Secure Rate Splitting Multiple Access: How Much of the Split Signal to Reveal?

Abdelhamid Salem, *Member, IEEE*, Christos Masouros, *Senior Member, IEEE*, and Bruno Clerckx, *Fellow, IEEE*

***Abstract*—Rate Splitting Multiple Access (RSMA) relies on multi-antenna rate splitting (RS) at the transmitter and successive interference cancellation (SIC) at the receiver. In RS the users' messages are split into a common message and private messages, where the common part is first decoded by the all users, while the private part is decoded only by the intended user using SIC technique. This split of the users' signals into common and private parts raises some interesting tradeoffs between maximizing sum rate versus secrecy rate. In this work we consider the secrecy performance of RSMA in multi-user multiple-input single-output (MU-MISO) systems, where secrecy is defined by the ability of any user to decode the signal intended for user k in the system. To that end, new analytical expressions for the ergodic sum-rate and ergodic secrecy rate are derived for two closed-form precoding techniques of the private messages, namely, 1) zero-forcing (ZF) precoding approach, 2) minimum mean square error (MMSE) approach. Then, based on the analytical expressions of the ergodic rates, novel power allocation strategies that maximize the sum-rate subject to a target secrecy rate for the two precoding schemes are presented and investigated. Our Monte Carlo simulations show a close match with our theoretical derivations. They also reveal that, by tuning the split of the messages, our power allocation approaches provide a scalable tradeoff between rate benefits and secrecy.**

***Index Terms*—Rate splitting, physical layer security, zero forcing, MMSE, power allocation.**

I. Introduction

Rate-Splitting Multiple Access (RSMA) to a general and emerging framework of multiple access, multi-user and interference management strategies relying on multi-antenna rate splitting (RS) techniques at the transmitter and Successive Interference Cancellation (SIC) at the receivers [1]. Under the RSMA umbrella, various RS architectures have been developed and have been shown to enhance the achievable sum-rate in multi-user multiple-input single-output (MU-MISO) systems [2]–[6]. With RS the users' messages are split into a common message and private messages, that are first encoded, linear precoded, and then superimposed in a common transmission. At the users side, the common stream is first decoded by the all users, then each private stream is decoded by the intended user using Successive Interference Cancellation (SIC) technique. By modifying the power allocated to the common and private streams, RS can enhance the sum rate of the communication systems in the presence of interference. RS technique has received a growing attention in the literature. For instance, in [4] the gain performed by RS over conventional multi-user linear precoding transmission scheme, e.g., without using RS (NoRS), under imperfect channel state information (CSI) at the base-station (BS) has been analyzed and investigated. Considering imperfect CSI at the BS, the authors in [3]–[6] formulated an optimization problem to optimize the precoders of the common and private streams in order to maximize the achievable sum rate. The results in these works explained the superiority of RS over classical transmission (NoRS). In [7], RS technique in massive multiple-input multiple-output (MIMO) systems has been investigated assuming imperfect CSI at the BS. In [6], RS has been implemented in a multi-pair MIMO cooperative systems to get higher performance compared to NoRS. In [8], RS has been designed for a multiple antennas multi-cell systems with imperfect CSI, in this work RS scheme showed the

Abdelhamid Salem and Christos Masouros are with the department of Electronic and Electrical Engineering, University College London, London, UK, (emails: {a.salem, c.masouros}@ucl.ac.uk). B. Clerckx is with the Electrical and Electronic Engineering Department, Imperial College London, London SW7 2AZ, U.K. (e-mail: b.clerckx@imperial.ac.uk).

superiority in a Degrees-of-Freedom sense over NoRS. The benefits of RS in multi-user multi-antenna systems have been included in [9], [10], and its performance gains were highlighted over both the conventional NoRS and Non-Orthogonal Multiple Access (NOMA) techniques. More recently, the performance of RS with practical finite constellation transmission was investigated, along with tailored power allocation schemes [11].

A critical challenge that arises with RS relates to the security of the signaling. The split of the users' messages into common and private parts makes them prone to eavesdropping, because the common stream rate is designed to be decodable to multiple users. No splitting the messages as in SDMA incurs a loss in sum-rate but is more robust to eavesdropping. On the other hand, encoding a message entirely into a common stream so that one user entirely decodes the message of another user (as in NOMA) cannot satisfy any secrecy constraints. By suitably splitting the messages, one can find the best tradeoff between sum-rate and secrecy maximization.. This implicates vulnerabilities with the security of the information, not only to external eavesdroppers, but also relating to privacy of the messages between the legitimate users of the RS multiple-access system. As a complement to higher layer cryptographic approaches, physical layer security (PHYSec) has been long developed in the literature. The concept of PHY-Sec was first introduced in [12], which showed that a secure communication can be achieved if the eavesdropper channel is a degraded version of the legitimate user channel. Consequently, several works have investigated PHYSec in different scenarios. For instance, the secrecy capacity of MIMO systems with an external eavesdropper was studied in [13]. Later on, in [14], an optimization problem was formulated to solve the secrecy capacity of a general MIMO scenario in the existence of a passive eavesdropper. The authors of [15] showed that antenna selection and combining techniques enhance the secrecy over MIMO channels. In [16], the ergodic secrecy rate of a downlink MU-MISO system achieved by implementing the regularized zero-forcing (ZF) precoding based on imperfect CSI was derived and investigated. In [17], closed-form expression of the ergodic secrecy sum-rate of downlink MU-MISO systems was derived in terms of channel condition. The authors in [18] considered PHYSec of MIMO systems, where the achievable secrecy sum-rate was derived. In addition, in [19] the secrecy performance of constructive exploitation precoding technique was investigated. In addition, the authors in [20] provided an analytical framework for the secrecy performance and optimum design of secure transmission in down-link MU-MISO random cellular systems considering limited CSI feedback. A novel scheme for inducing inter symbol interference at the eavesdropper was proposed and analyzed in [21]. Further work in [22] presented a novel spatial constellation design strategy based on generalized space shift keying, for PHYSec improvements in MU-MIMO communication systems. In [23] a new secure transmission strategy, which jointly applies generalized precoding-aided spatial modulation and rotating symbol modulation for improving PHY-Sec was proposed. The authors in [24] studied a PHYSec aided wireless interference system of multiple source-user pairs, which are wiretapped by multiple eavesdroppers that have better channel conditions than the legitimate users. In [25] a multiple antennas-based truncated channel inversion power control scheme was proposed to provide secure transmission.

The secrecy problem of RS has been studied in the literature. In [26] cooperative RS technique has been employed to improve the secrecy sum rate for the MISO broadcast channel which consists of two legitimate users and an eavesdropper. To ensure secure cooperative RS transmission, the common message has been used as both a desired message and artificial noise. The authors in this work proposed secure RS transmission scheme which advocates the dual use of the common message as a desired message and artificial noise. In [27] the max-min secrecy fairness of cellular networks was investigated, in which cooperative RS aided down-link transmissions are employed. A novel application of RSMA for joint communications and jamming with a Multi-Carrier waveform in a multi-antenna Cognitive Radio was proposed in [28]. The authors in [29] proposed a RS scheme to enhance the security, in which

the common message serving both as a desired message for legitimate users and artificial noise for the eavesdropper. The work in [30] proposed a RS-based secure transmit approach against multiple eavesdroppers in cache-enabled cloud radio access networks. In [31] a secure beamforming scheme for RSMA-based cognitive satellite terrestrial networks in the presence of multiple eavesdroppers has been presented.

It is important to note however that classical PHYSec approaches do not straightforwardly apply to RS. They typically address external eavesdroppers to the legitimate transmission. Indeed, in the RS case, revealing a portion of the users' signals in the split RS signaling raises unique security challenges, not only against external eavesdroppers, but also for potential eavesdropping within the multiple access network. The eavesdropper can detect first the common message and then his own private message using a first layer of SIC. It then tries to remove them using a second layer of SIC to eavesdrop the k^{th} private signal (unintended private signal).[1]. It further raises some interesting tradeoffs, where on one hand, increasing the split towards the common signals may increase the sum rate of RS, while on the other hand revealing the users' signals may harm the security performance. Accordingly this paper investigates the secrecy performance of RS scheme in MU-MISO systems. In this regard, using maximum ratio transmission (MRT) technique for the common message, the ergodic sum-rate and ergodic secrecy rate are analyzed for two closed-form precoding schemes of the private messages, namely, 1) zero forcing (ZF) precoding technique, and 2) minimum mean square error (MMSE) technique. Our analysis is presented for imperfect CSI at the BS. Additionally, since RS subsumes NoRS as a special case whenever no power is allocated to the common stream, the conventional transmission NoRS is also studied in this paper. Furthermore, splitting the users' signals into common and private parts enhances the achievable sum-rate, but reveals part of the users' messages making them prone to eavesdropping. Accordingly, using the above analysis, a power allocation scheme tailored for secure RS that maximizes the sum-rate subject to a target secrecy rate is proposed and investigated. By tuning the secrecy threshold, one can achieve a flexible tradeoff between the RS benefits and its security vulnerability. For clarity the major contributions of this work are:

1) We investigate the tradeoff between the achievable sum-rate and secrecy rate in RS scheme, and we formulate an analytical framework to determine how the messages should be split between the common and private parts to achieve both high sum-rate and secrecy rate. Split of the users' messages raises some tradeoffs between the sum rate and secrecy rate. On one hand, increasing the split towards the common message (with increasing the power of the common message) can lead to enhancing the sum rate, while on the other hand revealing the users' signals (by increasing the split towards the common message) results in degrading the secrecy rate. Thus the power should be allocated efficiently to split the signals between the private and common messages in order to maximize the sum-rate while achieving a target secrecy rate. The trade-off between the two is unaddressed in the literature, and we address this gap with the following analytical study.

2) New closed-form explicit analytical expressions for the ergodic sum-rate and ergodic secrecy rate are derived for MRT/ZF and MRT/MMSE transmission schemes with RS, when the CSI is imperfectly known at the BS. The derived rate expressions provide practical design insights into the impact of different system parameters on the achievable rates and secrecy performance. Based on these explicit expressions several techniques such as power allocation approaches can be developed in order to enhance the system performance. In addition, with these analytical expressions it takes much less time to evaluate the ergodic sum-rate and secrecy rate than it would take to carry out Monte-Carlo simulations.

3) Based on the derived expressions, a novel low-complexity power allocation technique to scale the split between the private and common parts is considered for the sake of maximizing the ergodic sum-rate while achieving a target secrecy rate. The proposed power allocation essentially answers the question: 'How much of the users'

[1]This is very common in communication, e.g., superposition coding with SIC (nowadays known as NOMA) where the strong user decodes the message of the weak user.

signal to reveal?' for the purpose of increasing the sum rates while at the same time preserving the users' signals secrecy.

4) Monte-Carlo simulations are also provided to confirm the accuracy of the analysis, then we examine and investigate the impact of several system parameters on the achievable rates. The numerical results show clearly that the ergodic sum-rates and secrecy rates enhance with increasing the transmit power and number of antennas at the BS, and MRT/MMSE precoding scheme has better RS secrecy performance than MRT/ZF precoding technique. In addition, the proposed power allocation schemes can provide a scalable tradeoff between the achievable sum-rate benefits and the secrecy of RS transmission technique.

II. System Model

We consider a downlink MU-MISO system, in which an $N-$antennas BS communicates with K-single antenna users using RS technique. The channels are modeled as independent identically distributed (i.i.d) Rayleigh fading channels [32], [33]. The channel matrix between the BS and the users is denoted by $\mathbf{H} \in \mathbb{C}^{K\times N}$. Building on the channel reciprocity in a time division duplex (TDD) protocol it is assumed that the channel responses are the same for both uplink and downlink. At the beginning of every coherence interval, all the users simultaneously transmit orthogonal pilot sequences to the BS. Considering minimum mean square error (MMSE) channel estimator, the relation between the real and estimated channels can be written as, $\mathrm{H} = \hat{\mathrm{H}} + \tilde{\mathbf{H}}$, where $\hat{\mathrm{H}} \sim \mathcal{CN}\left(0,\hat{\boldsymbol{D}}\right)$ is the estimated channel matrix, and $\tilde{\mathbf{H}} \sim \mathcal{CN}\left(0,\tilde{\mathbf{D}}\right)$ is the estimation error matrix, while $\tilde{\mathbf{D}}$ and $\hat{\boldsymbol{D}}$ are a diagonal matrices with $\left[\tilde{\mathbf{D}}\right]_{kk} = \sigma^2_{\tilde{\mathbf{h}}_k}$ and $\left[\hat{\boldsymbol{D}}\right]_{kk} = \sigma^2_{\hat{\mathbf{h}}_k}$, which are the variances of the error and estimated channel, respectively[2] [5], [35], [36].

In RS, the BS transmits K independent messages to the K users. Each user message is split into a private part and a common part, i.e., $x_{t,k} = \{x_{c,k}, x_k\}$[3]. The common message is formed by packing the common parts, e.g., $x_c = \{x_{c,1}, ..., x_{c,K}\}$ [4]. The resulting $K+1$ symbols of a given channel use are grouped in a vector $\mathbf{x} = [x_c, x_1, ..., x_K]^T \in \mathbb{C}^{K+1}$, where x_c and x_k are encoded common and private symbols, respectively, and $\mathcal{E}\left\{\mathbf{x}\mathbf{x}^H\right\} = \mathrm{I}$. Then the symbols are mapped to the BS antennas through a linear precoding matrix defined as $\mathbf{W} = [\mathbf{w}_c, \mathbf{w}_1, ...\mathbf{w}_K]$ where $\mathbf{w}_c \in \mathbb{C}^N$ is the common unit norm precoder and $\mathbf{w}_k \in \mathbb{C}^N$ denotes the k^{th} private unit norm precoder. Accordingly, the transmitted signal can be written as [2]–[4]

$$\mathbf{s} = \mathbf{W}\mathbf{x} = \sqrt{P_c}\mathbf{w}_c x_c + \sum_{i=1}^{K} \sqrt{P_p}\mathbf{w}_i x_i, \qquad (1)$$

where P_c is the power allocated to the common message and P_p is the power allocated to the private message, where $P_c = (1-t)\,P$ and $P_p = \dfrac{tP}{K}$, $0 < t \leq 1$ and P is the total power.
The received signal at the k^{th} user can be expressed as

$$y_k = \mathbf{h}_k\mathbf{s} + n_k = \mathbf{h}_k\mathbf{W}\mathbf{x} + n_k$$

$$= \sqrt{P_c}\mathbf{h}_k\mathbf{w}_c x_c + \sum_{i=1}^{K} \sqrt{P_p}\mathbf{h}_k\mathbf{w}_i x_i + n_k, \qquad (2)$$

where $\mathbf{h}_k$ is the channel vector from the BS to the k^{th} user, n_k is the additive white Gaussian noise (AWGN) at the user with zero mean and variance σ_k^2, i.e., $n_k \sim \mathcal{CN}\left(0,\, \sigma_k^2\right)$. At the user side, after perfectly removing the common message using SIC technique, the received signal at the k^{th} user can be written as,

[2]Channel reciprocity is an inherit feature of TDD systems, which is used to know the uplink/downlink channel from downlink/uplink channel measurements. Both 802.16 m and LTE provide mechanisms to estimate the channel on different bandwidths depending on the terminal's channel conditions [34].

[3]The subscripts t and c are used for total message, and common part, respectively.

[4]It should be noted that while the RS transmit signal model resembles a broadcasting system with unicast (private) streams and a multicast stream, the role of the common message is fundamentally different. The common message in a unicast-multicast system carries the musticast information, i.e. a public information intended as a whole to all users in the system, while the common message in RS encapsulates parts of the unicast messages, and its content not necessarily required by all users, although decoded by them all for interference mitigation purposes. Please refer to literature [2], [9], [10], [37], [38] for more details about RS.

$$\begin{aligned} y_k^p &= \sum_{i=1}^{K} \sqrt{P_p}\mathbf{h}_k\mathbf{w}_i x_i + n_k \\ &= \mathbf{h}_k\mathbf{W}^p\mathbf{x}^p + n_k, \end{aligned} \tag{3}$$

where $\mathbf{x}^p = [x_1, ..., x_K]^T$ and $\mathbf{W}^p = [\mathbf{w}_1, ...\mathbf{w}_K]$. The sum rate can be calculated by,

$$R = R^c + \sum_{k=1}^{K} R_k^p, \tag{4}$$

where $R^c = \min\left(R_1^c, R_2^c, .., R_k^c, .., R_K^c\right)$ is the rate for the common part, R_k^c is the rate for the common part at the k^{th} user, and R_k^p is the rate for the private part at the k^{th} user.

In this work imperfect CSI is assumed, and delay-tolerant transmission is considered. Thus, sending the common massage and the k^{th} private message at ergodic rates given by $\mathbb{E}\left\{R_k^c\right\}$ and $\mathbb{E}\left\{R_k^p\right\}$, respectively, guarantees successful decoding by user k [6]. To guarantee that x_c is successfully decoded and then removed by the users, x_c should be transmitted at an ergodic rate not exceeding $\min_j \left(\mathbb{E}\left\{R_j^c\right\}\right)_{j=1}^K$. Accordingly, the ergodic sum rate can be evaluated by [6]

$$\mathbb{E}\left\{R\right\} = \min_j \left(\mathbb{E}\left\{R_j^c\right\}\right)_{j=1}^K + \sum_{k=1}^{K} \mathbb{E}\left\{R_k^p\right\}. \tag{5}$$

In addition to the above sum rates, in this work we are interested in the particular vulnerabilities of RS to eavesdropping. In this model the eavesdropper can be any user, i , in the system trying to decode the private message of user k by exploiting the common message together with the leakage caused by the imperfect knowledge of the CSI. Therefore, the ergodic secrecy rate can be defined as

$$\begin{aligned} R_s &= \mathbb{E}\left\{[(R^c + R_k^p) \right. \\ &- \left. \max\left\{\left(R^c + R_{i\to k}^p\right), 1 \le i \le K, i \ne k\right\}]^+\right\} \\ &= \mathbb{E}\left\{[R_k^p - \max\left\{R_{i\to k}^p, 1 \le i \le K, i \ne k\right\}]^+\right\} \end{aligned} \tag{6}$$

where $[x]^+ = \max(0,\, x)$, $R_{i\to k}^p$ is the rate at which user i can decode user k signal. It is evident from the above, that by tuning the power allocated to the common vs private signals, a flexible tradeoff between the sum rate and secrecy rate can be achieved. To analyze and optimize this tradeoff, let us first derive the analytical expressions of the sum and secrecy rates for a number of precoding approaches.

III. Ergodic Sum-Rate and Ergodic Secrecy-Rate

In this section we analyze the ergodic sum-rate and the ergodic secrecy rate of MU-MISO systems using RS scheme for different closed form precoding techniques: 1) MRT for the common part and ZF for the private parts, 2) MRT for the common part and MMSE for the private parts, assuming imperfect CSI at the BS.

A. MRT/ZF

In this case MRT is implemented for the common stream and ZF precoding is applied for the private stream. Thus, precoding vector for the common message can be written as

$$\mathbf{w}_c = \frac{\sum_{i=1}^{K} \hat{\mathbf{h}}_i^H}{\left\| \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H \right\|}. \tag{7}$$

The pseudo-inverse of the estimated channel is,

$$\mathbf{F}^p = \hat{\mathbf{H}}^H \left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}. \tag{8}$$

Therefore, the precoding vector for the k^{th}private message, $\mathbf{w}_k^p$, can be written as

$$\mathbf{w}_k^p = \frac{\mathbf{f}_k^p}{\|\mathbf{f}_k^p\|}, \tag{9}$$

where $\mathbf{f}_k^p$ is the k^{th} vector in $\mathbf{F}^p$.

1) Ergodic rate for the common part: To derive the ergodic rate of the common part, the received signal at user k in (2) can also be expressed as

$$y_k = \sqrt{P_c}\hat{\mathbf{h}}_k\mathbf{w}_c x_c + \sqrt{P_c}\tilde{\mathbf{h}}_k\mathbf{w}_c x_c$$

$$+\beta_{p_k}\sqrt{P_p}x_k^p + \sum_{i=1}^{K} \sqrt{P_p}\tilde{\mathbf{h}}_k\mathbf{w}_i^p x_i + n_k, \tag{10}$$

where $\beta_{p_k} = \frac{1}{\left\|\mathbf{f}_k^p\right\|}$. For a given channel estimate $\hat{\mathbf{H}}$, the corresponding output SINR of the common part at the k^{th} user is [39], [40]

$$\gamma_k^c = \frac{P_c \left| \frac{\hat{\mathbf{h}}_k \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H}{\left\| \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H \right\|} \right|^2 + P_c \sigma^2_{\tilde{\mathbf{h}}_k}}{\frac{P_p}{\left[\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}\right]_{k,k}} + P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}. \quad (11)$$

Thus, the ergodic rate for the common part is

$$\mathbb{E}\left[R_k^c\right] = \mathbb{E}\left[\log_2\left(1+\gamma_k^c\right)\right]. \quad (12)$$

Theorem 1. *The ergodic rate of the common part at user k can be calculated as a function of the common and private signal powers P_c, P_{p_k}as*

$$R_k^c = \frac{1}{\ln(2)} \sum_{i=1}^{n} H_i \frac{1}{z_i} \times \left(1 - \left(\left(1+\frac{P_c \theta_k \, z_i}{\beta}\right)^{-K}\right) e^{-z P_c \sigma^2_{\tilde{\mathbf{h}}_k}}\right) \times \left(\left(1+\frac{P_p \Psi_k \, z_i}{\beta}\right)^{-1+K-N}\right), \quad (13)$$

where $\beta = K P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2$, z_i and H_i are the i^{th} zero and the weighting factor, respectively, of the Laguerre polynomials tabulated in [41, (25.245)].

Proof: The proof is presented in Appendix A. ■

2) Ergodic rate for the private part : To derive the ergodic rate of the private message, the private signal at the k^{th} user in (3) can also be expressed as

$$y_k^p = \beta_{p_k}\sqrt{P_p} x_k + \sum_{i=1}^{K} \sqrt{P_p}\tilde{\mathbf{h}}_k \mathbf{w}_i^p x_i + n_k. \quad (14)$$

For a given channel estimate $\hat{\mathbf{H}}$, the corresponding output SINR of the k^{th} user is [39], [40]

$$\gamma_k^p = \frac{\frac{P_p}{\left[\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}\right]_{k,k}} + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\sum_{\substack{i=1 \\ i\neq k}}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}. \quad (15)$$

Now, the ergodic private-rate can be calculated as

$$\mathbb{E}\left[R_k^p\right] = \mathbb{E}\left[\log_2\left(1+\gamma_k^p\right)\right]. \quad (16)$$

Theorem 2. *The ergodic rate of the private part at user k can be evaluated by*

$$\mathbb{E}\left[R_k^p\right] = \sum_{i=1}^{n} H_i \frac{1}{z_i} \log_2\left(1 + \frac{P_p y_i + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\sum_{\substack{i=1 \\ i\neq k}}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_1} + \sigma_k^2}\right) \times \frac{y_i^{(N-K)} \left(\Psi_k\right)^{N-K+1} e^{-\Psi_k y_i}}{\Gamma\left(N-K+1\right)}, \quad (17)$$

where z_i and H_i are the i^{th} zero and the weighting factor, respectively, of the Laguerre polynomials tabulated in [41, (25.245)].

Proof: The proof is presented in Appendix B. ■

3) Ergodic secrecy rate: The ergodic secrecy rate lower bound can be calculated by [42, page 4692] [43, Eq(5)]

$$\mathbb{E}\left[R_s\right] = \left[\mathbb{E}\left[R_{\mathrm{k}}^p\right] - \mathbb{E}\left[\max\left\{R_{i\to k}^p\right\}\right]\right]^+. \quad (18)$$

User i detects first the common message and his own private message, then removes them using SIC to eavesdrop the k^{th} private signal. Accordingly, the received signal at user i to detect user k signal is

$$y_{i\to k}^p = \sqrt{P_p}\tilde{\mathbf{h}}_i \mathbf{w}_k^p x_k + \sum_{\substack{j=1 \\ j\neq i}}^{K} \sqrt{P_p}\tilde{\mathbf{h}}_i \mathbf{w}_j^p x_j + n_i. \quad (19)$$

Thus the SINR can be written as

$$\gamma_{i\to k}^p = \frac{P_p \sigma^2_{\tilde{\mathbf{h}}_i}}{\sum_{\substack{j=1 \\ j\neq i}}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_i} + \sigma_i^2}. \quad (20)$$

The ergodic rate at the worst user (for user k) can be evaluated by

$$\mathbb{E}\left[\max\left\{R_{i\to k}^p\right\}\right] = \mathbb{E}\left[\max\left\{\log_2\left(1+\gamma_{i\to k}^p\right)\right\}\right]. \quad (21)$$

Theorem 3. *The ergodic secrecy rate in this case can be calculated by*

$$\mathbb{E}\left[R_s\right] = \frac{1}{\ln\left(2\right)} \sum_{i=1}^{n} \frac{H_i}{z_i}$$

$$\times \left(1 - \left(e^{-z_i P \sigma^2_{\tilde{\mathbf{h}}_k}} \left(1 + P_p \Psi_k \, z_i\right)^{-1+K-N}\right)\right)$$

$$\times e^{z_i \left(1 - \left(\sum_{i=2}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma^2_k\right)\right)}$$

$$- \log_2 \left(1 + \max_i \frac{P_p \sigma^2_{\tilde{\mathbf{h}}_i}}{\sum_{\substack{j=1 \\ j \neq i}}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_i} + \sigma^2_i} \right). \tag{22}$$

Proof: The proof is presented in Appendix C. ■

B. MRT/MMSE

In this case MRT is implemented for the common part and MMSE precoding is applied for the private parts. Thus, the MMSE precoding vector for user k can be written as

$$\mathbf{w}_k^p = \beta_k \left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H + a\,\mathbf{I}_N\right)^{-1} \hat{\mathbf{h}}_k, \tag{23}$$

where $\beta_k = \frac{1}{\left\|\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H + a\,\mathbf{I}\right)^{-1}\hat{\mathbf{h}}_k\right\|}$ and $a = \frac{K\sigma^2}{P_p}$ is the the regularization parameter.

1) Ergodic rate for the common part : The received signal at user k can also be written as

$$y_k = \sqrt{P_c}\hat{\mathbf{h}}_k \mathbf{w}_c x_c + \sqrt{P_c}\tilde{\mathbf{h}}_k \mathbf{w}_c x_c$$

$$+ \sum_{i=1}^{K} \sqrt{P_p}\hat{\mathbf{h}}_k \mathbf{w}_i^p x_i^p + \sum_{i=1}^{K} \sqrt{P_p}\tilde{\mathbf{h}}_k \mathbf{w}_i^p x_i + n_k. \tag{24}$$

For a given channel estimate $\hat{\mathbf{H}}$, the corresponding output SINR of the common part at the k^{th} user is [39], [40]

$$\gamma_k^c = \frac{P_c \left|\hat{\mathbf{h}}_k \mathbf{w}_c\right|^2 + P_c \sigma^2_{\tilde{\mathbf{h}}_k} \left\|\mathbf{w}_c\right\|^2}{\sum_{i=1}^{K} P_p \left|\hat{\mathbf{h}}_k \mathbf{w}_i^p\right|^2 + \sum_{i=1}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_k} \left\|\mathbf{w}_i^p\right\|^2 + \sigma_k^2}. \tag{25}$$

For simplicity in this scenario, we derive the ergodic rate upper bound. Using Jensen inequality, the upper-bound for the common part is

$$\hat{R}_k^c = \log_2\left(1 + \mathbb{E}\left[\gamma_k^c\right]\right). \tag{26}$$

Theorem 4. *The ergodic rate of the common part upper-bound can be approximated by,*

$$\hat{R}_k^c \approx \log_2 \left(1 + \frac{P_c\, K\, \theta_k + P_c \sigma^2_{\tilde{\mathbf{h}}_k}}{P_p \alpha + P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right), \tag{27}$$

where

$$\alpha = \sum_{i=1}^{K} \frac{(i-1)!}{(i-1+N-K)!}$$

$$\sum_{z=0}^{i-1}\sum_{l=0}^{i-1} (-1)^{z+l} \binom{i-1+N-K}{i-1-z}$$

$$\times \binom{i-1+N-K}{i-1-l} \frac{1}{z!l!} J_{2+N-K+z-l,2,1}\left(a\right), \tag{28}$$

while

$$J_{2+N-K+z-l,,2,1}\left(a\right) = \sum_{f=0}^{2+N-K+z-l,}$$

$$\binom{2+N-K+z-l,}{f}$$

$$\times \left(-a\right)^{2+N-K+z-l,-f} e^a J\left(a\right), \tag{29}$$

and

$$J\left(a\right) = \begin{cases} -E_i\left(1,a\right) + \frac{e^{-a}}{a^2} & if\, f = 0 \\ E_i\left(1,a\right) & if\, f = 1 \\ \Gamma\left(f-1,a\right) & if\, f \geq 2 \end{cases} \tag{30}$$

where $E_i\left(1,a\right)$ is the generalized exponential integral and $\Gamma\left(f-1,a\right)$ is the incomplete gamma function.

Proof: The proof is presented in Appendix D. ■

2) Ergodic rate for the private part : The received private signal at the k^{th} user can also be written as

$$y_k^p = \sqrt{P_p}\hat{\mathbf{h}}_k\mathbf{w}_k^p x_k + \sqrt{P_p}\tilde{\mathbf{h}}_k\mathbf{w}_k^p x_k + \sum_{\substack{i=1\\i\neq k}}^{K}\sqrt{P_p}\hat{\mathbf{h}}_k\mathbf{w}_i^p x_i + \sum_{\substack{i=1\\i\neq k}}^{K}\sqrt{P_p}\tilde{\mathbf{h}}_k\mathbf{w}_i^p x_i + n_k. \tag{31}$$

For a given estimate channels $\hat{\mathbf{H}}$, the corresponding output SINR of the k^{th} user is [39], [40]

$$\gamma_k^p = \frac{P_p\left|\hat{\mathbf{h}}_k\mathbf{w}_k^p\right|^2 + P_p\sigma^2_{\tilde{\mathbf{h}}_k}}{\sum\limits_{\substack{i=1\\i\neq k}}^{K} P_p\left|\hat{\mathbf{h}}_k\mathbf{w}_i^p\right|^2 + \sum\limits_{\substack{i=1\\i\neq k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_k}\left\|\mathbf{w}_i^p\right\|^2 + \sigma_k^2}. \tag{32}$$

Theorem 5. *The upper-bound of the private part can be calculated by,*

$$\hat{R}_k^p = \log_2\left(1 + \frac{P_p\delta_k + P_p\sigma^2_{\tilde{\mathbf{h}}_k}}{P_p\left(\alpha-\delta_k\right) + \sum\limits_{\substack{i=1\\i\neq k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right). \tag{33}$$

where $\delta_k = \frac{1}{K(K+1)}\left\{S_k^2 + Q_k\right\}$, S_k^2 and Q_k are defined in Theorem 1 and Lemma 1 in [44], respectively.

Proof: The proof is presented in Appendix E. ∎

3) Ergodic secrecy rate: The ergodic secrecy rate lower bound in this case can be calculated by

$$\mathbb{E}\left[R_s\right] = \left[\mathbb{E}\left[R_{\mathrm{k}}^p\right] - \mathbb{E}\left[\max\left\{R_{i\to k}^p\right\}\right]\right]^+. \tag{34}$$

User i detects first the common and his private messages, then will remove them using SIC to detect the k^{th} private message. The received signal at user i to detect user k signal is

$$y_{i\to k}^p = \sqrt{P_p}\hat{\mathbf{h}}_i\mathbf{w}_k^p x_k + \sqrt{P_p}\tilde{\mathbf{h}}_i\mathbf{w}_k^p x_k + \sum_{\substack{j=1\\j\neq i,k}}^{K}\sqrt{P_p}\hat{\mathbf{h}}_i\mathbf{w}_j^p x_j + \sum_{\substack{j=1\\j\neq i,k}}^{K}\sqrt{P_p}\tilde{\mathbf{h}}_i\mathbf{w}_j^p x_j + n_i. \tag{35}$$

Thus the SINR is

$$\gamma_{i\to k}^p = \frac{P_p\frac{\left|\hat{\mathbf{h}}_i\mathbf{w}_k^p\right|^2}{\left\|\mathbf{w}_k^p\right\|^2} + P_p\sigma^2_{\tilde{\mathbf{h}}_i}}{\sum\limits_{\substack{j=1\\j\neq i,k}}^{K} P_p\frac{\left|\hat{\mathbf{h}}_i\mathbf{w}_j^p\right|^2}{\left\|\mathbf{w}_j^p\right\|^2} + \sum\limits_{\substack{j=1\\j\neq i,k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_i} + \sigma_i^2}. \tag{36}$$

Theorem 6. *The ergodic secrecy rate in this case can be calculated by*

$$\mathbb{E}\left[R_s\right] = \log_2\left(1 + \frac{P_p\delta_k + P_p\sigma^2_{\tilde{\mathbf{h}}_k}}{P_p\left(\alpha-\delta_k\right) + \sum\limits_{\substack{i=1\\i\neq k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right) - \max_i \log_2\left(1 + \frac{P_p\sigma^2_{\hat{\mathbf{h}}_i} + P_p\sigma^2_{\tilde{\mathbf{h}}_i}}{P_p\Omega + \sum\limits_{\substack{j=1\\j\neq i,k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_i} + \sigma_i^2}\right). \tag{37}$$

Proof: The proof is presented in Appendix F. ∎

Remark 7. From the sum-rate and secrecy rate expressions derived in this section, we can observe the following. Firstly, it is obvious that the channel estimation error has a harmful impact on the achievable sum and secrecy rates of the considered precoding schemes. Actually, the ergodic rates are limited by the variances of the estimated channels, and the estimation errors. Moreover, from these expressions we can also notice that, the power fraction, t, between the private and the common parts plays an important rule in achieving high sum and secrecy rates. Accordingly, the optimal value of t that achieves optimal system performance should be obtained for each values of the system parameters. It is also clear that, increasing number of the BS antennas N and number of the

users K always lead to enhance the achievable rates. It is also worth to mention that, all the analytical expressions provided in this work are accurate, explicit and in closed-form, thus effective power allocation techniques can be developed based on these expressions.

IV. Power Allocation for Secure RS

Splitting the users' messages into a common message and private messages raises some tradeoffs between the sum rate and secrecy rate as we have explained earlier. Increasing the power of the common message can lead to enhancing the sum rate, while revealing the users' signals results in degrading the secrecy rate. Therefore, the power should be allocated efficiently between the private and common messages in order to maximize the sum-rate while achieving a target secrecy rate. In this section, based on the ergodic sum-rate and ergodic secrecy rate expressions, power allocation schemes are considered to split the signals between the private and common messages in order to maximize the ergodic sum-rate while achieving a target secrecy rate. With the above objective in mind, we formulate the optimization problem as

$$\max_{0<t\leq 1} \mathbb{E}\left\{R_c\right\} + \sum_{k=1}^{K} \left(\mathbb{E}\left\{R_k^p\right\}\right)$$

$$\text{s.t. } \left[\mathbb{E}\left[R_{\mathrm{k}}^p\right] - \mathbb{E}\left[\max\left\{R_{i\to k}^p\right\}\right]\right]^+ > r_s, \forall_{i,k}$$

$$P_c + KP_p \leq P \tag{38}$$

where r_s is secrecy rate threshold value, $P_c = (1-t)\,P$ and $P_p = \dfrac{tP}{K}$, $0 < t \leq 1$ and P is the total power. We propose a low complexity heuristic approach to solve this problem by first finding the value (t_s) of t that achieves the target secrecy rate, r_s. Clearly, any value above t_s will satisfy the secrecy constraint. Then the optimal value of t will be in the region $[t_s, 1]$, as illustrated in Fig. 1 below.

A. MRT/ZF

In this case the value of t_s is the value that can fulfill the secrecy constraint in (38). This value can be obtained numerically by changing t from 0 to 1. To gain some insights, we can derive the approximated value of t_s as follows. Using the first order Laguerre polynomial, the secrecy constrain in (38) holds when

$$r_s = \Xi \log_2\left(1 + \frac{tPy_1 + tP\sigma^2_{\tilde{\mathbf{h}}_k}}{\sum\limits_{\substack{i=1\\ i\neq k}}^{K} tP\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right)$$

$$-\max_i \log_2\left(1 + \frac{tP\sigma^2_{\tilde{\mathbf{h}}_i}}{\sum\limits_{\substack{j=1\\ j\neq i}}^{K} tP\sigma^2_{\tilde{\mathbf{h}}_i} + \sigma_i^2}\right), \tag{39}$$

where $\Xi = \mathrm{H}_1 \frac{1}{y_1} \frac{y_1^{(N-K)} (\Psi_k)^{N-K+1} e^{-\Psi_k y_1}}{\Gamma(N-K+1)}$. The value of t_s can be calculated by

$$t_s = \frac{\left(2^{\varrho}-1\right)\left(\sigma_k^2\right)}{Py_1 + P\sigma^2_{\tilde{\mathbf{h}}_k} - \left(2^{\varrho}-1\right)(K-1)\,P\sigma^2_{\tilde{\mathbf{h}}_k}}. \tag{40}$$

The proof of (40) is provided in Appendix G.

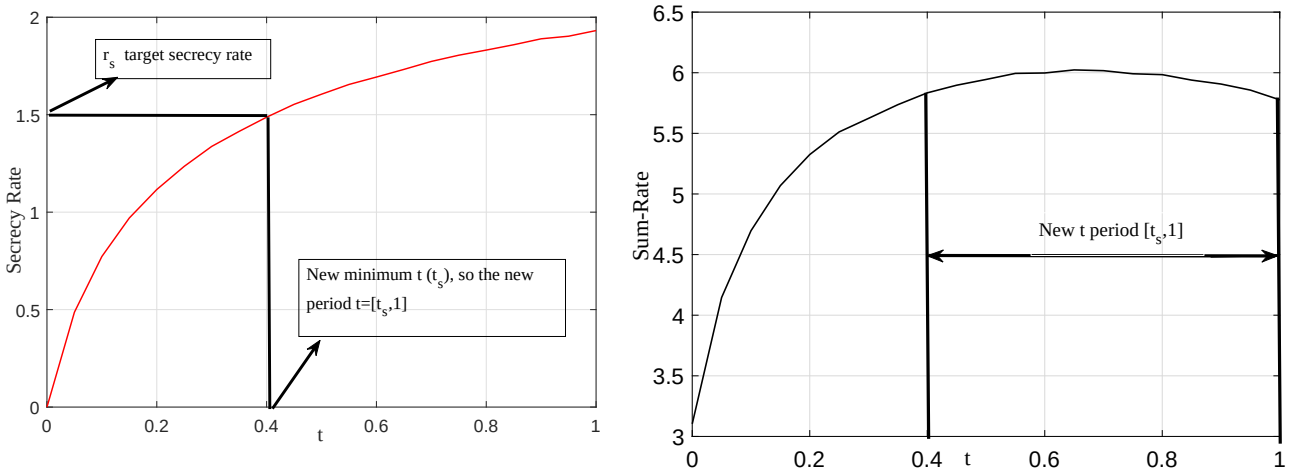
Now, the optimization problem can be written as,

$$\max_{t_s<t\leq 1} \mathbb{E}\left\{R_c\right\} + \sum_{k=1}^{K} \left(\mathbb{E}\left\{R_k^p\right\}\right)$$

$$\text{s.t. } P_c + KP_p \leq P \tag{41}$$

The optimal value of t can be found by a simple one dimensional search techniques, such as golden section method, over $t_s \leq t \leq 1$. The steps of golden section method are presented in Algorithm 1. It is known that, the golden section search converges to the global optimal point [45], [46]. Consequently, Algorithm 1 always converges to the optimal point [45], [46]. The complexity order of this algorithm for convergence to an ϵ-accurate solution is $\mathrm{O}\left(\log_2 \frac{1}{\epsilon}\right)$ [45], [46]. Number of iterations required in this method is $\log_2 \frac{1}{\epsilon}$ [45], [46].

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2022.3223961



(a) Ergodic secrecy rate versus t.

(b) Ergodic sum-rate versus t.

Figure 1: Power-Allocation scheme.

Algorithm 1 Golden Section Method.

Initialize $\vartheta = 0$, $\varphi = 1, \epsilon > 0$ and $\delta = \frac{-1+\sqrt{5}}{2}$.
Repeat
Update $t_1 = \vartheta + (1-\delta)\varphi$ and $t_2 = \varphi + (1-\delta)\vartheta$.
Obtain $\mathbb{E}\left[R\left(t_1\right)\right]$ and $\mathbb{E}\left[R\left(t_2\right)\right]$.
If $\mathbb{E}\left[R\left(t_1\right)\right] > \mathbb{E}\left[R\left(t_2\right)\right]$, set $\vartheta = t_1$. Else set $\varphi = t_2$.
Until $|\varphi - \vartheta| \leq \epsilon$.
Find $t^* = (\vartheta + \varphi)/2$.

B. MRT/MMSE

Similarly, the value of t_s in this case can be obtained numerically by changing t from 0 to 1. To gain some insights, we can derive the approximated value of t_s in the worst case as follows. The first constraint satisfied when,

$$r_s = \log_2\left(1 + \frac{P_p\delta_k + P_p\sigma^2_{\tilde{\mathbf{h}}_k}}{P_p\left(\alpha - \delta_k\right) + \sum\limits_{\substack{i=1\\ i\neq k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma^2_k}\right)$$

$$-\max_i \log_2\left(1 + \frac{P_p\sigma^2_{\tilde{\mathbf{h}}_i} + P_p\sigma^2_{\tilde{\mathbf{h}}_i}}{P_p\Omega + \sum\limits_{\substack{j=1\\ j\neq i,k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_i}}\right). \quad (42)$$

From (42) we can find t_s as

$$t_s = \frac{\Lambda\sigma^2_k}{P\delta_k + P\sigma^2_{\tilde{\mathbf{h}}_k} - \Lambda P\left(\alpha - \delta_k\right) - \Lambda\sum\limits_{\substack{i=1\\ i\neq k}}^{K} P\sigma^2_{\tilde{\mathbf{h}}_k}}. \quad (43)$$

The proof of (43) is provided in Appendix H. Now, the optimization problem can be reformulated as,

$$\max_{t_s<t\leq 1} \mathbb{E}\left\{R_c\right\} + \sum_{k=1}^{K}\left(\mathbb{E}\left\{R_k^p\right\}\right)$$

$$\text{s.t. } P_c + P_p \leq P \quad (44)$$

Now, the optimal value of t can be found by a simple one dimensional search techniques, such as golden section method, over $t_s \leq t \leq 1$ as presented in Algorithm 1.

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2022.3223961

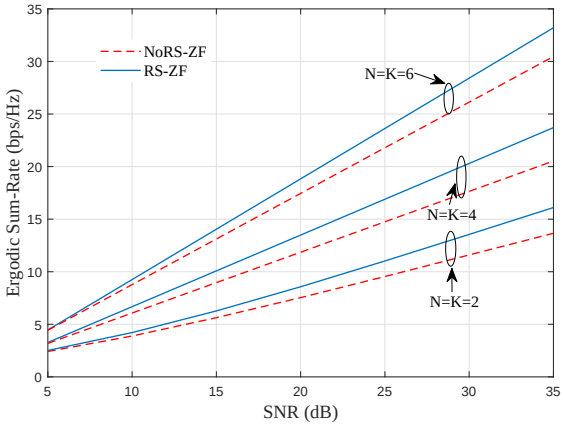


Figure 2: Ergodic sum-rate of RS and NoRS versus transmit SNR using ZF precoding for private stream with various values of N and K.

V. Numerical Results

In this section some numerical results of the mathematical expressions derived in this work are presented and investigated. To confirm our analysis, simulated results using Monte-Carlo simulation are also presented. Assuming the users have same noise power, σ^2, the transmit signal to noise ratio (SNR) is defined as SNR = $\frac{p}{\sigma^2}$. The channel error variance considered in this Section is given by, $\sigma^2_{\tilde{\mathbf{h}}_k} = \eta P^{-\zeta}$, where $\eta \geq 0$ and $\zeta \in [0, 1]$ are varied to represent different CSI accuracies and SNR scaling [6]. Accordingly, the CSI quality is allowed to be scaled with the SNR.

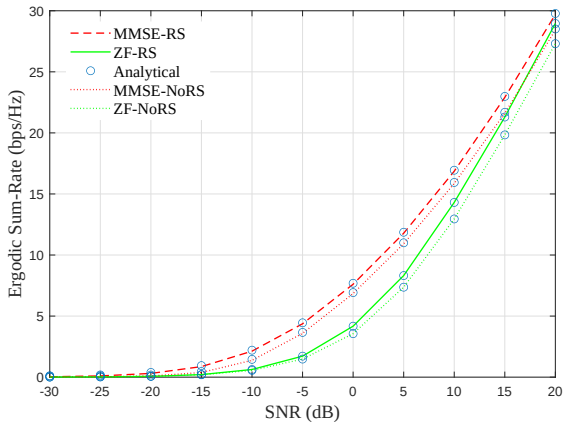
Firstly, in Fig. 2, we illustrate the ergodic sum-rate for the RS using MRT/ZF and NoRS using ZF when $N = K = 2, 4, 6$, $\eta = 1$ and $\zeta = 0.6$. It is clear from this figure that the RS scheme outperforms the conventional transmission NoRS for the all considered scenarios. These results explain clearly the superiority of RS over conventional transmission schemes and justify using RS transmission in MU-MISO systems.

In Fig. 3 we show the system performance under CSI errors that do not scale with SNR $(\zeta = 0)$, $\sigma^2_{\tilde{\mathbf{h}}_k} = 0.05$, when $N = K = 5$ for MMSE and ZF precoding schemes with RS and without applying RS when t is optimized using golden section technique. The good agreement between the analytical and simulated results confirms the validity of the analysis introduced in this paper. Looking closer at the results in this figure, it is clear that increasing the SNR enhances the ergodic sum-rate and secrecy rate. In addition, the MMSE and ZF precoding techniques can provide secure RS transmission, with clear superiority of MMSE over ZF. Having said this, increasing the SNR reduces the gap performance between the MMSE and ZF techniques. This figure confirms the superiority of RS over conventional transmission NoRS in terms of ergodic sum-rate and secrecy rate.

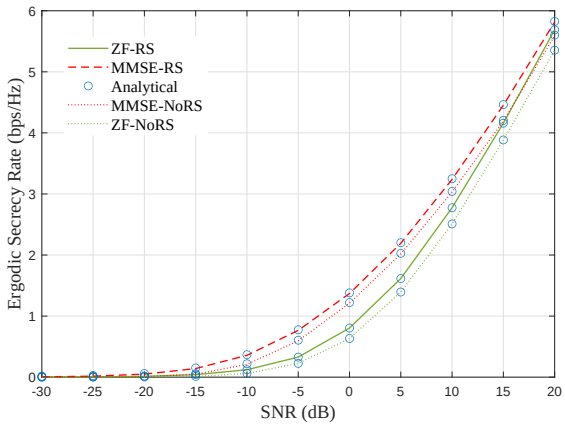
In Fig. 4 we plot the ergodic sum-rate and secrecy rate versus the SNR for the RS transmission scheme with MRT/MMSE and MRT/ZF when $N = K = 4$, and $N = 8, K = 4$ and t is optimized using line search methods such as golden section technique. Fig. 4a presents the sum-rate and Fig. 4b shows the secrecy-rate, when $\eta = 0.1$ and $\zeta = 0.5$. The good match between the analytical and simulated results confirms the analysis presented in this paper. It is clear that increasing the SNR and number of antennas N always improves the ergodic sum-rate and secrecy rate. In addition, secure RS transmission can be provided by applying MMSE or ZF precoding techniques. Furthermore, increasing the SNR and/or number of antennas N reduces the gap performance between the MMSE and ZF techniques. By comparing Fig. 4 and Fig. 3 we can notice that the highest error variance results in very low ergodic sum and secrecy rates. In addition, the superiority of MMSE over ZF can be seen for wider range of the transmit SNR.

To explain the impact of the channel error variance., i.e., the values of η and ζ, we plot in Fig. 5 the ergodic sum-rate and secrecy rate versus the SNR for the RS transmission scheme with

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2022.3223961

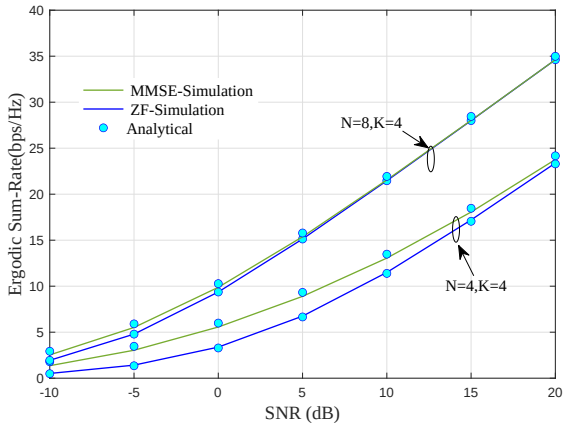


(a) Ergodic sum-rate of RS and NoRS versus transmit SNR using ZF and MMSE precoding schemes.

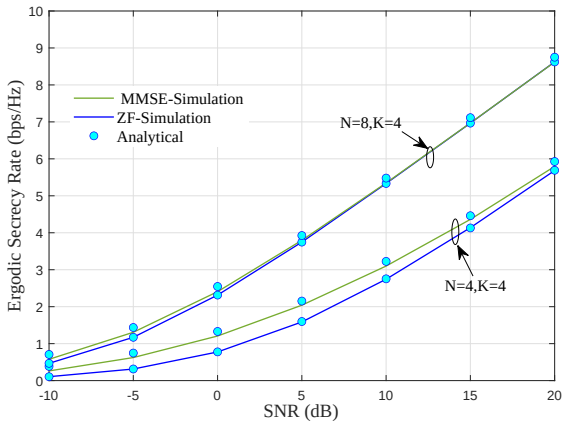


(b) Ergodic secrecy-rate of RS and NoRS versus transmit SNR using ZF and MMSE precoding schemes.

Figure 3: Ergodic sum-rate and secrecy rates of RS and NoRS versus transmit SNR using ZF and MMSE precoding for private streams with $N = K = 5$, $\eta = 0.05$ and $\zeta = 0$.



(a) Ergodic sum-rate of RS versus transmit SNR using ZF and MMSE precoding schemes.



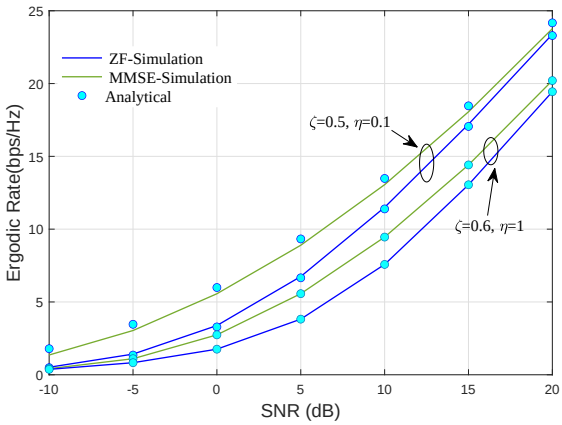
(b) Ergodic secrecy-rate of RS versus transmit SNR using ZF and MMSE precoding schemes.

Figure 4: Ergodic sum-rate and secrecy rates of RS versus transmit SNR using ZF and MMSE precoding for private streams with various values of N and K , when $\eta = 0.1$ and $\zeta = 0.5$.

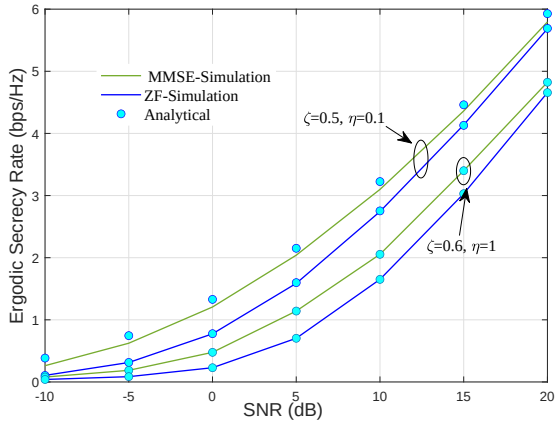
MRT/MMSE and MRT/ZF for different values of η and ζ when $N = K = 4$ and the power fraction t is optimized using golden section technique. It is evident and as expected that increasing η and ζ leads to increase the channel error variance $\sigma^2_{\tilde{\mathbf{h}}_k} = \eta P^{-\zeta}$ and this results in degrading the system performance.

In order to illustrate the power allocation scheme presented in this work, we plot in Fig. 6 the ergodic sum-rate and secrecy rate versus t for MMSE and ZF precoding techniques, when $N = K = 5$, SNR=5 dB and $\sigma^2_{\tilde{\mathbf{h}}_k} = 0.7$. The target secrecy rates are assumed to be $r_s = 0.41$ (bps/Hz) for ZF and $r_s = 0.72$ (bps/Hz) for MMSE as shown in Fig. 6a. Interestingly enough, it is noted from this figure that $t = 1$ is the best option for the secrecy, but for the sum-rate $t = 0.5$ is the best with MMSE and $t = 0.6$ is the best with ZF. This observation explains clearly the tradeoff between the secrecy rate and the achievable sum rates. The optimal value of t that can achieve the target secrecy rate r_s and optimize the sum-rate (t^*) is in the range $[0.7, 1]$ for MMSE and $[0.8, 1]$ for ZF scheme as explained in Fig.6b. By using Algorithm 1, the optimal value of t for MMSE scheme is $t^* = 0.7$ and for ZF is $t^* = 0.8$ as shown in Fig.6b. Therefore, the BS should allocate more power to the private messages in order to optimize

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2022.3223961

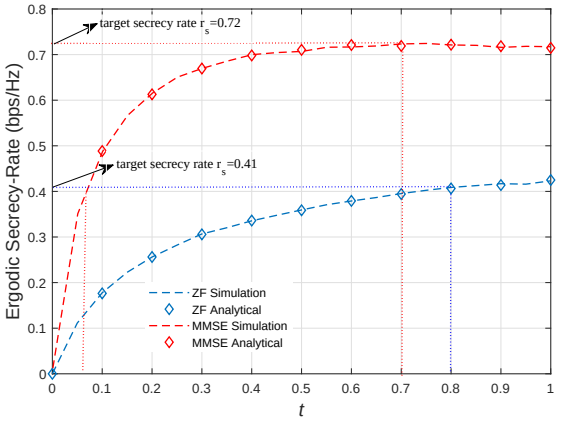


(a) Ergodic sum-rate of RS versus transmit SNR using ZF and MMSE precoding schemes.

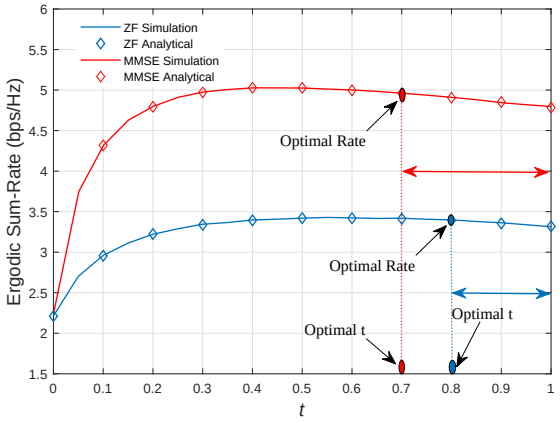


(b) Ergodic secrecy-rate of RS versus transmit SNR using ZF and MMSE precoding schemes.

Figure 5: Ergodic sum-rate and secrecy rates of RS versus transmit SNR using ZF and MMSE precoding for private streams with various values of η and ζ, when $N = K = 4$.



(a) Ergodic secrecy-rate versus t using ZF and MMSE schemes.



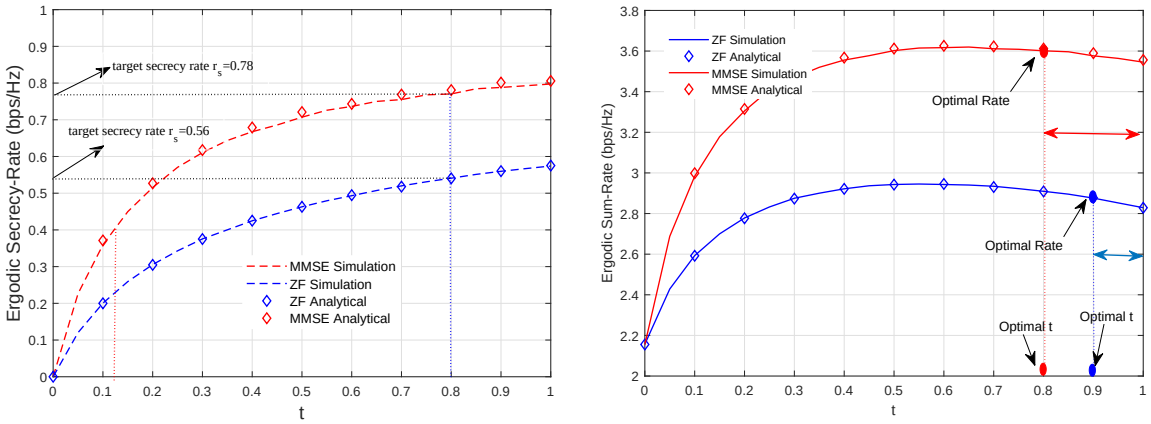
(b) Ergodic sum-rate versus t for ZF and MMSE schemes.

Figure 6: Ergodic sum-rate and secrecy rates of RS versus t using ZF and MMSE schemes for private streams with $N = K = 5$, $\eta = 0.7$ and $\zeta = 0$.

the sum rate and achieve the target secrecy rate. It is also clear that the secrecy constraint has considerable impact on the optimal value of t, where the optimal t without secrecy constraint in MMSE is about 0.5 and in ZF is about 0.6. Thus, in RS transmission without secrecy constraint, the BS allocates more power to the common part to achieve optimal sum-rate.

In order to investigate the impact of K and N on the optimal value of t, in Fig. 7 we plot the ergodic sum-rate and secrecy rate versus t for MMSE and ZF precoding techniques, when $N = K = 3$, SNR=5 dB, and $\sigma^2_{\mathbf{h}_k} = 0.7$ for the target secrecy rates $r_s = 0.56$ (bps/Hz) for ZF and $r_s = 0.78$ (bps/Hz) for MMSE. The tradeoff between the secrecy rate and the achievable sum rates can be observed clearly from the results in this figure where $t = 1$ is the best option for the secrecy rates, but for the sum-rate $t = 0.65$ is the best with MMSE and $t = 0.6$ is the best with ZF. The optimal value of t, is in the range $[0.8, 1]$ for MMSE and $[0.9, 1]$ for ZF scheme as shown in Fig.7b. By using Algorithm 1, the optimal value of t for MMSE is $t^* = 0.8$ and for ZF is $t^* = 0.9$ as in Fig.7b. Therefore, the BS should allocate most the power to the private messages in both MMSE and ZF cases. On the other hand, the optimal value of t without secrecy constraint in MMSE is about

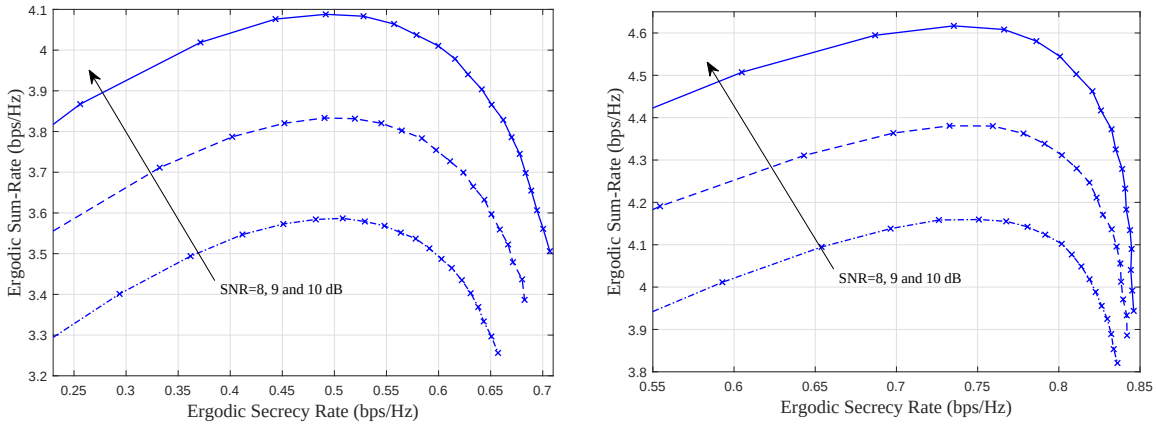
This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2022.3223961



(a) Ergodic secrecy-rate versus t using ZF and MMSE precoding schemes.

(b) Ergodic sum-rate versus t for ZF and MMSE precoding schemes.

Figure 7: Ergodic sum-rate and secrecy rates of RS versus t using ZF and MMSE schemes for private streams with $N = K = 3$, $\eta = 0.7$ and $\zeta = 0$.



(a) Ergodic sum-rate versus ergodic secrecy rate for ZF precoding scheme.

(b) Ergodic sum-rate versus ergodic secrecy rate for MMSE precoding scheme.

Figure 8: Ergodic sum-rate versus ergodic secrecy rate for ZF and MMSE precoding for private streams.

0.65 and in ZF is about 0.6. That means, without secrecy constraint the BS should allocate more power to the common part to achieve the optimal performance, and this explains clearly the impact of the secrecy constraint on the optimal value of t.

Finally, to explain the direct tradeoff between the sum rate and secrecy rate, in Fig. 8 we plot the sum rate versus secrecy rate for different values of t, when $N = K = 3$, SNR $= 8, 9$ and 10 dB, and $\sigma^2_{\tilde{\mathbf{h}}_k} = 0.7$. In Fig. 8a we present the sum rate versus secrecy rate for ZF precoding technique and in Fig. 8b we show the sum rate versus secrecy rate for MMSE precoding technique. From these results, it is apparent that there is an optimal value of the secrecy rate that maximizes the achievable sum rate. Therefore, the secrecy rate threshold value should be selected carefully in order to achieve higher sum-rate.

VI. Conclusions

In this paper the secrecy performance of RS scheme in MU-MISO systems was considered, in which the eavesdropper can be any user in the system. For this scenario, new analytical expressions for the ergodic sum-rate and secrecy rate have been derived for ZF and MMSE precoding techniques. Furthermore, a power allocation strategy that maximizes the sum-rate subject to a target

secrecy rate for the two precoding schemes was proposed and investigated. The results presented in this work demonstrated the inherent tradeoff between sum rate benefits and secrecy rates for RS, and provided a low complexity methodology for optimizing the split between common and private signaling to achieve this tradeoff.

APPENDIX A

The SINR of the common part at the k^{th} user in (11) can be written as

$$\gamma_k^c = \frac{P_c\, x + P_c \sigma^2_{\tilde{\mathbf{h}}_k}}{P_{p_k} y + P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}, \tag{45}$$

where $x = \left| \frac{\hat{\mathbf{h}}_k \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H}{\left\| \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H \right\|} \right|^2$ and $y = \frac{1}{\left[\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}\right]_{k,k}}$. Thus, the ergodic rate for the common part is $\mathbb{E}\left[R_k^c\right] = \mathbb{E}\left[\log_2\left(1+\gamma_k^c\right)\right]$. It is found in [47] that for any random variables $x, y > 0$

$$\mathbb{E}\left[\ln\left(1+\frac{x}{y}\right)\right] = \int_0^\infty \frac{1}{z}\left(\mathcal{M}_y\left(z\right) - \mathcal{M}_{y,x}\left(z\right)\right) dz, \tag{46}$$

where $\mathcal{M}_x\left(z\right) = \mathbb{E}\left[e^{-zx}\right]$ denotes the moment generating function (MGF) of x and $\mathcal{M}_{v,u}\left(z\right) = \mathbb{E}\left[e^{-z(v+u)}\right]$. Accordingly, (45) can be expressed as $\gamma_k^c = \frac{u}{v+\beta}$ where $u = P_c\, x + P_c \sigma^2_{\tilde{\mathbf{h}}_k}$, $v = P_{p_k} y$, and $\beta = P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2$. Now, from (46) the ergodic rate of the common part at user k can be calculated by

$$R_k^c = \frac{1}{\ln\left(2\right)} \int_0^\infty \frac{1}{z}\left(1 - \mathcal{M}_u\left(z\right) e^{-zP_c\sigma^2_{\tilde{\mathbf{h}}_k}}\right) \times \mathcal{M}_v\left(z\right) e^{-z\beta}\, dz, \tag{47}$$

Since u has gamma distribution, the MGF of u is

$$\mathcal{M}_u\left(z\right) = \left(1 + P_c \theta_k\, z\right)^{-K}. \tag{48}$$

The probability distribution function (PDF) of $y = \frac{1}{\left[\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}\right]_{k,k}}$ is $f_y\left(y\right) = \frac{y^{(N-K)}\left(\Psi_k\right)^{N-K+1} e^{-\Psi_k y}}{\Gamma(N-K+1)}$ where Ψ_k is the variance of the estimated channel. Then, the MGF of v can be calculated as

$$\mathcal{M}_v\left(z\right) = \left(1 + P_{p_k} \Psi_k\, z\right)^{-1+K-N}. \tag{49}$$

Substituting (48) and (49) into (47) we can find

$$R_k^c = \frac{1}{\ln\left(2\right)} \int_0^\infty \frac{1}{z}\left(1 - \left(\left(1 + P_c \theta_k\, z\right)^{-K}\right) e^{-zP_c\sigma^2_{\tilde{\mathbf{h}}_k}}\right) \times \left(\left(1 + P_{p_k} \Psi_k\, z\right)^{-1+K-N}\right) e^{-z\beta}\, dz. \tag{50}$$

By using Gaussian rules we can get the ergodic rate in Theorem 1.

APPENDIX B

The SINR of the private part at the k^{th} user in (15) can be expressed as

$$\gamma_k^p = \frac{P_P y + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\sum_{\substack{i=1 \\ i\neq k}}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}. \tag{51}$$

Now, the ergodic private-rate is given by $\mathbb{E}\left[R_k^p\right] = \mathbb{E}\left[\log_2\left(1+\gamma_k^p\right)\right]$ and

$$\mathbb{E}\left[R_k^p\right] = \int_0^\infty \log_2\left(1 + \frac{P_P y + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\sum_{\substack{i=1 \\ i\neq k}}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right) f_y\left(y\right) dy. \tag{52}$$

$$\mathbb{E}\left[R_k^p\right] = \int_0^\infty \log_2\left(1 + \frac{P_P y + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\sum_{\substack{i=1 \\ i\neq k}}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right) \times \frac{y^{(N-K)}\left(\Psi_k\right)^{N-K+1} e^{-\Psi_k y}}{\Gamma\left(N-K+1\right)} dy. \tag{53}$$

By using Gaussian rules we can find the expression in Theorem 2.

APPENDIX C

The ergodic secrecy rate can be calculated by

$$\mathbb{E}\left[R_s\right] = \left[\mathbb{E}\left[R_{\mathrm{k}}^{p}\right] - \mathbb{E}\left[\max\left\{R_{i\to k}^{p}\right\}\right]\right]^{+}, \quad (54)$$

where the ergodic rate at user k, $\mathbb{E}\left[R_{\mathrm{k}}^{p}\right]$, is derived in (17). The ergodic rate at the worst user, for user k, is calculated by

$$\mathbb{E}\left[\max\left\{R_{i\to k}^{p}\right\}\right] = \mathbb{E}\left[\max\left\{\log_2\left(1+\gamma_{i\to k}^{p}\right)\right\}\right]. \quad (55)$$

Substituting (20) into (55), the ergodic rate at the worst user, for user k, is

$$\mathbb{E}\left[\max\left\{R_{i\to k}^{p}\right\}\right] = \max_{i}\left\{\log_2\left(1+\frac{P_p\sigma^2_{\tilde{\mathbf{h}}_i}}{\sum\limits_{\substack{j=1\\ j\neq i}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_i}+\sigma_i^2}\right)\right\}. \quad (56)$$

Substituting (17) and (56) into (54), we can obtain the ergodic secrecy rate presented in Theorem 3.

APPENDIX D

The SINR in (25) can be written as

$$\gamma_k^c = \frac{P_c\, x + P_c\sigma^2_{\tilde{\mathbf{h}}_k}}{\sum\limits_{i=1}^{K} P_p y_i + P_p\sigma^2_{\tilde{\mathbf{h}}_k}+\sigma_k^2}, \quad (57)$$

where $x = \left|\frac{\hat{\mathbf{h}}_k\sum_{i=1}^{K}\hat{\mathbf{h}}_i^H}{\left\|\sum_{i=1}^{K}\hat{\mathbf{h}}_i^H\right\|}\right|^2$ and $y_i = \frac{\left|\hat{\mathbf{h}}_k\mathbf{w}_i^p\right|^2}{\left\|\mathbf{w}_i^p\right\|^2}$. The upper-bound can be derived by

$$\hat{R}_k^c \approx \log_2\left(1+\frac{P_c\,\mathbb{E}\left[x\right]+P_c\sigma^2_{\tilde{\mathbf{h}}_k}}{P_p\mathbb{E}\left[\sum\limits_{i=1}^{K} y_i\right]+P_p\sigma^2_{\tilde{\mathbf{h}}_k}+\sigma_k^2}\right). \quad (58)$$

Since x has gamma distribution, the expectation of x is $\mathbb{E}\left[x\right] = K\,\theta_k$. It has been shown in [44] that, $\mathbb{E}\left[\sum\limits_{i=1}^{K} y_i\right] = \alpha = \mathbb{E}_{\lambda_l}\left[\sum\limits_{l=1}^{K}\left(\frac{\lambda_l}{\lambda_l+a}\right)^2\right]$ where λ_l is the l^{th} eigenvalue of the matrix $\hat{\mathbf{H}}\hat{\mathbf{H}}^H$, this expectation has been presented in Theorem 1 in [44], which is given by

$$\alpha = \sum_{i=1}^{m}\frac{(i-1)!}{(i-1+n-m)!}$$
$$\sum_{z=0}^{i-1}\sum_{l=0}^{i-1}(-1)^{z+l}\binom{i-1+n-m}{i-1-z}$$
$$\times\binom{i-1+n-m}{i-1-l}\frac{1}{z!l!}J_{2+n-m+z-l,2,1}\left(a\right), \quad (59)$$

where $m = K$ and $n = N$.

For further discussion on the approximation used in (58), we refer the reader to Appendix I in [48].

APPENDIX E

The SINR in (32) can be written as,

$$\gamma_k^p = \frac{P_P\frac{\left|\hat{\mathbf{h}}_k\mathbf{w}_k^p\right|^2}{\left\|\mathbf{w}_k^p\right\|^2}+P_p\sigma^2_{\tilde{\mathbf{h}}_k}}{\sum\limits_{\substack{i=1\\ i\neq k}}^{K} P_P\frac{\left|\hat{\mathbf{h}}_k\mathbf{w}_i^p\right|^2}{\left\|\mathbf{w}_i^p\right\|^2}+\sum\limits_{\substack{i=1\\ i\neq k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_k}+\sigma_k^2}. \quad (60)$$

For simplicity in this scenario, we derive the ergodic rate upper bound. By using Jensen inequality, the upper bound for the private part is

$$\hat{R}_k^p = \log_2\left(1+\mathbb{E}\frac{P_p\frac{\left|\hat{\mathbf{h}}_k\mathbf{w}_k^p\right|^2}{\left\|\mathbf{w}_k^p\right\|^2}+P_p\sigma^2_{\tilde{\mathbf{h}}_k}}{\sum\limits_{\substack{i=1\\ i\neq k}}^{K} P_p\frac{\left|\hat{\mathbf{h}}_k\mathbf{w}_i^p\right|^2}{\left\|\mathbf{w}_i^p\right\|^2}+\sum\limits_{\substack{i=1\\ i\neq k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_k}+\sigma_k^2}\right). \quad (61)$$

$$\hat{R}_k^p = \log_2\left(1+\frac{P_p\mathbb{E}\left[x_k\right]+P_p\sigma^2_{\tilde{\mathbf{h}}_k}}{P_p\mathbb{E}\left[\sum\limits_{\substack{i=1\\ i\neq k}}^{K} y_i\right]+\sum\limits_{\substack{i=1\\ i\neq k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_k}+\sigma_k^2}\right), \quad (62)$$

where $\mathbb{E}\left[x_k\right] = \delta_k = \frac{1}{m(m+1)}\left\{S_k^2+Q_k\right\}$, $m = K$, S_k^2 and Q_k are defined in Theorem 1 and Lemma 1 in [44]. On the other hand,

$$R_{i\to k}^{\hat{p}} = \log_2\left(1+\mathbb{E}\left[\frac{P_p\frac{\left|\hat{\mathbf{h}}_i\mathbf{w}_k^p\right|^2}{\left\|\mathbf{w}_k^p\right\|^2}+P_p\sigma_{\tilde{\mathbf{h}}_i}^2}{\sum\limits_{\substack{j=1\\j\neq i,k}}^{K}P_p\frac{\left|\hat{\mathbf{h}}_i\mathbf{w}_j^p\right|^2}{\left\|\mathbf{w}_j^p\right\|^2}+\sum\limits_{\substack{j=1\\j\neq i,k}}^{K}P_p\sigma_{\tilde{\mathbf{h}}_i}^2+\sigma_i^2}\right]\right) \tag{64}$$

$$= \log_2\left(1+\frac{P_p\mathbb{E}\left[x_i\right]+P_p\sigma_{\tilde{\mathbf{h}}_i}^2}{P_p\mathbb{E}\left[\sum\limits_{\substack{j=1\\j\neq i,k}}^{K}y_j\right]+\sum\limits_{\substack{j=1\\j\neq i,k}}^{K}P_p\sigma_{\tilde{\mathbf{h}}_i}^2+\sigma_i^2}\right), \tag{65}$$

$$\mathbb{E}\left[\max\left\{R_{i\to 1}^p\right\}\right] = \max_i\left\{\log_2\left(1+\frac{P_p\sigma_{\hat{\mathbf{h}}_i}^2+P_p\sigma_{\tilde{\mathbf{h}}_i}^2}{P_p\Omega+\sum\limits_{\substack{j=1\\j\neq i,k}}^{K}P_p\sigma_{\tilde{\mathbf{h}}_i}^2+\sigma_i^2}\right)\right\}. \tag{66}$$

APPENDIX F

$$\mathbb{E}\left[\sum_{\substack{i=1\\i\neq k}}^{K}y_i\right] = \Theta_i = \mathbb{E}\left[\left\{\sum_{i=1}^{K}y_i\right\}-x_x\right]$$

$$= \mathbb{E}\left[\sum_{i=1}^{K}y_i\right]-\mathbb{E}\left[x_x\right] = \alpha-\delta_k. \tag{63}$$

The ergodic secrecy rate can be calculated by $\mathbb{E}\left[R_s\right] = \left[\mathbb{E}\left[R_{\mathrm{k}}^p\right]-\mathbb{E}\left[\max\left\{R_{i\to k}^p\right\}\right]\right]^+$where the ergodic rate at user k, $\mathbb{E}\left[R_{\mathrm{k}}^p\right]$, is derived in (33). We derive the ergodic rate upper bound as $\mathbb{E}\left[\max\left\{R_{i\to k}^p\right\}\right] = \max\left\{\log_2\left(1+\mathbb{E}\left[\gamma_{i\to k}^p\right]\right)\right\}$. Using Jensen inequality, the upper-bound can be given by (64) and (65), where $\mathbb{E}\left[x_i\right] = \sigma_{\hat{\mathbf{h}}_i}$, and $\mathbb{E}\left[\sum\limits_{\substack{j=1\\j\neq i,k}}^{K}y_j\right] = \Omega = \mathbb{E}\left[\sum\limits_{\substack{j=1\\j\neq i,k}}^{K}y_j\right]-\sigma_{\hat{\mathbf{h}}_i}-\delta_k$. Thus, the upper-bound of the common part can be calculated by (66).

APPENDIX G

In the worst case scenario (39) can be written as

$$r_s = \Xi\log_2\left(1+\frac{tPy_1+tP\sigma_{\tilde{\mathbf{h}}_k}^2}{\sum\limits_{\substack{i=1\\i\neq k}}^{K}tP\sigma_{\tilde{\mathbf{h}}_k}^2+\sigma_k^2}\right)$$

$$-\max_i\log_2\left(1+\frac{tP\sigma_{\tilde{\mathbf{h}}_i}^2}{\sum\limits_{\substack{j=1\\j\neq i}}^{K}tP\sigma_{\tilde{\mathbf{h}}_i}^2}\right). \tag{67}$$

which can be expressed as

$$\varrho = \log_2\left(1+\frac{tPy_1+tP\sigma_{\tilde{\mathbf{h}}_k}^2}{\sum\limits_{\substack{i=1\\i\neq k}}^{K}tP\sigma_{\tilde{\mathbf{h}}_k}^2+\sigma_k^2}\right), \tag{68}$$

where $\varrho = \frac{1}{\Xi}\left(r_s + \log_2\left(1 + \max_i \frac{a_1\sigma^2_{\tilde{\mathbf{h}}_i}}{\sum_{\substack{j=1\\ j\neq i}}^{K} a_j\sigma^2_{\tilde{\mathbf{h}}_i}}\right)\right)$.

The expression in (68) can be written as,

$$(2^{\varrho}-1)\left(\sum_{\substack{i=1\\ i\neq k}}^{K} tP\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2\right) = tPy_1 + tP\sigma^2_{\tilde{\mathbf{h}}_k}. \tag{69}$$

and

$$(2^{\varrho}-1)\,\sigma_k^2 = t$$

$$\times\left(Py_1 + P\sigma^2_{\tilde{\mathbf{h}}_k} - (2^{\varrho}-1)\sum_{\substack{i=1\\ i\neq k}}^{K} P\sigma^2_{\tilde{\mathbf{h}}_k}\right). \tag{70}$$

which conclude the proof.

Appendix H

(42) can also be written as

$$r_s = \log_2\left(\frac{1 + \frac{P_p\delta_k + P_p\sigma^2_{\tilde{\mathbf{h}}_k}}{P_p(\alpha-\delta_k) + \sum_{\substack{i=1\\ i\neq k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}}{1 + \max_i \frac{P_p\sigma_{\hat{\mathbf{h}}_i} + P_p\sigma^2_{\tilde{\mathbf{h}}_i}}{P_p\Omega + \sum_{\substack{j=1\\ j\neq i,k}}^{K} P_p\sigma^2_{\tilde{\mathbf{h}}_i}}}\right), \tag{71}$$

$$2^{r_s}\left(1 + \max_i \frac{tP\sigma_{\hat{\mathbf{h}}_i} + tP\sigma^2_{\tilde{\mathbf{h}}_i}}{tP\Omega + \sum_{\substack{i=1\\ i\neq k}}^{K} tP\sigma^2_{\tilde{\mathbf{h}}_i}}\right) =$$

$$\left(1 + \frac{tP\delta_k + tP\sigma^2_{\tilde{\mathbf{h}}_k}}{tP(\alpha-\delta_k) + \sum_{\substack{i=1\\ i\neq k}}^{K} tP\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right), \tag{72}$$

$$2^{r_s} - 1 = \frac{tP\delta_k + tP\sigma^2_{\tilde{\mathbf{h}}_k}}{tP(\alpha-\delta_k) + \sum_{\substack{i=1\\ i\neq k}}^{K} tP\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}$$

$$-2^{r_s}\max_i \frac{tP\sigma_{\hat{\mathbf{h}}_i} + tP\sigma^2_{\tilde{\mathbf{h}}_i}}{tP\Omega + \sum_{\substack{i=1\\ i\neq k}}^{K} tP\sigma^2_{\tilde{\mathbf{h}}_i}}. \tag{73}$$

and

$$\Lambda = \frac{tP\delta_k + tP\sigma^2_{\tilde{\mathbf{h}}_k}}{tP(\alpha-\delta_k) + \sum_{\substack{i=1\\ i\neq k}}^{K} tP\sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}, \tag{74}$$

where $\Lambda = 2^{r_s} - 1 + 2^{r_s}\max_i \frac{\sigma_{\hat{\mathbf{h}}_i} + \sigma^2_{\tilde{\mathbf{h}}_i}}{\Omega + \sum_{\substack{i=1\\ i\neq k}}^{K} \sigma^2_{\tilde{\mathbf{h}}_i}}$. After some manipulations we can find (43).

References

[1] Y. Mao, O. Dizdar, B. Clerckx, R. Schober, P. Popovski, and H. V. Poor, "Rate-splitting multiple access: Fundamentals, survey, and future research trends," *IEEE Communications Surveys and Tutorials*, pp. 1–1, 2022.

[2] B. Clerckx, H. Joudeh, C. Hao, M. Dai, and B. Rassouli, "Rate splitting for mimo wireless networks: a promising phy-layer strategy for lte evolution," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 98–105, May 2016.

[3] 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.

[4] C. Hao, Y. Wu, and B. Clerckx, "Rate analysis of two-receiver miso broadcast channel with finite rate feedback: A rate-splitting approach," *IEEE Transactions on Communications*, vol. 63, no. 9, pp. 3232–3246, Sept 2015.

[5] A. Papazafeiropoulos and T. Ratnarajah, "Rate-splitting robustness in multi-pair massive mimo relay systems," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5623–5636, Aug 2018.

[6] H. Joudeh and B. Clerckx, "Sum-rate maximization for linearly precoded downlink multiuser miso systems with partial csit: A rate-splitting approach," *IEEE Transactions on Communications*, vol. 64, no. 11, pp. 4847–4861, Nov 2016.

[7] M. Dai, B. Clerckx, D. Gesbert, and G. Caire, "A rate splitting strategy for massive mimo with imperfect csit," *IEEE Transactions on Wireless Communications*, vol. 15, no. 7, pp. 4611–4624, July 2016.

[8] C. Hao and B. Clerckx, "Miso networks with imperfect csit: A topological rate-splitting approach," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2164–2179, May 2017.

[9] H. Joudeh and B. Clerckx, "Rate-splitting for max-min fair multigroup multicast beamforming in overloaded systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7276–7289, Nov 2017.

[10] Y. Mao, B. Clerckx, and V. O. Li, "Rate-splitting multiple access for downlink communication systems: bridging, generalizing, and outperforming sdma and noma," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 133, May 2018. [Online]. Available: https://doi.org/10.1186/s13638-018-1104-7

[11] A. Salem, C. Masouros, and B. Clerckx, "Rate splitting with finite constellations: The benefits of interference exploitation vs suppression," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1541–1557, 2021.

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

[13] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sept. 2009.

[14] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2008, pp. 524–528.

[15] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sept. 2013.

[16] J. Zhang, C. Yuen, C. Wen, S. Jin, and X. Gao, "Ergodic secrecy sum-rate for multiuser downlink transmission via regularized channel inversion: Large system analysis," *IEEE Communications Letters*, vol. 18, no. 9, pp. 1627–1630, 2014.

[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, 2013.

[18] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user mimo regularized channel inversion precoding," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3472–3482, 2012.

[19] A. Salem, C. Masouros, and K.-K. Wong, "On the secrecy performance of interference exploitation with psk: A non-gaussian signaling analysis," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2021.

[20] L. Sun and X. Tian, "Physical layer security in multi-antenna cellular systems: Joint optimization of feedback rate and power allocation," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2022.

[21] S. V. Pechetti and R. Bose, "Channel-aware artificial inter-symbol interference for enhancing physical layer security," *IEEE Communications Letters*, vol. 23, no. 7, pp. 1182–1185, 2019.

[22] N. Su, E. Panayirci, M. Koca, and H. V. Poor, "Spatial constellation design-based generalized space shift keying for physical layer security of multi-user mimo communication systems," *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1785–1789, 2021.

[23] H. Wang, W.-Q. Wang, and S. Ji, "Joint precoding spatial and rotating symbol modulation for physical-layer security," *IEEE Communications Letters*, vol. 23, no. 12, pp. 2150–2153, 2019.

[24] Z. Sheng, H. D. Tuan, A. A. Nasir, H. V. Poor, and E. Dutkiewicz, "Physical layer security aided wireless interference networks in the presence of strong eavesdropper channels," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3228–3240, 2021.

[25] J. Hu, X. Shi, Y. Chen, H. Zheng, and F. Shu, "Multiple antennas-based secure communications with channel inversion power control," *IEEE Wireless Communications Letters*, pp. 1–1, 2022.

[26] P. Li, M. Chen, Y. Mao, Z. Yang, B. Clerckx, and M. Shikh-Bahaei, "Cooperative rate-splitting for secrecy sum-rate enhancement in multi-antenna broadcast channels," in *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, 2020, pp. 1–6.

[27] H. Bastami, M. Letafati, M. Moradikia, A. Abdelhadi, H. Behroozi, and L. Hanzo, "On the physical layer security of the cooperative rate-splitting-aided downlink in uav networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5018–5033, 2021.

[28] O. Dizdar and B. Clerckx, "Rate-splitting multiple access for communications and jamming in multi-antenna multi-carrier cognitive radio systems," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 628–643, 2022.

[29] H. Fu, S. Feng, W. Tang, and D. W. K. Ng, "Robust secure beamforming design for two-user downlink miso rate-splitting systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 12, pp. 8351–8365, 2020.

[30] J. Zhou, Y. Sun, and C. Tellambura, "Physical-layer security for cache-enabled c-rans via rate splitting," *IEEE Communications Letters*, pp. 1–1, 2022.

[31] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, "Secure and energy efficient transmission for rsma-based cognitive satellite-terrestrial networks," *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 251–255, 2021.

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

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

[34] B. Clerckx and C. Oestges, "Chapter 14 mimo in lte, lte advanced and wimax," in *Mimo Wireless Networks (Second Edition)*. Oxford: Academic Press, 2013, pp. 597–635. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780123850553000146

[35] Taesang Yoo and A. Goldsmith, "Capacity and power allocation for fading mimo channels with channel estimation error," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2203–2214, May 2006.

[36] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser mimo systems," *IEEE Transactions on Communications*, vol. 61, no. 4, pp. 1436–1449, April 2013.

[37] Y. Mao, O. Dizdar, B. Clerckx, R. Schober, P. Popovski, and H. V. Poor, "Rate-splitting multiple access: Fundamentals, survey, and future research trends," *IEEE Communications Surveys and Tutorials*, pp. 1–1, 2022.

[38] B. Clerckx, Y. Mao, R. Schober, E. A. Jorswieck, D. J. Love, J. Yuan, L. Hanzo, G. Y. Li, E. G. Larsson, and G. Caire, "Is noma efficient in multi-antenna networks? a critical look at next generation multiple access techniques," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1310–1343, 2021.

[39] T. X. Tran and K. C. Teh, "Spectral and energy efficiency analysis for slnr precoding in massive mimo systems with imperfect csi," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 4017–4027, June 2018.

[40] M. Sadek, A. Tarighat, and A. H. Sayed, "A leakage-based precoding scheme for downlink multi-user mimo channels," *IEEE Transactions on Wireless Communications*, vol. 6, no. 5, pp. 1711–1721, May 2007.

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

[42] 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.

[43] 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.

[44] H. Tataria, P. J. Smith, and P. A. Dmochowski, "On the general analysis of coordinated regularized zero-forcing precoding: An application to two-tier small-cell networks," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 3133–3150, 2017.

[45] J. Kim, H. Lee, C. Song, T. Oh, and I. Lee, "Sum throughput maximization for multi-user mimo cognitive wireless powered communication networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 913–923, Feb 2017.

[46] H. Lee, K. J. Lee, H. B. Kong, and I. Lee, "Sum-rate maximization for multiuser mimo wireless powered communication networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, pp. 9420–9424, Nov 2016.

[47] K. Hamdi, "A useful lemma for capacity analysis of fading interference channels," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 411–416, Feb. 2010.

[48] Q. Zhang, S. Jin, K. Wong, H. Zhu, and M. Matthaiou, "Power scaling of uplink massive mimo systems with arbitrary-rank channel means," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 966–981, 2014.