messages are encoded in s (which is a variable) strongest eigen-subchannels based on ordered eigenvalues of Wishart matrices, while AN signals are generated in remaining spaces. Strategy for Rician channels using the complex non-central Wishart distribution. A closed form expression for secrecy capacity is determined.
Rician fading (LOS + NLOS part with Rice factor) and not Rayleigh fading

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 14, 2017, accepted January 29, 2018, date of publication February 12, 2018, date of current version March 12, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2804924

Secrecy Capacity of Artificial Noise Aided Secure Communication in MIMO Rician Channels

MANSOOR AHMED[1] AND LIN BAI[1,2], (Senior Member, IEEE)
[1]School of Electronics and Information Engineering, Beihang University, Beijing 100191, China
[2]Beijing Laboratory for General Aviation Technology, Beihang University, Beijing 100191, China

Corresponding author: Lin Bai (l.bai@buaa.edu.cn)

This work was supported by the National Key Research and Development Program of China under Grant 2017YFB0503002 and Grant 2015BAG15B01.

ABSTRACT Recent research on the physical layer security of wireless systems focuses on artificial noise (AN) aided security. The main metric for analysis of such systems is the secrecy capacity of the system. Most of the AN schemes proposed in recent research are based on a hypothesis that the number of transmit antennas is larger than that of the receive antennas. Under this assumption, the system can utilize all eigen-subchannels, equal to the number of the receive antennas, to send secret messages. The remaining null spaces are used for transmitting AN signals. These AN signals null out at the legitimate receivers and degrade illegitimate receiver's channels. However, this strategy can significantly impair the secrecy capacity of the system if the number of transmit antennas is constrained or even smaller than the number of receive antennas. Recently, a new strategy has been proposed, where messages are encoded in s (which is a variable) strongest eigen-subchannels based on ordered eigenvalues of Wishart matrices, while AN signals are generated in remaining spaces. This paper extends this strategy to Rician channels using the complex non-central Wishart distribution. A closed form expression for secrecy capacity of such system is computed using majorization theory. Performance of a MIMO communication system in Rician fading environment is simulated and effect of the Rician factor on secrecy capacity is studied. The same approach is then extended to decode and forward relay network. Secrecy capacity of the said network is computed, and the effect of AN is studied using the same methodology.

INDEX TERMS Artificial noise, decode and forward relay network, eigenvalue distribution, MIMO channel capacity, physical layer security, Rician channels, secrecy capacity, Wishart matrices.

I. INTRODUCTION

Wireless network security is becoming an important factor in modern wireless communication networks. The techniques, already being used for wired networks, can be applied to secure network, but the special characteristics of wireless systems call for innovation. The broadcast nature of wireless transmissions enables any nearby receiver to act as an intruder and can tap into the transmission. Wireless devices have more limitations on energy and bandwidth, whereas wireless networks have more dynamic topology. Such special characteristics of wireless systems can be handled by employing physical layer security techniques.

The founder of theoretical secret communication is considered to be Shannon [1]. It was later enhanced considering scenario where the legitimate receiver and the illegitimate receiver (eavesdropper) have separate channels [2]. The author showed that security of transmission can be guaranteed if the channel capacity of eavesdropper – transmitter link is less than the receiver's channel. The paper generalized the scenario considered in [3] where the eavesdropper's channel was considered to be much degraded than the receiver's channel. The notion of 'secrecy capacity' is defined as the maximum rate at which the transmitter can reliably communicate a secure message to the legitimate receiver, making sure that the eavesdropper is unable to decode the message [3].

The concept of artificial noise (AN) was introduced by [4]. It was supposed the number of transmit antennas is larger than that of receive antennas. Under this assumption, the system can utilize all Eigen-subchannels, equal to number of receive antennas, of a MIMO system to send messages, and use remaining null spaces for transmitting AN signals. This paper also showed that the secrecy capacity of MIMO system behaves in a different manner than the MIMO capacity. Moreover, It was also concluded that the secrecy requirements drive the behavior of MIMO capacity. For example, the paper shows that the secrecy capacity does not increase

monotonically with the minimum of the number of transmit and receive antennas, unlike the notable result on usual MIMO capacity [5]. Consequently, the paper stressed the need to characterize MIMO secrecy capacity. Ahmed and Bai [6] used space-time block coding (STBC) technique to increase the secrecy capacity of the system employing two antennas each at transmitter and receiver while eavesdropper was equipped with a single antenna. The authors plotted the BER of such a system and showed that STBC aided with AN can guarantee secrecy [6].

A new technique was proposed by [7], where the messages are encoded in s (which is a variable) strongest eigen-subchannels based on ordered eigenvalues of Wishart matrices, while AN signals are generated in remaining spaces. The authors derived the average secrecy capacity expression for the said scheme. In this scheme, authors assumed a MIMO scenario where the eavesdropper is also equipped with multiple antennas.

Lai *et al.* [8] combined the technique of AN with the beamforming. But this paper also showed that incase when the eavesdropper and receiver are located in the same vicinity, beamforming would fail to improve the secrecy of information. Yan and Malaney [9] proposed a new optimal location-based beamforming (LBB) scheme for the wiretap channel. The paper assumed that both the main channel and the eavesdropper's channel are subject to Rician fading. This scheme also takes the location of the eavesdropper as an input.

In [10] the capacity of a MIMO system under the influence of Rician fading was studied. The authors assumed that perfect channel state information (CSI) is available at the receiver. The authors computed capacity closed-form expression for two cases, when the transmitter has knowledge of CSI and when it doesn't have any CSI available. New signaling scheme, which can achieve capacity using the Rician-ness of the channel, was proposed in the same paper discussed above.

The idea of using strongest eigen-subchannel for transmitting messages and sending AN signals using the remaining $t-1$ spaces, where t is number of transmitter antennas was presented in [11] and [12]. The proposed scheme showed that a positive secrecy capacity is achievable without multiplexing gains. In [13], r (number of receive antennas) eigen-subchannels were used to transmit messages and the remaining $t-r$ null spaces for sending AN signals. This scheme significantly improves the secrecy capacity of the system by offering multiplexing gain. A closed form expression for average secrecy capacity of this scheme was derived with the help of non-ordered eigenvalues of a Wishart matrix in [14]. However, $t-r$ is the precondition for all of these schemes to be optimal. As mentioned earlier, [7] devised a scheme that tackles this precondition by designing a better AN scheme to improve the secrecy capacity via selecting proper numbers of message-sending eigen-subchannels and AN-sending spaces.

Most of these works have supposed a Rayleigh fading environment for both receiver and eavesdropper's channel [15]. However, this assumption does not hold in many practical scenarios where both channels can experience different fading environment e.g. Rician fading. However the computation of exact capacities for a Rician channels is a challenging task and requires complex mathematical computations which is extensively analyzed in literature [16]–[19]. Guimaraes and Cavalcante [20] used majorization theory to derive the closed form ergodic capacity of spatially uncorrelated Rician channels and obtained a closed form upper bound for it. In this paper, the technique developed by [7] is used and it is further extended to the Rician fading channels using the mathematical technique used in [20].

The relay networks have also gained a lot of attention in improving the physical layer security. Authors have studied relay networks based on the information theoretic approach [21]–[24] as well as signal processing point of view [25]–[27]. While in Wang *et al.* have studied two way relay networks using distributed beamforming. In this paper, the proposed AN aided security technique is also extended to a decode and forward relay network employing a single relay.

The rest of the paper is organized as follows. Section II describes the system model and transmission scheme in detail. Section III illustrates the computation of secrecy capacity of the system. Section IV and V describe the simulation results and conclusions.

II. SYSTEM MODEL

Consider a MIMO communication system consisting of a transmitter with N_t transmit antennas, a legitimate receiver with N_r receive antennas, and an eavesdropper with N_e receive antennas, as shown in Fig. 1. As used commonly in literature, the transmitter, receiver, and eavesdropper are denoted as Alice, Bob and Eve respectively. It is also assumed that Alice has full CSI of Bob via a broadcast feedback channel. Only channel distribution information (CDI) of Eve is known at the transmitter. The main channel will also be referred to as a legitimate link and the wiretap channel as illegitimate link in the paper. Generally, the main channel between Alice and Bob, and the wiretap channel between Alice and Eve can be defined as complex Gaussian matrices $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$ and $\mathbf{H}_e \in \mathbb{C}^{N_e \times N_t}$ respectively. Here, $N_t > N_e$ is assumed for secure transmission, and define $m = \max(N_r, N_t)$ and $n = \min(N_r, N_t)$. Each element of $\mathbf{H}_e$ and $\mathbf{H}$ are Gaussian with independent real and imaginary parts each distributed as $\mathcal{N}(\mu/\sqrt{2}, \sigma^2)$. This is due to the fact that we are considering Rician fading channels, at both legitimate and illegitimate links.

A. CHANNEL MODEL

Both $\mathbf{H}_e$ and $\mathbf{H}$ are considered to be spatially uncorrelated, thus we can write the channel matrix as [19], [29]

$$\mathbf{H} = a\mathbf{H}_L + b\mathbf{H}_R \tag{1}$$

where $\mathbf{H}_L$ is a deterministic (specular) matrix depicting the line of sight (LoS) component and $\mathbf{H}_R$ is an i.i.d, zero mean circularly symmetric complex Gaussian and unit variance matrix $\sim \; C\mathcal{N}(0, \mathbf{I}_{N_r \times N_t})$. The entries, a and b are power

Non central wishart distribution: Wishart distribution coming from non zero mean Gaussian distribution

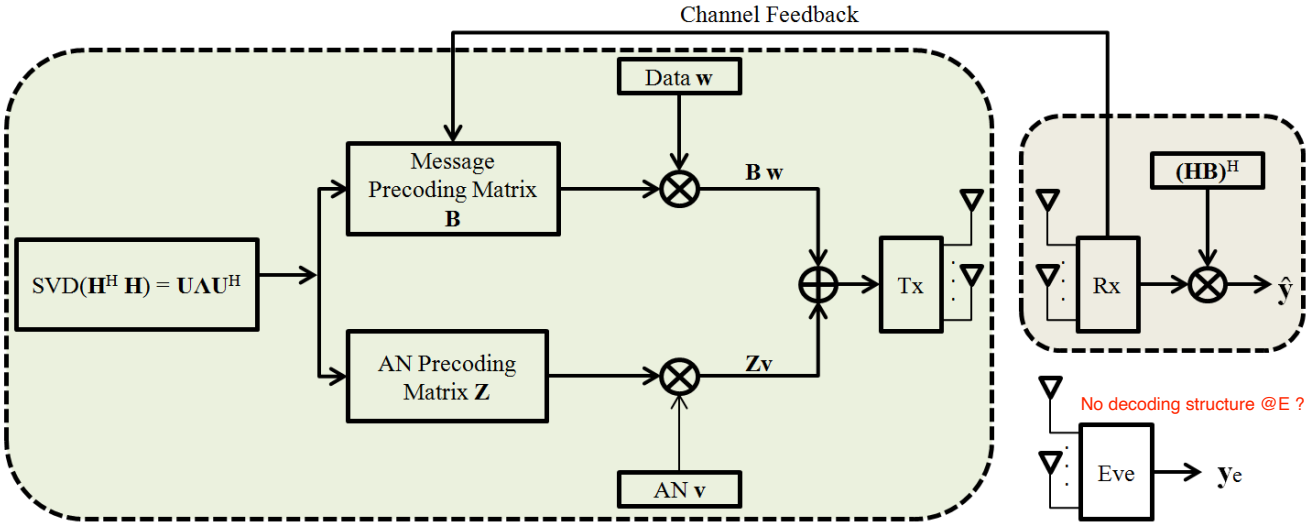


FIGURE 1. Detailed illustration of MIMO system under consideration [7].

normalization coeffiecients depending upon the Rician factor. In this paper two models are considered, as were supposed in [30], for Model A, $a = \sqrt{\kappa/(\kappa+1)}$ and b= $1/(\kappa+1)$, where κ is the Rician factor, and for Model B, $a = \sqrt{\kappa}$ and $b = 1$. In the case of Model A, $a^2 + b = 1$ and hence, the SNR per receive antenna is independent of κ. For Model B, the SNR per receive antenna depends on κ as $a^2 + b = (1+\kappa)$. As both the legitimate link and the illegitimate link are experiencing Rician fading so same applies to both $\mathbf{H}_e$ and $\mathbf{H}$.

As mentioned earlier, it is assumed the elements of this channel matrix $\mathbf{H}$ are independent to each other. So, the elements $(\mathbf{H})_{r,t}$ of $\mathbf{H}$ are i.i.d complex Gaussian random variables$(\mathbf{H})_{r,t} \sim C\mathcal{N}(\frac{\mu}{2}(1+i), 2\sigma^2)$, for $r = 1, 2, \cdots N_r$ and $t = 1, 2, \cdots N_t$, and the distribution of the magnitude of elements of $\mathbf{H}$ has the following Rician probability density function (pdf):

$$f_X(x) = 2(1+\kappa)\, x e^{-(1+\kappa)x^2-\kappa} I_0\left(2\sqrt{\kappa(1+\kappa)}\, x\right) \quad (2)$$

where I_0 is the modified Bessel function of the first kind and the Rician factor κ is defined as

$$\kappa = \frac{|\mu|^2}{2\sigma^2} \quad (3)$$

With the above suppositions $\mathbf{H}$ is now a complex normally distributed matrix, denoted as $(\mathbf{H})_{r,t} \sim C\mathcal{N}(\mathbf{M}, \mathbf{I}_{N_t} \bigotimes \sum)$, for the assumed model $\mathbf{M}$ and Σ are defined as

$$\Sigma = 2\sigma^2 \mathbf{I}_{N_r} \quad (4)$$

Σ = variance
M = mean

$$\mathbf{M} = \frac{\mu}{2}(1+i)\,\psi \quad (5)$$

where ψ denotes the $N_r \times N_t$ matrix of all ones.

$$\mathbf{W} = \begin{Bmatrix} \mathbf{H}\mathbf{H}^\dagger & if \;\; N_r \le N_t \\ \mathbf{H}^\dagger\mathbf{H} & if \;\; N_r > N_t \end{Bmatrix} \quad (6)$$

$\mathbf{W}$ is a $n \times n$ square matrix. The matrix $\mathbf{W}$ follows the complex non-central Wishart distribution with m degrees of freedom, covariance matrix $\sum$ and matrix of noncentrality parameters $\Omega = \Sigma^{-1}\mathbf{M}^H\mathbf{M}$. The pdf of $\mathbf{W} \sim W_n(m, \Sigma, \Omega)$ can be written as

$$f_{\mathbf{W}}(W) = \frac{1}{\Gamma_n(m)(det\,\Sigma)^m} etr\left(-\Sigma^{-1}W\right)(det\,W)^{m-n} \times etr(\Omega)\, {}_0F_1\left(m;;\Omega\Sigma^{-1}W\right) \quad (7)$$

Where ${}_0F_1\left(m;;\Omega\Sigma^{-1}W\right)$ is complex Bessel hypergeometrical function and $\Gamma_n(m)$ is the complex multivariate gamma function, both are as defined in [10]. Considering even distribution of power among all transmit antennas, we can write the ergodic MIMO channel capacity as

$$C = E\left[\log_2\left(|\mathbf{I}_m + (P/N_t)\,\mathbf{W}|\right)\right] \quad (8)$$

When no decoding techniques applied at both end (B and E)

The same expression applies to both transmitter-receiver link and transmitter-eavesdropper link.

B. TRANSMISSION METHODOLOGY

Liu *et al.* [7] considered s ($s \le N_t$) message-sending eigen-subchannels, which are selected by transmitter, based on the channel state information feedback from Bob. The sequence of operations at the transmitter can be summarized as follows:

1) Singular value decomposition (SVD) of $\mathbf{H}^\dagger\mathbf{H} \in \mathbb{C}^{N_t \times N_t}$ in a pre-processor.

$$\mathbf{H}^\dagger\mathbf{H} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^\dagger \quad (9)$$

where the unitary matrix $\mathbf{U} \in \mathbb{C}^{N_t \times N_t}$, its Hermitian transpose $\mathbf{U}^\dagger \in \mathbb{C}^{N_t \times N_t}$, and a diagonal matrix $\mathbf{\Lambda} \in \mathbb{R}^{N_t \times N_t}$, which consists of all non negative eigenvalues of $\mathbf{H}^\dagger\mathbf{H}$.

2) Generation of a message pre-coding matrix $\mathbf{B} \in \mathbb{C}^{N_t \times s}$, whose columns are the eigenvectors corresponding to

the first to the sth largest eigenvalues of $\mathbf{H}^{\dagger}\mathbf{H}$. The message vector $\mathbf{w}$ is multiplied by message precoding matrix i.e $\mathbf{Bw}$.

3) Generation of an AN precoding matrix $\mathbf{Z}\in\mathbb{C}^{N_t\times d}$, where $d = N_t - s$, whose columns are the eigenvectors of remaining eigenvalues of $\mathbf{H}^{\dagger}\mathbf{H}$. Artificial noise vector $\mathbf{v}$ is generated and multiplied by the precoding matrix $\mathbf{Zv}$.

It should be noted that $\mathbf{B}$ and $\mathbf{Z}$ are semi-unitary matrices derived from $\mathbf{H}$. Hence we write them as

$$\mathbf{B}^{\dagger}\mathbf{B} = \mathbf{I}_s \tag{10}$$
$$\mathbf{Z}^{\dagger}\mathbf{Z} = \mathbf{I}_d \tag{11}$$

The received signal at the legitimate receiver and eavesdropper can be written as, respectively

$$\mathbf{y} = \mathbf{HBw} + \mathbf{HZv} + \mathbf{n} \tag{12}$$
$$\mathbf{y}_e = \mathbf{H}_e\mathbf{Bw} + \mathbf{H}_e\mathbf{Zv} + \mathbf{n}_e \tag{13}$$

Both $\mathbf{w}$ and $\mathbf{v}$ are circularly symmetric complex Gaussian vectors with zero mean and covariance matrices as $(P/N_t)\mathbf{I}_s$ and $(P/N_t)\mathbf{I}_d$, respectively. For simplicity, the total power P is distributed evenly to each antenna. Khalighi *et al.* [15] have shown that even power distribution results in channel capacity approximate to optimal power allocation. $\mathbf{n}$ and $\mathbf{n}_e$ are additive white Gaussian noise vectors with covariance matrices $\mathbf{I}_r$ and $\mathbf{I}_e$ respectively.

The AN component $\mathbf{HZv}$ is nulled out at the legitimate receiver, while at the eavesdropper this AN creates additional component in the received signal hence degrading its channel. Resulting in lower capacity of illegitimate link. The process done at the legitimate receiver to eliminate AN can be written as

$$\widetilde{\mathbf{y}} = (\mathbf{HB})^{\dagger}\mathbf{y} \tag{14}$$
$$\widetilde{\mathbf{y}} = (\mathbf{HB})^{\dagger}\mathbf{HBw} + (\mathbf{HB})^{\dagger}\mathbf{HZv} + (\mathbf{HB})^{\dagger}\mathbf{n} \tag{15}$$

where we can write $(\mathbf{HB})^{\dagger}\mathbf{HZ}$ as

$$(\mathbf{HB})^{\dagger}\mathbf{HZ} = \mathbf{B}^{\dagger}\mathbf{H}^{\dagger}\mathbf{HZ} = \mathbf{B}^{\dagger}\mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^{\dagger}\mathbf{Z} \tag{16}$$
$$\mathbf{B}^{\dagger}\mathbf{U} = \begin{bmatrix}\mathbf{I}_s & \mathbf{0}_{s\times d}\end{bmatrix} \tag{17}$$
$$\mathbf{B}^{\dagger}\mathbf{U}\boldsymbol{\Lambda} = \begin{bmatrix}\boldsymbol{\Lambda}_s & \mathbf{0}_{s\times d}\end{bmatrix} \tag{18}$$
$$\mathbf{U}^{\dagger}\mathbf{Z} = \begin{bmatrix}\mathbf{0}_{s\times d}\\ \mathbf{I}_d\end{bmatrix} \tag{19}$$
$$(\mathbf{HB})^{\dagger}\mathbf{HZ} = \begin{bmatrix}\boldsymbol{\Lambda}_s & \mathbf{0}_{s\times d}\end{bmatrix}\begin{bmatrix}\mathbf{0}_{s\times d}\\ \mathbf{I}_d\end{bmatrix} = \mathbf{0}_{s\times d} \tag{20}$$

While the term involving the message signal can be written as

$$(\mathbf{HB})^{\dagger}\mathbf{HB} = \mathbf{B}^{\dagger}\mathbf{H}^{\dagger}\mathbf{HB} = \mathbf{B}^{\dagger}\mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^{\dagger}\mathbf{B} \tag{21}$$
$$(\mathbf{HB})^{\dagger}\mathbf{HB} = \boldsymbol{\Lambda}_s \tag{22}$$

So we can write the equation of the received signal as

$$\widetilde{\mathbf{y}} = \boldsymbol{\Lambda}_s\mathbf{w} + \widetilde{\mathbf{n}} \tag{23}$$

where $\widetilde{\mathbf{n}} = (\mathbf{HB})^{\dagger}\mathbf{n} \in \mathbb{C}^{s\times 1}$ is an AWGN vector with distribution $\mathcal{CN}(0, \boldsymbol{\Lambda}_s)$. $\boldsymbol{\Lambda}_s\in\mathbb{R}^{N_t\times N_t}$ is a diagonal matrix containing first s eigenvalues of $\mathbf{H}^{\dagger}\mathbf{H}$. This matrix of eigen-values is fixed and will not affect the channel capacity. At the eavesdropper, the channel will be degraded regardless of channel knowledge at it because

$$(\mathbf{HB})^{\dagger}\mathbf{H}_e\mathbf{Z} \neq 0 \tag{24}$$
$$(\mathbf{H_eB})^{\dagger}\mathbf{H}_e\mathbf{Z} \neq 0 \tag{25}$$

III. SECRECY CAPACITY OF THE SYSTEM

In the MIMO wiretap channel model, when the receiver and eavesdropper have perfect knowledge of their respective channels, the instantaneous secrecy capacity in terms of mutual information is given by

$$C_{\mathrm{s}} \geq \max_{\mathrm{p(w)},\mathrm{p(v)}} \left\{ I\left(\mathbf{y};\mathbf{w}\right) - \mathrm{I}\left(\mathbf{y_e};\mathbf{w}\right) \right\} \tag{26}$$

where the maximization is taken over all input distributions of p (w)and p(v). Considering both $\mathbf{w}$ and $\mathbf{v}$ as circularly symmetric complex Gaussian vectors, the instantaneous secrecy capacity can be expressed as

$$C_{\mathrm{s}} = [C_{\mathrm{m}} - C_{\mathrm{w}}]^{+} \tag{27}$$

where C_{m} is the capacity of main channel and C_{w} is the capacity of wiretap channel defined as follows.

$$C_{\mathrm{m}} = \log_2\left(\left|\mathbf{I}_{N_r} + (P/N_t)\,\mathbf{H}_1\mathbf{H}_1^{\dagger}\right|\right) \tag{28}$$
$$C_{\mathrm{w}} = \log_2\left(\left|\mathbf{I}_{N_e} + \frac{(P/N_t)\,\mathbf{H}_2\mathbf{H}_2^{\dagger}}{(P/N_t)\,\mathbf{H}_3\mathbf{H}_3^{\dagger} + \mathbf{I}_{\mathrm{e}}}\right|\right) \tag{29}$$

where

$$\mathbf{H}_1 = \mathbf{HB} \in \mathbb{C}^{N_r\times s}$$
$$\mathbf{H}_2 = \mathbf{H_eB} \in \mathbb{C}^{N_e\times s}$$
$$\mathbf{H}_3 = \mathbf{H_eZ} \in \mathbb{C}^{N_e\times d}$$

According to [7, Th. 2], considering both $\mathbf{w}$ and $\mathbf{v}$ as circularly symmetric complex Gaussian vectors, the average secrecy capacity can be defined as

$$\tilde{C}_s = \mathrm{E}_{\mathbf{H}}\left[C_{\mathrm{m}}\right] - \mathrm{E}_{\mathbf{H},\mathbf{H_e}}\left[C_{\mathrm{w}}\right] \tag{30}$$

To compute the exact secrecy capacity expression, for the case when $s \geq \min(N_t, N_r)$, given CSI matrix $\mathbf{H}$ and CDI matrix $\mathbf{H_e}$, the average secrecy capacity is given by

$$\tilde{C}_s = \mathrm{E}\left[\log_2\left(\left|\mathbf{I}_{\mathrm{N_r}} + (\mathrm{P/t})\,\mathbf{H}_1\mathbf{H}_1^{\dagger}\right|\right)\right] - \mathrm{E}\left[\log_2\left(\left|\mathbf{I}_{\mathrm{N_e}} + \frac{(\mathrm{P/t})\,\mathbf{H}_2\mathbf{H}_2^{\dagger}}{(\mathrm{P/t})\,\mathbf{H}_3\mathbf{H}_3^{\dagger} + \mathrm{I_e}}\right|\right)\right] \tag{31}$$

Using [7, Th. 3] the average secrecy capacity can be written as

$$\tilde{C}_s\left(\mathbf{w},\mathbf{v},\mathbf{H},\mathbf{H_e}\right) = C\left[\mathbf{H},(P/N_t)\right] + C\left[\mathbf{H}_3,(P/N_t)\right] - C\left[\mathbf{H}_4,(P/N_t)\right] \tag{32}$$

where $\mathbf{H}_4 = [\mathbf{H}_2, \mathbf{H}_3] = \mathbf{H_eU} \in \mathbb{C}^{\mathrm{N_e}\times\mathrm{N_t}}$

The average secrecy capacity expression is not in the closed form. We can write the $\mathrm{C}[\mathbf{A}, (\mathrm{P}/\mathrm{N_t})]$ for any $\mathbf{A} \in \mathbb{C}^{\alpha\times\beta}$, and $n = \min(\alpha,\beta)$, $m = \max(\alpha,\beta)$

$$\mathrm{C}[\mathbf{A}, (P/N_t)] = \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{E}\left[\log_2 (1+ (P/N_t)\, \lambda_{\mathrm{i}} (\mathbf{A}))\right] \quad (33)$$

The following approximations were given in [7]

$$\begin{cases} \log_2 (1+v) \approx v \log_2 (\mathrm{e}) & v \approx 0 \\ \log_2 (1+v) \approx \log_2 (v) & v \gg 1 \end{cases} \quad (34)$$

where e is the Euler's number. Apart from the equation mentioned above, majorization theory will also be used to simplify the equation (33).

A. MAJORIZATION THEORY

The fundamentals of majorization theory can be found in [31], while [32] studied some problems in wireless communication using it. The relevant elements of this theory will be discussed in this section.

Let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, where $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n)$, then $\mathbf{x}$ is majorized by $\mathbf{y}$ if the rearrangement of the components of $\mathbf{x}$ and $\mathbf{y}$ such that $x_{[1]} \geq x_{[2]} \cdots \geq x_{[n]}$, $y_{[1]} \geq y_{[2]} \cdots \geq y_{[n]}$ satisfy $\sum_{i=1}^{k} x_{[i]} \leq \sum_{i=1}^{k} y_{[i]}$, where $1 \leq k \leq (n-1)$ and $\sum_{i=1}^{n} x_{[i]} = \sum_{i=1}^{n} y_{[i]}$. It is denoted by $\mathbf{x} \prec \mathbf{y}$.

The function $\phi(.)$ is called Schur-convex if $\boldsymbol{x} \prec \boldsymbol{y}$ implies $\phi(\boldsymbol{x}) \leq \phi(\boldsymbol{y})$ any such function $\phi(.)$ is called Schur-concave, if $-\phi$ is Schur-convex.

Consider a real valued function $\phi(.)$ on $\mathbb{R}^n$. If function $g : \mathbb{R} \to \mathbb{R}$ is concave, then $\phi(.)$ defined by the following equation is Schur-concave [31].

$$\phi(\mathbf{x}) = \sum_{i=1}^{n} g(x_i) \quad (35)$$

If $\mathbf{A} \in \mathbb{C}^{nxn}$ is a Hermitian Matrix then

$$\mathrm{l}(\mathbf{A}) \prec \lambda(\mathbf{A}) \quad (36)$$

where $\mathrm{l}(\mathbf{A})$ represents the diagonal elements of $\mathbf{A}$.

B. SECRECY CAPACITY UPPER BOUND

Using the methodology adopted by [20], consider the vectors

$$\lambda(\mathbf{W}) = (\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_n) \quad (37)$$

$$\mathrm{l}(\mathbf{W}) = (l_1, l_2, l_3, \cdots, l_n) \quad (38)$$

where $\lambda(\mathbf{W})$ and $\mathrm{l}(\mathbf{W})$ are the eigenvalues and diagonal elements of matrix $\mathbf{W}$. As $\mathbf{W}$ is a Hermitian matrix, then according to [31],

$$\mathrm{l}(\mathbf{W}) \prec \lambda(\mathbf{W}) \quad (39)$$

where $\prec$ is the Majorization relation. The real-valued function $\phi : \mathbb{R}^p \to \mathbb{R}$ can be defined as

$$\phi(\mathbf{x}) = \sum_{i=1}^{p} \left[\log_2 (1+ (P/N_t)\, x_{\mathrm{i}})\right] \quad (40)$$

Suppose $\log_2 (1+ (\mathrm{P}/\mathrm{N_t})\, x_{\mathrm{i}})$ with $(\mathrm{P}/\mathrm{N_t}) > 0$, is the real-valued concave function, hence the $\phi(\mathbf{x})$ is Schur-concave and

$$\phi(\mathrm{l}(\mathbf{W})) \geq \phi(\lambda(\mathbf{W})) \quad (41)$$

Applying expectation in equation (41),

$$E[\phi(\mathrm{l}(\mathbf{W}))] \geq E[\phi(\lambda(\mathbf{W}))] \quad (42)$$

Therefore, the capacity can be written as

$$\begin{aligned} C &\leq E\left\{\sum_{i=1}^{n} \left[\log_2 (1+ (P/N_t)\, l_i)\right]\right\} \\ &= E\left\{\log_2 \left(\prod_{i=1}^{n} (1+ (P/N_t)\, l_i)\right)\right\} \\ &= \log_2 \left\{E\left(\prod_{i=1}^{n} (1+ (P/N_t)\, l_i)\right)\right\} \end{aligned} \quad (43)$$

where (43) is obtained using the Jensen's inequality. As $\mathbf{W}$ is defined in equation (6), note that $l_i = \sum_{j=1}^{m} |h_{ij}|^2$, for $i = 1, 2, \cdots, n$, and for the Model B of Rician channel defined earlier, the expected value of l_i can be written as $E[l_i] = m(\kappa+1)$. Hence, by using [20, eq. 26]

$$E\left(\prod_{i=1}^{n} l_i\right) = (m(\kappa+1))^n \quad (44)$$

Using (34) and (44), the equation (32) can be written as

$$\begin{aligned} C[\mathbf{A}, (P/N_t)] &= n\log_2 (P/N_t) + \log_2 \left((m(\kappa+1))^n\right) \\ &= n\log_2 (P/N_t) + n\log_2 (m(\kappa+1)) \end{aligned} \quad (45)$$

Expanding each term in equation (32)

$$C[\mathbf{H}, (P/N_t)] = x\log_2 (P/N_t) + x\log_2 (N_t(\kappa+1)) \quad (46)$$

$$C[\mathbf{H}_3, (P/N_t)] = y\log_2 (P/N_t) + y\log_2 (z(\kappa+1)) \quad (47)$$

$$C[\mathbf{H}_4, (P/N_t)] = e\log_2 (P/N_t) + e\log_2 (N_t(\kappa+1)) \quad (48)$$

where $y = \min(N_e, d)$, and $z = \max(N_e, d)$ and

$$x = \begin{cases} ccN_r & s = \min(N_t, N_r) \\ s & s < \min(N_t, N_r) \end{cases}$$

For high SNR region, the average secrecy capacity can be approximately written as

$$\begin{aligned} \tilde{C}_s^H \leq{}& (x+y-e)\log_2 (P/N_t) \\ &+ y\log_2 (z(\kappa+1)) + (x-e)\log_2 (N_t(\kappa+1)) \end{aligned} \quad (49)$$

Similarly for Model A [30], where $a = \sqrt{\kappa/(\kappa+1)}$ and $b = 1/(\kappa+1)$, $\tilde{C}_s^H$ can be written as

$$\begin{aligned} \tilde{C}_s^H \leq{}& (x+y-e)\log_2 (P/N_t) \\ &+ y\log_2 (z(\tau)) + (x-e)\log_2 (N_t(\tau)) \end{aligned} \quad (50)$$

where $\tau = (\kappa+1)^2/(\kappa^2+1)$. Equations (49) and (50) are the closed form secrecy capacity expressions for the system discussed in the previous section.

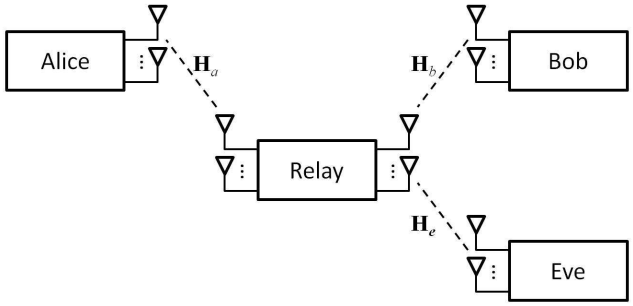


FIGURE 2. System model for a single relay MIMO network.

IV. SECRECY CAPACITY IN A RELAY NETWORK

Consider a half-duplex relay network comprising a single relay, a transmitter, a receiver and an eavesdropper as shown in Fig. 2. The transmitter and receiver have no direct link i.e the communication is taking place via the relay. It is also assumed that eavesdropper can only affect the relay to legitimate receiver's communication. The transmission takes place in two phases. During the first phase, Alice sends the message to the relay. The received signal at the relay can be written as

$$\mathbf{y}_r = \mathbf{H}_a\mathbf{w} + \mathbf{n}_a \tag{51}$$

The relay receives the message and under the assumption that relay knows the Alice-Relay and Relay-Bob channels, it decodes the received signal from the transmitter. The relay then adopts the same methodology as described in section II, the only difference here is the relay uses the channel matrix $\mathbf{H}_b$ i.e. the channel between Relay and Bob. It then performs the SVD, generates message pre-coding matrix and AN pre-coding matrix. It should be noted that the same procedure is applied here at relay that was being performed at the transmitter in section II. This is more useful in scenarios where transmitter and receiver are mobile stations and have computational and power limitations. The relay can be a base station or a fixed station with less computational and power constraints.

In the next phase, the relay amplifies the signal and transmits it. The transmitted signal can be written as

$$\mathbf{r}_b = \beta_1\mathbf{B}\mathbf{w} + \beta_2\mathbf{Z}\mathbf{v} \tag{52}$$

where β_1 and β_2 are the amplification factors for the message part and AN part of the transmitted signal respectively. These factors can be defined as [33]

$$\beta_1 = \varphi\sqrt{P/(P_s + \sigma_0)}, \quad \beta_2 = (1-\varphi)\sqrt{P/(P_s + \sigma_0)} \tag{53}$$

where φ is the signal to artificial noise ratio which ranges from 0 to 1 and P is transmit power of the relay. From here onward, N_t is the number of relay transmit antennas. Now the received signal at Bob and Eavesdropper can be written as

$$\mathbf{y}_b = \beta_1\mathbf{H}_b\mathbf{B}\mathbf{w} + \beta_2\mathbf{H}_b\mathbf{Z}\mathbf{v} + \mathbf{n}_b \tag{54}$$
$$\mathbf{y}_e = \beta_1\mathbf{H}_e\mathbf{B}\mathbf{w} + \beta_2\mathbf{H}_e\mathbf{Z}\mathbf{v} + \mathbf{n}_e \tag{55}$$

The receiver follows the same procedure as mentioned in section II to eliminate the AN component from the signal and recover the message. While the AN component and the amplification factor β effects the channel capacity of the eavesdropper's link. So the secrecy capacity of the system is affected. The channel capacity of main link and the wiretap channel can be written as

$$C_{\mathrm{m}} = \mathrm{E}\left[\log_2\left(\left|\mathbf{I}_{N_r} + (P/N_t)\,{\beta_1}^2\mathbf{H}_1\mathbf{H}_1^{\dagger}\right|\right)\right] \tag{56}$$
$$C_{\mathrm{w}} = \mathrm{E}\left[\log_2\left(\left|\mathbf{I}_{N_e} + \frac{(P/N_t)\,{\beta_1}^2\mathbf{H}_2\mathbf{H}_2^{\dagger}}{(P/N_t)\,{\beta_2}^2\mathbf{H}_3\mathbf{H}_3^{\dagger} + \mathbf{I}_{\mathrm{e}}}\right|\right)\right] \tag{57}$$

where $\mathbf{H}_1 = \mathbf{H}_b\mathbf{B}$, $\mathbf{H}_2 = \mathbf{H}_{\mathrm{e}}\mathbf{B}$ and $\mathbf{H}_3 = \mathbf{H}_{\mathrm{e}}\mathbf{Z}$. It can be noticed that these capacities are almost same as computed in section 3 because the same process is adopted by the relay. The factor β is the only change performed at the relay which will eventually affect the capacity. By using this methodology we can write equation (56) as

$$\mathrm{E}\left[\log_2\left(\left|\mathbf{I}_{N_r} + (P/N_t)\,{\beta_1}^2\mathbf{H}_1\mathbf{H}_1^{\dagger}\right|\right)\right] = C\left[\mathbf{H}_b, {\beta_1}^2\,(P/N_t)\right] \tag{58}$$

The equation (57) can be expanded as

$$C_{\mathrm{w}} = \mathrm{E}\left[\log_2(|X|)\right] - C\left[\mathbf{H}_3, {\beta_2}^2\,(P/N_t)\right] \tag{59}$$

where $X = \left(\mathbf{I}_{N_e} + (P/N_t)\,{\beta_1}^2\mathbf{H}_2\mathbf{H}_2^{\dagger} + (P/N_t)\,{\beta_2}^2\mathbf{H}_3\mathbf{H}_3^{\dagger}\right)$, using (34) and the identity $\log_2|X| = \mathrm{Tr}\left[\log_2(X)\right]$ the term containing X can be written as

$$\begin{aligned}&\mathrm{E}\left[\log_2(|X|)\right]\\ &= \mathrm{E}\left[\mathrm{Tr}\left((P/N_t)\,{\beta_1}^2\mathbf{H}_2\mathbf{H}_2^{\dagger} + (P/N_t)\,{\beta_2}^2\mathbf{H}_3\mathbf{H}_3^{\dagger}\right)\right]\\ &= (P/N_t)\,{\beta_1}^2\mathrm{E}\left[\mathrm{Tr}\left(\mathbf{H}_2\mathbf{H}_2^{\dagger}\right)\right] + (P/N_t)\,{\beta_2}^2\mathrm{E}\left[\mathrm{Tr}\left(\mathbf{H}_3\mathbf{H}_3^{\dagger}\right)\right]\end{aligned} \tag{60}$$

which can be approximated as

$$\mathrm{E}\left[\log_2(|X|)\right] = (P/N_t)\,{\beta_1}^2\,(yz) + (P/N_t)\,{\beta_2}^2\,(N_e s) \tag{61}$$

where y, z, N_e and s are as defined in section III. The average secrecy capacity can be written as

$$\begin{aligned}\tilde{C}_s(\mathbf{w}, \mathbf{v}, \mathbf{H}, \mathbf{H}_e) &= C\left[\mathbf{H}_b, {\beta_1}^2\,(P/N_t)\right]\\ &\quad + C\left[\mathbf{H}_3, (P/N_t)\right] - \mathrm{E}\left[\log_2(|X|)\right]\end{aligned} \tag{62}$$

where $\mathrm{E}\left[\log_2(|X|)\right]$ is defined in (61), while the other terms on right hand side of the above equation are defined as

$$C\left[\mathbf{H}_b, {\beta_1}^2\,(P/N_t)\right] = x\log_2\left({\beta_1}^2 P/N_t\right) + x\log_2\left(N_t\,(\kappa+1)\right) \tag{63}$$

$$C\left[\mathbf{H}_3, {\beta_1}^2\,(P/N_t)\right] = y\log_2\left({\beta_2}^2 P/N_t\right) + y\log_2\left(z\,(\kappa+1)\right) \tag{64}$$

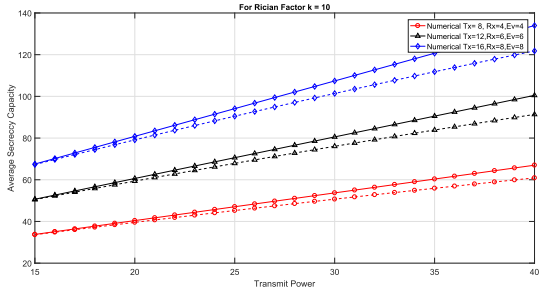


FIGURE 3. Average secrecy capacity of the system for different MIMO scenarios (dotted line show the simulation results).

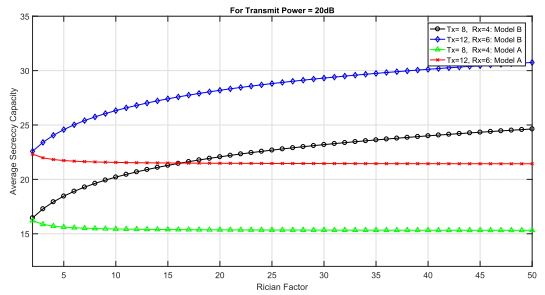


FIGURE 4. Average secrecy capacity against the Rician factor.

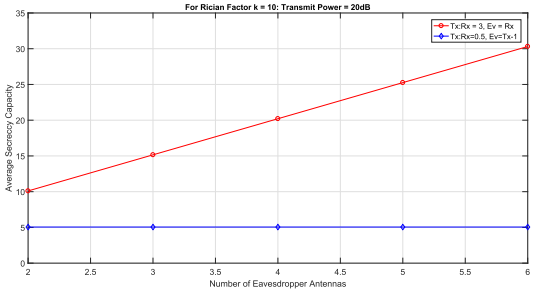


FIGURE 5. Average secrecy capacity against the eavesdropper's antennas.

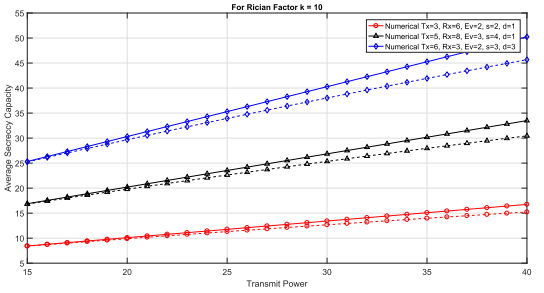


FIGURE 6. Average secrecy capacity for different values of t, r and e (dotted line show the simulation results).

V. SIMULATION RESULTS

To investigate the secrecy capacity of the system described in previous sections, simulations are carried out in Matlab ®. Secrecy capacity was computed for different values of SNR. As the expression of secrecy capacity is computed for high SNR regions, the secrecy capacity is simulated accordingly. Fig. 3 shows the average secrecy capacity of a system with multiple antennas transmitter, receiver, and an eavesdropper. As mentioned in previous sections, the channel between the transmitter-receiver and transmitter-eavesdropper is considered to be a Rician channel. Eavesdropper is a passive device and hence has no effect on the channel as it is not transmitting. We have considered the high SNR scenario and plotted the results for the case $t : r = 2$, and $s = r$. We have simulated for different number of transmit antennas as shown in the legend of Fig. 3. Equal power is considered at each transmit antenna, and perfect CSI is assumed at the receiver. These curves are plotted considering the Rician factor as 10. As it can be seen from the figure the secrecy capacity is increasing almost logarithmically with SNR. Both links are experiencing Rician fading, but due to the effect of AN, the capacity of legitimate link is more than that of illegitimate link resulting in increasing secrecy capacity.

Fig. 4 shows the curves of average secrecy capacity plotted against Rician factor. In this simulation different MIMO scenarios are considered as mentioned in the figure. As mentioned earlier, two power normalization models were considered, which are common in literature. For Model A, $a = \sqrt{\kappa/(\kappa+1)}$ and b= $1/(\kappa+1)$, while for Model B, $a = \sqrt{\kappa}$ and b= 1 is considered. For model A, it can be noticed that all the system mutual information plots decrease monotonically as the Rician factor increases. This is a result of a fixed SNR value. In fact, reduction in the level of scattering adversely affects the MIMO system, which decreases as k increases. The average secrecy capacity is decreasing with increasing Rician factor this is because of the fact that the channel capacity of the legitimate link is decreasing. Hence the eavesdropper's channel capacity is increasing resulting in reduced average secrecy capacity. For model B, the opposite occurs. The average secrecy capacity of the system is increasing with an increase in κ. These results are in accordance with the conclusions made in [30].

Fig. 5 shows the change in average secrecy capacity of the system with an increase in number of eavesdropper's antennas. It can be seen that if adequate number of transmit antennas are considered i.e. $t : r = 3$ and $e = r$, the average secrecy capacity increases with an increase in e. This is due to a high number of transmit antennas and effect of AN. In a case where number of transmit antennas are smaller than number of receive antennas i.e. $t : r = 0.5$ and $e = t - 1$, the system is still able to maintain positive secrecy capacity as it converges to a deterministic constant. These results are also in accordance with the conclusions made in [7], while considering the Rayleigh fading environment.

Moreover, the effect of the change in a ratio of transmit antennas to receive antenna on secrecy capacity of the system investigated. Fig. 6 shows that if the number of transmit antennas is smaller than number of receive antennas, still the system is able to maintain secrecy with optimal selection of s. Three cases were simulated i.e. $t; r; e = 3; 6; 2,\ 5; 3; 8$ and $6; 3; 2$. It can be seen that even with $t : r = 0.5$, the system is able to maintain secrecy which is even increasing with increase in SNR.

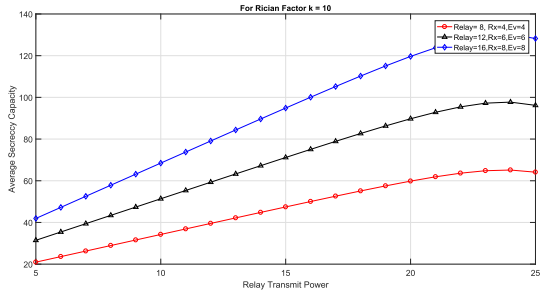


FIGURE 7. Average secrecy capacity vs different relay transmit antennas.

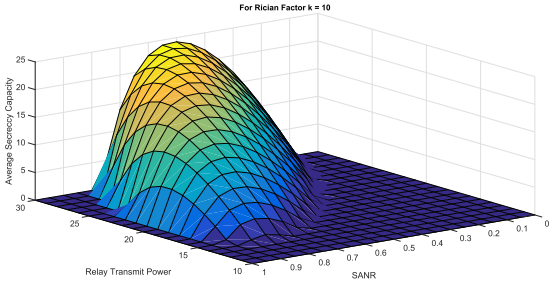


FIGURE 8. Average secrecy capacity vs relay transmit power and SANR.

Fig. 7 shows the secrecy capacity plotted against transmit power P of the relay with a different number of antennas. The signal to artificial noise ratio is fixed at 0.5, the power of the transmitter is set at 20dB and perfect CSI is assumed at the relay node. The power normalization Model B was considered in this simulation. It can be seen that secrecy capacity is increasing almost similar to the scenario without relay, except at higher SNR. At higher SNR the secrecy capacity is increasing in a different way as compared to Fig. 3, it is due to the amplification factor β added by the relay node.

Fig. 8 shows the plot of average secrecy capacity against the relay transmit power and signal to artificial noise ratio. In this simulation it is assumed that transmitter power is 20dB. It can be seen that as the secrecy capacity is increasing with increase power only when a suitable SANR is selected. The AN is main source of degrading the eavesdropper's channel so a reasonable power must be allocated to it.

VI. CONCLUSION

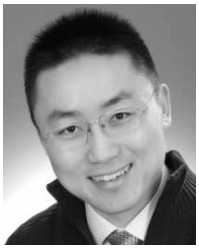
In this paper, the recently proposed strategy, where messages are encoded in s (which is a variable) strongest eigen-subchannels based on ordered eigenvalues of Wishart matrices, while AN signals are generated in remaining spaces, has been extended to Rician channels. Both legitimate link and the illegitimate link were experiencing Rician fading. A closed form expression for the upper bound secrecy capacity of the system was computed using majorization theory. Monte Carlo simulations were carried out to show the performance of the system in terms of average secrecy capacity. The main contribution of this paper is a simple closed form expression for the secrecy capacity MIMO Rician channels obtained using majorization theory. Optimal selection of number of message sending eigenvalues can greatly increase the secrecy capacity of the system. The system can perform well even without knowledge of eavesdropper's channel and number of its antennas. The effect of the Rician factor was also studied and simulation was done to show its effect on the average secrecy capacity of the system. The same system was extended to single relay network and the same processing was done at the relay which allows the source to be a less complex system. Such a system is feasible as the relay can be fixed with less computational and power constraints. Secrecy capacity expression for such a system was computed and simulations were carried out. It was shown that with AN and amplification at the relay node, secrecy capacity of the system can be increased.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[5] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Pers. Commun*, vol. 6, no. 3, pp. 311–335, 1998.
[6] M. Ahmed and L. Bai, "Space time block coding aided physical layer security in Gaussian MIMO channels," in *Proc. 14th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Jan. 2017, pp. 805–808.
[7] Y. Liu, H. Chen, and L. Wang, "Secrecy capacity analysis of artificial noisy MIMO channels—An approach based on ordered eigenvalues of Wishart matrices," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 617–630, Mar. 2017.
[8] S.-H. Lai, P.-H. Lin, S.-C. Lin, and H.-J. Su, "On optimal artificial-noise assisted secure beamforming for the fading eavesdropper channel," in *Proc. IEEE Pers. Indoor Radio Mobile Commun. (PIMRC)*, Sep. 2011, pp. 1167–1171.
[9] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.
[10] S. K. Jayaweera and H. V. Poor, "On the capacity of multiple-antenna systems in Rician fading," *IEEE IEEE Trans. Wireless Commun.*, vol. 4, no. 3, pp. 1102–1111, May 2005.
[11] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.
[12] M. R. A. Khandaker and K.-K. Wong, "Masked beamforming in the presence of energy-harvesting eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 40–54, Jan. 2015.
[13] S.-H. Tsai and H. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.
[14] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3901–3911, Jul. 2015.
[15] M.-A. Khalighi, J. Brossier, G. Jourdain, and K. Raoof, "Water filling capacity of Rayleigh MIMO channels," in *Proc. IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, San Diego, CA, USA, Sep. 2001, pp. 155–158.
[16] G. Lebrun, M. Faulkner, M. Shafi, and P. J. Smith, "MIMO Ricean channel capacity: An asymptotic analysis," *IEEE Trans. Wireless Commun.*, vol. 5, no. 6, pp. 1343–1350, Jun. 2006.
[17] M. R. McKay and I. B. Collings, "General capacity bounds for spatially correlated Rician MIMO channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3121–3145, Sep. 2005.
[18] B. O. Hogstad, G. Rafiq, V. Kontorovitch, and M. Pätzold, "Capacity studies of spatially correlated MIMO Rice channels," in *Proc. 5th IEEE Int. Symp. Wireless Pervasive Comput. (ISWPC)*, May 2010, pp. 45–50.

[19] S. Jin, X. Gao, and X. You, "On the ergodic capacity of rank-1 Ricean-fading MIMO channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 502–517, Feb. 2007.
[20] A. A. P. Guimar and C. C. Cavalcante, "Upper bound of ergodic capacity for MIMO channels with Ricean-fading using Majorization theory," *J. Commun. Inf. Syst.*, vol. 27, no. 1, pp. 10–14, Apr. 2012.
[21] O. Simeone and P. Popovski, "Secure communications via cooperating base stations," *IEEE Commun. Lett.*, vol. 12, no. 3, pp. 188–190, Mar. 2008.
[22] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secrect communication," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Porto, Portugal, May 2008, pp. 164–168.
[23] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[24] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.
[25] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secure broadcasting," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Princeton, NJ, USA, Apr. 2010, pp. 1–6.
[26] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. 44th Annu. Conf. Inf. Sci. Syst. (CISS)*, Sydney, NSW, Australia, Mar. 2010, pp. 1–6.
[27] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[28] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.
[29] A. Paulraj, R. Nabar, and D. Gore, *Introduction to Space-Time Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[30] M. R. McKay and I. B. Collings, "On the capacity of frequency-flat and frequency-selective Rician MIMO channels with single-ended correlation," *IEEE Trans. Wireless Commun.*, vol. 5, no. 8, pp. 2038–2043, Aug. 2006.
[31] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications*. San Francisco, CA, USA: Academic, 1979.
[32] D. P. Palomar and Y. Jiang, "MIMO transceiver design via Majorization theory," *Found. Trends Commun. Inf. Theory*, vol. 3, nos. 4–5, pp. 331–551, 2006.
[33] J. You, Z. Zhong, F. Gao, and G. Wang, "On the conditioning channel capacity of MIMO two-way relay networks against eavesdropper," in *Proc. 10th Int. Conf. Commun. Netw. China (ChinaCom)*, Shanghai, China, Aug. 2015, pp. 199–204.

MANSOOR AHMED received the B.Sc. degree in electronics engineering from the International Islamic University, Islamabad, Pakistan, in 2007, and the M.Sc. degree in communication engineering from Muhammad Ali Jinnah University, Islamabad, in 2009. He is currently pursuing the Ph.D. degree with the School of Electronics and Information Engineering, Beihang University, Beijing, China. Since 2009, he has been a Research Engineer with National Engineering and Scientific Commission, Islamabad. His research interests include wireless communications, channel modeling and estimation, and physical layer security.



LIN BAI (M'13–SM'17) received the B.Sc. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2004, the M.Sc. degree (Hons.) in communication systems from the University of Wales, Swansea, U.K., in 2007, and the Ph.D. degree in advanced telecommunications from the School of Engineering, Swansea University, U.K., in 2010. Since 2011, he has been with the School of Electronics and Information Engineering, Beihang University, Beijing, China, as an Associate Professor/Ph.D. Supervisor. He has authored two books *Low Complexity MIMO Detection* (Springer, 2012) and *Low Complexity MIMO Receivers* (Springer, 2014), respectively. His research interests include signal processing of wireless communications, particularly multiple-input multiple-output (MIMO) systems, array/smart antenna, lattice-based approaches, and non-orthogonal multiple access. He received an IEEE Communications Letters Exemplary Reviewers Certificate for 2012 and the Best Paper Award from ICNS 2013 (Conference). He currently serves as a Lead Guest Editor of the *IEEE Wireless Communication Magazine* and a Guest Editor of the IEEE Internet of Things Journal. He is an Editor/Associate Editor of several academic journals, including the IEEE Wireless Communication Letters, IEEE Access, *IET Communications*, and *KSII Transactions on Internet and Information Systems*, and the Managing Editor of the *Journal of Communications and Information Networks*. He also served as the Guest Editor of the *International Journal of Distributed Sensor Networks* from 2012 to 2014.