This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2020.3040964, IEEE Transactions on Vehicular Technology

Power Allocation and Outage Analysis for Secure MISO Cognitive Radio Networks With an Unknown Eavesdropper

Shaobo Jia, *Member, IEEE,* Jiankang Zhang, *Senior Member, IEEE,* Di Zhang, *Senior Member, IEEE,* Wanming Hao, *Member, IEEE,* Feifei Gao, *Fellow, IEEE,*

***Abstract*—This paper investigates the power allocation problem for secure secondary transmission in a multiple-input single-output cognitive wiretap system with artificial noise (AN). The secondary transmitter exchanges confidential information with the secondary destination in the presence of an unknown eavesdropper. Since the eavesdropper's channel state information (CSI) is unavailable, we propose an optimal adaptive power allocation scheme, and derive a closed-form expression of the optimal power allocation factor that minimizes the secrecy outage probability (SOP). A suboptimal fixed power allocation scheme is also proposed to reduce the system complexity. Moreover, exact closed-form expressions of SOP under both schemes are derived. Numerical results are provided to corroborate the accuracy of our analytical results and the superiority of the proposed schemes to the benchmarks.**

***Index Terms*—Physical layer security, cognitive radio, power allocation, artificial noise, secrecy outage probability.**

I. Introduction

Cognitive radio networks (CRNs) have attracted ever growing interest from the wireless community due to its potential in addressing the conflict between the stringent requirement and spectrum scarcity in the next generation of wireless communications [1]-[3]. The security issues in CRNs are of the utmost importance and have attracted widespread attention. To achieve communication confidentiality against eavesdropping attacks, physical layer security (PLS) is proposed by smartly exploiting intrinsic randomness of the communications media. Recently, significant effort has been devoted to the research on the PLS in CRNs [4]-[5]. To ensure the existence of a nonzero secrecy rate when the channel quality of the wiretap link is superior to that of the legitimate link, Goel *et al.* in [6] proposed to employ artificial noise (AN) to improve PLS. Triggered by [6], a numerous body of works have studied AN assisted schemes concerning on PLS [7].

In the AN assisted secure transmission scheme, the power allocation between the AN and the information signals is one of the major concerns [8]-[10]. In [8], the power allocation was optimized by minimizing the secrecy outage probability (SOP) under a given secrecy rate constraint in multiple-input single-output (MISO) wiretap channel. An AN-assisted optimal cognitive beamforming scheme was proposed in [9], in which the power allocation was optimized to maximize the achievable ergodic secrecy rate. Zhou *et al.* in [10] examined PLS of non-orthogonal multiple access CRNs using non-linear energy harvesting with perfect or imperfect knowledge of eavesdroppers' channel state information (CSI). In [11], the power allocation was designed for secure multi-antenna transmission under a stochastic geometry framework, wherein the closed-form expression of the optimal power allocation factor (PAF) was derived. In the aforementioned works, the eavesdroppers' channel statistics are required in order to optimize the power allocation. However, since the eavesdroppers usually remain silent in practical scenario, it is very challenging, if not impossible, to obtain their statistical information in real wiretap scenarios.

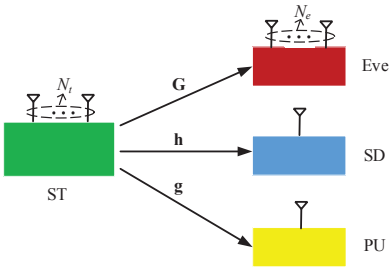

Fig. 1: MISO CRN consisting of a primary user (PU), a secondary transmitter (ST), a secondary destination (SD), and a multi-antenna eavesdropper (Eve).

In this paper, we investigate the secure secondary transmission in a multi-antenna cognitive wiretap system with AN. We seek to optimize the power allocation with an unknown eavesdropper. Our main contributions are three-fold: First, we propose an adaptive power allocation scheme which adaptively adjusts the PAF according to the instantaneous CSI of the legitimate channel, we further derive a closed-form expression of the optimal PAF by minimizing the SOP. Second, a suboptimal fixed power allocation scheme is presented to achieve a lower computational complexity with a near-optimal secrecy outage performance. Third, we derive novel closed-form expressions of SOP under both schemes. Interestingly, numerical results illustrate that, in comparison with the conventional fixed power allocation scheme which requires the eavesdropper's statistical CSI, the proposed adaptive power allocation scheme achieves a higher secrecy outage performance without the need of eavesdropper's any prior information.

II. System model

We consider an underlay MISO CRN as illustrated in Fig. 1, where a secondary transceiver shares the licensed spectrum of a PU, and a multi-antenna Eve tries to overhear

This work was supported by National Natural Science Foundation of China under Grant No. 61571401, and Innovative Talent of Colleges and University of Henan Province under Grant 18HASTIT021.*(Corresponding author: Di Zhang and Jiankang Zhang.)*

S. Jia, D. Zhang, and W. Hao are with School of Information Engineering, Zhengzhou University, Zhengzhou, 450001 China (email: jiashaobo2007@126.con, dr.di.zhang@ieee.org, iewmhao@zzu.edu.cn).

J. Zhang is with the School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China, and also with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: jz09v@ecs.soton.ac.uk).

F. Gao is with Institute for Artificial Intelligence, Tsinghua University (THUAI), State Key Lab of Intelligent Technologies and Systems, Tsinghua University, Beijing National Research Center for Information Science and Technology (BNRist), Department of Automation, Tsinghua University Beijing, P.R.China (email: feifeigao@ieee.org).

the secondary transmission. We assume that SD and PU are equipped with a single antenna, while ST and Eve with N_t and N_e antennas, respectively. Let $\mathbf{h} \in \mathbb{C}^{N_t \times 1}$, $\mathbf{g} \in \mathbb{C}^{1\times(N_t-1)}$ and $\mathbf{G} \in \mathbb{C}^{N_e\times(N_t-1)}$ denote the channels from ST to SD, PU and Eve, respectively. All wireless links are assumed to undergo independent Rayleigh fading. The channel gains are modeled as complex Gaussian random variables (RVs) with zero mean. Each entry of $\mathbf{h}$, $\mathbf{g}$ and $\mathbf{G}$ has a variance of $1/\lambda_S$, $1/\lambda_P$ and $1/\lambda_E$, repectively. Considering an unknown eavesdropper, we assume that the prior information of Eve (such as $\mathbf{G}$, N_e and λ_E) is unavailable for all nodes in the network.

Since the Eve is unknown, AN-aided secure scheme adopted in [12] is employed to guarantee the security for SD. ST transmits an information signal u in conjunction with an $(N_t-2)\times 1$ AN vector $\mathbf{v}$ to impair the Eve's channel. Accordingly, the transmit signal at ST is $\mathbf{x} = \mathbf{w}u + \mathbf{W}\mathbf{v}$, where the variance of u is χ_1 and each entry of $\mathbf{v}$ has a variance χ_N. Due to its lower computational load of implementation, the projected secret beamforming in [13] is chosen here, where $\mathbf{w}$ is given by

$$\mathbf{w} = \frac{(\mathbf{I} - \mathbf{g}(\mathbf{g}^H\mathbf{g})^{-1}\mathbf{g}^H)\mathbf{h}}{\|(\mathbf{I} - \mathbf{g}(\mathbf{g}^H\mathbf{g})^{-1}\mathbf{g}^H)\mathbf{h}\|}. \tag{1}$$

Here $(\cdot)^H$ is the conjugate transpose operation and $\|\cdot\|$ is Frobenius norm. Then, the precoding matrix $\mathbf{W} \in \mathbb{C}^{N_t\times(N_t-2)}$ of the jamming signal lies in the null space of $\mathbf{h}^H$ and $\mathbf{g}^H$. Therefore, we have $\tilde{\mathbf{W}} = [\mathbf{h}^H/\|\mathbf{h}\|, \mathbf{g}^H/\|\mathbf{g}\|, \mathbf{W}]$ forms an orthogonal basis of $\mathbb{C}^{N_T}$. Let P denotes the total transmit power at ST, we denote the fraction of transmit power allocated to u as the PAF ϕ, where $\phi \in (0, 1]$. Since ST does not know $\mathbf{G}$, the transmit power allocated to the AN is distributed equally to each entry of $\mathbf{v}$. Bearing this in mind, we have

$$\chi_1 = \phi P, \qquad \chi_N = \frac{(1-\phi)P}{N_t - 2}. \tag{2}$$

Since the Eve's noise level is typically unknown, we consider the worst-case scenario to guarantee the secure secondary transmission, where the noise power at the Eve is assumed to be zero [7], [9], [12]. Based on this, the instantaneous signal-to-noise ratios (SNRs) at SD and Eve can be respectively written as

$$\gamma_s = \frac{\chi_1}{\sigma^2}\left|\mathbf{h}^H\mathbf{w}\right|^2, \gamma_e = \frac{\chi_1}{\chi_N}\tilde{\mathbf{g}}^H(\tilde{\mathbf{G}}\tilde{\mathbf{G}}^H)^{-1}\tilde{\mathbf{g}}, \tag{3}$$

where $\tilde{\mathbf{g}} = \mathbf{G}\mathbf{w}$, $\tilde{\mathbf{G}} = \mathbf{G}\mathbf{W}$, and σ^2 is the noise variance at SD. Consequently, the instantaneous secrecy capacity in the multi-antenna CRN is expressed as

$$C_S = [C_D - C_E]^+, \tag{4}$$

where $[x]^+ \triangleq \max(0, x)$, $C_D = \log_2(1+\gamma_s)$ and $C_E = \log_2(1+\gamma_e)$ are the channel capacity of the main link and wiretap link, respectively.

III. Optimal power allocation

In this section, we optimize the PAF for the purpose of minimizing the SOP. To this end, intuitively, the closed-form expression of the SOP should be first derived under a given PAF, and then take the derivation of the derived SOP with respect to (w.r.t.) PAF targeting to obtain the optimal solution. However, in this way, the analytical expression is typically cumbersome, and a closed-form solution for the optimal PAF is intractable. In order to tackle this troublesome problem, our approach is to minimize the possibility of each secrecy outage event instead of the SOP as the objective function.

A. Optimal adaptive power allocation (OAPA)

By invoking the secrecy outage formulation in [14], the outage event is defined as

$$\mathcal{O}(R_S) := \{C_S < R_S\}, \tag{5}$$

where $R_S > 0$ is the target secrecy rate. Observing (5), we find that in order to avoid the secrecy outage event $\mathcal{O}(R_S)$ as much as possible, we can maximize the instantaneous secrecy capacity C_S by optimizing the PAF. However, C_S involves in the Eve's prior information which is considered to be unknown. In what follows, we make an ingenious transformation to cope with it.

Substituting (3) into (5), after some further mathematical manipulations, the secrecy outage event in (5) can be reformulated as

$$\mathcal{O}(R_S) := \left\{\omega(\phi) = \frac{(1-\varepsilon+\chi_1/\sigma^2 X)\chi_N}{\varepsilon\chi_1} < Y\right\}, \tag{6}$$

where $X \triangleq \left|\mathbf{h}^H\mathbf{w}\right|^2$, $Y \triangleq \tilde{\mathbf{g}}^H(\tilde{\mathbf{G}}\tilde{\mathbf{G}}^H)^{-1}\tilde{\mathbf{g}}$ and $\varepsilon \triangleq 2^{R_S}$. Fortunately, as shown in (6), $\omega(\phi)$ involves in the CSIs between ST and SD, ST and PU, which are the prior knowledge at ST. Y which is independent of ϕ comprises of the CSI between ST and Eve. Inspired by this observation, for the case of unknown Eve's prior information, the optimal PAF ϕ^* of the OAPA scheme is reasonably attained as

$$\phi^* = \arg\max_{0<\phi\le 1}\{\omega(\phi)\}. \tag{7}$$

Note that $\frac{\partial^2\omega(\phi)}{\partial\phi^2} = -\frac{2(\varepsilon-1)}{\varepsilon(N-2)\phi^3} < 0$, and therefore, $\omega(\phi)$ is a concave function. Then, we calculate the first derivative of $\omega(\phi)$ w.r.t. ϕ and set it to zero, ϕ^* is obtained as

$$\phi^* = \begin{cases} \sqrt{\frac{\varepsilon-1}{\bar{\gamma}X}}, & X \ge \frac{\varepsilon-1}{\bar{\gamma}}; \\ 1, & X < \frac{\varepsilon-1}{\bar{\gamma}}. \end{cases} \tag{8}$$

where $\bar{\gamma} = P/\sigma^2$.

Remark 1: The result of (8) reveals that ϕ^* is determined by the maximal achievable instantaneous SNR at SD $\Gamma_D = \bar{\gamma}X$ and the target secrecy rate R_S. When the maximal achievable instantaneous SNR at SD is large enough, i.e., $\Gamma_D > \varepsilon - 1$, ϕ^* decreases for a larger Γ_D or a smaller R_S, that is to say, when Γ_D increases or R_S decreases, more power should be allocated to the AN for minimizing the SOP. On the other hand, when $\Gamma_D \le \varepsilon - 1$, all the transmit power is allocated to the information signal, since the noise power at Eve is considered to be zero, a secrecy outage event will happen.

Remark 1 provides insightful guidelines for power allocation design in the absence of the Eve's prior information. As such, $\mathbf{h}$ and $\mathbf{g}$ in X can be obtained at ST through the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2020.3040964, IEEE Transactions on Vehicular Technology

channel estimation among legitimate nodes, while **G** is typically unknown in the passive eavesdropping environment. As a consequence, the proposed OAPA scheme which adaptively adjusts the PAF based on the instantaneous CSIs of legitimate links can be effectively applied into the practical networks to hold the optimal performance.

B. Suboptimal fixed power allocation (SFPA)

The optimal PAF of the OAPA scheme should be adjusted under each X, which imposes an excessive complexity. In order to ease the computational load of implementation, we hereafter proposed a SFPA scheme, where the optimal PAF remains fixed during transmissions. From the law of large numbers, we know that when N_t is sufficiently large (i.e., $N_t \to \infty$), (3) can be reexpressed as

$$\lim_{N_t\to\infty} \gamma_s = \frac{\chi_1 (N_t - 1)}{\sigma^2 \lambda_S}. \tag{9}$$

Similar procedure as we derive (8) can be followed to obtain the optimal PAF ϕ_∞^* of the SFPA scheme that minimizes the SOP as

$$\phi_\infty^* = \begin{cases} \sqrt{\frac{(\varepsilon-1)}{\bar{\Gamma}_B(N_t-1)}}, & \bar{\Gamma}_B \geq \frac{\varepsilon-1}{N_t-1}; \\ 1, & \bar{\Gamma}_B < \frac{\varepsilon-1}{N_t-1}, \end{cases} \tag{10}$$

where $\bar{\Gamma}_B = \bar{\gamma}\lambda_S^{-1}$ represents the maximum achievable average SNR at SD.

Remark 2: The result derived in (10) indicates that the optimal PAF ϕ_∞^* is independent of Eve's prior information. ϕ_∞^* is determined by $\bar{\Gamma}_B$, N_t and R_S. If $\bar{\Gamma}_B \geq \frac{\varepsilon-1}{N_t-1}$ holds, ϕ_∞^* decreases for a larger $\bar{\Gamma}_B$ (N_t) or a smaller R_S, that is to say, when $\bar{\Gamma}_B$ (N_t) increases or R_S decreases, more power should be allocated to the AN for minimizing the SOP.

Since the instantaneous CSIs of legitimate links vary rapidly, the application of the OAPA scheme is limited in fast fading environments owning to its implementation complexity. It is worth noting that, the paramters $\bar{\gamma}$, N_t, R_S and λ_S can be readily obtained at ST. Hence, the proposed SFPA scheme provides a simple yet efficient way for power allocation design. As will be indicated in the numerical results, the SFPA scheme guarantees a near-optimal secrecy outage performance.

IV. Secrecy outage performance analysis

In this section, exact closed-form expressions of the SOP in the considered cognitive wiretap system adopting the proposed OAPA and SFPA schemes are presented. SOP is characterized as the probability that the instantaneous secrecy rate is below a predefined threshold secrecy rate. Mathematically, SOP can be formulated as

$$P_{out} = \Pr\left(C_S < R_S\right) \tag{11}$$

By substituting (2), (3) and (8) into (11), after some algebraic manipulations, the expression of SOP for the OAPA scheme P_{out}^{OA} is derived as

$$\begin{aligned} P_{out}^{OA} &= \Pr\left(\frac{1+\frac{\chi_1}{\sigma^2}X}{1+\frac{\chi_1}{\chi_N}Y} < \varepsilon\right) \\ &= \Pr\left(Z < Y\right), \end{aligned} \tag{12}$$

where $Z = \frac{\left(\sqrt{\bar{\gamma}X} - \sqrt{\varepsilon-1}\right)^2}{\varepsilon(N_t-2)}$.

As shown in (12), to obtain the closed-form expression of SOP, we should characterize the probability density function (PDF) of the positive random variable Z. Mathematically, the cumulative distribution function (CDF) of Z is expressed as

$$\begin{aligned} F_Z(z) &= \Pr\left(\frac{\left(\sqrt{\bar{\gamma}X} - \sqrt{\varepsilon-1}\right)^2}{\varepsilon(N_t-2)} < z\right) \\ &= \Pr\left(X < \left(\sqrt{\varepsilon-1} + \sqrt{z\varepsilon(N_t-2)}\right)^2/\bar{\gamma}\right). \end{aligned} \tag{13}$$

Since X follows a Gamma distribution with parameters $(N_t - 1, 1/\lambda_S)$, the CDF of X is expressed as

$$F_X(x) = 1 - \sum_{k=0}^{N_t-2} \frac{(\lambda_S)^k x^k}{k!} e^{-\lambda_S x}. \tag{14}$$

Resorting to (13) and (14), the CDF of Z can be rewritten as

$$F_Z(z) = 1 - \sum_{k=0}^{N_t-2} \frac{A^k}{k!}\left(B + C\sqrt{z}\right)^{2k} e^{-A\left(B+C\sqrt{z}\right)^2}, \tag{15}$$

where $A = \frac{\lambda_S}{\bar{\gamma}}$, $B = \sqrt{\varepsilon-1}$ and $C = \sqrt{\varepsilon(N_t-2)}$. Substituting (15) into (12), P_{out}^{OA} can be further derived as

$$P_{out}^{OA} = 1 - \sum_{k=0}^{N_t-2} \frac{A^k}{k!} \int_0^\infty \left(B + C\sqrt{z}\right)^{2k} e^{-A\left(B+C\sqrt{z}\right)^2} f_Y(z) dz. \tag{16}$$

Based on [8, eq. (11)], the PDF of Y is given by

$$f_Y(y) = \sum_{m=0}^{N_e-1} \frac{\binom{N_t-2}{m}(N_t-2)y^m}{(1+y)^{N_t-1}} - \sum_{m=1}^{N_e-1} \frac{\binom{N_t-2}{m} m y^{m-1}}{(1+y)^{N_t-2}}, \tag{17}$$

$$\begin{aligned} P_{out}^{OA} = 1 - \sum_{k=0}^{N_t-2} \frac{A^k}{k!} \Bigg\{ & \sum_{m=0}^{N_e-1} \sum_{n=0}^{2k} \binom{N_t-2}{m} \binom{2k}{n} B^{2k-n} C^n (N_t-2) \Lambda_1 \big(\varphi_1 (2ABC)^{-\lambda_1} \mho(a_1, b_1, c_1, \lambda_1) \\ & + \varphi_2 (2ABC)^{-\lambda_2} \mho(a_1, b_1, c_1, \lambda_2)\big) - \sum_{m=1}^{N_e-1} \sum_{n=0}^{2k} \binom{N_t-2}{m} \binom{2k}{n} B^{2k-n} C^n m \Lambda_2 \\ & \times \left(\varphi_3 (2ABC)^{-\phi_1} \mho\left(a_2, b_2, c_2, \upsilon_1\right) + \varphi_4 (2ABC)^{-\phi_2} \mho\left(a_2, b_2, c_2, \upsilon_2\right)\right) \Bigg\} \end{aligned} \tag{24}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2020.3040964, IEEE Transactions on Vehicular Technology

where $\binom{K}{k} = \frac{K!}{(K-k)!k!}$ is the binomial coefficient. Substituting (17) into (16), after simple mathematical manipulations, P_{out}^{OA} can be further computed as

$$P_{out}^{OA} = 1 - \sum_{k=0}^{N_t-2} \frac{A^k}{k!} \Bigg\{ \sum_{m=0}^{N_e-1} \sum_{n=0}^{2k} \binom{N_t-2}{m} \binom{2k}{n} (N_t-2) \times B^{2k-n} C^n \underbrace{\int_0^\infty e^{-A(B+C\sqrt{z})^2} z^{m+\frac{n}{2}} (1+z)^{1-N_t} dz}_{\Xi_1} - \sum_{m=1}^{N_e-1} \sum_{n=0}^{2k} \binom{N_t-2}{m} \binom{2k}{n} B^{2k-n} C^n m \times \underbrace{\int_0^\infty e^{-A(B+C\sqrt{z})^2} z^{m+\frac{n}{2}-1} (1+z)^{2-N_t} dz}_{\Xi_2} \Bigg\}. \quad (18)$$

In what follows, we will proceed to derive Ξ_1 and Ξ_2, respectively. Apparently, it is rather cumbersome to directly calculate Ξ_1 and Ξ_2. Utilizing integration by substitution $z = t^2$, Ξ_1 can be derived as

$$\Xi_1 = 2 \int_0^\infty e^{-A(B+Ct)^2} \frac{t^{2m+n+1}}{(1+t^2)^{N_t-1}} dt. \quad (19)$$

Using integration by parts, we have

$$\begin{aligned} \Xi_1 &= -2 \int_0^\infty \frac{t^{2+2m+n} {}_2F_1(a_1, b_1, c_1, -t^2)}{2+2m+n} de^{-A(B+Ct)^2} \\ &= \varphi_1 \underbrace{\int_0^\infty t^{2+2m+n} e^{-2ABCt} {}_2F_1(a_1, b_1, c_1, -t^2) e^{-AC^2t^2} dt}_{\mathcal{J}_1} \\ &+ \varphi_2 \underbrace{\int_0^\infty t^{3+2m+n} e^{-2ABCt} {}_2F_1(a_1, b_1, c_1, -t^2) e^{-AC^2t^2} dt}_{\mathcal{J}_2}, \end{aligned} \quad (20)$$

where $a_1 = 1 + m + \frac{n}{2}$, $b_1 = N_t - 1$, $c_1 = 2 + m + \frac{n}{2}$, $\varphi_1 = \frac{4ABCe^{-AB^2}}{2+2m+n}$ and $\varphi_2 = \frac{4AC^2 \exp(-AB^2)}{2+2m+n}$ for ease of notation, ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ is the Gauss hypergeometric function [15, eq. (9.100)].

With the aid of [16, eq. (07.34.03.0228.01)] and [17, eq. (17)], the exponential function and the Gauss hypergeometric function can be written in terms of Meijer's *G*-function, then the integral $\mathcal{J}_1$ in (20) is evaluated as

$$\mathcal{J}_1 = \frac{\Gamma(c_1)}{\Gamma(a_1)\Gamma(b_1)} \int_0^\infty t^{2+2m+n} G_{0,1}^{1,0} \left[2ABCt \middle|_0^- \right] \times G_{2,2}^{1,2} \left[t^2 \middle| {}_{0,1-c_1}^{1-a_1,1-b_1} \right] G_{0,1}^{1,0} \left[AC^2t^2 \middle|_0^- \right] dt, \quad (21)$$

where $G_{m,n}^{p,q}[\cdot]$ is the Meijer's *G*-function [15, eq. (9.301)], $\Gamma(c) = \int_0^\infty t^{c-1} e^{-t} dt$ is the well-known Gamma function [15, eq. (8.310.1)]. By invoking the relationship between Meijer's *G*-function and Fox's *H*-function [16, eq. (07.34.26.0008.01)], the Meijer's *G*-function can be further expressed in terms of Fox's *H*-function, whose definition is given exactly in [18, eq. (1.2)]. Resorting to [18, eq. (2.3)], $\mathcal{J}_1$ is finally derived as

$$\mathcal{J}_1 = \Lambda_1 (2ABC)^{-\lambda_1} \mho(a_1, b_1, c_1, \lambda_1) \quad (22)$$

where

$$\mho(a, b, c, \lambda) \triangleq H_{1,0:0,1:2,2}^{0,1:1,0:1,2} \left[{}_{-}^{1-\lambda,2,2} \middle|_{(0,1)}^{-} \middle| {}_{(0,1),(1-c,1)}^{(1-a,1),(1-b,1)} \middle| \psi_1, \psi_2 \right]$$

with $\psi_1 = \frac{1}{4AB^2}$, $\psi_2 = \frac{1}{4A^2B^2C^2}$, $\lambda_1 = 2m + n + 3$, $\Lambda_1 = \frac{\Gamma(c_1)}{\Gamma(a_1)\Gamma(b_1)}$. $H_{p.q}^{m,n}[\cdot]$ denotes the Fox's *H*-function. $H_{p_1,q_1:p_2,q_2:p_3,q_3}^{m_1,n_1:m_2,n_2:m_3,n_3}[\cdot]$ represents the bivariate Fox's *H*-function. Notably, the implementation of bivariate Fox's *H*-function is available at the popular softwares, including MATLAB [19, Appendix A] and Mathematica [20, Table I]. Following a similar approach to that we derive $\mathcal{J}_1$, the exact expression of $\mathcal{J}_2$ can be computed as

$$\mathcal{J}_2 = \Lambda_1 (2ABC)^{-\lambda_2} \mho(a_1, b_1, c_1, \lambda_2), \quad (23)$$

where $\lambda_2 = 2m + n + 4$. Substituting (22) and (23) into (20), we can obtain Ξ_1.

Similarly, the exact expression of Ξ_2 can be also obtained following the derivation of Ξ_1. Substituting the obtained Ξ_1 and Ξ_2 into (18), we can finally obtain the closed-form expression of P_{out}^{OA} as (24), shown at the bottom of previous page, with $\varphi_3 = \frac{4ABCe^{-AB^2}}{2m+n}$, $\varphi_4 = \frac{4AC^2e^{-AB^2}}{2m+n}$, $a_2 = m + \frac{n}{2}$, $b_2 = N_t - 2$, $c_2 = 1 + m + \frac{n}{2}$, $\Lambda_2 = \frac{\Gamma(c_2)}{\Gamma(a_2)\Gamma(b_2)}$, $\upsilon_1 = 2m + n + 1$ and $\upsilon_2 = 2m + n + 2$.

By plugging ϕ_∞^* into [9, eq. (60)], the corresponding SOP for the SFPA scheme can be readily obtained as

$$P_{out}^{SF} = 1 - \sum_{k=0}^{N_t-2} \frac{(\lambda_S)^k}{k!} \sum_{l=0}^{k} \binom{k}{l} N^{k-l} M^l \times \left(\sum_{m=0}^{N_e-1} \binom{N_t-2}{m} (N_t-2)\Theta_1 - \sum_{m=1}^{N_e-1} \binom{N_t-2}{m} m\Theta_2 \right), \quad (25)$$

where $M = \frac{\varepsilon(N_t-2)}{\bar{\gamma}(1-\phi_\infty^*)}$, $N = \frac{\varepsilon-1}{\phi_\infty^*\bar{\gamma}}$, $\Theta_1 = e^{-\lambda_S N_t} \Gamma(1 + l + m) \mathrm{U}(1 + l + m, 3 + l + m - N_t, \lambda_S M)$ and $\Theta_2 = e^{-\lambda_S N_t} \Gamma(l+m) \mathrm{U}(l+m, 3+l+m-N_t, \lambda_S M)$ with $\mathrm{U}(\cdot,\cdot,\cdot)$ representing the confluent hypergeometric Kummer U function [15, eq. (9.211.4)].

V. Numerical results

We present numerical results for validation of the derived expressions. Without special instructions, we set $\lambda_S = \lambda_E = \lambda_P = 1$, the average receive noise power at SD is set as $\sigma^2 = 0$ dBm, the threshold secrecy rate is set as $R_S = 1$bits/s/Hz. We also compare the performance of the proposed scheme with existing schemes, namely, fixed power allocation (FPA) in [8] and equal power allocation (EPA) schemes as benchmarks.

Fig. 2 depicts the SOP of the proposed system using four different power allocation schemes versus P for different N_t. Fig. 2 confirms that the analytical results are in close agreement with the simulation results. Interestingly, it is observed that the proposed OAPA scheme outperforms the FPA one in the entire transmit power range granted that Eve's prior information is totally absent. This is due to the fact that, recalling (5) and (6), it is readily to know $\omega(\phi^*) \geq \omega(\alpha^*)$ (α^* represents the optimal PAF for the FPA scheme), thereby leading to a smaller probability of secrecy outage event for the OAPA case. A specific observation is that there is only

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2020.3040964, IEEE Transactions on Vehicular Technology

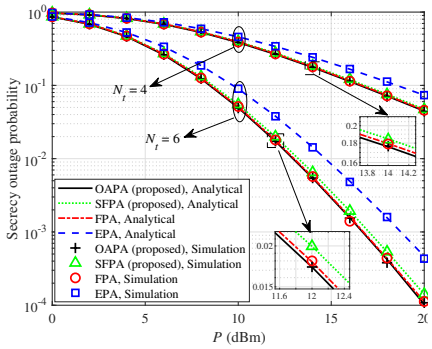

Fig. 2: SOP versus P with various N_t when $N_e = 2$.

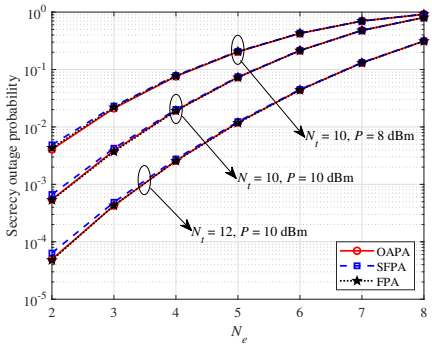

Fig. 3: SOP versus N_e with various N_t and P.

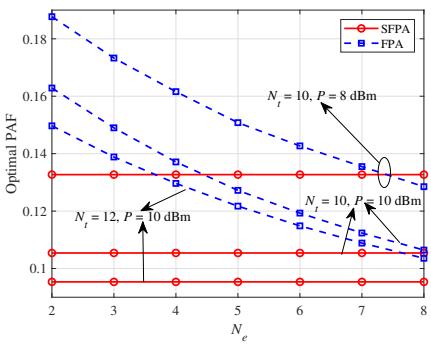

Fig. 4: Optimal PAF versus N_e with various N_t and P.

a slight performance degrade for the proposed SFPA scheme compared with the APA and FPA cases. It is worth pointing out that the OAPA and SFPA schemes are both performed in the absence of Eve's prior information, whilst the FPA scheme resorts to Eve's statistical CSI to implement the exhaustive search. This observation confirms that the proposed SFPA is a simple and generic strategy. In addition, it is evident that these three schemes are significantly superior to the EPA case.

Fig. 3 illustrates the SOP of the proposed system versus N_e for different N_t and P. It is observed that the SFPA scheme exhibits a considerably excellent SOP performance. Moreover, the performance gap can be further reduced with a larger N_e value. Under the identical parameters, the corresponding optimal PAFs for the FPA and SFPA schemes are also presented in Fig. 4. It is observed that ϕ_∞^* is independent of N_e, and the increasing N_e leads to a decrease in the value of optimal PAF α^* for the FPA scheme. Especially when $N_e = 2$, the maximum differences between α^* and ϕ_∞^* not exceed 0.06. These observations suggest that the propose SFPA scheme can achieve a near-optimal SOP performance. It is worth pointing out that N_e is required to be known for the FPA scheme, which are difficult to obtain in practice. It can be also seen that the increasing N_t or P leads to a decrease in the value of ϕ_∞^*. This conclusion is confirmed by the insights in **Remark 2**.

VI. Conclusion

This paper investigated the power allocation problem for secure secondary transmission in a MISO CRN coexisting with an unknown eavesdropper. An OAPA scheme was proposed, for which a novel explicit solution of the optimal PAF was derived by minimizing the SOP. A low-complexity SFPA scheme was also proposed. Closed-form expressions of SOP under both schemes were derived. Numerical results showed that, in comparison with the the conventional FPA scheme, the proposed OAPA scheme achieves a higher secrecy outage performance without the need of eavesdropper's prior information. Moreover, the SFPA scheme offers a comparable secrecy outage performance to that of FPA scheme but with a much lower complexity.

References

[1] J. Zhao, T. Yang, Y. Gong, J. Wang, and L. Fu, "Power control algorithm of cognitive radio based on non-cooperative game theory," *China Communications*, vol. 10, no. 11, pp. 143-154, Nov. 2013.

[2] J. Zhao, X. Guan, and X. Li, "Power allocation based on genetic simulated annealing algorithm in cognitive radio networks," *Chinese Journal of Electronics*, vol. 22, no. 1, pp. 177-180, Jan. 2013.

[3] H. Sun, F. Zhou, R. Q. Hu, and L. Hanzo, "Robust beamforming design in a NOMA cognitive radio network relying on SWIPT," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 142-155, Jan. 2019.

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

[5] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237-2250, Mar. 2017.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[7] S. Jia, J. Zhang, H. Zhao, and R. Zhang, "Relay selection for improved security in cognitive relay networks with jamming," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 662-665, Oct. 2017.

[8] D. Hu, P. Mu, W. Zhang, and W. Wang, "Minimization of secrecy outage probability with artificial-noise-aided beamforming for MISO wiretap channels," *IEEE Commun. Lett.*, Feb. 2020.

[9] A. Al-Nahari, G. Geraci, M. Al-Jamali, M. H. Ahmed, and N. Yang, "Beamforming with artificial noise for secure MISOME cognitive radio transmissions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1875-1889, Aug. 2018.

[10] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 918-931, Apr. 2018.

[11] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812-8817, Oct. 2016.

[12] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.

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

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

[15] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[16] Wolfram, The Wolfram Functions Site. [Online]. Available: http: //functions.wolfram.com/.

[17] V. Adamchik and O. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system," *in Proceedings of the international symposium on Symbolic and algebraic computation*, 1990, pp. 212-224.

[18] A. M. Mathai, R. K. Saxena, and H. J. Haubold, "*The H-Function: Theory and Applications*," New York, NY, USA: Springer-Verlag New York, 2010.

[19] K. P. Peppas, "A new formula for the average bit error probability of dual-hop amplify-and-forward relaying systems over generalized shadowed fading channels," *IEEE Wireless Commun. Lett.*, vol. 1, no. 2, pp. 85-88, Apr. 2012.

[20] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M. S. Alouini, "Secrecy capacity analysis over α-μ fading channels, *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445-1448, Jun. 2017.