On the Secrecy Performance of Interference Exploitation with PSK: A non-Gaussian Signaling Analysis

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), secrecy sum-rate, and intercept probability (IP). Firstly, new and exact analytical expressions for the average SEP of the legitimate users and the eavesdroppers are derived. In addition, for simplicity and in order to provide more insights, very accurate asymptotic approximation for the average SEPs are presented in closed-form. 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. Finally, we present analytical expressions of the IP with fixed and adaptive modulations. The numerical results in this work demonstrate that, the interference exploitation technique provide additional up to 17dB gain in the transmit SNR in terms of SEP, and up to 10dB gain in the transmit SNR in terms of the secrecy sum-rate and the IP, compared to the conventional interference suppression technique. Furthermore, significant performance improvement up to 66% can be achieved with the proposed AM scheme.

Index Terms

Finite constellation signaling, physical layer security, constructive interference.

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], [2], [3]. In MU-MISO systems, it is necessary to perform pre-processing at the base station (BS) to reduce the impact of the interferences and achieve the high spectral efficiency promised by implementing multiple-antennas at the BS [4]. Among various schemes, constructive interference (CI) precoding technique has received significant research interest in the past few years. The CI precoding exploits the well-known interferences to enhance the performance of MU-MISO systems [5], [6], [7], [8]. The interference is considered to be constructive if it pushes the received symbols deeper in the constructive region of the desired symbol. Therefore, with the knowledge of both the channel state information (CSI) and users' data symbols at the network access points, the precoder can be designed to make all the multi-user interference constructive to the received symbols. The CI exploitation technique has been extensively investigated over the past few years. This line of research has been presented in [5], where the CI precoding has been proposed for down-link multiple input multiple-output (MIMO) systems. The results in [5] showed that the CI precoding can greatly enhance the signal to interference-plus-noise ratio (SINR) without increasing the transmission power. In [6], a low-complexity vector precoding scheme for CI in down-link MU-MISO system was proposed including initial optimization-based CI precoding schemes. The authors in [7] presented transmit beam-forming techniques for MU-MISO systems in order to minimize the transmit power by exploiting the well-known interference. In [8], [9], CI precoding has been applied in energy-harvesting systems in order to minimize the transmit power whilst providing the required energy-harvested and the quality-of-service constraints for PSK symbols. Further work in [10] implemented the CI exploitation technique to massive-MIMO systems. The authors in [11] derived closed-form expression for CI precoding in the MU-MIMO downlink. This closed-form expression has paved the way to develop theoretical analysis of the CI precdoing technique. Based on this precoding expression, the performance analysis of the CI precoding in MU-MISO systems has been investigated in [12]. Very recently, the concept of CI has been proposed to enhance the physical layer security in communication systems. In [13] the interference exploitation technique has been used to design different artificial noise (AN) precoders. In [14], secure beam-forming for simultaneous wireless information and power transfer in MU-MIMO systems has been proposed based on the concept of CI exploitation techniques.

Building on the above CI approaches, our focus is on the analysis of the CI concept for physical layer security. The concept of physical layer security has been developed by Wyner in [15], where the wiretap channel for point-to-point channel has been presented. Then, Csiszar and Korner in [16] extended the wiretap channel to broadcast channels. These works reported that, achieving secure wireless communications is possible if the main/user channel quality is better than the wiretap/eavesdropper channel. Based on this fact, physical layer security of MU-MIMO systems has particularly attracted a significant amount of attention. However, most of the works in literature have focused on Gaussian signals, which is not practical assumption [17], [18], [19], [20]. The assumption of Gaussian input may lead to essential secrecy rate loss when the Gaussian input is replaced by finite-alphabet input. On the contrary, recently several works have considered the security of MU-MISO systems with finite alphabet signals. For instance, in [21] linear precoding design that aims to maximize the secrecy for MIMO systems under the constraint of finite-alphabet input and in the presence of multiple antennas eavesdropper has been studied. The authors in [22], [23] considered the impact of finite discrete constellation on the instantaneous and ergodic secrecy rates of MIMO systems. With statistical CSI of the eavesdropper's channel at the BS, in [24] approximated ergodic secrecy rate has been used to design secure communication of multi-antenna eavesdropper wiretap channels. Further work in [25] investigated secure transmission for large-scale MIMO systems with finite alphabet signals.

Accordingly, in this paper we analyze the secrecy performance of CI precoding technique in MU-MISO systems under a PSK input alphabet 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 extensively analyzed in terms of symbol error probability (SEP), secrecy sum-rate, and intercept probability (IP). 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, secrecy sum-rate and IP. 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. Throughout this paper, Monte-Carlo simulations are presented to confirm the correctness of the derived expressions in this work, and the impact of various system parameters on the secrecy performance has been investigated and discussed.

For clarity we list the major contributions of this work as follows.

1) Symbol Errror Probability: Firstly, we derive new exact analytical expressions for the average SEP of the legitimate users and eavesdroppers. In addition, for simplicity and in order to provide more insight, we also derive very accurate closed-form asymptotic approximation for the average SEPs.
2) Secrecy Sum-Rate with non-Gaussian Signaling: Furthermore, we extend our analysis to the secrecy sum-rate, and closed-form analytical expression of the ergodic secrecy sum-rate is provided.
3) Adaptive Modulation for Secrecy: Based on the derived expression of the ergodic secrecy sum-rate, we propose employing AM technique to enhance the secrecy sum-rate for the MU-MISO systems with PSK signals. In this regard, new analytical expression of the secrecy sum-rate for AM scheme is derived.
4) Intercept probability: analytical expressions of the IP with fixed and adaptive modulations are presented, including a simplified analytical expression of the IP based on the received SINRs.

The results in this paper show that, the interference exploitation technique yields superior performance over the conventional interference suppression techniques in terms of SEP, secrecy sum-rate and the IP. Particularly, the CI precoding can provide up to 17dB gain in the transmit SNR in terms of SEP, and up to 10dB gain in the transmit SNR in terms of the secrecy sum-rate and the IP. In addition, the proposed AM scheme outperforms the fixed modulation scheme by up to 66% at given values of the transmit SNR.

Next, Section II describes the MU-MISO system model. Section III, derives the exact and approximate analytical expressions for the average SEP of the users and the eavesdroppers. Section IV, presents the derivation of the ergodic secrecy sum-rate for fixed and adaptive modulation schemes. Section V, considers the intercept probability for the CI precoding in MU-MISO systems. Numerical and simulation results are presented and discussed in Section VI. Finally, the main conclusions of this work are stated in Section VII.

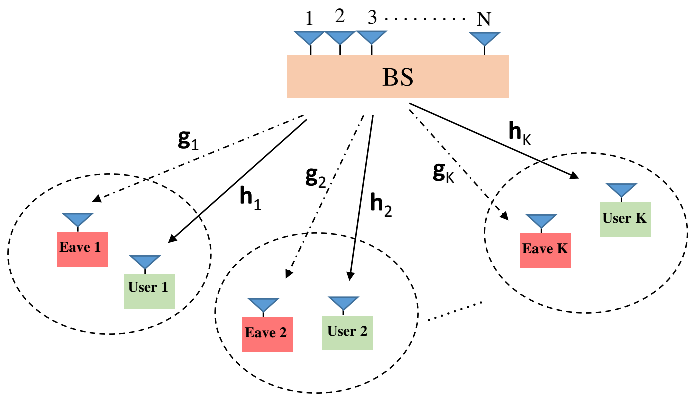


Figure 1: MU-MISO down-link with N antennas BS, single-antenna user-eavesdropper pairs.

II. System Model

We consider a MU-MISO system consisting of a BS and K user-eavesdropper pairs, where each legitimate user is wiretapped by an eavesdropper as illustrated in Fig. 1. The BS is equipped with N antennas, while each user and eavesdropper equipped with single antenna. The BS intends to transmit K confidential messages to the wiretapped users, and each eavesdropper tries to wiretap the user in the same pair, as in [26], [19], [27]. This scenario can occur in many practical applications, such as in the applications where the user-paring technique is implemented and the BS transmits confidential messages to only one user in each pair. The down-link $K \times N$ channel matrix between the BS and the legitimate users is denoted by $\mathbf{H}$, which is modeled as $\mathbf{H} = \mathbf{D}^{1/2}\tilde{\mathbf{H}}$, where the $K \times N$ matrix $\tilde{\mathbf{H}}$ represents the small-scale fading coefficients from the BS to the legitimate users which are assumed to be independent, circularly symmetric complex Gaussian random variables with zero mean and unit variance, and $\mathbf{D}$ is a $K \times K$ diagonal matrix models the path-loss with $[\mathbf{D}]_{kk} = \varpi_k = d_k^{-m}$ where d_k denotes the distance from the BS to the k^{th} user and m denotes the path-loss exponent. The $K \times N$ channel matrix between the BS and the K eavesdroppers is $\mathbf{G}$, which is modeled as $\mathbf{G} = \mathfrak{D}^{1/2}\tilde{\mathbf{G}}$ where the $K \times N$ matrix $\tilde{\mathbf{G}}$ represents the small-scale fading coefficients from the BS to the eavesdroppers which are also assumed to be independent, circularly symmetric complex Gaussian random variables with zero mean and unit variance and $\mathfrak{D}$ is a $K \times K$ diagonal matrix models the path-loss with $[\mathfrak{D}]_{kk} = \omega_k = \mathfrak{d}_k^{-m}$ where $\mathfrak{d}_k$ is the distance between the BS and the k^{th} eavesdropper. It is assumed that the the BS knows the users' CSI but it knows only the statistics of evesdrppers' channels due to the eavesdroppers' passive nature. It is also assumed that the signal is equi-probably drawn from an M-PSK constellation.

The received signals at the k^{th} user and the k^{th} eavesdropper in the considered system can be written, respectively, as

$$y_{d,k} = \sqrt{P}\mathbf{h}_k \mathbf{W}\mathbf{s} + n_{d,k} = \sqrt{P}\sum_{i=1}^{K} \mathbf{h}_k \left[\mathrm{W}\right]_i s_i + n_{d,k} \tag{1}$$

$$y_{e,k} = \sqrt{P}\boldsymbol{g}_k \mathbf{W}\mathbf{s} + n_{e,k} \tag{2}$$

where $\mathbf{s} = \left[s_1, s_2, ..., s_K\right]^H$ is the PSK-modulated signal vector, P is the BS transmission power, $\mathbf{h}_k$ is the channel vector from the BS to user k, $\boldsymbol{g}_k$ is the channel vector from the BS to eavesdropper k, $\mathbf{W}$ is the precoding matrix, $n_{d,k}$ and $n_{e,k}$ are the additive wight Gaussian noise (AWGN) at the k^{th} user, $n_{d,k} \sim \mathcal{CN}\left(0, \sigma^2_{d,k}\right)$, and the k^{th} eavesdropper, $n_{e,k} \sim \mathcal{CN}\left(0, \sigma^2_{e,k}\right)$, respectively. The CI precoding matrix with PSK signaling can be expressed as [11], [12]

$$\mathbf{W} = \frac{1}{K}\beta\, \mathbf{H}^H \left(\mathbf{H}\mathbf{H}^H\right)^{-1} \mathrm{diag}\left\{\mathbf{V}^{-1}\mathbf{u}\right\} \mathbf{s}\mathbf{s}^H, \tag{3}$$

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

III. Analysis of Symbol Error Probability

Secure transmission schemes can be designed 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 minimum required difference between the SEPs of the legitimate users and the eavesdroppers [28]. Consequently, in this section we analyze the symbol error performance of both the k^{th} user and the j^{th}eavesdropper as follows.

A. Average SEP of the Legitimate Users

In CI precoding the resulting interference contributes to the useful signal power, thus it has been shown that the received SNR at the k^{th} user can be written as

$$\gamma_{d,k} = \frac{\left|\sqrt{P}\boldsymbol{h}_k \mathbf{W}\mathbf{s}\right|^2}{\sigma_{d,k}^2} \tag{4}$$

Substituting (3) into (4) we can get

$$\gamma_{d,k} = \frac{\left|\frac{\sqrt{P}\beta}{K}\mathbf{bD}\boldsymbol{c}\frac{\boldsymbol{b}\mathbf{A}\boldsymbol{c}}{\mathbf{bDc}}s_k\right|^2}{\sigma_{d,k}^2} = \alpha_k \left|\Psi\right|^2 \tag{5}$$

where $\mathbf{A} = \mathbf{H}\mathbf{H}^H$, $\mathbf{b} = \mathbf{a}_k\left(\mathrm{diag}\left(\mathbf{s}^H\right)\right)$, $\boldsymbol{c} = \left(\mathrm{diag}\left(\mathbf{s}\right)\right)\mathbf{u}$, $\mathbf{a}_k$ is a $1 \times K$ vector the k^{th} element of this vector is one, and all the other elements are zeros, $\beta = \frac{1}{\sqrt{\mathbf{u}^H \mathrm{diag}(\mathbf{s}^H)^{-1} N \mathrm{D}(\mathrm{diag}(\mathbf{s}))^{-1}\mathbf{u}}}$ [29], [12], $\alpha_k = \frac{\left|\frac{\sqrt{P}\beta}{K}\mathbf{bD}\boldsymbol{c}\right|^2}{\sigma_k^2}$ and $\Psi = \frac{\boldsymbol{b}\mathbf{A}\boldsymbol{c}}{\mathbf{bDc}}$. It was shown in literature that Ψ has Gamma distribution with shape parameter ν and scale parameter θ, $\Psi \sim \Gamma\left(\nu, \theta\right)$, where in the considered scenario $\nu = N$ and $\theta = 1$ [29]. Consequently, the received SNR, $\gamma_{d,k}$, has General Gamma distribution $\Gamma\left(\rho, \varrho, \kappa_k\right)$ with $\rho = \frac{1}{2}$, $\varrho = \frac{\nu}{2}$ and $\kappa_k = \alpha_k$. Therefore, the cumulative distribution function (CDF) and the probability density function (PDF) of the received SNR, $\gamma_{d,k}$ can be written, respectively, as

$$F_{\gamma_{d,k}}\left(\gamma\right) = \left(\frac{\varphi\left(\varrho/\rho, \left(\gamma/\kappa_k\right)^{\rho}\right)}{\Gamma\left(\varrho/\rho\right)}\right), \qquad f_{\gamma_{d,k}}\left(\gamma\right) = \left(\frac{\left(\frac{\rho}{\kappa_k^{\varrho}}\right)\gamma^{\varrho-1}e^{-\left(\frac{\gamma}{\kappa_k}\right)^{\rho}}}{\Gamma\left(\frac{\varrho}{\rho}\right)}\right) \tag{6}$$

where $\varphi\left(.\right)$ is the lower incomplete Gamma function.

1) Exact SEP: The exact average SEP of a legitimate user in the considered scenario can be evaluated using the following Theorem.

Theorem 1. *The exact analytical expression of the average SEP of the k^{th} legitimate user is*

$$SP_k = \frac{1}{\pi}\int_0^{\frac{\pi(M-1)}{M}}\int_0^{\infty}\frac{e^{-z\gamma}\left(\frac{\rho}{\kappa_k^{\varrho}}\right)\gamma^{\varrho-1}e^{-\left(\frac{\gamma}{\kappa_k}\right)^{\rho}}}{\Gamma\left(\frac{\varrho}{\rho}\right)}d\gamma d\Phi \tag{7}$$

and

$$SP_k = \frac{1}{\pi}\sum_{i=1}^{n}\int_0^{\frac{\pi(M-1)}{M}}\frac{H_i\sin^2\Phi}{\sin^2\left(\frac{\pi}{M}\right)}\frac{\left(\frac{\rho}{\kappa_k^{\varrho}}\right)\left(\frac{\gamma_i\sin^2\Phi}{\sin^2\left(\frac{\pi}{M}\right)}\right)^{\varrho-1}e^{-\left(\frac{\gamma_i\sin^2\Phi}{\sin^2\left(\frac{\pi}{M}\right)\kappa_k}\right)^{\rho}}}{\Gamma\left(\frac{\varrho}{\rho}\right)}d\Phi + R_i \tag{8}$$

where $z = \frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2 \Phi}$*,* γ_i *and* H_i *are the* i^{th} *zero and the weighting factor of the Laguerre polynomials, respectively, and the remainder* R_i *is negligible for* $n > 15$ *[30].*

Proof: Using a standard approach provided in literature [31], [32, (5.67)], the average SEP of M-PSK can be calculated by [31, (5.67)]

$$SP_k = \frac{1}{\pi} \int\limits_0^{\frac{\pi(M-1)}{M}} \mathcal{M}_{\gamma_{d,k}} \left(-\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2 \Phi} \right) d\Phi = \frac{1}{\pi} \int\limits_0^{\frac{\pi(M-1)}{M}} \mathcal{M}_{\gamma_{d,k}} \left(z \right) d\Phi \tag{9}$$

where $\mathcal{M}_{\gamma_{d,k}} \left(z \right)$ is the the moment-generating function (MGF) of the received SNR and $z = \frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2 \Phi}$. Therefore, the MGF of the received SNR, $\gamma_{d,k}$, can be derived as

$$\mathcal{M}_{\gamma} \left(z \right) = \int\limits_0^{\infty} e^{-z\gamma} f_{\gamma_{d,k}} \left(\gamma \right) d\gamma \tag{10}$$

Substituting the PDF in (6) into (10), we can find

$$\mathcal{M}_{\gamma_k} \left(z \right) = \int\limits_0^{\infty} e^{-z\gamma} \left(\frac{\left(\frac{\rho}{\kappa_k^{\varrho}}\right) \gamma^{\varrho - 1} e^{-\left(\frac{\gamma}{\kappa_k}\right)^{\rho}}}{\Gamma\left(\frac{\varrho}{\rho}\right)} \right) d\gamma \tag{11}$$

Applying Gaussian Quadrature rule, the MGF can be obtained by,

$$\mathcal{M}_{\gamma_k} \left(z \right) = \sum_{i=1}^{n} \frac{\mathrm{H}_i}{z} \left(\frac{\left(\frac{\rho}{\kappa_k^{\varrho}}\right) \left(\frac{\gamma_i}{z}\right)^{\varrho - 1} e^{-\left(\frac{\gamma_i}{z\kappa_k}\right)^{\rho}}}{\Gamma\left(\frac{\varrho}{\rho}\right)} \right) + R_i \tag{12}$$

where γ_i and H_i are the i^{th} zero and the weighting factor of the Laguerre polynomials, respectively, and the remainder R_i is negligible for $n > 15$ [30]. By substituting (11) and (12) into (9), we can find the exact average SEP as in (7) and (8). ■

2) Closed-form approximate SEP: The exact SEP expression in Theorem 1 is presented with only single integration which can be evaluated efficiently using numerical integration techniques. In order to provide more insights, in the next Theorem we present very accurate closed-form approximation of the average SEP.

Theorem 2. *Very accurate closed-form expression of the average SEP of the* k^{th} *legitimate user is*

$$SP_k = \left(\frac{\frac{\pi(M-1)}{M}}{2\pi} - \frac{1}{6}\right)\sum_{i=1}^{n}\frac{\boldsymbol{H}_i}{\sin^2\left(\frac{\pi}{M}\right)}\left(\frac{\left(\frac{\rho}{\kappa_k^{\varrho}}\right)\left(\frac{\gamma_i}{\sin^2\left(\frac{\pi}{M}\right)}\right)^{\varrho-1} e^{-\left(\frac{\gamma_i}{\kappa_k \sin^2\left(\frac{\pi}{M}\right)}\right)^{\rho}}}{\Gamma\left(\frac{\varrho}{\rho}\right)}\right)$$

$$+\frac{1}{4}\sum_{i=1}^{n}\frac{3\boldsymbol{H}_i}{4\sin^2\left(\frac{\pi}{M}\right)}\left(\frac{\left(\frac{\rho}{\kappa_k^{\varrho}}\right)\left(\frac{3\gamma_i}{4\sin^2\left(\frac{\pi}{M}\right)}\right)^{\varrho-1} e^{-\left(\frac{3\gamma_i}{4\kappa_k \sin^2\left(\frac{\pi}{M}\right)}\right)^{\rho}}}{\Gamma\left(\frac{\varrho}{\rho}\right)}\right)$$

$$+\left(\frac{\frac{\pi(M-1)}{M}}{2\pi} - \frac{1}{4}\right)\sum_{i=1}^{n}\frac{\boldsymbol{H}_i \sin^2\frac{\pi(M-1)}{M}}{\sin^2\left(\frac{\pi}{M}\right)}\left(\frac{\left(\frac{\rho}{\kappa_k^{\varrho}}\right)\left(\frac{\gamma_i \sin^2\frac{\pi(M-1)}{M}}{\sin^2\left(\frac{\pi}{M}\right)}\right)^{\varrho-1} e^{-\left(\frac{\gamma_i \sin^2\frac{\pi(M-1)}{M}}{\kappa_k \sin^2\left(\frac{\pi}{M}\right)}\right)^{\rho}}}{\Gamma\left(\frac{\varrho}{\rho}\right)}\right) \tag{13}$$

Proof: Firstly, (9) can be written as

$$SP_k = \mathcal{E}\left[\frac{1}{\pi}\int_{0}^{\frac{\pi}{2}} \exp\left(-\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\theta}\right)d\theta + \frac{1}{\pi}\int_{\frac{\pi}{2}}^{\frac{\pi(M-1)}{M}} \exp\left(-\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\theta}\right)d\theta\right] \tag{14}$$

The first and the second terms in (14) can be efficiently approximated by [32], [33]

$$\frac{1}{\pi}\int_{0}^{\frac{\pi}{2}} \exp\left(-\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\theta}\right)d\theta \approx \frac{1}{12}e^{\left(-\sin^2\left(\frac{\pi}{M}\right)\right)} + \frac{1}{4}e^{\left(-\frac{4\sin^2\left(\frac{\pi}{M}\right)}{3}\right)} \tag{15}$$

$$\frac{1}{\pi}\int_{\frac{\pi}{2}}^{\frac{\pi(M-1)}{M}} \exp\left(-\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\theta}\right)d\theta \approx \frac{1}{2\pi}\left(e^{\left(-\sin^2\left(\frac{\pi}{M}\right)\right)} + \frac{1}{4}e^{\left(-\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\frac{\pi(M-1)}{M}}\right)}\right)\left(\frac{\pi\left(M-1\right)}{M} - \frac{\pi}{2}\right) \tag{16}$$

Now substituting (15) and (16) into (14), we can find approximate expression of SEP as [32], [33]

$$SP_k = \mathcal{E}\left[\frac{1}{12}e^{\left(-\sin^2\left(\frac{\pi}{M}\right)\right)} + \frac{1}{4}e^{\left(-\frac{4\sin^2\left(\frac{\pi}{M}\right)}{3}\right)} + \frac{1}{2\pi}\left(e^{\left(-\sin^2\left(\frac{\pi}{M}\right)\right)} + \frac{1}{4}e^{\left(-\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\frac{\pi(M-1)}{M}}\right)}\right)\left(\frac{\pi\left(M-1\right)}{M} - \frac{\pi}{2}\right)\right] \tag{17}$$

and

$$SP_k = \left(\frac{\frac{\pi(M-1)}{M}}{2\pi} - \frac{1}{6}\right)\mathcal{M}_\gamma\left(\sin^2\left(\frac{\pi}{M}\right)\right)+\frac{1}{4}\mathcal{M}_\gamma\left(\frac{4\sin^2\left(\frac{\pi}{M}\right)}{3}\right)+\left(\frac{\frac{\pi(M-1)}{M}}{2\pi} - \frac{1}{4}\right)\mathcal{M}_\gamma\left(\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\frac{\pi(M-1)}{M}}\right) \tag{18}$$

Finally, substituting (12) into (18), the approximate expression can be written as in (13). ■

B. Average SEP of the Eavesdroppers

Here we derive the exact and the approximate expressions for the average SEP of the k^{th} eavesdropper. After substituting (3) into (2) and collecting terms, the received signal at the k^{th} eavesdropper can be expressed as

$$y_{e,k} = \frac{\sqrt{P}\beta}{K}\boldsymbol{g}_j\, \left[\mathbf{H^H}\right]_k u_k s_k + \frac{\sqrt{P}\beta}{K}\sum_{r=1,r\neq k}^{K}\boldsymbol{g}_k\left[\mathbf{H^H}\right]_r u_r s_r + n_{e,k} \tag{19}$$

Hence, the SINR at the k^{th} eavesdropper using CI precoding can be written as

$$\gamma_{e,k} = \frac{\left|\frac{\sqrt{P}\beta}{K}\boldsymbol{g}_k\, \left[\mathbf{H^H}\right]_k u_k\right|^2}{\sum\limits_{r=1,r\neq k}^{K}\left|\frac{\sqrt{P}\beta}{K}\boldsymbol{g}_k\, \left[\mathbf{H^H}\right]_r u_r\right|^2 + \sigma_{e,k}^2} \tag{20}$$

This SINR expression in (20) can also be expressed as

$$\gamma_{e,k} = \frac{\frac{\left|\boldsymbol{g}_k\left[\mathbf{H^H}\right]_k u_k\right|^2}{\left\|\boldsymbol{g}_j\right\|^2}}{\sum\limits_{r=1,r\neq k}^{K}\frac{\left|\boldsymbol{g}_k\left[\mathbf{H^H}\right]_r u_r\right|^2}{\left\|\boldsymbol{g}_k\right\|^2} + \frac{\delta_k}{\left\|\boldsymbol{g}_k\right\|^2}} \tag{21}$$

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

$$F_{\gamma_{e,k}}\left(\bar{\gamma}\right) = \Pr\left(\gamma_{e,k} < \bar{\gamma}\right) = \Pr\left(\frac{X}{Y+Z} < \bar{\gamma}\right) \tag{22}$$

where $X = \frac{\left|\boldsymbol{g}_k\left[\mathbf{H^H}\right]_r u_r\right|^2}{\left\|\boldsymbol{g}_k\right\|^2}$, $Y = \sum\limits_{r=1,r\neq k}^{K}\frac{\left|\boldsymbol{g}_k\left[\mathbf{H^H}\right]_k u_k\right|^2}{\left\|\boldsymbol{g}_k\right\|^2}$ and $Z = \frac{\delta_k}{\left\|\boldsymbol{g}_k\right\|^2}$. Hence, by conditioning on Y and Z we can write

$$F_{\gamma_{e,k}}\left(\bar{\gamma}\left|Y,Z\right.\right)=\Pr\left(X<\bar{\gamma}Y+\bar{\gamma}Z\right) \tag{23}$$

Since X has exponential distribution with parameter λ_x, the conditional distribution can be expressed as

$$F_{\gamma_{e,k}}\left(\bar{\gamma}\left|Y,Z\right.\right)=1-e^{-\lambda_x\left(\bar{\gamma}Y+\bar{\gamma}Z\right)}, \tag{24}$$

In addition, Y has sum of exponential distributions, i.e., Gamma distribution, $Y\sim\Gamma\left(\kappa,\tilde{\beta}\right)$, with shape parameter $\kappa=K-1$ and inverse scale parameter $\tilde{\beta}$, and PDF given by $f_Y\left(y\right)=\frac{y^{\kappa-1}e^{-\tilde{\beta}y}\tilde{\beta}^{\kappa}}{\Gamma(\kappa)}$. Thus, the CDF conditioning on Z can be found as

$$F_{\gamma_{e,k}}\left(\bar{\gamma}\left|Z\right.\right)=\int\limits_0^{\infty}\left(1-e^{-\lambda_x\left(\bar{\gamma}y+\bar{\gamma}Z\right)}\right)\left(\frac{y^{\kappa-1}e^{-\tilde{\beta}y}\tilde{\beta}^{\kappa}}{\Gamma\left(\kappa\right)}\right)dy,\ \text{for}\ \bar{\gamma}Y+\bar{\gamma}Z\geq 0 \tag{25}$$

$$F_{\gamma_{e,k}}\left(\bar{\gamma}\left|Z\right.\right)=1-\tilde{\beta}^{\kappa}e^{-\bar{\gamma}\lambda_x Z}\left(\tilde{\beta}+\bar{\gamma}\lambda_x\right)^{-\kappa},\ \bar{\gamma}>0 \tag{26}$$

Since Z has inverse Gamma distribution, the PDF of Z is $f_Z\left(z\right)=\frac{\left(\frac{1}{z}\right)^{v+1}\delta_k^{v}e^{-\frac{\delta_k}{z}}}{\Gamma(v)}$, where v is the shape parameter which is equal N. Finally, the CDF of $\gamma_{e,k}$ can be found as

$$F_{\gamma_{e,k}}\left(\bar{\gamma}\right)=1-\frac{2\tilde{\beta}^{\kappa}\delta_k^{\frac{v}{2}}\left(\lambda_x\bar{\gamma}\right)^{\frac{v}{2}}\left(\tilde{\beta}+\lambda_x\bar{\gamma}\right)^{-\kappa}\mathrm{J}\left[v,2\sqrt{\delta_k\lambda_x\bar{\gamma}}\right]}{\Gamma\left(v\right)},\ \bar{\gamma}>0 \tag{27}$$

where $\mathrm{J}\left[.\right]$ is the Besselk function.

1) Exact SEP: The exact average SEP of an eavesdropper in the system can be calculated as in the following Theorem.

Theorem 3. *The exact expression of the average SEP of the k^{th} eavesdropper is*

$$SP_{e,k}=\frac{1}{\pi}\int\limits_0^{\frac{\pi(M-1)}{M}}\left(1-z\int\limits_0^{\infty}e^{-z\bar{\gamma}}\left(\frac{2\tilde{\beta}^{\kappa}\delta_k^{\frac{v}{2}}\left(\lambda_x\bar{\gamma}\right)^{\frac{v}{2}}\left(\tilde{\beta}+\lambda_x\bar{\gamma}\right)^{-\kappa}J\left[v,2\sqrt{\delta_k\lambda_x\bar{\gamma}}\right]}{\Gamma\left(v\right)}\right)d\bar{\gamma}\right)d\Phi \tag{28}$$

and

$$SP_{e,k} = \frac{1}{\pi} \int\limits_{0}^{\frac{\pi(M-1)}{M}} \left(1 - \sum_{i=1}^{n} H_i \frac{2\tilde{\beta}^{\kappa} \delta_k^{\frac{v}{2}} \left(\frac{\lambda_x \bar{\gamma}_i}{z}\right)^{\frac{v}{2}} \left(\tilde{\beta} + \frac{\lambda_x \bar{\gamma}_i}{z}\right)^{-\kappa} J\left[v, 2\sqrt{\frac{\delta \lambda_x \bar{\gamma}_i}{z}}\right]}{\Gamma(v)} \right) d\Phi + R_i \tag{29}$$

where $z = \frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2 \Phi}$*,* $\bar{\gamma}_i$ *and* H_i *are the* i^{th} *zero and the weighting factor of the Laguerre polynomials, respectively, and the remainder* R_i *is negligible for* $n > 15$ *[30].*

Proof: Using a standard approach, the SEP with M-PSK can be expressed as [31, (5.67)]

$$SP_{e,k} = \frac{1}{\pi} \int\limits_{0}^{\frac{\pi(M-1)}{M}} \mathcal{M}_{\gamma_{e,k}}(z)\, d\Phi \tag{30}$$

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

$$\mathcal{M}_{\gamma_{e,k}}(z) = 1 - z \int\limits_{0}^{\infty} e^{-z\bar{\gamma}} \left(1 - F_{\gamma_{e,k}}(\bar{\gamma})\right) d\bar{\gamma} \tag{31}$$

Substituting (27) into (31) we can get

$$\mathcal{M}_{\gamma_{e,k}}(z) = 1 - z \int\limits_{0}^{\infty} e^{-z\bar{\gamma}} \frac{2\tilde{\beta}^{\kappa} \delta_k^{\frac{v}{2}} \left(\lambda_x \bar{\gamma}\right)^{\frac{v}{2}} \left(\tilde{\beta} + \lambda_x \bar{\gamma}\right)^{-\kappa} \mathrm{J}\left[v, 2\sqrt{\delta_k \lambda_x \bar{\gamma}}\right]}{\Gamma(v)} d\bar{\gamma} \tag{32}$$

Applying Gaussian Quadrature rule, the MGF can be obtained by

$$\mathcal{M}_{\gamma_{e,k}}(z) = 1 - \sum_{i=1}^{n} \mathrm{H}_i \frac{2\tilde{\beta}^{\kappa} \delta_k^{\frac{v}{2}} \left(\frac{\lambda_x \bar{\gamma}_i}{z}\right)^{\frac{v}{2}} \left(\tilde{\beta} + \frac{\lambda_x \bar{\gamma}_i}{z}\right)^{-\kappa} \mathrm{J}\left[v, 2\sqrt{\frac{\delta_k \lambda_x \bar{\gamma}_i}{z}}\right]}{\Gamma(v)} + R_i \tag{33}$$

Substituting (32) and (33) into (30), we can obtain the exact SEP of the eavesdropper as in (28) and (29). ∎

2) Closed-form approximate SEP: The single integration in Theorem 3 can be calculated using numerical integration methods, to provide more insights very accurate closed-form approximation of the average SEP is presented in the next Theorem.

Theorem 4. *Very accurate closed-form expression of the average SEP of the* k^{th} *eavesdropper is*

$$SP_{e,k}=\left(\frac{\Theta}{2\pi}-\frac{1}{6}\right)\left(1-\sum_{i=1}^{n}\boldsymbol{H}_i\frac{2\tilde{\beta}^{\kappa}\delta_k^{\frac{v}{2}}\left(\frac{\lambda_x\bar{\gamma}}{\sin^2\left(\frac{\pi}{M}\right)}\right)^{\frac{v}{2}}\left(\tilde{\beta}+\frac{\lambda_x\bar{\gamma}}{\sin^2\left(\frac{\pi}{M}\right)}\right)^{-\kappa}\boldsymbol{J}\left[v,2\sqrt{\frac{\delta_k\lambda_x\bar{\gamma}}{\sin^2\left(\frac{\pi}{M}\right)}}\right]}{\Gamma\left(v\right)}\right)$$

$$+\frac{1}{4}\left(1-\sum_{i=1}^{n}\boldsymbol{H}_i\frac{2\tilde{\beta}^{\kappa}\delta_k^{\frac{v}{2}}\left(\frac{3\lambda_x\bar{\gamma}}{4\sin^2\left(\frac{\pi}{M}\right)}\right)^{\frac{v}{2}}\left(\tilde{\beta}+\frac{3\lambda_x\bar{\gamma}}{4\sin^2\left(\frac{\pi}{M}\right)}\right)^{-\kappa}\boldsymbol{J}\left[v,2\sqrt{\frac{3\delta_k\lambda_x\bar{\gamma}}{4\sin^2\left(\frac{\pi}{M}\right)}}\right]}{\Gamma\left(v\right)}\right)$$

$$+\left(\frac{\Theta}{2\pi}-\frac{1}{4}\right)\left(1-\sum_{i=1}^{n}\boldsymbol{H}_i\frac{2\tilde{\beta}^{\kappa}\delta_k^{\frac{v}{2}}\left(\frac{\sin^2\Theta\lambda_x\bar{\gamma}}{\sin^2\left(\frac{\pi}{M}\right)}\right)^{\frac{v}{2}}\left(\tilde{\beta}+\frac{\sin^2\Theta\lambda_x\bar{\gamma}}{\sin^2\left(\frac{\pi}{M}\right)}\right)^{-\kappa}\boldsymbol{J}\left[v,2\sqrt{\frac{\sin^2\Theta\delta_k\lambda_x\bar{\gamma}}{\sin^2\left(\frac{\pi}{M}\right)}}\right]}{\Gamma\left(v\right)}\right) \tag{34}$$

Proof: Using the expression in (18), we can find the approximation as [32], [33]

$$SP_{e,k}=\left(\frac{\Theta}{2\pi}-\frac{1}{6}\right)\mathcal{M}_{\gamma_{e,k}}\left(\sin^2\left(\frac{\pi}{M}\right)\right)+\frac{1}{4}\mathcal{M}_{\gamma_{ek}}\left(\frac{4\sin^2\left(\frac{\pi}{M}\right)}{3}\right)+\left(\frac{\Theta}{2\pi}-\frac{1}{4}\right)\mathcal{M}_{\gamma_{e,k}}\left(\frac{\sin^2\left(\frac{\pi}{M}\right)}{\sin^2\Theta}\right) \tag{35}$$

Substituting (33) into (35) we can get (34). ■

The numerical results show that the approximate expression in (34) is very tight to the exact one.

IV. Analysis of Secrecy Sum-Rate

To measure the security level of a communication network, the secrecy rate is usually considered which is basically defined by the maximum difference between the mutual information of the main and eavesdropper channels. In this work, it is assumed that the BS does not have any knowledge of the eavesdroppers channels (only statistics). In this case, the ergodic secrecy sum-rate can be obtained by [17], [18], [19], [20]

$$\bar{R}_s=\sum_{k=1}^{K}\left[\bar{R_{d_k}}-\bar{R_{e_k}}\right]^{+} \tag{36}$$

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

A. Ergodic Rate of the Users

Following the principles of CI, very accurate approximation of the ergodic rate for user k under PSK signaling using CI precoding technique can be written as[34], [35]

$$\bar{R_{d_k}} = \log_2 M - \frac{1}{M^N} \sum_{m=1}^{M^N} \underbrace{\mathcal{E}_{\mathbf{h}} \left\{ \log_2 \sum_{i=1}^{M^N} e^{\frac{-\left|\sqrt{P}\mathbf{h}_k [\mathrm{W}]_k s_{m,i}\right|^2}{2\sigma_{d,k}^2}} \right\}}_{\psi} \tag{37}$$

where $s_{m,i} = s_m - s_i$, s_m and s_i are symbols taken from the M signal constellation.

Theorem 5. *The ergodic rate of user k using CI precoding technique is*

$$\bar{R_{d_k}} = \log_2 M - \frac{1}{M^N} \sum_{m=1}^{M^N} \log_2 \sum_{i=1}^{M^N} \mathit{\Lambda}_{k_{m,i}}. \tag{38}$$

where

$$\begin{aligned} \mathit{\Lambda}_{k_{m,i}} = & \left(\left(\frac{2^{\left(\frac{1}{2}(N-K-1)\right)} K^{(N-K+1)} \left|s_{m,i}\right|^{-2+K-N}}{(N-K)!} \right) \left(\left(\frac{\varsigma_k^2}{\sigma_{d,k}^2} \right)^{\frac{1}{2}(K-N-1)} \right) \right) \\ & \times \left(\left(\varsigma_k^2 \left|s_{m,i}\right|\right) \Gamma \left(\frac{1}{2} (N-K+1) \right) {}_1\mathrm{F}_1 \left(\frac{1}{2} (N-K+1), \frac{1}{2}, \frac{K^2 \sigma_{d,k}^2}{2\varsigma_k^2 \left|s_{m,i}\right|^2} \right) \right. \\ & \left. -\sqrt{2} K \varsigma_k \sigma_{d,k}^2 \Gamma \left(\frac{1}{2} (N-K+2) \right) {}_1\mathrm{F}_1 \left(\frac{1}{2} (N-K+2), \frac{3}{2}, \frac{K^2 \sigma_{d,k}^2}{2\varsigma_k^2 \left|s_{m,i}\right|^2} \right) \right) \end{aligned} \tag{39}$$

where ${}_1\mathrm{F}_1$ is the Hypergeometric function and $\varsigma_k = \frac{\sqrt{P}\beta \mathbf{a}_k \mathbf{D} \boldsymbol{u}}{K}$.

Proof: Substituting (3) into (37), we can write the average rate as

$$\bar{R_{d_k}} = \log_2 M - \frac{1}{M^N} \sum_{m=1}^{M^N} \underbrace{\mathcal{E}_{\mathbf{h}} \left\{ \log_2 \sum_{i=1}^{M^N} e^{\frac{-\left|\frac{\sqrt{P}\beta}{K} \mathbf{a}_k \mathbf{F} \mathbf{u} s_{m,i}\right|^2}{2\sigma_{d,k}^2}} \right\}}_{\psi}. \tag{40}$$

where $\mathbf{F} = \mathbf{V}^{-1}$. By using Jensen inequality, ψ, can be written as

$$\psi = \mathcal{E}_{\mathbf{h}} \left\{ \log_2 \sum_{i=1}^{M^N} e^{\frac{-\left| \frac{\sqrt{P}\beta}{K} \mathbf{a}_k \mathbf{Fu} s_{m,i} \right|^2}{2\sigma_{d,k}^2}} \right\} \leq \log_2 \sum_{i=1}^{M^N} \underbrace{\mathcal{E}_{\mathbf{h}} \left\{ e^{\frac{-\left| \varsigma_k \, Y \, s_{m,i} \right|^2}{2\sigma_{d,k}^2}} \right\}}_{\Lambda_{k_{m,i}}} \tag{41}$$

where $Y = \frac{\mathbf{a}_k \mathbf{F} \boldsymbol{u}}{\mathbf{a}_k \mathbf{Du}}$, which has Gamma distribution, $Y \sim \Gamma(\nu, \theta)$ [29]. Therefore the average can be calculated by

$$\Lambda_{k_{m,i}} = \int_0^\infty e^{-\frac{\left| \varsigma_k \, Y s_{m,i} \right|^2}{2\sigma_{d,k}^2}} \frac{e^{-Ky} \left(Ky\right)^{N-K} K}{(N-K)!} dy, \tag{42}$$

which can be obtained as in (39). ■

B. Ergodic Rate of the Eavesdroppers

Similarly, following the principles of CI, very accurate approximation of the average rate for eavesdropper k under PSK signaling, using CI precoding technique can be written as[34], [35],

$$\bar{R_{e_k}} = \log_2 M - \frac{1}{M^N} \sum_{m=1}^{M^N} \underbrace{\mathcal{E} \left\{ \log_2 \sum_{i=1}^{M^N} e^{\frac{-\left| \frac{\sqrt{P}\beta}{K} \boldsymbol{g}_k \, \mathbf{H^H} \tilde{\mathbf{s}}_{m,i} + n_{e,k} \right|^2}{\sigma_{e,k}^2}} \right\}}_{\varphi}$$

$$+ \frac{1}{M^{N-1}} \sum_{m=1}^{M^{N-1}} \underbrace{\mathcal{E} \left\{ \log_2 \sum_{i=1}^{M^{N-1}} e^{\frac{-\left| \frac{\sqrt{P}\beta}{K} \boldsymbol{g}_k \, \mathbf{B} \mathfrak{s}_{m,i} + n_{e,k} \right|^2}{\sigma_{e,k}^2}} \right\}}_{\psi}, \tag{43}$$

where $\mathbf{B}$ is the matrix $\mathbf{H^H}$without vector k, and $\mathfrak{s}_{m,i}$ is a vector contains all the users' signals except user k signal.

Theorem 6. *The ergodic rate of eavesdropper k using CI precoding technique is*

$$\bar{R_{e_k}} = \log_2 M - \frac{1}{M^N} \sum_{m=1}^{M^N} \log_2 \sum_{i=1}^{M^N} \Upsilon_{k_{m,i}} + \frac{1}{M^{N-1}} \sum_{m=1}^{M^{N-1}} \log_2 \sum_{i=1}^{M^{N-1}} \Delta_{k_{m,i}}, \tag{44}$$

where

$$\Upsilon_{k_{m,i}} = \sum_{j=0}^{N} \frac{H_j}{2\sigma_{e,k}^2} \left(\frac{\delta_k^{\frac{v}{2}+\frac{1}{2}} \left(\frac{P\beta^2\tilde{\gamma}_j}{\omega_k\lambda_\nu 2K^2\sigma_{e,k}^2}\right)^{\frac{v}{2}-\frac{1}{2}} \left(\boldsymbol{J}\left(v-1, 2\sqrt{\frac{P\beta^2\delta_k\tilde{\gamma}_j}{2K^2\sigma_{e,k}^2\omega_k\lambda_\nu}}\right) + \boldsymbol{J}\left(v+1, 2\sqrt{\frac{P\beta^2\delta_k\tilde{\gamma}_j}{2K^2\sigma_{e,k}^2\omega_k\lambda_\nu}}\right)\right)}{\lambda_v\Gamma(v)} - \frac{\delta^{\frac{v}{2}} \left(\frac{P\beta^2\tilde{\gamma}_j}{2K^2\sigma_{e,k}^2\omega_k\lambda_\nu}\right)^{\frac{v}{2}-1} v\boldsymbol{J}\left(v, 2\sqrt{\frac{P\beta^2\delta_k\tilde{\gamma}_j}{2K^2\sigma_{e,k}^2\omega_k\lambda_\nu}}\right)}{\lambda_{\bar{v}}\Gamma(v)} \right) \tag{45}$$

and

$$\Delta_{k_{m,i}} = \sum_{j=0}^{N} \frac{H_j}{2\sigma_{e,k}^2} \left(\frac{\delta_k^{\frac{v}{2}+\frac{1}{2}} \left(\frac{P\beta^2\tilde{\gamma}_j}{\lambda_\upsilon 2K^2\sigma_{e,k}^2}\right)^{\frac{v}{2}-\frac{1}{2}} \left(\boldsymbol{J}\left(v-1, 2\sqrt{\frac{P\beta^2\delta_k\tilde{\gamma}_j}{2K^2\sigma_{e,k}^2\lambda_\upsilon}}\right) + \boldsymbol{J}\left(v+1, 2\sqrt{\frac{P\beta^2\delta_k\tilde{\gamma}_j}{2K^2\sigma_{e,k}^2\lambda_\upsilon}}\right)\right)}{\lambda_v\Gamma(v)} - \frac{\delta^{\frac{v}{2}} \left(\frac{P\beta^2\tilde{\gamma}_j}{2K^2\sigma_{e,k}^2\lambda_\upsilon}\right)^{\frac{v}{2}-1} v\boldsymbol{J}\left(v, 2\sqrt{\frac{P\beta^2\delta_k\tilde{\gamma}_j}{2K^2\sigma_{e,k}^2\lambda_\upsilon}}\right)}{\lambda_v\Gamma(v)} \right) \tag{46}$$

while $\tilde{\gamma}_j$ and H_j are the j^{th} zero and the weighting factor of the Laguerre polynomials, respectively, $\lambda_\nu = \|\tilde{\mathbf{s}}_{m,i}\|^2$, and $\lambda_\upsilon = \|\mathfrak{s}_{m,i}\|^2$.

Proof: By invoking Jensen inequality, the first term in (43), φ, can be expressed by

$$\varphi = \mathcal{E}\left\{\log_2 \sum_{i=1}^{M^N} e^{\frac{-\left|\frac{\sqrt{P}\beta}{K}\boldsymbol{g}_k \mathbf{H}^{\mathbf{H}}\tilde{\mathbf{s}}_{m,i}+n_{e,k}\right|^2}{\sigma_{e,k}^2}}\right\} \leq \log_2 \sum_{i=1}^{M^N} \mathcal{E}\left\{e^{\frac{-\left|\frac{\sqrt{P}\beta}{K}\boldsymbol{g}_k \mathbf{H}^{\mathbf{H}}\tilde{\mathbf{s}}_{m,i}+n_{e,k}\right|^2}{\sigma_{e,k}^2}}\right\} \tag{47}$$

Since the noise, $n_{e,k}$, has Gaussian distribution, the average over the noise can be derived as

$$\mathcal{E}_n\left\{e^{\frac{-\left|\frac{\sqrt{P}\beta}{K}\boldsymbol{g}_k \mathbf{H}^{\mathbf{H}}\tilde{\mathbf{s}}_{m,i}+n_{e,k}\right|^2}{\sigma_{e,k}^2}}\right\} = \frac{1}{\pi\sigma^2}\int_n e^{-\frac{\left|\frac{\sqrt{P}\beta}{K}\boldsymbol{g}_k \mathbf{H}^{\mathbf{H}}\tilde{\mathbf{s}}_{m,i}+n_{e,k}\right|^2+\left|n_{e,k}\right|^2}{\sigma_{e,k}^2}} dn. \tag{48}$$

Using the integrals of exponential function in [30], we can find

$$\mathcal{E}_n\left\{e^{\frac{-\left|\frac{\sqrt{P}\beta}{K}\boldsymbol{g}_k\,\mathbf{H}^{\mathbf{H}}\tilde{\mathbf{s}}_{m,i}+n_{e,k}\right|^2}{\sigma_{e,k}^2}}\right\}\approx\frac{1}{2}e^{-\frac{P\beta^2\left|\boldsymbol{g}_k\,\mathbf{H}^{\mathbf{H}}\tilde{\mathbf{s}}_{m,i}\right|^2}{2K^2\sigma_{e,k}^2}}. \quad (49)$$

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

$$F_{\mathit{\Omega}}\left(\tilde{\gamma}\right)=\Pr\left(\left|\boldsymbol{g}_k\,\mathbf{H}^{\mathbf{H}}\tilde{\mathbf{s}}_{m,i}\right|^2<\tilde{\gamma}\right)=\Pr\left(\underbrace{\frac{\left|\boldsymbol{g}_k\,\mathbf{H}^{\mathbf{H}}\tilde{\mathbf{s}}_{m,i}\right|^2}{\left\|\tilde{\boldsymbol{g}}_k\right\|^2}}_{\bar{v}}<\frac{\tilde{\gamma}}{\left\|\tilde{\boldsymbol{g}}_k\right\|^2}\right) \quad (50)$$

It is shown that $\bar{v}$ has exponential distribution with CDF, $F_{\bar{v}}\left(\bar{v}\right)=1-e^{-\frac{\bar{v}}{\lambda_{\bar{v}}}}$ and $\lambda_{\bar{v}}=\omega_k\left\|\tilde{\mathbf{s}}_{m,i}\right\|^2$. Let $Z=\frac{1}{\left\|\tilde{\boldsymbol{g}}_k\right\|^2}$, now by conditioning on Z we can find,

$$\Pr\left(v<Z\,\tilde{\gamma}\right)=\int_0^{\infty}\left(1-e^{-\frac{Z\,\tilde{\gamma}}{\lambda_{\bar{v}}}}\right)f_Z\left(z\right)dz \quad (51)$$

Since Z has inverse Gamma distribution with PDF is given by $f_Z\left(z\right)=\frac{\left(\frac{1}{z}\right)^{v+1}\delta_k^{v}e^{-\frac{\delta}{z}}}{\Gamma(v)}$, the CDF can be found as

$$F_{\mathit{\Omega}}\left(\tilde{\gamma}\right)=\int_0^{\infty}\left(1-e^{-\frac{Z\,\tilde{\gamma}}{\lambda_{\bar{v}}}}\right)\frac{\left(\frac{1}{z}\right)^{v+1}\delta_k^{v}e^{-\frac{\delta}{z}}}{\Gamma\left(v\right)}dz=1-\frac{2\delta_k^{\frac{v}{2}}\left(\frac{\bar{\gamma}}{\lambda_{\bar{v}}}\right)^{\frac{v}{2}}\mathrm{J}\left[v,2\sqrt{\frac{\delta_k\bar{\gamma}}{\lambda_{\bar{v}}}}\right]}{\Gamma\left(v\right)} \quad (52)$$

Now the PDF can be obtained as

$$f_{\mathit{\Omega}}\left(\tilde{\gamma}\right)=\frac{\partial F_{\mathit{\Omega}}\left(\tilde{\gamma}\right)}{\partial\tilde{\gamma}} \quad (53)$$

$$=\frac{\delta_k^{\frac{v}{2}+\frac{1}{2}}\left(\frac{\tilde{\gamma}}{\lambda_{\bar{v}}}\right)^{\frac{v}{2}-\frac{1}{2}}\left(\mathrm{J}\left(v-1,2\sqrt{\frac{\delta_k\tilde{\gamma}}{\lambda_{\bar{v}}}}\right)+\mathrm{J}\left(v+1,2\sqrt{\frac{\delta_k\tilde{\gamma}}{\lambda_{\bar{v}}}}\right)\right)}{\lambda_{\bar{v}}\Gamma\left(v\right)}-\frac{\delta_k^{\frac{v}{2}}\left(\frac{\tilde{\gamma}}{\lambda_{\bar{v}}}\right)^{\frac{v}{2}-1}v\mathrm{J}\left(v,2\sqrt{\frac{\delta_k\tilde{\gamma}}{\lambda_{\bar{v}}}}\right)}{\lambda_{\bar{v}}\Gamma\left(v\right)} \quad (54)$$

Consequently, the average over the channels in (49) can be found as

$$\mathcal{E}\left\{e^{-\frac{P\beta^2\mathit{\Omega}}{2K^2\sigma_{e,k}^2}}\right\}=\Upsilon_{m,i}=\int_0^{\infty}\left(e^{-\frac{P\beta^2\mathit{\Omega}}{2K^2\sigma_{e,k}^2}}\right)f_{\mathit{\Omega}}\left(\tilde{\gamma}\right)d\tilde{\gamma} \quad (55)$$

$$\Upsilon_{m,i} = \int_0^{\infty} \left(e^{-\frac{P\beta^2 \Omega}{2K^2\sigma_{e,k}^2}} \right) \left(\frac{\delta_k^{\frac{v}{2}+\frac{1}{2}} \left(\frac{\tilde{\gamma}}{\lambda_{\bar{v}}} \right)^{\frac{v}{2}-\frac{1}{2}} \left(\mathbf{J}\left(v-1, 2\sqrt{\frac{\delta_k \tilde{\gamma}}{\lambda_{\bar{v}}}} \right) + \mathbf{J}\left(v+1, 2\sqrt{\frac{\delta_k \tilde{\gamma}}{\lambda_{\bar{v}}}} \right) \right)}{\lambda_{\bar{v}} \Gamma(v)} \right.$$

$$\left. - \frac{\delta_k^{\frac{v}{2}} \left(\frac{\tilde{\gamma}}{\lambda_{\bar{v}}} \right)^{\frac{v}{2}-1} v \mathbf{J}\left(v, 2\sqrt{\frac{\delta_k \tilde{\gamma}}{\lambda_{\bar{v}}}} \right)}{\lambda_{\bar{v}} \Gamma(v)} d\tilde{\gamma} \right) \tag{56}$$

Applying Gaussian Quadrature rule, we can find (45). For the second term, ψ,

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

By using Jensen inequality we can write

$$\psi = \mathcal{E} \left\{ \log_2 \sum_{i=1}^{M^{N-1}} e^{\frac{-\left| \frac{\sqrt{P}\beta}{K} \boldsymbol{g}_k \mathbf{B}\mathfrak{s}_{m,i} + n_{e,k} \right|^2}{\sigma_{e,k}^2}} \right\} \leq \log_2 \sum_{i=1}^{M^{N-1}} \mathcal{E} \left\{ e^{\frac{-\left| \frac{\sqrt{P}\beta}{K} \boldsymbol{g}_k \mathbf{B}\mathfrak{s}_{m,i} + n_{e,k} \right|^2}{\sigma_{e,k}^2}} \right\} \tag{57}$$

Similarly as in (48), since $n_{e,k}$ has Gaussian distribution, we can write

$$\varDelta_{m,i} = \mathcal{E} \left\{ e^{\frac{-P\beta^2 \left| \boldsymbol{g}_k \mathbf{B}\mathfrak{s}_{m,i} \right|^2}{2K^2\sigma_{e,k}^2}} \right\} \tag{58}$$

To derive the average over the channel we need firstly to find the distribution of $\tilde{\varOmega} = |\boldsymbol{g}_k \mathbf{B}\mathfrak{s}_{m,i}|^2$. The CDF of $\tilde{\varOmega}$ has the same formula as the CDF of $\varOmega$, hence the average over the channel can be found as in (46). ■

Now, we are ready to presnet the final analytical expression of the ergodic secrecy sum-rate as in the following Theorem.

Theorem 7. *The ergodic secrecy sum-rate of MU-MISO systems using CI precoding technique is*

$$\bar{R}_s = \sum_{k=1}^{K} \frac{1}{M^N} \left[\left(\sum_{m=1}^{M^N} \log_2 \sum_{i=1}^{M^N} \varLambda_{k_{m,i}} \right) + \left(\sum_{m=1}^{M^N} \log_2 \sum_{i=1}^{M^N} \Upsilon_{k_{m,i}} \right) - \left(M \sum_{m=1}^{M^{N-1}} \log_2 \sum_{i=1}^{M^{N-1}} \varDelta_{k_{m,i}} \right) \right]^+ \tag{59}$$

Proof: The ergodic secrecy sum-rate expression can be obtained by substituting (39) and (44) into (36). ■

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 the user's rate and the 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 [21], [22], [23], [24], [25]. In addition, from the above expressions and from the following results in Section VI, we can also observe that for each modulation scheme there is an optimal value of the transmit SNR that maximizes 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 scheme that can maximize the secrecy rate and achieve the SEP requirement. If none of the modulation schemes can achieve the target SEP, the BS selects the modulation scheme with the smallest constellation size [36], [37], [38], [39]. At SNRs 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 $\mathscr{N}$ available choices $\{M_1$,M_2, ...,$M_{\mathscr{N}}\}$ according to the following rule. The modulation order is $M = M_n = 2^n$ if $SP_{\max} = \max_k \left(SP_{k,M_n}\right) < \mathcal{P}$, where $n \in [1, \mathscr{N}]$, SP_{k,M_n} is the SEP of user k using the modulation order M_n. Let η_t be the transmit SNR, the optimal value of the transmit SNR using M_n-PSK can be defined as

$$\beta_n = \max_{\eta_t} \quad \bar{R}_{s,M_n}, \forall n. \tag{60}$$

where $\bar{R}_{s,M_n}$ is taken from (59). Based on the fact that, the SEP of each user depends on the received SNR at the user, we can define the user with maximum SEP, $SP_{\max}$, as the user who has minimum received SNR, $\gamma_{\min} = \min\left(\gamma_{d,1}, \gamma_{d,2}, ..., \gamma_{d,K}\right)$. Therefore, the AM selection can be performed by dividing the minimum SNR region into $\mathscr{N}+1$ fading regions defined by SNR thresholds, $\mu_0 < \mu_1 <$ ..... $< \mu_{\mathscr{N}+1} = \infty$. If the minimum SNR, $\gamma_{\min}$, is in the fading region of $\mu_n \leq \gamma_{\min} < \mu_{n+1}$, the M_n constellation size is chosen. The transmit SNR for each modulation scheme should be $\eta_t \leq \beta_n$. The conditional maximum SEP can be calculated by [31]

$$SP_{\max} = \frac{1}{\pi} \int_{0}^{\frac{\pi(M-1)}{M}} e^{\left(-\frac{\gamma_{\min} \sin^2\left(\frac{\pi}{M}\right)}{\sin^2\theta}\right)} d\theta \tag{61}$$

Since (61) is non-invertible, the region boundaries can only be obtained numerically as function of modulation order and the target SEP using the expression

$$\mathcal{P} = \frac{1}{\pi} \int\limits_{0}^{\frac{\pi(M_n-1)}{M_n}} e^{\left(-\frac{\mu_n \sin^2\left(\frac{\pi}{M}\right)}{\sin^2\theta}\right)} d\theta \tag{62}$$

According to the AM strategy described above, we can obtain the secrecy sum-rate expression as in the following Theorem.

Theorem 8. *The secrecy sum-rate using AM scheme, $\bar{R}_{s,am}$, in MU-MISO systems using CI precoding technique is*

$$\begin{aligned}\bar{R}_{s,am} =&\sum_{n=1}^{\mathcal{N}} \left(a_n \left(\prod_{k=1}^{K} \left[1 - \left(\frac{\varphi\left(N, (\mu_1/\kappa_k)^{\frac{1}{2}}\right)}{\Gamma(N)} \right) \right] + \prod_{k=1}^{K} \left[1 - \left(\frac{\varphi\left(N, (\mu_0/\kappa_k)^{\frac{1}{2}}\right)}{\Gamma(N)} \right) \right] \right) \right. \\ &+ \left. \left(\prod_{k=1}^{K} \left[1 - \left(\frac{\varphi\left(N, (\mu_{n+1}/\kappa_k)^{\frac{1}{2}}\right)}{\Gamma(N)} \right) \right] + \prod_{k=1}^{K} \left[1 - \left(\frac{\varphi\left(N, (\mu_n/\kappa_k)^{\frac{1}{2}}\right)}{\Gamma(N)} \right) \right] \right) \right) \\ &\times \left(\sum_{k=1}^{K} \frac{1}{M_n^N} \left[\left(\sum_{m=1}^{M_n^N} \log_2 \sum_{i=1}^{M_n^N} \mathit{\Lambda}_{k_{m,i}} \right) + \left(\sum_{m=1}^{M_n^N} \log_2 \sum_{i=1}^{M_n^N} \Upsilon_{k_{m,i}} \right) - \left(M_n \sum_{m=1}^{M_n^{N-1}} \log_2 \sum_{i=1}^{M_n^{N-1}} \mathit{\Delta}_{k_{m,i}} \right) \right]^{+} \right)\end{aligned} \tag{63}$$

Proof: The secrecy rate using AM scheme, $\bar{R}_{s,am}$, can be calculated by

$$\bar{R}_{s,am} =\sum_{n=1}^{\mathcal{N}} \left(a_n p_{0+} p_n\right) \bar{R}_{s,M_n} \tag{64}$$

where p_n is the probability that $\gamma_{\min}$ falls in the n^{th} region, and it is given by

$$p_n = \Pr\left(\mu_n \le \gamma_{\min} < \mu_{n+1}\right) = \int\limits_{\mu_n}^{\mu_{n+1}} f_{\gamma_{\min}}\left(\bar{\gamma}\right) d\bar{\gamma} = F_{\gamma_{\min}}\left(\mu_{n+1}\right) - F_{\gamma_{\min}}\left(\mu_n\right) \tag{65}$$

The CDF of $\gamma_{\min}$, $F_{\gamma_{\min}}\left(\bar{\gamma}\right)$, can be derived by [40]

$$F_{\gamma_{min}}\left(\bar{\gamma}\right) = 1 - \Pr\left(\gamma_{d,1} > \bar{\gamma}, ..., \gamma_{d,k} > \bar{\gamma}, ..., \gamma_{d,K} > \bar{\gamma}\right) \tag{66}$$

Since the received SNRs have correlated Gamma distribution, the CDF of $\gamma_{\min}$ can be bounded by [40, Section 5.4]

$$F_{\gamma_{min}}\left(\bar{\gamma}\right) = 1 - \prod_{k=1}^{K} \left[1 - F_{\gamma_{d,k}}\left(\bar{\gamma}\right)\right] \tag{67}$$

Substituting the CDF in (6) into (67) we can get

$$F_{\gamma_{min}}\left(\bar{\gamma}\right) = 1 - \prod_{k=1}^{K} \left[1 - \left(\frac{\varphi\left(N, \left(\bar{\gamma}/\kappa_k\right)^{\frac{1}{2}}\right)}{\Gamma\left(N\right)}\right)\right] \tag{68}$$

Now the probability p_n can be calculated by

$$p_n = \left(1 - \prod_{k=1}^{K} \left[1 - \left(\frac{\varphi\left(N, \left(\mu_{n+1}/\kappa_k\right)^{\frac{1}{2}}\right)}{\Gamma\left(N\right)}\right)\right]\right) - \left(1 - \prod_{k=1}^{K} \left[1 - \left(\frac{\varphi\left(N, \left(\mu_{n}/\kappa_k\right)^{\frac{1}{2}}\right)}{\Gamma\left(N\right)}\right)\right]\right) \tag{69}$$

Moreover, p_0 in (64) represents the probability that the minimum SNR, $\gamma_{\min}$, is below $\mu_1$which is given by

$$p_0 = \Pr\left(\mu_0 \leq \gamma_{\min} < \mu_1\right) = F_{\gamma_{\min}}\left(\mu_1\right) - F_{\gamma_{\min}}\left(\mu_0\right) \tag{70}$$

In this case non of the modulation schemes can achieve the target SEP, and the BS uses the smallest modulation scheme based on the value of the SNR, η_t, where $a_n$is defined as $a_n = 1$ if $\beta_{n-1} < \eta_t \leq \beta_n, \beta_0 = 0$, and $a_n = 0$ otherwise. ■

V. Intercept Probability

The intercept probability (IP) is a performance metric used to describe the secrecy performance of the wireless communication systems. The IP is defined as the probability that the eavesdropper is capable of successfully decoding the confidential signal intended for the legitimate user. Therefore, it is the probability that the achievable secrecy rate is less than zero, i.e., the rate of the main channel is less than that of the wiretap channel [41], [42]. The exact IP of pair k can be evaluated by [41], [42]

$$P_{in,k} = \Pr\left(R_{d_k} - R_{e_k} < 0\right) = \Pr\left(R_{d_k} < R_{e_k}\right) \tag{71}$$

In AM technique the IP can be defined as

$$P_{in,k} = \Pr\left(\sum_{n=1}^{\mathscr{N}} R_{d_k,M_n} < \sum_{n=1}^{\mathscr{N}} R_{e_k,M_n}\right) \tag{72}$$

The total intercept probability $(P_{in})$of this system is, $P_{in} = \sum_{k=1}^{K} P_{in,k}$ [41], [42]. As we can see in finite alphabet scenarios the rate expressions at the user and the eavesdropper are complicated, and thus any closed form solution of the IP is hard to find. However, the exact results of the IP can be obtained using Monte-Carlo simulation, as will be presented in Section (VI). For simplicity and to gain some insights in this section we consider the IP based on the received SINRs, $\left(P_{in}^{SINR_k}\right)$, which is presented in the following Theorem.

Theorem 9. *The IP of MU-MISO systems using CI precoding technique based on the received SINRs can be calculated by*

$$P_{in}^{SINR_k} = \left(\frac{\varphi\left(\varrho/\rho, (\gamma/\kappa_k)^{\rho}\right)}{\Gamma\left(\varrho/\rho\right)}\right) \times \left(\frac{2\beta^{\kappa}\delta_k^{\frac{v}{2}}\left(\lambda_x\bar{\gamma}\right)^{\frac{v}{2}}\left(\beta+\lambda_x\bar{\gamma}\right)^{-\kappa} J\left[v, 2\sqrt{\delta_k\lambda_x\bar{\gamma}}\right]}{\Gamma\left(v\right)}\right) \tag{73}$$

Proof: The IP can be defined as

$$P_{in}^{SINR_k} = \Pr\left(\gamma_{d,k} < \bar{\gamma}\right) \times \Pr\left(\gamma_{e,k} > \bar{\gamma}\right) \tag{74}$$

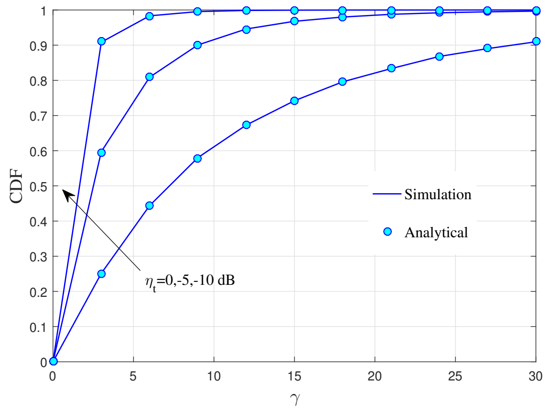
where $\bar{\gamma}$ is the threshold value. Using (27) the eavesdropper probability can be calculated by

$$\Pr\left(\gamma_{e,k} > \bar{\gamma}\right) = \frac{2\beta^{\kappa}\delta_k^{\frac{v}{2}}\left(\lambda_x\bar{\gamma}\right)^{\frac{v}{2}}\left(\beta+\lambda_x\bar{\gamma}\right)^{-\kappa} \mathrm{J}\left[v, 2\sqrt{\delta_k\lambda_x\bar{\gamma}}\right]}{\Gamma\left(v\right)} \tag{75}$$

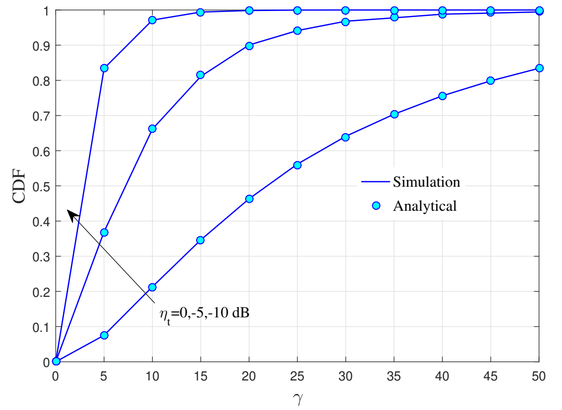
From (6) the user reception probability can be obtained as

$$\Pr\left(\gamma_{d,k} < \bar{\gamma}\right) = \left(\frac{\varphi\left(\varrho/\rho, (\gamma/\kappa_k)^{\rho}\right)}{\Gamma\left(\varrho/\rho\right)}\right) \tag{76}$$

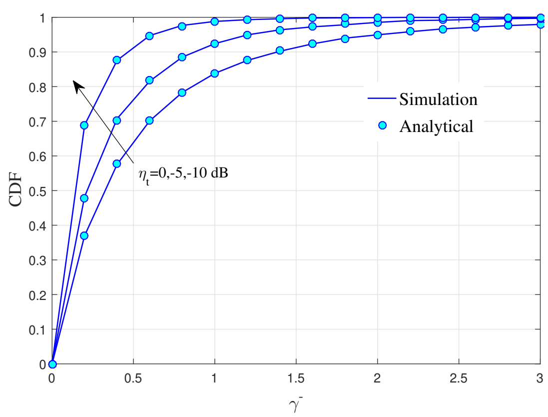
By substituting (75) and (76) into (74), we can obtain the final result in (73). ■



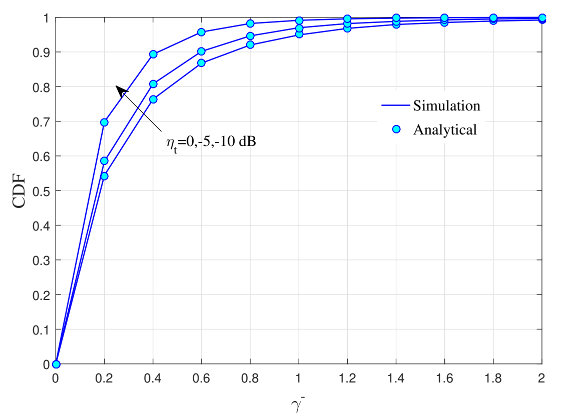
(a) The CDF of the received SNR of user k for different transmit SNR values,η_t, when $N = K = 3$.



(b) The CDF of the received SNR of user k for different transmit SNR values,η_t, when $N = K = 5$.



(c) The CDF of the received SINR of eavesdropper k for different transmit SNR values,η_t, when $N = K = 3$.



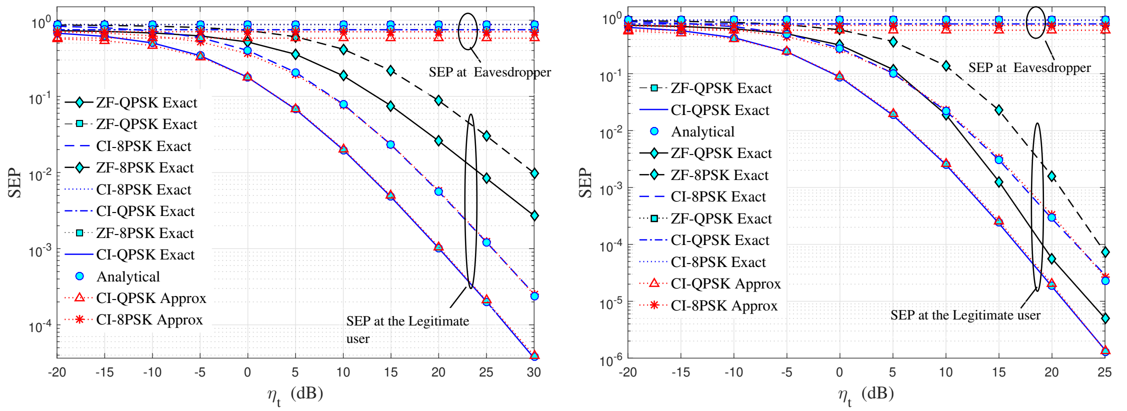
(d) The CDF of the received SINR of eavesdropper k for different transmit SNR values,η_t, when $N = K = 5$.

Figure 2: The CDF of the received SINRs for user k and eavesdropper k with different values of the transmit SNR, η_t, number of users K, and number of BS antennas N.

VI. Numerical Results

In this section we present some numerical and simulation results of the derived expressions in this work. Monte-Carlo simulations are performed with 10^6 independent trials. For simplicity, equal noise variances are assumed at the users, σ^2, thus the transmit SNR (η_t) can be defined as $\eta_t = \frac{P}{\sigma^2}$, and the path loss exponent is chosen to be $m = 2.7$. For sake of comparison, some simulation results of the interference suppression, ZF, scheme are also presented in this section.

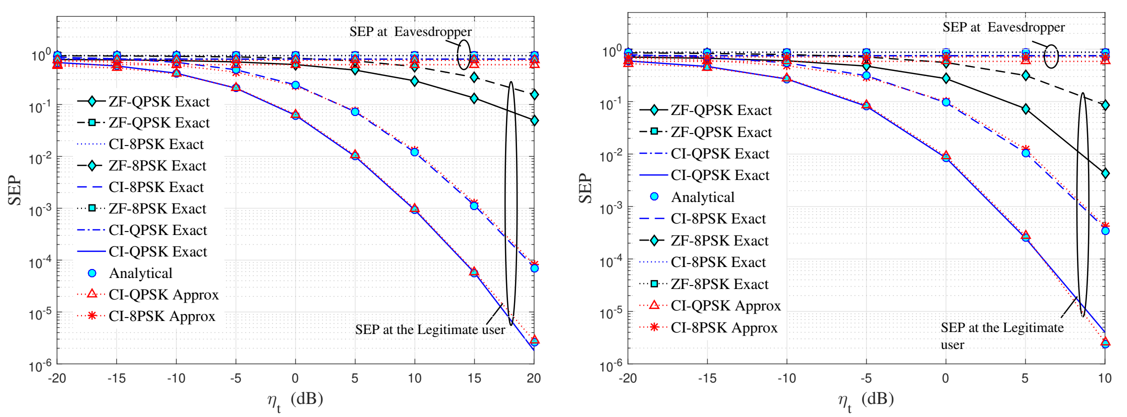
Firstly, in Fig. 2 we plot the CDF of the received SINRs of the k^{th} user and the k^{th} eavesdropper for different values of the transmit SNR, η_t, number of users, K, and number of BS antennas, N. It is evident that, the analytical and simulation results are in well agreement, which confirms the accuracy of the distribution considered in Section (III). It is worth mentioning that, the results presented in



(a) SEP versus transmit SNR, η_t, with different types of input, when $N = K = 3$.

(b) SEP versus transmit SNR, η_t, with different types of input, when $N = 5,\ K = 3$.

Figure 3: SEP versus transmit SNR with different types of input, and number of BS antennas.



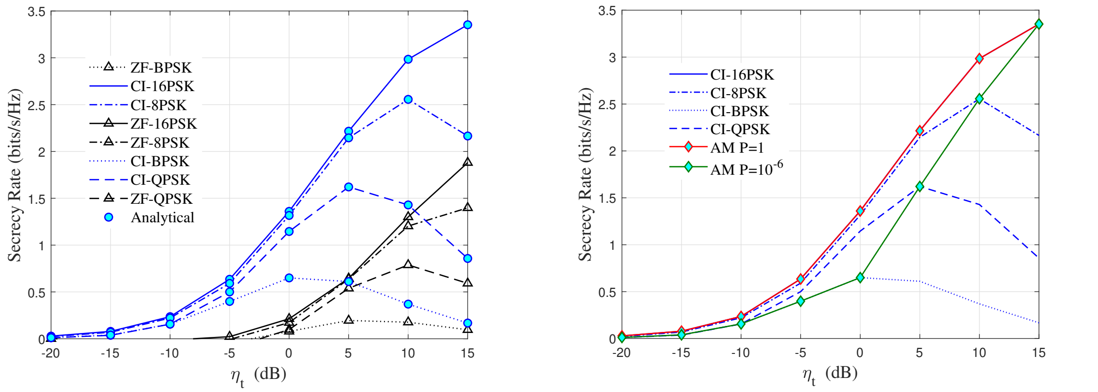
(a) SEP versus transmit SNR, η_t, with different types of input, when $N = K = 6$.

(b) SEP versus transmit SNR, η_t, with different types of input, when $N = 12,\ K = 6$.

Figure 4: SEP versus transmit SNR with different types of input, and number of BS antennas.

Fig. 2, can be used also to present the outage probability of the users and the eavesdroppers for CI precoding technique. The outage probability is the probability that the received SINR, falls below an acceptable threshold value, γ_{th}. Therefore, we can obtain the outage probability of the users and the eavesdroppers by replacing γ and $\bar{\gamma}$ with γ_{th}. From this perspective, it is clear that the legitimate users have better performance than the eavesdroppers, and the values of N and K have notable impact on the CDFs and thus on the secrecy performance in general.

In Fig. 3, we show the exact and approximate average SEPs with respect to the transmit SNR, η_t, for QPSK and 8-PSK. Fig. 3a, presents the SEPs when $N = K = 3$, and Fig. 3b, presents the SEPs when $N = 5,$ and $K = 3$. Firstly, it is evident that, the analytical and simulation results are in



(a) Secrecy rate versus transmit SNR, η_t, for fixed modulation schemes, when $N = K = 2$.

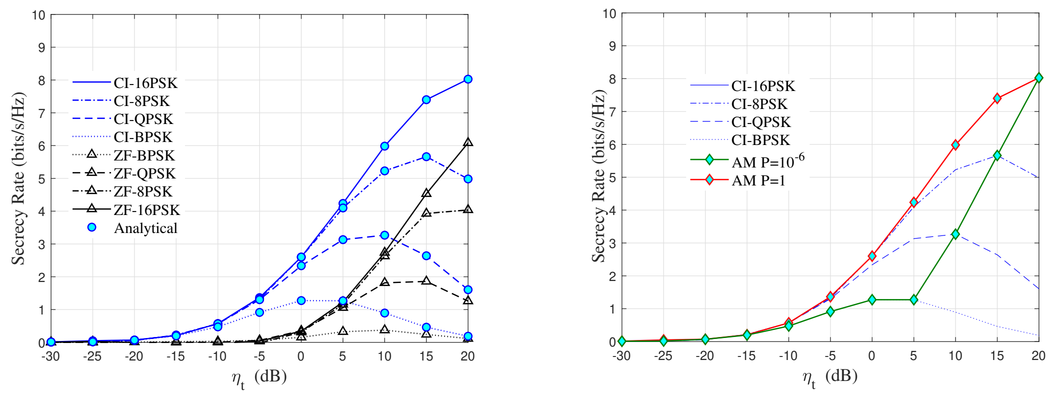
(b) Secrecy rate versus transmit SNR, η_t, for AM scheme, when $N = K = 2$, and $\mathcal{P} = 10^{-6}$, and 1.

Figure 5: Secrecy rate versus transmit SNR with different types of input for fixed and adaptive modulations.

well agreement, which confirms the accuracy of the analysis in Section (III). It is also clear that the approximate and exact analytical results are very close to each other. 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. 3a and 3b, it can also be noted that increasing number of BS antennas increases the gap between the SEPs of the users and the eavesdroppers, and reduces the gap between the CI and ZF techniques.

To illustrate the effect of users' number on the average SEPs, in Fig. 4 we present the average SEPs for the CI and ZF precoding techniques, when $N = K = 6$, as in Fig. 4a and when $N = 12$, $K = 6$ as in Fig. 4b. We can see from these results that, increasing number of BS antennas N and/or number of users K result in enhancing the secrecy performance. Furthermore, the CI precoding can provide additional up to 15dB gain in η_t compared to ZF scheme.

Fig. 5 illustrates the ergodic secrecy sum-rate versus the transmit SNR, for various input types when $N = K = 2$ for fixed and adaptive modulation schemes. Firstly, in Fig. 5a, we present the ergodic secrecy sum-rate for CI and ZF with different fixed modulation schemes. The analytical and simulation results of the ergodic secrecy rate are in well agreement, which confirms the derived expressions in Section (IV). It is also apparent 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



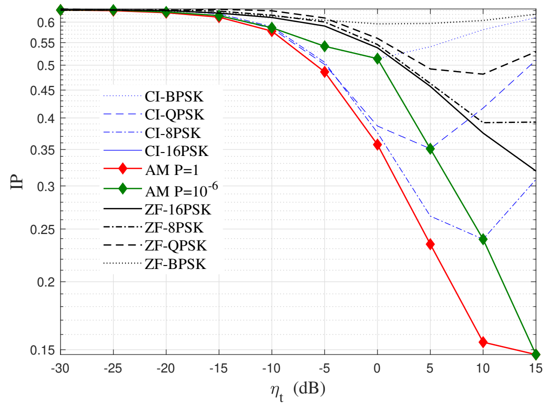
(a) Secrecy rate versus transmit SNR, η_t, for fixed modulation schemes, when $N = K = 3$.

(b) Secrecy rate versus transmit SNR, η_t, for AM scheme, when $N = K = 3$, and $\mathcal{P} = 10^{-6}$, and 1.

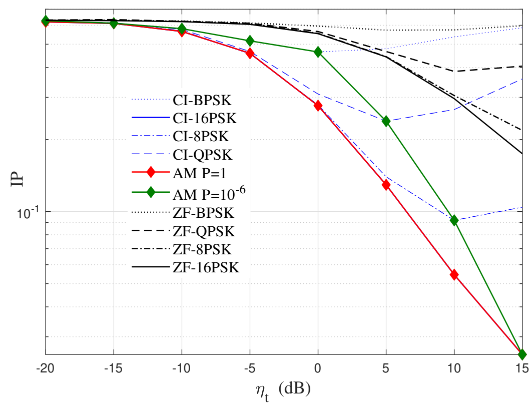
Figure 6: Secrecy rate versus transmit SNR with different types of input for fixed and adaptive modulations.

alphabet systems both the user's rate and the eavesdropper's rate will saturate at, $\log_2 M$, in high-SNR regime. Therefore the secrecy rate will tend to zero in the high SNR regime. This therefore necessitates the use of AM scheme. 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 in Fig. 5b the secrecy sum-rate of AM for CI versus the transmit SNR for different values of the target SEP, $\mathcal{P} = 1$ and 10^{-6}. In the first case when the target SEP is very high, $SP_{th} = 1$, the BS selects the highest modulation scheme, this scenario can be considered 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.

To show the impact of the number of users and number of BS antennas on the ergodic secrecy sum-rate, in Fig. 6 we present the ergodic secrecy sum-rate for the CI and ZF precoding techniques, when $N = K = 3$. Fig. 6a, shows the ergodic secrecy sum-rate for CI and ZF with different fixed modulation schemes, while Fig. 6b shows the secrecy sum-rate of AM for CI versus the transmit SNR for different values of the target SEP, $SP_{th} = 1$ and 10^{-6}. Comparing the results in Fig. 6 with the results in Fig. 5, it is evident that increasing number of BS antennas N and/or number of users K lead to enhance the secrecy sum-rate. In addition, the CI precoding can provide additional up to 10dB



(a) Exact IP versus transmit SNR, for fixed and adaptive modulations when $N = K = 2$ and $\mathcal{P} = 10^{-6}, 1$.



(b) Exact IP versus transmit SNR, for fixed and adaptive modulations when $K = N = 3$ and $\mathcal{P} = 10^{-6}, 1$.

Figure 7: Exact IP versus transmit SNR.

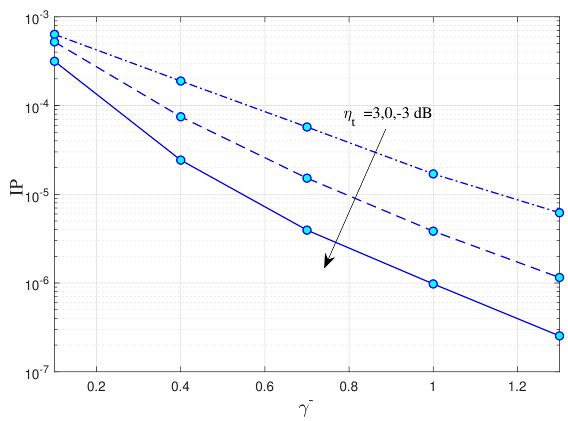


Figure 8: The IP based on the SINRs for the kth user versus $\bar{\gamma}$ for different values of the transmit SNR, when $N = K = 3$.

gain in η_t compared to ZF scheme.

In Fig. 7, we present the exact IP with respect to the transmit SNR, η_t, for fixed and adaptive modulation schemes. Fig. 7a, shows the exact IP when $N = K = 2$, while Fig. 7b, shows the exact IP when $N = K = 3$ for different values of the target SEP $\mathcal{P} = 10^{-6}, 1$. From these results it can be observed that, the IP for CI and ZF precoding techniques are severely degraded with increasing the transmit SNR in high-SNR regime. This is because the IP depends on the achievable rates at the user and the eavesdropper, which are saturated at, $\log_2 M$, in high-SNR regime, hence IP tends to one. In addition, the IP achieved by the CI precoding is always lower than that achieved by ZF scheme. Considering the IP achieved using AM scheme, when the target SEP is very high, $\mathcal{P} = 1$, the BS selects the highest modulation scheme, whilst in case the target SEP is very low, $\mathcal{P} = 10^{-6}$, the BS selects the modulation scheme with lower SEP when the IP of this scheme is in the decreasing region. Comparing Figs. 7a and 7b, it is clear that increasing the size of MU-MISO system results in enhancing the IP, and the CI precoding offers additional up to 13dB gain in η_t compared to ZF scheme.

Finally, in Fig. 2 we plot the IP based on the SINRs for different values of the transmit SNR, η_t, when $N = K = 3$. It is evident that, the analytical and simulation results are in well agreement, which confirms the simple expression presented in Section (V). In addition, the IP reduces with increasing the transmit SNR, and the threshold value of the received SINRs $\bar{\gamma}$.

VII. Conclusions

In this paper we investigated the secrecy performance of CI precoding in MU-MISO systems in the presence of multiple passive eavesdroppers. Firstly, new exact and approximate analytical expressions for the average 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. Finally, simple analytical expressions of the IP with fixed and adaptive modulations were derived. The results in this paper explained that, the CI precoding can achieve a considerable performance gain over interference suppression, ZF, technique. In addition, increasing number of users and BS antennas can enhance the system security, and the proposed AM scheme achieves significant performance improvement in terms of the secrecy sum-rate and the intercept probability.

References

[1] M. S. John G. Proakis, *Digital Communications, Fifth Edition*. McGraw-Hill, NY USA, 2008.

[2] C. B. P. Howard Huang and S. Venkatesan, *MIMO Communication for cellular Networks*. Springer, 2012, 2008.

[3] Y. Wu, C. Xiao, X. Gao, J. D. Matyjas, and Z. Ding, "Linear precoder design for mimo interference channels with finite-alphabet signaling," *IEEE Transactions on Communications*, vol. 61, no. 9, pp. 3766–3780, September 2013.

[4] H. Joudeh and B. Clerckx, "Robust transmission in downlink multiuser miso systems: A rate-splitting approach," *IEEE Transactions on Signal Processing*, vol. 64, no. 23, pp. 6227–6242, Dec 2016.

[5] 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.

[6] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Vector perturbation based on symbol scaling for limited feedback miso downlinks," *IEEE Transactions on Signal Processing*, vol. 62, no. 3, pp. 562–571, Feb 2014.

[7] 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.

[8] S. Timotheou, G. Zheng, C. Masouros, and I. Krikidis, “Exploiting constructive interference for simultaneous wireless information and power transfer in multiuser downlink systems,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1772–1784, May 2016.

[9] M. R. A. Khandaker, C. Masouros, and K. 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, Sept 2018.

[10] P. V. Amadori and C. Masouros, “Large scale antenna selection and precoding for interference exploitation,” *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4529–4542, Oct 2017.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] A. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[16] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[17] P. K. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[18] J. Li and A. P. Petropulu, “On ergodic secrecy rate for gaussian miso wiretap channels,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, April 2011.

[19] 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.

[20] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, “Secrecy sum rate optimization for downlink mimo nonorthogonal multiple access systems,” *IEEE Signal Processing Letters*, vol. 24, no. 8, pp. 1113–1117, Aug 2017.

[21] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, “Linear precoding for finite-alphabet signaling over mimome wiretap channels,” *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2599–2612, July 2012.

[22] S. Bashar, Z. Ding, and C. Xiao, “On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input,” *IEEE Communications Letters*, vol. 15, no. 5, pp. 527–529, May 2011.

[23] ——, “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.

[24] K. Cao, Y. Cai, Y. Wu, and W. Yang, “Secure transmission for misome wiretap channels with finite alphabet inputs,” *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 570–573, Aug 2018.

[25] 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.

[26] P. Zhao, M. Zhang, H. Yu, H. Luo, and W. Chen, "Robust beamforming design for sum secrecy rate optimization in mu-miso networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1812–1823, Sep. 2015.

[27] M. Zhang, M. Ding, L. Gui, H. Luo, and M. Bennis, "Sum secrecy rate maximization for relay-aided multiple-source multiple-destination networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4098–4109, May 2017.

[28] 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.

[29] R. J. Muirhead, *Aspects of Multivariate Statistical Theory*, 1982.

[30] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tabl*, Washington,D.C.: U.S. Dept. Commerce, 1972.

[31] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels*. John wiley and Sons, Inc., 2000.

[32] M. R. Mckay, A. Zanella, I. B. Collings, and M. Chiani, "Error probability and sinr analysis of optimum combining in rician fading," *IEEE Transactions on Communications*, vol. 57, no. 3, pp. 676–687, March 2009.

[33] M. Chiani, D. Dardari, and M. K. Simon, "New exponential bounds and approximations for the computation of error probability in fading channels," *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, pp. 840–845, July 2003.

[34] Y. Wu, C. Xiao, X. Gao, J. D. Matyjas, and Z. Ding, "Linear precoder design for mimo interference channels with finite-alphabet signaling," *IEEE Transactions on Communications*, vol. 61, no. 9, pp. 3766–3780, September 2013.

[35] 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.

[36] U. Fernandez-Plazaola, E. Martos-Naya, J. F. Paris, and A. J. Goldsmith, "Adaptive modulation for mimo systems with channel prediction errors," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2516–2527, August 2010.

[37] A. H. Bastami and A. Olfat, "Selection relaying schemes for cooperative wireless networks with adaptive modulation," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 4, pp. 1539–1558, May 2011.

[38] M. Z. Hassan, M. J. Hossain, and J. Cheng, "Performance of non-adaptive and adaptive subcarrier intensity modulations in gamma-gamma turbulence," *IEEE Transactions on Communications*, vol. 61, no. 7, pp. 2946–2957, July 2013.

[39] C. Kim, S. Lee, and J. Lee, "Sinr and throughput analysis for random beamforming systems with adaptive modulation," *IEEE Transactions on Wireless Communications*, vol. 12, no. 4, pp. 1460–1471, April 2013.

[40] H. David., *Order Statistics*, 1970:John Wiley and Sons.

[41] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, October 2013.

[42] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1319–1329, Feb 2017.