Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Secure analysis on artificial-noise-aided simultaneous wireless information and power transfer systems*

Wei-min HOU[1], Qing-shan TANG[†‡2]

[1]*School of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang 050018, China*
[2]*School of Physics & Electronic Science, Changsha University of Science & Technology, Changsha 410114, China*
[†]E-mail: cstqs001@126.com

Received Feb. 21, 2020; Revision accepted June 27, 2020; Crosschecked Sept. 16, 2020

Abstract: In this paper, we investigate the secrecy outage performance in simultaneous wireless information and power transfer (SWIPT) systems taking artificial noise assistance into account. Multiple antennas in the source and a single antenna in both the legitimate receiver and the eavesdropper are assumed. Specifically, the transmitted signal at the source is composed of two parts, where the first part is the information symbols and the other is the noise for the eavesdropper. To avoid making noise in the legitimate receiver, these two parts in the transmitted signals are modulated into two orthogonal dimensions according to the instantaneous channel state between the source and the legitimate receiver. We derive an approximate closed-form expression for the secrecy outage probability (SOP) by adopting the Gauss-Laguerre quadrature (GLQ) method, where the gap between the exact SOP and our approximate SOP converges with increase of the summation terms in the GLQ. To obtain the secrecy diversity order and secrecy array gain for the considered SWIPT system, the asymptotic result of the SOP is also derived. This is tight in the high signal-to-noise ratio region. A novel and robust SOP approximation is also analyzed given a small variance of the signal-to-interference-plus-noise ratio at the eavesdropper. Some selected Monte-Carlo numerical results are presented to validate the correctness of the derived closed-form expressions.

Key words: Artificial noise; Multi-antenna systems; Secrecy outage probability; Simultaneous wireless information and power transfer
https://doi.org/10.1631/FITEE.2000083 **CLC number:** TN929.5

1 Introduction

In wireless communications, one main medium for the delivery over the physical channel is the radio-frequency (RF) signal radiated by ambient transmitters. This is also regarded as a viable energy source. In fact, RF signals have been widely used as a carrier for information transmission in wireless networks, which makes RF signals more convenient to act as the energy source. This also explains why simultaneous wireless information and power transfer (SWIPT) systems are more and more popular in both theory and applications (Sudevalayam and Kulkarni, 2011). Another important reason for the popularity of SWIPT is that SWIPT can provide a convenient, safe, and green alternative for energy-harvesting. For example, in wireless sensor networks, it may be difficult or even impossible to replace the batteries of sensors, especially when some sensors are embedded in building structures. If SWIPT is used, there is no need to replace batteries of the sensors for a long time, thereby prolonging the life of these sensors. If the networks operate in some high radiation environments, it is very hazardous for humans to replace the batteries (Sudevalayam and Kulkarni, 2011).

‡ Corresponding author
* Project supported by the Hebei Key and Research Program, China (No. 19255901D)
ORCID: Wei-min HOU, https://orcid.org/0000-0003-0956-7057; Qing-shan TANG, https://orcid.org/0000-0002-8797-7732

There are two main working modes in SWIPT systems, i.e., time-splitting (TS) and power-splitting (PS) modes (Zhang R and Ho, 2013; Zhou et al., 2013; Shi et al., 2014). In the TS scheme, the time is divided into two time slots, and the system is switched between information signal transmission and energy-harvesting in different time slots. However, this TS mode typically extends the total delivery time, resulting in more delay at the users. In contrast, in the PS scheme, the system carries out information signal transmission and energy-harvesting simultaneously, where a fraction of the received signal energy at the users is used for information decoding and the other part is used for energy-harvesting. Although the signal-to-noise ratio (SNR) at the users for information decoding decreases under the PS scheme due to PS, the resulting delay for users can be much smaller than the one in the TS case.

In wireless communication networks, given the open access of RF signals, the security issue should be considered. Bloch et al. (2008) first proposed a physical layer design for security, where secure transmission can be guaranteed if the channel state between the source and the legitimate receiver is better than that over the wiretap channel. There are some typical studies on physical layer security analysis based on the work of Bloch et al. (2008) (Zou et al., 2015; Zhao et al., 2016, 2017, 2019a, 2019b; Liu et al., 2017). Because multi-antenna systems have more spatial diversity and higher transmission rates (Tian and Chen, 2019), multi-antenna techniques for physical layer security have been widely investigated and well outlined in Chen et al. (2017) and Qi et al. (2020).

Unfortunately, SWIPT systems have an eavesdropper-attack problem, especially when the source needs to transmit information signals and energy to different users (Pan et al., 2015, 2016b, 2017a, 2017b; Wang et al., 2019). Pan et al. (2015, 2016b, 2017a) analyzed the secrecy outage performance in SWIPT systems, where the source transmitted information signals to a user (legitimate receiver), and another user (eavesdropper) harvested energy from the transmitted signal for the legitimate receiver and decoded the delivered information. Pan et al. (2017b) studied the secrecy outage performance of a hybrid visible light and RF communication system, in which light energy harvesting is enabled, considering the randomness of the terminals. In Wang et al. (2019), the secrecy outage performance in TS SWIPT systems was investigated over generalized-K fading channels. However, Pan et al. (2015, 2016b, 2017a, 2017b) and Wang et al. (2019) did not consider the structure of the transmitted signals for the legitimate receiver. In fact, by designing the signal structure, a better secrecy outage performance can be achieved (Yang et al., 2015; Zhang X et al., 2015; Deng et al., 2016; Zhang M et al., 2016; El Shafie et al., 2017). However, most of studies on artificial noise focus on the optimization aspect for the secrecy outage probability (SOP) or secrecy capacity (Khandaker et al., 2019), and there are few studies on performance analysis, because of the complexity of the SNR distribution at the eavesdropper.

In this study, the secrecy outage performance of an SWIPT system is analyzed, by designing artificial noise for the eavesdropper in the transmitted signals. The main contributions are outlined as follows:

1. A simple closed-form expression for the SOP is derived using the Gauss-Laguerre quadrature (GLQ) method, where a few summation terms in GLQ can make a very tight approximation to the exact SOP. The truncated error in the GLQ will almost vanish when the number of summation terms is sufficiently large.

2. The asymptotic analysis for the SOP in the high SNR region is performed to show the secrecy diversity order and secrecy array gain in this SWIPT system, and to simplify the expression for the SOP.

3. In the low variance region of the signal-to-interference-plus-noise ratio (SINR) at the eavesdropper, a robust approximation for the SOP proposed in Holtzman (1992), Pan et al. (2016a), and Zhao et al. (2019c) is presented. The numerical results show that this robust approximation becomes tight when the variance of the SINR at the eavesdropper is sufficiently small.

2 System model

As shown in Fig. 1, a source equipped with L ($L \geq 2$) transmitting antennas communicates with a legitimate receiver equipped with a single antenna, because of the size limitation, denoted by Bob. At the same time, a single antenna user (eavesdropper), denoted by Eve, is harvesting energy from the transmitted signals for Bob and wants to overhear the

information delivered by the source to Bob under the PS scheme.

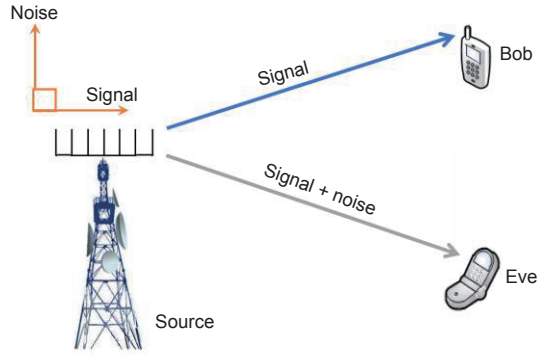

Fig. 1 A secure artificial-noise-aided SWIPT system

The transmitted signal $\boldsymbol{x} \in \mathbb{C}^L$ ($\mathbb{C}$ denotes the whole complex number set) at the source with L transmitting antennas in the equal power allocation case (i.e., the transmit power at each transmit antenna is identical) is

$$\boldsymbol{x} = \sqrt{\alpha \frac{P_{\mathrm{s}}}{L}} \boldsymbol{p} s + \sqrt{(1-\alpha)\frac{P_{\mathrm{s}}}{L}} \boldsymbol{p}^{\perp} z, \tag{1}$$

where $s \in \mathbb{C}$ with zero mean and unit power is the information symbol picked from a Gaussian codebook, $z \in \mathbb{C}$ following the complex standard normal distribution (i.e., zero mean and unit variance) is the artificial noise, $\alpha \in (0,1)$ is the power allocation factor for information symbol and artificial noise, P_{s} is the total transmit power at the source, $\boldsymbol{p} \in \mathbb{C}^L$ denotes the normalized precode vector determined by the instantaneous channel state vector ($\boldsymbol{h}_{\mathrm{B}}$) between the source and Bob, and $\boldsymbol{p}^{\perp} \in \mathbb{C}^L$ is the orthonormal vector of the linear space spanned by $\boldsymbol{p}$. Specifically, $\boldsymbol{p}$ is given by

$$\boldsymbol{p} = \left(\frac{\boldsymbol{h}_{\mathrm{B}}^{\mathrm{H}}}{\|\boldsymbol{h}_{\mathrm{B}}\|} \right)^{\mathrm{T}}, \tag{2}$$

where $||\cdot||$ denotes the norm-2 operator of a vector, and superscripts "H" and "T" denote the conjugate transpose and non-conjugate transpose of a vector, respectively. Clearly, full channel state information (CSI) between the source and Bob is a precondition for the source to design this precoding scheme. For example, CSI acquisition at the source can be realized by adopting the time division duplex mode (Chen and Jia, 2018). Actually, CSI availability at the source is a common assumption in many existing works, such as the works outlined in Table IV of Chen et al. (2017).

After signal delivery, the signal received at Bob is

$$\begin{aligned} y_{\mathrm{B}} &= \boldsymbol{h}_{\mathrm{B}}^{\mathrm{T}} \boldsymbol{x} + n_{\mathrm{B}} \\ &= \boldsymbol{h}_{\mathrm{B}}^{\mathrm{T}} \left(\sqrt{\alpha \frac{P_{\mathrm{s}}}{L}} \boldsymbol{p} s + \sqrt{(1-\alpha)\frac{P_{\mathrm{s}}}{L}} \boldsymbol{p}^{\perp} z \right) + n_{\mathrm{B}} \\ &= \sqrt{\alpha \frac{P_{\mathrm{s}}}{L}} \|\boldsymbol{h}_{\mathrm{B}}\| s + n_{\mathrm{B}}, \end{aligned} \tag{3}$$

where n_{B} is the Gaussian noise with power N_{B}. The corresponding SNR at Bob is

$$\gamma_{\mathrm{B}} = \frac{\|\boldsymbol{h}_{\mathrm{B}}\|^2 \alpha \frac{P_{\mathrm{s}}}{L}}{N_{\mathrm{B}}}. \tag{4}$$

As the conjugate channel state vector between the source and Eve $(\boldsymbol{h}_{\mathrm{E}}^{\mathrm{H}})^{\mathrm{T}} \in \mathbb{C}^L$ is not orthogonal to $\boldsymbol{p}^{\perp}$, the artificial noise in the transmitted signal from the source cannot be canceled at Eve's side. The signal received at Eve is

$$y_{\mathrm{E}} = \sqrt{\alpha \frac{P_{\mathrm{s}}}{L}} \boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}} \boldsymbol{p} s + \underbrace{\sqrt{(1-\alpha)\frac{P_{\mathrm{s}}}{L}} \boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}} \boldsymbol{p}^{\perp} z}_{\text{artificial noise}} + n_{\mathrm{E}}, \tag{5}$$

where n_{E} denotes the Gaussian noise with power N_{E}. If the PS strategy is adopted at Eve for harvesting energy from the received signals, the signal for information decoding at Eve is given by

$$\begin{aligned} y'_{\mathrm{E}} =& \sqrt{\alpha\beta \frac{P_{\mathrm{s}}}{L}} \boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}} \boldsymbol{p} s + \sqrt{(1-\alpha)\beta \frac{P_{\mathrm{s}}}{L}} \boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}} \boldsymbol{p}^{\perp} z \\ &+ \sqrt{\beta} n_{\mathrm{E}} + z_0, \end{aligned} \tag{6}$$

where z_0 is the PS noise subject to a circularly symmetric complex normal distribution with zero mean and variance N_0, and $\beta \in (0,1)$ denotes the power splitting factor (i.e., a fraction β of the received signal's energy is used for information decoding and the remaining for energy harvesting). The resulting SINR at Eve is given by

$$\gamma_{\mathrm{E}} = \frac{\left|\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}} \boldsymbol{p}\right|^2 \alpha\beta \frac{P_{\mathrm{s}}}{L}}{\left|\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}} \boldsymbol{p}^{\perp}\right|^2 (1-\alpha)\beta \frac{P_{\mathrm{s}}}{L} + \beta N_{\mathrm{E}} + N_0}. \tag{7}$$

In this study, all channels are subject to Rayleigh fading, and any two fading channels are

mutually independent. Furthermore, each element in $\boldsymbol{h}_{\mathrm{B}}$ (or $\boldsymbol{h}_{\mathrm{E}}$) follows an identical and independent distribution. Without loss of generality, we assume that $h_{\mathrm{B},i} \in \boldsymbol{h}_{\mathrm{B}}$ and $h_{\mathrm{E},i} \in \boldsymbol{h}_{\mathrm{E}}$ $(i = 1, 2, \cdots, L)$ follow circularly symmetric complex normal distributions with zero mean and unit variance, i.e., $h_{\mathrm{B},i} \sim \mathcal{CN}(0,1)$ and $h_{\mathrm{E},i} \sim \mathcal{CN}(0,1)$. The distribution of γ_{B} is the Gamma distribution, and the probability density function (PDF) and cumulative distribution function (CDF) of γ_{B} are respectively

$$f_{\gamma_{\mathrm{B}}}(x) = \frac{x^{L-1}}{\Gamma(L)\,\overline{\gamma}_{\mathrm{B}}^{L}} \exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right), \tag{8}$$

$$\begin{aligned} F_{\gamma_{\mathrm{B}}}(x) &= \frac{1}{\Gamma(L)} \Upsilon\left(L, \frac{x}{\overline{\gamma}_{\mathrm{B}}}\right) \\ &\overset{\text{(a)}}{=} 1 - \sum_{k=0}^{L-1} \frac{x^k}{k!\overline{\gamma}_{\mathrm{B}}^{k}} \exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right), \end{aligned} \tag{9}$$

where $\Gamma(\cdot)$ denotes the Gamma function, $\Upsilon(\cdot,\cdot)$ denotes the lower incomplete Gamma function (Gradshteyn and Ryzhik, 2007), $\overline{\gamma}_{\mathrm{B}} = \dfrac{\alpha P_{\mathrm{s}}}{LN_{\mathrm{B}}}$, and (a) follows the positive integer assumption for L.

Let $X = \boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\boldsymbol{p}$ and $Y = \boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\boldsymbol{p}^{\perp}$. It is clear that X and Y still follow complex Gaussian distributions with zero mean and unit variance, because X and Y are summations of L independent and identical complex Gaussian random variables, and $\boldsymbol{p}$ and $\boldsymbol{p}^{\perp}$ are normalized vectors. Furthermore, X and Y are independent, because $\boldsymbol{p}^{\perp}$ is orthogonal to $\boldsymbol{p}$. Mathematically, we have

$$\begin{aligned} \mathbb{E}\left\{XY^{\mathrm{H}}\right\} &= \mathbb{E}\left\{\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\boldsymbol{p}\left(\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\boldsymbol{p}^{\perp}\right)^{\mathrm{H}}\right\} \\ &= \mathbb{E}\left\{\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\boldsymbol{p}\left(\boldsymbol{p}^{\perp}\right)^{\mathrm{H}}\left(\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\right)^{\mathrm{H}}\right\} \\ &\overset{\text{(a)}}{=} \mathbb{E}\left\{\mathrm{tr}\left\{\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\boldsymbol{p}\left(\boldsymbol{p}^{\perp}\right)^{\mathrm{H}}\left(\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\right)^{\mathrm{H}}\right\}\right\} \\ &\overset{\text{(b)}}{=} \mathbb{E}\left\{\mathrm{tr}\left\{\left(\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\right)^{\mathrm{H}}\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\boldsymbol{p}\left(\boldsymbol{p}^{\perp}\right)^{\mathrm{H}}\right\}\right\} \\ &\overset{\text{(c)}}{=} \mathrm{tr}\left\{\underbrace{\mathbb{E}\left\{\left(\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\right)^{\mathrm{H}}\boldsymbol{h}_{\mathrm{E}}^{\mathrm{T}}\right\}}_{=\boldsymbol{I}_L}\boldsymbol{p}\left(\boldsymbol{p}^{\perp}\right)^{\mathrm{H}}\right\} \\ &= \mathrm{tr}\left\{\boldsymbol{p}\left(\boldsymbol{p}^{\perp}\right)^{\mathrm{H}}\right\} \overset{\text{(d)}}{=} \mathrm{tr}\left\{\left(\boldsymbol{p}^{\perp}\right)^{\mathrm{H}}\boldsymbol{p}\right\} \overset{\text{(e)}}{=} 0, \end{aligned} \tag{10}$$

where $\mathbb{E}\{\cdot\}$ denotes the expectation operator, $\mathrm{tr}\{\cdot\}$ denotes the trace of a matrix, $\boldsymbol{I}_L \in \mathbb{C}^{L\times L}$ denotes the unitary matrix, (a) follows $A = \mathrm{tr}\{A\}$ for $A \in \mathbb{C}$, (b) and (d) follow $\mathrm{tr}\{AB\} = \mathrm{tr}\{BA\}$, (c) follows the exchange of the trace operator and expectation operator, and (e) follows orthogonality between $\boldsymbol{p}$ and $\boldsymbol{p}^{\perp}$. As X and Y are two complex Gaussian random variables and the correlation coefficient between X and Y is zero (derived from $\mathbb{E}\left\{XY^{\mathrm{H}}\right\} = 0$), X and Y are independent. The distributions of $|X|^2$ and $|Y|^2$ are clearly exponential distributions with a unit rate, i.e., $|X|^2 \sim \exp(1)$ and $|Y|^2 \sim \exp(1)$.

3 Secrecy outage probability

In this section, a simple and tight approximate closed-form expression for the SOP will be derived based on the GLQ method (Lemma 1).

The secrecy capacity (C_{s}) is defined as (Bloch et al., 2008)

$$C_{\mathrm{s}} = \max\{\log_2(1+\gamma_{\mathrm{B}}) - \log_2(1+\gamma_{\mathrm{E}}), 0\}, \tag{11}$$

where $\log_2(1+\gamma_{\mathrm{B}})$ and $\log_2(1+\gamma_{\mathrm{E}})$ are the instantaneous capacities of the source–Bob link and the source–Eve link, respectively.

Assume that there is no channel state feedback from Eve to the source, i.e., a silent eavesdropping scenario, which is most practical and reasonable for Eve to protect itself from being detected. In this silent eavesdropping case, secure transmission cannot be guaranteed because the source has no choice but to adopt a constant rate of confidential information (C_{th}). Unfortunately, C_{th} may not always be smaller than C_{s} in each channel realization. There is a probability that C_{th} is greater than C_{s}, i.e., the secrecy outage. The SOP is mathematically written as

$$\begin{aligned} &\mathrm{SOP} \\ &= \Pr\left\{\log_2(1+\gamma_{\mathrm{B}}) - \log_2(1+\gamma_{\mathrm{E}}) \le C_{\mathrm{th}}\right\} \\ &= \Pr\left\{\gamma_{\mathrm{B}} \le \lambda\gamma_{\mathrm{E}} + \lambda - 1\right\} \\ &= \int_0^{\infty}\int_0^{\infty} F_{\gamma_{\mathrm{B}}}(\lambda\gamma_{\mathrm{E}} + \lambda - 1) f_X(x) f_Y(y)\mathrm{d}x\mathrm{d}y \\ &= \int_0^{\infty}\int_0^{\infty} F_{\gamma_{\mathrm{B}}}\left(\frac{\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}x}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}y + \beta N_{\mathrm{E}} + N_0} + \lambda - 1\right) \\ &\quad \cdot f_X(x) f_Y(y)\mathrm{d}x\mathrm{d}y, \end{aligned} \tag{12}$$

where $\lambda = 2^{C_{\mathrm{th}}}$, and $f_X(\cdot)$ and $f_Y(\cdot)$ denote the PDF of X and Y, respectively.

Lemma 1 A simple and approximate closed-form expression for the SOP in this artificial-noise-aided SWIPT system can be derived as

$$\mathrm{SOP} \approx 1-\sum_{k=0}^{L-1}\frac{\exp\left(-\dfrac{\lambda-1}{\overline{\gamma}_{\mathrm{B}}}\right)}{k!\overline{\gamma}_{\mathrm{B}}^{k}}\sum_{f=0}^{k}\binom{k}{f}(\lambda-1)^{k-f}\cdot\left(\lambda\alpha\beta\frac{P_{\mathrm{s}}}{L}\right)^{f}\sum_{n=1}^{N}\omega_n f(x_n), \tag{13}$$

where x_n, ω_n, and N are the point, weight, and summation terms of GLQ respectively, and

$$f(x)=\frac{\Gamma(f+1)}{\left[(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}x+\beta N_{\mathrm{E}}+N_0\right]^{f}}\cdot\frac{\left[(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}\overline{\gamma}_{\mathrm{B}}x+\beta N_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}}+N_0\overline{\gamma}_{\mathrm{B}}\right]^{f+1}}{\left[(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}\overline{\gamma}_{\mathrm{B}}x+\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}+\beta N_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}}+N_0\overline{\gamma}_{\mathrm{B}}\right]^{f+1}}. \tag{14}$$

Proof Substituting the CDF of γ_{B} in the SOP expression in Eq. (12) yields Eq. (15), which is at the bottom of this page, where the integral with respect to x can be solved as Eq. (16). The double integral in the SOP expression after the second equal sign in Eq. (15) is defined as $\mathcal{I}$, which can be simplified as

$$\mathcal{I}=\int_0^{\infty}\frac{\Gamma(f+1)\exp(-y)}{\left[(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}y+\beta N_{\mathrm{E}}+N_0\right]^{f}}\cdot\frac{\left[(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}\overline{\gamma}_{\mathrm{B}}y+\beta N_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}}+N_0\overline{\gamma}_{\mathrm{B}}\right]^{f+1}}{\left[(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}\overline{\gamma}_{\mathrm{B}}y+\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}+\beta N_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}}+N_0\overline{\gamma}_{\mathrm{B}}\right]^{f+1}}\mathrm{d}y. \tag{17}$$

It is difficult to derive a concise and exact closed-form expression for $\mathcal{I}$. Thus, we turn to the GLQ method to obtain an approximate expression of $\mathcal{I}$ for

$$\begin{aligned}\mathrm{SOP}&=1-\sum_{k=0}^{L-1}\frac{\exp\left(-\dfrac{\lambda-1}{\overline{\gamma}_{\mathrm{B}}}\right)}{k!\overline{\gamma}_{\mathrm{B}}^{k}}\int_0^{\infty}\int_0^{\infty}\left(\frac{\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}x}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}y+\beta N_{\mathrm{E}}+N_0}+\lambda-1\right)^{k}\\&\quad\cdot\exp\left(-\frac{\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}x}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}\overline{\gamma}_{\mathrm{B}}y+\beta N_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}}+N_0\overline{\gamma}_{\mathrm{B}}}\right)f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y\\&=1-\sum_{k=0}^{L-1}\frac{\exp\left(-\dfrac{\lambda-1}{\overline{\gamma}_{\mathrm{B}}}\right)}{k!\overline{\gamma}_{\mathrm{B}}^{k}}\sum_{f=0}^{k}\binom{k}{f}(\lambda-1)^{k-f}\left(\lambda\alpha\beta\frac{P_{\mathrm{s}}}{L}\right)^{f}\int_0^{\infty}\frac{1}{\left[(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}y+\beta N_{\mathrm{E}}+N_0\right]^{f}}\\&\quad\cdot\int_0^{\infty}x^{f}\exp\left(-\frac{\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}x}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}\overline{\gamma}_{\mathrm{B}}y+\beta N_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}}+N_0\overline{\gamma}_{\mathrm{B}}}\right)f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y.\end{aligned} \tag{15}$$

$$\int_0^{\infty}x^{f}\exp\left(-\frac{\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}x}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}\overline{\gamma}_{\mathrm{B}}y+\beta N_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}}+N_0\overline{\gamma}_{\mathrm{B}}}-x\right)\mathrm{d}x=\frac{\Gamma(f+1)}{\left(\dfrac{\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}\overline{\gamma}_{\mathrm{B}}y+\beta N_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}}+N_0\overline{\gamma}_{\mathrm{B}}}+1\right)^{f+1}}. \tag{16}$$

analytical purpose. This is given by

$$\mathcal{I} \approx \sum_{n=1}^{N} \omega_n f(x_n). \tag{18}$$

Finally, a simple approximation for the SOP is derived as Eq. (13), by substituting Eq. (18) into Eq. (15).

Remark 1 Although the closed-form expression in Lemma 1 is complicated, Lemma 1 provides us with a baseline to calculate the SOP with an arbitrarily high accuracy by summing sufficient terms in the GLQ. Generally speaking, we can obtain a high accuracy result by summing several terms in the GLQ (see numerical results in Figs. 2–5).

4 Asymptotic analysis

In this section, the exact closed-form expression for the asymptotic SOP (ASOP) will be derived when the average SNR at Bob is sufficiently large and the average SNR at Eve remains finite, where the secrecy diversity order and secrecy array gain are presented (Lemma 2).

Lemma 2 The closed-form expression for the ASOP valid in the high SNR region of the source–Bob link is given by

$$\mathrm{SOP} \overset{\overline{\gamma}_{\mathrm{B}}\to\infty}{\approx} \left(G_{\mathrm{a}}\overline{\gamma}_{\mathrm{B}}\right)^{-L} + o\left(\overline{\gamma}_{\mathrm{B}}^{-L-1}\right), \tag{19}$$

where $o(\cdot)$ denotes the higher-order term, L is the secrecy diversity order, and G_{a} denotes the secrecy array gain, given by

$$G_{\mathrm{a}} = \left[\sum_{j=0}^{L}\binom{L}{j}\frac{(\lambda-1)^{L-j}\lambda^j\alpha^j}{\Gamma(L+1)}\frac{\Gamma(j+1)}{(1-\alpha)^j}\right.$$
$$\left.\cdot\exp\left(\frac{\beta N_{\mathrm{E}}+N_0}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}}\right)\Gamma\left(1-j,\frac{\beta N_{\mathrm{E}}+N_0}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}}\right)\right]^{-1/L}, \tag{20}$$

where $\Gamma(\cdot,\cdot)$ denotes the upper incomplete Gamma function (Gradshteyn and Ryzhik, 2007).

Proof When $\overline{\gamma}_{\mathrm{B}}\to\infty$, using $\Upsilon(L,x)\overset{x\to0}{\simeq}\dfrac{x^L}{L}$, the CDF of γ_{B} can be approximated by

$$F_{\gamma_{\mathrm{B}}}(x) \simeq \frac{1}{\Gamma(L+1)}\frac{x^L}{\overline{\gamma}_{\mathrm{B}}^{L}}. \tag{21}$$

Using this asymptotic CDF of $\overline{\gamma}_{\mathrm{B}}$ in Eq. (21), the ASOP can be written as Eq. (22) at the bottom of this page.

Substituting PDFs of X and Y into ASOP and using some mathematical manipulations, we can finally derive the closed-form expression for the ASOP in Eq. (19).

Remark 2 From the asymptotic analysis for the SOP derived in Lemma 2, we can easily see that the SOP with respect to $\overline{\gamma}_{\mathrm{B}}$ can be approximated by a linear function whose slope and intercept of the horizontal axis are L and $L\log G_{\mathrm{a}}$, respectively, in the log-scale (i.e., dB scale in $\overline{\gamma}_{\mathrm{B}}$).

Remark 3 Lemma 2 also shows that when $\overline{\gamma}_{\mathrm{B}}$ is sufficiently large, the SOP with a larger L will be always better than the one with a smaller L, although the transmitting power at each transmitting antenna decreases as L increases. This is because a larger L means a higher secrecy diversity order (the slope of SOP in the log-scale of $\overline{\gamma}_{\mathrm{B}}$) because of more spatial diversity.

5 Robust approximation

In this section, a robust approximation for the SOP will be derived based on the works of Holtzman (1992), Pan et al. (2016a), and Zhao et al. (2019c), when the variance of the SINR at Eve is sufficiently small.

Lemma 3 When the variance of γ_{E} is not too large, we can adopt the robust approximation for the SOP,

$$\mathrm{SOP} \simeq \frac{\overline{\gamma}_{\mathrm{B}}^{-L}}{\Gamma(L+1)}\int_0^\infty\int_0^\infty\left(\frac{\lambda\alpha\beta\dfrac{P_{\mathrm{s}}}{L}x}{(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}y+\beta N_{\mathrm{E}}+N_0}+\lambda-1\right)^L f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y$$
$$= \frac{\overline{\gamma}_{\mathrm{B}}^{-L}}{\Gamma(L+1)}\sum_{j=0}^{L}\binom{L}{j}(\lambda-1)^{L-j}\left(\lambda\alpha\beta\frac{P_{\mathrm{s}}}{L}\right)^j\int_0^\infty\int_0^\infty\frac{x^j}{\left[(1-\alpha)\beta\dfrac{P_{\mathrm{s}}}{L}y+\beta N_{\mathrm{E}}+N_0\right]^j}f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y. \tag{22}$$

given by

$$\mathrm{SOP} \approx F_{\gamma_\mathrm{B}}\left(\lambda\overline{\gamma}_\mathrm{E}+\lambda-1\right)+\frac{\sigma_\mathrm{E}^2}{2}\frac{\partial^2 F_{\gamma_\mathrm{B}}\left(\lambda\overline{\gamma}_\mathrm{E}+\lambda-1\right)}{\partial\overline{\gamma}_\mathrm{E}^2}, \tag{23}$$

where $\sigma_\mathrm{E}^2=\mathbb{E}\{\gamma_\mathrm{E}^2\}-\mathbb{E}^2\{\gamma_\mathrm{E}\}$ denotes the variance of γ_E, the n^{th} $(n=1,2,\cdots)$ moment of γ_E (i.e., $\mathbb{E}\{\gamma_\mathrm{E}^n\}$) is shown in Eq. (27), and the second derivative of $F_{\gamma_\mathrm{B}}\left(\lambda\overline{\gamma}_\mathrm{E}+\lambda-1\right)$ with respect to $\overline{\gamma}_\mathrm{E}$ is given by

$$\begin{aligned}&\frac{\partial^2 F_{\gamma_\mathrm{B}}\left(\lambda\overline{\gamma}_\mathrm{E}+\lambda-1\right)}{\partial\overline{\gamma}_\mathrm{E}^2}\\&=\frac{\partial^2}{\partial\overline{\gamma}_\mathrm{E}^2}\left[1-\frac{\Gamma\left(L,\lambda\overline{\gamma}_\mathrm{E}+\lambda-1\right)}{\Gamma\left(L\right)}\right]\\&=\frac{-1}{\Gamma\left(L\right)}\lambda^2\exp\left[-\left(\lambda\overline{\gamma}_\mathrm{E}+\lambda-1\right)\right]\left(\lambda\overline{\gamma}_\mathrm{E}+\lambda-1\right)^{L-2}\\&\quad\cdot\left(\lambda\overline{\gamma}_\mathrm{E}+\lambda-L\right).\end{aligned} \tag{24}$$

Proof From the SOP definition in Eq. (12), we can easily observe that

$$\begin{aligned}\mathrm{SOP}&=\int_0^\infty F_{\gamma_\mathrm{B}}\left(\lambda\gamma_\mathrm{E}+\lambda-1\right)f_{\gamma_\mathrm{E}}\left(\gamma_\mathrm{E}\right)\mathrm{d}\gamma_\mathrm{E}\\&=\mathbb{E}_{\gamma_\mathrm{E}}\left\{F_{\gamma_\mathrm{B}}\left(\lambda\gamma_\mathrm{E}+\lambda-1\right)\right\},\end{aligned} \tag{25}$$

where $f_{\gamma_\mathrm{E}}(\cdot)$ denotes the PDF of γ_E.

From Holtzman (1992), we know that if $P(X)$ is a real-valued function with respect to X, where X is a random variable with mean μ_X and variance σ_X^2, the expectation of $P(X)$ can be robustly approximated by

$$\mathbb{E}\left\{P\left(X\right)\right\}\approx P\left(\mu_X\right)+\frac{\sigma_X^2}{2}\frac{\partial^2 P\left(\mu_X\right)}{\partial\mu_X^2}. \tag{26}$$

Note that this robust approximation proposed in Holtzman (1992) is tight when σ_X^2 is sufficiently small.

In view of the robust approximation in Holtzman (1992), Pan et al. (2016a), and Zhao et al. (2019c), the SOP can be robustly approximated as Eq. (23).

For the derivation of σ_E^2, we can alternatively derive the n^{th} moment of γ_E. Although it is difficult to derive the PDF of γ_E, the n^{th} moment of γ_E can be easily derived by

$$\begin{aligned}\mathbb{E}\left\{\gamma_\mathrm{E}^n\right\}&=\mathbb{E}\left\{\frac{\left(\alpha\beta\dfrac{P_\mathrm{s}}{L}\right)^n x^n}{\left[\left(1-\alpha\right)\beta\dfrac{P_\mathrm{s}}{L}y+\beta N_\mathrm{E}+N_0\right]^n}\right\}\\&=\int_0^\infty\int_0^\infty\frac{\left(\alpha\beta\dfrac{P_\mathrm{s}}{L}\right)^n x^n f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y}{\left[\left(1-\alpha\right)\beta\dfrac{P_\mathrm{s}}{L}y+\beta N_\mathrm{E}+N_0\right]^n}\\&=\left(\alpha\beta\frac{P_\mathrm{s}}{L}\right)^n\int_0^\infty\frac{\exp\left(-y\right)\mathrm{d}y}{\left[\left(1-\alpha\right)\beta\dfrac{P_\mathrm{s}}{L}y+\beta N_\mathrm{E}+N_0\right]^n}\\&\quad\cdot\int_0^\infty x^n\exp\left(-x\right)\mathrm{d}x\\&\overset{\text{(a)}}{=}\frac{\alpha^n}{\left(1-\alpha\right)^n}\exp\left(\frac{\beta N_\mathrm{E}+N_0}{\left(1-\alpha\right)\beta\dfrac{P_\mathrm{s}}{L}}\right)\Gamma\left(n+1\right)\\&\quad\cdot\Gamma\left(1-n,\frac{\beta N_\mathrm{E}+N_0}{\left(1-\alpha\right)\beta\dfrac{P_\mathrm{s}}{L}}\right),\end{aligned} \tag{27}$$

where (a) follows Eqs. (3.381.4) and (3.462.15) in Gradshteyn and Ryzhik (2007).

Remark 4 Actually, we consider an eavesdropper far away from the transmitter in Lemma 3 such that the variance of the eavesdropping SINR is small. This eavesdropping scenario is reasonable and practical, indicating the wide application of Lemma 3 to robustly approximate the SOP.

6 Numerical results

In this section, some selected Monte-Carlo numerical results will be presented, as well as the analytical results derived in this study, to validate the accuracy of our derived expressions for the SOP.

To simplify the parameter settings in the numerical results, $C_\mathrm{th}=1$ and $P_\mathrm{s}=10$ dB are assumed. Furthermore, $N=15$ is adopted in the GLQ approximation, and 10^7 channel state realizations are generated. In the following simulation results, $\overline{\gamma}=\dfrac{P_\mathrm{s}}{N_\mathrm{B}}$ is defined.

Fig. 2 plots the SOP versus $\overline{\gamma}$ with different numbers of transmitting antennas. It is clear that the SOP is improved by increasing the number of transmitting antennas, because of more spatial diversity. This implies that although the transmitted

power at each transmitting antenna decreases with increasing the number of transmitting antennas, the advantage of spatial diversity dominates the secrecy outage performance. From the asymptotic analysis for the SOP, we can also know that the slope of SOP with a larger L is steeper, resulting in a better secrecy outage performance. Note that the SOP is a decreasing function with respect to $\overline{\gamma}$. This is because a larger $\overline{\gamma}$ means a better average channel state between the source and Bob.

In Fig. 3, we compare the secrecy outage performance for some selected values of α and β. We can easily see that the SOP decreases as β decreases, because less power is used for information decoding at Eve, leading to a lower SINR at Eve. The decrease in α from 0.5 to 0.1 results in a worse SOP, which may not always be true. This is because although the decrease in α means more power for artificial noise, resulting in the decrease in SINRs at Eve, a smaller α also means less power for signal symbols, also leading to a lower SNR at Bob. To investigate the impact of α, we present the SOP versus α changing from 0 to 1 in Fig. 4. From Fig. 4, we can observe that there is a unique minimum point of α, at which the SOP arrives to a floor; i.e., the SOP is a convex function with respect to α. There is an increasing trend in SOP with decreasing N_{E}, because a smaller N_{E} means an improved ratio of $P_{\mathrm{s}}/N_{\mathrm{E}}$ at Eve. Actually, the impact of N_{E} can also reflect the average channel state between the source and Eve.

To present the tight bound for the SOP in robust approximation, we plot the SOP with different values of N_0 in Fig. 5, where the SOP becomes better as N_0 increases, because of more power splitting noise during information decoding at Eve. As a larger N_0 means a smaller average SINR at Eve (equivalent to a smaller variance of SINR at Eve), the matching performance of robust approximation for the SOP becomes better.

From Figs. 2–5, it is clear that the gap between the GLQ approximation for the SOP and the numerical SOP (exact SOP) almost vanishes when the number of summation terms in GLQ is just 15.

7 Conclusions

In this paper, a closed-form expression for the SOP in an artificial-noise-aided SWIPT system has

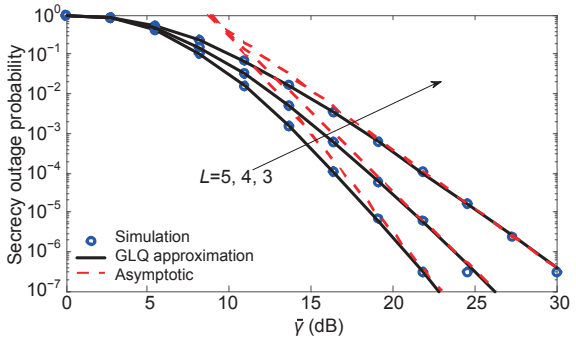

Fig. 2 SOP versus $\overline{\gamma}$ for $N_0 = N_{\mathrm{E}} = 0$ dB and $\alpha = \beta = 0.5$

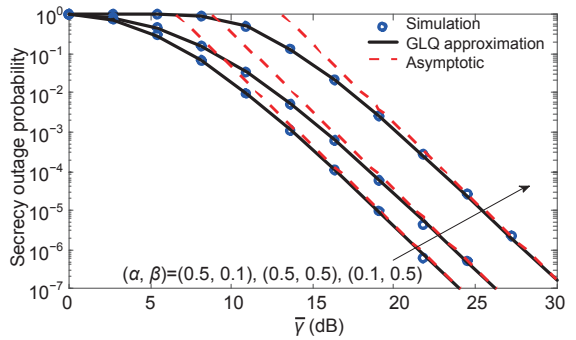

Fig. 3 SOP versus $\overline{\gamma}$ for $N_0 = N_{\mathrm{E}} = 0$ dB and $L = 4$

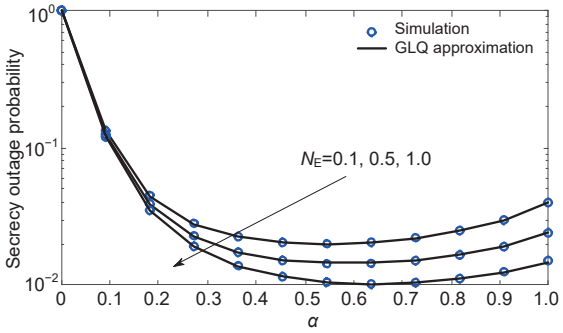

Fig. 4 SOP versus α for $\overline{\gamma} = 15$ dB, $N_0 = 0$ dB, $L = 3$, and $\beta = 0.8$

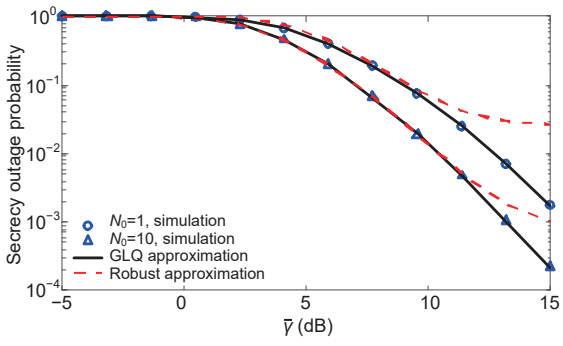

Fig. 5 SOP versus $\overline{\gamma}$ for $N_{\mathrm{E}} = 0$ dB, $L = 4$, and $\alpha = \beta = 0.5$

been derived via the GLQ approximation method. To obtain the secrecy diversity order and secrecy array gain of this system, asymptotic analysis for the SOP has also been performed, where the derived ASOP was almost identical to the exact SOP in the high SNR region of the source–Bob link. Building on the works of Holtzman (1992), Pan et al. (2016a), and Zhao et al. (2019c), we also derived a robust approximation for the SOP when the variance of SINRs at Eve was not large. Finally, Monte-Carlo simulations have been presented to demonstrate the correctness of the derived closed-form expressions, as well as presenting the impacts of some parameters of interest on the SOP.

Contributors

Wei-min HOU designed the research and drafted the manuscript. Qing-shan TANG helped organize the manuscript. Wei-min HOU and Qing-shan TANG revised and finalized the paper.

Compliance with ethics guidelines

Wei-min HOU and Qing-shan TANG declare that they have no conflict of interest.

References

Bloch M, Barros J, Rodrigues MRD, et al., 2008. Wireless information-theoretic security. *IEEE Trans Inform Theory*, 54(6):2515-2534. https://doi.org/10.1109/TIT.2008.921908

Chen XM, Jia RD, 2018. Exploiting rateless coding for massive access. *IEEE Trans Veh Technol*, 67(11):11253-11257. https://doi.org/10.1109/TVT.2018.2866279

Chen XM, Ng DWK, Gerstacker WH, et al., 2017. A survey on multiple-antenna techniques for physical layer security. *IEEE Commun Surv Tutor*, 19(2):1027-1053. https://doi.org/10.1109/COMST.2016.2633387

Deng YS, Wang LF, Zaidi SAR, et al., 2016. Artificial-noise aided secure transmission in large scale spectrum sharing networks. *IEEE Trans Commun*, 64(5):2116-2129. https://doi.org/10.1109/TCOMM.2016.2544300

El Shafie A, Tourki K, Al-Dhahir N, 2017. An artificial-noise-aided hybrid TS/PS scheme for OFDM-based SWIPT systems. *IEEE Commun Lett*, 21(3):632-635. https://doi.org/10.1109/LCOMM.2016.2642105

Gradshteyn IS, Ryzhik IM, 2007. Table of Integrals, Series, and Products (7^{th} Ed.). Academic Press, Salt Lake City, USA.

Holtzman JM, 1992. A simple, accurate method to calculate spread-spectrum multiple-access error probabilities. *IEEE Trans Commun*, 40(3):461-464. https://doi.org/10.1109/26.135712

Khandaker MRA, Masouros C, Wong KK, et al., 2019. Secure SWIPT by exploiting constructive interference and artificial noise. *IEEE Trans Commun*, 67(2):1326-1340. https://doi.org/10.1109/TCOMM.2018.2874658

Liu YW, Qin ZJ, Elkashlan M, et al., 2017. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. *IEEE Trans Wirel Commun*, 16(3):1656-1672. https://doi.org/10.1109/TWC.2017.2650987

Pan GF, Tang CQ, Li TT, et al., 2015. Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems. *IEEE Trans Commun*, 63(9):3423-3433. https://doi.org/10.1109/TCOMM.2015.2458317

Pan GF, Tang CQ, Zhang X, et al., 2016a. Physical-layer security over non-small-scale fading channels. *IEEE Trans Veh Technol*, 65(3):1326-1339. https://doi.org/10.1109/TVT.2015.2412140

Pan GF, Lei HJ, Deng YS, et al., 2016b. On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI. *IEEE Trans Commun*, 64(9):3831-3843. https://doi.org/10.1109/TCOMM.2016.2573822

Pan GF, Lei HJ, Yuan Y, et al., 2017a. Performance analysis and optimization for SWIPT wireless sensor networks. *IEEE Trans Commun*, 65(5):2291-2302. https://doi.org/10.1109/TCOMM.2017.2676815

Pan GF, Ye J, Ding ZG, 2017b. Secure hybrid VLC-RF systems with light energy harvesting. *IEEE Trans Commun*, 65(10):4348-4359. https://doi.org/10.1109/TCOMM.2017.2709314

Qi Q, Chen XM, Zhong CJ, et al., 2020. Physical layer security for massive access in cellular Internet of Things. *Sci China Inform Sci*, 63(2):121301. https://doi.org/10.1007/s11432-019-2650-4

Shi QJ, Liu L, Xu WQ, et al., 2014. Joint transmit beamforming and receive power splitting for MISO SWIPT systems. *IEEE Trans Wirel Commun*, 13(6):3269-3280. https://doi.org/10.1109/TWC.2014.041714.131688

Sudevalayam S, Kulkarni P, 2011. Energy harvesting sensor nodes: survey and implications. *IEEE Commun Surv Tutor*, 13(3):443-461. https://doi.org/10.1109/SURV.2011.060710.00094

Tian FY, Chen XM, 2019. Multiple-antenna techniques in nonorthogonal multiple access: a review. *Front Inform Technol Electron Eng*, 20(12):1665-1697. https://doi.org/10.1631/FITEE.1900405

Wang ZJ, Zhao H, Wang S, et al., 2019. Secrecy analysis in SWIPT systems over generalized-K fading channels. *IEEE Commun Lett*, 23(5):834-837. https://doi.org/10.1109/LCOMM.2019.2907490

Yang N, Yan SH, Yuan JH, et al., 2015. Artificial noise: transmission optimization in multi-input single-output wiretap channels. *IEEE Trans Commun*, 63(5):1771-1783. https://doi.org/10.1109/TCOMM.2015.2419634

Zhang M, Liu Y, Zhang R, 2016. Artificial noise aided secrecy information and power transfer in OFDMA systems. *IEEE Trans Wirel Commun*, 15(4):3085-3096. https://doi.org/10.1109/TWC.2016.2516528

Zhang R, Ho CK, 2013. MIMO broadcasting for simultaneous wireless information and power transfer. *IEEE Trans Wirel Commun*, 12(5):1989-2001. https://doi.org/10.1109/TWC.2013.031813.120224

Zhang X, McKay MR, Zhou XY, et al., 2015. Artificial-noise-aided secure multi-antenna transmission with limited feedback. *IEEE Trans Wirel Commun*, 14(5):2742-2754. https://doi.org/10.1109/TWC.2015.2391261

Zhao H, Tan YY, Pan GF, et al., 2016. Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks. *IEEE Trans Veh Technol*, 65(12):10236-10242. https://doi.org/10.1109/TVT.2016.2529704

Zhao H, Tan YY, Pan GF, et al., 2017. Ergodic secrecy capacity of MRC/SC in single-input multiple-output wiretap systems with imperfect channel state information. *Front Inform Technol Electron Eng*, 18(4):578-590. https://doi.org/10.1631/FITEE.1500430

Zhao H, Liu ZD, Yang L, et al., 2019a. Secrecy analysis in DF relay over generalized-K fading channels. *IEEE Trans Commun*, 67(10):7168-7182. https://doi.org/10.1109/TCOMM.2019.2926719

Zhao H, Zhang JY, Yang L, et al., 2019b. Secure mmWave communications in cognitive radio networks. *IEEE Wirel Commun Lett*, 8(4):1171-1174. https://doi.org/10.1109/LWC.2019.2910530

Zhao H, Liu YW, Sultan-Salem A, et al., 2019c. A simple evaluation for the secrecy outage probability over generalized-K fading channels. *IEEE Commun Lett*, 23(9):1479-1483. https://doi.org/10.1109/LCOMM.2019.2926360

Zhou X, Zhang R, Ho CK, 2013. Wireless information and power transfer: architecture design and rate-energy tradeoff. *IEEE Trans Commun*, 61(11):4754-4767. https://doi.org/10.1109/TCOMM.2013.13.120855

Zou YL, Champagne B, Zhu WP, et al., 2015. Relay-selection improves the security-reliability trade-off in cognitive radio systems. *IEEE Trans Commun*, 63(1):215-228. https://doi.org/10.1109/TCOMM.2014.2377239