamma}_{\epsilon}}{2K^2 \sigma_{e,k}^2 \lambda_v}} \right] \right)}{\lambda_v \Gamma(v)} \right. \\ & \left. - \frac{\delta^{\frac{v}{2}} \left( \frac{P\beta^2 \tilde{\gamma}_{\epsilon}}{2K^2 \sigma_{e,k}^2 \lambda_v} \right)^{\frac{v}{2}-1} v \mathbf{J} \left[ v, 2\sqrt{\frac{P\beta^2 \delta \tilde{\gamma}_{\epsilon}}{2K^2 \sigma_{e,k}^2 \lambda_v}} \right]}{\lambda_v \Gamma(v)} \right) \end{aligned} \quad (31)$$

Substituting (29) into (30), the average of the first term,  $\varphi$ , can be obtained as in (31), where  $\tilde{\gamma}_{\epsilon}$  and  $H_{\epsilon}$  are the  $\epsilon^{\text{th}}$  zero and the weighting factor of the Laguerre polynomials, respectively [16]. The second term in (24),  $\psi$ , using Jensen inequality, can be written as

$$\psi \leq \log_2 \sum_{i=1}^{M^{N-1}} \mathcal{E}_{g,n} \left\{ e^{-\frac{|\frac{\sqrt{P}\beta}{K} \mathbf{g}_k \mathbf{B} \mathbf{s}_{m,i+n_{e,k}}|^2}{\sigma_{e,k}^2}} \right\} \quad (32)$$

Similarly, since  $n_{e,k}$  has Gaussian distribution, the average over the noise can be found as  $\psi = \log_2 \sum_{i=1}^{M^{N-1}} \mathcal{E}_{g} \left\{ \frac{1}{2} e^{-\frac{P\beta^2 \tilde{\Omega}}{2K^2 \sigma_{e,k}^2}} \right\}$ , where  $\tilde{\Omega} = |\mathbf{g}_k \mathbf{B} \mathbf{s}_{m,i}|^2$ . Following similar steps as in the first term, the average of the second term  $\psi$  can be obtained as in (33), where the exponential parameter  $\lambda_v = \|\mathbf{s}_{m,i}\|^2$ .

From the secrecy rate expression and the rates at the legitimate user and the eavesdropper in (19) and (24), respectively, we can notice that the secrecy rate will go to zero in high-

SNR regime [19], [20]. This is because with finite-alphabet inputs both the user's rate and the eavesdropper's rate will saturate at  $\log_2 M$  in high-SNR regime. This point will be discussed in details in Section (V). In order to tackle this issue, adaptive modulation scheme is proposed in this work.

### C. Adaptive Modulation (AM) Scheme

From the secrecy sum-rate expression and the ergodic rates at the legitimate user and the eavesdropper we can notice that, both a legitimate user's rate and an eavesdropper's rate will saturate at  $\log_2 M$  in high-SNR regime. Therefore, the secrecy rate will tend to zero in high-SNR regime [19], [20]. In addition, from the above expressions and from the results in Section V, we can also observe that for each modulation scheme there is an optimal transmit SNR value that optimizes the secrecy sum-rate. In order to tackle this issue and enhance the secrecy rate, AM scheme is proposed in this section. In AM technique, the BS selects the highest modulation order that can maximize the secrecy rate and achieve the SEP requirement. If no one of the available modulation schemes can achieve the target SEP, the BS selects the smallest modulation order. At SNRs

$$\psi = \log_2 \frac{\sum_{i=1}^{M^{N-1}} \sum_{\epsilon=0}^n \frac{H_\epsilon}{4\sigma_{e,k}^2} \left( \frac{\delta^{\frac{v}{2} + \frac{1}{2}} \left( \frac{P\beta^2 \delta \gamma_\epsilon}{\lambda_v 2K^2 \sigma_{e,k}^2} \right)^{\frac{v}{2} - \frac{1}{2}} \left( \text{J} \left[ v-1, 2\sqrt{\frac{P\beta^2 \delta \gamma_\epsilon}{2K^2 \sigma_{e,k}^2 \lambda_v}} \right] + \text{J} \left[ v+1, 2\sqrt{\frac{P\beta^2 \delta \gamma_\epsilon}{2K^2 \sigma_{e,k}^2 \lambda_v}} \right] \right)}{\lambda_v \Gamma(v)} \right.}{\left. \frac{\delta^{\frac{v}{2}} \left( \frac{P\beta^2 \delta \gamma_\epsilon}{2K^2 \sigma_{e,k}^2 \lambda_v} \right)^{\frac{v}{2} - 1} v \text{J} \left[ v, 2\sqrt{\frac{P\beta^2 \delta \gamma_\epsilon}{2K^2 \sigma_{e,k}^2 \lambda_v}} \right]}{\lambda_v \Gamma(v)} \right)} \quad (33)$$

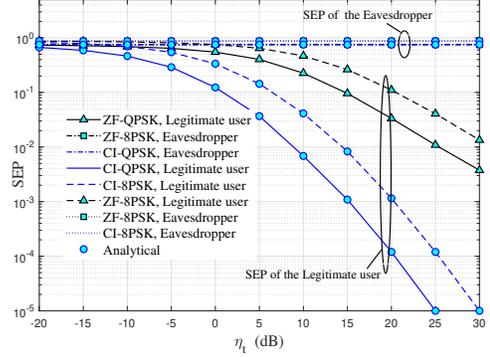
above the optimal value for a given modulation, the BS switches to the next higher modulation scheme. In practice based on the values of the secrecy rate and the target SEP requirement ( $\mathcal{P}$ ), the BS selects a modulation order from  $\mathcal{N}$  available choices  $\{M_1, M_2, \dots, M_{\mathcal{N}}\}$  according to the following rule. The modulation order is  $M = M_n = 2^n$  if  $SP_{\max} = \max_k (SP_{k, M_n}) < \mathcal{P}$ , where  $n \in [1, \mathcal{N}]$ ,  $SP_{k, M_n}$  is the SEP of user  $k$  using the modulation order  $M_n$  which can be evaluated using (9). Let  $\eta_t$  be the transmit SNR, the optimal value of the transmit SNR using  $M_n$ -PSK can be defined as,  $\beta_n = \max_{\eta_t} \bar{R}_{s, M_n}, \forall n$ , where  $\bar{R}_{s, M_n}$  is taken from (18). Therefore, the secrecy rate using AM scheme with SEP constraint,  $\bar{R}_{s, am}$ , can be calculated by,  $\bar{R}_{s, am} = \sum_{n=1}^{\mathcal{N}} a_n \bar{R}_{s, M_n}$ , where  $a_n = 1$  only if  $\bar{R}_{s, M_n} < \beta_n$ ,  $SP_{k, M_{n+1}} > SP_{th}$  and  $a_n = 0$  otherwise<sup>1</sup>.

## V. NUMERICAL RESULTS

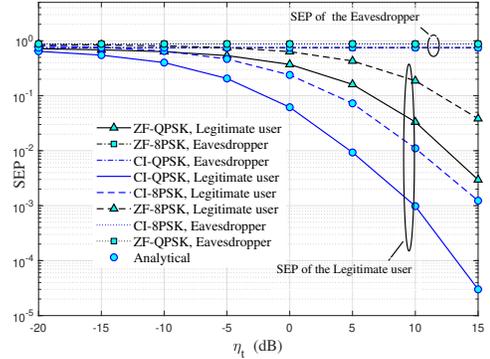
This section presents some analytical and Monte-Carlo simulation results of the mathematical expressions derived in this paper. For simplicity, equal noise variances are assumed at the users,  $\sigma^2$ , thus the transmit SNR ( $\eta_t$ ) can be defined as  $\eta_t = \frac{P}{\sigma^2}$ , and  $m = 2.7$ . For sake of comparison, some simulation results of the interference suppression, ZF, scheme are also presented in this section.

Fig. 2 shows numerical and simulation results of the SEPs versus the transmit SNR for various input types when  $N = K = 4$ , as in Fig. 2a and when  $N = 6, K = 4$  as in Fig. 2b. Firstly, it is clear that the numerical results are in well agreement with the simulation results. In addition, the CI exploitation technique has always better secrecy performance than the ZF scheme. It is apparent that, the SEP of the users reduces with increasing the transmit SNR, while the SEP of the eavesdroppers is very high and almost constant. From Figs. 2a and 2b, it can also be noted that using large number of antennas leads to increase the gap between the SEPs of the users and the eavesdroppers, and reduce the gap between the CI and ZF techniques.

Fig. 3 illustrates the ergodic secrecy sum-rate versus the transmit SNR, for various input types when  $N = K = 3$  for fixed and adaptive modulation schemes. In Fig. 3a, we present the ergodic secrecy sum-rate for CI and ZF



(a) SEP versus transmit SNR,  $\eta_t$ , with different types of input, when  $N = K = 4$ .

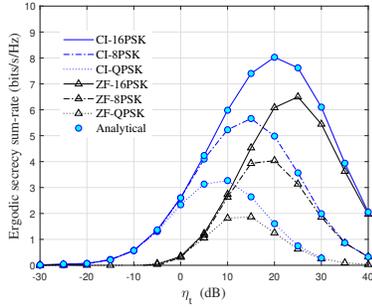


(b) SEP versus transmit SNR,  $\eta_t$ , with different types of input, when  $N = 6, K = 4$ .

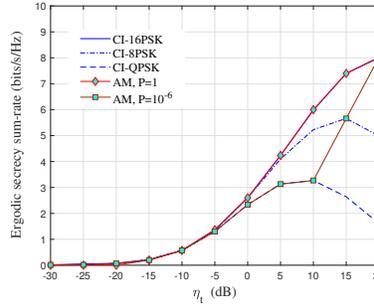
Figure 2: SEP versus transmit SNR with different types of input, and number of antennas.

with different fixed modulation schemes. From this figure it is observed that, the secrecy sum-rates achieved by CI and ZF precoding techniques are severely degraded with increasing the transmit SNR in high-SNR regime. This is because in finite alphabet systems both the user's rate and the eavesdropper's rate will saturate at,  $\log_2 M$ , in high-SNR regime. In addition, it is clear that the CI precoding achieves higher secrecy rate than ZF technique. Furthermore, in order to explain the secrecy sum-rate achieved using AM scheme, we plot the secrecy sum-rate of AM for CI versus the transmit SNR for different values of the target SEP,  $\mathcal{P}$ . Firstly, Fig. 3b, presents the secrecy sum-rate of AM scheme when the target SEP  $\mathcal{P} = 1$  and  $10^{-6}$ . In the first case when the target SEP is very high,  $\mathcal{P} = 1$ , the BS selects the highest modulation scheme, this scenario can be considered

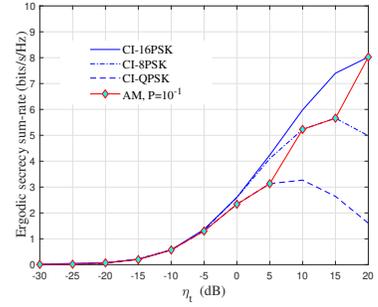
<sup>1</sup>Due to the paper length limitation, only simulation results have been presented for AM scheme.



(a) Ergodic secrecy sum-rate versus transmit SNR,  $\eta_t$ , for fixed modulation schemes.



(b) Ergodic secrecy sum-rate versus transmit SNR,  $\eta_t$ , for AM scheme, when  $\mathcal{P} = 1, 10^{-6}$ .



(c) Ergodic secrecy sum-rate versus transmit SNR,  $\eta_t$ , for AM scheme, when  $\mathcal{P} = 10^{-1}$ .

Figure 3: Ergodic secrecy sum-rate versus transmit SNR with different types of input for fixed and adaptive modulations.

as the secrecy rate of AM without SEP constraint. On the other hand, when the target SEP is very low,  $\mathcal{P} = 10^{-6}$ , in this case non of the modulation schemes can achieve the target SEP in the considered SNR range. Therefore, the BS tries to select the modulation scheme that has lower SEP when the secrecy sum-rate of this scheme is in the rising region. Finally, in Fig. 3c, we plot the secrecy sum-rate of AM when  $\mathcal{P} = 10^{-1}$ , in this case the BS always selects the higher modulation scheme that can achieve the target SEP.

## VI. CONCLUSIONS

In this paper we investigated the secrecy achievement of CI exploitation scheme in MU-MISO systems in the presence of multiple passive eavesdroppers. Firstly, new exact expressions for the SEPs of the users and the eavesdroppers were derived. Then, closed form analytical expression of the ergodic secrecy sum-rate was provided. Based on these, AM scheme was proposed to enhance the secrecy rate in finite-alphabet systems. The results explained that, the CI exploitation technique can achieve a considerable performance gain over interference suppression, ZF, technique. In addition, the security of the system can be enhanced by increasing number of BS antennas, and the proposed AM scheme offers significant secrecy performance improvement.

## REFERENCES

- [1] M. S. John G. Proakis, *Digital Communications, Fifth Edition*. McGraw-Hill, NY USA, 2008.
- [2] C. Masouros and E. Alsusa, "Dynamic linear precoding for the exploitation of known interference in mimo broadcast systems," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1396–1404, March 2009.
- [3] C. Masouros and G. Zheng, "Exploiting known interference as green signal power for downlink beamforming optimization," *IEEE Transactions on Signal Processing*, vol. 63, no. 14, pp. 3628–3640, July 2015.
- [4] A. Li and C. Masouros, "Interference exploitation precoding made practical: Optimal closed-form solutions for psk modulations," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2018.
- [5] A. Salem, C. Masouros, and K. Wong, "Sum rate and fairness analysis for the mu-mimo downlink under psk signalling: Interference suppression vs exploitation," *IEEE Transactions on Communications*, pp. 1–1, 2019.
- [6] A. Salem and C. Masouros, "On the finite constellation sum rates for zf and ci precoding," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2019, pp. 1–6.
- [7] —, "Rate splitting approach under psk signaling using constructive interference precoding technique," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2019, pp. 1–6.
- [8] A. Salem, C. Masouros, and B. Clerckx, "Rate Splitting with Finite Constellations: The Benefits of Interference Exploitation vs Suppression," *arXiv e-prints*, p. arXiv:1907.08457, Jul 2019.
- [9] A. Salem and C. Masouros, "Error Probability Analysis and Power Allocation for Interference Exploitation Over Rayleigh Fading Channels," *arXiv e-prints*, p. arXiv:1910.03102, Oct 2019.
- [10] M. R. A. Khandaker, C. Masouros, and K. Wong, "Constructive interference based secure precoding: A new dimension in physical layer security," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2256–2268, Sep. 2018.
- [11] M. R. A. Khandaker, C. Masouros, K. Wong, and S. Timotheou, "Secure swipt by exploiting constructive interference and artificial noise," *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1326–1340, Feb 2019.
- [12] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Processing Letters*, vol. 20, no. 2, pp. 141–144, Feb 2013.
- [13] S. Rezaei Aghdam, A. Nooraiepour, and T. M. Duman, "An overview of physical layer security with finite-alphabet signaling," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1829–1850, Secondquarter 2019.
- [14] R. J. Muirhead, *Aspects of Multivariate Statistical Theory*, 1982.
- [15] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels*. John Wiley and Sons, Inc., 2000.
- [16] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tabl*, Washington, D.C.: U.S. Dept. Commerce, 1972.
- [17] X. Chen and R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited csi feedback," *IEEE Wireless Communications Letters*, vol. 2, no. 5, pp. 503–506, October 2013.
- [18] Y. Wu, M. Wang, C. Xiao, Z. Ding, and X. Gao, "Linear precoding for mimo broadcast channels with finite-alphabet constraints," *IEEE Transactions on Wireless Communications*, vol. 11, no. 8, pp. 2906–2920, August 2012.
- [19] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of mimo wiretap channels driven by finite-alphabet input," *IEEE Transactions on Communications*, vol. 60, no. 12, pp. 3816–3825, December 2012.
- [20] Y. Wu, J. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Transactions on Communications*, vol. 65, no. 8, pp. 3614–3628, Aug 2017.