On Physical Layer Security of Correlated Multiantenna Cognitive Radio Receivers

Brijesh Soni*, Dhaval K. Patel*, Sagar Kavaiya*, Mazen O. Hasna†, Miguel López-Benítez‡
*School of Engineering and Applied Science, Ahmedabad University, India
†Department of Electrical Engineering, Qatar University, Doha.
‡Department of Electrical Engineering and Electronics, University of Liverpool, United Kingdom
‡ARIES Research Centre, Antonio de Nebrija University, Madrid, Spain
Email:*{brijesh.soni, dhaval.patel, sagar.k}@ahduni.edu.in, †hasna@qu.edu.qa, ‡M.Lopez-Benitez@liverpool.ac.uk

***Abstract*—In limited space scenarios, the antennas in the multiantenna cognitive radio (CR) system are closely spaced and often experience correlation among them. In this work, the secrecy performance of correlated multiantenna CR receiver over Nakagami-m fading channels with imperfect channel state information is studied and analyzed. We consider the underlay CR paradigm wherein Alice in the secondary network communicates with Bob while Eve tries to overhear the communication. We also consider that the antennas at Bob and Eve are closely spaced and thus uniformly correlated. To this extent, we derive the analytical expressions for the first and second order secrecy measures like secrecy outage probability, average secrecy outage rate & average secrecy outage duration, respectively for the CR receiver. Moreover, in order to gain insights at high SNR, asymptotic analysis of secrecy outage probability is derived, thus obtaining the secrecy diversity gain of order L_D (i.e., the number of antennas at Bob). Monte Carlo simulations are carried out to validate the proposed analytical framework.**

***Index Terms*—Physical layer security, multiantenna, secrecy outage probability, and average secrecy outage rate.**

I. Introduction

Due to the broadcasting nature of wireless medium, communication systems are often susceptible to eavesdropping. Thus, secured communications have always been of major concern [1]. Conventional cryptography techniques implemented at the higher OSI layers are robust and efficient [2]. However, for network architectures where the devices are of low complexities, for instance in fifth-generation (5G) and beyond wireless networks, issues of key management or computational complexity make the use of data encryption difficult [3]. In such scenarios, physical layer security (PLS) has been considered as a promising approach to better realize the secured communications [4].

Owing to the fact that 5G and beyond wireless networks pose significant demand on limited spectrum resource, cognitive radio (CR) communications has emerged as a potential solution that opportunistically utilizes the idle licensed spectrum bands [5]. CR users often use diversity branches to combat the effect of fading. However, due to multiple wireless links, multiantenna CR systems are prone to interception by an eavesdropper [6]. There have been a plethora of works in literature that have analysed the PLS for multiantenna CR systems, for instance in [7]–[10]. However, the aforementioned works have assumed the antennas to be spaced apart and thus spatially uncorrelated.

As the diversity branches in the multiantenna system increases, and due to space limitation in specific scenarios, for instance, in vehicular applications, antennas become closely spaced. In such scenarios, inter-branch correlation among them cannot be neglected [11], [12]. Few works in the literature have studied the effect of antenna correlation on the secrecy performance, for instance in [13]–[16]. However, the above works were mainly concerned with non CR multiantenna systems.

All the aforementioned work in the literature considered the legitimate transmitter, receiver and eavesdropper to be static. The key secrecy measures presented in the literature for such system are primarily the secrecy outage probability (SOP) and secrecy capacity (C_s), also known as first order statistics [17]. Recently, there have been few works, for instance [18]- [19], that have analysed PLS for vehicular networks. However, to gain better insights on the performance of such systems, the second order statistics like average secrecy outage rate (ASOR) and average secrecy outage duration (ASOD) are more useful [17]. Although SOP provides the idea about the secured link level connection where the channel can support a certain rate, it fails to provide the idea about the average length (realizations) over which a secured communication cannot be established. Moreover, when the user nodes are mobile, the second order secrecy measures like ASOR and ASOD helps to gain better insights into the system design [20]. To the best of the authors' knowledge, the analysis of impact of correlation among closely spaced multiantenna CR receiver from the first order (SOP) and second order secrecy measures (ASOR and ASOD) viewpoint is yet to be reported in literature. The contributions of our work are threefold and can be summarized as:

- First, a comprehensive analysis of first order secrecy measures like SOP is presented for the uniformly correlated. CR antennas at Bob and Eve. Additionally, the effect of imperfect CSI is also taken into account.
- Secondly, in order to gain insights at high SNR, asymptotic analysis of SOP is carried out, thus obtaining the secrecy diversity gain of order L_D.
- Thirdly, the performance analysis of second order secrecy measures like ASOR and ASOD is carried out for the considered system model. These expressions are useful to draw insights for the multiantenna CR enabled vehicles.

The rest of this paper is organized as follows: Section II describes the system and channel models. Section III describes

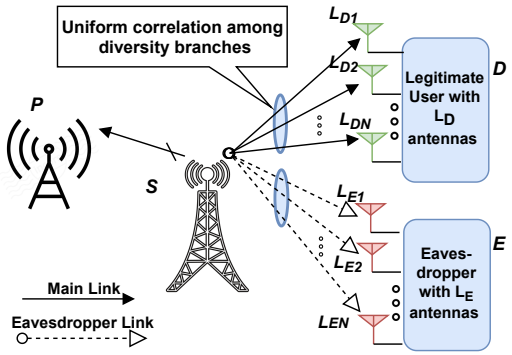

Fig. 1: The system model

the analysis of SOP over correlated Nakagami-m channels followed by its asymptotic analysis. Secrecy analysis of second order statistics is performed in Section IV. Numerical results are discussed in Section V. Finally, Section VI concludes the paper.

II. System and Channel Models

The considered system model is shown in Fig. 1. An underlay CR network is considered which consists of a primary user (P), a secondary user transmitter (referred to as Alice (S)) communicating with a legitimate secondary receiver (referred to as Bob (D)) under the malicious intention of an eavesdropper (referred to as Eve (E)). P and S are assumed to be equipped with single antennas while Bob and Eve are equipped with L_D and L_E antennas, respectively and employing maximal ratio combining (MRC) diversity reception scheme. Furthermore, antennas mounted on Bob and Eve are assumed to be closely spaced and thus uniformly correlated. However, Bob and Eve are assumed to be sufficiently spaced apart and thus the main link ($S-D$) and the eavesdropper link ($S-E$) are independent of each other. We consider that both primary and secondary networks experience quasi static Nakagami-m fading channel. Due to rapid channel variations, the imperfect channel fading coefficient (h_k) between S and k is given as [21]

$$h_k = \psi_k \hat{h}_k + \sqrt{1-\psi_k^2}\varepsilon, \tag{1}$$

where $k \in (D,E)$, $\hat{h}_k$ is the Nakagami-m fading channel between S and k, $\psi_k \in [0,1]$ is the magnitude of imperfect coefficient between h_k and $\hat{h}_k$ with $\psi_k = 1$ referring to perfect channel state information (CSI), and ε is the channel estimation error modelled as complex valued Gaussian random variable with zero mean and unit variance, independent of $\hat{h}_k$.

III. Performance Analysis of Secrecy Outage

A. Preliminaries of Distribution of the Instantaneous SNR

The instantaneous signal to noise ratio (SNR) at receiving node 'k' can be expressed as [21]

$$\gamma_k = \sum_{i=1}^{L_k} \gamma_i^k = \left(\frac{P_S}{\sigma^2}\right) Y_k, \tag{2}$$

where γ_i stands for instantaneous SNR per antenna, L_k is the number of antennas, P_s is the transmission power at S, σ^2 is the noise variance and $Y_k = \sum_{i=1}^{L_k} |h_i^k|^2$ are the channel gains of uniformly correlated L antennas at k. The probability density function (PDF) of Y_k can be written as [11]

$$f_{Y_k}(y) = \frac{A_k}{D_k} y^{L_k m-1} e^{-B_k y} {}_1F_1(m, L_k m; C_k y), \tag{3}$$

where $A_k = \left(\frac{m}{\hat{\gamma}_k}\right)^{L_k m}$, $B_k = \frac{m}{\hat{\gamma}_k(1-\rho_k)}$, $C_k = \frac{L_k m \rho_k}{\hat{\gamma}_k(1-\rho_k)(1-\rho_k+L_k\rho_k)}$, $D_k = (1-\rho_k)^{m(L_k-1)}(1-\rho_k+L_k\rho_k)^m \Gamma(L_k m)$, ρ_k is the uniform correlation coefficient for closely spaced L_k antennas, $\hat{\gamma}_k$ is the average SNR under imperfect CSI, and ${}_1F_1(\cdot,\cdot;\cdot)$ is the confluent hypergeometric function [22, Eq. (9.210.1)]. Furthermore, ${}_1F_1(\cdot,\cdot;\cdot)$ can be represented as

$${}_1F_1(a_1,b_1;x) = \frac{\Gamma(b_1)}{\Gamma(a_1)} \sum_{n=0}^{\infty} \frac{\Gamma(a_1+n)x^n}{\Gamma(b_1+n)n!}, \tag{4}$$

where $\Gamma(\cdot)$ indicates the Gamma function [22, Eq. (8.310.1)]. On integrating (3) as per the definition of cumulative distribution function (CDF), we obtain

$$F_{Y_k}(y) = \frac{A_k}{D_k}\frac{\Gamma(L_k m)}{\Gamma(m)} \sum_{n=0}^{\infty} \frac{\Gamma(m+n)C_k^n B_k^{-L_k m-n}}{\Gamma(L_k m+n)n!} \times \int_0^y x^{L_k m+n-1} e^{-B_k x} dx. \tag{5}$$

On solving (5) with the aid of [22, Eq.(8.350.1)] yields the CDF of Y_k as

$$F_{Y_k}(y) = \frac{A_k}{D_k}\frac{\Gamma(L_k m)}{\Gamma(m)} \sum_{n=0}^{\infty} \frac{\Gamma(m+n)C_k^n}{\Gamma(L_k m+n)n!} B_k^{-L_k m-n} \times g(L_k m+n, B_k y), \tag{6}$$

where $g(\cdot,\cdot)$ denotes the lower incomplete Gamma function [22, Eq. (8.350.1)]. Moreover, the imperfect CSI at k, represented as $\hat{\gamma}_k$, can be expressed as [21]

$$\hat{\gamma}_k = \frac{\psi_k^2 \bar{\gamma}_k}{\bar{\gamma}_k(1-\psi_k^2)+1}. \tag{7}$$

It can be noted that when $\psi_k = 1$, perfect CSI is obtained and thus $\hat{\gamma}_k = \bar{\gamma}_k$, the average SNR along L_k. Substituting A_k, B_k, C_k and D_k in (3) and (6) results in the distributions of instantaneous SNR of uniformly correlated antennas at k, performing MRC under imperfect CSI.

For underlay CRNs, the transmission power at S is $P_S = min\left(P_{max}, \frac{I_P}{X}\right)$, where P_{max} is the maximum transmit power at S, I_P is the peak interference power at P and $X = |h_P|^2$ is the channel gain between S and P. The PDF and CDF of X can be written as

$$f_X(y) = \frac{y^{m_P-1}}{\Gamma(m_P)}\left(\frac{m_P}{\Omega_P}\right)^{m_P} e^{\left(-\frac{m_P}{\Omega_P}\right)y}, \tag{8}$$

$$F_X(y) = 1 - \frac{1}{\Gamma(m_P)} G\left(m_P, \frac{m_P}{\Omega_P} y\right), \tag{9}$$

respectively, where m_p is the fading parameter, Ω_P is the average channel power gain and $G(\cdot,\cdot)$ is the upper incomplete Gamma function [22, Eq. (8.350.2)].

B. Secrecy Outage Probability

SOP is defined as the probability that the instantaneous secrecy capacity falls below a target rate 'R_s' i.e., $P_r(C_s < R_s)$. Secrecy capacity can be written as [3]

$$C_s(\gamma_D,\gamma_E) = \mathrm{C}_D - \mathrm{C}_E = \max\{\ln(1+\gamma_D) - \ln(1+\gamma_E), 0\}, \quad (10)$$

where $\mathrm{C}_D = \ln(1+\gamma_D)$ and $\mathrm{C}_E = \ln(1+\gamma_E)$ are channel capacities of Bob and Eve, respectively. The SOP for underlay CRN depends on P_s and can be defined as [8],

$$\begin{aligned}\mathrm{SOP} = Pr\{C_s(\gamma_D,\gamma_E) \le R_s\} = &\underbrace{Pr\{C_s(\gamma_D,\gamma_E) \le R_s, P_S = P_{max}\}}_{\equiv P_1} \\ &+ \underbrace{Pr\left\{C_s(\gamma_D,\gamma_E) \le R_s, P_S = \frac{I_P}{X}\right\}}_{\equiv P_2}.\end{aligned} \quad (11)$$

Probabilities P_1 and P_2 can be further analyzed as follows:

$$\begin{aligned}P_1 &= Pr\left\{Y_D \le \theta Y_E + \frac{\theta-1}{\alpha}\right\} Pr\left\{X \le \frac{I_P}{P_{max}}\right\} \\ &= \underbrace{\int_0^\infty F_{Y_D}\left(\theta y + \frac{\theta-1}{\alpha}\right) f_{Y_E}(y)\ \mathrm{d}y}_{I_1} \underbrace{Pr\left\{X \le \frac{I_P}{P_{max}}\right\}}_{I_2},\end{aligned} \quad (12)$$

where $\alpha = \frac{P_{max}}{\sigma^2}$ and $\theta = e^{R_s}$. For detailed derivation of Integral I_1, kindly refer to appendix. Moreover, with the aid of (9), I_2 can be rewritten as

$$I_2 = Pr\left\{X \le \frac{I_P}{P_{max}}\right\} = 1 - \frac{1}{\Gamma(m)} G\left(m, \frac{mI_P}{\Omega_P P_{max}}\right). \quad (13)$$

On substituting (31) and (13) in (12), P_1 can be obtained. Further, P_2 can be written as

$$\begin{aligned}P_2 &= Pr\left\{C_s(\gamma_D,\gamma_E) \le R_s, P_S = \frac{I_P}{X}\right\} \\ &= Pr\left\{Y_D \le \theta Y_E + \frac{(\theta-1)X}{\beta}, X > \frac{I_P}{P_{max}}\right\} \\ &= \int_{\frac{I_P}{P_{max}}}^\infty \underbrace{\int_0^\infty F_{Y_D}\left(\theta y + \frac{(\theta-1)x}{\beta}\right) f_{Y_E}(y)\ \mathrm{d}y}_{H(x)} f_X(x)\ \mathrm{d}x,\end{aligned} \quad (14)$$

where $\beta = \frac{I_P}{\sigma^2}$. $H(x)$, the inner integral in (14) is simplified in similar lines with (31) and obtained as

$$\begin{aligned}H(x) = &\frac{A_D}{D_D}\frac{\Gamma(L_D m)}{\Gamma(m)} \sum_{n_3=0}^\infty \frac{\Gamma(m+n_3) C_D^{n_3} B_D^{-L_D m - n_3}}{\Gamma(L_D m + n_3) n_3!} \frac{A_E}{D_E} \\ &\times \frac{\Gamma(L_E m)}{\Gamma(m)} \sum_{n_4=0}^\infty \frac{\Gamma(m+n_4) C_E^{n_4}}{\Gamma(L_E m + n_4) n_4!} \sum_{k_2=0}^{n4+L_E m-1} \left(\frac{x(1-\theta)}{\beta\theta}\right)^{k_2} \\ &\times \theta^{-L_E m - n_4 + k_2} \binom{n_4 + L_E m - 1}{k_2} \left(e^{B_E\left(\frac{(\theta-1)x}{\beta\theta}\right)}\right) \\ &\times \sum_{v=0}^\infty \frac{\Gamma(L_D m + n_3) B_D^{L_D m + n_3 + v}}{\Gamma(L_D m + n_3 + v + 1)} \frac{\Gamma\left(\Theta, \left(\frac{(\theta-1)x}{\alpha}\right)\left(B_D + \frac{B_E}{\theta}\right)\right)}{\left(B_D + \frac{B_E}{\theta}\right)^\Theta}.\end{aligned} \quad (15)$$

On utilizing the definition of upper incomplete Gamma function and on further substituting (8) and (15) in (14) and evaluating the integral, P_2 can be obtained as

$$\begin{aligned}P_2 = &\frac{A_D}{D_D}\frac{\Gamma(L_D m)}{\Gamma(m)} \sum_{n_3=0}^\infty \frac{\Gamma(m+n_3) C_D^{n_3} B_D^{-L_D m - n_3}}{\Gamma(L_D m + n_3) n_3!} \frac{A_E}{D_E} \frac{\Gamma(L_E m)}{\Gamma(m)} \\ &\times \sum_{n_4=0}^\infty \frac{\Gamma(m+n_4) C_E^{n_4}}{\Gamma(L_E m + n_4) n_4!} \left(\frac{m}{\Omega}\right)^m \frac{1}{\Gamma(m)} \sum_{k_2=0}^{n4+L_E m-1} \left(\frac{1-\theta}{\beta\theta}\right)^{k_2} \\ &\times \theta^{-L_E m - n_4 + k_2} \binom{n_4 + L_E m - 1}{k_2} \sum_{v=0}^\infty \frac{\Gamma(L_D m + n_3) \times B_D^{L_D m + n_3 + v}}{\Gamma(L_D m + n_3 + v + 1)\left(B_D + \frac{B_E}{\theta}\right)^\Theta} \\ &\times \sum_{r=0}^{\Theta-1} \left(\left(B_D + \frac{B_E}{\theta}\right)\left(\frac{\theta-1}{\beta}\right)\right)^r \frac{(\Theta-1)!}{r!} \\ &\times \frac{\Gamma\left(k_2 + m + r, \frac{I_p}{P_{max}} \times \left\{\frac{m}{\Omega} - \varpi + \nu\right\}\right)}{\left[\frac{m}{\Omega} - \varpi + \nu\right]^{k_2 + m + r}},\end{aligned} \quad (16)$$

where $\varpi = \frac{B_E(\theta-1)}{\beta\theta}$, $\nu = \left(\frac{\theta-1}{\beta}\right)\left(B_D + \frac{B_E}{\theta}\right)$ and $\Theta = L_D m + n_3 + L_E m + n_4 + v - k_2$. The analytical expression of SOP is obtained by substituting the simplified (12) and (16) in (11). Note that although the final expression of SOP contains an infinite series term, it converges quickly due to the monotonically decreasing upper incomplete Gamma function, demonstrated further in the numerical results section.

C. Asymptotic Analysis of Secrecy Outage Probability

To gain further insights of the system performance at high SNR, asymptotic analysis of SOP is carried out converting to the form $SOP^\infty \approx G_c \hat{\gamma}_k^{G_d}$, where G_c is the secrecy array gain and G_d is the secrecy diversity gain. For simplicity, we bifurcate the analysis in two cases:

Case 1- *$\hat{\gamma}_D \to \infty$ and $\hat{\gamma}_E$ is fixed:* From the expression of SOP in (11) and (12), we can notice that for the considered case, only integrals I_1 and P_2 will be influenced. On rewriting I_1, we have

$$I_{1,\infty} = \int_0^\infty F_{Y_D,\infty}\left(\theta y + \frac{\theta-1}{\alpha}\right) f_{Y_E}(y)\ \mathrm{d}y. \quad (17)$$

In order to solve the above expression, we analyze (6) at high SNR. From (6), it follows that the dominating term is obtained for $n = 0$. Furthermore, using the approximation $\lim_{x\to\infty} g(s,x) = \Gamma(s)$ in (6), $F_{Y_D,\infty}$ can be simplified as,

$$F_{Y_D,\infty}\left(\theta y + \frac{\theta-1}{\alpha}\right) = \frac{A_D}{D_D} B_D^{-L_D m} \Gamma(L_D m). \quad (18)$$

On substituting (18) and (3) in (17) and on further simplification, $I_{1,\infty}$ can be obtained as

$$\begin{aligned}I_{1,\infty} = &\frac{A_D}{D_D}\frac{A_E}{D_E} B_D^{-L_D m} \Gamma(L_D m) \\ &\times \int_0^\infty y^{L_E m - 1} e^{-B_E y}\, {}_1F_1(m, L_E m; C_E y)\ \mathrm{d}y.\end{aligned} \quad (19)$$

With the aid of [22, Eq. (7.621.4)], the above expression can be rewritten as

$$I_{1,\infty} = \frac{A_D}{D_D}\frac{A_E}{D_E} B_D^{-L_D m}\Gamma(L_D m)\Gamma(L_E m) B_E^{-L_E m} \times F\left(B_E, L_E m, L_E m, \frac{C_E}{B_E}\right), \tag{20}$$

where $F(\cdot)$ is the hypergeometric function. Similarly, on solving P_2 in (11) in a similar fashion as above and on comparing with SOP^{∞}, the secrecy diversity gain obtained is of order L_D.

Case 2- *$\hat{\gamma}_E \to \infty$ and $\hat{\gamma}_D$ is fixed:* In this case, since $\hat{\gamma}_E \to \infty$, the secrecy diversity order obtained is zero and thus the probability of successful eavesdropping is approaching one.

IV. Performance Analysis of Secrecy Outage Rate and Secrecy Outage Duration

In this section, the performance analysis of second order statistics like ASOR and ASOD is carried out.

A. Average Secrecy Outage Rate

The ASOR quantifies the expected number of downward crossings of the C_s per second at a certain threshold. It can be defined as the average secrecy level crossing rate of the instantaneous C_s at a certain threshold level [20]. Based on the definition of C_s, when $P_s = P_{max}$, the event $\mathfrak{R}_1$ is equivalent to $\left[r_1 = \frac{h_{\text{SD}}}{\sqrt{N_0}} \le \sqrt{\frac{e^{R_s}(1+\alpha\gamma_E)-1}{P_{max}}}\right]$. Similarly, when $P_s = \frac{I_P}{X}$, the event $\mathfrak{R}_2$ is equivalent to $\left[r_2 = \frac{h_{\text{SD}}}{\sqrt{N_0}} \le \sqrt{\frac{e^{R_s}(1+\beta\gamma_E)-1}{I_P}}\right]$. Here, r_1 and r_2 are the instantaneous fading amplitudes of the uniformly correlated Nakagami-m fading channels. Since underlay CRN is considered, two terms are obtained in accordance with (11).

Furthermore, p_{r_1}, the PDF of r_1 can be written with the aid of (3) as

$$p_{r_1} = \frac{A_D}{D_D}\ 2r_1^{L_D m-1} e^{-B_D r_1^2}\,{}_1F_1(m, L_D m; C_D r_1^2). \tag{21}$$

Note that when the correlation is assumed zero by substituting $\rho_D = 0$ in the subsequent values of A_D, B_D, C_D, and D_D, as defined below (6), the PDF of instantaneous fading amplitude is obtained as [20, Eq. (6)], thus showing the backward mathematical compatibility. Moreover, $p_{\dot{r}_1}(\dot{r}_1)$, the PDF of time derivative of r_1 is independent of amplitude. With the aid of [23, Eq. (13)], it can be expressed as

$$p_{\dot{r}_1}(\dot{r}_1) = \frac{1}{\sqrt{2\,\pi}\ \sigma_{\text{SD}}}\ \exp\left(-\frac{\dot{r}_1{}^2}{2\ \sigma_{\text{SD}}^2}\right), \tag{22}$$

where $\sigma_{\text{SD}}^2 = \pi^2 f_{max}^2(\Omega_D/m)$, f_{max} is the maximum Doppler frequency, and Ω_D is the average channel power gain at D.

Based on the general formula provided in [24], the ASOR for the multiantenna CRN can thus be formulated as

$$\mathfrak{R}(R_s) = \mathfrak{R}_1(R_s)\mathrm{P}_r\left(X \le \frac{I_p}{P_{max}}\right) + \mathfrak{R}_2(R_s)\mathrm{P}_r\left(X > \frac{I_p}{P_{max}}\right) \tag{23}$$

where,

$$\mathfrak{R}_1(R_s) = \int_0^{\infty}\int_0^{\infty} \dot{r}_1\ p_{r_1}(r_{th1})\ p_{\dot{r}_1}(\dot{r}_1)\ p_{\gamma_{\text{E}}}(y)\ \mathrm{d}\dot{r}_1\ \mathrm{d}y, \tag{24}$$

$$\mathfrak{R}_2(R_s) = \int_0^{\infty}\int_0^{\infty} \dot{r}_2\ p_{r_2}(r_{th2})\ p_{\dot{r}_2}(\dot{r}_2)\ p_{\gamma_{\text{E}}}(y)\ \mathrm{d}\dot{r}_2\ \mathrm{d}y. \tag{25}$$

Note that p_{r_1}, $p_{\dot{r}_1}$, p_{r_2} and $p_{\dot{r}_2}$ are the PDFs of r_1, $\dot{r}_1$, r_2 and $\dot{r}_2$ respectively. On substituting $p_{\dot{r}_1}$ from (22) to (24), and on further simplifying with the aid of [23], we obtain

$$\mathfrak{R}_1(R_s) = \frac{\sigma_{\text{SD}}}{\sqrt{2\,\pi}}\int_0^{\infty} p_{r_1}(r_{th1})\ p_{\gamma_{\text{E}}}(y)\ \mathrm{d}y. \tag{26}$$

On further substituting p_{r_1} from (21), and p_{γ_E} from (3) in (26), and on re-writing, we obtain

$$\mathfrak{R}_1(R_s) = \frac{\sigma_{\text{SD}}}{\sqrt{2\,\pi}}\frac{2A_D\ A_E}{D_D\ D_E}\int_0^{\infty} r_{th1}^{L_D m-1} e^{-B_D r_{th1}^2} \times {}_1F_1(m, L_D m; C_D r_{th1}^2)\ y^{L_E m-1} e^{-B_E y}\,{}_1F_1(m, L_E m; C_E y)\ \mathrm{d}y. \tag{27}$$

On substituting the value of r_1 in place of r_{th1} in the above expression, we obtain

$$\mathfrak{R}_1(R_s) = \frac{\sigma_{\text{SD}}}{\sqrt{\pi}}\frac{\sqrt{2}A_D\ A_E}{D_D\ D_E}\int_0^{\infty}\left(\frac{e^{R_s}(1+\alpha y)-1}{P_{max}}\right)^{L_D m-1} \times\exp\left(-B_D\left(\frac{e^{R_s}(1+\alpha y)-1}{P_{max}}\right)\right) y^{L_E m-1} e^{-B_E y} \times {}_1F_1\left(m, L_D m; C_D\left(-B_D\left(\frac{e^{R_s}(1+\alpha y)-1}{P_{max}}\right)\right)\right) \times {}_1F_1(m, L_E m; C_E y)\ \mathrm{d}y. \tag{28}$$

On further applying Laguerre theorem with the aid of [25], the expression of $\mathfrak{R}_1$ can be simplified as,

$$\mathfrak{R}_1(R_s) \approx \frac{\sigma_{\text{SD}}\sqrt{2}A_D A_E}{\sqrt{\pi}D_D\ D_E}\sum_{n=1}^{N} w_n\left(\frac{e^{R_s}(1+\alpha x_n)-1}{P_{max}}\right)^{L_D m-1} \times\exp\left(-B_D\left(\frac{e^{R_s}(1+\alpha x_n)-1}{P_{max}}\right)\right) x_n^{L_E m-1} e^{-B_E x_n} \times {}_1F_1\left(m, L_D m; C_D\left(-B_D\left(\frac{e^{R_s}(1+\alpha x_n)-1}{P_{max}}\right)\right)\right) \times {}_1F_1(m, L_E m; C_E x_n), \tag{29}$$

where x_n and w_n are the n^{th} root and weight of the N^{th} order Laguerre polynomial, respectively. On solving $\mathfrak{R}_2$ in (25) in similar manner to the above analysis, the final expression of $\mathfrak{R}_2$ is obtained.

B. Average Secrecy Outage Duration

The ASOD quantifies the average time duration for which the system remains in the secrecy outage status. As per the definition in [24], the ASOD can be expressed as

$$T(R_s) = \frac{\mathrm{SOP}(R_s)}{\mathfrak{R}(R_s)}. \tag{30}$$

On substituting the final expressions of SOP and $\mathfrak{R}$ in the above equation, the ASOD for multiantenna CRN is obtained. Note that on substituting $R_s = 0$, $m = 1$ and, $\rho = 0$, we find that ASOD depends only on σ_{SD}, i.e., on the maximum Doppler frequency (f_{max}).

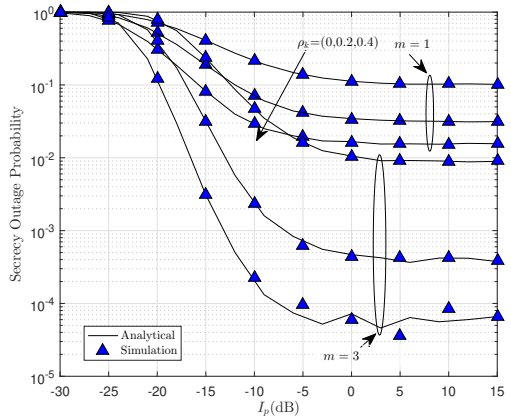

Fig. 2: SOP v/s I_p with $\bar{\gamma}_D = 10$ dB, $\bar{\gamma}_E = 0$ dB and $\psi_k = 1$

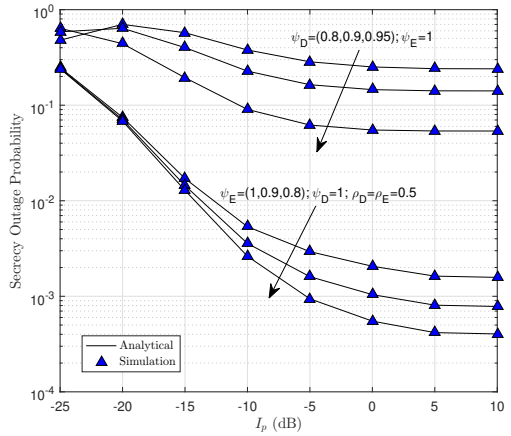

Fig. 3: SOP v/s I_p; $\bar{\gamma}_D = 15$ dB, $\bar{\gamma}_E = 0$ dB, $L_D, L_E = 3$, and $m = 2$

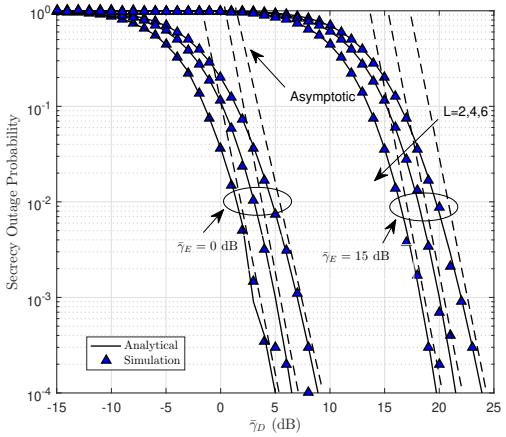

Fig. 4: SOP v/s $\bar{\gamma}_D$ with $\psi_k = 1$, $\rho_k = 0$, $m = 2$ and $I_p = 0$ dB

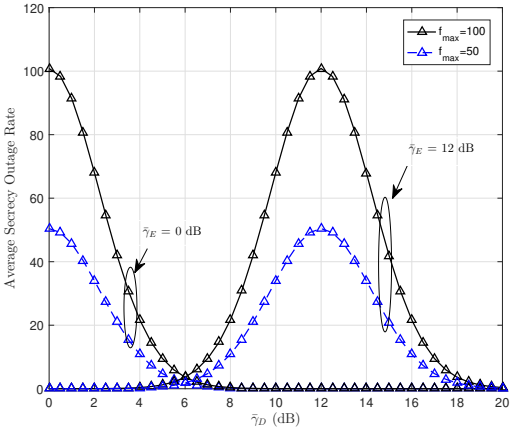

Fig. 5: ASOR v/s $\bar{\gamma}_D$; $L_D, L_E = 2$, $m = 4$, $\rho_k = 0$, and $I_P = 0$ dB

V. Numerical Results

In this section, we analyze the first and second order secrecy measures for the considered system model. The simulation parameters are listed in the Table I.

TABLE I: List of the configured simulation parameters

Parameter	MonteCarlo Trials	P_{max}	R_s	N	n_1, n_2, u	n_3, n_4	v
Value	15000	1W	0.1	30	2	4	12

Fig. 2 shows the plot of SOP versus I_P for $m = 1$ and 3, $L_D = L_E = 3$, assuming perfect CSI at Bob and Eve. It can be observed from the graph that SOP is highest for uncorrelated case $\rho_k = 0$ and it decreases as ρ_k increases. To confirm the result, we investigated the scenarios considering i) the antenna correlation only at Bob, ii) antenna correlation only at Eve, and iii) equal correlation at Bob and Eve. We notice that the effect of antenna correlation is more detrimental at Bob. Thus, we conclude that the antenna correlation improves the secrecy performance in a sense that the harm caused due to correlation at Eve's channel outperforms the loss introduced by correlation on Bob's channel (as also confirmed by other numerical results not included in this paper due to space limitations). Furthermore, it can also be observed from the result that SOP is low for $m = 3$ as compared to $m = 1$. This is intuitive from the fact that $m = 1$ represents a Rayleigh fading scenario and $m = 3$ represents a better channel condition. Fig. 3 shows the effect of ψ_k on SOP. The upper and lower set of plots represents the imperfect CSI at Bob and Eve respectively. We can notice that as the CSI at Bob improves, the SOP decreases. Furthermore, Eve being an unintended user can be expected to have more imperfectness in CSI. We notice that as ψ_E increases, SOP increases. This is due to the fact that increasing ψ_E improves Eve's channel estimation and thus increasing the SOP. Note that when perfect CSI is assumed, our analysis remains valid for correlated antennas. We can also observe that SOP floor exists at high I_p due to P_{max} as per the condition $P_S = min\left(P_{max}, \frac{I_P}{X}\right)$. Moreover, when $\rho_k = 0$ and $\psi_k = 1$ is assumed, our results match with [6] when $m = 1$, and with [26] when $L_D = L_E = 1$ and $P_s = \frac{I_p}{X}$ is considered. Fig. 4 shows the plot of SOP versus $\bar{\gamma}_D$ for different values of $\bar{\gamma}_E$ and L_k. We can infer from the plot that when $\bar{\gamma}_E$ increases, SOP increases. This is due to the fact that high $\bar{\gamma}_E$ implies a high SNR in $(S-E)$ link and thus a higher secrecy outage. Furthermore, as the number of diversity branches L_k increases, the gain in the SOP improves. The dashed lines indicate the asymptotic

performance. We can notice that slopes of all the asymptotic lines are the same. This confirms our analysis that the secrecy diversity gain order is of the order L_D. Fig. 5 demonstrates the plot of ASOR versus $\bar{\gamma}_D$ for $L_D = L_E = 2$, $m = 4$, $R_s = 0$, $\rho_D = \rho_E = 0$, and $I_P = 0$ dB for different values of f_{max} and $\bar{\gamma}_E$. As f_{max} increases, the ASOR increases. This is because the higher value of f_{max} indicates that the Bob/Eve is moving at a higher speed. This causes a fast variation in secrecy capacity and thus increases the ASOR. We also observe from the plot that a maximum value of ASOR occurs when $\bar{\gamma}_D = \bar{\gamma}_E$. This non monotonic behaviour is expected because as C_s becomes zero, it crosses the zero threshold ($R_s = 0$) maximum times as compared to the threshold crossings when the difference between $\bar{\gamma}_D$ and $\bar{\gamma}_E$ is comparable.

VI. Conclusions

In this work, the secrecy performance for uniformly correlated CR antennas at Bob and Eve is carried out. In particular, the first and second order secrecy measures like SOP and ASOR & ASOD respectively are analysed. The analytical expressions are verified by the Monte Carlo simulations. This work considers maximum power constraint along with the interference power constraint. We conclude that the secrecy outage depends on the antenna correlation factor of multiantenna systems and also on CSI estimates at Bob and Eve. Moreover, asymptotic analysis of secrecy outage probability reveals the secrecy diversity gain of order L_D. Furthermore, this work provides a rigorous study and offers a realistic framework on the first and second order measures that could be useful in the secrecy analysis of correlated multiantenna CR users for 5G and beyond networks.

Appendix: Evaluation of Integral I_1

On transforming the variable and assuming $\theta y + \frac{\theta-1}{\alpha} = z$ to simplify integral I_1, with the aid of (3) and (6), on subsequently performing the binomial expansion of $\left(\frac{z}{\theta} - \frac{\theta-1}{\alpha\theta}\right)^{n_2+L_E m-1}$ after transforming the variable, and using $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^n$, we obtain, the intermediate integral I_1 in terms of 'z'. On further replacing the lower incomplete Gamma function as $g(s,v) = v^s \Gamma(v) e^{-v} \sum_{u=0}^{\infty} \frac{v^u}{\Gamma(s+u+1)}$, and on simple manipulation, I_1 can be expressed as

$$
\begin{aligned}
I_1 = {} & \frac{A_D}{D_D} \frac{\Gamma(L_D m)}{\Gamma(m)} \sum_{n_1=0}^{\infty} \frac{\Gamma(m+n_1) C_D^{n_1} B_D^{-L_D m - n_1}}{\Gamma(L_D m + n_1) n_1!} \\
& \times \frac{A_E}{D_E} \frac{\Gamma(L_E m)}{\Gamma(m)} \sum_{n_2=0}^{\infty} \frac{\Gamma(m+n_2) C_E^{n_2}}{\Gamma(L_E m + n_2) n_2!} \sum_{k_1=0}^{n_2+L_E m-1} \left(\frac{1-\theta}{\alpha\theta}\right)^{k_1} \\
& \times \theta^{-L_E m - n_2 + k_1} \binom{n_2 + L_E m - 1}{k_1} \left(e^{B_E\left(\frac{\theta-1}{\alpha\theta}\right)}\right) \\
& \times \sum_{u=0}^{\infty} \frac{\Gamma(L_D m + n_1) B_D^{L_D m + n_1 + k}}{\Gamma(L_D m + n_1 + k + 1)} \frac{\Gamma\left(\Xi, \left(\frac{\theta-1}{\alpha}\right)\left(B_D + \frac{B_E}{\theta}\right)\right)}{\left(B_D + \frac{B_E}{\theta}\right)^{\Xi}},
\end{aligned}
\tag{31}
$$

where $\Xi = L_D m + n_1 + L_E m + n_2 + u - k_1$.

References

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

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

[3] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, 2015.

[5] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[6] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[7] Y. Pei, Y. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[8] H. Lei, H. Zhang, I. S. Ansari, G. Pan, and K. A. Qaraqe, "Secrecy outage analysis for SIMO underlay cognitive radio networks over generalized-K fading channels," *IEEE Signal Process. Lett.*, vol. 23, no. 8, pp. 1106–1110, 2016.

[9] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10 236–10 242, Dec. 2016.

[10] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Physical layer security of a multiantenna-based CR network with single and multiple primary users," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11 011–11 022, Dec. 2017.

[11] V. A. Aalo, "Performance of maximal-ratio diversity systems in a correlated Nakagami-fading environment," *IEEE Trans. Commun.*, vol. 43, no. 8, pp. 2360–2369, Aug. 1995.

[12] D. K. Patel, B. Soni, Y. L. Guan, S. Sun, Y. C. Chang, and J. M. Lim, "Performance analysis of arbitrary correlated multiantenna receiver for mobile cognitive user," in *Proc. of IEEE GLOBECOM*, 2020, pp. 1–6.

[13] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in correlated channel with maximal ratio combining diversity," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6745–6751, Dec. 2012.

[14] J. Si, Z. Li, J. Cheng, and C. Zhong, "Secrecy performance of multiantenna wiretap channels with diversity combining over correlated Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 444–458, Jan. 2019.

[15] A. Mathur, Y. Ai, M. Cheffena, and G. Kaddoum, "Secrecy performance of correlated α - μ fading channels," *IEEE Commun. Lett.*, vol. 23, no. 8, pp. 1323–1327, 2019.

[16] J. Sun, H. Bie, X. Li, J. Zhang, G. Pan, and K. M. Rabie, "Secrecy performance analysis of SIMO systems over correlated $\kappa - \mu$ shadowed fading channels," *IEEE Access*, vol. 7, pp. 86 090–86 101, 2019.

[17] Lin Yang, M. O. Hasna, and M. . Alouini, "Average outage duration of multihop communication systems with regenerative relays," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1366–1371, 2005.

[18] S. Kavaiya, D. K. Patel, Y. L. Guan, S. Sun, Y. C. Chang, and J. M. Y. Lim, "On physical layer security over $\alpha - \eta - \kappa - \mu$ fading for relay based vehicular networks," in *Proc. of SPCOM*, 2020, pp. 1–5.

[19] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, 2018.

[20] A. Omri and M. O. Hasna, "Average secrecy outage rate and average secrecy outage duration of wireless communication systems with diversity over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3822–3833, 2018.

[21] F. S. Al-Qahtani, Y. Huang, S. Hessien, R. M. Radaydeh, C. Zhong, and H. M. Alnuweiri, "Secrecy analysis of MIMO wiretap channels with low-complexity receivers under imperfect channel estimation," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 257–270, Feb. 2017.

[22] D. Zwillinger, *"Table of Integrals, Series, and Products", Eighth Edition*, 2014.

[23] K. Y. Huang and Y. A. Chau, "Analytical second-order statistics of maximal-ratio diversity over spatially correlated Nakagami fading channels," *Journal of the Chinese institute of engineers*, vol. 33, no. 2, pp. 207–213, 2010.

[24] G. L. Stüber, "Radio resource management," in *Principles of Mobile Communication*. Springer, 2017, pp. 593–641.

[25] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. New York, NY, USA: Dover, 1965.

[26] C. Tang, G. Pan, and T. Li, "Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 609–612, Dec. 2014.