VNU Journal of Science: Comp. Science & Com. Eng, Vol. 34, No. 1 (2018) 52–62

VNU Journal of Science:
Computer Science and Communication Engineering

Journal homepage: http://www.jcsce.vnu.edu.vn/index.php/jcsce

Impacts of Licensed Interference and Inaccurate Channel Information on Information Security in Spectrum Sharing Environment

Do Dac Thiem[1,2], Ho Van Khuong[1,*]

[1] *Department of Telecommunications Engineering, Ho Chi Minh City University of Technology, No. 268 Ly Thuong Kiet Street, Ward 14, District 10, Ho Chi Minh City, Vietnam*

[2] *Faculty of Information Technology and Electrical Electronic Engineering, Thu Dau Mot University, No. 6 Tran Van On Street, Thu Dau Mot City, Binh Duong Province, Vietnam*

Abstract

Spectrum sharing environment creates cross-interference between licensed network and unlicensed network. Most existing works consider unlicensed interference (i.e., interference from unlicensed network to licensed network) while ignoring licensed interference (i.e., interference from licensed network to unlicensed network). Moreover, existing channel estimation algorithms cannot exactly estimate channel information. In this paper, impacts of licensed interference and inaccurate channel information on information security in the spectrum sharing environment is analyzed under peak transmit power bound, peak interference power bound, and Rayleigh fading. Toward this end, a secrecy outage probability formula is proposed in an exact form and validated by simulations. Various results illustrate that secrecy outage probability is constant in a range of large peak interference powers or large peak transmit powers, and is severely affected by licensed interference and inaccurate channel information.

Received 16 March 2018, Revised 12 June 2018, Accepted 01 July 2018

Keywords: Information security, underlay, inaccurate channel information.

1. Introduction

Increasing emergence of new wireless applications and inefficient licensed radio spectrum utilization have pushed spectrum scarcity circumstance more and more severe. In the spectrum sharing[1] environment, secondary/unlicensed users (namely, cognitive radios) can overcome such a circumstance by exploiting unutilized frequency bands of primary/licensed users in a wise manner [1]. Cognitive radios preferably operate in the underlay mode [2] where their communications is allowed on licensed frequency band unless such communications does not cause any harm to licensed users. This can be achieved by limiting the power of unlicensed transmitters such that interference power induced at licensed

* Corresponding author. Email.: khuong.hovan@yahoo.ca
https://doi.org/10.25073/2588-1086/vnucsce.199
[1]Spectrum sharing and cognitive radio are interchangeably used in this paper.

receivers is below a tolerable level, which is known as peak interference power [3]. Moreover, transmit power of unlicensed users is limited by its designed peak transmit power. Both peak transmit power bound and interference power bound impose a strict power allocation for unlicensed users [4]. Furthermore, simultaneous transmission of licensed and unlicensed users causes cross-interference between them and hence, licensed interference cannot be neglected in general and practical set-ups[2].

Permitting unlicensed users to utilize frequency bands of licensed users induces the spectrum sharing environment more vulnerable to malicious wire-tapping than the spectrum non-sharing environment. Consequently, besides efficiently exploiting the spectrum sharing technology for improving spectrum utilization efficiency, information security problem in the spectrum sharing environment needs a special attention. An emerging modern solution to secure information transmission in the spectrum sharing environment is the physical layer security technology, which utilizes physical characteristics of wireless channels to mitigate interception of wire-tappers [17, 18]. However, physical characteristics of wireless channels (shortly, channel information) must be estimated and hence, they cannot be available without any error [19–23]. As such, the impact of inaccurate channel information on security performance of physical layer security techniques in the spectrum sharing environment needs to be addressed.

Results on the secrecy outage probability (SOP) in the spectrum sharing environment under interference power bound and peak transmit power bound are presented in [24–32]. More specifically, the authors in [24–26] present the SOP analysis for the partial relay selection in the dual-hop full-duplex spectrum sharing environment, multi-hop relaying with multi-antenna half-duplex receivers, and non-relaying with a multi-antenna full-duplex receiver, respectively. Different from [24] in the relay selection scheme and the operation mode, [27] analyzes the SOP for K^{th} best relay selection in the half-duplex spectrum sharing environment. In [28] and [29], transmit antenna selection in the half-duplex spectrum sharing environment with multi-antenna terminals is proposed to improve security performance. Nevertheless, [24–29] do not take into account two important conditions of licensed interference and channel information inaccuracy in the SOP analysis. In [30], the SOP analysis for the partial relay selection in the half-duplex spectrum sharing environment is implemented with consideration of outdated relay-destination channel information but licensed interference is ignored. In [31], only simulated results on the SOP in the spectrum sharing environment with energy harvesting are provided without consideration of channel information inaccuracy and licensed interference. The authors in [32] present the SOP analysis in the multi-hop relaying spectrum sharing environment but neglect licensed interference and peak transmit power bound. Furthermore, [32] assumes channel information inaccuracy only for channels from unlicensed transmitters to licensed receivers.

The literature review in [24–32] reveals that the SOP analysis in the spectrum sharing environment under practical and general conditions including channel information inaccuracy for all channels, licensed interference, interference power bound and peak transmit power bound is still an open problem, which is targeted to solve in this paper. To be continued, Section 2 presents system and channel models under consideration. Then, the SOP is analyzed in Section 3. Also, a possible extension to other analyses such as non-zero secrecy capacity probability and intercept probability is discussed in the end of Section 3. Analytical and simulated results to validate the proposed analysis and to evaluate security performance in key specifications are provided in Section 4. Finally, conclusions terminate the paper in Section 5.

[2]Licensed interference is ignored in most published works for analysis tractability (e.g., [5–16]).

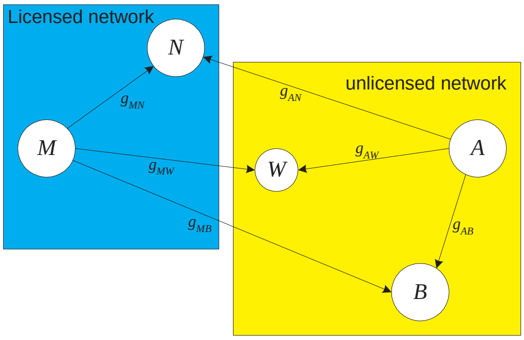

Figure 1. System model.

2. System and channel models

Consider a spectrum sharing environment as shown in Figure 1 where an unlicensed network comprises an unlicensed transmitter A, an unlicensed receiver B, and an unlicensed wire-tapper W while a licensed network consists of a licensed transmitter M and a licensed receiver N. A communicates with B at the same time that M communicates with N. As such, cross-interference between these communications incurs. Most existing works only consider interference from unlicensed transmitters to licensed receivers while ignoring interference from licensed transmitters to unlicensed receivers (e.g., [5–16]). Although neglecting the licensed interference is reasonable in some scenarios (e.g., the licensed transmitter M is distant from the unlicensed receivers (B, W) or the licensed interference is Gaussian-distributed), practical and general scenarios should account for this interference. As such, the current paper investigates this interference to well fit such general and practical scenarios. It is assumed that W is merely interested in wire-tapping information communicated between A and B. This assumption is practical for several system set-ups such as [18, 24–32].

In Figure 1, g_{uv} denotes a $\mathrm{u} \to \mathrm{v}$ channel coefficient with $\mathrm{u} \in \{M, A\}$ and $\mathrm{v} \in \{N, B, W\}$. For independent frequency non-selective Rayleigh fading channels under consideration, g_{uv} is modelled as a zero-mean ρ_{uv}-variance circular symmetric complex Gaussian random variable (r.v.). Mathematically, such a random variable is written as $g_{\mathrm{uv}} \sim \mathcal{CN}(0, \rho_{\mathrm{uv}})$. The real channel coefficient g_{uv} must be estimated at corresponding receiver v for signal detection. Due to the limited accuracy of the current channel estimation algorithms, the estimated channel coefficient $\hat{g}_{\mathrm{uv}}$ cannot exactly match g_{uv}. If β_{uv} denotes a correlation factor between g_{uv} and $\hat{g}_{\mathrm{uv}}$, then the relation between g_{uv} and $\hat{g}_{\mathrm{uv}}$ can be modelled as

$$\hat{g}_{\mathrm{uv}} = \beta_{\mathrm{uv}} g_{\mathrm{uv}} + \sqrt{1 - \beta_{\mathrm{uv}}^2} \epsilon_{\mathrm{uv}}, \quad (1)$$

according to widely accepted works (e.g., [19–23]) where ϵ_{uv} is the channel estimation error and both ϵ_{uv} and $\hat{g}_{\mathrm{uv}}$ are modeled as $\mathcal{CN}(0, \rho_{\mathrm{uv}})$. Moreover, $0 \leq \beta_{\mathrm{uv}} \leq 1$ represents the quality of channel estimators and hence, the larger the β_{uv} is, the more accurate the channel estimation is.

Obviously, the current system model differs those in the open literature of the SOP analysis in the spectrum sharing environment (e.g., [24–32]) in two key points: *i*) the licensed interference is taken into account and *ii*) channel information at all corresponding receivers is not assumed to be perfectly known (this is reflected in (1)). These two key points make the problem of the SOP analysis in the spectrum sharing environment not only practical and general but also complicated as shown in the following. Solving such a problem will bring complete and valuable insights on information security performance in the spectrum sharing environment. As such, this problem deserves to be treated in our paper.

In the spectrum sharing environment, unlicensed transmitters are permitted to transmit information concurrently with information transmission of licensed transmitters. Nevertheless, interference caused by unlicensed transmitters to licensed receivers must be below a tolerable level. Additionally, unlicensed transmitters must send their information with a designed peak transmit power. Moreover, this paper investigates inaccurate channel information at receivers. Combining all conditions (interference power bound, peak transmit power bound, information channel inaccuracy) together, the unlicensed transmitter A allocates its power as

$$P_A = \min\left(\frac{I_p}{|\hat{g}_{AN}|^2}, P_p\right), \tag{2}$$

according to [21] where P_p is the peak transmit power of unlicensed transmitters and I_p is the peak interference power tolerated by licensed receivers.

As shown in Figure 1, A transmits the signal x_A with the power of P_A at the same time that M transmits the signal x_M with the power of P_M. As such, the received signal at $\mathrm{v} \in \{B, W\}$ is modeled as

$$y_{\mathrm{v}} = g_{A\mathrm{v}} x_A + g_{M\mathrm{v}} x_M + n_{\mathrm{v}}, \tag{3}$$

where $n_{\mathrm{v}} \sim \mathcal{CN}(0, \sigma^2)$ is the thermal noise at the receiver v.

Plugging (1) into (3) results in

$$y_{\mathrm{v}} = \frac{\hat{g}_{A\mathrm{v}}}{\beta_{A\mathrm{v}}} x_A - \frac{\sqrt{1-\beta_{A\mathrm{v}}^2}}{\beta_{A\mathrm{v}}} \epsilon_{A\mathrm{v}} x_A + g_{M\mathrm{v}} x_M + n_{\mathrm{v}}. \tag{4}$$

Because the receiver v merely has the estimated channel information $\hat{g}_{A\mathrm{v}}$, the first term in (4) is the desired signal while the remaining terms in (4) are a combination of interferences and noise. Therefore, the signal-to-interference plus noise ratio (SINR) at $\mathrm{v} \in \{B, W\}$ is computed from (4) as

$$\begin{aligned}\Phi_{\mathrm{v}} &= \frac{\Xi_{x_A}\left\{\left|\frac{\hat{g}_{A\mathrm{v}}}{\beta_{A\mathrm{v}}} x_A\right|^2\right\}}{\Xi_{\epsilon_{A\mathrm{v}}, x_A, x_M, n_{\mathrm{v}}}\left\{\left|g_{M\mathrm{v}} x_M + n_{\mathrm{v}} - \frac{\sqrt{1-\beta_{A\mathrm{v}}^2}}{\beta_{A\mathrm{v}}} \epsilon_{A\mathrm{v}} x_A\right|^2\right\}} \\ &= \frac{|\hat{g}_{A\mathrm{v}}|^2 P_A}{\left(1-\beta_{A\mathrm{v}}^2\right)\rho_{A\mathrm{v}} P_A + |g_{M\mathrm{v}}|^2 \beta_{A\mathrm{v}}^2 P_M + \beta_{A\mathrm{v}}^2 \sigma^2},\end{aligned} \tag{5}$$

where $\Xi_Y\{\cdot\}$ is the statistical average with respect to the r.v. Y.

The $A - \mathrm{v}$ channel capacity, $\mathrm{v} \in \{B, W\}$, is given by

$$C_{A\mathrm{v}} = \log_2(1 + \Phi_{\mathrm{v}}). \tag{6}$$

According to [33], the secrecy capacity, R_s, is the difference between the $A - B$ main channel capacity and the $A - W$ wire-tapping channel capacity, i.e.

$$\begin{aligned} R_s &= \max(C_{AB} - C_{AW}, 0) \\ &= \max\left(\log_2\left(\frac{1+\Phi_B}{1+\Phi_W}\right), 0\right). \end{aligned} \tag{7}$$

3. Secrecy outage probability analysis

The secrecy outage probability is a critical security performance metric in information-theoretic aspect. This section derives a SOP formula for the spectrum sharing environment under inaccurate channel information, licensed interference, peak transmit power bound, and interference power bound. The proposed SOP formula can be used directly to find the non-zero achievable secrecy capacity probability formula and the intercept probability formula. Such formulas are helpful in completely assessing the security performance in the spectrum sharing environment without exhaustive Monte-Carlo simulations.

A secrecy outage event is captured as the secrecy capacity R_s falls below an expected security level R_0. If $\Pr\{\mathcal{H}\}$ denotes the probability that the event $\mathcal{H}$ happens, then the SOP is expressed as

$$\mathcal{S}(R_0) = \Pr\{R_s < R_0\}. \tag{8}$$

Substituting (7) into (8) results in

$$\begin{aligned}
\mathcal{S}(R_0) &= \Pr\left\{\left[\log_2\left(\frac{1+\Phi_B}{1+\Phi_W}\right)\right]^+ < R_0\right\} \\
&= \Pr\{\Phi_B < \Phi_W\}\Pr\{0 < R_0 | \Phi_B < \Phi_W\} \\
&+ \Pr\{\Phi_B > \Phi_W\}\times \\
&\Pr\left\{\log_2\left(\frac{1+\Phi_B}{1+\Phi_W}\right) < R_0 \middle| \Phi_B > \Phi_W\right\} \\
&= \Pr\{\Phi_B < \Phi_W\} \\
&+ \Pr\{\Phi_B > \Phi_W\}\times \\
&\Pr\left\{\Phi_B < 2^{R_0}(1+\Phi_W) - 1 \middle| \Phi_B > \Phi_W\right\} \\
&= \Pr\{\Phi_B < 2^{R_0}(1+\Phi_W) - 1\}.
\end{aligned} \tag{9}$$

In (9), Φ_B and Φ_W are statistically dependent because they contain P_A according to (5). Consequently, (9) can be solved in two steps. The first step relates the computation of the conditional probability conditioned on P_A, namely $\Theta = \Pr\{\Phi_B < 2^{R_0}(1+\Phi_W) - 1 | P_A\}$ and the second step averages Θ over P_A. If $f_Y(y|P_A)$ and $F_Y(y|P_A)$ denote the conditional probability density function (PDF) and the conditional cumulative distribution function (CDF) of the r.v. Y conditioned on P_A, correspondingly, then (9) is rewritten as

$$\mathcal{S}(R_0) = \Xi_{P_A}\{\Theta\}, \tag{10}$$

where

$$\Theta = \int_0^\infty F_{\Phi_B}\left(2^{R_0}[1+y] - 1 \middle| P_A\right) f_{\Phi_W}(y|P_A)\,dy. \tag{11}$$

In the following, we first derive $F_{\Phi_B}(x|P_A)$ and $f_{\Phi_W}(x|P_A)$ and then compute (11), which indirectly completes (10).

Lemma 1. *The conditional CDF of Φ_B conditioned on P_A is represented in closed-form as*

$$F_{\Phi_B}(x|P_A) = 1 - \frac{\rho_{AB}P_A e^{-\lambda_{AB}x}}{\rho_{AB}P_A + \beta_{AB}^2\rho_{MB}P_M x}, \tag{12}$$

where

$$\lambda_{AB} = 1 - \beta_{AB}^2 + \frac{\beta_{AB}^2\sigma^2}{\rho_{AB}P_A}. \tag{13}$$

Proof. The SINR at B in (5) can be rewritten as $\Phi_B = \frac{T}{H}$ where $T = |\hat{g}_{AB}|^2 P_A$ and $H = \left(1-\beta_{AB}^2\right)\rho_{AB}P_A + |g_{MB}|^2\beta_{AB}^2 P_M + \beta_{AB}^2\sigma^2$. It is recalled that $\hat{g}_{AB} \sim \mathcal{CN}(0,\rho_{AB})$ and $g_{MB} \sim \mathcal{CN}(0,\rho_{MB})$ and hence, the conditional PDFs of T and H conditioned on P_A are correspondingly expressed as

$$f_T(t|P_A) = \frac{e^{-\frac{t}{P_A\rho_{AB}}}}{P_A\rho_{AB}}, \quad t \geq 0 \tag{14}$$

$$f_H(h|P_A) = \frac{e^{-\frac{h-\tau}{\beta_{AB}^2 P_M\rho_{MB}}}}{\beta_{AB}^2 P_M\rho_{MB}}, \quad h \geq \tau \tag{15}$$

where

$$\tau = \left(1-\beta_{AB}^2\right)\rho_{AB}P_A + \beta_{AB}^2\sigma^2. \tag{16}$$

Given $\Phi_B = \frac{T}{H}$ and with the help of [36, eq. (6-58)], the conditional CDF of Φ_B conditioned on P_A is represented as

$$F_{\Phi_B}(x|P_A) = \int_\tau^\infty \left[\int_0^{xh} f_T(t|P_A)\,dt\right] f_H(h|P_A)\,dh. \tag{17}$$

Plugging $f_T(t|P_A)$ in (14) and $f_H(h|P_A)$ in (15) into (17) and after some algebraic manipulations, (17) is simplified to (12), accomplishing the proof. □

Lemma 2. *The closed form of the conditional PDF of Φ_W conditioned on P_A is given by*

$$f_{\Phi_W}(x|P_A) = \omega\lambda_{AW}\frac{e^{-\lambda_{AW}x}}{x+\omega} + \omega\frac{e^{-\lambda_{AW}x}}{(x+\omega)^2}, \tag{18}$$

where

$$\lambda_{AW} = 1 - \beta_{AW}^2 + \frac{\beta_{AW}^2\sigma^2}{\rho_{AW}P_A}, \tag{19}$$

$$\omega = \frac{\rho_{AW}P_A}{\beta_{AW}^2\rho_{MW}P_M}. \tag{20}$$

Proof. By replacing B with W in (12), the conditional CDF of Φ_W conditioned on P_A can be accomplished as

$$F_{\Phi_W}(x|P_A) = 1 - \frac{\rho_{AW}P_A e^{-\lambda_{AW}x}}{\rho_{AW}P_A + \beta_{AW}^2\rho_{MW}P_M x}, \quad (21)$$

where λ_{AW} is given by (19).

The conditional PDF of Φ_W conditioned on P_A can be inferred from (21) as (22) at the top of the next page.

Using ω in (20), one can represent (22) as (18), accomplishing the proof. □

Changing variables in (12) and (18) appropriately and then plugging the results into (11), the compact form of (11) is obtained as

$$\Theta = \int_0^\infty \left[1 - \zeta\frac{e^{-\lambda_{AB}2^{R_0}x}}{x+\delta}\right] \times \left[\omega\lambda_{AW}\frac{e^{-\lambda_{AW}x}}{x+\omega} + \omega\frac{e^{-\lambda_{AW}x}}{(x+\omega)^2}\right]dx, \quad (23)$$

where

$$\zeta = \frac{\rho_{AB}P_A e^{-\lambda_{AB}(2^{R_0}-1)}}{\beta_{AB}^2\rho_{MB}P_M 2^{R_0}}, \quad (24)$$

$$\delta = \frac{\rho_{AB}P_A}{\beta_{AB}^2\rho_{MB}P_M 2^{R_0}} + \frac{2^{R_0}-1}{2^{R_0}}. \quad (25)$$

Decomposing (23) by using the partial fraction expansion, one obtains (26).

It is seen that (26) can be solved in closed-form after expressing integral forms of $\int_0^\infty \frac{e^{-qx}}{x+p}dx$ and $\int_0^\infty \frac{e^{-qx}}{(x+p)^2}dx$ in closed-form. Given the definition of the exponential integral function $Ei(\cdot)$ in [34], one can express $\int_0^\infty \frac{e^{-qx}}{x+p}dx$ in closed-form as

$$\int_0^\infty \frac{e^{-qx}}{x+p}dx = -e^{qp}Ei(-qp). \quad (27)$$

Meanwhile, applying the integral by part to $\int_0^\infty \frac{e^{-qx}}{(x+p)^2}dx$ and then using the result in (27), one can express $\int_0^\infty \frac{e^{-qx}}{(x+p)^2}dx$ in closed-form as

$$\int_0^\infty \frac{e^{-qx}}{(x+p)^2}dx = \frac{1}{p} + qe^{qp}Ei(-qp). \quad (28)$$

Applying (27) and (28) with appropriate variable changes for integrals in the last equality of (26), one obtains (29) in the next page.

Let $X = |\hat{g}_{AN}|^2$. According to (2), P_A is a function of X. Moreover, λ_{AB} in (13), λ_{AW} in (19), ω in (20), ζ in (24), δ in (25) are functions of P_A and thus, they are also functions of X. Therefore, the conditional SOP Θ in (29) conditioned on P_A is also a function of X. Because $\hat{g}_{AN} \sim \mathcal{CN}(0, \rho_{AN})$, X has a PDF as $f_X(x) = \frac{1}{\rho_{AN}}e^{-\frac{x}{\rho_{AN}}}$, $x \geq 0$. By statistically averaging Θ over X, one obtains the exact formula of the SOP in (10) in terms of the single-variable integral, i.e.

$$\mathcal{S}(R_0) = \int_0^\infty \Theta f_X(x)\,dx = \frac{1}{\rho_{AN}}\int_0^\infty e^{-\frac{x}{\rho_{AN}}}\Theta dx. \quad (30)$$

It is noted that the single-variable integral can be numerically evaluated in most computation softwares such as Matlab, Mathematica, ... Under the support of these computation softwares, the SOP in (30) can be computed for fast security performance assessment in key specifications. According to the authors' knowledge, the exact formula in (30), which accounts for multiple practical conditions such as licensed interference, inaccurate channel information at all receivers, peak transmit power bound, and interference power bound, has not been presented in any published works. In addition, (30) can be used to infer other important security performance metrics such as the non-zero secrecy capacity probability and the intercept probability, as well as to eliminate exhaustive Monte-Carlo simulations in security performance evaluation.

$$
\begin{aligned}
f_{\Phi_W}(x|P_A) &= \frac{dF_{\Phi_W}(x|P_A)}{dx} \\
&= -\rho_{AW}P_A \frac{-\lambda_{AW}e^{-\lambda_{AW}x}\left(\rho_{AW}P_A + \beta_{AW}^2\rho_{MW}P_M x\right) - e^{-\lambda_{AW}x}\beta_{AW}^2\rho_{MW}P_M}{\left(\rho_{AW}P_A + \beta_{AW}^2\rho_{MW}P_M x\right)^2}.
\end{aligned} \tag{22}
$$

$$
\begin{aligned}
\Theta &= \omega\lambda_{AW}\int_0^\infty \frac{e^{-\lambda_{AW}x}}{x+\omega}dx + \omega\int_0^\infty \frac{e^{-\lambda_{AW}x}}{(x+\omega)^2}dx \\
&- \zeta\omega\lambda_{AW}\int_0^\infty \frac{e^{-(\lambda_{AB}2^{R_0}+\lambda_{AW})x}}{(x+\delta)(x+\omega)}dx - \zeta\omega\int_0^\infty \frac{e^{-(\lambda_{AB}2^{R_0}+\lambda_{AW})x}}{(x+\delta)(x+\omega)^2}dx \\
&= \omega\lambda_{AW}\int_0^\infty \frac{e^{-\lambda_{AW}x}}{x+\omega}dx + \omega\int_0^\infty \frac{e^{-\lambda_{AW}x}}{(x+\omega)^2}dx + \frac{\omega\zeta}{\omega-\delta}\int_0^\infty \frac{e^{-(\lambda_{AB}2^{R_0}+\lambda_{AW})x}}{(x+\omega)^2}dx \\
&+ \frac{\omega\zeta}{\omega-\delta}\left(\lambda_{AW} + \frac{1}{\omega-\delta}\right)\left(\int_0^\infty \frac{e^{-(\lambda_{AB}2^{R_0}+\lambda_{AW})x}}{x+\omega}dx - \int_0^\infty \frac{e^{-(\lambda_{AB}2^{R_0}+\lambda_{AW})x}}{x+\delta}dx\right).
\end{aligned} \tag{26}
$$

The non-zero secrecy capacity event happens as the secrecy capacity is greater than zero. As such, the non-zero secrecy capacity probability is related to the SOP as

$$
\begin{aligned}
\mathcal{N} &= \Pr\{R_s > 0\} \\
&= 1 - \Pr\{R_s \le 0\} \\
&= 1 - \mathcal{S}(0).
\end{aligned} \tag{31}
$$

Meanwhile, the intercept event happens as the secrecy capacity is less than zero. Therefore, the intercept probability is also related to the SOP as

$$
\mathcal{I} = \Pr\{R_s < 0\} = \mathcal{S}(0). \tag{32}
$$

4. Results and discussions

Both analytical and simulated results are presented to assess the impacts of important specifications such as channel information inaccuracy level, licensed interference, peak transmit power, peak interference power, and expected security level on the SOP in the spectrum sharing environment as well as to confirm the precision of the proposed analysis. We take into account both the path-loss and the small-scale Rayleigh fading by modelling the $\mathtt{u} - \mathtt{v}$ fading channel power $\rho_{\mathtt{uv}}$ as $\rho_{\mathtt{uv}} = d_{\mathtt{uv}}^{-\alpha}$ with α being the path-loss exponent ($\alpha = 4$ is considered in this paper) and $d_{\mathtt{uv}}$ being the distance from the transmitter $\mathtt{u}$ to the receiver $\mathtt{v}$ [35]. Users are placed in a two-dimension plane with exemplified coordinates: A at $(0.0, 0.0)$, B at $(1.0, 0.0)$, W at $(0.9, 0.5)$, M at $(0.3, 0.8)$, N at $(0.8, 0.7)$. Moreover, we assume same channel estimation accuracy at all receivers (i.e., $\beta_{\mathtt{uv}} = \beta$). In the sequel, "Sim." and "Ana." are abbreviations for "Simulation" and "Analysis", respectively. All the following figures demonstrate the perfect match between analytical and simulated results, verifying the precision of (30).

Fig. 2 illustrates the impact of the licensed interference, which can be represented by the licensed transmit power-to-noise variance ratio P_M/σ^2, on the SOP in the spectrum sharing

$$\begin{aligned}\Theta &= -\omega\lambda_{AW}e^{\lambda_{AW}\omega}Ei\left(-\lambda_{AW}\omega\right) + \omega\left[\frac{1}{\omega} + \lambda_{AW}e^{\lambda_{AW}\omega}Ei\left(-\lambda_{AW}\omega\right)\right] \\ &+ \frac{\omega\zeta}{\omega-\delta}\left(\lambda_{AW} + \frac{1}{\omega-\delta}\right)\left[\frac{Ei\left(-\left[\lambda_{AB}2^{R_0}+\lambda_{AW}\right]\delta\right)}{e^{-\left(\lambda_{AB}2^{R_0}+\lambda_{AW}\right)\delta}} - \frac{Ei\left(-\left[\lambda_{AB}2^{R_0}+\lambda_{AW}\right]\omega\right)}{e^{\left(\lambda_{AB}2^{R_0}+\lambda_{AW}\right)\omega}}\right] \\ &+ \frac{\omega\zeta}{\omega-\delta}\left[\frac{1}{\omega} + \left(\lambda_{AB}2^{R_0}+\lambda_{AW}\right)e^{\left(\lambda_{AB}2^{R_0}+\lambda_{AW}\right)\omega}Ei\left(-\left[\lambda_{AB}2^{R_0}+\lambda_{AW}\right]\omega\right)\right] \\ &= 1 + \frac{\zeta}{\omega-\delta} + \frac{\omega\zeta}{\omega-\delta}\left(\lambda_{AW}+\frac{1}{\omega-\delta}\right)e^{\left(\lambda_{AB}2^{R_0}+\lambda_{AW}\right)\delta}Ei\left(-\left[\lambda_{AB}2^{R_0}+\lambda_{AW}\right]\delta\right) \\ &+ \frac{\omega\zeta}{\omega-\delta}\left(\lambda_{AB}2^{R_0}-\frac{1}{\omega-\delta}\right)e^{\left(\lambda_{AB}2^{R_0}+\lambda_{AW}\right)\omega}Ei\left(-\left[\lambda_{AB}2^{R_0}+\lambda_{AW}\right]\omega\right).\end{aligned} \tag{29}$$

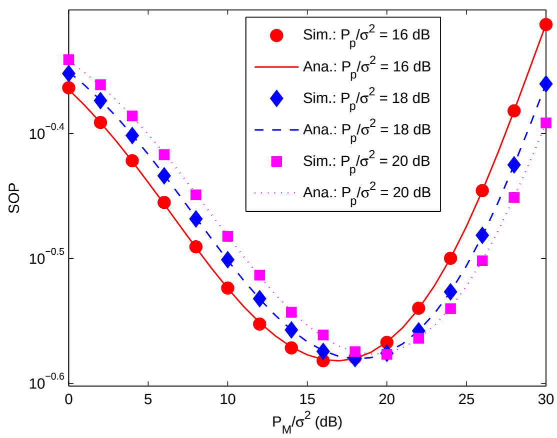

Figure 2. SOP versus P_M/σ^2.

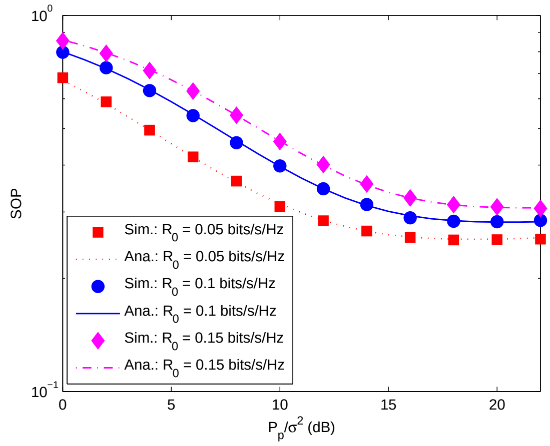

Figure 3. SOP versus P_p/σ^2.

environment for channel information inaccuracy level $\beta = 0.9$, peak interference power-to-noise variance ratio $I_p/\sigma^2 = 17$ dB, expected security level $R_0 = 0.05$ bits/s/Hz, and different unlicensed peak transmit power-to-noise variance ratios of $P_p/\sigma^2 = 16, 18, 20$ dB. This figure reveals that the security performance is optimum at a certain value of P_M/σ^2 (e.g., the SOP is minimum at $\left(P_M/\sigma^2\right)_{opt} = 17$ dB for $P_p/\sigma^2 = 16$ dB). Furthermore, the SOP is proportional to P_p/σ^2 when P_M/σ^2 is below $\left(P_M/\sigma^2\right)_{opt}$. However, the SOP is inversely proportional to P_p/σ^2 when P_M/σ^2 is above $\left(P_M/\sigma^2\right)_{opt}$.

Fig. 3 demonstrates the SOP in the spectrum sharing environment versus P_p/σ^2 for $P_M/\sigma^2 = 18$ dB, $\beta = 0.95$, $I_p/\sigma^2 = 16$ dB, and $R_0 = 0.05, 0.1, 0.15$ bits/s/Hz. This figure exposes that the SOP is unchanged at high values of P_p/σ^2. This can be interpreted from the power allocation scheme for unlicensed transmitters in the spectrum sharing environment. Indeed, the transmit power of A is $P_A = \min\left(\frac{I_p}{|\hat{g}_{AN}|^2}, P_p\right)$ according to (2). Therefore, when P_p is larger than a certain value (e.g., 20 dB in Fig. 3), P_A is independent of P_p, making the SOP unchanged. Furthermore, information security is inversely proportional to the expected security level. This is reasonable because the high security requirement under unchanged operation conditions increases

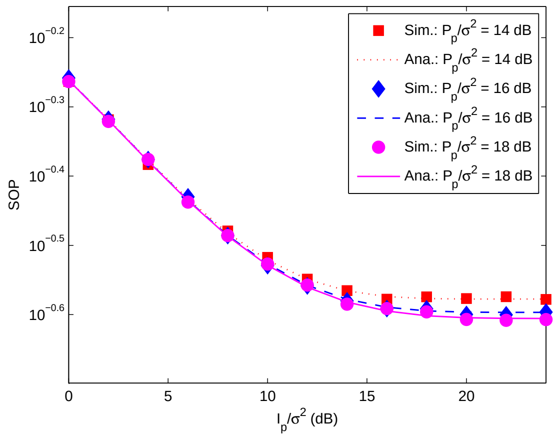

Figure 4. SOP versus I_p/σ^2.

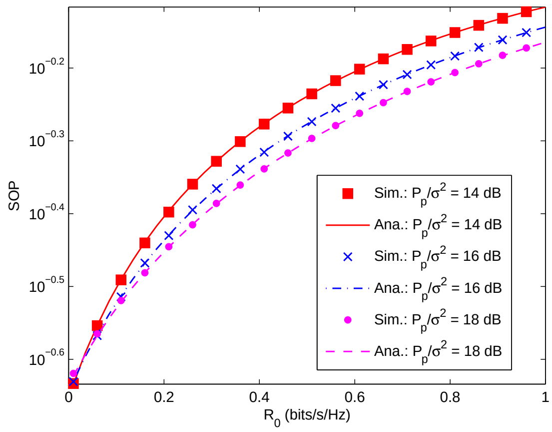

Figure 5. SOP versus R_0.

the SOP.

Fig. 4 plots the SOP in the spectrum sharing environment versus I_p/σ^2 for $P_M/\sigma^2 = 18$ dB, $\beta = 0.95$, $R_0 = 0.05$ bits/s/Hz, and $P_p/\sigma^2 = 14, 16, 18$ dB. It is observed that the security performance is unchanged at high values of I_p/σ^2. This phenomenon can be explained from the power allocation scheme for unlicensed transmitters in the spectrum sharing environment. Moreover, the SOP is inversely proportional to P_p/σ^2.

Fig. 5 demonstrates the SOP in the spectrum sharing environment versus R_0 for $P_M/\sigma^2 = 18$ dB, $\beta = 0.9$, $I_p/\sigma^2 = 16$ dB, and $P_p/\sigma^2 = 14, 16, 18$ dB. This figure shows that the SOP is proportional to R_0 as expected. Furthermore, the security performance is better with the increase in P_p/σ^2.

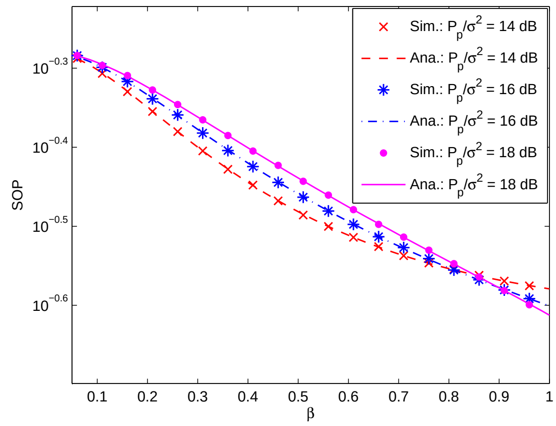

Figure 6. SOP versus β.

Fig. 6 illustrates the impact of channel information inaccuracy (represented by a correlation factor β) on the SOP in the spectrum sharing environment for $P_M/\sigma^2 = 18$ dB, $R_0 = 0.05$ bits/s/Hz, $I_p/\sigma^2 = 16$ dB, and $P_p/\sigma^2 = 14, 16, 18$ dB. It is seen that the SOP is inversely proportional to β as expected. Furthermore, the security performance is enhanced with the decrease in P_p/σ^2 when β is small (e.g., $\beta \leq 0.85$). Nevertheless, the security performance improvement is proportional to P_p/σ^2 when β is large (e.g., $\beta \geq 0.85$).

5. Conclusions

This paper suggested an exact SOP formula for quickly evaluating the information security capability in the spectrum sharing environment under interference power bound, peak transmit power bound, channel information inaccuracy, licensed interference, and Rayleigh fading. The proposed formula is corroborated by Monte-Carlo simulations and various results reveal that channel information inaccuracy and licensed interference adversely affect information security. Furthermore, a SOP floor appears at large values of either peak interference power or peak transmit power.

Acknowledgements

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2017.01

References

[1] Y. He, J. Xue, T. Ratnarajah, M. Sellathurai, and F. Khan, On the Performance of Cooperative Spectrum Sensing in Random Cognitive Radio Networks, IEEE Systems Journal, 12 (2018), pp. 881−892.

[2] K. L. Law, C. Masouros, and M. Pesavento, Transmit Precoding for Interference Exploitation in the Underlay Cognitive Radio Z-channel, IEEE Transactions on Signal Processing, 65 (2017), pp. 3617−3631.

[3] K. Ho-Van, P. C. Sofotasios, G. C. Alexandropoulos, and S. Freear, Bit error rate of underlay decode-and-forward cognitive networks with best relay selection, IEEE/KICS Journal of Communications and Networks, 17 (2015), pp. 162−171.

[4] K. Ho-Van, Exact outage analysis of underlay cooperative cognitive networks over Nakagami-m fading channels, IET Communications, 7 (2013), pp. 1254−1262.

[5] B. Fang, Z. Qian, W. Zhong, and W. Shao, AN-Aided Secrecy Precoding for SWIPT in Cognitive MIMO Broadcast Channels, IEEE Communications Letters, 19 (2015), pp. 1632−1635.

[6] V. D. Nguyen, T. Q. Duong, O. A. Dobre, and O. S. Shin, oint Information and Jamming Beamforming for Secrecy Rate Maximization in Cognitive Radio Networks, IEEE Transactions on Information Forensics and Security, 11 (2016), pp. 2609-2623.

[7] B. Fang, Z. Qian, W. Shao, and W. Zhong, Precoding and Artificial Noise Design for Cognitive MIMOME Wiretap Channels, IEEE Transactions on Vehicular Technology, 65 (2016), pp. 6753-6758.

[8] Y. Wu, X. Chen, and X. Chen, Secure beamforming for cognitive radio networks with artificial noise, in Proceedings of IEEE WCSP, Nanjing, China, 15-17 Oct. 2015, pp. 1−5.

[9] X. Hu, X. Zhang, H. Huang, and Y. Li, Secure transmission via jamming in cognitive radio networks with possion spatially distributed eavesdroppers, in Proceedings of IEEE PIMRC, Valencia, Spain, 4-7 Sep. 2016, pp. 1−6.

[10] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, Cooperative jamming for secure communications in MIMO cooperative cgnitive radio networks, in Proceedings of IEEE ICC, London, UK, 8-12 Jun. 2015, pp. 7609−7614.

[11] W. Liu, L. Guo, T. Kang, J. Zhang, and J. Lin, Secure cognitive radio system with cooperative secondary networks, in Proceedings of IEEE ICT, Sydney, Australia, 27-29 April 2015, pp. 6-10.

[12] T. He, H. Chen, and Q. Liu, QoS-based beamforming with cooperative jamming in cognitive radio networks, in Proceedings of ICCCAS, Chengdu, China, 15-17 Nov. 2013, pp. 42−45.

[13] W. Liu, M. Z. I. Sarkar, T. Ratnarajah, and H. Du, Securing cognitive radio with a combined approach of beamforming and cooperative jamming, IET Communications, 11 (2017), pp. 1-9.

[14] Y. Zou, Physical-Layer Security for Spectrum Sharing Systems, IEEE Transactions on Wireless Communications, 16 (2017), pp. 1319-1329.

[15] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, Relay Selection for Security Enhancement in Cognitive Relay Networks, IEEE Wireless Communications Letters, 4 (2015), pp. 46-49.

[16] P. Chakraborty and S. Prakriya, Secrecy Performance of an Idle Receiver Assisted Underlay Secondary Network, IEEE Transactions on Vehicular Technology, 66 (2017), pp. 9555-9560.

[17] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, A survey on multiple-antenna techniques for physical layer security, IEEE Communications Surveys & Tutorials, 19 (2017), pp. 1027−1053.

[18] J. Ouyang, M. Lin, Y. Zou, W. P. Zhu, and D. Massicotte, Secrecy energy efficiency maximization in cognitive radio networks, IEEE Access, 5 (2017), pp. 2641−2650.

[19] X. Zhang, J. Xing, Z. Yan, Y. Gao, and W. Wang, Outage Performance Study of Cognitive Relay Networks with Imperfect Channel Knowledge, Communications Letters, IEEE, 17 (2013), pp. 27-30.

[20] H. Ding, J. Ge, D. B. da Costa, and Z. Jiang, Asymptotic Analysis of Cooperative Diversity Systems With Relay Selection in a Spectrum-Sharing Scenario, IEEE Transactions on Vehicular Technology, 60 (2011), pp. 457-472.

[21] H. A. Suraweera, P. J. Smith, and M. Shafi, Capacity Limits and Performance Analysis of Cognitive Radio With Imperfect Channel Knowledge, IEEE Transactions on Vehicular Technology, 59 (2010), pp. 1811-1822.

[22] J. Chen, J. Si, Z. Li, and H. Huang, On the Performance of Spectrum Sharing Cognitive Relay Networks with Imperfect CSI, IEEE Communications Letters, 16 (2012), pp. 1002-1005.

[23] K. S. Ahn and R. W. Heath, Performance analysis of maximum ratio combining with imperfect channel estimation in the presence of cochannel interferences, IEEE Transactions on Wireless Communications, 8 (2009), pp. 1080-1085.

[24] M. A. b. Azaman, N. P. Nguyen, D. B. Ha, and T. V. Truong, Secrecy outage probability of full-duplex networks with cognitive radio environment and partial relay selection, in Proceedings of IEEE SigTelCom,

Danang, Vietnam, 9−11 Jan. 2017, pp. 119−123.

[25] Q. Yang, J. Ding and J. Yang, Secrecy outage probability of dual-hop DF cognitive relay networks under interference constraints, in Proceedings of IEEE APCC, Yogyakarta, Indonesia, 25−27 Aug. 2016, pp. 76−80.

[26] T. Zhang, Y. Huang, Y. Cai, C. Zhong, W. Yang, and G. K. Karagiannidis, Secure Multiantenna Cognitive Wiretap Networks, IEEE Transactions on Vehicular Technology, 66 (2017), pp. 4059-4072.

[27] M. N. Nguyen, N. P. Nguyen, D. B. D. Costa, H. K. Nguyen, and R. T. D. Sousa, Secure cooperative half-duplex cognitive radio networks with K-th best relay selection, IEEE Access, 5 (2017), pp. 6678−6687.

[28] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, et al., Secrecy Outage Performance of Transmit Antenna Selection for MIMO Underlay Cognitive Radio Systems Over Nakagami- m Channels, IEEE Transactions on Vehicular Technology, 66 (2017), pp. 2237-2250.

[29] 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 Transactions on Vehicular Technology, 65 (2016), pp. 10236-10242.

[30] R. Zhao, Y. Yuan, L. Fan, and Y. C. He, Secrecy Performance Analysis of Cognitive Decode-and-Forward Relay Networks in Nakagami-m Fading Channels, IEEE Transactions on Communications, 65 (2017), pp. 549-563.

[31] S. Raghuwanshi, P. Maji, S. D. Roy and S. Kundu, Secrecy performance of a dual hop cognitive relay network with an energy harvesting relay, in Proceedings of IEEE ICACCI, Jaipur, India, 21−24 Sep. 2016, pp. 1622−1627.

[32] K. Shim, N. T. Do, B. An and S. Y. Nam, Outage performance of physical layer security for multi-hop underlay CRNs with imperfect channel state information, in Proceedings of IEEE ICEIC, Danang, Vietnam, 27−30 Jan. 2016, pp.1-4.

[33] A. D. Wyner, The wire-tap channel, The Bell System Technical Journal, 54 (1975), pp. 1355-1387.

[34] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series and Products, 6th ed. San Diego, CA: Academic, 2000.

[35] N. Ahmed, M. Khojastepour, and B. Aazhang, Outage minimization and optimal power control for the fading relay channel, in Proceedings of IEEE Information Theory Workshop, San Antonio, TX, USA, Oct. 2004, pp. 458−462.

[36] A. Papoulis and S. U. Pillai, Probability, Random Variables and Stochastic Processes, 4th edition, McGraw-Hill, 2002.