On Secrecy Capacity of Full-Duplex Cognitive Cooperative Radio Networks

Thi My Chinh Chu and Hans-Jürgen Zepernick
Blekinge Institute of Technology, SE-37179 Karlskrona, Sweden
E-mail: {cch, hjz}@bth.se

Abstract—**In this paper, we analyze the secrecy capacity of a full-duplex underlay cognitive cooperative radio network (CCRN) in the presence of an eavesdropper and under the interference power constraint of a primary network. The full-duplex mode is used at the secondary relay to improve the spectrum efficiency which in turn leads to an improvement of the secrecy capacity of the full-duplex CCRN. We utilize an approximation-and-fitting method to convert the complicated expression of the signal-to-interference-plus-noise ratio into polynomial form which is then utilized to derive an expression for the secrecy capacity. Numerical results are provided to illustrate the effect of network parameters such as transmit power, interference power limit, self-interference parameters of the full-duplex mode, and distances among links on the secrecy capacity. To reveal the benefits of the full-duplex CCRN, we compare the secrecy capacity obtained when the secondary relay operates in full-duplex and half-duplex mode.**

I. Introduction

Due to the broadcasting nature of radio transmission, guaranteeing secure communication in the presence of eavesdroppers has been a major challenge with mobile radio systems. Typically, security is implemented in several protocol layers by using suitable cryptographic and authentication techniques [1], [2]. However, exchanging cryptographic keys among nodes in complex network topologies such as ad-hoc or relay networks is complicated and becomes vulnerable to attacks as nodes join or leave the network randomly [3], [4]. In these types of networks, it is beneficial to utilize physical layer characteristics such as fading or interference to facilitate a more secure transmission of confidential information [5], [6]. The basic idea of such physical layer security is the notion of secrecy capacity coined by Wyner in [7] defining the maximum rate at which a system can transmit confidential information as the difference between the capacity of the link from source to intended receiver and from the source to the eavesdropper.

Another challenge is the growing demand on bandwidth-hungry mobile services such as mobile multimedia, mobile gaming, and mobile augmented and virtual reality which puts significant stress on the radio spectrum. Cognitive radio networks (CRNs) have received large recognition as a effective technology that can improve spectrum efficiency [8]. This approach allows unlicensed users or secondary users (SUs) to access frequency bands belonging to licensed users or primary users (PUs) as long as the quality of the PUs is guaranteed. Spectrum may be accessed by SUs either opportunistically (interweave [9]) or concurrently (overlay and underlay [10], [11]) with the PUs. Interweave schemes avoid interference to PUs as spectrum access for SUs is allowed only if PUs do not occupy the respective licensed bands. However, SUs may suffer from long periods of blocking when resources are occupied by PUs which would be not suitable for delay-sensitive services. On the other hand, as prerequisite of concurrent transmission without limitation on access time, overlay and underlay spectrum sharing must control the transmit powers of the SUs such that the interference power limit at the PUs is not exceeded. The relatively small radio coverage caused by this limitation on the SU transmit power can be alleviated by deploying cooperative relays resulting in a cognitive cooperative radio network (CCRN). When it comes to implementation issues, underlay spectrum sharing is simpler to deploy compared to overlay spectrum sharing as it does not require knowledge about the primary network (PN).

As for the security aspects of CRNs, recent research has commenced to put increased attention to physical layer security. This is motivated by the fact that SUs of interweave schemes have to dynamically join or leave spectrum bands based on the activity of the PUs and hence significantly depend on effective spectrum access in the physical layer. Further, power control and interference mitigation associated with overlay and underlay spectrum access schemes also take place in the physical layer. Therefore, a substantial body of works on the security in CRNs is currently focusing on physical layer security [12]. In particular, a state-of-the-art survey along with an overview on research trends in the area of security threats/attacks and countermeasures on the physical layer of CRNs have been discussed in [13]. The work reported in [14] has proposed protocols to achieve secure transmission for CRNs in the presence of multiple eavesdroppers. However, these works have considered only single-hop CRNs. In [15], a CRN has been studied where SUs serve as amplify-and-forward (AF) relays for the PN to enhance physical layer security for the PN. However, spectrum utilization of this scheme is quite low because each transmission of the PN and CRN required three times slots.

Apart from using cognitive radio concepts, due to the rapid advances in radio frequency circuit design, spectral utilization can be improved by full-duplex transmission which allows to simultaneously transmit and receive using the same radio channel. In the context of CRNs, deploying full-duplex transmission has shown significantly enhanced spectrum utilization as reported in [16]. In [17], an underlay CRN has been considered in which the secondary destination operates in

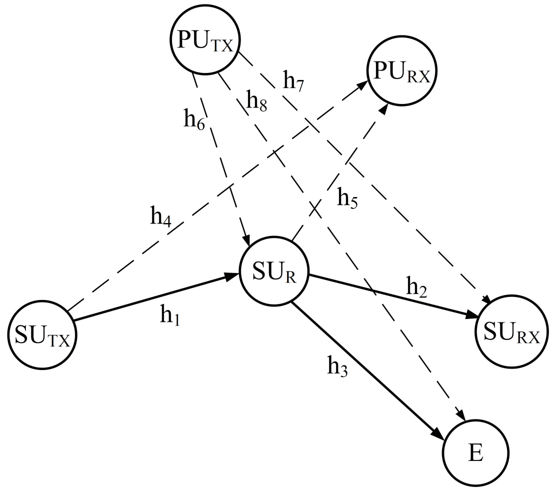

Fig. 1. System model of a CCRN with a full-duplex relay in the presence of an eavesdropper (Solid lines: Communication/Eavesdropper link; Dashed lines: Interference links).

full-duplex mode with two antennas. One antenna is used to receiver signals from the source and the other is used to transmit jamming signals to the eavesdropper. However, all these works did not consider full-duplex relaying for CCRNs.

In this paper, we therefore deploy relaying transmission to improve the signal-to-interference-plus-noise ratio (SINR) of an underlay CCRN subject to the interference power constraint of the PN and in the presence of an eavesdropper. Specifically, to improve spectrum utilization, the full-duplex mode is utilized at the secondary relay which also leads to an enhancement in the secrecy capacity of the CCRN. In order to derive a mathematical expression for the secrecy capacity, we apply an approximation-and-fitting method for transforming the complicated SINR expression into a simpler polynomial form. Finally, numerical examples are provided for the secrecy capacity of the CCRN to show the impact of network parameters such as transmit power and interference power limit of the PN, self-interference (SI) parameters of the full-duplex transmission, and distances of the links among the nodes in the PN and CCRN.

The remainder of the paper is organized as follows. Section II provides the system and channel model along with expressions of the SINR at the secondary receiver and eavesdropper. In Section III, an approximation of the pseudo SINR is derived to support a more efficient calculation of the secrecy capacity. The analysis of the secrecy capacity of the full-duplex underlay CCRN is provided in Section IV. Numerical results are reported and discussed in Section V. Finally, Section VI contains a summary.

II. System and Channel Model

We consider a CCRN consisting of a secondary transmitter SU$_{\mathrm{TX}}$, a secondary relay SU$_{\mathrm{R}}$, and a secondary receiver SU$_{\mathrm{RX}}$ as shown in Fig. 1. The CCRN utilizes underlay spectrum access to concurrently operate in the presence of a primary network (PN). The PN consists of a primary transmitter PU$_{\mathrm{TX}}$ and a primary receiver PU$_{\mathrm{RX}}$. In order to further improve spectrum utilization, the SU$_{\mathrm{R}}$ deploys full-duplex amplify-and-forward (AF) processing. Given the amplified signal flow at the full-duplex AF relay, a passive eavesdropper E is strategically located in the transmission range of SU$_{\mathrm{R}}$ to overhear the communication of the CCRN. The communication, eavesdropper, and interference links are subject to Nakagami-m fading with fading severity parameter m. The channel coefficients of the links SU$_{\mathrm{TX}} \rightarrow$ SU$_{\mathrm{R}}$, SU$_{\mathrm{R}} \rightarrow$ SU$_{\mathrm{RX}}$, SU$_{\mathrm{R}} \rightarrow$ E, SU$_{\mathrm{TX}} \rightarrow$ PU$_{\mathrm{RX}}$, SU$_{\mathrm{R}} \rightarrow$ PU$_{\mathrm{RX}}$, PU$_{\mathrm{TX}} \rightarrow$ SU$_{\mathrm{R}}$, PU$_{\mathrm{TX}} \rightarrow$ SU$_{\mathrm{RX}}$, PU$_{\mathrm{TX}} \rightarrow$ E are denoted as h_1, h_2, h_3, h_4, h_5, h_6, h_7, and h_8, respectively.

Let x_i be the transmit signal of SU$_{\mathrm{TX}}$ at discrete time i with average transmit power P_s. Because the secondary relay operates in full-duplex mode, SU$_{\mathrm{R}}$ can simultaneously receive a signal from SU$_{\mathrm{TX}}$ and transmit a signal to SU$_{\mathrm{RX}}$. Then, the signal received at the secondary relay SU$_{\mathrm{R}}$ at discrete time i can be written as

$$r_i = h_1 x_i + s_i + i_{r,i} + n_{r,i} \tag{1}$$

where $n_{r,i}$ denotes additive white Gaussian noise (AWGN) $\mathcal{CN}(0, N_0)$ with zero-mean and variance N_0. Further, $i_{r,i}$ represents the interference from the primary transmitter PU$_{\mathrm{TX}}$ to the secondary relay SU$_{\mathrm{R}}$ which is approximated as AWGN $\mathcal{CN}(0, N_{r,i})$ with zero-mean and average interference power

$$N_{r,i} = P_p d_6^{-n} \tag{2}$$

as in [18], [19]. In this approximation, P_p is the transmit power of PU$_{\mathrm{TX}}$, d_6 is the distances from PU$_{\mathrm{TX}}$ to SU$_{\mathrm{R}}$, and n is the path-loss exponent. Thus, the interference plus noise at SU$_{\mathrm{R}}$ can be approximated as another AWGN random variable $z_{r,i}$ with zero-mean and variance

$$Z_r = N_0 + N_{r,i} \tag{3}$$

Furthermore, in (1), s_i denotes the residual SI due to the full-duplex operation of SU$_{\mathrm{R}}$. As in [20], [21], the residual SI is modeled as a zero-mean Gaussian random variable $\mathcal{CN}(0, Z_I)$. The variance Z_I of the residual SI is proportional to the transmit power P_r of SU$_{\mathrm{R}}$ and depends on the interference cancelation technique at the relay, i.e.,

$$Z_I = \beta \mathrm{P}_r^{\lambda} \tag{4}$$

where $0 \leq \beta \leq 1$ and $0 \leq \lambda \leq 1$ are parameters representing the effectiveness of the SI cancelation technique. Then, the received signal at SU$_{\mathrm{R}}$ at discrete time i can be formulated as

$$r_i = h_1 x_i + s_i + z_{r,i} \tag{5}$$

As for the processing at SU$_{\mathrm{R}}$, it amplifies the signal r_{i-1} received at the preceding discrete time $i-1$ with a gain G and forwards the resulting signal to SU$_{\mathrm{RX}}$ while simultaneously receiving the signal r_i of the current discrete time i. Specifically, the amplifying gain is given by

$$G = \sqrt{\frac{P_r}{P_s |h_1|^2 + \beta {P_r}^{\lambda} + Z_r}} \tag{6}$$

$$\gamma_D = \frac{Q^2 X_1 X_2 {X_5}^{\lambda}}{Q Z_d X_1 {X_5}^{1+\lambda} + Q Z_r X_2 X_4 {X_5}^{\lambda} + Q^{1+\lambda}\beta X_2 X_4 + Q^{\lambda}\beta Z_d X_4 X_5 + Z_r Z_d X_4 {X_5}^{1+\lambda}} \tag{14}$$

$$\gamma_E = \frac{Q^2 X_1 X_3 {X_5}^{\lambda}}{Q Z_e X_1 {X_5}^{1+\lambda} + Q Z_r X_3 X_4 {X_5}^{\lambda} + Q^{1+\lambda}\beta X_3 X_4 + Q^{\lambda}\beta Z_e X_4 X_5 + Z_r Z_e X_4 {X_5}^{1+\lambda}} \tag{15}$$

where $| \cdot |$ returns the absolute magnitude of its argument. Because $\mathrm{SU_{TX}}$ and $\mathrm{SU_R}$ access licensed spectrum concurrently with the PN, the transmit power P_s of $\mathrm{SU_{TX}}$ and P_r of $\mathrm{SU_R}$ must be adapted to satisfy the following interference power constraint:

$$P_s \left|h_4\right|^2 + P_r \left| h_5 \right|^2 \leq I \tag{7}$$

where I is the interference power limit of the $\mathrm{PU_{RX}}$.

In order to obtain best performance, the CCRN controls its transmit power such that the interference power limit I at $\mathrm{PU_{RX}}$ is reached with equality. For the sake of exposition, let us assume that the interference caused by $\mathrm{SU_{TX}}$ and $\mathrm{SU_R}$ to $\mathrm{PU_{RX}}$ is the same, i.e., $Q = I/2$. In this case, the transmit powers at $\mathrm{SU_{TX}}$ and $\mathrm{SU_R}$ are given by

$$P_s = \frac{Q}{|h_4|^2} \tag{8}$$

$$P_r = \frac{Q}{|h_5|^2} \tag{9}$$

Then, the received signal at $\mathrm{SU_{RX}}$ at discrete time i can be expressed as

$$y_i = G h_2 h_1 x_{i-1} + G h_2 s_{i-1} + G h_2 z_{r,i-1} + z_{d,i} \tag{10}$$

where $z_{d,i}$ is the interference from $\mathrm{PU_{TX}}$ to $\mathrm{SU_{RX}}$ plus noise. In particular, $z_{d,i}$ is approximated as an AWGN $\mathcal{CN}(0, Z_d)$ with zero-mean and variance

$$Z_d = N_0 + P_p d_7^{-n} \tag{11}$$

where d_7 denotes the distance from $\mathrm{PU_{TX}}$ to $\mathrm{SU_{RX}}$. Similarly, the received signal at eavesdropper E is given by

$$e_i = G h_3 h_1 x_{i-1} + G h_3 s_{i-1} + G h_3 z_{r,i-1} + z_{e,i} \tag{12}$$

where $z_{e,i}$ is a zero-mean AWGN $\mathcal{CN}(0, Z_e)$ with variance

$$Z_e = N_0 + P_p d_8^{-n} \tag{13}$$

and d_8 is the distance from $\mathrm{PU_{TX}}$ to E. In view of the above received signals, and interference and noise terms, the SINRs at $\mathrm{SU_{RX}}$ and E are given by (14) and (15) where $X_j = |h_j|^2, j = 1, \ldots, 5$ are the channel power gains of the respective links.

As the considered full-duplex CCRN is assumed to operate under Nagakami-m fading, the probability density function (PDF) of channel coefficient $R_j = |h_j|$ for such a channel with fading severity parameter m_j and channel mean power Ω_j is given by

$$f_{R_j}(r) = \frac{2}{\Gamma(m_j)} \left(\frac{m_j}{\Omega_i}\right)^{m_j} r^{2m_j - 1} \exp\left(-\frac{m_j}{\Omega_j} r^2\right) \tag{16}$$

where $\Gamma(\cdot)$ denotes the gamma function defined in [22, eq. (8.310.1)]. For integer values of m_j, the PDF of a Nagakami-m fading channel coefficient R_j can be expressed in the form of the PDF of a generalized Nagakami-m (GNM) fading channel coefficient with fading severity parameter m_j, shaping parameter ξ_j, and channel mean power Ω_j as

$$f_{R_j}(r) = \frac{2}{\Gamma(m_j)} \left(\frac{\beta_j}{\Omega_j}\right)^{\xi_j m_j} r^{2\xi_j m_j - 1} \exp\left(-\left(\frac{\beta_j}{\Omega_j}\right)^{\xi_j} r^{2\xi_j}\right) \tag{17}$$

where parameter $\xi_j = 1$ and β_j is defined as

$$\beta_j = \frac{\Gamma\left(m_j + \frac{1}{\xi_j}\right)}{\Gamma(m_j)} \tag{18}$$

In view of [23, eq. (2-3)], the PDF and the cumulative distribution function (CDF) of a generalized Nagakami-m fading channel coefficient R_j can also be expressed in the form of the Fox H-function as

$$f_{R_j}(r) = \frac{2}{\Gamma\left(m_j\right) r} H_{0,1}^{1,0}\left[\frac{\beta_j}{\Omega_j} r^2 \middle| \begin{matrix} - - - \\ \left(m_j, \frac{1}{\xi_j}\right) \end{matrix}\right] \tag{19}$$

$$F_{R_j}(r) = \frac{1}{\Gamma(m_j)} H_{1,2}^{1,1}\left[\frac{\beta_j}{\Omega_j} r^2 \middle| \begin{matrix} (1,1) \\ (m_j, \frac{1}{\xi_j})(0,1) \end{matrix}\right] \tag{20}$$

Note that the Fox H-function is defined in [24, eq. (8.3 .1)] by a Mellin-Barnes integral as

$$H_{p,q}^{m,n}\left[z \middle| \begin{matrix} (a_1, A_1) & (a_2, A_2) & \cdots & (a_p, A_p) \\ (b_1, B_1) & (b_2, B_2) & \cdots & (b_q, B_q) \end{matrix}\right] = \frac{1}{2\pi\iota} \int_L \frac{\left(\prod\limits_{k=1}^{m} \Gamma(b_k - B_k s)\right)\left(\prod\limits_{k=1}^{n} \Gamma(1 - a_k + A_k s)\right) z^s}{\left(\prod\limits_{k=m+1}^{q} \Gamma(1 - b_k + B_k s)\right)\left(\prod\limits_{k=n+1}^{p} \Gamma(a_k - A_k s)\right)} ds \tag{21}$$

where $\iota^2 = -1$, $0 \leq m \leq q$, $0 \leq n \leq p$, and L is a certain contour (suitable path) separating the poles of the two factors in the numerator such that the poles of $\Gamma(b_k - B_k s); k = 1, \ldots, m$ lie on the right side of the contour and the poles of $\Gamma\left(1 - a_k + A_k s\right); k = 1, \ldots, n$ lie on the left side of the contour.

III. Approximation of the Pseudo SINR

The secrecy capacity is the maximum rate that a transmitter can communicate to an intended receiver through the main channel while guaranteeing that an arbitrary small amount of information is received at the eavesdropper through a wiretap

$$\gamma_S(\mathbf{x}) = \frac{QZ_eX_1X_2{X_5}^{1+\lambda} + QZ_rX_2X_3X_4{X_5}^{\lambda} + Q^{1+\lambda}\beta X_2X_3X_4 + Q^{\lambda}\beta Z_eX_2X_4X_5 + Z_rZ_eX_2X_4X_5^{1+\lambda}}{QZ_dX_1X_3{X_5}^{1+\lambda} + QZ_rX_2X_3X_4{X_5}^{\lambda} + Q^{1+\lambda}\beta X_2X_3X_4 + Q^{\lambda}\beta Z_dX_3X_4X_5 + Z_rZ_dX_3X_4{X_5}^{1+\lambda}} \tag{24}$$

channel. As in [25], the secrecy capacity is mathematically expressed as the difference between the Shannon capacity of the main channel and the wiretap channel. In the context of the considered full-duplex underlay CCRN, the related instantaneous secrecy capacity is expressed as

$$C_s = [\log_2(1+\gamma_D) - \log_2(1+\gamma_E)]^+ = [\log_2(\gamma_S)]^+ \tag{22}$$

where $[\,\cdot\,]^+ = \max(\cdot, 0)$ and pseudo SINR γ_S is defined as

$$\gamma_S = \frac{1+\gamma_D}{1+\gamma_E} \tag{23}$$

In order to express the pseudo SINR γ_S as a function of the channel power gains X_j, let us define the vector $\mathbf{x} = [X_1, X_2, X_3, X_4, X_5]^T$. Then, γ_S can be rewritten in terms of $\mathbf{x}$ as in (24). Because the expression of γ_S in (24) is given in a rather cumbersome ratio of two polynomials, analyzing the secrecy capacity of the CCRN becomes complicated. Therefore, we utilize the approximation-and-fitting method described in [26] to approximate $\gamma_S(\mathbf{x})$ in (24) by a monomial function of channel power gains X_j as

$$\gamma_S(\mathbf{x}) \approx c\prod_{j=1}^{5} X_j^{a_j} \tag{25}$$

The parameters c and $a_j, j = 1, \ldots, 5$ of the approximation (25) can be calculated as follows.

Firstly, we apply the log-transform to both sides of (25) yielding

$$g(\mathbf{y}) \approx \log(c) + \sum_{j=1}^{5} a_j Y_j \tag{26}$$

where $Y_j = \log(X_j)$ and vector $\mathbf{y}$ is defined as

$$\mathbf{y} = [Y_1, Y_2, \ldots, Y_5]^T \tag{27}$$

Furthermore, $g(\cdot)$ is the log-transform of $\gamma_S(\cdot)$ giving

$$g(\mathbf{y}) = \log(\gamma_S(\mathbf{x})) \tag{28}$$

Let us define the following vector

$$\mathbf{a} = [a_1, a_2, ..., a_5]^T \tag{29}$$

Then, we can rewrite (26) as

$$g(\mathbf{y}) = \log(c) + \mathbf{a}^T\mathbf{y} \tag{30}$$

Secondly, we use the first order Taylor expansion of $g(\mathbf{y})$ at any value $\mathbf{y}_0$ that makes $g(\mathbf{y})$ differentiable at $\mathbf{y}_0$ and $g(\mathbf{y}) > 0$. Let $\mathbf{x}_0 = (\Omega_1, \Omega_2, \Omega_3, \Omega_4, \Omega_5)^T$ be a vector that contains the channel mean powers of the channel coefficients h_j, i.e., $\Omega_j = E\{X_j\}$. Here, we select $\mathbf{y}_0 = (\log\Omega_1, \log\Omega_2, \log\Omega_3, \log\Omega_4, \log\Omega_5)$ to approximate $g(\mathbf{y})$ as

$$g(\mathbf{y}) \approx g(\mathbf{y}_0) + \nabla g(\mathbf{y}_0)^T(\mathbf{y} - \mathbf{y}_0) \tag{31}$$

where $\boldsymbol{\nabla} g(\mathbf{y}_0)$ is the gradient of $g(\mathbf{y})$ at $\mathbf{y}_0$. From (30) and (31), we have

$$g(\mathbf{y}_0) - \nabla g(\mathbf{y}_0)^T\mathbf{y}_0 + \nabla g(\mathbf{y}_0)^T\mathbf{y} = \log(c) + \mathbf{a}^T\mathbf{y} \tag{32}$$

which implies that

$$\log(c) = g(\mathbf{y}_0) - \nabla g(\mathbf{y}_0)^T\mathbf{y}_0 \tag{33}$$

$$\mathbf{a} = \nabla g(\mathbf{y}_0) \tag{34}$$

As a result, the parameter a_j can be obtained by

$$a_j = \left.\frac{\partial(g(\mathbf{y}))}{\partial Y_j}\right|_{\mathbf{y}=\mathbf{y}_0} \tag{35}$$

Since $g(\mathbf{y}) = \log(\gamma_S(\mathbf{y}))$ and $Y_j = \log X_j$, we obtain a_j as

$$a_j = \left.\frac{X_j}{\gamma_S(\mathbf{x})}\,\frac{\partial\gamma_S(\mathbf{x})}{\partial X_j}\right|_{\mathbf{x}=\mathbf{x}_0} \tag{36}$$

From (33), the parameter c can be expressed as

$$c = \exp\left(g\left(\mathbf{y}_0\right) - \nabla g\left(\mathbf{y}_0\right)^T\mathbf{y}_0\right) \tag{37}$$

Substituting (34) into (37), we can write

$$c = \frac{\exp(g(\mathbf{y}_0))}{\exp(\mathbf{a}^T\mathbf{y}_0)} \tag{38}$$

From (28), the numerator of c is obtained as

$$\exp(g(\mathbf{y}_0)) = \gamma_S(\mathbf{x}_0) \tag{39}$$

After some modifications, we can derive the denominator of c from (27) and (29) as

$$\exp(\mathbf{a}^T\mathbf{y}_0) = \exp\left(\sum_{j=1}^{5} a_j\log(\Omega_j)\right) = \prod_{j=1}^{5}\Omega_j^{a_j} \tag{40}$$

Finally, substituting (39) and (40) into (38), we obtain

$$c = \gamma_S(\mathbf{x}_0)\prod_{j=1}^{5}\Omega_j^{-a_j} \tag{41}$$

After determining the parameters c and $a_j, j = 1, \ldots, 5$, the approximation of γ_S in (25) is fully specified.

IV. Secrecy Capacity of the Full-Duplex CCRN

Given the pseudo SINR γ_S in (25) along with the related parameters, we can now commence with deriving an analytical expression of the secrecy capacity C_{FD} of the full-duplex CCRN. For this purpose, let us define a random variable $Z = \prod_{j=1}^{5} X_j^{a_j}$ which allows us to write (25) as

$$\gamma_S = cZ \tag{42}$$

$$f_{\gamma_S}(\gamma) = \frac{2}{\gamma \prod_{l=1}^{5} \Gamma(m_l)} H_{0,5}^{5,0}\left[\frac{\gamma^2 \prod_{l=1}^{N} {m_l}^{2a_l}}{c^2 \prod_{l=1}^{N} {\Omega_l}^{2a_l}} \middle| \begin{array}{c} - - - \\ (m_1, 2a_1)(m_2, 2a_2)(m_3, 2a_3)(m_4, 2a_4)(m_4, 2a_4) \end{array} \right] \tag{49}$$

$$F_{\gamma_S}(\gamma) = \frac{1}{\prod_{l=1}^{5} \Gamma(m_l)} H_{1,6}^{5,1}\left[\frac{\gamma^2 \prod_{l=1}^{N} {m_l}^{2a_l}}{c^2 \prod_{l=1}^{N} {\Omega_i}^{2a_l}} \middle| \begin{array}{c} (1,1) \\ (m_1, 2a_1)(m_2, 2a_2)(m_3, 2a_3)(m_4, 2a_4)(m_4, 2a_4)(0,1) \end{array} \right] \tag{50}$$

The PDF and CDF of the pseudo SINR γ_S can then be obtained, respectively, by a simple transform of variables as

$$f_{\gamma_S}(\gamma) = \frac{1}{c} f_Z\left(\frac{\gamma}{c}\right) \tag{43}$$

$$F_{\gamma_S}(\gamma) = F_Z\left(\frac{\gamma}{c}\right) \tag{44}$$

Because $X_j^{a_j} = R_j^{2a_j} = |h_j|^{2a_j}$, the random variable Z is the product of power functions in $2a_j$ of five independent but non-identically distributed (i.n.i.d.) GNM channel coefficients R_j with fading severity parameter m_j, shaping parameter ξ_j, channel mean power Ω_j, and parameter β_j. Given [23, eq. (7-12)], the PDF and CDF of the product Z are given by

$$f_Z(z) = \frac{\kappa}{z} H_{0,5}^{5,0}\left[\frac{z^2}{\omega} \middle| \begin{array}{c} - - - \\ \phi_1, \phi_2, ..., \phi_5 \end{array} \right] \tag{45}$$

$$F_Z(z) = \frac{\kappa}{2} H_{1,6}^{5,1}\left[\frac{z^2}{\omega} \middle| \begin{array}{c} (1,1) \\ \phi_1, \phi_2, ..., \phi_5, (0,1) \end{array} \right] \tag{46}$$

where parameters κ, ω, and ϕ_j are defined as

$$\kappa = 2 \prod_{j=1}^{5} \frac{1}{\Gamma(m_j)}, \ \omega = \prod_{j=1}^{5} \left(\frac{\Omega_j}{\beta_j}\right)^{2a_j}, \ \phi_j \triangleq \left(m_j, \frac{2a_j}{\xi_j}\right) \tag{47}$$

In our case, we consider integer values of the fading severity parameter m_j of Nagakami-m fading, i.e. $\xi_j = 1$ and $\beta_j = m_j$. Then, parameters κ, ω, and ϕ_j are calculated as

$$\kappa = \frac{2}{\prod_{j=1}^{5} \Gamma(m_j)}, \ \omega = \frac{\prod_{j=1}^{5} \Omega_j^{2a_j}}{\prod_{j=1}^{5} m_j^{2a_j}}, \ \phi_j \triangleq (m_j, 2a_j) \tag{48}$$

By substituting (45), (46), and (48) into (43) and (44), after performing some mathematical conversions, the PDF and CDF of γ_S are obtained as in (49) and (50), respectively. Thus, the secrecy capacity of the full-duplex CCRN is given by

$$C_{\text{FD}} = \int_0^\infty \log(\gamma) f_{\gamma_S}(\gamma) d\gamma = \frac{1}{\ln 2} \int_0^\infty \frac{1 - F_{\gamma_S}(\gamma)}{1 + \gamma} d\gamma \tag{51}$$

Substituting (50) into (51), we obtain an analytically expression for the secrecy capacity of the full-duplex underlay CCRN. The obtained expression can be efficiently calculated using mathematical symbolic computation tools such as Mathematica.

V. Numerical Results

In this section, we provide numerical examples to illustrate the impact of system parameters such as fading conditions, transmit power and interference power limit of the PN, and distances between PN and CCRNs on the secrecy capacity of the full-duplex CCRN. Let d_1, d_2, d_3, d_4, d_5, d_6, d_7, and d_8 denote the normalized distances of the links $\text{SU}_{\text{TX}} \rightarrow \text{SU}_{\text{R}}$, $\text{SU}_{\text{R}} \rightarrow \text{SU}_{\text{RX}}$, $\text{SU}_{\text{R}} \rightarrow \text{E}$, $\text{SU}_{\text{TX}} \rightarrow \text{PU}_{\text{RX}}$, $\text{SU}_{\text{R}} \rightarrow \text{PU}_{\text{RX}}$, $\text{PU}_{\text{TX}} \rightarrow \text{SU}_{\text{R}}$, $\text{PU}_{\text{TX}} \rightarrow \text{SU}_{\text{RX}}$, $\text{PU}_{\text{TX}} \rightarrow \text{E}$, respectively. The system is assumed to operate in an urban area cellular radio environment where the path-loss exponent of all channel is selected as $n = 3$.

Fig. 2 depicts the secrecy capacity of the CCRN versus interference power-to-noise ratio Q/N_0 of the PN for different fading severity parameters m. In these examples, normalized distances are selected as $d_1 = d_2 = 0.5$, $d_3 = 1.2$, $d_4 = d_5 = 0.8$, and $d_6 = d_7 = d_8 = 1.2$. Further, the transmit signal-to-noise ratio (SNR) of the PN is fixed at $P_P/N_0 = 12$ dB and the SI parameters due to the full-duplex mode of the relay are selected as $\lambda = \beta = 0.1$. Three cases of fading severity parameters are examined, i.e., from Rayleigh fading $m_j = 1$ to less severe fading intensity $m_j = 2$ and $m_j = 3, j \in \{1, \ldots, 8\}$. Fig. 2 shows that the secrecy capacity significantly increases as the fading severity parameters increase. In other words, both the communication and eavesdropper link benefit from the decreasing fading intensity. Further, the secrecy capacity increases with the increase of Q/N_0, i.e. when the PN tolerates higher interference power. It also indicates that it may be beneficial to balance security mechanisms between physical layer and higher layers of the protocol stack depending on the Q/N_0 imposed by the PN.

Fig. 3 illustrates the effect of the transmit SNR P_P/N_0 of the PN on the secrecy capacity of the full-duplex CCRN. Here, the normalized distances among PN and CCRN, and SI parameters are selected as in Fig. 2. The fading severity parameters are fixed $\forall j : m_j = 2$. Apparently, increasing the transmit SNR of the PN causes increased interference to the full-duplex CCRN as well as to the eavesdropper. This, in turn, reduces the capacity on these links as well as the resulting secrecy capacity. As for the progression of secrecy capacity versus interference power-to-noise ratio, secrecy capacity increases because the interference power constraint of the PN becomes looser. This allows the nodes in the full-duplex CCRN to transmit with higher power.

Fig. 4 and Fig. 5 show the effect of interference link distances between the PN, CCRN, and eavesdropper on secrecy capacity. In particular, Fig. 4 varies the normalized distances d_4 and d_5 of the interference links from the CCRN to PU_{RX} while fixing the normalized distances of the interference links from PU_{TX} to the CCRN and eavesdropper as $d_6 = d_7 =$

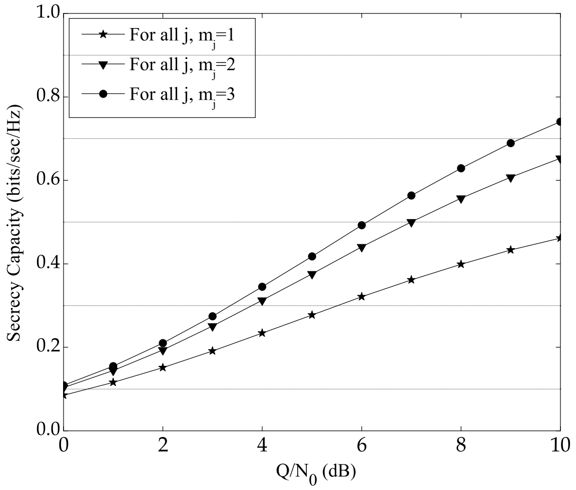

Fig. 2. Secrecy capacity of the CCRN versus interference power-to-noise ratio of the PN for different fading severity parameters.

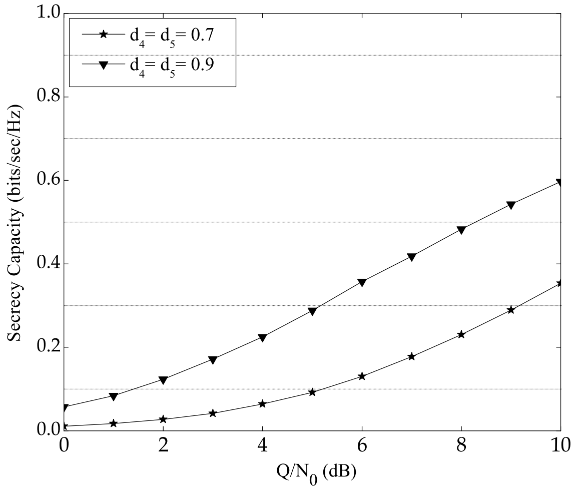

Fig. 4. Secrecy capacity of the CCRN versus interference power-to-noise ratio for different interference distances from CCRN to $\mathrm{PU_{RX}}$.

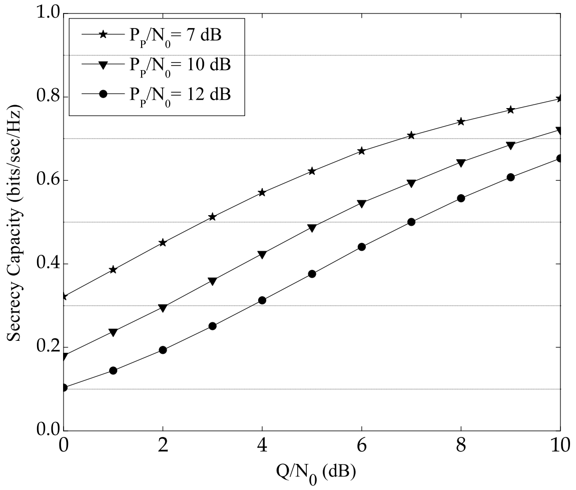

Fig. 3. Secrecy capacity of the CCRN versus interference power-to-noise ratio for various transmit SNRs of the PN.

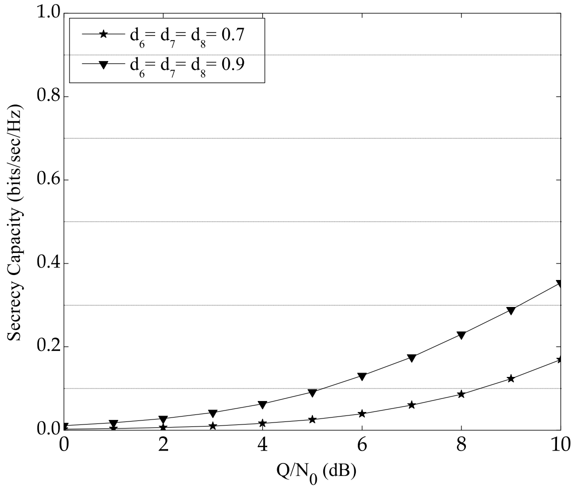

Fig. 5. Secrecy capacity of the CCRN versus interference power-to-noise ratio for different interference distances from $\mathrm{PU_{TX}}$ to CCRN and eavesdropper.

$d_8 = 0.9$ In contrast, in Fig. 5, we vary the interference distances d_6 and d_7 from $\mathrm{PU_{TX}}$ to the CCRN and d_8 from $\mathrm{PU_{TX}}$ to the eavesdropper. The common parameters applicable to both figures are the normalized distances $d_1 = d_2 = 0.5$, and $d_3 = 1.2$, transmit SNR of the PN is set as 12 dB, SI parameters remain as $\lambda = \beta = 0.1$ and fading severity parameters are set $\forall j : m_j = 2$. From Fig. 4, it can be seen that secrecy capacity increases when the PN is farther away from the full-duplex CCRN. This is because the nodes in the full-duplex CCRN can transmit with higher power the farther the PN is away. Similarly, the results in Fig. 5 show that the secrecy capacity improves when the primary transmitter is farther away because it inflicts lower interference to both full-duplex CCRN and eavesdropper.

Finally, Fig. 6 compares the secrecy capacity obtained with full-duplex relay and half-duplex relay. The varies normalized distances of the PN and CCRN are selected as $d_3 = 1.2$, $d_4 = d_5 = 0.9$, and $d_6 = d_7 = d_8 = 1.2$. The transmit SNR of the PN is set to $P_P/N_0 = 10$ dB and the SI parameters of the full-duplex relay are selected as Case 1: $\lambda = \beta = 0.1$ with normalized distances $d_1 = d_2 = 0.5$, and Case 2: $\lambda = 1$, $\beta = 0, 0.1, 0.2$ with normalized distances $d_1 = d_2 = 0.4$.

As for Case 1, in the low Q/N_0 regime 0–2 dB, the secrecy capacity of the CCRN for full-duplex and half-duplex relaying differ not much. This is because the interference power limit in this Q/N_0 range is rather strict allowing the nodes in the CCRN to transmit only with relatively low power. The advantages of higher spectrum efficiency appears to be diminished by SI and low link capacities for low transmit powers. The advantage of higher spectrum efficiency offered by the full-duplex relay compared to the impairments caused by SI becomes much more pronounced in the high Q/N_0 regime 2–10 dB resulting in a significantly higher secrecy capacity compared to half-duplex relaying. Regarding Case 2, the secrecy capacity of the CCRN for full-duplex is significantly larger compared to half-duplex relaying for the selected SI parameters. However, an increase of the SI parameter β from 0 (no SI) over 0.1 to 0.2 causes the secrecy capacity of the

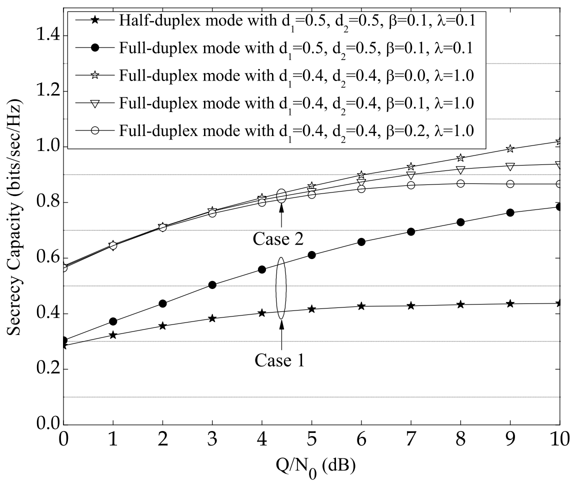

Fig. 6. Secrecy capacity of full-duplex and half-duplex CCRN versus interference power-to-noise ratio.

full-duplex CCRN to decrease.

Although the secrecy capacity is rather low in the low interference power-to-noise ratio regime for some of the shown results, it should be noted that the secrecy capacity is measured here in bits/sec/Hz and would hence need to be multiplied by the bandwidth of the particular system at hand.

VI. Summary

In this paper, we have analyzed the secrecy capacity of a full-duplex underlay CCRN. An approximation-and-fitting method has been applied to simplify the complicated expression of the pseudo SINR in the CCRN. Based on the obtained simpler polynomial form of the pseudo SINR, an expression for the secrecy capacity has been derived. Numerical results have been provided showing the effect of system settings such as fading severity parameter, transmit power and interference power limit of the PN, parameters of the full-duplex mode, and link distances on secrecy capacity. Finally, a comparison of the secrecy capacity offered by full-duplex and half-duplex relaying has been provided revealing operational modes under which the full-duplex CCRN significantly outperforms the half-duplex CCRN. As such, our results contribute towards an understanding of designing full-duplex CCRNs in the presence of eavesdroppers.

References

[1] J. Harshan, S. Y. Chang, and Y. C. Hu, "Insider-attacks on physical-layer group secret-key generation in wireless networks," in *Proc. IEEE Wireless Commun. and Netw. Conf.*, San Francisco, USA, May 2017, pp. 1–6.

[2] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE Trans. Commun.*, vol. 10, no. 2, pp. 431–436, Feb. 2011.

[3] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, "Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930–3941, May. 2017.

[4] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular Ad Hoc networks," *IEEE Trans. on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016.

[5] L. Lai and H. E. Gamal, "Cooperative secrecy: The relay-eavesdropper channel," in *Proc. IEEE Int. Symp. on Inf. Theory*, Nice, France, Jun. 2007, pp. 931–935.

[6] T. X. Zheng, H. M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless Ad Hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. PP, no. 99, pp. 1–30, Mar. 2017.

[7] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[9] A. Kaushik, S. K. Sharma, S. Chatzinotas, B. Ottersten, and F. K. Jondral, "Sensing-throughput tradeoff for interweave cognitive radio system: A deployment-centric viewpoint," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3690–3702, May 2016.

[10] S. Mosleh, J. Abouei, and M. R. Aghabozorgi, "Distributed opportunistic interference alignment using threshold-based beamforming in MIMO overlay cognitive radio," *IEEE Trans. Veh. Technol.*, vol. 63, no. 8, pp. 3783–3793, Oct. 2014.

[11] C. Lameiro, I. Santamaria, and P. J. Schreier, "Benefits of improper signaling for underlay cognitive radio," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 22–25, Feb. 2015.

[12] T. V. Mai, J. A. Molnar, and K. Rudd, "Security vulnerabilities in physical layer of cognitive radio," in *Proc. International Midwest Symposium on Circuits and Systems*, Seoul, Korea, Aug. 2011, pp. 1–4.

[13] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 1023–1043, Feb. 2015.

[14] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with Poisson distributed eavesdroppers," *IEEE Trans. on Inf. Forensics and Security*, vol. 11, no. 2, pp. 373–387, Feb. 2016.

[15] A. H. A. El-Malek and S. A. Zummo, "Cooperative cognitive radio model for enhancing physical layer security in two-path amplify-and-forward relaying networks," in *Proc. IEEE Global Commun. Conf.*, San Diego, USA, Dec. 2015, pp. 1–6.

[16] T. M. C. Chu and H. J. Zepernick, "On capacity of full-duplex cognitive cooperative radio networks with optimal power allocation," in *Proc. IEEE Wireless Commun. and Networking Conf.*, San Francisco, USA, Mar. 2017, pp. 1–6.

[17] J. Zhang, G. Pan, and H. M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, no. 16217716, pp. 3887–3893, Jul. 2016.

[18] M. Aljuaid and H. Yanikomeroglu, "Investigating the Gaussian convergence of the distribution of the aggregate interference power in large wireless networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 9, pp. 4418–4424, Nov. 2010.

[19] H. Inaltekin, "Gaussian approximation for the wireless multi-access interference distribution," *IEEE Trans. Signal Process.*, vol. 60, no. 11, pp. 6114–6120, Nov. 2012.

[20] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.

[21] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *Journal of Applied Mathematics and Stochastic Analysis*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[22] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.

[23] F. Yilmaz and M. S. Alouini, "Product of the powers of generalized Nakagami-m variates and performance of cascaded fading channels," in *Proc. IEEE Global Telecommun. Conf.*, Honolulu, USA, Nov. 2009, pp. 1–8.

[24] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and series: Volume 3, More Special Functions*. New York: Gordon and Breach Science Publishers, 1990.

[25] 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. 2009.

[26] M. Chiang, "Geometric programming for communication systems," *Foundations and Trends in Communications and Information Theory*, vol. 2, no. 1/2, pp. 1–154, 2005.