Journal of Engineering and Applied Science Vol. 4, No. 1, pp. 10–19, June 2020

Journal of Engineering and Applied Science

Contents are available at www.jeas.ruet.ac.bd

Security in Correlated Cognitive Radio Channels with Interference

T. Kumar, M. Z. I. Sarkar, D. K. Sarker

Department of Electrical & Electronic Engineering, Rajshahi University of Engineering & Technology, Rajshahi-6204, Bangladesh

ARTICLE INFORMATION

Received date: 30 Jun 2019
Revised date: 25 Dec 2019
Accepted date: 02 Feb 2020

Keywords

Antenna correlation
Cognitive radio diversity
Ergodic secrecy capacity
Interference

ABSTRACT

Cognitive radio network is capable of adopting the best wireless channels by dynamic spectrum management avoiding user interference and congestion. In this paper, secure wireless communication scenario is considered through a multiple-input multiple-output (MIMO) cognitive interference radio network over Rayleigh fading channel. It consists of a primary user A, a secondary user C, a primary receiver B, a secondary receiver D and an eavesdropper E. When A communicates with B, it interferes D, and E tries to decode information from A. In a similar manner, when C communicates with D, it interferes B, and E tries to decode information from C. It is assumed that the terminals of users, receivers and eavesdropper all are equipped with correlated multiple antennas. On the basis of these considerations, we derive the closed-form analytical expression of the ergodic secrecy capacity at the receivers with antenna correlations of all terminals. The effects of transmitting and receiving antennas, their correlations and diversities on the ergodic secrecy capacity are investigated in the presence of eavesdropper. In addition, the effect of antenna correlation with interference case is compared with the case of without interference. Moreover, the effects of eavesdropper antennas and their correlations on the ergodic secrecy capacity are also investigated.

1. Introduction

In the recent years, security has become an important issue for wireless communication systems due to the spreading nature of wireless medium and susceptible to eavesdropping [1-5]. On the other hand, the demand of wireless radio is increasing day by day due to the expansion of mobile network applications. But mobile network suffers from a

*Corresponding authors: Department of Electrical & Electronic Engineering, Rajshahi University of Engineering & Technology, Rajshahi-6204, Bangladesh
E-mail address: dks_ms@yahoo.com (D. K. Sarker)

problem of spectrum scarcity, and conventional spectrum allocation method is not able to mitigate this problem. Cognitive radio can be utilized to solve this issue [6-9]. Because it can automatically detect the available channels in a wireless spectrum and thus changes the transmission parameters for enhancing the link quality of radio channels. In the last two decades, multi-antenna transmission and reception technique of wireless signals becomes popular in the world for enhancing the capacity of wireless channels [10-13]. But it suffers from the problem of capacity degradation due to antenna correlations [10,11]. The physical layer security of cognitive radio channel was studied in [1], and derived the closed-form expressions for the exact and asymptotic secrecy outage probability. A cognitive interference network was studied in [2], deriving the expression of secure outage probability. The security-reliability trade-off analysis was carried out for CRN in [3] and derived the closed-form expressions for the secure outage and intercept probability. The analytical expressions of ergodic secrecy capacity of an artificial noise-aided CRN was derived in [4] for investigating the impact of interference of a secondary system on the primary system in the presence of eavesdroppers. Secure communication through a cognitive interference channel was studied in [5], where authors calculate the secrecy rate of the receiver and proposed three cooperative jamming and beamforming techniques together to misguide the eavesdropper and cancel out jamming interference at receivers. The security and reliability performance of cooperative non-orthogonal multiple access cognitive networks was studied in [6] deriving the expressions of connection outage and secure outage probability. The security reliability tradeoff had been investigated for a multiuser scheduling-aided energy harvesting cognitive radio network in [7] and found the expressions of intercept probability and outage probability. The reliability and security performance of cognitive millimeter wave networks had been studied in [8] deriving the expressions of connection outage probability, secure outage probability and secrecy throughput. The secure outage probability performance of a dual-hop energy RF cognitive radio network was studied in [9] over Rayleigh fading channel.

The capacity distribution of spatially correlated, MIMO channels was investigated in [10] and found the expression for the mean value of the capacity for arbitrary correlation matrices. The capacity performance of MIMO Rayleigh-fading channels was analyzed in [11] with spatial fading correlation deriving the characteristic function of the capacity. Two MIMO transmission techniques such as spatial modulation and spatial multiplexing were proposed and studied in [12] to mitigate the adverse effect of interference of spatial modulation. Based on the theory of matrix variate distribution, the capacity of MIMO Rayleigh fading channels was investigated in [13] with Rayleigh co-channel interference and derived the expressions of moment generating function and ergodic capacity. The performance of secure communications over correlated fading channels was studied in [14] and found the expressions for the secrecy capacity and the secure outage probability in the form of infinite series. An analytical framework on the secrecy capability of a CRN was proposed in [16], with transmit and interference power constraint and showed via simulation that the security of CRN can be enhanced employing primary interference power. Recently, the feasibility of interference alignment in MIMO broadcast channels is studied in [15] with antenna correlation and showed that superior performance of a MIMO system can be achieved even under significant antenna correlation. Motivated by all of the above, we, for the first time, analyze the security of a cognitive radio network taking into account the antenna correlation and interference. The contributions of this paper are pointed out as follows;

- we describe the correlated MIMO channels and their PDFs consisting of two transmitting users (primary and secondary), two receivers (primary and secondary) and an eavesdropper considering antenna correlations and mutual interference created by the users.
- defining the ergodic secrecy capacity at the primary receiver, we derive the closed-form analytical expressions for the ergodic secrecy capacity considering antenna correlation at all the terminals without and with interference.
- we investigate the effects of transmitting and receiving antennas, their correlations and diversities on the ergodic secrecy capacity in the presence of eavesdropper. The effects of eavesdropper antennas and their correlations on the ergodic secrecy capacity are also investigated.
- the effect of antenna correlation with interference case is compared with the case of without interference.

The rest of the paper is structured as follows. Section 2 outlines the system model and formulation of the problem. Section 3 describe the formulation of the analytical expressions for the ergodic secrecy capacity. In Section 4, numerical results are presented. Finally, discussion on the analysis is stated in Section 5, and this paper is concluded in Section 6.

Notations: Scalars, vectors and matrices are denoted by lower case, bold lower case and bold upper case letters, respectively. $\mathbf{I}_n$ represents the $n \times n$ identity matrix. The superscript $(\cdot)^\dagger$ stands for the complex conjugate transpose and $\mathbb{E}[\cdot]$ is the expectation operator. $\mathrm{tr}(\cdot)$ and $\det(\cdot)$ denote the trace operator and the determinant, respectively.

2. System Model and Problem Formulation

We consider a MIMO cognitive radio network over Rayleigh fading environment consists of a primary user A, a secondary user C, a primary receiver B, a secondary receiver D and an eavesdropper E is shown in Fig.1. It is desired that A communicates with B and C communicates with D. But while A sends information to B, it interferes D, and E tries to decode information of A. By similar ways, while C sends information to D, it interferes B, and E tries to decode information of C. During communication between user and receiver under the eavesdropper situated nearby the primary and secondary receivers tries to extract information, but it cannot able to get information from the legitimate channels due to secure transmission rate, $\mathscr{R}_s$ of the users. The secure transmission rate can be determined by subtracting the capacity of the eavesdropper's channel from the capacity of the receivers channels [17]. These circumstances are depicted in Figs.2 and 3, respectively. It is assumed that the terminals of A, C, B, D and E are equipped with n_a, n_c, n_b, n_d and n_e correlated antennas, respectively. The channel matrices from A to B and C to B denoted respectively by $\mathbf{H}_{a,b}$

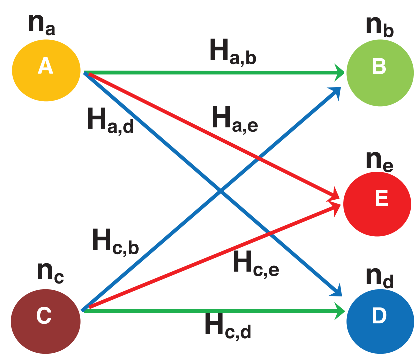

Figure 1. MIMO cognitive radio network with correlated antennas at the primary and secondary terminals.

and $\mathbf{H}_{c,b}$ can be modeled by

$$\mathbf{H}_{a,b} = \Psi_b^{\frac{1}{2}} \mathbf{H}_{ab_0} \Psi_a^{\frac{1}{2}}, \tag{1}$$

$$\mathbf{H}_{c,b} = \Psi_b^{\frac{1}{2}} \mathbf{H}_{cb_0} \Psi_c^{\frac{1}{2}}, \tag{2}$$

where $\mathbf{H}_{ab_0} \sim \tilde{\mathscr{N}}_{n_b,n_a}\left(0, I_{n_b}, I_{n_a}\right)$, $\mathbf{H}_{cb_0} \sim \tilde{\mathscr{N}}_{n_b,n_c}\left(0, I_{n_b}, I_{n_c}\right)$, $\Psi_b \in \mathbb{C}^{n_b \times n_b} > 0$ is the receive correlation matrix at the receiver B and, $\Psi_a \in \mathbb{C}^{n_a \times n_a} > 0$ and $\Psi_c \in \mathbb{C}^{n_c \times n_c} > 0$ denote the transmit correlation matrices at users A and C, respectively. The channel matrices from C to D and A to D denoted respectively by $\mathbf{H}_{c,d}$ and $\mathbf{H}_{a,d}$ can be modeled by

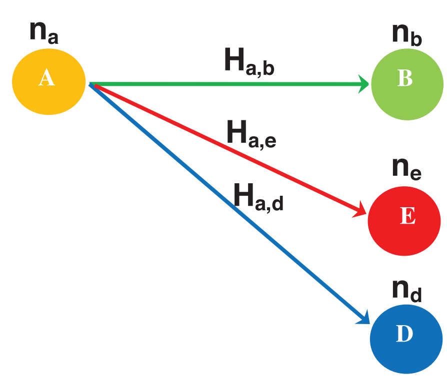

Figure 2. Interference at the secondary receiver due to the signals of primary user.

$$\mathbf{H}_{c,d} = \Psi_d^{\frac{1}{2}} \mathbf{H}_{cd_0} \Psi_c^{\frac{1}{2}}, \tag{3}$$

$$\mathbf{H}_{a,d} = \Psi_d^{\frac{1}{2}} \mathbf{H}_{ad_0} \Psi_a^{\frac{1}{2}}, \tag{4}$$

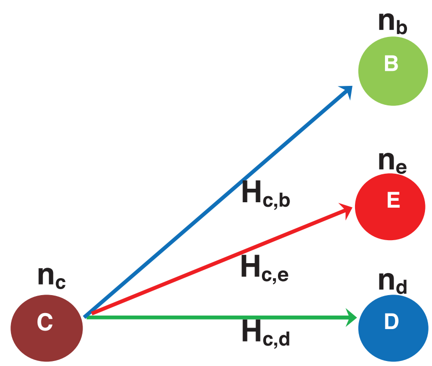

Figure 3. Interference at the primary receiver due to the signals of secondary user.

where $\mathbf{H}_{cd_0} \sim \tilde{\mathcal{N}}_{n_d,n_c}\left(0, I_{n_d}, I_{n_c}\right)$, $\mathbf{H}_{ad_0} \sim \tilde{\mathcal{N}}_{n_d,n_a}\left(0, I_{n_d}, I_{n_a}\right)$, $\Psi_d \in \mathbb{C}^{n_d \times n_d} > 0$ is the receive correlation matrix at the receiver, D. The channel matrices from A to E and C to E denoted respectively by $\mathbf{H}_{a,e}$ and $\mathbf{H}_{c,e}$ can be modeled by

$$\mathbf{H}_{a,e} = \Psi_e^{\frac{1}{2}} \mathbf{H}_{ae_0} \Psi_a^{\frac{1}{2}}, \tag{5}$$

$$\mathbf{H}_{c,e} = \Psi_e^{\frac{1}{2}} \mathbf{H}_{ce_0} \Psi_c^{\frac{1}{2}}, \tag{6}$$

where $\mathbf{H}_{ae_0} \sim \tilde{\mathcal{N}}_{n_e,n_a}(0, I_{n_e}, I_{n_a})$, $\mathbf{H}_{ce_0} \sim \tilde{\mathcal{N}}_{n_e,n_c}(0, I_{n_e}, I_{n_c})$, $\Psi_e \in \mathbb{C}^{n_e \times n_e} > 0$ is the receive correlation matrix at the receiver, E.

2.1. Received Signal Vectors at the Receivers and Eavesdroppers

The received signal vectors at B, D and E denoted respectively by $\mathbf{y_b} \in \mathbb{C}^{n_b \times 1}$, $\mathbf{y_d} \in \mathbb{C}^{n_d \times 1}$ and $\mathbf{y_e} \in \mathbb{C}^{n_e \times 1}$ can be expressed as

$$\mathbf{y}_b = \sqrt{P_a}\mathbf{H}_{a,b}\mathbf{x}_a + \sqrt{P_c}\mathbf{H}_{c,b}\mathbf{x}_c + \mathbf{z_b}, \tag{7}$$

$$\mathbf{y}_d = \sqrt{P_c}\mathbf{H}_{c,d}\mathbf{x}_c + \sqrt{P_a}\mathbf{H}_{a,d}\mathbf{x}_a + \mathbf{z_d}, \tag{8}$$

$$\mathbf{y}_e = \sqrt{P_a}\mathbf{H}_{a,e}\mathbf{x}_a + \sqrt{P_c}\mathbf{H}_{c,e}\mathbf{x}_c + \mathbf{z_e}. \tag{9}$$

where $\mathbf{x_a} \in \mathbb{C}^{n_a \times 1}$ and $\mathbf{x_c} \in \mathbb{C}^{n_c \times 1}$ are the transmitted signal vectors from A and C respectively. P_a denotes the power at user A and P_c denotes the power at user C. $\mathbf{z}_b$, $\mathbf{z}_d$ and $\mathbf{z}_e$ are the n_b, n_d and n_e dimensional additive white Gaussian noise (AWGN) vectors at B, D and E respectively. The transformation from $\mathbf{H}_{a_0}$ to $\mathbf{H}_{a,b}$, $\mathbf{H}_{c_0}$ to $\mathbf{H}_{c,b}$, $\mathbf{H}_{c_0}$ to $\mathbf{H}_{c,d}$, $\mathbf{H}_{a_0}$ to $\mathbf{H}_{a,d}$, $\mathbf{H}_{a_0}$ to $\mathbf{H}_{a,e}$ and $\mathbf{H}_{c_0}$ to $\mathbf{H}_{c,e}$ with the Jacobian yield respectively $\mathbf{H}_{a,b} \sim \tilde{\mathcal{N}}_{n_b,n_a}\left(0, \Psi_{n_b}, \Psi_{n_a}\right)$, $\mathbf{H}_{c,b} \sim \tilde{\mathcal{N}}_{n_b,n_c}\left(0, \Psi_{n_b}, \Psi_{n_c}\right)$, $\mathbf{H}_{c,d} \sim \tilde{\mathcal{N}}_{n_d,n_c}\left(0, \Psi_{n_d}, \Psi_{n_c}\right)$, $\mathbf{H}_{a,d} \sim \tilde{\mathcal{N}}_{n_d,n_a}\left(0, \Psi_{n_d}, \Psi_{n_a}\right)$, $\mathbf{H}_{a,e} \sim \tilde{\mathcal{N}}_{n_e,n_a}(0, \Psi_{n_e}, \Psi_{n_a})$ and $\mathbf{H}_{c,e} \sim \tilde{\mathcal{N}}_{n_e,n_c}\left(0, \Psi_{n_e}, \Psi_{n_c}\right)$.

2.2. Probability Density Functions of the Channel Matrices

The probability density functions (pdfs) of the channel matrices from A to B, A to D and A to E are given respectively by [18]

$$f_{\mathbf{H_{a,b}}}(\mathbf{H_{a,b}}) = \pi^{-n_a n_b} \det(\Psi_b)^{-n_a} \det(\Psi_a)^{-n_b} e^{-tr(\Psi_b^{-1}\mathbf{H_{a,b}}\Psi_a^{-1}\mathbf{H}_{\mathbf{a,b}}^{\dagger})}, \tag{10}$$

$$f_{\mathbf{H_{a,d}}}(\mathbf{H_{a,d}}) = \pi^{-n_a n_d} \det(\Psi_d)^{-n_a} \det(\Psi_a)^{-n_d} e^{-tr(\Psi_d^{-1}\mathbf{H_{a,d}}\Psi_a^{-1}\mathbf{H}_{\mathbf{a,d}}^{\dagger})}, \tag{11}$$

$$f_{\mathbf{H_{a,e}}}(\mathbf{H_{a,e}}) = \pi^{-n_a n_e} \det(\Psi_e)^{-n_a} \det(\Psi_a)^{-n_e} e^{-tr(\Psi_e^{-1}\mathbf{H_{a,e}}\Psi_a^{-1}\mathbf{H}_{\mathbf{a,e}}^{\dagger})}. \tag{12}$$

The pdf of the channel matrices from C to D, C to B and C to E are given respectively by

$$f_{\mathbf{H_{c,d}}}(\mathbf{H_{c,d}}) = \pi^{-n_c n_d}\det(\Psi_d)^{-n_c}\det(\Psi_c)^{-n_d} e^{-tr(\Psi_d^{-1}\mathbf{H_{c,d}}\Psi_c^{-1}\mathbf{H}_{\mathbf{c,d}}^{\dagger})}, \tag{13}$$

$$f_{\mathbf{H_{c,b}}}(\mathbf{H_{c,b}}) = \pi^{-n_c n_b}\det(\Psi_b)^{-n_c}\det(\Psi_c)^{-n_b} e^{-tr(\Psi_b^{-1}\mathbf{H_{c,b}}\Psi_c^{-1}\mathbf{H}_{\mathbf{c,b}}^{\dagger})}, \tag{14}$$

$$f_{\mathbf{H_{c,e}}}(\mathbf{H_{c,e}}) = \pi^{-n_c n_e}\det(\Psi_e)^{-n_c}\det(\Psi_c)^{-n_e} e^{-tr(\Psi_e^{-1}\mathbf{H_{c,e}}\Psi_c^{-1}\mathbf{H}_{\mathbf{c,e}}^{\dagger})}. \tag{15}$$

3. Ergodic Secrecy Capacity

In this section, taking into account the realistic propagation environments such as spatial fading correlation, we provide analytical expressions for the ergodic secrecy capacity of cognitive MIMO networks without and with interference.

3.1 Ergodic secrecy capacity without interference

From equations (10) and (12), the ergodic secrecy capacity at the receiver, B can be expressed as

$$\begin{aligned}\langle C_s\rangle &= \mathbb{E}\left[\ln\det\left(I_{n_b} + \gamma_b \mathbf{H_{a,b}}\mathbf{H}_{\mathbf{a,b}}^{\dagger}\right)\right] - \mathbb{E}\left[\ln\det\left(I_{n_e} + \gamma_e \mathbf{H_{a,e}}\mathbf{H}_{\mathbf{a,e}}^{\dagger}\right)\right] \\ &= \ln\left[\sum_{k=0}^{\min(n_b,n_a)} \gamma_b^k k! \sum_{1\le i_1\cdots<i_{k\le n_a}} \det\left(\Psi_{a\,i_1,i_2\cdots i_k}^{\;i_1,i_2\cdots i_k}\right) \sum_{1\le u_1\cdots<u_{k\le n_b}} \det\left(\Psi_{b\,u_1,u_2\cdots u_k}^{\;u_1,u_2\cdots u_k}\right)\right] \\ &\quad - \ln\left[\sum_{l=0}^{\min(n_e,n_a)} \gamma_e^l l! \sum_{1\le j_1\cdots<j_{l\le n_a}} \det\left(\Psi_{a\,j_1,j_2\cdots j_l}^{\;j_1,j_2\cdots j_l}\right) \sum_{1\le v_1\cdots<v_{l\le n_e}} \det\left(\Psi_{e\,v_1,v_2\cdots v_l}^{\;v_1,v_2\cdots v_l}\right)\right].\end{aligned} \tag{16}$$

where γ_b and γ_e are the average SNRs for the channels $\mathbf{H_{a,b}}$ and $\mathbf{H_{a,e}}$, respectively. The transmit correlation matrix at A with correlation coefficient $\xi_{n_a} \in [0,1)$, denoted by $\Phi_{n_a}(\xi_{n_a})$ and its' determinant denoted by $\det(\Psi_a)$ can be expressed as

$$\det(\Psi_a) = \Phi_{n_a}(\xi_a) = \begin{bmatrix} 1 & \xi_a & \xi_a & \cdots & \xi_a \\ \xi_a & 1 & \xi_a & \cdots & \xi_a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_a & \xi_a & \xi_a & \cdots & 1 \end{bmatrix}_{n_a\times n_a}. \tag{17}$$

Since eigenvalues of $\Phi_{n_a}(\xi_a)$ are $1+(n_a-1)\xi_a$ and $1-\xi_a$ with n_a-1 multiplicities, its determinant can be written as

$$\det(\Psi_a) = \det(\Phi_{n_a}(\xi_a)) = (1-\xi_a)^{n_a-1}(1-\xi_a+n_a\xi_a). \tag{18}$$

For kth and lth order transmit correlation matrices, their determinant can be written respectively as

$$\det\left(\Psi_{a\,i_1,i_2\cdots i_k}^{\;i_1,i_2\cdots i_k}\right) = \det(\Phi_{n_a}(\xi_a)) = (1-\xi_a)^{k-1}(1-\xi_a+k\xi_a), \tag{19}$$

$$\det\left(\Psi_{a\,j_1,j_2\cdots j_l}^{\;j_1,j_2\cdots j_l}\right) = \det(\Phi_{n_a}(\xi_a)) = (1-\xi_a)^{l-1}(1-\xi_a+l\xi_a). \tag{20}$$

The receive correlation matrices at B and E with correlation coefficient $\xi_{n_b} \in [0,1)$ and $\xi_{n_e} \in [0,1)$, denoted by $\Phi_{n_b}(\xi_{n_b})$ and $\Phi_{n_e}(\xi_{n_e})$, and it's determinant denoted by $\det(\Psi_b)$ and $\det(\Psi_e)$ can be expressed respectively as

$$\det(\Psi_b) = \Phi_{n_b}(\xi_b) = \begin{bmatrix} 1 & \xi_b & \xi_b & \cdots & \xi_b \\ \xi_b & 1 & \xi_b & \cdots & \xi_b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_b & \xi_b & \xi_b & \cdots & 1 \end{bmatrix}_{n_b\times n_b}, \tag{21}$$

and

$$\det(\Psi_e) = \Phi_{n_e}(\xi_e) = \begin{bmatrix} 1 & \xi_e & \xi_e & \cdots & \xi_e \\ \xi_e & 1 & \xi_e & \cdots & \xi_e \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_e & \xi_e & \xi_e & \cdots & 1 \end{bmatrix}_{n_e\times n_e}. \tag{22}$$

Hence,

$$\det(\Psi_b) = \det\left(\Phi_{n_b}(\xi_b)\right) = (1-\xi_b)^{n_b-1}(1-\xi_b+n_b\xi_b), \tag{23}$$

$$\det(\Psi_e) = \det(\Phi_{n_e}(\xi_e)) = (1-\xi_e)^{n_e-1}(1-\xi_e+n_e\xi_e). \tag{24}$$

For kth and lth order receive correlation matrices, their determinant can be expressed respectively as

$$\det\left(\Psi_{b\,u_1,u_2\cdots u_k}^{\;u_1,u_2\cdots u_k}\right) = \det\left(\Phi_{n_b}(\xi_b)\right) = (1-\xi_b)^{k-1}(1-\xi_b+k\xi_b), \tag{25}$$

$$\det\left(\Psi_{e\,v_1,v_2\cdots v_l}^{\;v_1,v_2\cdots v_l}\right) = \det(\Phi_{n_e}(\xi_e)) = (1-\xi_e)^{l-1}(1-\xi_e+l\xi_e). \tag{26}$$

Substituting equations (19), (20), (25) and (26) into equation (16) yields

$$\begin{aligned}\langle C_s\rangle = \ln&\left[\sum_{k=0}^{\min(n_b,n_a)} \gamma_b^k k!\binom{n_a}{k}\binom{n_b}{k}\{(1-\xi_a)(1-\xi_b)\}^{k-1}\{1+(k-1)\xi_a\}\{1+(k-1)\xi_b\}\right]\\ -\ln&\left[\sum_{l=0}^{min(n_e,n_a)} \gamma_e^l l!\binom{n_a}{l}\binom{n_e}{l}\{(1-\xi_a)(1-\xi_e)\}^{l-1}\{1+(l-1)\xi_a\}\{1+(l-1)\xi_e\}\right].\end{aligned} \tag{27}$$

3.2 Ergodic secrecy capacity with interference

From equations (10), (14) and (12), the ergodic secrecy capacity at the receiver, B can be expressed as

$$\begin{aligned}\langle C_s\rangle^{int} &= \mathbb{E}\left[\ln\det\left(I_{n_b}+\gamma_b\mathbf{H_{a,b}}\mathbf{H_{a,b}^\dagger}\right)\right]^{int} - \mathbb{E}\left[\ln\det\left(I_{n_e}+\gamma_e\mathbf{H_{a,e}}\mathbf{H_{a,e}^\dagger}\right)\right]^{int}\\ &= \ln\left[\sum_{g=0}^{\min(n_b,n_a+n_c)} \gamma_b^g g! \sum_{1\le f_1\cdots<f_{g\le n_a}} \det\left(\Psi_{a,c\,f_1,f_2\cdots f_g}^{\;\;f_1,f_2\cdots f_g}\right) \sum_{1\le h_1\cdots<h_{g\le n_b}} \det\left(\Psi_{b\,h_1,h_2\cdots h_g}^{\;h_1,h_2\cdots h_g}\right)\right]\\ &\quad -\ln\left[\sum_{s=0}^{\min(n_e,n_a+n_c)} \gamma_e^s s! \sum_{1\le r_1\cdots<r_{s\le n_a}} \det\left(\Psi_{a,c\,r_1,r_2\cdots r_s}^{\;\;r_1,r_2\cdots r_l}\right) \sum_{1\le t_1\cdots<t_{s\le n_e}} \det\left(\Psi_{e\,t_1,t_2\cdots t_s}^{\;t_1,t_2\cdots t_s}\right)\right].\end{aligned} \tag{28}$$

where $\Psi_{a,c} \in \mathbb{C}^{(n_a+n_c)\times(n_a+n_c)} > 0$ denote the mutual transmit correlation matrix between users A and C with correlation coefficient $\xi_{(n_a+n_c)} \in [0,1)$, denoted by $\Phi_{(n_a+n_c)}(\xi_{(n_a+n_c)})$ and its' determinant denoted by $\det(\Psi_{a,c})$ can be expressed as

$$\det(\Psi_{a,c}) = \Phi_{(n_a+n_c)}(\xi_{ac}) = \begin{bmatrix} 1 & \xi_{ac} & \xi_{ac} & \cdots & \xi_{ac}\\ \xi_{ac} & 1 & \xi_{ac} & \cdots & \xi_{ac}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ \xi_{ac} & \xi_{ac} & \xi_{ac} & \cdots & 1 \end{bmatrix}_{(n_a+n_c)\times(n_a+n_c)}. \tag{29}$$

Since eigenvalues of $\Phi_{(n_a+n_c)}(\xi_{ac})$ are $1+(n_a+n_c-1)\xi_{ac}$ and $1-\xi_{ac}$ with n_a+n_c-1 multiplicities, its determinant can be written as

$$\det(\Psi_{a,c}) = \det\left(\Phi_{(n_a+n_c)}(\xi_{ac})\right) = (1-\xi_{ac})^{n_a+n_c-1}\{1-\xi_{ac}+(n_a+n_c)\xi_{ac}\}. \tag{30}$$

For gth and sth order mutual transmit correlation matrices, their determinant can be written respectively as

$$\det\left(\Psi_{a,c\,f_1,f_2\cdots f_g}^{\;\;f_1,f_2\cdots f_g}\right) = \det\left(\Phi_{(n_a+n_c)}(\xi_{ac})\right) = (1-\xi_{ac})^{g-1}\{1-\xi_{ac}+g\xi_{ac}\}, \tag{31}$$

$$\det\left(\Psi_{a,c\,r_1,r_2\cdots r_s}^{\;\;r_1,r_2\cdots r_l}\right) = \det\left(\Phi_{(n_a+n_c)}(\xi_{ac})\right) = (1-\xi_{ac})^{s-1}\{1-\xi_{ac}+s\xi_{ac}\}. \tag{32}$$

By similar ways as equations (25) and (26), for gth and sth order receive correlation matrices, their determinant can be written respectively as

$$\det\left(\Psi_{b\,h_1,h_2\cdots h_g}^{\;h_1,h_2\cdots h_g}\right) = \det\left(\Phi_{n_b}(\xi_b)\right) = (1-\xi_b)^{g-1}(1-\xi_b+g\xi_b), \tag{33}$$

$$\det\left(\Psi_{e\,t_1,t_2\cdots t_s}^{\;t_1,t_2\cdots t_s}\right) = \det(\Phi_{n_e}(\xi_e)) = (1-\xi_e)^{s-1}(1-\xi_e+s\xi_e). \tag{34}$$

Substituting equations (31), (32), (33) and (34) into equation (28) yields

$$\langle C_s\rangle^{int} = \ln\left[\sum_{g=0}^{\min(n_b,n_a+n_c)} \gamma_b^g g!\binom{n_a+n_c}{g}\binom{n_b}{g}\{(1-\xi_{ac})(1-\xi_b)\}^{g-1}\{1+(g-1)\xi_{ac}\}\{1+(g-1)\xi_b\}\right]$$
$$-\ln\left[\sum_{s=0}^{min(n_e,n_a+n_c)} \gamma_e^s s!\binom{n_a+n_c}{s}\binom{n_e}{s}\{(1-\xi_{ac})(1-\xi_e)\}^{s-1}\{1+(s-1)\xi_{ac}\}\{1+(s-1)\xi_e\}\right]. \quad (35)$$

4. Numerical Results

In this section, we present the numerical results obtained from the closed-form analytical expressions of equations (27) and (35) described in Section 3. These are newly derived equations incorporating the antenna correlation parameter in the analysis of security performance of cognitive radio interference network, which are absent in the previous works related to the security of cognitive radio networks [6-9]. Throughout the investigations, we consider the value of correlation coefficient, ξ from 0.1 to 0.99 and the average SNR at the receivers are varied from -10dB to 35dB. The effect of correlation on the ergodic secrecy capacity has been investigated with interference of one user to another and without interference.

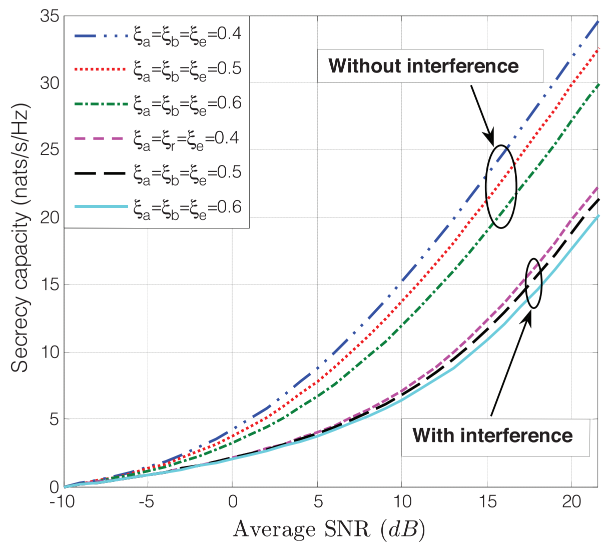

Figure 4. The analytical results of ergodic secrecy capacity versus average SNR of primary channel with and without interference, with $n_a = n_c = 8$, $n_b = n_e = 12$, $\xi_{ac} = 0.95$ and γ_e=-10dB.

Fig.4 illustrates, the ergodic secrecy capacity as a function of average SNR of primary channel (i.e., the channel between primary user and primary receiver) for investigating the effect of antenna correlations with and without interference. In order to show the effect of correlations and interference, the correlation parameters ξ_a, ξ_b and ξ_e are varied from 0.4 to 0.6. It is observed that ergodic secrecy capacity decreases with the increase of the correlation parameters and interference. It is also noticed that although ergodic secrecy capacity significantly decreases with the interference of other channels, but the effect correlation is substantially reduced in the presence of interference.

The analytical results of the ergodic secrecy capacity as a function of average SNR of primary receiver is shown in Fig.5 with $\xi_a = \xi_b = \xi_c = 0.7$, $n_e = 3$ and γ_e=-10dB for investigating the effects of spatial diversity on the ergodic secrecy capacity. From this figure we can see that ergodic secrecy capacity increases significantly with the increase of the number of transmitting and receiving antennas. This enhancement of ergodic secrecy capacity is due to transmit/receive diversity i.e., spatial diversity provided by simultaneous cooperation of transmitting and receiving antennas. It is also observed that the rate of capacity enhancement reduces gradually with the increase of the number of transmitting and receiving antennas.

Fig.6 depicts the analytical results of ergodic secrecy capacity as a function of average SNR of primary channel to show the effects of eavesdropper antenna, n_e and correlation coefficient, ξ_e on the ergodic secrecy capacity. In the first

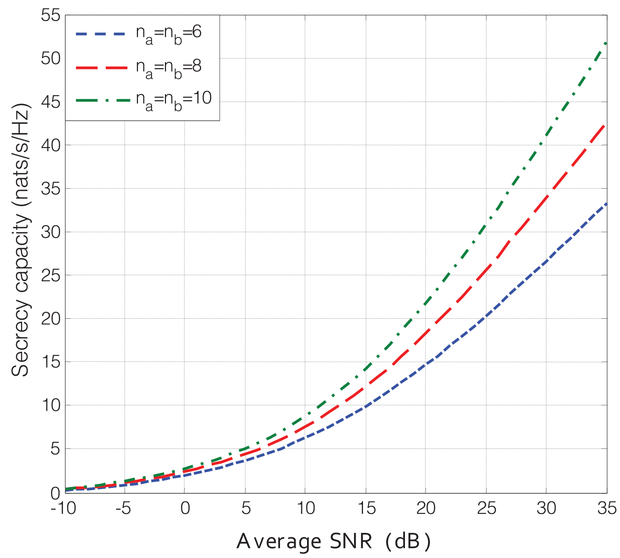

Figure 5. The analytical results of ergodic secrecy capacity as a function of average SNR of the primary receiver with $\xi_a = \xi_b = \xi_c = 0.7$, $n_e = 3$ and γ_e=-10dB.

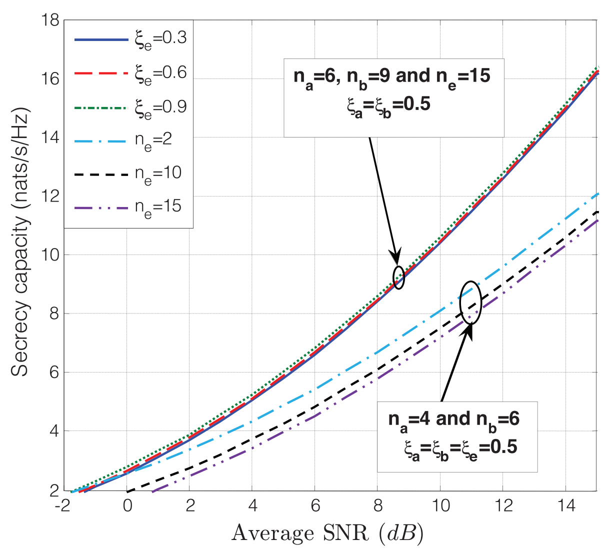

Figure 6. The analytical results of ergodic secrecy capacity versus average SNR of primary channel with n_a=4, n_b=6 and $\xi_a = \xi_b = \xi_e = 0.5$ and, $n_a = 6$, $n_b = 9$, $n_e = 15$ and $\xi_a = \xi_b = 0.5$.

case, the value of $n_e =$ is taken as 2, 10 and 15 with $n_a = 4$, $n_b = 6$ and $\xi_a = \xi_b = \xi_e = 0.5$, and in the second case, the value of $\xi_e =$ is considered as 0.3, 0.6 and 0.9. Observing these two cases, we can see that the secrecy capacity significantly decreases with n_e and slightly increases with ξ_e.

The analytical results of ergodic secrecy capacity as a function of average SNR of primary channel is shown in Fig.7 for investigating the effects of transmit and receive correlations ξ_a and ξ_b on the ergodic secrecy capacity. In these observations, both the transmit and receive correlations are considered as 0.2, 0.5 and 0.8. From our investigations, we can see that the effects of ξ_a and ξ_b are almost same and both these two effects play substantial role in the decrement of the secrecy capacity of wireless channels.

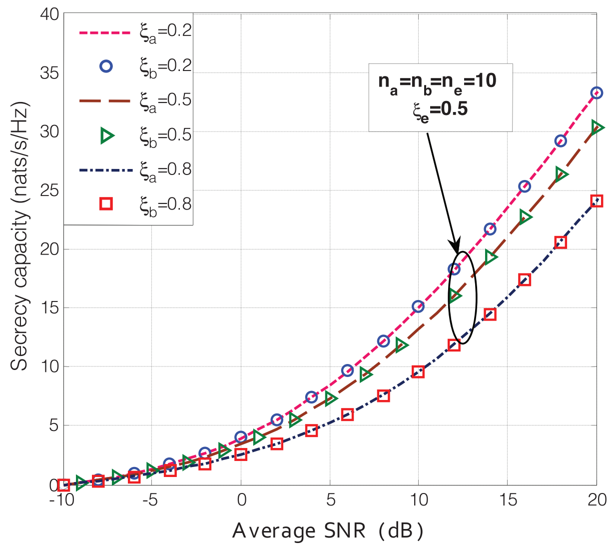

Figure 7. The analytical results of ergodic secrecy capacity versus average SNR of primary channel with $n_a = n_b = n_e = 10$ and $\xi_e = 0.5$.

5. Discussion

We derive the closed-form analytical expression for the ergodic secrecy capacity at the receivers of a MIMO cognitive interference radio network considering antenna correlation at the terminals of cognitive radio networks. The effects of transmitting and receiving antennas, their correlations and diversities on the ergodic secrecy capacity are investigated in the presence of an eavesdropper. The effect of antenna correlations with interference case is also compared with the case of without interference. In addition, the effects of eavesdropper antennas and their correlations on the ergodic secrecy capacity are investigated. Although, ergodic secrecy capacity of cognitive radio network significantly decreases with interference, but the effect correlation is substantially reduced in the presence of interference. The enhancement in ergodic secrecy capacity of a MIMO cognitive radio network is due to the transmit/receive diversity i.e., spatial diversity provided by simultaneous cooperation of transmitting and receiving antennas. The effects of correlations of transmitting and receiving antennas are almost same and both of them play a substantial role in the decrease of the secrecy capacity of wireless channels.

6. Conclusion

The Key contribution of this paper is to derive the closed-form analytical expression for the ergodic secrecy capacity at the receivers of a MIMO cognitive interference radio network considering antenna correlations at the terminals of cognitive radio networks. Based on our observations and from the numerical results, it can be concluded that although, ergodic secrecy capacity of a MIMO channels can be appreciably enhanced by increasing the number of transmitting/receiving antennas, but spatial correlation effect of antennas significantly reduces the ergodic secrecy capacity of a MIMO cognitive interference radio network. As the effect correlation is reduced in the presence of interference, so a MIMO network system (which suffers from correlation effect) will be suitable for interference channel scenarios. Moreover, a tradeoff between the number of transmitting/receiving antennas and correlation is necessary for achieving better performance from a MIMO cognitive interference radio network.

References

[1] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, A. Nallanathan, "On the security of cognitive radio networks", Transactions on Vehicular Technology, IEEE, Vol.64, No.8, pp.3790 – 3795, 2015.

[2] Z. Shu, Y. Yang, Y. Qian, R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network", in Proc. IEEE Global Telecommunications Conference (GLOBECOM 2011), 2011, pp.1–6.

[3] J. Zhu, "Security-reliability trade-off for cognitive radio networks in the presence of eavesdropping attack", Journal on Advances in Signal Processing, EURASIP, Vol.1, pp.169, 2013.

[4] V. Nguyen, T. M. Hoang, O. Shin, “Secrecy capacity of the primary system in a cognitive radio network”, Transactions on Vehicular Technology, IEEE, Vol.64, No.8, pp.3834 – 3843, 2015.

[5] W. Liu, M. Z. I. Sarkar, T. Ratnarajah, H. Du, “Securing cognitive radio with a combined approach of beamforming and cooperative jamming”, Communications, IET, Vol.11, No.1, pp.1–9, 2017.

[6] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou, and R.Q. Hu, “Security-reliability Tradeoff analysis for cooperative NOMA in cognitive radio networksŤ, Transactions on Communications, IEEE, Vol.67, No.1, pp.83–96, 2019.

[7] X. Ding , Y. Zou , G. Zhang , X. Chen, X. Wang, and L. Hanzo, “The securityŰreliability tradeoff of multiuser scheduling-aided energy harvesting cognitive radio networksŤ, Transactions on Communications, IEEE, Vol.67, No.6, pp.3890–3904, 2019.

[8] Y. Song, W. Yang, X. Yang, Z. Xiang, and B. Wang, “Physical layer security in cognitive millimeter wave networksŤ, IEEE Access, IEEE, Vol.7, pp.109162–109180, 2019.

[9] M. Bouabdellah, F. E. Bouanani, P. C. Sofotasios, S. Muhaidat, D. Benevides D. Costa , K. Mezher, H. Ben-Azza, and G. K. Karagiannidis, “Cooperative energy harvesting cognitive radio networks with spectrum sharing and security constraintsŤ, IEEE Access, IEEE, Vol.7, pp.173329–173343, 2019.

[10] M. Chiani, M. Z. Win, A. Zanella, “On the capacity of spatially correlated MIMO Rayleigh-fading channels”, Transactions on Information Theory, IEEE, Vol.49, No.10, pp.2363–2371, 2003.

[11] H. Shin, M. Z. Win, J. H. Lee, M. Chiani, “On the capacity of doubly correlated MIMO channels”, Transactions on Wireless Communications, IEEE, Vol.5, No.8, pp.2253–2265, 2006.

[12] D. A. Basnayaka, H. Haas, “MIMO interference channel between spatial multiplexing and spatial modulation”, Transactions on Communications, IEEE, Vol.64, No.8, pp.3369–3381, 2016.

[13] Y. Wang, D.-W. Yue, “Capacity of MIMO Rayleigh fading channels in the presence of interference and receive correlation”, Transactions on Vehicular Technology, IEEE, Vol.58, No.8, pp.4398 – 4405, 2009.

[14] X. Sun, J. Wang, W. Xu, C. Zhao, “Performance of secure communications over correlated fading channels”, Signal Processing Letters, IEEE, Vol.19, No.8, pp.479–482, 2012.

[15] G. Nauryzbayev, E. Alsusa, M. Abdallah, “On the feasibility of interference alignment in compounded MIMO broadcast channels with antenna correlation and mixed user classes”, Transactions on Vehicular Technology, IEEE, Vol.67, No.3, pp.2130 – 2140, 2018.

[16] K. H.Van, T. D. Dac, “Impact of primary interference on secrecy performance of physical layer security in cognitive radio networks”, Wireless Personal Communications, Springer, pp.1099–1127, 2018.

[17] M. S. A. D. K. Sarker, M. Z. I. Sarkar, “Secure wireless multicasting with linear equalization”, Physical Communication, Elsevier, Vol.25, No.1, pp.201–2013, 2017.

[18] H. Shin, “Capacity and error exponents for multiple-input multipleo-utput wireless channels”, Ph.D. thesis, Seoul National University, Seoul, Korea, 2004.