Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 5457176, 15 pages
https://doi.org/10.1155/2018/5457176

Research Article

Reliability-Security Trade-Off Analysis of Cognitive Radio Networks with Jamming and Licensed Interference

Khuong Ho-Van and Thiem Do-Dac

Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam

Correspondence should be addressed to Khuong Ho-Van; khuong.hovan@yahoo.ca

Received 26 July 2017; Revised 20 November 2017; Accepted 13 December 2017; Published 22 January 2018

Academic Editor: Donatella Darsena

Cognitive radio networks (CRNs) allow coexistence of unlicensed users (UUs) and licensed users (LUs) and hence, mutual interference between UUs and LUs is neither ignored nor considered as Gaussian-distributed quantity. Additionally, exploiting jamming signals to purposely interfere with signal reception of eavesdroppers is a feasible solution to improve security performance of CRNs. This paper analyzes reliability-security trade-off, which accounts for maximum transmit power constraint, interference power constraint, jamming signal, and Rayleigh fading, and considers interference from LUs as non-Gaussian-distributed quantity. Toward this end, exact closed-form expressions of successful detection probability and successful eavesdropping probability, from which reliability-security trade-off is straightforwardly visible, are first suggested and then validated by Monte-Carlo simulations. Various results demonstrate that interference from LUs considerably decreases both probabilities while jamming signal enlarges the difference between them, emphasizing its effectiveness in improving security performance.

1. Introduction

High data rate and strong information security are two among obligatory requirements in designing next generation wireless communication networks (e.g., 5G) [1]. The former can be achieved by cognitive radio technique whose advantage is high spectrum utilization efficiency by permitting both UUs and LUs to operate in the same frequency band primarily allocated to LUs [2]. It is coexistence of both UUs and LUs that causes mutual interference between them [3] and hence, interference from LUs (shortly, licensed interference) is neither ignored nor considered as Gaussian-distributed quantity. On the other hand, physical layer security, which exploits space-time characteristics of wireless channels to secure information transmission, is a feasible solution to satisfy the latter [4–8]. Therefore, physical layer security for CRNs, which can meet simultaneously both above requirements, has recently received a great deal of attention from both academia and industry. Among physical layer security solutions, generating jamming signals, which purposely destroys signal reception of eavesdroppers without degrading quality of service (QoS) of legal receivers, is an effective solution to improve security performance [9, 10]. For a certain physical layer security solution, it is interesting to assess successful detection probability at legal receiver (i.e., probability for legal receiver to successfully restore legitimate signals) and successful eavesdropping probability at eavesdropper (i.e., probability for eavesdropper to successfully decode/steal legitimate signals). Obviously, successful detection probability represents communication reliability while successful eavesdropping probability represents security level. Therefore, reliability-security trade-off is represented by relation between successful detection probability and successful eavesdropping probability. Because the difference (or ratio) between successful detection probability and successful eavesdropping probability has an equivalent physical meanings as the difference (or ratio) between signal power and noise power in communication theory, this difference (or ratio) can represent security performance. This paper analyzes reliability-security trade-off to assess information securing capability of CRNs under both interferences from licensed transmitter and jammer.

Table 1: Related works where jamming signal and legitimate signal are combined and simultaneously transmitted by a UU. The characteristic marked with "x" implies that it is considered in the corresponding reference.

Reference	Interference from LUs	Maximum transmit power constraint	Interference power constraint	Thermal noise	Reliability-security trade-off analysis
[14]	x			x	
[17]	x	x		x	
[18–21]		x	x	x	
[22]			x	x	
[23]	x				
[24]	x	x		x	

1.1. Related Works. This subsection reviews only publications relevant to jamming signal generation to guarantee information transmission securely in underlay CRNs (physical layer security solutions are various. For example, [11] deploys a friendly jammer to interfere with the eavesdropper; [12] proposes a relay selection scheme; [13] implements the joint power control in wiretap interference channels. However, most solutions are proposed for noncognitive radio networks (e.g., [11–13]). Because this paper focuses on jamming signal generation to guarantee information transmission securely in underlay CRNs, literature review on physical layer security solutions for noncognitive radio networks (e.g., [11–13]) should not be further investigated). Such a review is based on typical characteristics such as interference from licensed transmitter, maximum transmit power constraint, interference power constraint, thermal noise, and reliability-security trade-off analysis, and through it, contributions of this paper can be summarized in next subsection.

In [14], an unlicensed source transmits a jamming signal to secure information transmission of LUs in exchange for utilizing licensed spectrum in presence of interference from licensed transmitters. However, [14] does not account for power constraints of unlicensed transmitters such as interference power constraint and maximum transmit power constraint [15, 16]. In [17], cooperative relaying combines jamming signal generation to guarantee information transmission of LUs securely in cognitive two-way networks where one of two UUs sends both jamming signal and legitimate signal while the other UU merely amplifies and forwards the received signal together with its own signal. Optimum power allocation to jamming signal and legitimate signal is proposed there without being subjected to interference power constraint even though both jamming signal and interference from LUs and maximum transmit power constraint are accounted. In [18–21], beamforming vectors for jamming signal and legitimate signal are designed to optimize power allocation to jamming signal and legitimate signal at an unlicensed transmitter subject to maximum transmit power constraint and interference power constraint. Nevertheless, interference from licensed transmitter is not considered there. In [22], a UU transmits both jamming signal and legitimate signal under a simple context, which ignores maximum transmit power constraint and interference from licensed transmitter, to optimize the secrecy throughput of the wiretap channel for CRNs. The same optimization problem as [22] is revisited in [23]. However, [23] considers a different context where interference from licensed transmitter, the connection outage constraint (i.e., the probability for signal-to-interference-plus-noise ratio (SINR) at licensed receiver below a preset level is less than a certain value), and no thermal noise at corresponding receivers, and all randomly located users are investigated. It is noted that the connection outage constraint makes transmit power of UUs unchanged. Therefore, the connection outage constraint together with ignored thermal noise considerably simplifies information securing capability analysis in [23]. The authors in [24] design a beamforming vector at the multiantenna unlicensed source to maximize the minimum secrecy rate of the unlicensed network while guaranteeing the minimum secrecy rate of the licensed network and satisfying maximum transmit power constraint for cognitive multicast communications. Besides beamforming the legitimate signals, the source transmits the jamming signal together with them to further secure information transmission. However, [24] ignores interference power constraint. Table 1 summarizes typical characteristics considered in [14, 17–24] with an emphasis that reliability-security trade-off analysis is not implemented there.

In contrast to [14, 17–24] where jamming signal and legitimate signal are merged and concurrently broadcasted by an unlicensed transmitter, [25–32] suggest new techniques to prevent eavesdroppers from stealing confidential information in CRNs where jamming signal and legitimate signal are transmitted by two different users. To be more specific, jamming signal and legitimate signal are separately transmitted by two different UUs to guarantee LUs' communication securely while maintaining QoS of UUs [25]. Nevertheless, [25] neglects interference from licensed transmitter and interference power constraint. The authors in [26] complement the idea in [25] by further considering interference power constraint. Similar to [25, 26] where jamming signal and legitimate signal are transmitted by different UUs, [27] proposes design of a weight vector for jamming signals forwarded by different relays to achieve maximum signal-to-noise ratio (SNR) at legal receiver while restricting SNR at the eavesdropper below a certain level in a context where both interference power constraint and maximum transmit power constraint are accounted. However, [27] ignores interference from licensed transmitter. The authors in [28] complement the work in [27] by accounting for this interference to maximize the secrecy rate. Instead of designing a weight

Table 2: Related works where jamming signal and legitimate signal are transmitted by two different users. The characteristic marked with "x" implies that it is considered in the corresponding reference.

Reference	Interference from LUs	Maximum transmit power constraint	Interference power constraint	Thermal noise	Reliability-security trade-off analysis
[25]		x		x	
[26]		x	x	x	
[27]		x	x	x	
[28]	x	x	x	x	
[29]		x	x	x	
[30]				x	
[31]			x	x	
[32]		x	x	x	

vector for jamming signals forwarded by different relays, each equipped with single antenna as in [27, 28], the authors in [29] implement design of a beamforming vector at a single multiantenna relay. Therefore, [27–29] solve quite similar problems. Furthermore, interference from licensed transmitter is ignored in [29]. In [30], a UU is selected to transmit merely jamming signals not only to deteriorate QoS of the eavesdropper but also to assist secrete communication of another UU. However, power constraints and interference from licensed transmitter are neglected there, which are not reasonable for CRNs where UUs and LUs concurrently operate. For secure transmission of an unlicensed source, [31] adopts two unlicensed relays while [32] chooses an unlicensed relay and an unlicensed destination. However, [31, 32] neglect interference from LUs. Furthermore, [31] does not investigate maximum transmit power constraint. Table 2 summarizes typical characteristics considered in [25–32] with an emphasis that reliability-security trade-off analysis is not implemented there.

1.2. Contributions. The above literature survey [14, 17–32] shows that reliability-security trade-off analysis of CRNs, where legitimate signal and jamming signal are simultaneously transmitted by two different unlicensed transmitters, under interference from licensed transmitter, maximum transmit power constraint, interference power constraint, and thermal noise, has not been reported in any open literature. We aim to perform this analysis with threefold contributions:

(i) Investigate a physical layer security solution for CRNs where an unlicensed jammer transmits a jamming signal at the same time that an unlicensed transmitter sends its confidential signal to purposely interfere with signal reception of the eavesdropper without degrading the performance of the legal receiver under maximum transmit power constraint, interference power constraint, interference from licensed transmitter, and thermal noise.

(ii) Propose exact closed-form expressions of successful detection probability and successful eavesdropping probability, from which reliability-security trade-off is straightforwardly visible for promptly evaluating security performance without the need of time-consuming Monte-Carlo simulations.

(iii) Illustrate various results to have useful insights into security performance of underlay cognitive networks such as interference from licensed transmitter adversely decreases successful detection probability and successful eavesdropping probability while jamming signal offers a large difference between them, exposing its effectiveness in securing confidential information.

1.3. Organization. The paper is organized as follows. System model under consideration is described in Section 2. The analysis of successful detection probability and successful eavesdropping probability is presented in Section 3. Numerous results for evaluation and validation of the proposed analysis are presented in Section 4. The paper is concluded in Section 5.

2. System Model

Figure 1 demonstrates a system model for cognitive radio networks under investigation where an unlicensed source $\mathtt{U}_\mathtt{S}$ transmits confidential information to an unlicensed destination $\mathtt{U}_\mathtt{D}$ (namely, legal receiver) and this transmission is illegally wire-tapped by an eavesdropper $\mathtt{E}$. Unlicensed users operate in the underlay paradigm [33] and hence, communication between $\mathtt{U}_\mathtt{S}$ and $\mathtt{U}_\mathtt{D}$ concurrently takes place with communication between a licensed transmitter $\mathtt{L}_\mathtt{T}$ and a licensed receiver $\mathtt{L}_\mathtt{R}$, inducing mutual interference to each other. All terminals are assumed to be equipped with single antenna and operated in the half-duplex mode. In order to secure communication between $\mathtt{U}_\mathtt{S}$ and $\mathtt{U}_\mathtt{D}$, an unlicensed jammer $\mathtt{U}_\mathtt{J}$ transmits a jamming signal $\sqrt{P_j}v_j$ at the same time that $\mathtt{U}_\mathtt{S}$ transmits a legitimate signal $\sqrt{P_s}v_s$ to purposely interfere with signal reception of $\mathtt{E}$ where P_j and P_s are transmit powers of $\mathtt{U}_\mathtt{J}$ and $\mathtt{U}_\mathtt{S}$, respectively; v_j and v_s are correspondingly a jamming signal and a legitimate signal which are assumed to be Gaussian-distributed and have unity power (i.e., $v_j \sim \mathscr{CN}(0,1)$ and $v_s \sim \mathscr{CN}(0,1)$ where $h_{\mathtt{ab}} \sim \mathscr{CN}(0,\lambda_{\mathtt{ab}})$ stands for a circular symmetric complex Gaussian random variable (CSCGRV) with zero mean and variance $\lambda_{\mathtt{ab}}$).

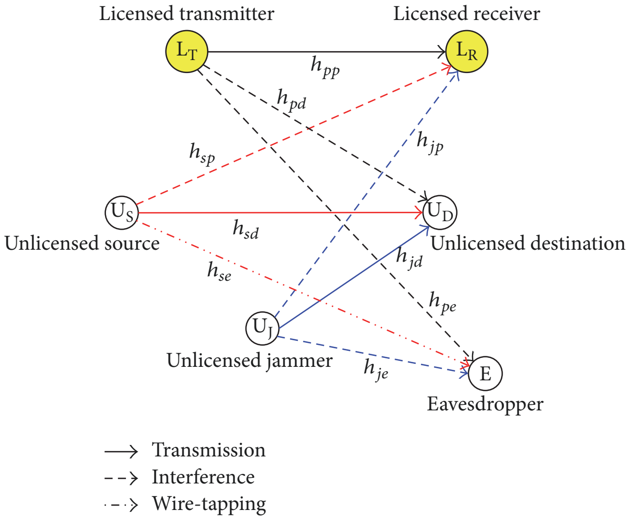


Figure 1: System model.

Thus, received signals at $\mathtt{U_D}$ and $\mathtt{E}$ are correspondingly represented as

$$u_d = h_{sd}\sqrt{P_s}v_s + h_{jd}\sqrt{P_j}v_j + h_{pd}\sqrt{P_p}v_p + n_d, \tag{1}$$

$$u_e = h_{se}\sqrt{P_s}v_s + h_{je}\sqrt{P_j}v_j + h_{pe}\sqrt{P_p}v_p + n_e, \tag{2}$$

where P_p is power of the licensed transmitter $\mathtt{L_T}$; v_p is the signal transmitted by $\mathtt{L_T}$ and is normalized to have unity power and Gaussian-distributed (i.e., $v_p \sim \mathscr{CN}(0,1)$); n_d and n_e are additive white Gaussian noise at $\mathtt{U_D}$ and $\mathtt{E}$, correspondingly, each modelled as $\mathscr{CN}(0,N_0)$; $h_{\mathtt{ab}}$ stands for a channel coefficient between a transmitter $\mathtt{a}$ and a receiver $\mathtt{b}$, which is assumed to be independent, frequency flat, and Rayleigh distributed and hence, $h_{\mathtt{ab}}$ is modelled as a CSCGRV with zero mean and variance $\lambda_{\mathtt{ab}}$, that is, $h_{\mathtt{ab}} \sim \mathscr{CN}(0,\lambda_{\mathtt{ab}})$, $\mathtt{a} \in \{\mathtt{U_S},\mathtt{L_T},\mathtt{U_J}\}$, and $\mathtt{b} \in \{\mathtt{U_D},\mathtt{L_R},\mathtt{E}\}$.

Since the transmit power of $\mathtt{U_S}$ is P_s, $P_s|h_{sp}|^2$ is the interference power caused by $\mathtt{U_S}$ to $\mathtt{L_R}$. Similarly, $P_j|h_{jp}|^2$ is the interference power caused by $\mathtt{U_J}$ to $\mathtt{L_R}$. Therefore, the total interference power induced by $\mathtt{U_S}$ and $\mathtt{U_J}$ to $\mathtt{L_R}$ is $P_s|h_{sp}|^2 + P_j|h_{jp}|^2$. To guarantee reliable signal reception at LUs, this interference power must be controlled below maximum interference power I_m that licensed receivers can tolerate, that is, $P_s|h_{sp}|^2 + P_j|h_{jp}|^2 \le I_m$. In addition, each licensed transmitter is designed with a certain maximum transmit power (i.e., $\widehat{P}_s$ for $\mathtt{U_S}$ and $\widehat{P}_j$ for $\mathtt{U_J}$) and hence, P_s and P_j are limited by $\widehat{P}_s$ and $\widehat{P}_j$, that is, $P_s \le \widehat{P}_s$ and $P_j \le \widehat{P}_j$. Briefly, the transmit powers of $\mathtt{U_S}$ and $\mathtt{U_J}$ are subjected to the following constraints:

$$P_s \le \widehat{P}_s, \tag{3}$$

$$P_j \le \widehat{P}_j, \tag{4}$$

$$P_s\left|h_{sp}\right|^2 + P_j\left|h_{jp}\right|^2 \le I_m, \tag{5}$$

where (3) and (4) are maximum transmit power constraints while (5) is interference power constraint.

From (5), one can select

$$P_s\left|h_{sp}\right|^2 \le \alpha I_m, \tag{6}$$

$$P_j\left|h_{jp}\right|^2 \le (1-\alpha) I_m, \tag{7}$$

where $0 < \alpha \le 1$ is an interference power distribution factor for $\mathtt{U_S}$ and $\mathtt{U_J}$. $\alpha = 1$ means no jammer. α can be optimally selected not only to control interference to $\mathtt{L_R}$ but also to increase interference to $\mathtt{E}$.

Combining maximum transmit power constraint in (3) and interference power constraint in (6), transmit power of $\mathtt{U_S}$ must satisfy $P_s \le \min(\alpha I_m/|h_{sp}|^2, \widehat{P}_s)$. For maximum radio coverage, the equality should hold, that is,

$$P_s = \min\left(\frac{\alpha I_m}{\left|h_{sp}\right|^2}, \widehat{P}_s\right). \tag{8}$$

Similarly, to meet both maximum transmit power constraint in (4) and interference power constraint in (7) as well as maximize radio coverage, transmit power of $\mathtt{U_J}$ is established as

$$P_j = \min\left(\frac{(1-\alpha) I_m}{\left|h_{jp}\right|^2}, \widehat{P}_j\right). \tag{9}$$

The jamming signal v_j is intentionally generated by $\mathtt{U_J}$ to only cause interference to $\mathtt{E}$ without inducing performance degradation of $\mathtt{U_D}$. This can be achieved by allowing $\mathtt{U_J}$ to share v_j with $\mathtt{U_D}$ (e.g., the seed of the jamming signal generator at $\mathtt{U_J}$ is shared with $\mathtt{U_D}$ in a secure manner through a cooperation agreement only between $\mathtt{U_J}$ and $\mathtt{U_D}$ before information transmission starts). Such a jamming signal generation is widely accepted in open literature (e.g., [5, 8, 19–22, 25, 30–32] and references therein). As such, the legal receiver $\mathtt{U_D}$ can accurately predict the jamming signal and completely eliminate it out of $\mathtt{U_D}$'s received signal, ultimately resulting in the jamming-free signal as $\widetilde{u}_d = h_{sd}\sqrt{P_s}v_s + h_{pd}\sqrt{P_p}v_p + n_d$. Based on the jamming-free signal, one can infer SINR at $\mathtt{U_D}$ as

$$\beta_d = \frac{\mathscr{E}_{v_s}\left\{\left|h_{sd}\sqrt{P_s}v_s\right|^2\right\}}{\mathscr{E}_{v_p,n_d}\left\{\left|h_{pd}\sqrt{P_p}v_p + n_d\right|^2\right\}} = \frac{P_s\left|h_{sd}\right|^2}{P_p\left|h_{pd}\right|^2 + N_0}, \tag{10}$$

where $\mathscr{E}_{X,Y,\ldots}\{\cdot\}$ denotes the expectation operation over random variables $X, Y, \ldots$.

Because the knowledge of the jamming signal v_j is only shared between $\mathtt{U_J}$ and $\mathtt{U_D}$ for information securing purpose, the eavesdropper does not know it. Therefore, the SINR at $\mathtt{E}$ is inferred from (2) as

$$\begin{aligned}\beta_e &= \frac{\mathscr{E}_{v_s}\left\{\left|h_{se}\sqrt{P_s}v_s\right|^2\right\}}{\mathscr{E}_{v_p,v_j,n_e}\left\{\left|h_{je}\sqrt{P_j}v_j + h_{pe}\sqrt{P_p}v_p + n_e\right|^2\right\}} \\ &= \frac{P_s\left|h_{se}\right|^2}{P_j\left|h_{je}\right|^2 + P_p\left|h_{pe}\right|^2 + N_0}.\end{aligned} \tag{11}$$

It is worth mentioning that the licensed transmitter $\mathtt{L_T}$ introduces interference powers at $\mathtt{U_D}$ and $\mathtt{E}$ as $|h_{pd}|^2 P_p$ and $|h_{pe}|^2 P_p$, respectively, according to (10) and (11). These interference powers are neither ignored nor considered as Gaussian-distributed quantity but rather treated as exponentially distributed random variables. Additionally, $\mathtt{U_J}$ deliberately generates jamming power $P_j|h_{je}|^2$ to the eavesdropper. As such, increasing this jamming power is expected to secure information transmission of $\mathtt{U_S}$.

Channel capacities at $\mathtt{U_D}$ and $\mathtt{E}$ are, respectively, given by [34]

$$\begin{aligned} C_d &= \log_2\left(1+\beta_d\right), \\ C_e &= \log_2\left(1+\beta_e\right), \end{aligned} \tag{12}$$

which are helpful in analyzing successful detection probability of the legal receiver $\mathtt{U_D}$ and successful eavesdropping probability of the eavesdropper $\mathtt{E}$ in next section.

3. Performance Analysis

This section analyzes successful detection probability of the legal receiver $\mathtt{U_D}$, P_{det}, and successful eavesdropping probability of the eavesdropper $\mathtt{E}$, P_{eav}. According to information theory, P_{det} and P_{eav} are correspondingly defined as probabilities for channel capacities of $\mathtt{U_D}$ and $\mathtt{E}$ to be larger than a required level. In other words, successful detection probability of $\mathtt{U_D}$ and successful eavesdropping probability of $\mathtt{E}$ are probabilities for $\mathtt{U_D}$ and $\mathtt{E}$ to successfully decode $\mathtt{U_S}$'s information, respectively. As such, they are important metrics for evaluating communication reliability and information securing capability. The larger P_{det}, the more reliable the signal reception at $\mathtt{U_D}$. Meanwhile, the larger P_{eav}, the less secure the information transmission of $\mathtt{U_S}$. Therefore, the relation between P_{det} and P_{eav} represents reliability-security trade-off. Furthermore, the difference (or ratio) between successful detection probability and successful eavesdropping probability has an equivalent physical meanings as the difference (or ratio) between signal power and noise power in communication theory and hence, this difference (or ratio) can represent security performance.

The successful detection probability of $\mathtt{U_D}$ and the successful eavesdropping probability of $\mathtt{E}$ are respectively expressed as

$$P_{\text{det}} = \Pr\left\{C_d \geq C_{\text{th}}\right\} = \Pr\left\{\beta_d \geq x\right\}, \tag{13}$$

$$P_{\text{eav}} = \Pr\left\{C_e \geq C_{\text{th}}\right\} = \Pr\left\{\beta_e \geq x\right\}, \tag{14}$$

where C_{th} is the threshold for successfully decoding $\mathtt{U_S}$'s information, $x = 2^{C_{\text{th}}} - 1$, and $\Pr\{\mathcal{Q}\}$ is the probability of the event $\mathcal{Q}$.

Theorem 1. *The exact closed-form representation of the successful detection probability of the legal receiver* $\mathtt{U_D}$ *is given by*

$$\begin{aligned} P_{\text{det}} = {} & \left(\frac{xP_p\lambda_{pd}}{\widehat{P}_s\lambda_{sd}}+1\right)^{-1} e^{-xN_0/\widehat{P}_s\lambda_{sd}} \left(1-e^{-\alpha I_m/\widehat{P}_s\lambda_{sp}}\right) \\ & - \frac{\alpha I_m\lambda_{sd}}{\lambda_{sp}P_p\lambda_{pd}x} \\ & \cdot e^{N_0/P_p\lambda_{pd}+\alpha I_m\lambda_{sd}/\lambda_{sp}P_p\lambda_{pd}x} Ei\left(-\left[\frac{xN_0}{\lambda_{sd}}+\frac{\alpha I_m}{\lambda_{sp}}\right]\right. \\ & \left.\cdot\left[\frac{1}{\widehat{P}_s}+\frac{\lambda_{sd}}{P_p\lambda_{pd}x}\right]\right), \end{aligned} \tag{15}$$

where $Ei(x)$ *is the exponential integral function [35].*

Proof. Please see Appendix A. □

Before deriving the exact closed-form expression of the successful eavesdropping probability of $\mathtt{E}$, we introduce two special results in the following lemmas.

Lemma 2. *The integrand*

$$\mathscr{L}\left(a,b,c,g\right) = \int_a^\infty e^{-bz} Ei\left(-cz-g\right) dz \tag{16}$$

can be represented in closed form as

$$\begin{aligned} \mathscr{L}\left(a,b,c,g\right) = {} & Ei\left(-g-ac\right)\frac{e^{-ab}}{b} \\ & + \frac{e^{-g}}{b}\mathscr{H}\left(a,b+c,\frac{g}{c}\right), \end{aligned} \tag{17}$$

where

$$\mathscr{H}\left(a,b,c\right) = -e^{bc} Ei\left(-ab-bc\right). \tag{18}$$

Proof. Please see Appendix B. □

Lemma 3. *The integrand*

$$\mathscr{M}\left(a,b,c,g,l\right) = \int_a^\infty \frac{e^{-bx}}{x+c} Ei\left(-gx-l\right) dx \tag{19}$$

can be represented in closed form as

$$\mathscr{M}\left(a,b,c,g,l\right) = -e^{bl/g}\left(\mathtt{C}\varphi_1+\varphi_2+\sum_{k=1}^{\infty}\frac{\varphi_3}{k\cdot k!}\right), \tag{20}$$

where

$$\varphi_1 = -\mathscr{H}\left(ag+l,\frac{b}{g},cg-l\right) \tag{21}$$

$$\varphi_2 = 2e^{b/g}\sum_{k=1}^{\infty}\sum_{n=0}^{2k-1}\sum_{s=0}^{n}\binom{2k-1}{n}\binom{n}{s}\frac{(-1)^s}{2k-1}\zeta \tag{22}$$

$$\zeta = \begin{cases} \mathscr{H}\left(ag+l+1, \dfrac{b}{g}, cg-l-1\right), & s = 2k-1 \\ \theta, & s \neq 2k-1 \end{cases} \tag{23}$$

$$\begin{aligned} \theta &= p\mathscr{H}\left(ag+l+1, \frac{b}{g}, cg-l-1\right) \\ &\quad + \sum_{v=1}^{2k-s-1} q_{2k-s-v}\mathscr{B}\left(ag+l+1, \frac{b}{g}, v\right) \end{aligned} \tag{24}$$

$$p = \frac{1}{(l+1-cg)^{2k-s-1}} \tag{25}$$

$$q_m = \frac{(-1)^{m-1}}{(cg-l-1)^m} \tag{26}$$

$$\mathscr{B}(a,b,v) = b^{v-1}(ab)^{-0.5v}e^{-0.5ab}\mathrm{W}_{-0.5v,0.5(1-v)}(ab) \tag{27}$$

$$\begin{aligned} \varphi_3 &= (-1)^{k+1} \\ &\quad \cdot e^{-(b/g)(l-cg)}\left[(l-cg)^k\mathscr{H}\left([a+c]g, \frac{b}{g}, 0\right)\right. \\ &\quad \left. + \sum_{n=1}^{k}\binom{k}{n}(l-cg)^{k-n}\mathscr{D}\left([a+c]g, \frac{b}{g}, n-1\right)\right] \end{aligned} \tag{28}$$

$$\mathscr{D}(a,b,n) = e^{-ab}\sum_{k=0}^{n}\frac{n!}{k!}\frac{a^k}{b^{n-k+1}} \tag{29}$$

and $\mathtt{C} = 0.5772156649$ *is the Euler-Mascheroni constant and* $\mathrm{W}_{a,b}(c)$ *is the Whittaker function [35, eq. (9.220.4)].*

Proof. Please see Appendix C. □

Using the results in Lemmas 2 and 3, one can represent the successful eavesdropping probability of $\mathtt{E}$ in closed form as follows.

Theorem 4. *The successful eavesdropping probability of the eavesdropper* $\mathtt{E}$ *has an exact closed form as*

$$\begin{aligned} P_{\mathrm{eav}} &= \left\{\left(1 - e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right)\left(\frac{x\lambda_{je}\widehat{P}_j}{\lambda_{se}\widehat{P}_s} + 1\right)^{-1}\right. \\ &\quad + e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}} + \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}\widehat{P}_s} \\ &\quad \cdot e^{x\lambda_{je}(1-\alpha)I_m/\lambda_{se}\lambda_{jp}\widehat{P}_s}Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}\right. \\ &\quad \left.\left. - \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}\widehat{P}_s}\right)\right\}\left(\frac{xP_p\lambda_{pe}}{\lambda_{se}\widehat{P}_s} + 1\right)^{-1}\left(1\right. \\ &\quad \left. - e^{-\alpha I_m/\widehat{P}_s\lambda_{sp}}\right)e^{-xN_0/\lambda_{se}\widehat{P}_s} \\ &\quad + \frac{\lambda_{se}\alpha I_m}{x\lambda_{sp}}\left(\frac{1 - e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}}{P_p\lambda_{pe} - \lambda_{je}\widehat{P}_j} + \frac{e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}}{P_p\lambda_{pe}}\right) \\ &\quad \cdot \mathscr{H}\left(\frac{\alpha I_m}{\widehat{P}_s}, \frac{xN_0}{\lambda_{se}\alpha I_m} + \frac{1}{\lambda_{sp}}, \frac{\lambda_{se}\alpha I_m}{xP_p\lambda_{pe}}\right) \\ &\quad - \frac{\lambda_{se}\alpha I_m\left(1 - e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right)}{x\lambda_{sp}\left(P_p\lambda_{pe} - \lambda_{je}\widehat{P}_j\right)}\mathscr{H}\left(\frac{\alpha I_m}{\widehat{P}_s}, \frac{xN_0}{\lambda_{se}\alpha I_m}\right. \\ &\quad \left. + \frac{1}{\lambda_{sp}}, \frac{\lambda_{se}\alpha I_m}{x\lambda_{je}\widehat{P}_j}\right) + \frac{\lambda_{je}(1-\alpha)I_m}{P_p\lambda_{pe}\lambda_{jp}\lambda_{sp}}\mathscr{L}\left(\frac{\alpha I_m}{\widehat{P}_s},\right. \\ &\quad \frac{xN_0}{\alpha I_m\lambda_{se}} + \frac{1}{\lambda_{sp}} - \frac{x\lambda_{je}(1-\alpha)}{\alpha\lambda_{se}\lambda_{jp}}, \frac{x\lambda_{je}(1-\alpha)}{\lambda_{se}\lambda_{jp}\alpha}, \\ &\quad \left.\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}\right) - \frac{\lambda_{je}\lambda_{se}\alpha(1-\alpha)}{x\lambda_{jp}\lambda_{sp}}\left(\frac{I_m}{P_p\lambda_{pe}}\right)^2 \\ &\quad \cdot \mathscr{M}\left(\frac{\alpha I_m}{\widehat{P}_s}, \frac{xN_0}{\alpha I_m\lambda_{se}} + \frac{1}{\lambda_{sp}} - \frac{x\lambda_{je}(1-\alpha)}{\alpha\lambda_{se}\lambda_{jp}},\right. \\ &\quad \left.\frac{\lambda_{se}\alpha I_m}{xP_p\lambda_{pe}}, \frac{x\lambda_{je}(1-\alpha)}{\lambda_{se}\lambda_{jp}\alpha}, \frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}\right). \end{aligned} \tag{30}$$

Proof. Please see Appendix D. □

It is worth mentioning that although the exact closed-form expressions of the successful detection probability of $\mathtt{U_D}$ and the successful eavesdropping probability of $\mathtt{E}$ in (15) and (30), respectively, are relatively long, they are simply computed since they encompass simple built-in functions such as the Whittaker function and the exponential integral function. Therefore, (15) and (30) are helpful in quickly assessing the trade-off between the communication reliability and the information security in underlay CRNs under interference from licensed transmitter, jamming signal, maximum transmit power constraint, and interference power constraint, without exhaustive Monte-Carlo simulations.

4. Results and Discussion

This section provides numerous results to illustrate the trade-off between the communication reliability and the information security in CRNs under interference from licensed transmitter and jamming signal. Theoretical results are obtained from analytical expressions in (15) and (30) while simulation results are generated from Monte-Carlo simulations with 10^6 channel realizations. The coordinates of $\mathtt{L_T}$, $\mathtt{L_R}$, $\mathtt{U_S}$, $\mathtt{U_D}$, and $\mathtt{E}$ are arbitrarily chosen as $(0.1, 0.9)$, $(0.8, 0.7)$, $(0.0, 0.0)$, $(1.0, 0.0)$, and $(0.9, 0.2)$, correspondingly, for illustration purpose while $\mathtt{U_J}$ is on the straight line connecting $\mathtt{U_S}$ and $\mathtt{U_D}$; that is, the coordinate of $\mathtt{U_J}$ is $(d, 0)$ where $0 < d < 1$. Additionally, the fading power for the $\mathtt{a}$-$\mathtt{b}$ channel is modelled as $\lambda_{\mathtt{ab}} = m_{\mathtt{ab}}^{-\chi}$ according to [36] where χ is the path-loss exponent and $m_{\mathtt{ab}}$ is the distance between the transmitter $\mathtt{a}$ and the

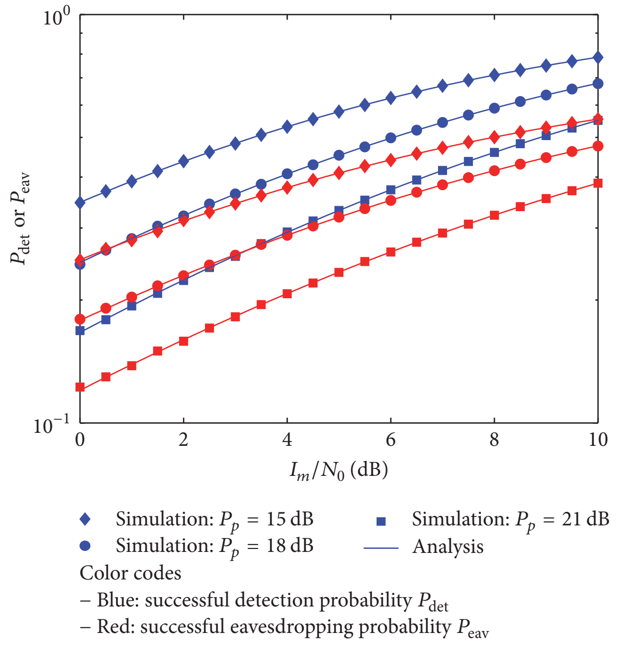


FIGURE 2: Successful detection probability and successful eavesdropping probability versus I_m/N_0.

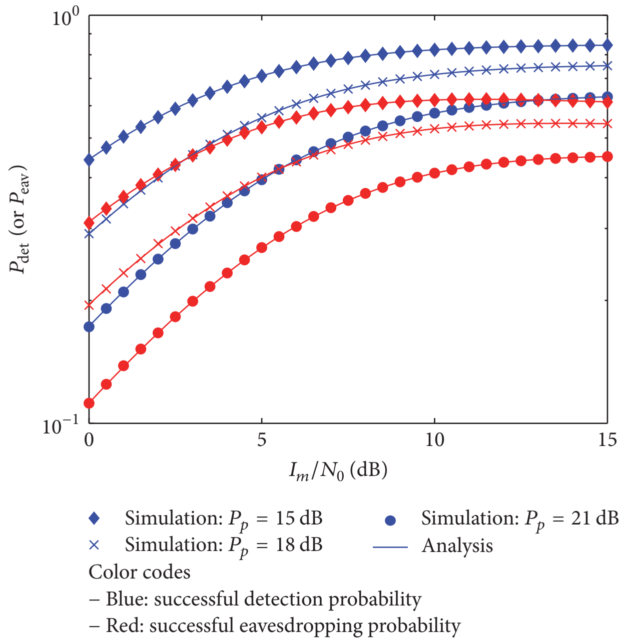


FIGURE 3: Successful detection probability and successful eavesdropping probability versus P_m/N_0.

receiver b. To limit case-studies, $\chi = 3$, and equal maximum transmit powers of unlicensed users (i.e., $\widehat{P}_s = \widehat{P}_j = P_m$) are investigated throughout this paper.

Figure 2 illustrates the trade-off between the communication reliability and the information security in CRNs with respect to the maximum interference power-to-noise power ratio I_m/N_0 for the maximum transmit power-to-noise power ratio $P_m/N_0 = 20$ dB, the required channel capacity $C_{\rm th} = 0.1$ bits/s/Hz, different interference levels from licensed transmitter ($P_p/N_0 = 15, 18, 21$ dB), the interference power distribution factor $\alpha = 0.3$, and $d = 0.3$. It is observed that the analysis accurately matches the simulation, confirming the validity of (15) and (30). Additionally, both the successful detection probability $P_{\rm det}$ and the successful eavesdropping probability $P_{\rm eav}$ are proportional to I_m. This is due to the fact that I_m upper-bounds the power of unlicensed transmitters according to $P_s = \min(\alpha I_m/|h_{sp}|^2, P_m)$ and $P_j = \min((1-\alpha)I_m/|h_{jp}|^2, P_m)$ and hence, the increase in I_m raises the transmit power, ultimately increasing β_d and β_e according to (10) and (11). In other words, the probabilities for β_d and β_e to be greater than a threshold increase proportionally to I_m. The fact that both $P_{\rm det}$ and $P_{\rm eav}$ are proportional to I_m shows that the communication reliability (i.e., $P_{\rm det}$) trades off the security capability (i.e., $P_{\rm eav}$). Moreover, interference from licensed transmitter decreases SINRs at both $\mathtt{U}_{\rm D}$ and E and hence, the decrease in SINRs at $\mathtt{U}_{\rm D}$ and E drastically reduces the successful detection probability and the successful eavesdropping probability. However, the successful detection probability is significantly larger than the successful eavesdropping probability. This signifies that the probability for the legal receiver $\mathtt{U}_{\rm D}$ to successfully recover the source information is larger than the probability for the illegal receiver E to do so, creating high security performance.

In the same context as Figure 2 except $I_m/N_0 = 12$ dB, Figure 3 demonstrates the trade-off between the communication reliability and the information security in CRNs with respect to the change of P_m/N_0. It is seen that the simulation and the analysis are in excellent agreement. This again validates the accuracy of (15) and (30). Additionally, same remarks as Figure 2 can be withdrawn such as the increase in the successful detection probability and the successful eavesdropping probability with respect to the increase in P_m, the degradation of the successful detection probability and the successful eavesdropping probability with respect to the increase in interference level from licensed transmitter, and the superiority of the successful detection probability to the successful eavesdropping probability which indicates a high information securing capability.

Figure 4 shows the trade-off between the communication reliability and the information security in CRNs with respect to the required channel capacity $C_{\rm th}$ for $d = 0.3$, $P_m/N_0 = 19$ dB, $I_m/N_0 = 15$ dB, $\alpha = 0.5$, and different interference levels from licensed transmitter ($P_p/N_0 = 15, 18, 21$ dB). It is observed that the analysis coincides with the simulation, confirming the validity of (15) and (30). Moreover, interference from licensed transmitter (i.e., P_p increases) dramatically reduces the successful detection probability and the successful eavesdropping probability. Furthermore, higher required channel capacity lowers these probabilities. This is reasonable because, given operation parameters, channel capacities at $\mathtt{U}_{\rm D}$ and E are only achieved at a certain level and hence, more stringent channel capacity requirement reduces the successful detection probability and the successful eavesdropping probability. Nevertheless, the successful detection probability outperforms the successful eavesdropping probability, indicating high security performance.

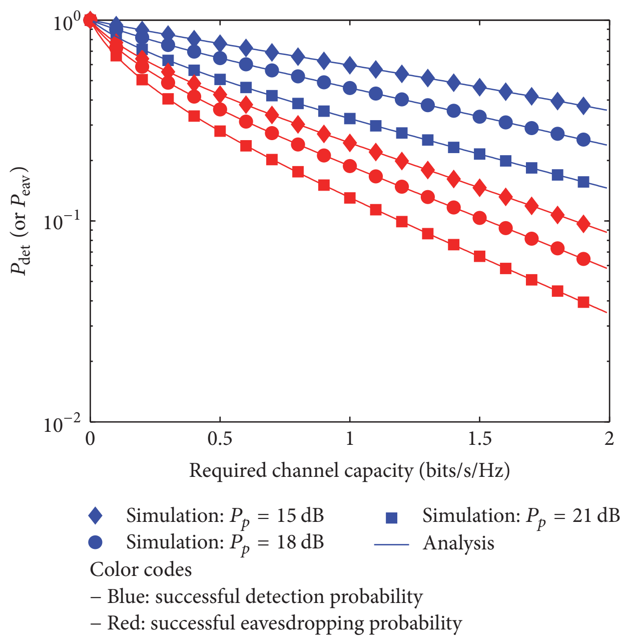


Figure 4: Successful detection probability and successful eavesdropping probability versus required channel capacity.

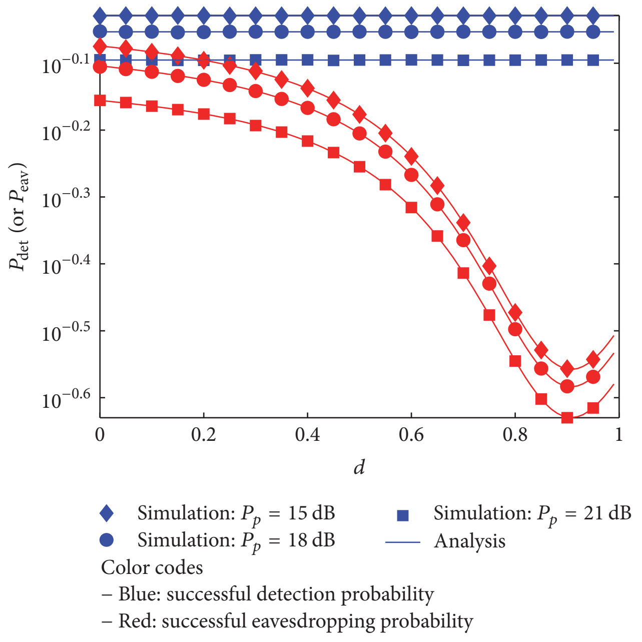


Figure 5: Successful detection probability and successful eavesdropping probability versus jammer's position.

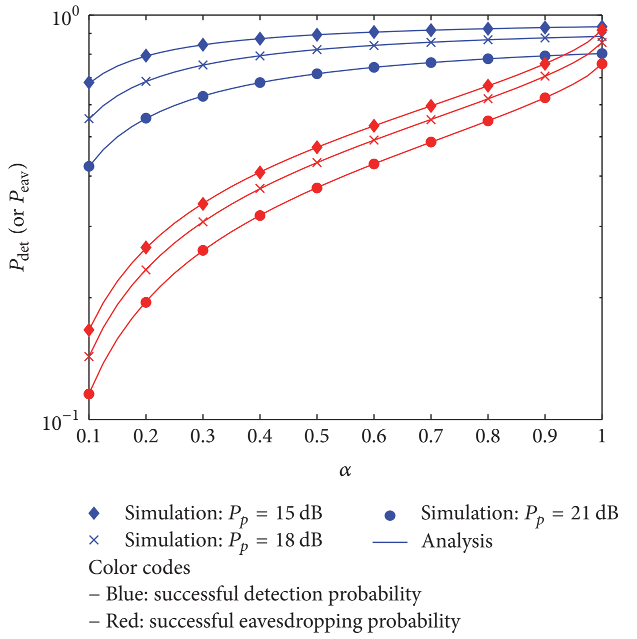


Figure 6: Successful detection probability and successful eavesdropping probability versus the interference power distribution factor.

Figure 5 illustrates the trade-off between the communication reliability and the information security in CRNs with respect to the jammer's position (i.e., d) for $P_m/N_0 = I_m/N_0 = 15$ dB, $C_{\rm th} = 0.1$ bits/s/Hz, $\alpha = 0.5$, and different interference levels from licensed transmitter ($P_p/N_0 = 15, 18, 21$ dB). It is observed that the simulation accurately matches the analysis, validating (15) and (30). Additionally, interference from licensed transmitter (i.e., P_p increases) significantly decreases the successful detection probability and the successful eavesdropping probability. Moreover, the successful detection probability is independent of the jammer's position. This is because the jamming signal is to purposely harm the signal reception of $\mathtt{E}$ without degrading the performance of $\mathtt{U}_{\rm D}$. However, the successful eavesdropping probability is severely dependent on the jammer's position. More specifically, because the jammer is located at $(0.9, 0.2)$, when the jammer moves toward the eavesdropper (i.e., d increases from 0 to 0.9), the successful eavesdropping probability drops abruptly due to the increase in the receive power of the jamming signal at $\mathtt{E}$. This enlarges the difference between the successful detection probability and the successful eavesdropping probability, securing information transmission of $\mathtt{U}_{\rm S}$ and emphasizing the role of the jammer in improving security performance. Furthermore, when the jammer moves away from the eavesdropper (i.e., d increases from 0.9 to 1), the successful eavesdropping probability increases significantly owing to the decrease in the receive power of the jamming signal at $\mathtt{E}$, reducing security performance. For all the jammer's position under consideration in Figure 5, the difference between the successful detection probability and the successful eavesdropping probability is very large, indicating high security performance.

Figure 6 demonstrates the trade-off between the communication reliability and the information security in CRNs with respect to the interference power distribution factor (i.e., α) for $P_m/N_0 = 15$ dB, $I_m/N_0 = 12$ dB, $C_{\rm th} = 0.1$ bits/s/Hz, $d = 0.7$, and different interference levels from licensed transmitter ($P_p/N_0 = 15, 18, 21$ dB). It is seen that the simulation and the analysis are in a perfect agreement, validating (15) and (30). Moreover, interference from licensed transmitter (i.e.,

P_p increases) considerably reduces the successful detection probability and the successful eavesdropping probability. Furthermore, the successful detection probability (or the successful eavesdropping probability) slowly (or quickly) increases with the increase of α, making the difference between them inversely proportional to α. The large difference between them represents the dominance of the successful detection probability to the successful eavesdropping probability (equivalently, high security capability). Therefore, Figure 6 shows that small values of α are good for information security.

5. Conclusions

The successful detection probability and the successful eavesdropping probability in underlay cognitive networks are analyzed in this paper under interferences from licensed transmitter and jammer, the maximum transmit power constraint, the interference power constraint, and Rayleigh fading to assess the communication reliability and the information security of CRNs without exhaustive simulations. Exact closed-form expressions of the successful detection probability and the successful eavesdropping probability are derived and verified by Monte-Carlo simulations. Numerous results illustrate that interference from licensed transmitter considerably reduces both probabilities while interference from the jammer makes the successful detection probability significantly larger than the successful eavesdropping probability, demonstrating the jammer's efficacy in enhancing security performance.

Appendix

A. Proof of Theorem 1

Because $P_s = \min(\alpha I_m/|h_{sp}|^2, \widehat{P}_s)$, P_s is a random variable. Hence, (13) can be computed indirectly through conditional probability as

$$P_{\text{det}} = \mathscr{E}_{|h_{sp}|^2}\left\{\underbrace{\Pr\left\{\beta_d \geq x \mid P_s\right\}}_{\eta}\right\}, \tag{A.1}$$

where η can be computed by inserting the explicit form of β_d in (10) into (A.1) and after some manipulations, one obtains

$$\begin{aligned}\eta &= \Pr\left\{\frac{P_s\left|h_{sd}\right|^2}{P_p\left|h_{pd}\right|^2 + N_0} \geq x \mid P_s\right\} = \Pr\left\{\left|h_{sd}\right|^2 \right.\\ &\left.\geq \frac{x\left(P_p\left|h_{pd}\right|^2 + N_0\right)}{P_s} \mid P_s\right\}\\ &= \mathscr{E}_{|h_{pd}|^2}\left\{\Pr\left\{\left|h_{sd}\right|^2 \right.\right.\\ &\left.\left.\geq \frac{x\left(P_p\left|h_{pd}\right|^2 + N_0\right)}{P_s} \mid \left|h_{pd}\right|^2, P_s\right\}\right\}.\end{aligned} \tag{A.2}$$

Because $h_{\text{ab}} \sim \mathscr{CN}(0, \lambda_{\text{ab}})$, $|h_{\text{ab}}|^2$ is exponentially distributed with mean of $1/\lambda_{\text{ab}}$; that is, $\Pr\{|h_{\text{ab}}|^2 \geq y\} = e^{-y/\lambda_{\text{ab}}}$ and the probability density function (PDF) of $|h_{\text{ab}}|^2$ is $f_{|h_{\text{ab}}|^2}(y) = e^{-y/\lambda_{\text{ab}}}/\lambda_{\text{ab}}$, $y \geq 0$. Based on this result, (A.2) is further simplified as

$$\begin{aligned}\eta &= \mathscr{E}_{|h_{pd}|^2}\left\{e^{-x(P_p|h_{pd}|^2+N_0)/P_s\lambda_{sd}} \mid \left|h_{pd}\right|^2, P_s\right\}\\ &= \int_0^\infty e^{-x(P_p y+N_0)/P_s\lambda_{sd}} f_{|h_{pd}|^2}(y)\,dy\\ &= \int_0^\infty e^{-x(P_p y+N_0)/P_s\lambda_{sd}} \frac{1}{\lambda_{pd}} e^{-y/\lambda_{pd}}\,dy\\ &= \frac{1}{\lambda_{pd}} e^{-xN_0/P_s\lambda_{sd}} \int_0^\infty e^{-(xP_p/P_s\lambda_{sd}+1/\lambda_{pd})y}\,dy\\ &= \left(\frac{P_p\lambda_{pd}x}{P_s\lambda_{sd}} + 1\right)^{-1} e^{-xN_0/P_s\lambda_{sd}}.\end{aligned} \tag{A.3}$$

Plugging $P_s = \min(\alpha I_m/|h_{sp}|^2, \widehat{P}_s)$ into (A.3) and then averaging η over $|h_{sp}|^2$, one can rewrite (A.1) as

$$\begin{aligned}P_{\text{det}} &= \mathscr{E}_{|h_{sp}|^2}\left\{\left(\frac{xP_p\lambda_{pd}}{\min\left(\alpha I_m/\left|h_{sp}\right|^2, \widehat{P}_s\right)\lambda_{sd}} + 1\right)^{-1}\right.\\ &\quad\left.\cdot e^{-xN_0/\min(\alpha I_m/|h_{sp}|^2,\widehat{P}_s)\lambda_{sd}}\right\}\\ &= \int_0^\infty \left(\frac{xP_p\lambda_{pd}}{\min\left(\alpha I_m/\left|h_{sp}\right|^2, \widehat{P}_s\right)\lambda_{sd}} + 1\right)^{-1}\\ &\quad\cdot e^{-xN_0/\min(\alpha I_m/|h_{sp}|^2,\widehat{P}_s)\lambda_{sd}} f_{|h_{sp}|^2}(y)\,dy.\end{aligned} \tag{A.4}$$

By dividing $\min(\alpha I_m/|h_{sp}|^2, \widehat{P}_s)$ into two cases, (A.4) is further simplified as

$$P_{\text{det}} = \widetilde{P}_{\text{det}} + \overline{P}_{\text{det}}, \tag{A.5}$$

where

$$\begin{aligned}\widetilde{P}_{\text{det}} &= \int_0^{\alpha I_m/\widehat{P}_s} \left(\frac{xP_p\lambda_{pd}}{\widehat{P}_s\lambda_{sd}} + 1\right)^{-1}\\ &\quad\cdot e^{-xN_0/\widehat{P}_s\lambda_{sd}} f_{|h_{sp}|^2}(y)\,dy = \left(\frac{xP_p\lambda_{pd}}{\widehat{P}_s\lambda_{sd}} + 1\right)^{-1}\\ &\quad\cdot e^{-xN_0/\widehat{P}_s\lambda_{sd}}\left(1 - e^{-\alpha I_m/\widehat{P}_s\lambda_{sp}}\right),\end{aligned}$$

$$\begin{aligned}\overline{P}_{\text{det}} &= \int_{\alpha I_m/\widehat{P}_s}^{\infty}\left(\frac{xP_p\lambda_{pd}}{(\alpha I_m/y)\,\lambda_{sd}}+1\right)^{-1} \\ &\quad\cdot e^{-xN_0/(\alpha I_m/y)\lambda_{sd}} f_{|h_{sp}|^2}(y)\,dy \\ &= \int_{\alpha I_m/\widehat{P}_s}^{\infty}\left(\frac{P_p\lambda_{pd}x}{\alpha I_m\lambda_{sd}}y+1\right)^{-1} e^{-(xN_0/\alpha I_m\lambda_{sd})y} \\ &\quad\cdot\frac{1}{\lambda_{sp}}e^{-y/\lambda_{sp}}dy = -\frac{\alpha I_m\lambda_{sd}}{\lambda_{sp}P_p\lambda_{pd}x} \\ &\quad\cdot e^{N_0/P_p\lambda_{pd}+\alpha I_m\lambda_{sd}/\lambda_{sp}P_p\lambda_{pd}x} Ei\left(-\left[\frac{xN_0}{\lambda_{sd}}+\frac{\alpha I_m}{\lambda_{sp}}\right]\right. \\ &\quad\left.\cdot\left[\frac{1}{\widehat{P}_s}+\frac{\lambda_{sd}}{P_p\lambda_{pd}x}\right]\right).\end{aligned} \tag{A.6}$$

Inserting (A.6) into (A.5), it is apparent that (A.5) exactly becomes (15), completing the proof.

B. Proof of Lemma 2

Performing the integral by part on (16), one obtains

$$\begin{aligned}\mathscr{L}(a,b,c,g) &= -Ei(-g-cz)\left.\frac{e^{-bz}}{b}\right|_a^{\infty} \\ &\quad+\int_a^{\infty}\frac{e^{-bz}}{b}c\frac{e^{-g-cz}}{g+cz}dz \\ &= -Ei(-g-cz)\left.\frac{e^{-bz}}{b}\right|_a^{\infty} \\ &\quad+\frac{e^{-g}}{b}\int_a^{\infty}\frac{e^{-(b+c)z}}{z+g/c}dz.\end{aligned} \tag{B.1}$$

By denoting

$$\mathscr{H}(a,b,c) = \int_a^{\infty}\frac{e^{-bx}}{x+c}dx, \tag{B.2}$$

it is straightforward to express the integrand in (B.2) in terms of the $Ei(\cdot)$ function as (18). Given the $\mathscr{H}(a,b,c)$ function in (B.2), one can express (B.1) as (17), completing the proof.

C. Proof of Lemma 3

Performing the variable change and then applying the series representation of $Ei(x)$ in [35, eq. (8.214.1)] to (19) result in

$$\begin{aligned}\mathscr{M}(a,b,c,g,l) &= -\frac{1}{g} \\ &\quad\cdot\int_{-ag-l}^{-\infty}\frac{e^{b((y+l)/g)}}{-(y+l)/g+c}Ei(y)\,dy \\ &= -e^{bl/g}\int_{-\infty}^{-ag-l}\frac{e^{(b/g)y}}{y+l-cg}\left(\mathtt{C}+\ln(-y)\right. \\ &\quad\left.+\sum_{k=1}^{\infty}\frac{y^k}{k\cdot k!}\right)dy.\end{aligned} \tag{C.1}$$

By denoting

$$\varphi_1 = \int_{-\infty}^{-ag-l}\frac{e^{(b/g)y}}{y+l-cg}dy, \tag{C.2}$$

$$\varphi_2 = \int_{-\infty}^{-ag-l}\frac{e^{(b/g)y}}{y+l-cg}\ln(-y)\,dy, \tag{C.3}$$

$$\varphi_3 = \int_{-\infty}^{-ga-l}\frac{y^k}{y-cg+l}e^{(b/g)y}dy, \tag{C.4}$$

it is apparent that (C.1) perfectly matches (20). Therefore, the proof is completed after representing integrands in (C.2), (C.3), and (C.4) as (21), (22), and (28), correspondingly.

Start with φ_1. Performing the variable change, one can rewrite φ_1 as

$$\varphi_1 = -\int_{\infty}^{ag+l}\frac{e^{-(b/g)x}}{-x-cg+l}dx = -\int_{ag+l}^{\infty}\frac{e^{-(b/g)x}}{x+cg-l}dx. \tag{C.5}$$

Using (B.2), one can express (C.5) as (21).

Performing the variable change and then applying the series representation of $\ln(x)$ in [35, eq. (1.512.2)], one can simplify φ_2 as

$$\begin{aligned}\varphi_2 &= -\int_{\infty}^{ag+l}\frac{e^{-(b/g)x}}{-x-cg+l}\ln(x)\,dx \\ &= -\int_{ag+l}^{\infty}\frac{e^{-(b/g)x}}{x+cg-l}\left[2\sum_{k=1}^{\infty}\frac{1}{2k-1}\left(\frac{x-1}{x+1}\right)^{2k-1}\right]dx \\ &= -\sum_{k=1}^{\infty}\frac{2}{2k-1}\int_{ag+l}^{\infty}\frac{e^{-(b/g)x}}{x+cg-l}\left(\frac{x-1}{x+1}\right)^{2k-1}dx.\end{aligned} \tag{C.6}$$

Applying the binomial expansion in [35, eq. (1.111)] to $(x-1)^{2k-1}$ of (C.6), one obtains

$$\begin{aligned}\varphi_2 &= -\sum_{k=1}^{\infty}\frac{2}{2k-1} \\ &\quad\cdot\int_{ag+l}^{\infty}\frac{e^{-(b/g)x}}{x+cg-l}\frac{\sum_{n=0}^{2k-1}\binom{2k-1}{n}x^n(-1)^{2k-1-n}}{(x+1)^{2k-1}}dx \\ &= -\sum_{k=1}^{\infty}\frac{2}{2k-1}\sum_{n=0}^{2k-1}\binom{2k-1}{n}(-1)^{2k-1-n} \\ &\quad\cdot\int_{ag+l}^{\infty}\frac{x^ne^{-(b/g)x}}{(x+cg-l)(x+1)^{2k-1}}dx,\end{aligned} \tag{C.7}$$

where the notation $\binom{2k-1}{n} = (2k-1)!/n!(2k-1-n)!$ is the binomial coefficient.

Again perform the variable change and then apply the binomial expansion to simplify (C.7) as

$$\begin{aligned}\varphi_2 &= -\sum_{k=1}^{\infty}\frac{2}{2k-1}\sum_{n=0}^{2k-1}\binom{2k-1}{n}(-1)^{2k-1-n} \\ &\cdot\int_{ag+l+1}^{\infty}\frac{(y-1)^n e^{-(b/g)(y-1)}}{(y-1+cg-l)\,y^{2k-1}}dy = -\sum_{k=1}^{\infty}\frac{e^{(b/g)}2}{2k-1} \\ &\cdot\sum_{n=0}^{2k-1}\binom{2k-1}{n}(-1)^{2k-1-n} \\ &\cdot\int_{ag+l+1}^{\infty}\frac{e^{-(b/g)y}}{(y+cg-l-1)\,y^{2k-1}}\left[\sum_{s=0}^{n}\binom{n}{s}y^s(-1)^{n-s}\right]dy \\ &= 2e^{b/g}\sum_{k=1}^{\infty}\sum_{n=0}^{2k-1}\sum_{s=0}^{n}\binom{2k-1}{n}\binom{n}{s} \\ &\cdot\frac{(-1)^s}{2k-1}\int_{ag+l+1}^{\infty}\frac{y^s e^{-(b/g)y}}{(y+cg-l-1)\,y^{2k-1}}dy.\end{aligned} \tag{C.8}$$

By denoting

$$\zeta = \int_{ag+l+1}^{\infty}\frac{y^s e^{-(b/g)y}}{(y+cg-l-1)\,y^{2k-1}}dy, \tag{C.9}$$

it is apparent that (C.8) perfectly matches (22). Hence, we must prove that the integrand in (C.9) can be represented as (23) to complete the proof of (22). Toward this end, we divide the problem into two cases: $s = 2k-1$ (Case 1) and $s \neq 2k-1$ (Case 2). For Case 1, ζ is rewritten as $\int_{ag+l+1}^{\infty}(e^{-(b/g)y}/(y+cg-l-1))dy$, which becomes $\mathscr{H}(ag+l+1, b/g, cg-l-1)$ as shown in (23). For Case 2, we denote $\theta = \int_{ag+l+1}^{\infty}(e^{-(b/g)y}/(y+cg-l-1)y^{2k-s-1})dy$. Combining two cases shows that (C.9) coincides with (23). Therefore, the remaining work is to prove that θ is given by (24).

Applying the partial fraction decomposition, θ can be simplified as

$$\begin{aligned}\theta &= p\int_{ag+l+1}^{\infty}\frac{e^{-(b/g)x}}{y+cg-l-1}dy \\ &+ \sum_{v=1}^{2k-s-1}q_{2k-s-1-v+1}\int_{ag+l+1}^{\infty}\frac{e^{-(b/g)y}}{y^v}dy,\end{aligned} \tag{C.10}$$

where p and q_m are defined in (25) and (26), respectively.

By denoting

$$\mathscr{B}(a,b,v) = \int_a^{\infty}\frac{e^{-bx}}{x^v}dx, \tag{C.11}$$

and noting that the first integrand of (C.10) can be represented in terms of the $\mathscr{H}(\cdot)$ function in (B.2), it is obvious that (C.10) becomes (24). The $\mathscr{B}(a,b,v)$ function can be represented as (27) by firstly performing the variable change and then using [35, eq. (3.381.6)].

Finally, we process φ_3. By performing the variable change and applying the binomial expansion, (C.4) is simplified as

$$\begin{aligned}\varphi_3 &= -\int_{\infty}^{ag+l}\frac{(-x)^k}{-x-cg+l}e^{-(b/g)x}dx = (-1)^{k+1} \\ &\cdot\int_{ag+l+cg-l}^{\infty}\frac{(y+l-cg)^k}{y}e^{-(b/g)(y+l-cg)}dy \\ &= (-1)^{k+1} \\ &\cdot e^{-(b/g)(l-cg)}\int_{ag+cg}^{\infty}\left[\sum_{n=0}^{k}\binom{k}{n}y^n(l-cg)^{k-n}\right] \\ &\cdot\frac{1}{y}e^{-(b/g)y}dy = (-1)^{k+1} \\ &\cdot e^{-(b/g)(l-cg)}\sum_{n=0}^{k}\binom{k}{n}(l-cg)^{k-n} \\ &\cdot\int_{(a+c)g}^{\infty}y^{n-1}e^{-(b/g)y}dy = (-1)^{k+1} \\ &\cdot e^{-(b/g)(l-cg)}\left[(l-cg)^k\int_{(a+c)g}^{\infty}\frac{e^{-(b/g)y}}{y}dy\right. \\ &\left.+\sum_{n=1}^{k}\binom{k}{n}(l-cg)^{k-n}\int_{(a+c)g}^{\infty}y^{n-1}e^{-(b/g)y}dy\right].\end{aligned} \tag{C.12}$$

By denoting

$$\mathscr{D}(a,b,n) = \int_a^{\infty}y^n e^{-by}dy, \tag{C.13}$$

whose exact closed form is given by (29) with the aid of [35, eq. (3.351.2)], it is apparent that the first integral in (C.12) is $\mathscr{H}([a+c]g, b/g, 0)$ and the second integral in (C.12) is $\mathscr{D}([a+c]g, b/g, n-1)$. As such, (C.12) exactly matches (28), completing the proof.

D. Proof of Theorem 4

Plugging (11) into (14) and after some simplification, one obtains

$$\begin{aligned}P_{\text{eav}} &= \Pr\left\{\frac{P_s\left|h_{se}\right|^2}{P_j\left|h_{je}\right|^2+P_p\left|h_{pe}\right|^2+N_0}\geq x\right\} \\ &= \Pr\left\{\left|h_{se}\right|^2\geq\frac{x}{P_s}\left(P_j\left|h_{je}\right|^2+P_p\left|h_{pe}\right|^2+N_0\right)\right\} \\ &= \mathscr{E}_{|h_{sp}|^2,|h_{jp}|^2,|h_{je}|^2,|h_{pe}|^2}\left\{e^{-x(P_j|h_{je}|^2+P_p|h_{pe}|^2+N_0)/P_s\lambda_{se}}\right\} \\ &= \mathscr{E}_{|h_{sp}|^2,|h_{jp}|^2}\left\{e^{-xN_0/P_s\lambda_{se}}\kappa\mu\right\},\end{aligned} \tag{D.1}$$

where

$$\begin{aligned}\kappa &= \mathscr{E}_{|h_{je}|^2}\left\{e^{-(xP_j/P_s\lambda_{se})|h_{je}|^2}\right\},\\ \mu &= \mathscr{E}_{|h_{pe}|^2}\left\{e^{-(xP_p/P_s\lambda_{se})|h_{pe}|^2}\right\}.\end{aligned} \tag{D.2}$$

Applying the definition of the expectation, one obtains the closed form of κ as

$$\begin{aligned}\kappa &= \int_0^\infty e^{-(xP_j/P_s\lambda_{se})y} f_{|h_{je}|^2}(y)\,dy\\ &= \int_0^\infty e^{-(xP_j/P_s\lambda_{se})y}\frac{1}{\lambda_{je}}e^{-y/\lambda_{je}}dy\\ &= \left(\frac{xP_j\lambda_{je}}{P_s\lambda_{se}}+1\right)^{-1}.\end{aligned} \tag{D.3}$$

Following the derivation of κ, one can also infer

$$\mu = \left(\frac{xP_p\lambda_{pe}}{P_s\lambda_{se}}+1\right)^{-1}. \tag{D.4}$$

Inserting (D.3) and (D.4) into (D.1), one can simplify (D.1) as

$$\begin{aligned}P_{\mathrm{eav}} &= \mathscr{E}_{|h_{sp}|^2,|h_{jp}|^2}\left\{e^{-xN_0/P_s\lambda_{se}}\left(\frac{xP_j\lambda_{je}}{P_s\lambda_{se}}+1\right)^{-1}\right.\\ &\quad\left.\cdot\left(\frac{xP_p\lambda_{pe}}{P_s\lambda_{se}}+1\right)^{-1}\right\}\\ &= \mathscr{E}_{|h_{sp}|^2}\left\{e^{-xN_0/P_s\lambda_{se}}\left(\frac{xP_p\lambda_{pe}}{P_s\lambda_{se}}+1\right)^{-1}\rho\right\},\end{aligned} \tag{D.5}$$

where

$$\rho = \mathscr{E}_{|h_{jp}|^2}\left\{\left(\frac{xP_j\lambda_{je}}{P_s\lambda_{se}}+1\right)^{-1}\right\}. \tag{D.6}$$

By plugging (9) into (D.6), one can decompose ρ as

$$\begin{aligned}&\rho\\ &= \mathscr{E}_{|h_{jp}|^2}\left\{\left[\frac{x\lambda_{je}}{P_s\lambda_{se}}\min\left(\frac{(1-\alpha)I_m}{\left|h_{jp}\right|^2},\widehat{P}_j\right)+1\right]^{-1}\right\}\\ &= \widetilde{\rho}+\overline{\rho},\end{aligned} \tag{D.7}$$

where

$$\begin{aligned}\widetilde{\rho} &= \int_0^{(1-\alpha)I_m/\widehat{P}_j}\left(\frac{x\lambda_{je}\widehat{P}_j}{P_s\lambda_{se}}+1\right)^{-1} f_{|h_{jp}|^2}(y)\,dy\\ &= \left(\frac{x\lambda_{je}\widehat{P}_j}{P_s\lambda_{se}}+1\right)^{-1}\left(1-e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right),\end{aligned}$$

$$\begin{aligned}\overline{\rho} &= \int_{(1-\alpha)I_m/\widehat{P}_j}^\infty\left(\frac{x\lambda_{je}}{P_s\lambda_{se}}\frac{(1-\alpha)I_m}{y}+1\right)^{-1}\\ &\quad\cdot f_{|h_{jp}|^2}(y)\,dy\\ &= \int_{(1-\alpha)I_m/\widehat{P}_j}^\infty\left(\frac{x\lambda_{je}}{P_s\lambda_{se}}\frac{(1-\alpha)I_m}{y}+1\right)^{-1}\\ &\quad\cdot\frac{1}{\lambda_{jp}}e^{-y/\lambda_{jp}}dy = \frac{1}{\lambda_{jp}}\int_{(1-\alpha)I_m/\widehat{P}_j}^\infty\left[1\right.\\ &\quad\left.-\frac{x\lambda_{je}(1-\alpha)I_m}{P_s\lambda_{se}}\left(y+\frac{x\lambda_{je}(1-\alpha)I_m}{P_s\lambda_{se}}\right)^{-1}\right]\\ &\quad\cdot e^{-y/\lambda_{jp}}dy = e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}+\frac{x\lambda_{je}(1-\alpha)I_m}{P_s\lambda_{se}\lambda_{jp}}\\ &\quad\cdot e^{x\lambda_{je}(1-\alpha)I_m/P_s\lambda_{se}\lambda_{jp}}Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}\right.\\ &\quad\left.-\frac{x\lambda_{je}(1-\alpha)I_m}{P_s\lambda_{se}\lambda_{jp}}\right).\end{aligned} \tag{D.8}$$

By substituting (D.8) into (D.7) and then plugging the result together with (8) into (D.5), one can partition P_{eav} into two terms as

$$\begin{aligned}P_{\mathrm{eav}} &= \mathscr{E}_{|h_{sp}|^2}\left\{e^{-xN_0/P_s\lambda_{se}}\left(\frac{xP_p\lambda_{pe}}{P_s\lambda_{se}}+1\right)^{-1}\right.\\ &\quad\cdot\left[\left(\frac{x\lambda_{je}\widehat{P}_j}{P_s\lambda_{se}}+1\right)^{-1}\left(1-e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right)\right.\\ &\quad+e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}+\frac{x\lambda_{je}(1-\alpha)I_m}{P_s\lambda_{se}\lambda_{jp}}\\ &\quad\cdot e^{x\lambda_{je}(1-\alpha)I_m/P_s\lambda_{se}\lambda_{jp}}Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}\right.\\ &\quad\left.\left.\left.-\frac{x\lambda_{je}(1-\alpha)I_m}{P_s\lambda_{se}\lambda_{jp}}\right)\right]\right\} = \mathscr{E}_{|h_{sp}|^2}\left\{\left(1\right.\right.\\ &\quad\left.-e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right)\left(\frac{xP_p\lambda_{pe}}{\lambda_{se}\min\left(\alpha I_m/\left|h_{sp}\right|^2,\widehat{P}_s\right)}\right.\\ &\quad\left.+1\right)^{-1}\left(\frac{x\lambda_{je}\widehat{P}_j}{\lambda_{se}\min\left(\alpha I_m/\left|h_{sp}\right|^2,\widehat{P}_s\right)}+1\right)^{-1}\\ &\quad\cdot e^{-xN_0/\lambda_{se}\min(\alpha I_m/|h_{sp}|^2,\widehat{P}_s)}\end{aligned}$$

$$
\begin{aligned}
&+ e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}} \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}\min\left(\alpha I_m/\left|h_{sp}\right|^2, \widehat{P}_s\right)} \right. \\
&\left. + 1 \right)^{-1} e^{-xN_0/\lambda_{se}\min(\alpha I_m/|h_{sp}|^2, \widehat{P}_s)} \\
&+ \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}} \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}} \right. \\
&\left. + \min\left(\frac{\alpha I_m}{\left|h_{sp}\right|^2}, \widehat{P}_s \right) \right)^{-1} \\
&\cdot e^{(\lambda_{je}(1-\alpha)I_m/\lambda_{se}\lambda_{jp} - N_0/\lambda_{se})(x/\min(\alpha I_m/|h_{sp}|^2, \widehat{P}_s))} \\
&\cdot Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}} \right. \\
&\left. \left. - \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}\min\left(\alpha I_m/\left|h_{sp}\right|^2, \widehat{P}_s\right)} \right) \right\} = \widetilde{P}_{\text{eav}} \\
&+ \overline{P}_{\text{eav}},
\end{aligned}
\tag{D.9}
$$

where

$$
\begin{aligned}
\widetilde{P}_{\text{eav}} = \int_0^{\alpha I_m/\widehat{P}_s} &\left\{ \left(1 - e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right) \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}\widehat{P}_s} \right. \right. \\
&\left. + 1 \right)^{-1} \left(\frac{x\lambda_{je}\widehat{P}_j}{\lambda_{se}\widehat{P}_s} + 1 \right)^{-1} e^{-xN_0/\lambda_{se}\widehat{P}_s} \\
&+ \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}} \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}} + \widehat{P}_s \right)^{-1} \\
&\cdot e^{(\lambda_{je}(1-\alpha)I_m/\lambda_{se}\lambda_{jp} - N_0/\lambda_{se})(x/\widehat{P}_s)} Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}} \right. \\
&\left. - \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}\widehat{P}_s} \right) + e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}} \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}\widehat{P}_s} \right. \\
&\left. \left. + 1 \right)^{-1} e^{-xN_0/\lambda_{se}\widehat{P}_s} \right\} f_{|h_{sp}|^2}(y)\, dy,
\end{aligned}
\tag{D.10}
$$

$$
\begin{aligned}
\overline{P}_{\text{eav}} = \int_{\alpha I_m/\widehat{P}_s}^{\infty} &\left\{ \left(1 - e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right) \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}(\alpha I_m/y)} \right. \right. \\
&\left. + 1 \right)^{-1} \left(\frac{x\lambda_{je}\widehat{P}_j}{\lambda_{se}(\alpha I_m/y)} + 1 \right)^{-1} e^{-xN_0/\lambda_{se}(\alpha I_m/y)} \\
&+ \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}} \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}} + \frac{\alpha I_m}{y} \right)^{-1} \\
&\cdot e^{(\lambda_{je}(1-\alpha)I_m/\lambda_{se}\lambda_{jp} - N_0/\lambda_{se})(x/(\alpha I_m/y))} Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}} \right. \\
&\left. - \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}(\alpha I_m/y)} \right) \\
&+ e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}} \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}(\alpha I_m/y)} + 1 \right)^{-1} \\
&\left. \cdot e^{-xN_0/\lambda_{se}(\alpha I_m/y)} \right\} f_{|h_{sp}|^2}(y)\, dy.
\end{aligned}
\tag{D.11}
$$

Plugging $f_{|h_{sp}|^2}(y) = e^{-y/\lambda_{sp}}/\lambda_{sp}$ into (D.10) and after some simplification, one obtains the exact closed-form representation of $\widetilde{P}_{\text{eav}}$ as

$$
\begin{aligned}
\widetilde{P}_{\text{eav}} = &\left\{ \left(1 - e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right) \left(\frac{x\lambda_{je}\widehat{P}_j}{\lambda_{se}\widehat{P}_s} + 1 \right)^{-1} \right. \\
&+ e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}} + \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}\widehat{P}_s} \\
&\cdot e^{x\lambda_{je}(1-\alpha)I_m/\lambda_{se}\lambda_{jp}\widehat{P}_s} Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}} \right. \\
&\left. \left. - \frac{x\lambda_{je}(1-\alpha)I_m}{\lambda_{se}\lambda_{jp}\widehat{P}_s} \right) \right\} \left(\frac{xP_p\lambda_{pe}}{\lambda_{se}\widehat{P}_s} + 1 \right)^{-1} \left(1 \right. \\
&\left. - e^{-\alpha I_m/\widehat{P}_s\lambda_{sp}} \right) e^{-xN_0/\lambda_{se}\widehat{P}_s}.
\end{aligned}
\tag{D.12}
$$

Substituting $f_{|h_{sp}|^2}(y) = e^{-y/\lambda_{sp}}/\lambda_{sp}$ into (D.11) and performing the partial fraction decomposition, one can simplify (D.11) as

$$
\begin{aligned}
\overline{P}_{\text{eav}} = &\frac{\lambda_{se}\alpha I_m}{x\lambda_{sp}} \left(\frac{1 - e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}}{P_p\lambda_{pe} - \lambda_{je}\widehat{P}_j} + \frac{e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}}{P_p\lambda_{pe}} \right) \int_{\alpha I_m/\widehat{P}_s}^{\infty} \frac{e^{-(xN_0/\lambda_{se}\alpha I_m + 1/\lambda_{sp})y}}{y + \lambda_{se}\alpha I_m/xP_p\lambda_{pe}} dy \\
&- \frac{\lambda_{se}\alpha I_m\left(1 - e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right)}{x\lambda_{sp}\left(P_p\lambda_{pe} - \lambda_{je}\widehat{P}_j\right)} \int_{\alpha I_m/\widehat{P}_s}^{\infty} \frac{e^{-(xN_0/\lambda_{se}\alpha I_m + 1/\lambda_{sp})y}}{y + \lambda_{se}\alpha I_m/x\lambda_{je}\widehat{P}_j} dy
\end{aligned}
$$

$$\begin{aligned}&+\frac{\lambda_{je}(1-\alpha)I_m}{P_p\lambda_{pe}\lambda_{jp}\lambda_{sp}}\int_{\alpha I_m/\widehat{P}_s}^{\infty}e^{(x\lambda_{je}(1-\alpha)/\alpha\lambda_{se}\lambda_{jp}-xN_0/\alpha I_m\lambda_{se}-1/\lambda_{sp})y}Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}-\frac{x\lambda_{je}(1-\alpha)}{\lambda_{se}\lambda_{jp}\alpha}y\right)dy\\&-\frac{\lambda_{je}\lambda_{se}\alpha(1-\alpha)}{x\lambda_{jp}\lambda_{sp}}\left(\frac{I_m}{P_p\lambda_{pe}}\right)^2\int_{\alpha I_m/\widehat{P}_s}^{\infty}\frac{e^{(x\lambda_{je}(1-\alpha)/\alpha\lambda_{se}\lambda_{jp}-xN_0/\alpha I_m\lambda_{se}-1/\lambda_{sp})y}}{y+\lambda_{se}\alpha I_m/xP_p\lambda_{pe}}Ei\left(-\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}-\frac{x\lambda_{je}(1-\alpha)}{\lambda_{se}\lambda_{jp}\alpha}y\right)dy.\end{aligned}\tag{D.13}$$

Representing the integrals in (D.13) in terms of $\mathscr{L}(\cdot)$ in (17), $\mathscr{H}(\cdot)$ in (18), and $\mathscr{M}(\cdot)$ in (20), one obtains the exact closed-form expression of $\overline{P}_{\text{eav}}$ as

$$\begin{aligned}\overline{P}_{\text{eav}}&=\frac{\lambda_{se}\alpha I_m}{x\lambda_{sp}}\Bigg(\frac{1-e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}}{P_p\lambda_{pe}-\lambda_{je}\widehat{P}_j}\\&\quad+\frac{e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}}{P_p\lambda_{pe}}\Bigg)\mathscr{H}\Bigg(\frac{\alpha I_m}{\widehat{P}_s},\frac{xN_0}{\lambda_{se}\alpha I_m}+\frac{1}{\lambda_{sp}},\\&\quad\frac{\lambda_{se}\alpha I_m}{xP_p\lambda_{pe}}\Bigg)-\frac{\lambda_{se}\alpha I_m\left(1-e^{-(1-\alpha)I_m/\widehat{P}_j\lambda_{jp}}\right)}{x\lambda_{sp}\left(P_p\lambda_{pe}-\lambda_{je}\widehat{P}_j\right)}\mathscr{H}\Bigg(\frac{\alpha I_m}{\widehat{P}_s},\\&\quad\frac{xN_0}{\lambda_{se}\alpha I_m}+\frac{1}{\lambda_{sp}},\frac{\lambda_{se}\alpha I_m}{x\lambda_{je}\widehat{P}_j}\Bigg)+\frac{\lambda_{je}(1-\alpha)I_m}{P_p\lambda_{pe}\lambda_{jp}\lambda_{sp}}\\&\quad\cdot\mathscr{L}\Bigg(\frac{\alpha I_m}{\widehat{P}_s},\frac{xN_0}{\alpha I_m\lambda_{se}}+\frac{1}{\lambda_{sp}}-\frac{x\lambda_{je}(1-\alpha)}{\alpha\lambda_{se}\lambda_{jp}},\\&\quad\frac{x\lambda_{je}(1-\alpha)}{\lambda_{se}\lambda_{jp}\alpha},\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}\Bigg)\\&\quad-\frac{\lambda_{je}\lambda_{se}\alpha(1-\alpha)}{x\lambda_{jp}\lambda_{sp}}\left(\frac{I_m}{P_p\lambda_{pe}}\right)^2\mathscr{M}\Bigg(\frac{\alpha I_m}{\widehat{P}_s},\frac{xN_0}{\alpha I_m\lambda_{se}}\\&\quad+\frac{1}{\lambda_{sp}}-\frac{x\lambda_{je}(1-\alpha)}{\alpha\lambda_{se}\lambda_{jp}},\frac{\lambda_{se}\alpha I_m}{xP_p\lambda_{pe}},\frac{x\lambda_{je}(1-\alpha)}{\lambda_{se}\lambda_{jp}\alpha},\\&\quad\frac{(1-\alpha)I_m}{\widehat{P}_j\lambda_{jp}}\Bigg).\end{aligned}\tag{D.14}$$

Inserting (D.12) and (D.14) into (D.9) results in (30), completing the proof.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

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

References

[1] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.

[2] M. Tavana, A. Rahmati, V. Shah-Mansouri, and B. Maham, "Cooperative sensing with joint energy and correlation detection in cognitive radio networks," *IEEE Communications Letters*, vol. 21, no. 1, pp. 132–135, 2017.

[3] D. Darsena, G. Gelli, and F. Verde, "An opportunistic spectrum access scheme for multicarrier cognitive sensor networks," *IEEE Sensors Journal*, vol. 17, no. 8, pp. 2596–2606, 2017.

[4] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[5] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.

[6] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in Cognitive Radio Networks," *China Communications*, vol. 12, no. 3, Article ID 7084371, pp. 132–150, 2015.

[7] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48–54, 2015.

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

[9] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8812–8817, 2016.

[10] J. Hu, Y. Cai, N. Yang, X. Zhou, and W. Yang, "Artificial-Noise-Aided Secure Transmission Scheme with Limited Training and Feedback Overhead," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 193–205, 2017.

[11] X. Ding, T. Song, Y. Zou, and X. Chen, "Security-Reliability Tradeoff for Friendly Jammer Assisted User-Pair Selection in the Face of Multiple Eavesdroppers," *IEEE Access*, vol. 4, pp. 8386–8393, 2016.

[12] M. Li, Z. Dong, and G. Wang, "Security versus Reliability Analysis for Multi-Eavesdropper Cooperation Wireless Networks with Best Relay," in *Proceedings of the 2017 IEEE International Conference on Energy Internet (ICEI)*, pp. 244–249, Beijing, China, April 2017.

[13] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3810–3823, 2015.

[14] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading

channels," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1814–1827, 2014.

[15] K. Ho-Van, "Outage analysis in cooperative cognitive networks with opportunistic relay selection under imperfect channel information," *International Journal of Electronics and Communications*, vol. 69, no. 11, pp. 1700–1708, 2015.

[16] K. Ho-Van, "Exact outage probability analysis of proactive relay selection in cognitive radio networks with MRC receivers," *Journal of Communications and Networks*, vol. 18, no. 3, Article ID 7575795, pp. 288–298, 2016.

[17] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Cooperative relaying and jamming for primary secure communication in cognitive two-way networks," in *Proceedings of the 83rd IEEE Vehicular Technology Conference, VTC Spring 2016*, Nanjing, China, May 2016.

[18] B. Fang, Z. Qian, W. Zhong, and W. Shao, "AN-Aided Secrecy Precoding for SWIPT in Cognitive MIMO Broadcast Channels," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1632–1635, 2015.

[19] V.-D. Nguyen, T. Q. Duong, O. A. Dobre, and O.-S. Shin, "Joint Information and Jamming Beamforming for Secrecy Rate Maximization in Cognitive Radio Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2609–2623, 2016.

[20] B. Fang, Z. Qian, W. Shao, and W. Zhong, "Precoding and Artificial Noise Design for Cognitive MIMOME Wiretap Channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6753–6758, 2016.

[21] Y. Wu, X. Chen, and X. Chen, "Secure beamforming for cognitive radio networks with artificial noise," in *Proceedings of the 2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, pp. 1–5, Nanjing, China, October 2015.

[22] 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 the 27th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, PIMRC 2016*, Spain, September 2016.

[23] Y. Cai, X. Xu, and W. Yang, "Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise," *IET Communications*, vol. 10, no. 15, pp. 1904–1913, 2016.

[24] V. Nguyen, T. Q. Duong, O. Shin, A. Nallanathan, and G. K. Karagiannidis, "Enhancing PHY Security of Cooperative Cognitive Radio Multicast Communications," *IEEE Transactions on Cognitive Communications and Networking*, 2017.

[25] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, "Cooperative jamming for secure communications in MIMO Cooperative Cognitive Radio Networks," in *Proceedings of the IEEE International Conference on Communications, ICC 2015*, pp. 7609–7614, London, UK, June 2015.

[26] W. Liu, L. Guo, T. Kang, J. Zhang, and J. Lin, "Secure cognitive radio system with cooperative secondary networks," in *Proceedings of the 2015 22nd International Conference on Telecommunications, ICT 2015*, pp. 6–10, Sydney, Australia, April 2015.

[27] T. He, H. Chen, and Q. Liu, "QoS-based beamforming with cooperative jamming in Cognitive Radio Networks," in *Proceedings of the 2013 International Conference on Communications, Circuits and Systems, ICCCAS 2013*, pp. 42–45, Chengdu, China, November 2013.

[28] W. Liu, M. Z. I. Sarkar, and T. Ratnarajah, "On the security of cognitive radio networks: Cooperative jamming with relay selection," in *Proceedings of the 2014 European Conference on Networks and Communications, EuCNC 2014*, Bologna, Italy, June 2014.

[29] 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*, vol. 11, no. 1, pp. 1–9, 2017.

[30] Y. Zou, "Physical-Layer Security for Spectrum Sharing Systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1319–1329, 2017.

[31] Y. W. Liu, L. F. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 46–49, 2015.

[32] P. Chakraborty and S. Prakriya, "Secrecy Performance of an Idle Receiver Assisted Underlay Secondary Network," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9555–9560, 2017.

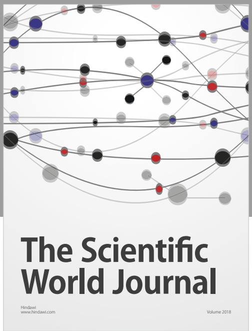
[33] K. Ho-Van, P. C. Sofotasios, and S. Freear, "Underlay cooperative cognitive networks with imperfect Nakagami-m fading channel information and strict transmit power constraint: Interference statistics and outage probability analysis," *Journal of Communications and Networks*, vol. 16, no. 1, pp. 10–17, 2014.

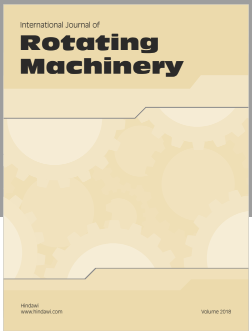
[34] E. Biglieri, J. Proakis, and S. Shamai, "Fading channels: information-theoretic and communications aspects," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 44, no. 6, pp. 2619–2692, 1998.

[35] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic Press, San Diego, CA, USA, 6th edition, 2000.

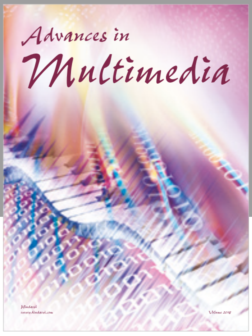
[36] N. Ahmed, M. A. Khojastepour, and B. Aazhang, "Outage minimization and optimal power control for the fading relay channel," in *Proceedings of the 2004 IEEE Information Theory Workshop - Proceedings, ITW*, pp. 458–462, San Antonio, TX, USA, October 2004.

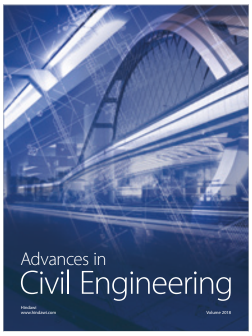
Journal of
Engineering

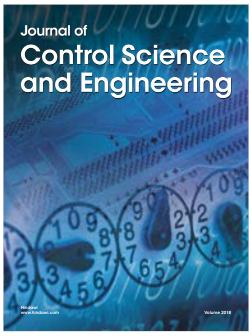

The Scientific
World Journal


International Journal of
Rotating
Machinery

Journal of
Sensors

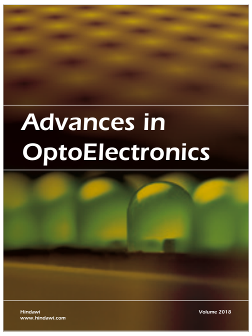

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

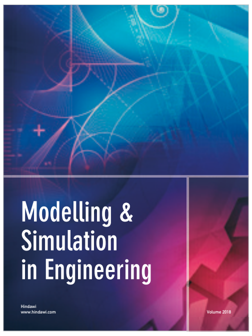
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

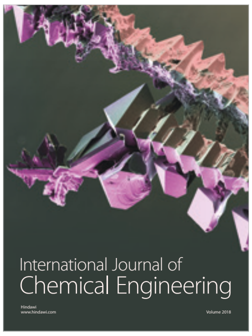

Advances in
OptoElectronics

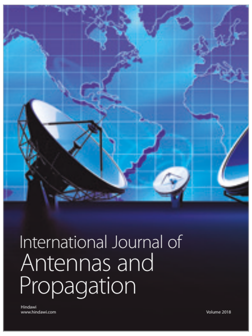
VLSI Design

International Journal of
Navigation and
Observation

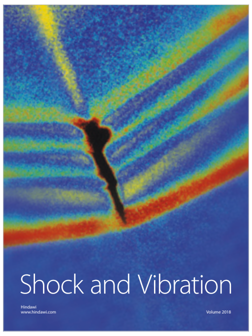

Modelling &
Simulation
in Engineering

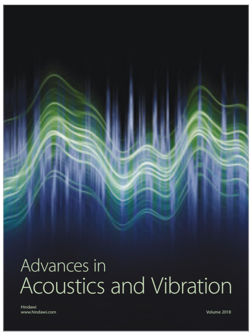
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration