Impact of Channel Estimation-and-Artificial Noise Cancellation Imperfection on Artificial Noise-Aided Energy Harvesting Overlay Networks

Khuong Ho-Van (hvkhuong@hcmut.edu.vn)
Ho Chi Minh City University of Technology https://orcid.org/0000-0001-7044-4131
Thiem Do-Dac
Thu Dau Mot University

Research Article

Keywords: Overlay, secrecy outage probability, energy harvesting, channel estimation imperfection, artificial noise cancellation.

Posted Date: February 25th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-176103/v1

Version of Record: A version of this preprint was published at Telecommunication Systems on July 5th, 2021. See the published version at https://doi.org/10.1007/s11235-021-00808-8.

Impact of Channel Estimation-and-Artificial Noise Cancellation Imperfection on Artificial Noise-Aided Energy Harvesting Overlay Networks

K. Ho-Van and T. Do-Dac

Abstract

EHONs (Energy Harvesting Overlay Networks) satisfy stringent design requirements such as high energy-and-spectrum utilization efficiencies. However, due to open access nature of these networks, eavesdroppers can emulate cognitive radios to wire-tap legitimate information, inducing information security to become a great concern. In order to protect legitimate information against eavesdroppers, this paper generates artificial noise transmitted simultaneously with legitimate information to interfere eavesdroppers. Nonetheless, artificial noise cannot be perfectly suppressed at legitimate receivers as for its primary purpose of interfering only eavesdroppers. Moreover, channel information used for signal detection is hardly estimated at receivers with absolute accuracy. As such, to quickly evaluate impact of channel estimation-and-artificial noise cancellation imperfection on secrecy performance of secondary/primary communication in ANaEHONs (Artificial Noise-aided EHONs), this paper firstly proposes precise closed-form formulas of primary/secondary SOP (Secrecy Outage Probability). Then, computer simulations are provided to corroborate these formulas. Finally, various results are illustrated to shed insights into secrecy performance of ANaEHON with key system parameters from which optimum parameters are recognized. Notably, secondary/primary communication can be secured at different levels by flexibly adjusting various parameters of the proposed system model.

Index Terms

Overlay; secrecy outage probability; energy harvesting; channel estimation imperfection; artificial noise cancellation.

K. Ho-Van and T. Do-Dac are with HCMUT, VN (e-mail: hvkhuong@hcmut.edu.vn); Thiem Do-Dac is also with TDMU, VN (dodacthiem@gmail.com).

I. INTRODUCTION

Advanced wireless networks such as 5G/6G (Fifth/Sixth Generation) open a door to a large number of emerging wireless applications but impose an immense pressure on telecommunications infrastructure which requires advanced technology solutions of high (spectrum utilization, energy, spectral) efficiencies to release it [1]–[3]. Indeed, a key application of 5G networks is IoT (Internet of Things), which is deployed extensively from civilian (e.g., transportation, electricity, healthcare, public safety, ...) to military (e.g., tactical reconnaissance, smart bases, ...) [4]. However, when deploying IoT, an enormous number of concurrently connected terminals consume tremendous amount of energy and hence, it is essential to improve energy efficiency to not only extend the lifetime of terminals but also reduce energy need. Moreover, IoT demands a large bandwidth to allot concurrently a huge number of terminals and thus, in the spectrum shortage-and-scarcity situation as nowadays, solutions of enhancing spectral efficiency should be devised. Similarly to IoT, 5G mobile wireless communications, which serves the growing number of mobile terminals and demands increasingly high data transmission speed, needs efficient energy-and-spectrum utilization solutions to meet its requirements [5].

CRs (Cognitive Radios), which typically operate in overlay, underlay, and interweave modes, can access the licensed frequency band of PUs (Primary Users) without causing any performance degradation for PUs, thus significantly improving spectral efficiency and mitigating spectrum scarcity issue [6]. In the underlay mode, CRs utilize the licensed spectrum but must upper-bound interference caused at PUs. The overlay mode allows concurrent transmission of CRs and PUs but signal reception quality at primary receivers must be remained or enhanced with complicated signal processing techniques. In the meantime, the interweave mode merely leaves blank licensed spectrum for CRs to utilize. While literature has intensively focused on the underlay and interweave modes, few works have studied the overlay one. The overlay mode can trade-off performances between primary and secondary communication better than other modes and hence, it is of a special attention in the current paper.

Energy efficiency of wireless communication can be enhanced by several viable solutions (e.g., network planning, EH (Energy Harvesting), hardware solutions) amongst which, RF (Radio Frequency) energy harvesting neither requires additional energy scavenging equipments (e.g., solar panels, wind turbines) nor depends time-variant energy resources. Such advantages of this energy harvesting solution enable it to be integrated into (5G/6G mobile or IoT) users to supply

energy, extend the life-time of wireless devices, and improve energy efficiency [7]. Relaying communication [8]–[10] or simultaneous wireless information and power transfer [11]–[13] is currently a means to implement this solution.

EHONs can exploit simultaneously advantages of both feasible (cognitive radio and energy harvesting) technologies to meet several standards of advanced wireless networks requiring high energy-and-spectral efficiencies [14]. Nevertheless, that both licensed and unlicensed users in these networks are permitted to utilize the licensed spectrum simultaneously may enable eavesdroppers to emulate legitimate users to steal secret information, seriously warning security issues. To supplement and improve secrecy capability for traditional cryptographic and encryption techniques, PLS (physical layer security) has recently been suggested [15]. Amongst various PLS methods (e.g., opportunistic scheduling, transmit beam-forming, transmit antenna selection, on-off transmission, jamming, relaying), jamming (or generating artificial noise) is of a great concern due to its simple, efficient, and flexible implementation [16]. Therefore, this paper applies artificial noise in EHONs to secure primary/secondary communication.

Most references (e.g., [17]–[21]) assumed artificial noise to be exactly known at legitimate receivers. Accordingly, these receivers completely eliminate its detrimental effect while eavesdroppers suffer severely this effect. Nevertheless, the amount of artificial noise received at legitimate receivers is variable due to uncertainties such as noise and fading. As such, assumption on perfect artificial noise cancellation at these receivers seems unrealistic. Moreover, channel information affects successful probability of signal detection not only at legitimate receivers but also eavesdroppers, eventually impact security capability. Nonetheless, it is certain that any channel estimator has some accuracy degree [22] and hence, it is practical to investigate channel estimation imperfection in ANaEHON. Therefore, this paper evaluates effect of channel estimation-and-artificial noise cancellation imperfection on security performance of PUs/CRs in ANaEHON.

A. Prior works

This paper considers ANaEHON where a primary transmitter-receiver pair cannot communicate with each other directly due to some reasons and a secondary transmitter-receiver pair assists primary communication in reward for their access to primary spectrum. The secondary transmitter harvests RF energy from the primary transmitter and transmits not only its private

signal but also the primary transmitter's signal and artificial noise. Information transmission of the secondary transmitter is wire-tapped by an eavesdropper.

While publications on information security for energy harvesting (interweave/underlay) networks have been blooming, few works have been interested in the overlay mode [18]–[21], [23]–[25]. More specifically, [18] and [19] considered the almost same system model as ours but EHONs are secured by letting the primary receiver jam the eavesdropper and the secondary transmitter helps primary communication by the AF (Amplify-and-Forward) mechanism[1]. In [20], a dedicated jammer was employed to interfere the eavesdropper instead of the primary receiver as [18] and [19]. In addition, [20] differs [18] and [19] in the EH method, the EH-capable terminal, and the assistance mechanism. The former used the EH-capable jammer, which harvests energy based on the time splitting technique [27], and employed the secondary transmitter as a DF (Decode-and-Forward) relay. Meanwhile, the latter used the secondary transmitter as the AF relay and as an energy harvester which is based on the power splitting technique [28]. To further secure primary transmission, [21] proposed to jam the eavesdropper by both the primary receiver and the dedicated jammer. However, security performance of primary/secondary communication in terms of SOP was not analyzed in [18]–[21]. In [23], the transmit antenna selection and the multi-user scheduling were proposed to secure EHONs and the ergodic rate of secondary communication and the SOP of primary communication were derived in closed-form. Nonetheless, different from [18]–[21], the secondary user relays the primary signal and transmits its private signal separately in [23]. This significantly mitigates complexity in analyzing the SOP and hence, making the analysis in [23] tractable.

Although [23] analyzed the ergodic rate of secondary communication and the SOP of primary communication in EHONs, the SU (Secondary User) relays the primary signal and transmits its private signal separately. This requires at least three stages (Stage I: energy harvesting and PU's transmission, Stage II: SU's transmission to PU, Stage III: SU's transmission to SU) to complete a transmission process of both SU and PU, considerably reducing spectral efficiency. Recently, [24] and [25] proposed a two-stage transmission scheme with artificial noise generation in EHONs to improve spectral efficiency and secrecy performance. More specifically, [24] and [25] proposed the secondary transmitter to play dual role as the traditional secondary transmitter

[1]The system model in [18] and [19] was studied in [26]. However, the secondary transmitter was assumed to scavenge energy from the ambient rather than RF signals, considerably simplifying the analysis. Furthermore, [26] did not employ artificial noise. Therefore, references like [26] are not objectives to be surveyed.

operating in the overlay mode (i.e., relay primary message and transmit secondary message) and the jammer by network-coding three (primary, secondary, artificial noise) signals. Moreover, [24] and [25] proposed the SOP analysis.

B. Motivations and Contributions

Imperfect channel estimation and artificial noise cancellation are ineluctable in practical systems and hence, this paper studies their impact on security performance of ANaEHON in [24] and [25]. It contributes the following:

- Propose a novel operation mechanism of the secondary transmitter which enables it to harvest energy from the primary transmitter, decode and forward primary information, and generate a signal combination of primary information, secondary information, and artificial noise. This mechanism is flexible in compromising security performance of primary communication with that of secondary communication and optimizing system design by selecting appropriately the (power splitting, time splitting, power allocation) factors.
- Propose precise closed-form SOP formulas for promptly assessing security performance of secondary/primary communication under channel estimation-and-artificial noise cancellation imperfection. These formulas serve as a key starting point to obtain formulas for other pivotal secrecy performance indicators comprising IP (Intercept Probability), STP (Secrecy Throughput), PSCP (Positive Secrecy Capacity Probability).
- Search optimum pivotal specifications for the best secrecy performance and the best performance trade-off between secondary and primary communication.
- Provide insightful results on security performance of primary/secondary communication in important system parameters.

C. Structure

Part II describes the system model. Next, Part III derives detailedly the SOP of primary/secondary communication. Subsequently, Part IV provides illustrative results and finally, Part V closes the paper.

II. System Model

Figure 1 shows an ANaEHON in which direct communication between a primary transmitter-receiver pair, $PT-PR$, is not of good quality owing to uncertainties (e.g., long distance, severe

TABLE I

SUMMARY OF SYMBOLS

Symbol	Meaning
x_p	Transmit symbol of PT
x_s	Transmit symbol of ST
x_a	Artificial noise
P_p	Transmit power of PT
P_s	Transmit power of ST
n_s	Noise at ST
$\tilde{n}_s$	Noise due to the passband-to-baseband signal conversion at ST
n_e	Noise at E
n_r	Noise at SR
n_p	Noise at PR
h_{ps}	$PT-ST$ channel coefficient
h_{sp}	$ST-PR$ channel coefficient
h_{se}	$ST-E$ channel coefficient
h_{sr}	$ST-SR$ channel coefficient
μ_{ps}	Fading power of $PT-ST$ channel
μ_{sp}	Fading power of $ST-PR$ channel
μ_{se}	Fading power of $ST-E$ channel
μ_{sr}	Fading power of $ST-SR$ channel
y_s	Received signal at ST
y_e	Received signal at E
y_r	Received signal at SR
y_p	Received signal at PR
T	Total transmission time
α	Time splitting factor
λ	Power splitting factor
θ	Power allocation factor for desired signals and artificial noise when ST decodes successfully PT's signal
τ	Power allocation factor for artificial noise and secondary signal as ST decodes incorrectly PT's signal
κ	Power allocation factor for primary and secondary signals
C_t	Transmission rate required by ST
C_0	Required secrecy capacity
γ_s	SNR at ST
γ_e	SINR at E
γ_r	SINR at SR
γ_p	SINR at PR
$\Pr\{X\}$	Probability of the event X
$X\sim\mathcal{CN}(0,m)$	Zero-mean m-variance circular symmetric complex Gaussian random variable
ς	Path-loss exponent
d_{uv}	Distance between a corresponding transmitter-receiver pair
ρ_{uv}	Correlation coefficient between true and estimated channels
χ	Artificial noise residue level

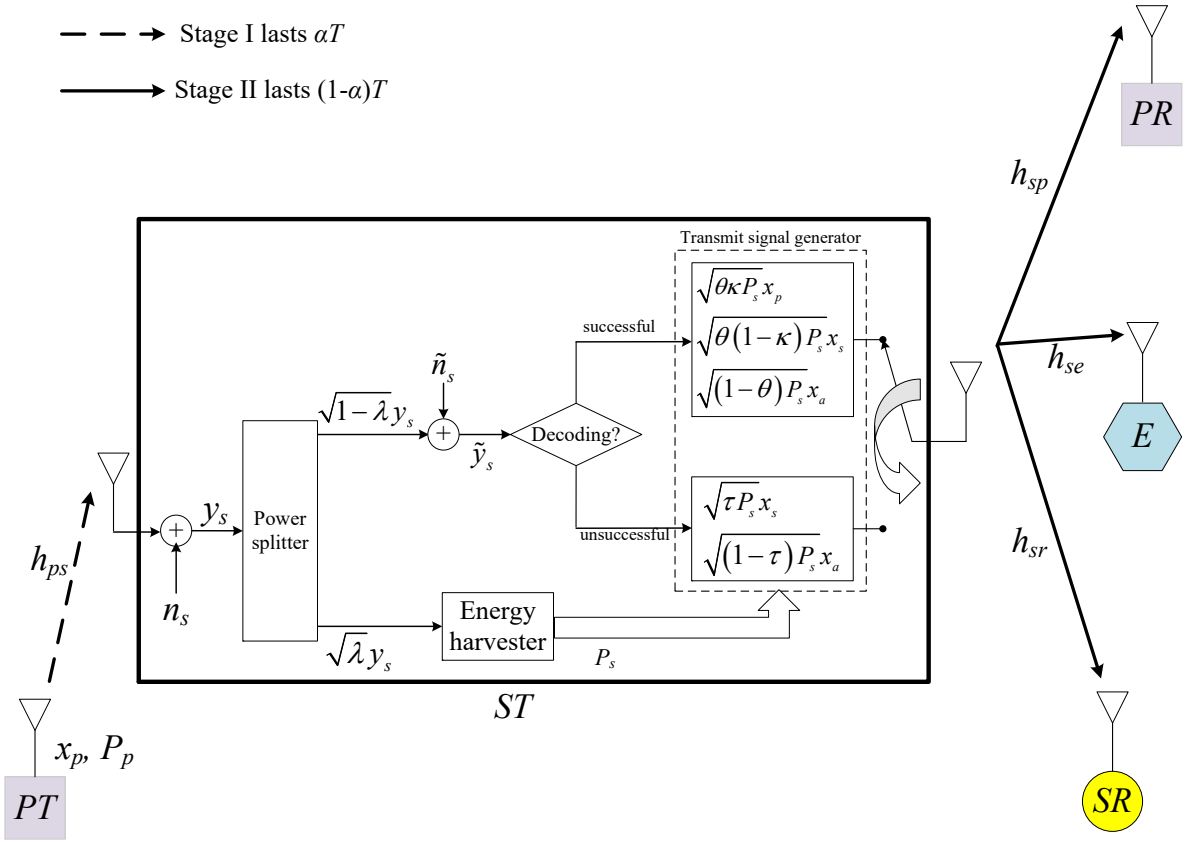

Fig. 1. System model.

fading, ...). Therefore, the secondary transmitter ST, which is in the transmission range of PT, can assist PT in relaying the PT's signal to PR. ST is assumed to be capable of harvesting RF energy from PT and consumes the scavenged energy for its communication operation. Additionally, ST operates in the overlay mechanism where it not only relays the PT's signal to PR but also sends its private signal to the secondary receiver SR. Information transmission of ST is stolen by an eavesdropper E. In order to reduce the wire-tapping capability of E, ST transmits artificial noise together with information signals of PT and ST.

Table I summarizes main notations used throughout this paper. More specifically, as shown in Figure 1, h_{ps}, h_{sp}, h_{se}, and h_{sr} correspondingly signify channel coefficients between PT and ST, ST and PR, ST and E, ST and SR. In the current paper, these channel coefficients are modelled as $h_{ps} \sim \mathcal{CN}(0, \mu_{ps})$, $h_{sp} \sim \mathcal{CN}(0, \mu_{sp})$, $h_{se} \sim \mathcal{CN}(0, \mu_{se})$, and $h_{sr} \sim \mathcal{CN}(0, \mu_{sr})$, respectively. Such a channel model indicates Rayleigh fading. Path-loss can be incorporated into

$\mu_{\mathtt{uv}}$ with $\mathtt{u} \in \{p, s\}$ and $\mathtt{v} \in \{s, p, r, e\}$ as $\mu_{\mathtt{uv}} = d_{\mathtt{uv}}^{-\varsigma}$ in which ς is the path-loss exponent and $d_{\mathtt{uv}}$ is the $\mathtt{u}$-$\mathtt{v}$ distance. Then, the probability density function (PDF) and the cumulative distribution function (CDF) of $|h_{\mathtt{uv}}|^2$ are correspondingly expressed as $f_{|h_{\mathtt{uv}}|^2}(x) = e^{-x/\mu_{\mathtt{uv}}}/\mu_{\mathtt{uv}}$ and $F_{|h_{\mathtt{uv}}|^2}(x) = 1 - e^{-x/\mu_{\mathtt{uv}}}$, where $x \geq 0$.

In Figure 1, the total transmission time T for both PT and ST to complete their information transmission to corresponding receivers is divided into two stages. Stage I with the time of αT with $\alpha \in (0, 1)$ being the time splitting factor is for PT to transmit its unit-power symbol x_p with the transmit power of P_p in order for ST to harvest energy based on the power splitting technique and decode the PT's information. This technique separates the received signal of ST, y_s, into two portions: one portion $\sqrt{\lambda}y_s$ with $\lambda \in (0, 1)$ being the power splitting factor for decoding the PT's information[2] and another portion $\sqrt{1-\lambda}y_s$ for harvesting energy. Dependent on the decoding status[3], ST transmits distinct signals. To be specific, if ST successfully restores the PT's information, it sends a combination of three signals $\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta(1-\kappa)P_s}x_s + \sqrt{(1-\theta)P_s}x_a$ (P_s, θ and κ are the transmit power of ST, the power allocation factor for desired signals and artificial noise as ST decodes correctly the PT's signal and the power allocation factor for primary and secondary signals, respectively): the PT's decoded information x_p, the ST's private information x_s, and the artificial noise x_a. In the case that ST unsuccessfully decodes the PT's information, it transmits a superposition of two signals $\sqrt{\tau P_s}x_s + \sqrt{(1-\tau)P_s}x_a$ (τ is the power allocation factor for desired signal and artificial noise as ST decodes incorrectly the PT's signal): the ST's private information x_s and the artificial noise x_a. Stage II with the time of $(1-\alpha)T$ is for ST to send its signal to SR, PR, and E.

In Stage I, ST receives the following signal

$$y_s = h_{ps}\sqrt{P_p}x_p + n_s, \tag{1}$$

where the receive antenna at ST induces the noise $n_s \sim \mathcal{CN}(0, \sigma_s^2)$.

According to Figure 1, ST scavenges the total energy in Stage I as

$$E_s = \eta\Xi\left\{\left|\sqrt{\lambda}y_s\right|^2\right\}\alpha T = \alpha\eta\lambda\left(P_p\mu_{ps} + \sigma_s^2\right)T, \tag{2}$$

[2]The information decoder assumably consumes negligible energy, which is widely acknowledged in previous publications (e.g., [20], [29]–[34]).

[3]In [20], ST always relays PT's message in Stage II. This can cause error propagation for PT's message. However, [20] did not analyze the SOP of primary/secondary communication and hence, error propagation was not accounted for the SOP analysis.

where $\Xi\{\cdot\}$ is the expectation operator and $\eta \in (0,1)$ is the energy conversion efficiency.

The power which ST can consume in Stage II is

$$P_s = \frac{E_s}{(1-\alpha)T} = \frac{\alpha\eta\lambda}{1-\alpha}\left(P_p\mu_{ps} + \sigma_s^2\right). \tag{3}$$

Figure 1 shows that the signal used for decoding the PT's information is

$$\tilde{y}_s = \sqrt{1-\lambda}y_s + \tilde{n}_s, \tag{4}$$

where the passband-to-baseband signal conversion induces the noise $\tilde{n}_s \sim \mathcal{CN}(0, \tilde{\sigma}_s^2)$.

Plugging (1) into (4) results in

$$\tilde{y}_s = \sqrt{(1-\lambda)P_p}h_{ps}x_p + \sqrt{1-\lambda}n_s + \tilde{n}_s. \tag{5}$$

Channel estimators suffer a certain error and hence, channel state information is not perfectly estimated. For performance analysis, channel estimation imperfection should be modelled appropriately. This paper employs a well-known channel estimation error model as [22]

$$\tilde{h}_{\mathrm{uv}} = \rho_{\mathrm{uv}}h_{\mathrm{uv}} + \sqrt{1-\rho_{\mathrm{uv}}^2}\varepsilon_{\mathrm{uv}} \tag{6}$$

where h_{uv} is the true channel, $\tilde{h}_{\mathrm{uv}}$ is the estimated channel, $\varepsilon_{\mathrm{uv}}$ is the estimation error; all random variables h_{uv}, $\tilde{h}_{\mathrm{uv}}$, $\varepsilon_{\mathrm{uv}}$ are modelled as $\mathcal{CN}(0, \mu_{\mathrm{uv}})$; the correlation coefficient $0 \le \rho_{\mathrm{uv}} \le 1$ is a constant, representing the exactness of channel estimation.

Inserting (6) into (5), one obtains

$$\begin{aligned}\tilde{y}_s &= \sqrt{(1-\lambda)P_p}\left(\frac{\tilde{h}_{ps}}{\rho_{ps}} - \frac{\sqrt{1-\rho_{ps}^2}}{\rho_{ps}}\varepsilon_{ps}\right)x_p + \sqrt{1-\lambda}n_s + \tilde{n}_s \\ &= \frac{\sqrt{(1-\lambda)P_p}}{\rho_{ps}}\tilde{h}_{ps}x_p - \frac{\sqrt{(1-\lambda)P_p\left(1-\rho_{ps}^2\right)}}{\rho_{ps}}\varepsilon_{ps}x_p + \sqrt{1-\lambda}n_s + \tilde{n}_s.\end{aligned} \tag{7}$$

It is inferred from (7) that the SNR (Signal-to-Noise Ratio) achievable for decoding the PT's information is given by

$$\gamma_s = \frac{\Xi\left\{\left|\frac{\sqrt{(1-\lambda)P_p}}{\rho_{ps}}\tilde{h}_{ps}x_p\right|^2\right\}}{\Xi\left\{\left|-\frac{\sqrt{(1-\lambda)P_p\left(1-\rho_{ps}^2\right)}}{\rho_{ps}}\varepsilon_{ps}x_p + \sqrt{1-\lambda}n_s + \tilde{n}_s\right|^2\right\}} = D\left|\tilde{h}_{ps}\right|^2, \tag{8}$$

where

$$D = \frac{P_p}{P_p\left(1-\rho_{ps}^2\right)\mu_{ps} + \left(\sigma_s^2 + \frac{\tilde{\sigma}_s^2}{1-\lambda}\right)\rho_{ps}^2}. \tag{9}$$

The channel capacity that ST can obtain is $C_s = \alpha \log_2(1+\gamma_s)$ bps/Hz with the pre-logarithm factor α owing to Stage I of αT. The communication theory addressed that ST decodes exactly the PT's information merely if its channel capacity is larger than the required transmission rate C_t, i.e., $C_s \geq C_t$. In other words, x_p is decoded accurately at ST if $\gamma_s \geq \gamma_t$ where $\gamma_t = 2^{C_t/\alpha} - 1$.

If ST decodes successfully the PT's information, it broadcasts the combination of three signals in the form of $\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta(1-\kappa)P_s}x_s + \sqrt{(1-\theta)P_s}x_a$ in Stage II. Otherwise, it broadcasts the combination of solely two signals in the form of $\sqrt{\tau P_s}x_s + \sqrt{(1-\tau)P_s}x_a$ in Stage II. Therefore, PR, SR, and E receive signals in Stage II, correspondingly, as

$$y_p = \begin{cases} h_{sp}\left(\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta(1-\kappa)P_s}x_s + \sqrt{(1-\theta)P_s}x_a\right) + n_p & , \gamma_s \geq \gamma_t \\ h_{sp}\left(\sqrt{\tau P_s}x_s + \sqrt{(1-\tau)P_s}x_a\right) + n_p & , \gamma_s < \gamma_t \end{cases}, \tag{10}$$

$$y_r = \begin{cases} h_{sr}\left(\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta(1-\kappa)P_s}x_s + \sqrt{(1-\theta)P_s}x_a\right) + n_r & , \gamma_s \geq \gamma_t \\ h_{sr}\left(\sqrt{\tau P_s}x_s + \sqrt{(1-\tau)P_s}x_a\right) + n_r & , \gamma_s < \gamma_t \end{cases} \tag{11}$$

$$y_e = \begin{cases} h_{se}\left(\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta(1-\kappa)P_s}x_s + \sqrt{(1-\theta)P_s}x_a\right) + n_e & , \gamma_s \geq \gamma_t \\ h_{se}\left(\sqrt{\tau P_s}x_s + \sqrt{(1-\tau)P_s}x_a\right) + n_e & , \gamma_s < \gamma_t \end{cases} \tag{12}$$

where $n_p \sim \mathcal{CN}\left(0, \sigma_p^2\right)$, $n_r \sim \mathcal{CN}\left(0, \sigma_r^2\right)$, $n_e \sim \mathcal{CN}\left(0, \sigma_e^2\right)$ are respectively the noises impaired by the receive antennas at PR, SR, and E.

Most works (e.g., [17]–[21]) assumed the artificial noise x_a to be completely known at the legitimate receivers (PR and SR), not at E, in order for PR and SR to totally eliminate the effect of x_a on their received signal but this assumption seems impractical because the regeneration of x_a is hardly achieved with the absolute probability. Therefore, this paper assumes x_a to be regenerated at PR and SR with the accuracy of $1-\chi$, $\chi \in [0,1]$, which indicates that χx_a represents the residual artificial noise due to imperfect artificial noise cancellation at PR and SR. Accordingly, PR and SR obtain signals with less artificial noise after partly removing x_a, respectively, as

$$\tilde{y}_p = \begin{cases} h_{sp}\left(\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta(1-\kappa)P_s}x_s + \chi\sqrt{(1-\theta)P_s}x_a\right) + n_p & , \gamma_s \geq \gamma_t \\ h_{sp}\left(\sqrt{\tau P_s}x_s + \chi\sqrt{(1-\tau)P_s}x_a\right) + n_p & , \gamma_s < \gamma_t \end{cases} \tag{13}$$

$$\tilde{y}_r = \begin{cases} h_{sr}\left(\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta(1-\kappa)P_s}x_s + \chi\sqrt{(1-\theta)P_s}x_a\right) + n_r & , \gamma_s \geq \gamma_t \\ h_{sr}\left(\sqrt{\tau P_s}x_s + \chi\sqrt{(1-\tau)P_s}x_a\right) + n_r & , \gamma_s < \gamma_t \end{cases} \tag{14}$$

Inserting (6) into (13), one obtains

$$\tilde{y}_p = \begin{cases} \left(\frac{\tilde{h}_{sp}}{\rho_{sp}} - \frac{\sqrt{1-\rho_{sp}^2}}{\rho_{sp}}\varepsilon_{sp}\right)\left(\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta\left(1-\kappa\right)P_s}x_s + \chi\sqrt{\left(1-\theta\right)P_s}x_a\right) + n_p & ,\gamma_s \geq \gamma_t \\ h_{sp}\left(\sqrt{\tau P_s}x_s + \chi\sqrt{\left(1-\tau\right)P_s}x_a\right) + n_p & ,\gamma_s < \gamma_t \end{cases}$$

$$= \begin{cases} \frac{\sqrt{\theta\kappa P_s}}{\rho_{sp}}\tilde{h}_{sp}x_p - \frac{\sqrt{\theta\kappa\left(1-\rho_{sp}^2\right)P_s}}{\rho_{sp}}\varepsilon_{sp}x_p + \left(\frac{\tilde{h}_{sp}}{\rho_{sp}} - \frac{\sqrt{1-\rho_{sp}^2}}{\rho_{sp}}\varepsilon_{sp}\right)\left(\sqrt{\theta(1-\kappa)P_s}x_s + \chi\sqrt{(1-\theta)P_s}x_a\right) + n_p, \gamma_s \geq \gamma_t \\ h_{sp}\left(\sqrt{\tau P_s}x_s + \chi\sqrt{\left(1-\tau\right)P_s}x_a\right) + n_p & ,\gamma_s < \gamma_t \end{cases} \tag{15}$$

Based on (17), SINR (Signal-to-Interference plus Noise Ratio) for decoding x_p at PR is expressed as

$$\gamma_p = \begin{cases} \frac{\Xi\left\{\left|\frac{\sqrt{\theta\kappa P_s}}{\rho_{sp}}\tilde{h}_{sp}x_p\right|^2\right\}}{\Xi\left\{\left|-\frac{\sqrt{\theta\kappa(1-\rho_{sp}^2)P_s}}{\rho_{sp}}\varepsilon_{sp}x_p + \left(\frac{\tilde{h}_{sp}}{\rho_{sp}} - \frac{\sqrt{1-\rho_{sp}^2}}{\rho_{sp}}\varepsilon_{sp}\right)\left(\sqrt{\theta(1-\kappa)P_s}x_s + \chi\sqrt{(1-\theta)P_s}x_a\right) + n_p\right|^2\right\}} & ,\gamma_s \geq \gamma_t \\ 0 & ,\gamma_s < \gamma_t \end{cases}$$

$$= \begin{cases} \frac{\theta\kappa P_s\left|\tilde{h}_{sp}\right|^2}{[\theta(1-\kappa)+\chi^2(1-\theta)]P_s\left|\tilde{h}_{sp}\right|^2 + [\theta+\chi^2(1-\theta)]\left(1-\rho_{sp}^2\right)\mu_{sp}P_s + \rho_{sp}^2\sigma_p^2} & ,\gamma_s \geq \gamma_t \\ 0 & ,\gamma_s < \gamma_t \end{cases} \tag{16}$$

Similarly, inserting (6) into (14), one obtains

$$\tilde{y}_r = \begin{cases} \left(\frac{\tilde{h}_{sr}}{\rho_{sr}} - \frac{\sqrt{1-\rho_{sr}^2}}{\rho_{sr}}\varepsilon_{sr}\right)\left(\sqrt{\theta\kappa P_s}x_p + \sqrt{\theta\left(1-\kappa\right)P_s}x_s + \chi\sqrt{\left(1-\theta\right)P_s}x_a\right) + n_r & ,\gamma_s \geq \gamma_t \\ \left(\frac{\tilde{h}_{sr}}{\rho_{sr}} - \frac{\sqrt{1-\rho_{sr}^2}}{\rho_{sr}}\varepsilon_{sr}\right)\left(\sqrt{\tau P_s}x_s + \chi\sqrt{\left(1-\tau\right)P_s}x_a\right) + n_r & ,\gamma_s < \gamma_t \end{cases}$$

$$= \begin{cases} \sqrt{\theta(1-\kappa)P_s}\frac{\tilde{h}_{sr}}{\rho_{sr}}x_s - \frac{\sqrt{(1-\rho_{sr}^2)\theta(1-\kappa)P_s}}{\rho_{sr}}\varepsilon_{sr}x_s + \left(\frac{\tilde{h}_{sr}}{\rho_{sr}} - \frac{\sqrt{1-\rho_{sr}^2}}{\rho_{sr}}\varepsilon_{sr}\right)\left(\sqrt{\theta\kappa P_s}x_p + \chi\sqrt{\left(1-\theta\right)P_s}x_a\right) + n_r, \gamma_s \geq \gamma_t \\ \frac{\tilde{h}_{sr}}{\rho_{sr}}\sqrt{\tau P_s}x_s - \frac{\sqrt{(1-\rho_{sr}^2)\tau P_s}}{\rho_{sr}}\varepsilon_{sr}x_s + \left(\frac{\tilde{h}_{sr}}{\rho_{sr}} - \frac{\sqrt{1-\rho_{sr}^2}}{\rho_{sr}}\varepsilon_{sr}\right)\chi\sqrt{\left(1-\tau\right)P_s}x_a + n_r & ,\gamma_s < \gamma_t \end{cases} \tag{17}$$

Based on (17), SINR for decoding x_s at SR is given by

$$\gamma_r = \begin{cases} \dfrac{\Xi\left\{\left|\sqrt{\theta(1-\kappa)P_s}\frac{\tilde{h}_{sr}}{\rho_{sr}}x_s\right|^2\right\}}{\Xi\left\{\left|-\frac{\sqrt{(1-\rho_{sr}^2)\theta(1-\kappa)P_s}}{\rho_{sr}}\varepsilon_{sr}x_s+\left(\frac{\tilde{h}_{sr}}{\rho_{sr}}-\frac{\sqrt{1-\rho_{sr}^2}}{\rho_{sr}}\varepsilon_{sr}\right)\left(\sqrt{\theta\kappa P_s}x_p+\chi\sqrt{(1-\theta)P_s}x_a\right)+n_r\right|^2\right\}} & ,\gamma_s \geq \gamma_t \\ \dfrac{\Xi\left\{\left|\frac{\tilde{h}_{sr}}{\rho_{sr}}\sqrt{\tau P_s}x_s\right|^2\right\}}{\Xi\left\{\left|-\frac{\sqrt{(1-\rho_{sr}^2)\tau P_s}}{\rho_{sr}}\varepsilon_{sr}x_s+\left(\frac{\tilde{h}_{sr}}{\rho_{sr}}-\frac{\sqrt{1-\rho_{sr}^2}}{\rho_{sr}}\varepsilon_{sr}\right)\chi\sqrt{(1-\tau)P_s}x_a+n_r\right|^2\right\}} & ,\gamma_s < \gamma_t \end{cases}$$

$$= \begin{cases} \dfrac{\theta(1-\kappa)P_s\left|\tilde{h}_{sr}\right|^2}{(\theta\kappa+\chi^2[1-\theta])P_s\left|\tilde{h}_{sr}\right|^2+(1-\rho_{sr}^2)P_s(\theta+\chi^2[1-\theta])\mu_{sr}+\rho_{sr}^2\sigma_r^2} & ,\gamma_s \geq \gamma_t \\ \dfrac{\tau P_s\left|\tilde{h}_{sr}\right|^2}{\chi^2(1-\tau)P_s\left|\tilde{h}_{sr}\right|^2+(1-\rho_{sr}^2)P_s(\tau+\chi^2[1-\tau])\mu_{sr}+\rho_{sr}^2\sigma_r^2} & ,\gamma_s < \gamma_t \end{cases} \tag{18}$$

The knowledge of the artificial noise x_a is merely shared among ST, PR, and SR for securing x_s and x_p but E is blind with it. As such, the SINRs at E for recovering x_s and x_p are inferred from (12). Inserting (6) into (12) results in

$$y_e = \begin{cases} \left(\frac{\tilde{h}_{se}}{\rho_{se}}-\frac{\sqrt{1-\rho_{se}^2}}{\rho_{se}}\varepsilon_{se}\right)\left(\sqrt{\theta\kappa P_s}x_p+\sqrt{\theta\left(1-\kappa\right)P_s}x_s+\sqrt{\left(1-\theta\right)P_s}x_a\right)+n_e & ,\gamma_s \geq \gamma_t \\ \left(\frac{\tilde{h}_{se}}{\rho_{se}}-\frac{\sqrt{1-\rho_{se}^2}}{\rho_{se}}\varepsilon_{se}\right)\left(\sqrt{\tau P_s}x_s+\sqrt{\left(1-\tau\right)P_s}x_a\right)+n_e & ,\gamma_s < \gamma_t \end{cases} \tag{19}$$

from which the SINRs at E for restoring x_s and x_p are respectively derived as

$$\gamma_{Es} = \begin{cases} \dfrac{\Xi\left\{\left|\sqrt{\theta(1-\kappa)P_s}x_s\frac{\tilde{h}_{se}}{\rho_{se}}\right|^2\right\}}{\Xi\left\{\left|-\frac{\sqrt{(1-\rho_{se}^2)\theta(1-\kappa)P_s}}{\rho_{se}}x_s\varepsilon_{se}+\left(\frac{\tilde{h}_{se}}{\rho_{se}}-\frac{\sqrt{1-\rho_{se}^2}}{\rho_{se}}\varepsilon_{se}\right)\left(\sqrt{\theta\kappa P_s}x_p+\sqrt{(1-\theta)P_s}x_a\right)+n_e\right|^2\right\}} & ,\gamma_s \geq \gamma_t \\ \dfrac{\Xi\left\{\left|\frac{\tilde{h}_{se}}{\rho_{se}}\sqrt{\tau P_s}x_s\right|^2\right\}}{\Xi\left\{\left|-\frac{\sqrt{(1-\rho_{se}^2)\tau P_s}}{\rho_{se}}x_s\varepsilon_{se}+\left(\frac{\tilde{h}_{se}}{\rho_{se}}-\frac{\sqrt{1-\rho_{se}^2}}{\rho_{se}}\varepsilon_{se}\right)\sqrt{(1-\tau)P_s}x_a+n_e\right|^2\right\}} & ,\gamma_s < \gamma_t \end{cases}$$

$$= \begin{cases} \dfrac{\theta(1-\kappa)P_s\left|\tilde{h}_{se}\right|^2}{(\theta\kappa+1-\theta)P_s\left|\tilde{h}_{se}\right|^2+P_s(1-\rho_{se}^2)\mu_{se}+\rho_{se}^2\sigma_e^2} & ,\gamma_s \geq \gamma_t \\ \dfrac{\tau P_s\left|\tilde{h}_{se}\right|^2}{(1-\tau)P_s\left|\tilde{h}_{se}\right|^2+P_s(1-\rho_{se}^2)\mu_{se}+\rho_{se}^2\sigma_e^2} & ,\gamma_s < \gamma_t \end{cases} \tag{20}$$

$$\gamma_{Ep} = \begin{cases} \dfrac{\Xi\left\{\left|\frac{\tilde{h}_{se}}{\rho_{se}}\sqrt{\theta\kappa P_s}x_p\right|^2\right\}}{\Xi\left\{\left|-\frac{\sqrt{(1-\rho_{se}^2)\theta\kappa P_s}}{\rho_{se}}x_p\varepsilon_{se}+\left(\frac{\tilde{h}_{se}}{\rho_{se}}-\frac{\sqrt{1-\rho_{se}^2}}{\rho_{se}}\varepsilon_{se}\right)\left(\sqrt{\theta(1-\kappa)P_s}x_s+\sqrt{(1-\theta)P_s}x_a\right)+n_e\right|^2\right\}} & ,\gamma_s \geq \gamma_t \\ 0 & ,\gamma_s < \gamma_t \end{cases}$$

$$= \begin{cases} \dfrac{\theta\kappa P_s\left|\tilde{h}_{se}\right|^2}{(1-\theta\kappa)P_s\left|\tilde{h}_{se}\right|^2+P_s(1-\rho_{se}^2)\mu_{se}+\rho_{se}^2\sigma_e^2} & ,\gamma_s \geq \gamma_t \\ 0 & ,\gamma_s < \gamma_t \end{cases} \tag{21}$$

It is worth emphasizing from (20) and (21) that ST purposely generates the artificial noise power to corrupt the eavesdropper. Accordingly, increasing the artificial noise would secure information transmission for x_s and x_p. Moreover, channel estimation imperfection, which is represented by terms in the denominators of (16), (18), (20), (21) weighted by $1-\rho_{\mathtt{uv}}^2$, degrades the performance of all receivers (PR, SR, E).

The channel capacities at PR and SR in Stage II are inferred from (16) and (18), correspondingly, as

$$C_p = (1-\alpha)\log\left(1+\gamma_p\right), \tag{22}$$

$$C_r = (1-\alpha)\log\left(1+\gamma_r\right), \tag{23}$$

where $(1-\alpha)$ is the pre-logarithm factor due to Stage II of $(1-\alpha)T$.

Similarly, the channel capacities at E for decoding x_s and x_p in Stage II are inferred from (20) and (21), correspondingly, as

$$C_{Es} = (1-\alpha)\log\left(1+\gamma_{Es}\right), \tag{24}$$

$$C_{Ep} = (1-\alpha)\log\left(1+\gamma_{Ep}\right). \tag{25}$$

The secrecy capacity for x_s is the difference between the capacities at SR and E for recovering x_s, i.e.,

$$\tilde{C}_s = \left[C_r - C_{Es}\right]^+ = (1-\alpha)\left[\log\frac{1+\gamma_r}{1+\gamma_{Es}}\right]^+, \tag{26}$$

where $[x]^+$ denotes $\max(x,0)$.

Similarly, the secrecy capacity for x_p is the difference between the capacities at PR and E for restoring x_p, i.e.,

$$\tilde{C}_p = (1-\alpha)\left[\log\frac{1+\gamma_p}{1+\gamma_{Ep}}\right]^+. \tag{27}$$

III. SOP Analysis

The SOP indicates the possibility which the secrecy capacity is below the preset security threshold C_0. Therefore, it quantifies the secrecy capability of ANaEHON. This section proposes precise closed-form SOP formulas for quickly assessing the secrecy capability for x_s and x_p without time-consuming simulations. Moreover, these formulas serve as a good starting point to achieve the formulas for other pivotal security measures such as IP, PSCP, STP.

A. SOP for primary information x_p

The SOP for primary information x_p is given by

$$SOP_p\left(C_0\right) = \Pr\left\{\tilde{C}_p < C_0\right\}. \tag{28}$$

$SOP_p\left(C_0\right)$ is divided into two cases, dependent on whether ST successfully decodes the PT's information or not:

$$SOP_p\left(C_0\right) = \Pr\left\{\tilde{C}_p < C_0 \middle| C_s \geq C_t\right\}\Pr\left\{C_s \geq C_t\right\} + \Pr\left\{\tilde{C}_p < C_0 \middle| C_s < C_t\right\}\Pr\left\{C_s < C_t\right\}. \tag{29}$$

Substituting $\tilde{C}_p$ in (27) into (29), one has

$$\begin{aligned} SOP_p\left(C_0\right) = &\underbrace{\Pr\left\{1+\gamma_p < 2^{C_0/(1-\alpha)}\left(1+\gamma_{Ep}\right) \middle| \gamma_s \geq \gamma_t\right\}}_{\Upsilon}\underbrace{\Pr\left\{\gamma_s \geq \gamma_t\right\}}_{\Delta} \\ &+ \underbrace{\Pr\left\{\tilde{C}_p < C_0 \middle| \gamma_s < \gamma_t\right\}}_{\psi}\underbrace{\Pr\left\{\gamma_s < \gamma_t\right\}}_{1-\Delta}. \end{aligned} \tag{30}$$

The term Δ in (30) is equivalently rewritten as

$$\Delta = \Pr\left\{\gamma_s = D\left|\tilde{h}_{ps}\right|^2 \geq \gamma_t\right\} = e^{-\gamma_t/(\mu_{ps}D)}. \tag{31}$$

In ANaEHONs, if ST unsuccessfully decodes the PT's information, it does not relay the PT's information and the SINR at PR for decoding x_p is zero (i.e., $\gamma_p = 0$ for $\gamma_s < \gamma_t$ as shown in (16)). Therefore, in this scenario, the secrecy capacity for x_p is also zero (i.e., $\tilde{C}_p = 0$ conditioned on $\gamma_s < \gamma_t$), resulting in $\psi = 1$.

The term Υ in (30) is rewritten after using (16) and (21) for the case of $\gamma_s \geq \gamma_t$ as

$$\Upsilon = \Pr\left\{X < 2^{C_0/(1-\alpha)}Y\right\}, \tag{32}$$

where

$$X = 1 + \frac{A\left|\tilde{h}_{sp}\right|^2}{B\left|\tilde{h}_{sp}\right|^2 + \tilde{\sigma}_p^2}, \tag{33}$$

$$Y = 1 + \frac{A\left|\tilde{h}_{se}\right|^2}{C\left|\tilde{h}_{se}\right|^2 + \tilde{\sigma}_e^2}, \tag{34}$$

with

$$A = \theta\kappa P_s, \tag{35}$$

$$B = \left[\theta\left(1-\kappa\right) + \chi^2\left(1-\theta\right)\right] P_s, \tag{36}$$

$$C = \left(1-\theta\kappa\right) P_s, \tag{37}$$

$$\tilde{\sigma}_p^2 = \left[\theta + \chi^2\left(1-\theta\right)\right]\left(1-\rho_{sp}^2\right)\mu_{sp}P_s + \rho_{sp}^2\sigma_p^2, \tag{38}$$

$$\tilde{\sigma}_e^2 = P_s\left(1-\rho_{se}^2\right)\mu_{se} + \rho_{se}^2\sigma_e^2. \tag{39}$$

It is shown in Appendix A that Υ has a precise form as

$$\Upsilon = \begin{cases} 1 - Ue^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B} + \frac{\tilde{\sigma}_e^2}{\mu_{se}C}}\Lambda, & N < L \\ 1 - Ue^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B} + \frac{\tilde{\sigma}_e^2}{\mu_{se}C}}\varphi, & 1 \le L < N \\ 1, & L < 1 \end{cases} \tag{40}$$

where

$$M = 1 + A/B. \tag{41}$$

$$N = 1 + A/C. \tag{42}$$

$$L = 2^{-C_0/(1-\alpha)}M, \tag{43}$$

$$J = \frac{\tilde{\sigma}_p^2 A}{\mu_{sp}B^2}2^{-C_0/(1-\alpha)}, \tag{44}$$

$$U = \frac{\tilde{\sigma}_e^2 A}{\mu_{se}C^2}, \tag{45}$$

$$\begin{aligned}\Lambda = e^{\frac{J}{N-L}}\Bigg\{&\frac{e^{-U/(N-1)}}{U} - \frac{Je^{U/(L-N)}}{\left(N-L\right)^2}Ei\left(-UV\right) + \\ &\sum_{n=2}^{\infty}\frac{J^n(-U)^{n-1}}{\left(N-L\right)^{2n}n!\left(n-1\right)!}\left[e^{-\frac{U}{N-1}}\sum_{k=1}^{n-1}\frac{(k-1)!}{\left(-UV\right)^k} - e^{\frac{U}{L-N}}Ei\left(-UV\right)\right]\Bigg\}\end{aligned} \tag{46}$$

$$V = \frac{1}{N-1} - \frac{1}{N-L}, \tag{47}$$

$$\varphi = e^{\frac{J-U}{N-L}}\left\{\frac{e^{-UV}-1}{U} + \sum_{n=1}^{\infty}\frac{J^n}{\left(N-L\right)^{2n}n!}\left(\sum_{k=1}^{n-1}\frac{\left(-U\right)^{k-1}V^{k-n}}{e^{UV}\prod_{i=1}^{k}\left(n-i\right)} - \frac{\left(-U\right)^{n-1}}{(n-1)!}Ei\left(-UV\right)\right)\right\}, \tag{48}$$

with $Ei(\cdot)$ being the exponential-integral function [35] built in computational softwares (e.g., Mathematica, Matlab).

Inserting Υ in (40), Δ in (31), and $\psi = 1$ into (30) results in the precise closed-form formula of $SOP_p(C_0)$.

B. SOP for secondary information x_s

The SOP for secondary information x_s is given by

$$SOP_s(C_0) = \Pr\left\{\tilde{C}_s < C_0\right\}. \tag{49}$$

$SOP_s(C_0)$ is divided into two cases, dependent on whether ST successfully decodes the PT's information or not:

$$SOP_s(C_0) = \Pr\left\{\tilde{C}_s < C_0 \middle| C_s \geq C_t\right\}\Pr\{C_s \geq C_t\} + \Pr\left\{\tilde{C}_s < C_0 \middle| C_s < C_t\right\}\Pr\{C_s < C_t\}. \tag{50}$$

Substituting $\tilde{C}_s$ in (26) into (50), one has

$$\begin{aligned} SOP_s(C_0) = {} & \overbrace{\Pr\left\{1+\gamma_r < 2^{C_0/(1-\alpha)}(1+\gamma_{Es}) \middle| \gamma_s \geq \gamma_t\right\}}^{Z_1}\overbrace{\Pr\{\gamma_s \geq \gamma_t\}}^{\Delta} \\ & + \underbrace{\Pr\left\{1+\gamma_r < 2^{C_0/(1-\alpha)}(1+\gamma_{Es}) \middle| \gamma_s < \gamma_t\right\}}_{Z_2}\underbrace{\Pr\{\gamma_s < \gamma_t\}}_{1-\Delta}. \end{aligned} \tag{51}$$

The term Δ in (51) was already computed in (31) while the term Z_1 in (51) is rewritten after using (18) and (20) for the case of $\gamma_s \geq \gamma_t$ as

$$Z_1 = \Pr\left\{1 + \frac{A_1\left|\tilde{h}_{sr}\right|^2}{B_1\left|\tilde{h}_{sr}\right|^2 + \tilde{\sigma}_r^2} < 2^{C_0/(1-\alpha)}\left(1 + \frac{A_1\left|\tilde{h}_{se}\right|^2}{C_1\left|\tilde{h}_{se}\right|^2 + \tilde{\sigma}_e^2}\right)\right\}, \tag{52}$$

where

$$A_1 = \theta(1-\kappa)P_s, \tag{53}$$

$$B_1 = \left(\theta\kappa + \chi^2[1-\theta]\right)P_s, \tag{54}$$

$$C_1 = (\theta\kappa + 1 - \theta)P_s, \tag{55}$$

$$\tilde{\sigma}_r^2 = \left(1-\rho_{sr}^2\right)P_s\left(\theta + \chi^2[1-\theta]\right)\mu_{sr} + \rho_{sr}^2\sigma_r^2, \tag{56}$$

The quantity Z_1 has the same form as Υ in (32). Therefore, by substituting variables appropriately into Υ in (32), one can achieve the precise closed-form formula of Z_1. More specifically,

Z_1 is computed by using Υ in (40) with $A_1 \to A$, $B_1 \to B$, $C_1 \to C$, $\mu_{sr} \to \mu_{sp}$, $\tilde{\sigma}_r^2 \to \tilde{\sigma}_p^2$. As a result, the derivation of Z_1 is skipped here for compactness.

The term Z_2 in (51) is rewritten after using (18) and (20) for the case of $\gamma_s < \gamma_t$ as

$$Z_2 = \Pr\left\{1 + \frac{A_2\left|\tilde{h}_{sr}\right|^2}{B_2\left|\tilde{h}_{sr}\right|^2 + \breve{\sigma}_r^2} < 2^{C_0/(1-\alpha)}\left(1 + \frac{A_2\left|\tilde{h}_{se}\right|^2}{C_2\left|\tilde{h}_{se}\right|^2 + \tilde{\sigma}_e^2}\right)\right\}, \tag{57}$$

where

$$A_2 = \tau P_s, \tag{58}$$

$$B_2 = \chi^2\left(1-\tau\right)P_s, \tag{59}$$

$$C_2 = \left(1-\tau\right)P_s, \tag{60}$$

$$\breve{\sigma}_r^2 = \left(1-\rho_{sr}^2\right)P_s\left(\tau + \chi^2\left[1-\tau\right]\right)\mu_{sr} + \rho_{sr}^2\sigma_r^2. \tag{61}$$

The quantity Z_2 has the same form as Υ in (32). Therefore, by substituting variables appropriately into Υ in (32), one can achieve the precise closed-form formula of Z_2. More specifically, Z_2 is computed by using Υ in (40) with $A_2 \to A$, $B_2 \to B$, $C_2 \to C$, $\mu_{sr} \to \mu_{sp}$, $\breve{\sigma}_r^2 \to \tilde{\sigma}_p^2$. As a result, the derivation of Z_2 is skipped here for compactness.

Inserting the above-derived precise closed-form formulas of Δ, Z_1, and Z_2 into (51), one achieves the precise closed-form formula of $SOP_s\left(C_0\right)$.

C. Remarks

The precise closed-form formulas of SOP_p and SOP_s are useful in quickly assessing the security measure of secondary/primary communication in ANaEHON without exhaustive simulations. Up to the best of our understanding, these formulas have not been reported yet. Moreover, they can be exploited to achieve the formulas for other pivotal security measures. More specifically, IP addresses the probability of negative secrecy capacity. Accordingly, IPs of secondary and primary communication are respectively computed as

$$IP_s = \Pr\left\{\tilde{C}_s < 0\right\} = SOP_s\left(0\right), \tag{62}$$

$$IP_p = \Pr\left\{\tilde{C}_p < 0\right\} = SOP_p\left(0\right). \tag{63}$$

PSCP indicates the probability of positive secrecy capacity. As such, PSCPs of secondary and primary communication are respectively expressed as

$$PSCP_s = \Pr\left\{\tilde{C}_s > 0\right\} = 1 - SOP_s\left(0\right), \tag{64}$$

$$PSCP_p = \Pr\left\{\tilde{C}_p > 0\right\} = 1 - SOP_p\left(0\right). \tag{65}$$

Finally, STP is the product of the secrecy communication probability at a certain secrecy capacity with that secrecy capacity. Consequently, STPs of secondary and primary communication are respectively expressed as

$$STP_s = \left[1 - SOP_s\left(C_0\right)\right] C_0, \tag{66}$$

$$STP_p = \left[1 - SOP_p\left(C_0\right)\right] C_0. \tag{67}$$

IV. Results and Discussions

The SOP of secondary/primary communication in ANaEHON is assessed through pivotal specifications. Unless otherwise stated, a set of arbitrary parameters is used to illustrate the following results: PT at $(-0.6, 0.2)$, PR at $(0.5, -0.2)$, ST at $(0.0, 0.0)$, SR at $(0.6, 0.0)$, E at $(0.6, -0.1)$, $\eta = 0.9$, $\sigma_s^2 = \sigma_e^2 = \sigma_p^2 = \sigma_r^2 = \tilde{\sigma}_s^2 = N_0$, $\rho_{\text{uv}} = \rho$, $\varsigma = 3$, $P_p/N_0 = 10$ dB, $\alpha = \lambda = \tau = 0.6$, $\theta = 0.8$, $\kappa = 0.7$, $C_t = C_0 = 0.1$ bps/Hz. Figures 2-11 respectively denote "Sim." and "Ana." as simulated and analytical results, and demonstrate the agreement between analysis and simulation, ratifying the exactness of the analysis in (30) and (51).

Figure 2 shows the SOPs versus channel estimation imperfection reflected by ρ. This figure demonstrates that channel estimation error drastically affects the SOP of primary/secondary communication. More specifically, large SOPs are almost unchanged over a wide range of bad channel estimation error ($0 \leq \rho \leq 0.9$) while SOP_p (or SOP_s) significantly drops (or increases) with a slight channel estimation improvement ($0.9 \leq \rho \leq 1$). Additionally, imperfect artificial noise cancellation at legitimate receivers degrades security performance of primary/secondary communication (i.e., SOPs increase with increasing χ) as expected. Moreover, the SOP of primary communication is smaller than that of secondary communication at the same levels of channel estimation error and artificial noise cancellation. This is because the power allocation factor for primary and secondary signals is $\kappa = 0.7$, which means that 70% ($\kappa = 0.7$) of the ST's total transmit power allocated for legitimate information (i.e., θP_s) is for relaying the PT's information while 30% ($1 - \kappa = 0.3$) of that is for transmitting the ST's information.

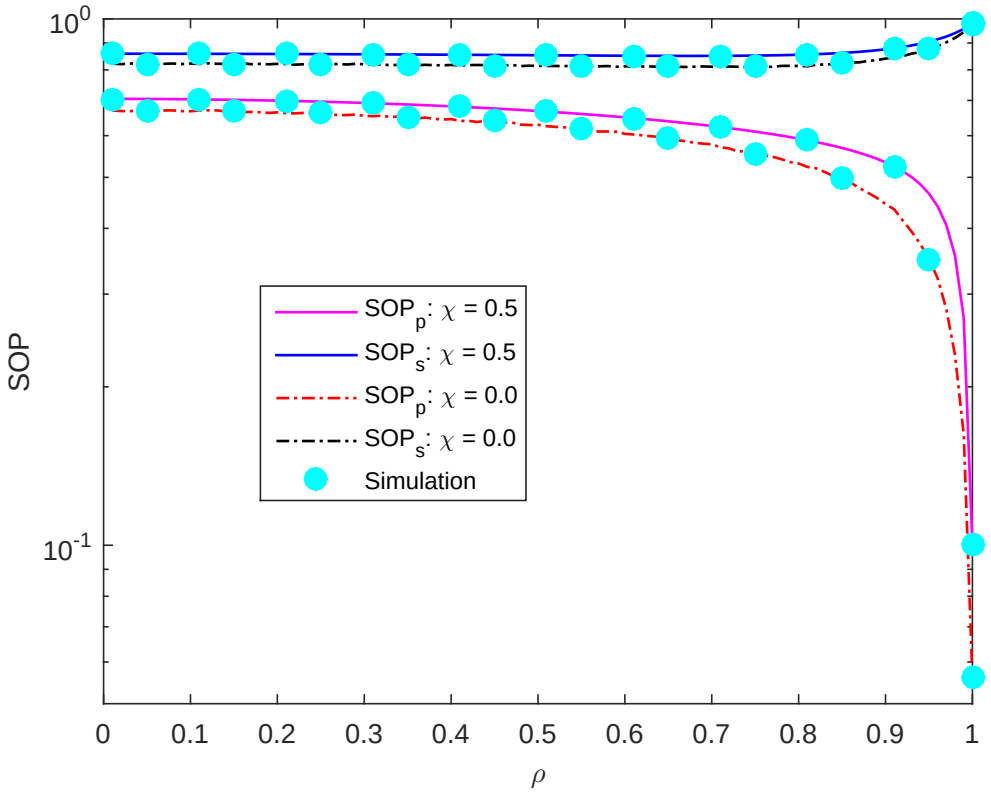

Fig. 2. SOPs versus ρ.

Figure 3 illustrates the SOPs versus imperfect artificial noise cancellation reflected by χ. This figure shows the increase of SOPs with increasing χ, which is expected because of increasing artificial noise residue at legitimate receivers. Additionally, security performance of primary communication is considerably improved (or deteriorated) with reducing channel estimation imperfection (i.e., increasing ρ) in the range of low (or high) artificial noise residue (e.g., SOP_p at $\rho = 1.0$ is smaller than SOP_p at $\rho = 0.9$ for $\chi < 0.675$ but the reverse happens for $\chi > 0.675$). Nonetheless, security performance of secondary communication is always degraded with reducing channel estimation imperfection irrespective of χ (e.g., SOP_s at $\rho = 1.0$ is larger than SOP_s at $\rho = 0.9$ for any χ). Furthermore, due to $\kappa = 0.7$ as Figure 2, primary communication is more secure than secondary communication at the same levels of channel estimation error and artificial noise cancellation, as expected.

Figure 4 shows the SOPs versus P_p/N_0. It is seen that owing to $\kappa = 0.7$ as Figure 2, primary communication is more secure than secondary communication at the same levels of

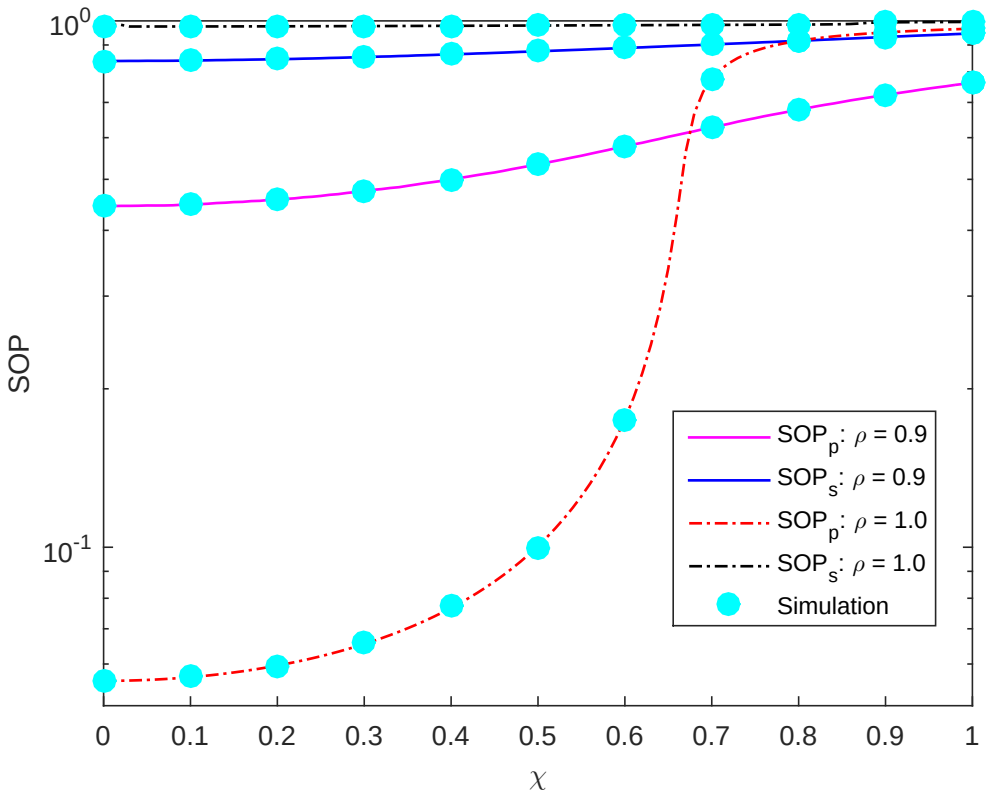

Fig. 3. SOPs versus χ.

channel estimation error and artificial noise cancellation, as expected. In addition, SOP_p is drastically reduced with better channel estimation and artificial noise cancellation, especially when the transmit power of PT increases, i.e., SOP_p at $(\rho = 1.0, \chi = 0.0)$ is considerably smaller than SOP_p at $(\rho = 0.9, \chi = 0.5)$. Nonetheless, the reversed security performance trend is observed for secondary transmission, i.e., SOP_s at $(\rho = 1.0, \chi = 0.0)$ is larger than SOP_s at $(\rho = 0.9, \chi = 0.5)$. Furthermore, security performance of primary communication compromises that of secondary communication with P_p/N_0 (i.e., SOP_p reduces while SOP_s increases with P_p/N_0).

Figure 5 plots the SOPs versus θ. This figure demonstrates optimum values of θ, which minimize the SOP of primary/secondary communication. These optimum values balance the transmit powers for the legitimate (primary and secondary) information and the artificial noise. Moreover, SOP_p is lower than SOP_s at the same levels of channel estimation error and artificial noise cancellation, which can be interpreted from the fact that $\kappa = 0.7$ allocates more power for

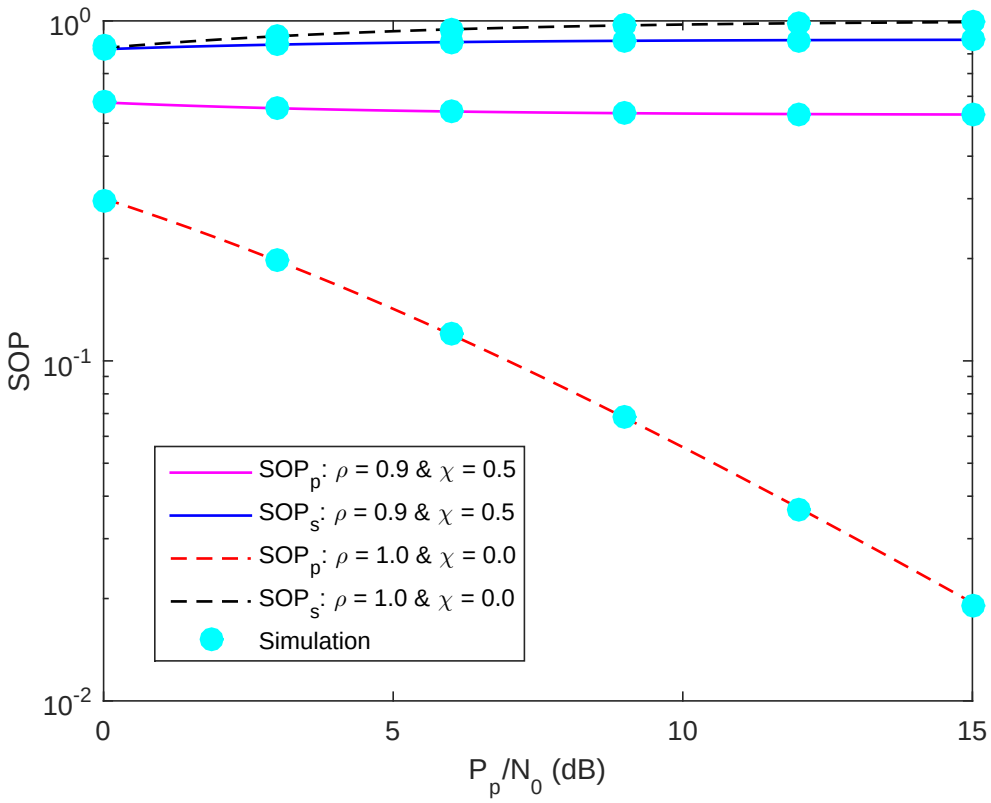

Fig. 4. SOPs versus P_p/N_0.

the ST to transmit the PT's information than the ST's information. Furthermore, better channel estimation and artificial noise cancellation improve security performance of secondary/primary communication in a certain region of θ (e.g., SOP_s (or SOP_p) at $(\rho = 1.0, \chi = 0.0)$ is smaller than SOP_s (or SOP_p) at $(\rho = 0.9, \chi = 0.5)$ when $\theta < 0.575$ (or $\theta < 0.925$)) but degrade that performance in another region (e.g., SOP_s (or SOP_p) at $(\rho = 1.0, \chi = 0.0)$ is larger than SOP_s (or SOP_p) at $(\rho = 0.9, \chi = 0.5)$ when $\theta > 0.575$ (or $\theta > 0.925$)).

Figure 6 plots the SOPs versus κ. The results illustrate that increasing κ improves secrecy capability of primary communication (i.e., SOP_p decreases) while deteriorates that of secondary communication (i.e., SOP_s increases), showing the security trade-off between secondary and primary communication. This is obvious because κ interprets the percentage of the ST's transmit power allotted for the PT's information while $1-\kappa$ interprets the percentage of the ST's transmit power allotted for the ST's information. Therefore, increasing κ decreases SOP_p but increases SOP_s. Due to the conflicting security performance trend of SOP_p and SOP_s with respect to κ,

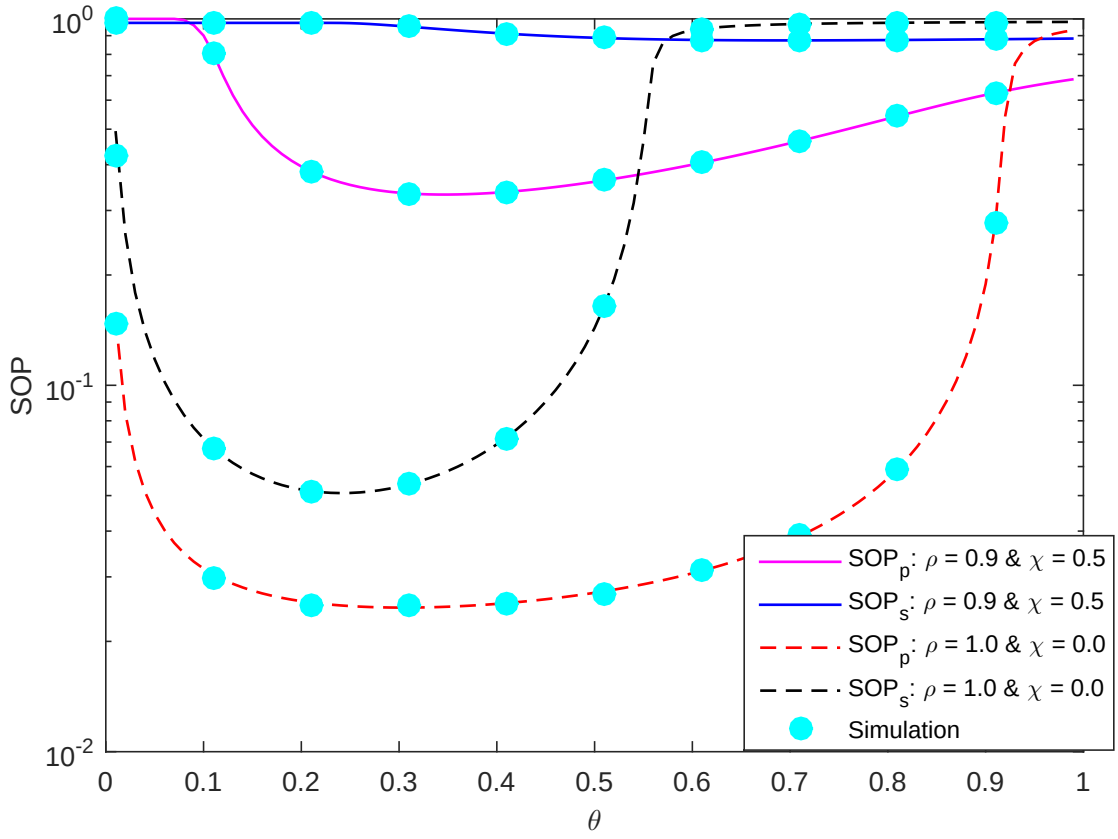

Fig. 5. SOPs versus θ.

there exists a value of κ where SOP_p and SOP_s are equal (e.g., $\kappa \simeq 0.535$ for $(\rho = 0.9, \chi = 0.5)$ and $\kappa \simeq 0.5$ for $(\rho = 1.0, \chi = 0.0)$ as shown in Figure 6), which means the best security balance between primary and secondary communication. Moreover, the primary (or secondary) communication is in outage over a certain region of κ (e.g., $SOP_s = 1$ for $\kappa \geq 0.7$ and $SOP_p = 1$ for $\kappa \leq 0.2$ when $\rho = 1.0$ and $\chi = 0.0$ as shown in Figure 6). Furthermore, better channel estimation and artificial noise cancellation improve security performance of primary/secondary communication in a certain region of κ (e.g., SOP_s (or SOP_p) at $(\rho = 1.0, \chi = 0.0)$ is smaller than SOP_s (or SOP_p) at $(\rho = 0.9, \chi = 0.5)$ when $\kappa < 0.52$ (or $\kappa > 0.48$)) but degrade that performance in another region (e.g., SOP_s (or SOP_p) at $(\rho = 1.0, \chi = 0.0)$ is larger than SOP_s (or SOP_p) at $(\rho = 0.9, \chi = 0.5)$ when $0.52 < \kappa < 0.7$ (or $0.2 < \theta < 0.48$)).

Figure 7 plots the SOPs versus C_t. It is seen that increasing C_t improves secrecy capability of secondary communication but deteriorates that of primary communication. This is because increasing C_t (i.e., increasing the transmission rate required by the PT) reduces the proba-

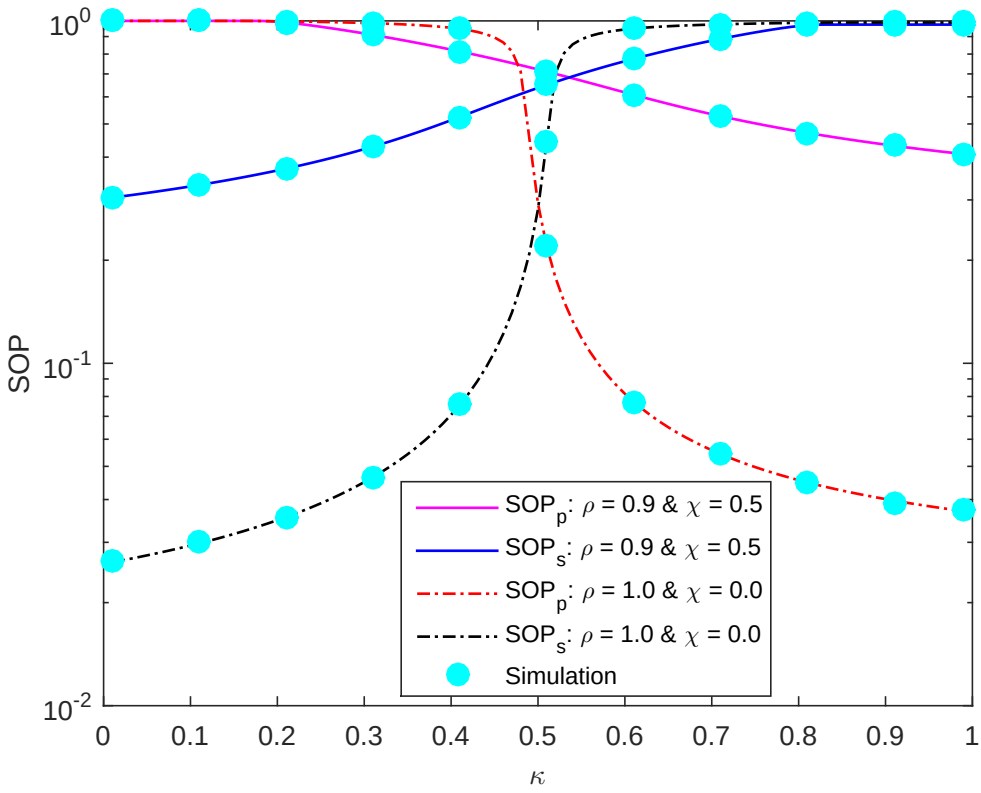

Fig. 6. SOPs versus κ.

bility of decoding successfully the PT's information at the ST, eventually limiting the PT's information relayed to PR and increasing the SOP_p. While the PT's information is rarely relayed to PR by ST, the information of ST has more chances to be transmitted with higher transmit power, intimately reducing the SOP_s. Due to opposite security performance trends of secondary and primary networks with respect to C_t, it is possible to balance security performance for these networks by setting the appropriate required primary transmission rate; for instance, $SOP_s = SOP_p$ at $C_t = 0.79$ bps/Hz for $(\rho = 0.9, \chi = 0.5)$ and at $C_t = 1.85$ bps/Hz for $(\rho = 1.0, \chi = 0.0)$. Moreover, better channel estimation and artificial noise cancellation improve security performance of primary communication but degrades that of secondary communication, i.e., SOP_p (or SOP_s) at $(\rho = 1.0, \chi = 0.0)$ is smaller (or larger) than SOP_p (or SOP_s) at $(\rho = 0.9, \chi = 0.5)$.

Figure 8 plots the SOPs versus C_0. This figure exposes that increasing C_0 degrades security capability of primary/secondary communication until a complete outage, as expected. Interest-

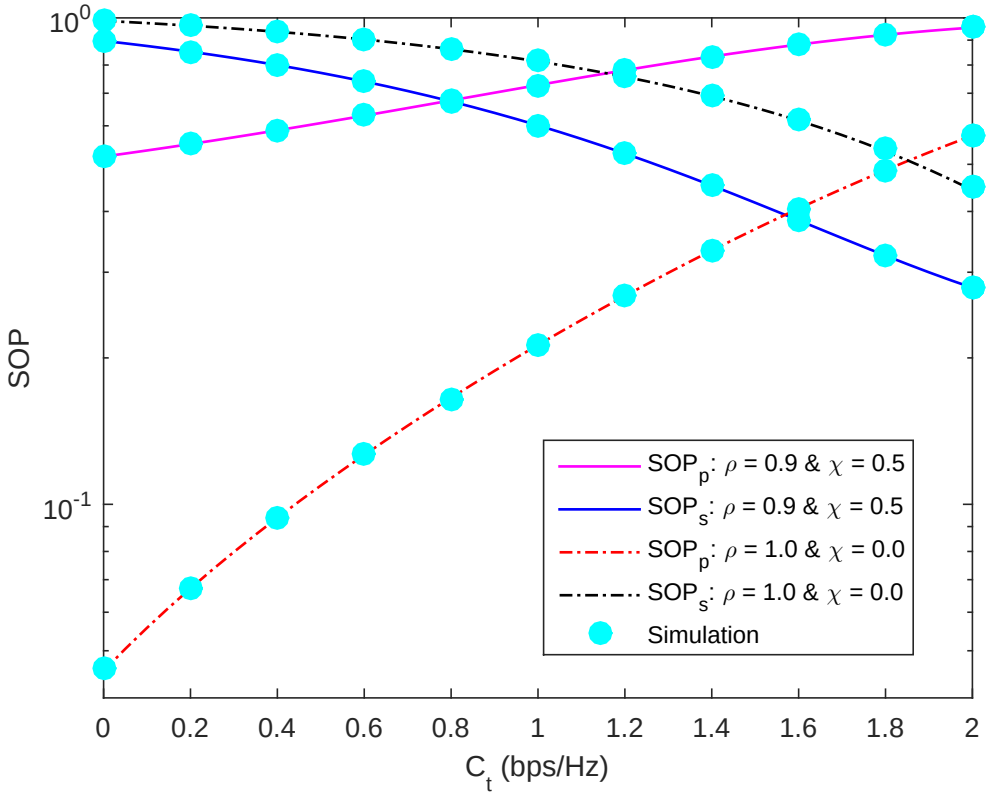

Fig. 7. SOPs versus C_t.

ingly, secrecy performance of secondary communication may be superior or inferior to that of primary communication over a certain region of C_0 (e.g., $SOP_s < SOP_p$ for $C_0 \leq 0.016$ bps/Hz but $SOP_s > SOP_p$ for $C_0 > 0.016$ bps/Hz when $\rho = 1.0$ and $\chi = 0.0$). Moreover, better channel estimation and artificial noise cancellation also improve security performance of secondary/primary communication in a certain region of C_0; for instance, SOP_p (or SOP_s) at $(\rho = 1.0, \chi = 0.0)$ is smaller than SOP_p (or SOP_s) at $(\rho = 0.9, \chi = 0.5)$ when C_0 is smaller than 0.232 (or 0.049) bps/Hz.

Figure 9 demonstrates the SOPs versus α. The results expose that the security measure of primary/secondary communication can be optimized with relevant selection of α. The optimum value of α, which minimizes SOPs, is interpreted as follows. Increasing α offers the ST to harvest more energy from the PT and to recover successfully the PT's information with a higher probability in Stage I, thus probably enhancing security performance. Nonetheless, this increment degrades security capability in Stage II due to the decrease in secrecy capacity

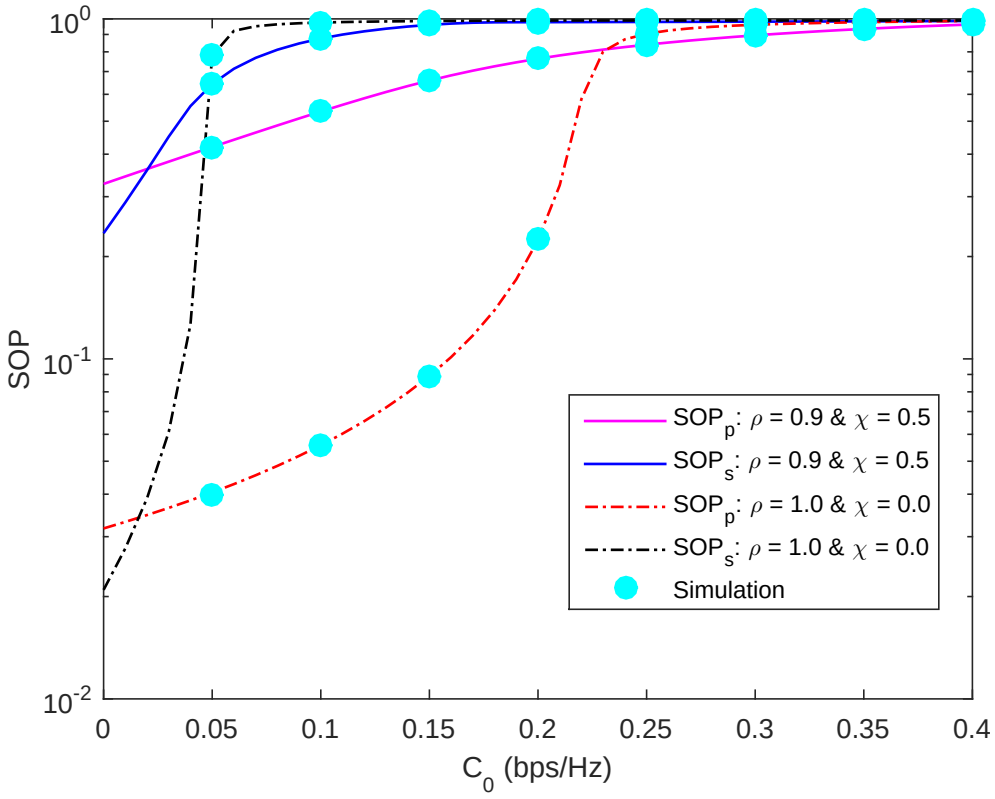

Fig. 8. SOPs versus C_0.

which is proportional to $1-\alpha$. Accordingly, α should be optimized to balance gains in two stages. Moreover, security performance of primary/secondary communication at the optimal value of α is improved with better channel estimation and artificial noise cancellation, i.e., SOP_p (or SOP_s) at the optimal value of α for $(\rho = 1.0, \chi = 0.0)$ is smaller than SOP_p (or SOP_s) at the optimal value of α for $(\rho = 0.9, \chi = 0.5)$. Nonetheless, the best security of primary communication is superior to that of secondary communication at channel estimation-and-artificial noise cancellation perfection (i.e., $SOP_p < SOP_s$ at the optimal value of α for $(\rho = 1.0, \chi = 0.0)$) but channel estimation-and-artificial noise cancellation imperfection reverses the performance tendency where the best security of primary communication is inferior to that of secondary communication (i.e., $SOP_p > SOP_s$ at the optimal value of α for $(\rho = 0.9, \chi = 0.5)$).

Figure 10 exposes the SOPs versus λ. The results show that secrecy performance of the secondary communication is almost constant and only improved for high λ (e.g., $\lambda \geq 0.95$). This is because large λ enables the ST to harvest more energy from PT and reduces signal

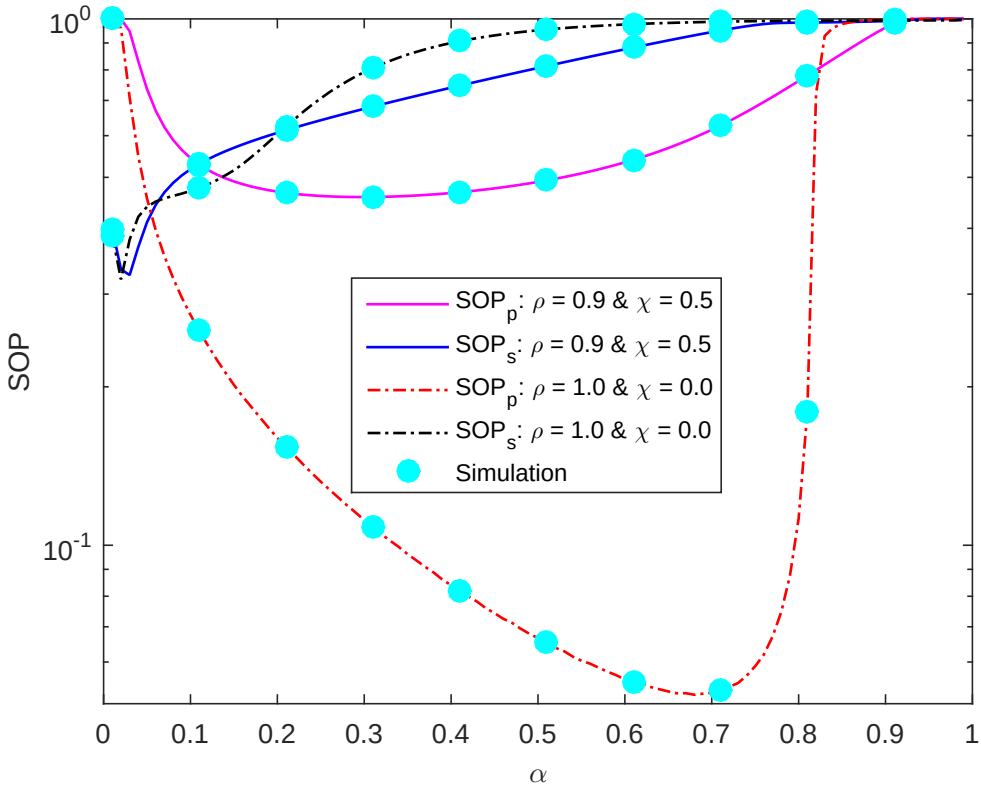

Fig. 9. SOPs versus α.

power at the decoder of ST (i.e., reduces the probability of decoding successfully the PT's information); thus, the ST's information is transmitted with higher power in Stage II, eventually declining SOP_s. Nevertheless, λ can be selected appropriately to optimize secrecy performance of primary communication. The optimum value of λ for minimum SOP_p is to balance between harvested energy and the probability of decoding the PT's information at the ST. Moreover, secrecy performance of primary communication is better than that of secondary communication due to $\kappa = 0.7$, which is a similar comment observed from the previous figures. Furthermore, better channel estimation and artificial noise cancellation enhance security capability of primary communication but deteriorate that of secondary communication.

It is noted that τ is the power allocation factor for artificial noise and secondary signal as the ST decodes incorrectly the PT's signal. Therefore, to observe the affect of τ clearly, it is better to consider the case that the ST decodes unsuccessfully the PT's signal. This case can be set-up by selecting a large value of C_t. Figure 11 demonstrates the SOPs versus τ for

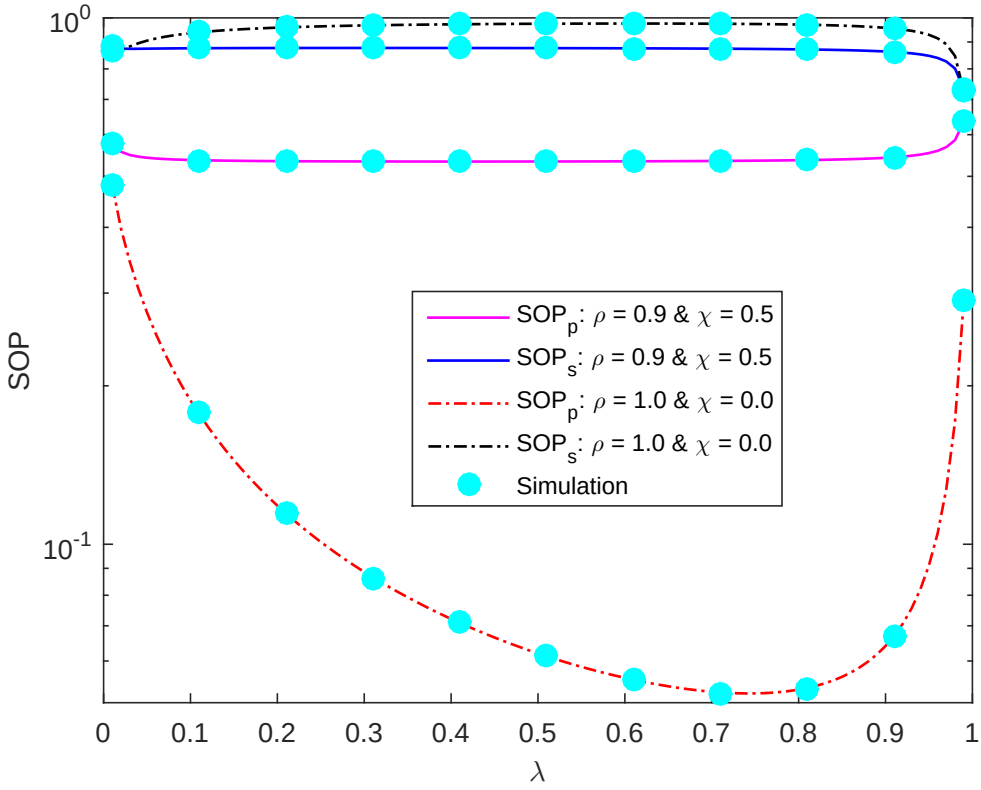

Fig. 10. SOPs versus λ.

$C_t = 5$ bps/Hz. This figure exposes that primary communication is in outage because the large C_t causes the ST to fail in decoding the PT's information and hence, PR does not receive it for decoding. Moreover, there exists the optimum value of τ which maximizes secrecy performance of secondary communication. This optimum τ aims to balance the power allocation for the ST's information and the artificial noise. Furthermore, better channel estimation and artificial noise cancellation enhance security performance of secondary communication, i.e., SOP_s at $(\rho = 1.0, \chi = 0.0)$ is smaller than SOP_s at $(\rho = 0.9, \chi = 0.5)$.

V. Conclusion

This paper implemented the overlay mechanism in cognitive radio networks where the secondary transmitter assists the information transmission of the primary transmitter as well as transmits its private information. The secondary transmitter is capable of harvesting radio frequency energy and generating the artificial noise to self-power its operation and secure primary/secondary

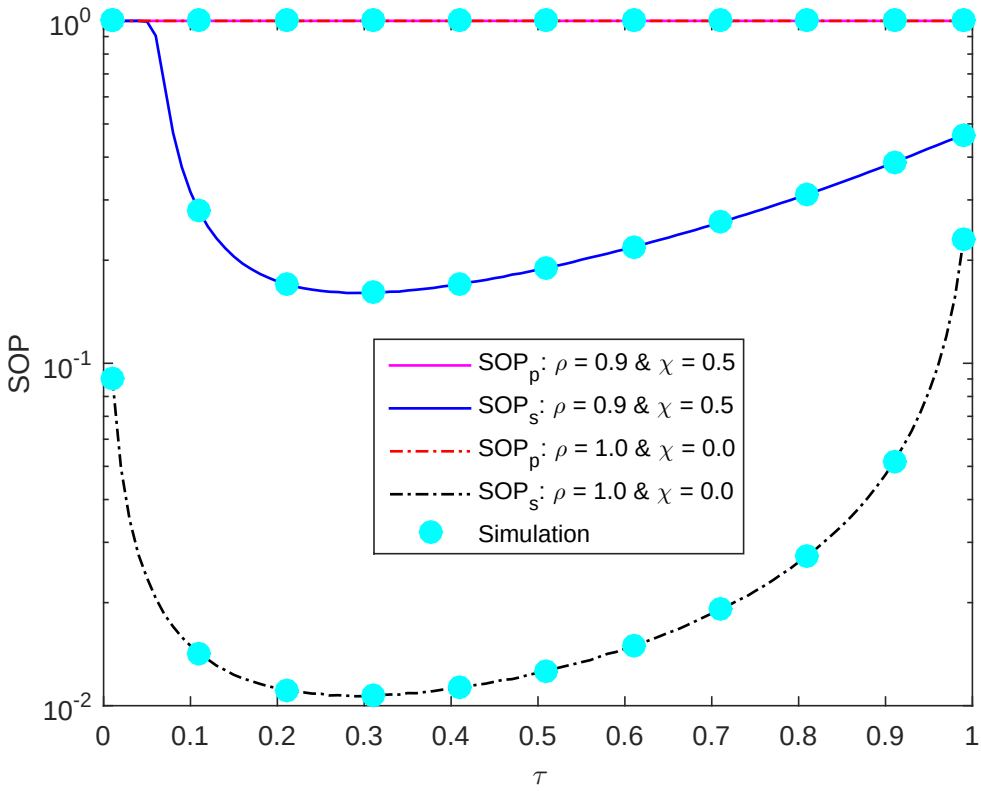

Fig. 11. SOPs versus τ.

communication against eavesdroppers. Secrecy capability of primary/secondary communication is measured in terms of primary/secondary secrecy outage probability under uncertainties of channel estimation and artificial noise cancellation imperfection, which was numerically evaluated by the proposed precise closed-form formulas. Various results are generated to validate these formulas as well as shed insights into security measure of artificial noise-aided energy harvesting overlay networks with respect to main system parameters. Moreover, optimum system parameters can be found through exhaustive searches based on the proposed formulas, which well serves as a design guideline. Furthermore, the secrecy performance compromise between primary and secondary communication can be managed by adjusting system parameters appropriately.

APPENDIX A: PROOF OF (40)

Before proving (40), one needs to prepare the PDFs of X in (33) and Y in (34). It is seen that both X and Y have a common form of

$$W = 1 + \frac{aZ}{bZ + c}, \tag{68}$$

where Z is the exponential random variable with the PDF of $f_Z(z) = \frac{1}{\mu_Z} e^{-\frac{z}{\mu_Z}}$, $z \geq 0$.

From (68), one infers

$$Z = \frac{(W-1)\,c}{a + b - Wb}. \tag{69}$$

Because $Z \geq 0$, W must fall in $1 \leq W < \frac{a}{b} + 1$. The Jacobian coefficient is given by

$$\frac{dZ}{dW} = \frac{ac}{(a + b - Wb)^2}. \tag{70}$$

As such, the PDF of W can be inferred from the PDF of Z as

$$f_W(w) = f_Z\left(\frac{(w-1)\,c}{a + b - wb}\right)\left|\frac{dZ}{dW}\right|. \tag{71}$$

Inserting $f_Z(z) = \frac{1}{\mu_Z} e^{-\frac{z}{\mu_Z}}$ and the Jacobian coefficient into (71), one infers the PDF of W as

$$f_W(w) = \frac{ac}{\mu_Z b^2} \frac{e^{\frac{w-1}{w - \frac{a}{b} - 1}\frac{c}{\mu_Z b}}}{\left(w - \frac{a}{b} - 1\right)^2}, \qquad 1 \leq w \leq \frac{a}{b} + 1. \tag{72}$$

Now, applying ($a = A$, $b = B$, $c = \tilde{\sigma}_p^2$, $Z = \left|\tilde{h}_{sp}\right|^2$, $W = X$) into (72), one can obtain the PDF of X as

$$f_X(x) = \frac{A\tilde{\sigma}_p^2}{\mu_{sp} B^2} \frac{e^{\frac{x-1}{x-M}\frac{\tilde{\sigma}_p^2}{\mu_{sp} B}}}{(x-M)^2} \quad , 1 \leq x < M \tag{73}$$

where M is given in (41).

Similarly, applying ($a = A$, $b = C$, $c = \tilde{\sigma}_e^2$, $Z = \left|\tilde{h}_{se}\right|^2$, $W = Y$) into (72), one derives the PDF of Y as

$$f_Y(y) = \frac{A\tilde{\sigma}_e^2}{\mu_{se} C^2} \frac{e^{\frac{y-1}{y-N}\frac{\tilde{\sigma}_e^2}{\mu_{se} C}}}{(y-N)^2} \quad , 1 \leq y < N \tag{74}$$

where N is given in (42).

Also, before showing the proof of (40), one needs to prepare the following result:

$$\Omega\left(a, b, B, M, \mu_{sp}, \tilde{\sigma}_p^2\right) = \int_a^b f_X(x)\,dx. \tag{75}$$

Inserting $f_X(x)$ in (73) into (75) and after performing some variable changes, one obtains

$$\begin{aligned}\Omega\left(a,b,B,M,\mu_{sp},\tilde{\sigma}_p^2\right) &= \int_a^b \frac{A\tilde{\sigma}_p^2}{\mu_{sp}B^2}\frac{e^{\frac{x-1}{x-M}\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}}}{(x-M)^2}dx \\ &\overset{z=x-M}{=} \int_{a-M}^{b-M} \frac{A\tilde{\sigma}_p^2}{\mu_{sp}B^2}\frac{e^{\frac{z+M-1}{z}\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}}}{z^2}dz \\ &\overset{x=-z}{=} -\frac{A\tilde{\sigma}_p^2}{\mu_{sp}B^2}e^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}}\int_{M-a}^{M-b}\frac{e^{-\frac{\tilde{\sigma}_p^2(M-1)}{\mu_{sp}Bx}}}{x^2}dx \\ &= e^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}}\left(e^{-\frac{\tilde{\sigma}_p^2(M-1)}{\mu_{sp}B(M-a)}} - e^{-\frac{\tilde{\sigma}_p^2(M-1)}{\mu_{sp}B(M-b)}}\right).\end{aligned} \tag{76}$$

Now, the proof of (40) starts as follows. Because X and Y are independent, Υ in (32) is rewritten as

$$\Upsilon = \iint\limits_{x<2^{C_0/(1-\alpha)}y} f_X(x)\, f_Y(y)\, dxdy. \tag{77}$$

Since $f_X(x)$ is non-zero for $1 \le x < M$, the upper bound $2^{C_0/(1-\alpha)}y$ on x must be considered whether it falls in $[1, M)$ or not. Therefore, Υ must be computed for three cases as follows:

$$\Upsilon = \underbrace{\iint\limits_{x<2^{C_0/(1-\alpha)}y<1} f_X(x)\, f_Y(y)\, dxdy}_{\text{Case 1: } 2^{C_0/(1-\alpha)}y<1} + \underbrace{\iint\limits_{x<2^{C_0/(1-\alpha)}y} f_X(x)\, f_Y(y)\, dxdy}_{\text{Case 2: } 1\le 2^{C_0/(1-\alpha)}y<M} + \underbrace{\iint\limits_{x<M} f_X(x)\, f_Y(y)\, dxdy}_{\text{Case 3: } 2^{C_0/(1-\alpha)}y>M}. \tag{78}$$

Because $f_Y(y)$ is non-zero for $1 \le y < N$ and "Case 1" is equivalent to $y < 2^{-C_0/(1-\alpha)} < 1$, $f_Y(y) = 0$ in "Case 1" and hence, the first term in (78) is zero. Moreover, "Case 2" and "Case 3" are respectively equivalent to $2^{-C_0/(1-\alpha)} \le y < L$ and $y > L$ where L is given by (43). Since $f_Y(y)$ is non-zero for $1 \le y < N$, L must be considered whether it falls in $[1, N)$ or not. Therefore, three scenarios for L need to be investigated as follows (please see Figure 12):

***Scenario 1*:** $N < L$

In this scenario, the last term is (78) is rewritten as $\underbrace{\int_{y=L}^{\infty}\left[\int_{x=1}^{M} f_X(x)\,dx\right] f_Y(y)\,dy}_{\text{Case 3: } y>L}$, which is zero because $f_Y(y) = 0$ when $y = L > N$. Therefore, (78) is of the compact form as

$$\Upsilon = \underbrace{\int_{y=1}^{N}\left[\int_{x=1}^{2^{C_0/(1-\alpha)}y} f_X(x)\,dx\right] f_Y(y)\,dy}_{\text{Case 2: } 2^{-C_0/(1-\alpha)}\le y<L}. \tag{79}$$

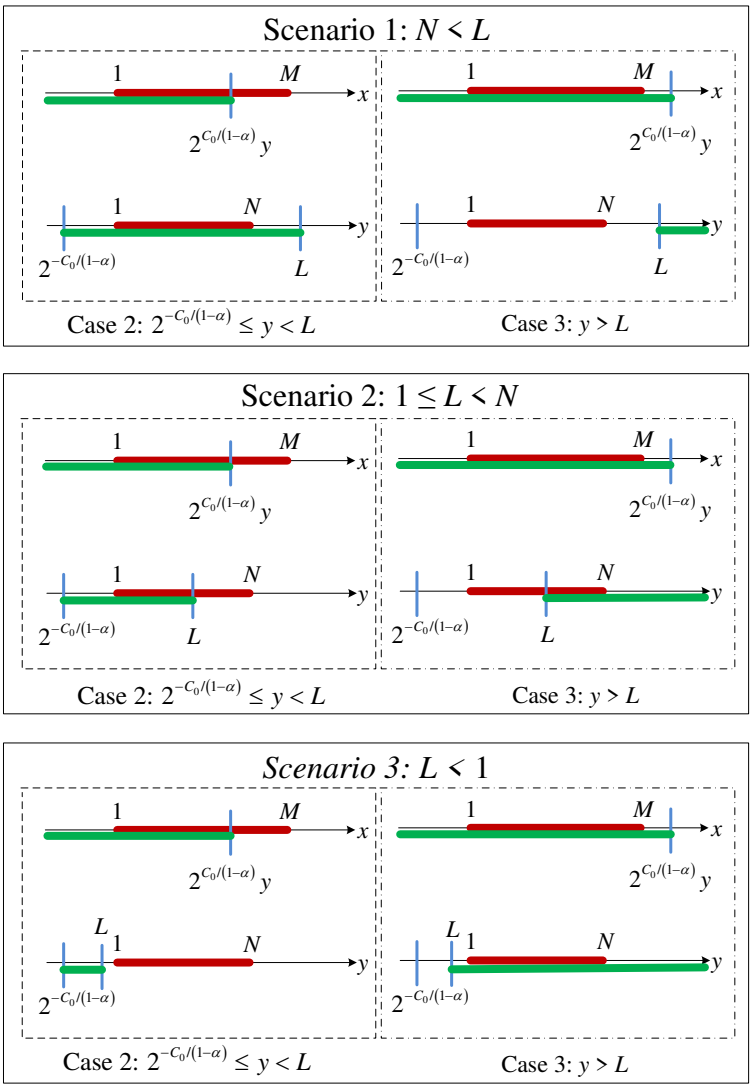

Fig. 12. Scenarios for computing Υ.

Using (75) to compute the inner integral in (75), one obtains

$$\begin{aligned}\Upsilon &= \int_1^N e^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}} \left(e^{-\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}} - e^{-\frac{\tilde{\sigma}_p^2(M-1)}{\mu_{sp}B\left(M-2^{C_0/(1-\alpha)}y\right)}} \right) f_Y(y)\, dy \\ &= 1 - e^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}} \int_1^N e^{-\frac{\tilde{\sigma}_p^2(M-1)}{\mu_{sp}B\left(M-2^{C_0/(1-\alpha)}y\right)}} f_Y(y)\, dy.\end{aligned} \tag{80}$$

It is noted that the last equality in (80) holds because $\int_1^N f_Y(y)\, dy = 1$. Inserting $f_Y(y)$ in (74) into the last integral of (80) and after some manipulations, Υ in (80) matches Υ in (40) for

$N < L$ where

$$\Lambda = \int_{1}^{N} \frac{e^{\frac{J}{y-L}+\frac{U}{y-N}}}{(y-N)^2} dy. \tag{81}$$

with J and U being given in (44) and (45), respectively.

Therefore, to complete the proof of Υ for $N < L$, one must prove that (81) matches (46). Towards this end, some appropriate variable changes are applied to reduce (81) to

$$\begin{aligned}
\Lambda &\overset{x=1/(y-N)}{=} -\int_{1/(1-N)}^{-\infty} e^{\frac{J}{N-L+1/x}+Ux} dx \\
&\overset{y=-x}{=} \int_{1/(N-1)}^{\infty} e^{\frac{J}{N-L}\frac{y}{y-1/(N-L)}-Uy} dy \\
&= e^{\frac{J}{N-L}} \int_{1/(N-1)}^{\infty} e^{\frac{J/(N-L)^2}{y-1/(N-L)}-Uy} dy.
\end{aligned} \tag{82}$$

Performing the series expansion $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ for the term $e^{\frac{J/(N-L)^2}{y-1/(N-L)}}$ in (82) results in

$$\begin{aligned}
\Lambda &= e^{\frac{J}{N-L}} \int_{1/(N-1)}^{\infty} e^{-Uy} \left(\sum_{n=0}^{\infty} \frac{1}{n!} \left[\frac{J/(N-L)^2}{y-1/(N-L)} \right]^n \right) dy \\
&= e^{\frac{J}{N-L}} \sum_{n=0}^{\infty} \frac{J^n}{(N-L)^{2n} n!} \int_{1/(N-1)}^{\infty} \frac{e^{-Uy}}{[y-1/(N-L)]^n} dy \\
&= e^{\frac{J}{N-L}} \left\{ \int_{1/(N-1)}^{\infty} e^{-Uy} dy + \frac{J}{(N-L)^2} \int_{1/(N-1)}^{\infty} \frac{e^{-Uy}}{y+1/(L-N)} dy \right. \\
&\quad \left. + \sum_{n=2}^{\infty} \frac{J^n}{(N-L)^{2n} n!} \int_{1/(N-1)}^{\infty} \frac{e^{-Uy}}{[y+1/(L-N)]^n} dy \right\}.
\end{aligned} \tag{83}$$

The first integral in the last equality of (83) is straightforwardly computed. Also, based on the definition of the exponential-integral function, the second integral in the last equality of (83) is solved easily. The last integral in (83) is evaluated in closed-form with the help of [35, eq. (3.353.1)]. After computing these three integrals, one reduces (83) to (46). This finishes the proof of Υ for $N < L$.

***Scenario 2*:** $1 \leq L < N$

In this scenario, (78) is rewritten after noting that $1 \leq L < N$:

$$\Upsilon = \underbrace{\int_{y=2^{-C_0/(1-\alpha)}}^{L} \left[\int_{x=1}^{2^{C_0/(1-\alpha)}y} f_X(x)\,dx \right] f_Y(y)\,dy}_{\text{Case 2: } 2^{-C_0/(1-\alpha)} \leq y < L} + \underbrace{\int_{y=L}^{N} \left[\int_{x=1}^{M} f_X(x)\,dx \right] f_Y(y)\,dy}_{\text{Case 3: } y > L}. \tag{84}$$

Before computing (84), it is worth noting that $f_X(x)$ is non-zero for $x \in [1, M)$ and hence, $\int_{x=1}^{M} f_X(x)\,dx = 1$. Also, the integral $\int_{x=1}^{2^{C_0/(1-\alpha)}y} f_X(x)\,dx$ can be solved as $\Omega\left(1, 2^{C_0/(1-\alpha)}y, B, M, \mu_{sp}, \tilde{\sigma}_p^2\right)$ according to (75). Therefore, the compact form of (84) is as follows:

$$\begin{aligned}
\Upsilon &= \int_{1}^{L} \Omega\left(1, 2^{C_0/(1-\alpha)}y, B, M, \mu_{sp}, \tilde{\sigma}_p^2\right) f_Y(y)\,dy + \int_{L}^{N} f_Y(y)\,dy \\
&= \int_{1}^{L} e^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}} \left(e^{-\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}} - e^{-\frac{\tilde{\sigma}_p^2(M-1)}{\mu_{sp}B\left(M-2^{C_0/(1-\alpha)}y\right)}} \right) f_Y(y)\,dy + \int_{L}^{N} f_Y(y)\,dy \\
&= \int_{1}^{L} f_Y(y)\,dy - e^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}} \int_{1}^{L} e^{-\frac{\tilde{\sigma}_p^2(M-1)}{\mu_{sp}B\left(M-2^{C_0/(1-\alpha)}y\right)}} f_Y(y)\,dy + \int_{L}^{N} f_Y(y)\,dy \\
&= 1 - e^{\frac{\tilde{\sigma}_p^2}{\mu_{sp}B}} \int_{1}^{L} e^{-\frac{\tilde{\sigma}_p^2(M-1)}{\mu_{sp}B\left(M-2^{C_0/(1-\alpha)}y\right)}} f_Y(y)\,dy.
\end{aligned} \tag{85}$$

It is noted that the last equality in (85) is obtained because $\int_{1}^{N} f_Y(y)\,dy = 1$. Inserting $f_Y(y)$ in (74) into the last integral of (85) and after some manipulations, Υ in (85) is exactly the same as (40) for $1 \leq L < N$ where

$$\varphi = \int_{1}^{L} \frac{e^{J/(y-L)+U/(y-N)}}{(y-N)^2} dy. \tag{86}$$

To complete the proof of Υ for $1 \leq L < N$, one must prove that (86) matches (48). Towards this end, some appropriate variable changes and the series expansion (similarly to steps in (82) and (83)) are applied to reduce (86) to

$$\begin{aligned}
\varphi &= e^{\frac{J-U}{N-L}} \sum_{n=0}^{\infty} \frac{J^n}{(N-L)^{2n} n!} \int_{V}^{0} \frac{e^{-Ux}}{x^n} dx \\
&= e^{\frac{J-U}{N-L}} \left\{ \int_{V}^{0} e^{-Ux} dx + \sum_{n=1}^{\infty} \frac{J^n}{(N-L)^{2n} n!} \int_{V}^{0} \frac{e^{-Ux}}{x^n} dx \right\}
\end{aligned} \tag{87}$$

The first integral in (87) is straightforwardly computed while the second one is computed with the aid of [35, eq. (2.324.2)]. Plugging the results of these two integrals into (87), one reduces (87) to (48). This finishes the proof of Υ for $1 \leq N < L$.

***Scenario 3*:** $L < 1$

In this scenario, (78) is rewritten after noting that $L < 1$:

$$\Upsilon = \underbrace{\int_{y=2^{-C_0/(1-\alpha)}}^{L} \left[\int_{x=1}^{2^{C_0/(1-\alpha)}y} f_X(x)\, dx \right] f_Y(y)\, dy}_{\text{Case 2: } 2^{-C_0/(1-\alpha)} \leq y < L} + \underbrace{\int_{y=1}^{N} \left[\int_{x=1}^{M} f_X(x)\, dx \right] f_Y(y)\, dy}_{\text{Case 3: } y > L}. \tag{88}$$

Because $f_Y(y) = 0$ when $y = L < 1$, the first term in (88) is zero. Moreover, $f_X(x)$ is non-zero for $1 \leq x < M$ and $f_Y(y)$ is non-zero for $1 \leq y < N$ and hence, the second term in (88) is one. Plugging these results into (88), one infers $\Upsilon = 1$, which coincides with (40) for $L < 1$, finishing the proof of Υ for $L < 1$.

By integrating three above scenarios, one can prove that Υ is exactly represented as (40).

REFERENCES

[1] M. Wazid et al., "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap," IEEE Access, vol. 9, pp. 4466-4489, Dec. 2020.

[2] U. Gustavsson et al., "Implementation Challenges and Opportunities in Beyond-5G and 6G Communication," IEEE Journal of Microwaves, vol. 1, no. 1, pp. 86-100, Jan. 2021.

[3] O. L. A. Lpez et al., "Massive Wireless Energy Transfer: Enabling Sustainable IoT Towards 6G Era," IEEE IoT Journal, accepted.

[4] B. Djamaa et al., "Efficient and Stateless P2P Routing Mechanisms for the Internet of Things," IEEE IoT Journal, accepted.

[5] M. Ali et al., "LTE-U WiFi HetNets: Enabling Spectrum Sharing for 5G/Beyond 5G Systems," IEEE IoT Mag., vol. 3, no. 4, pp. 60-65, Dec. 2020.

[6] K. Ho-Van et al., "Security Enhancement for Energy Harvesting Cognitive Networks with Relay Selection," Wire. Commun. and Mobile Computing, vol. 2020, Article ID 8867148, pp. 1-13.

[7] M. Koca et al., "Empirical Feasibility Analysis for Energy Harvesting Intravehicular Wireless Sensor Networks," IEEE IoT Journal, vol. 8, no. 1, pp. 179-186, Jan. 2021.

[8] T. Le Anh et al., "Secrecy Performance of a Multi-NOMA-MIMO System in the UEH Relaying Network Using the PSO Algorithm," IEEE Access, vol. 9, pp. 2317-2331, Dec. 2020.

[9] Y. Nie et al., "Achievable Rate Region of Energy-Harvesting Based Secure Two-Way Buffer-Aided Relay Networks," IEEE Trans. Info. Forensics and Security, vol. 16, pp. 1610-1625, Nov. 2020.

[10] E. Stai et al., "Optimal Resource Allocation in Multihop Wireless Networks Relying on Energy Harvesting," IEEE Commun. Lett., vol. 25, no. 1, pp. 224-228, Jan. 2021.

[11] I. Budhiraja et al., "SWIPT-enabled D2D Communication Underlaying NOMA-Based Cellular Networks in Imperfect CSI," IEEE Trans. Veh. Tech., accepted.

[12] B. Kim et al., "Joint Channel Estimation, Training Design, Tx Power Allocation, and Rx Power Splitting for MIMO SWIPT Systems," IEEE Commun. Lett., accepted.

[13] D. Masotti et al., "RF Systems Design for Simultaneous Wireless Information and Power Transfer (SWIPT) in Automation and Transportation," IEEE Journal of Microwaves, vol. 1, no. 1, pp. 164-175, Jan. 2021.

[14] A. Prathima et al., "Performance Analysis and Optimization of Bidirectional Overlay Cognitive Radio Networks With Hybrid-SWIPT," IEEE Trans. Veh. Tech., vol. 69, no. 11, pp. 13467-13481, Nov. 2020.

[15] S. Thapar et al., "Decoding Orders for Securing Untrusted NOMA," IEEE Networking Lett., accepted.

[16] Z. Abdullah et al., "Enhanced Secrecy Performance of Multihop IoT Networks With Cooperative Hybrid-Duplex Jamming," IEEE Trans. Info. Forensics and Security, vol. 16, pp. 161-172, Jun. 2020.

[17] F. Wang et. al., "Secure Resource Allocation for Polarization-Based Non-Linear Energy Harvesting Over 5G Cooperative CRNs," IEEE Wire. Commun. Lett., accepted.

[18] R. Su et al., "Destination-Assisted Jamming for Physical-Layer Security in SWIPT Cognitive Radio Systems," in Proc. IEEE WCNC, Barcelona, Spain, 2018, pp. 1-6.

[19] R. Su et al., "Secure Cooperative Transmission in Cognitive AF Relay Systems with Destination-Aided Jamming and Energy Harvesting," in Proc. IEEE PIMRC, Istanbul, Turkey, 2019, pp. 1-5.

[20] D. Wang et al., "Primary Privacy Preserving With Joint Wireless Power and Information Transfer for Cognitive Radio Networks," IEEE Trans. Cogn. Commun. and Networking, vol. 6, no. 2, pp. 683-693, Jun. 2020.

[21] M. Xu et al., "Secure Transmission Solutions in Energy Harvesting Enabled Cooperative Cognitive Radio Networks," in Proc. IEEE WCNC, Barcelona, Spain, 2018, pp. 1-6.

[22] D. Wang and C. Tellambura, "Performance Analysis of Energy Beamforming WPCN Links With Channel Estimation Errors," IEEE OJ-CS, vol. 1, pp. 1153-1170, Jul. 2020.

[23] M. Li et al. "Physical Layer Security in Overlay Cognitive Radio Networks With Energy Harvesting," IEEE Trans. Veh. Tech., vol. 67, pp. 11274-11279, Sep. 2018.

[24] H. Dang-Ngoc et al., "Key Secrecy Performance Metrics of Overlay Networks with Energy Scavenging and Artificial Noise," in Proc. IEEE SigTelCom, Hanoi, Vietnam, 28-29 Aug. 2020, pp. 77-81.

[25] N. Pham-Thi-Dan et al., "Secrecy Throughput Analysis of Energy Scavenging Overlay Networks with Artificial Noise," in Proc. IEEE ATC, Nha Trang, Vietnam, 8-10 Aug. 2020, pp. 90-94.

[26] L. Chen et al., "Primary Secrecy Is Achievable: Optimal Secrecy Rate in Overlay CRNs with an Energy Harvesting Secondary Transmitter," in Proc. ICCCN, Las Vegas, USA, 2015, pp. 1-6.

[27] F. Benkhelifa et al., "A Thresholding-based Antenna Switching in MIMO Cognitive Radio Networks with SWIPT-enabled Secondary Receiver," in Proc. IEEE ICC, Paris, France, 21-25 May 2017, pp. 1-6.

[28] X. Zhou et al., "Wireless Information and Power Transfer: Architecture Design and Rate-Energy Tradeoff," IEEE Trans. Commun., vol. 61, no. 11, pp. 4754-4767, Nov. 2013.

[29] K. Ho-Van et al., "Security Performance of Underlay Cognitive Relaying Networks with Energy Harvesting," Wire. Per. Commun., vol. 110, no. 2, pp. 829-846, Jan. 2020.

[30] K. Ho-Van et al., "Security Analysis for Underlay Cognitive Network with Energy Scavenging Capable Relay over Nakagami-m Fading Channels," Wire. Commun. and Mobile Computing, vol. 2019, Article ID 5080952, pp. 1-16.

[31] P. Nguyen-Huu et al., "Secrecy Outage Analysis of Energy Harvesting Two-Way Relaying Networks with Friendly Jammer," IET Commun., vol. 13, no. 13, pp. 18771885, Aug. 2019.

[32] L. Ge et. al., "Performance Analysis for Multihop Cognitive Radio Networks With Energy Harvesting by Using Stochastic Geometry," IEEE IoT Journal, vol. 7, no. 2, pp. 1154-1163, Feb. 2020.

[33] S. Solanki et. al., “Performance Analysis of Piece-Wise Linear Model of Energy Harvesting-Based Multiuser Overlay Spectrum Sharing Networks,” IEEE OJ-CS, vol. 1, pp. 1820-1836, Nov. 2020.

[34] S. Bayat et. al., “Resource Allocation for MC MISO-NOMA SWIPT-Enabled HetNets With Non-Linear Energy Harvesting,” IEEE Access, vol. 8, pp. 192270-192281, Oct. 2020.

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

Figures

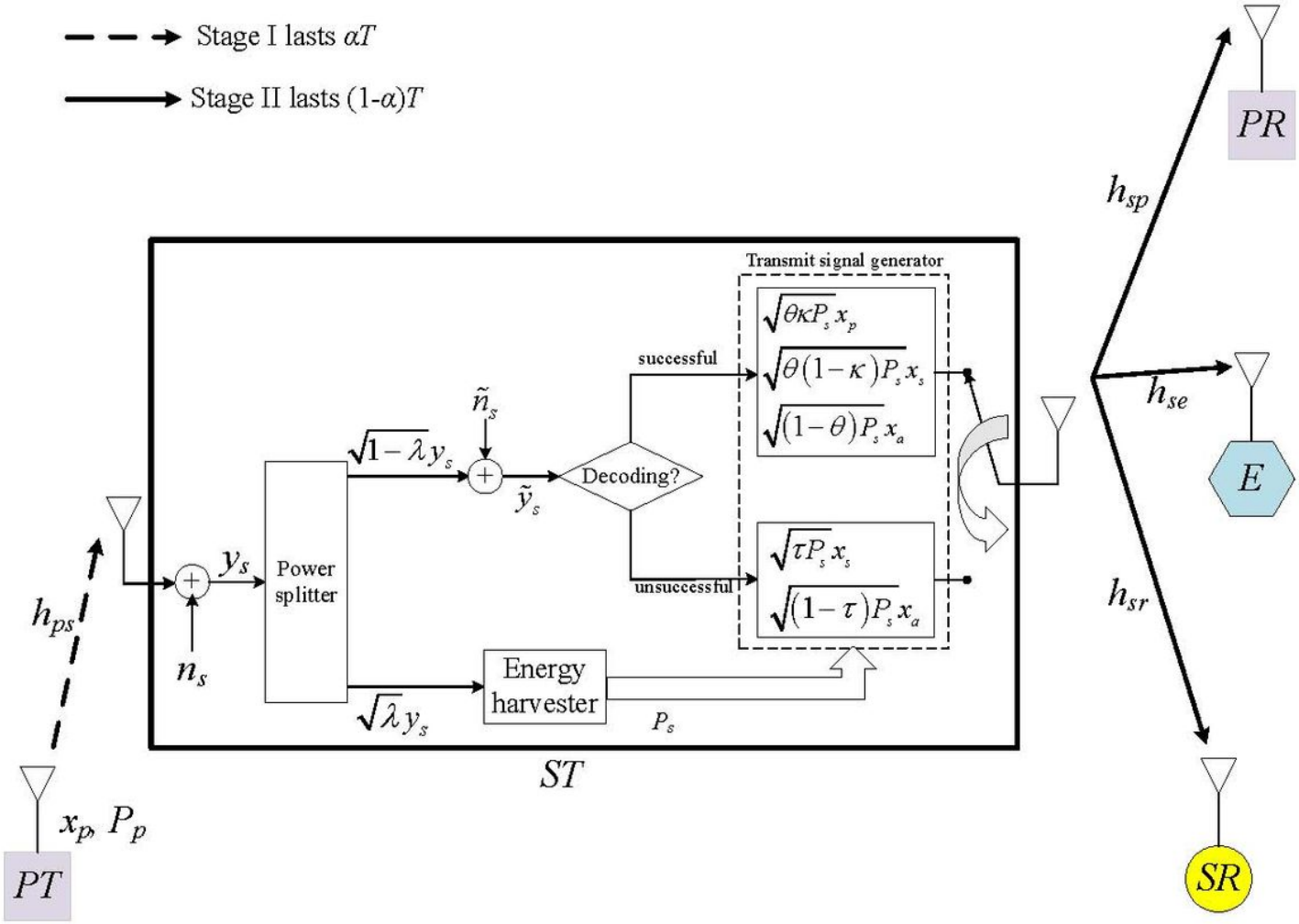

Figure 1

System model.

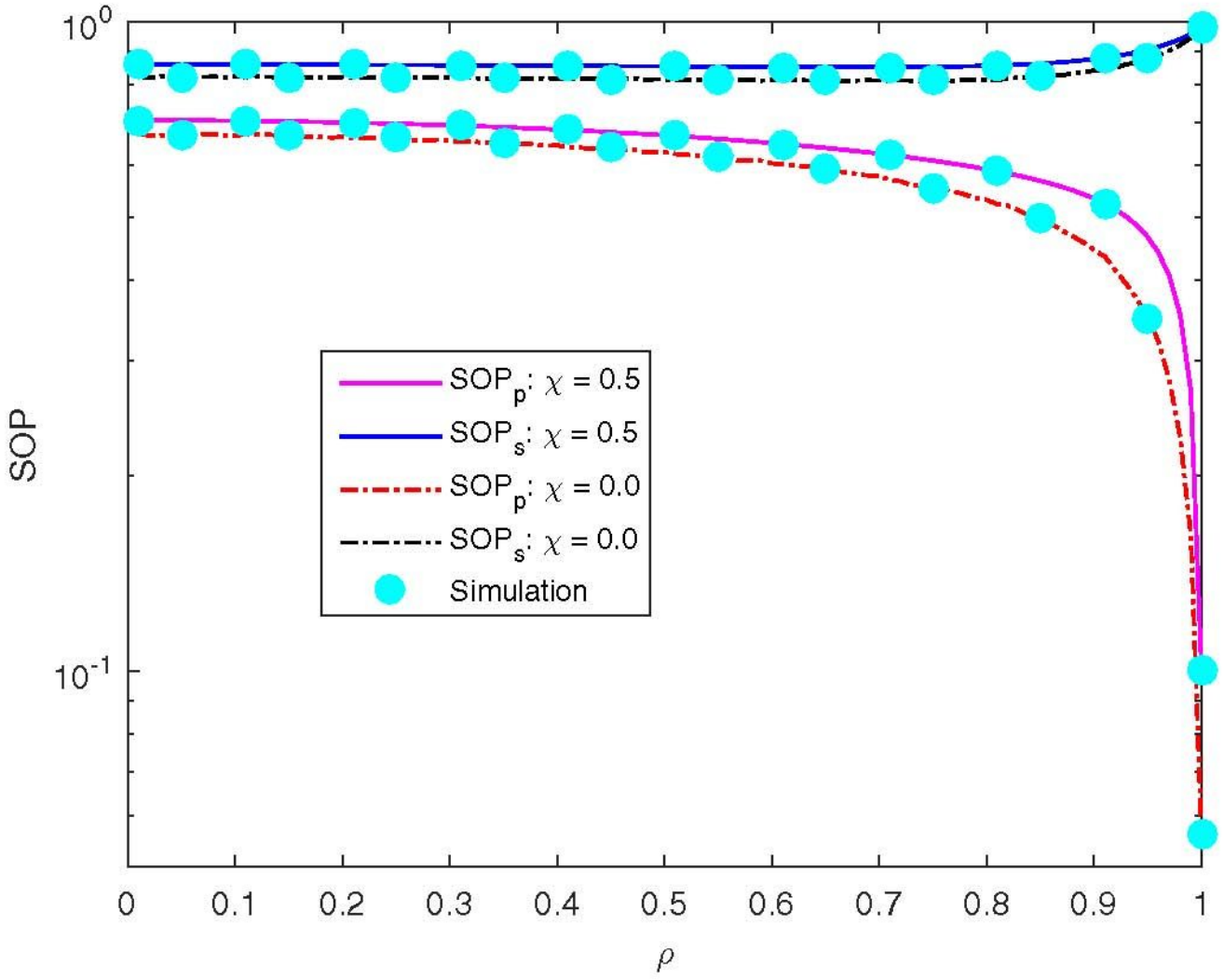

Figure 2

SOPs versus ρ.

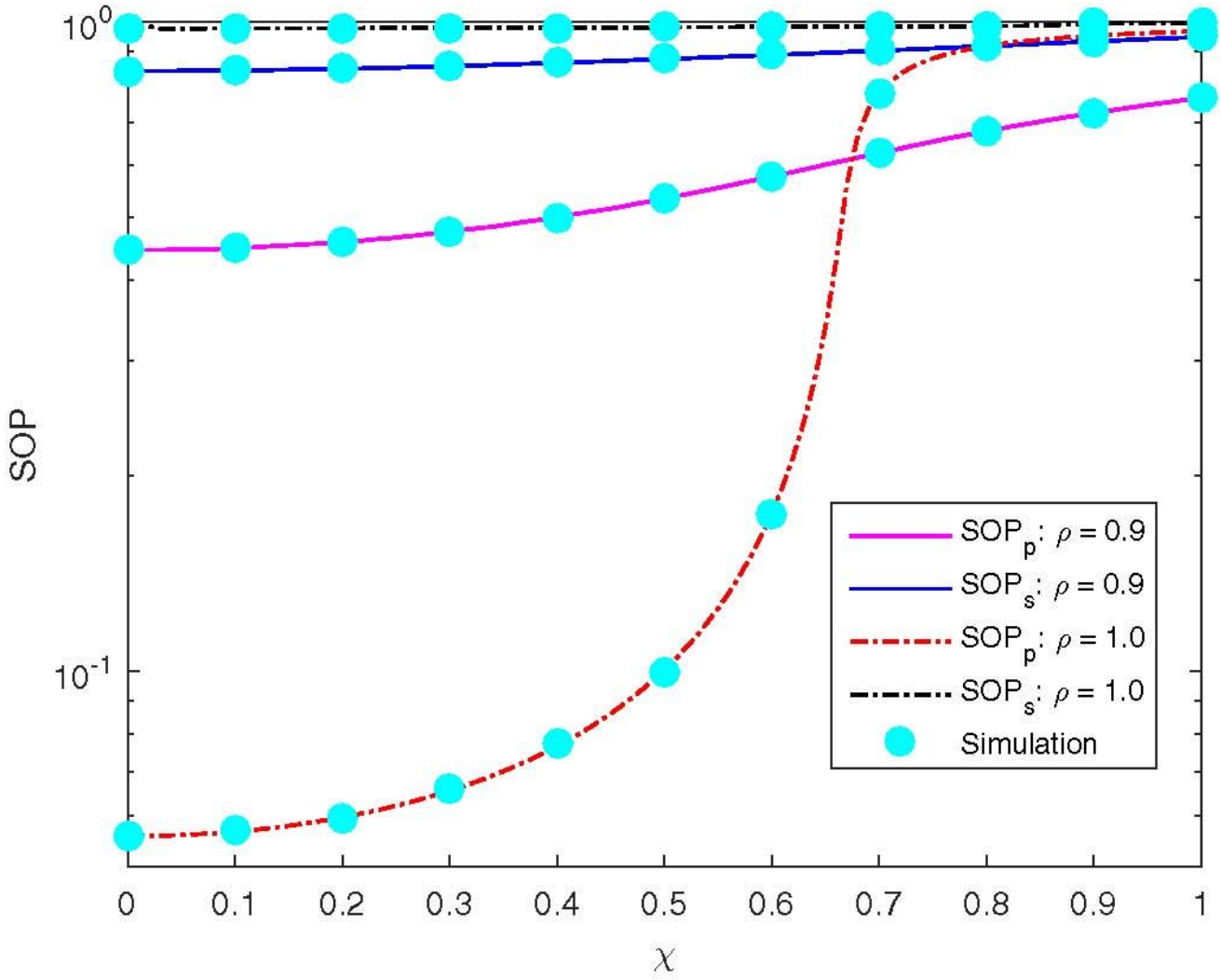

Figure 3

SOPs versus χ.

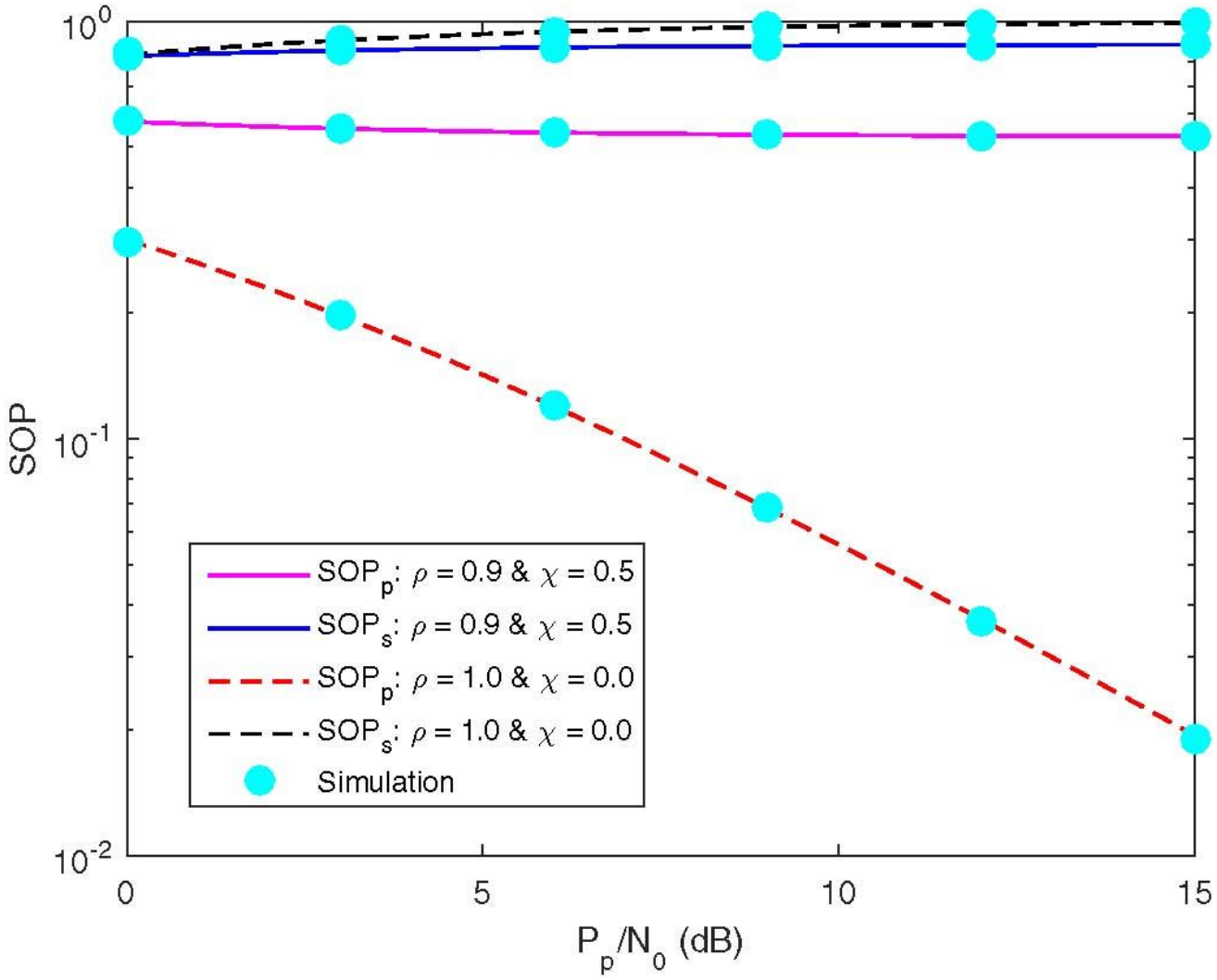

Figure 4

SOPs versus Pp/N0.

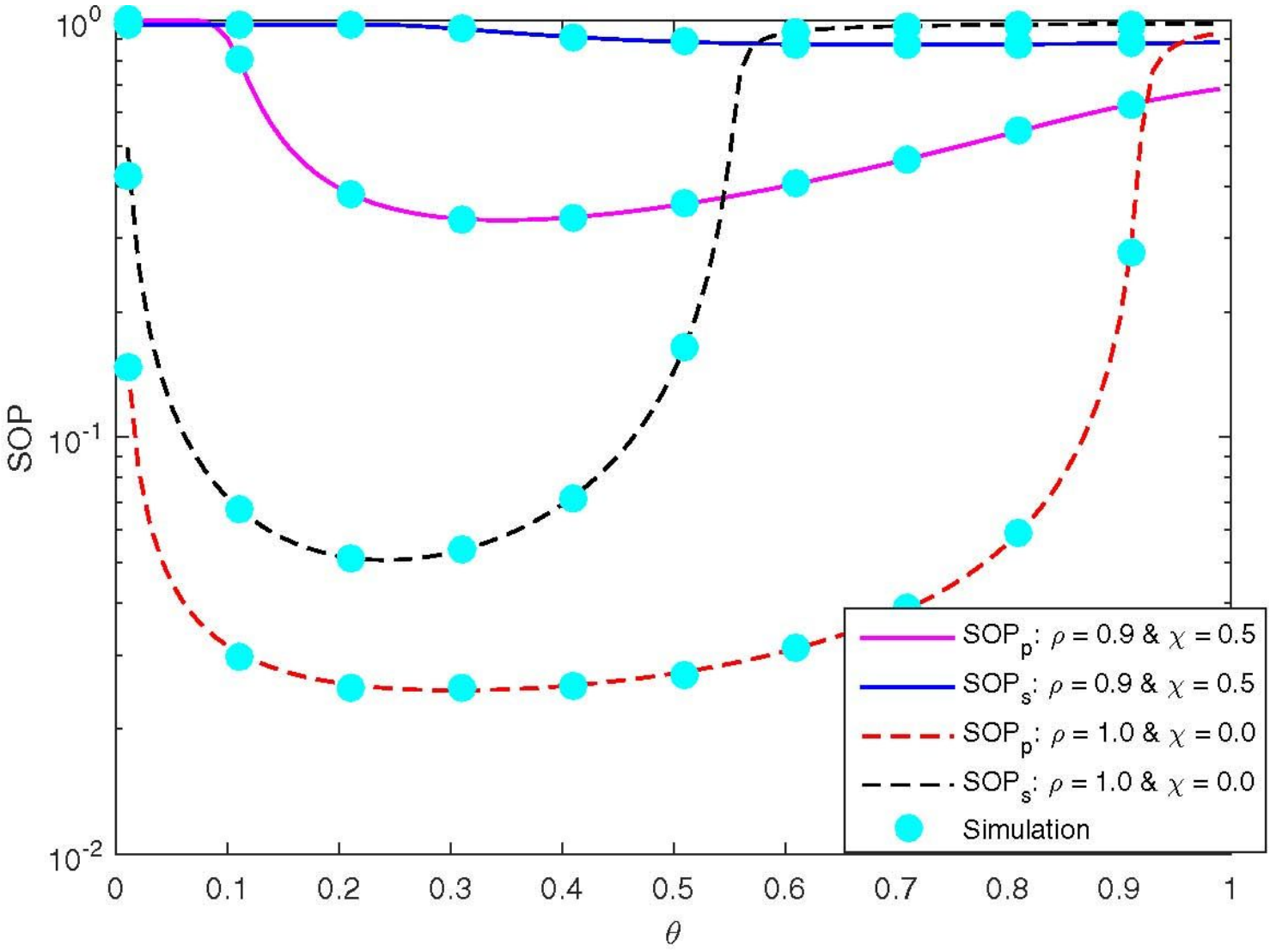

Figure 5

SOPs versus θ.

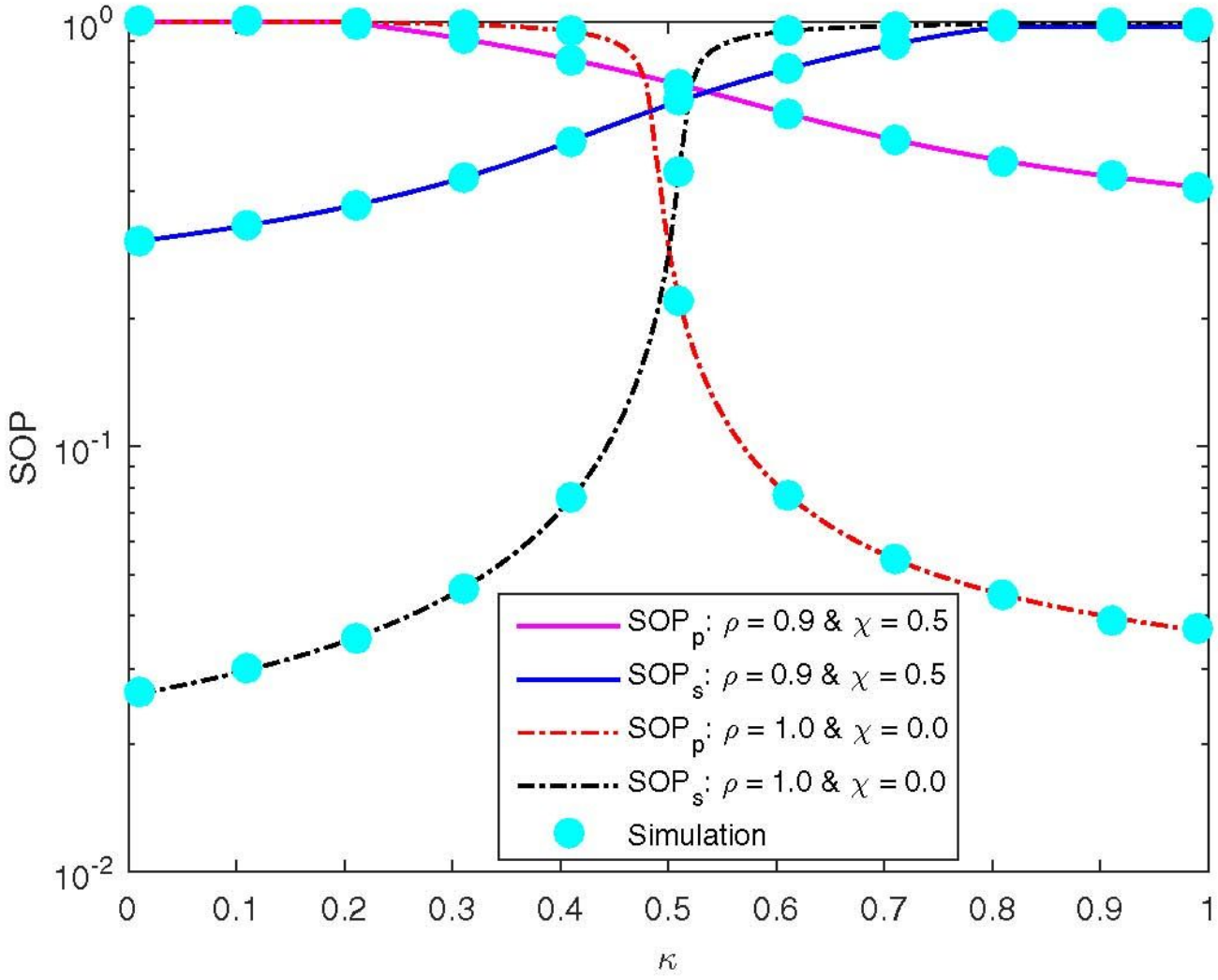

Figure 6

SOPs versus κ.

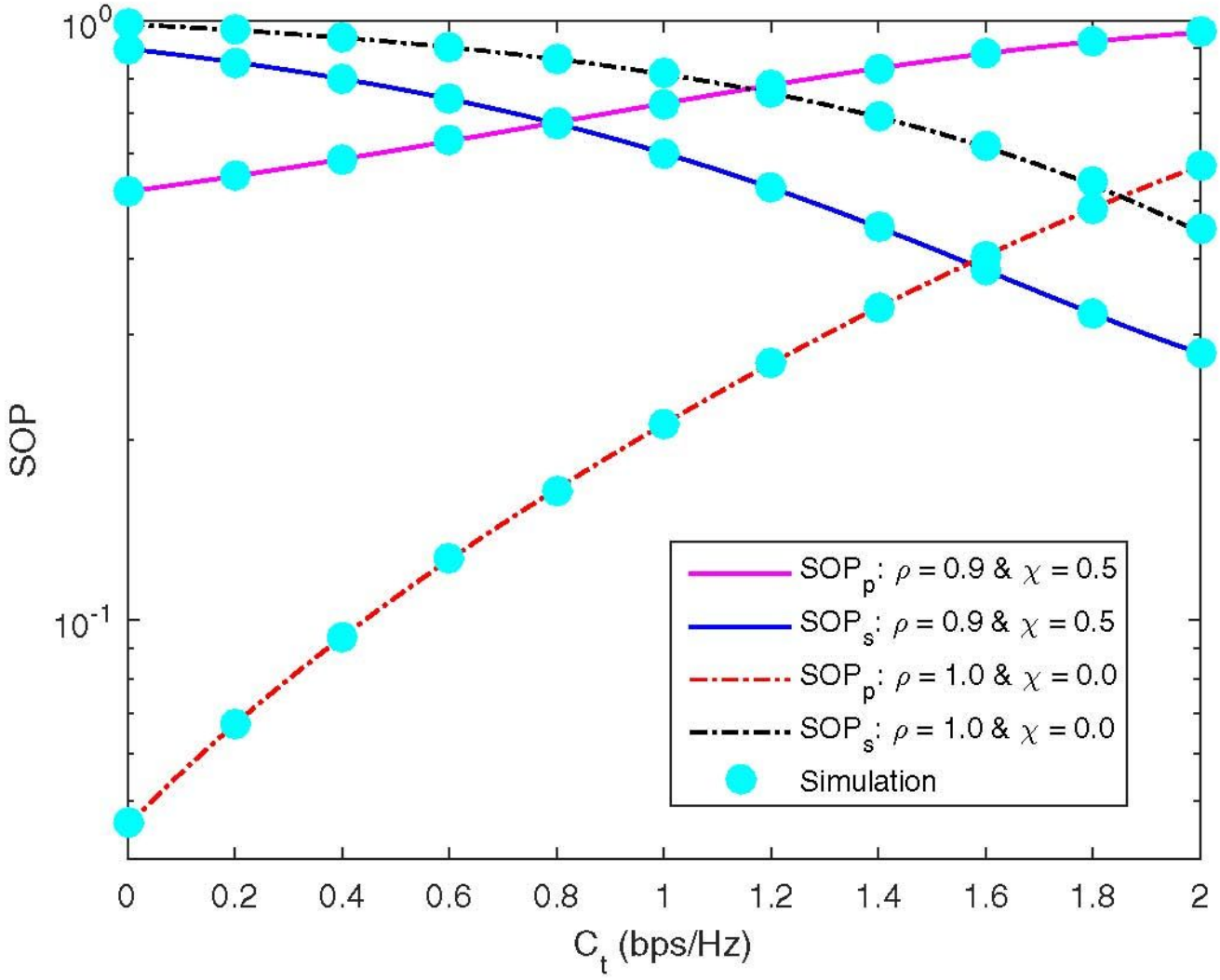

Figure 7

SOPs versus Ct.

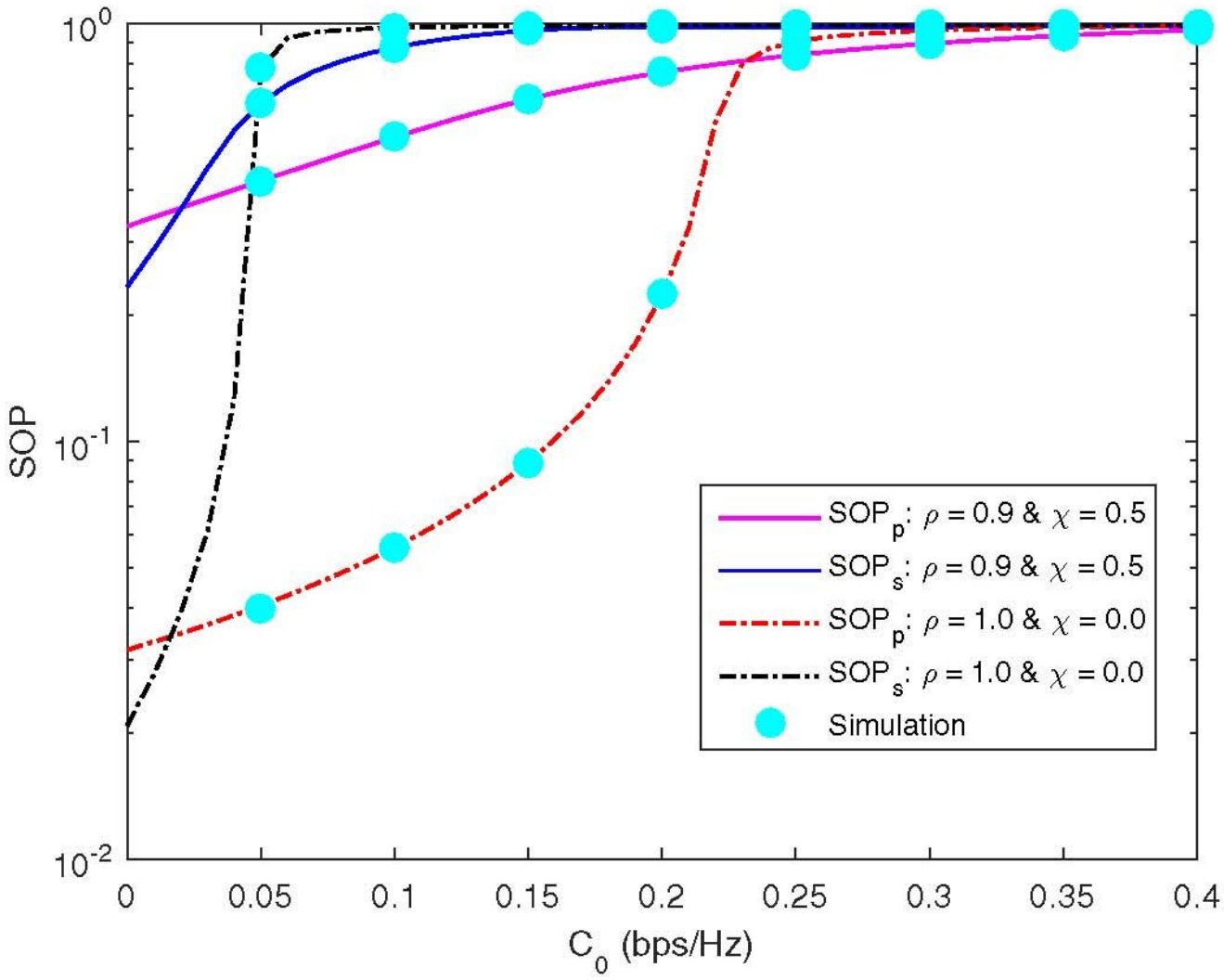

Figure 8

SOPs versus C0.

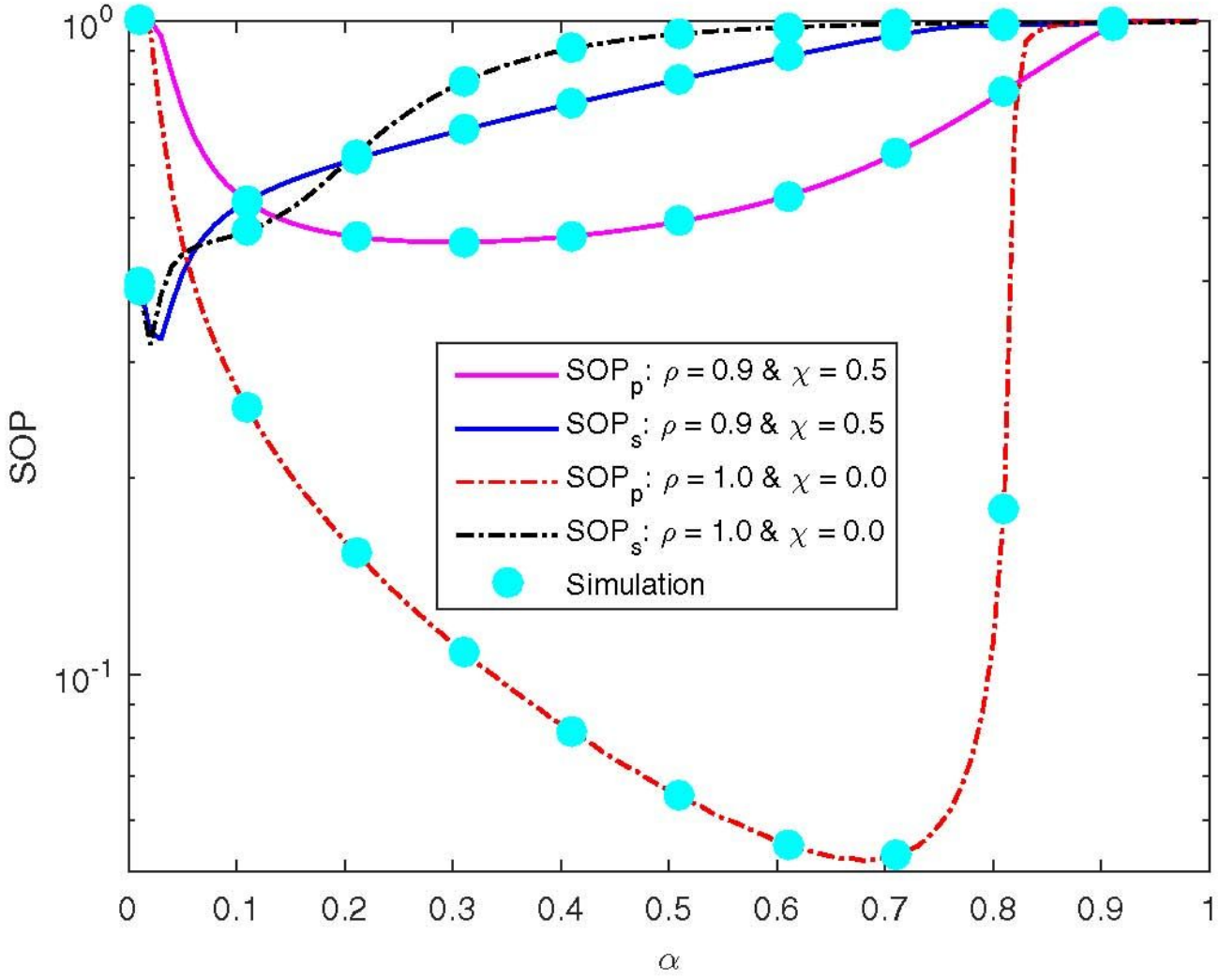

Figure 9

SOPs versus α.

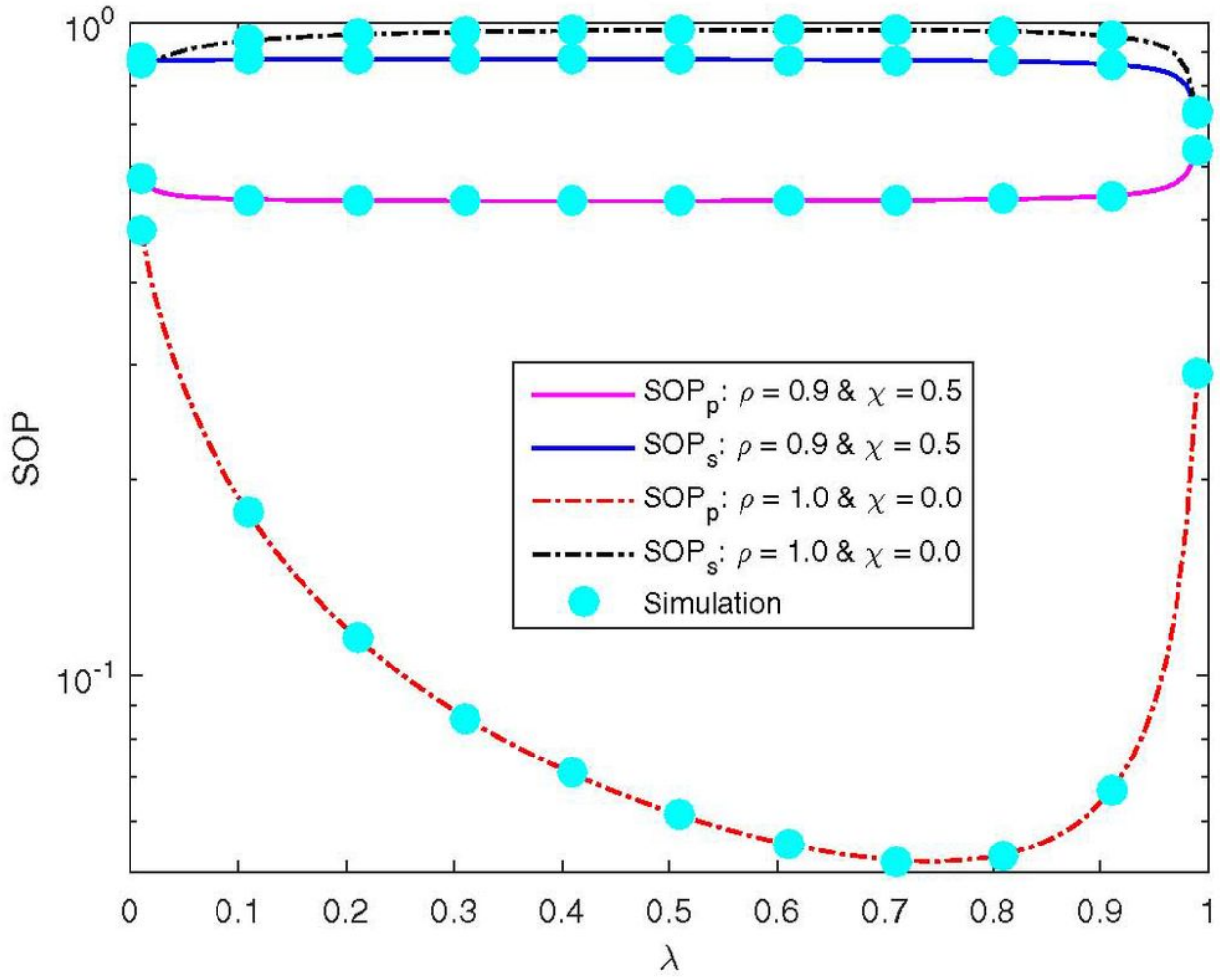

Figure 10

SOPs versus λ.

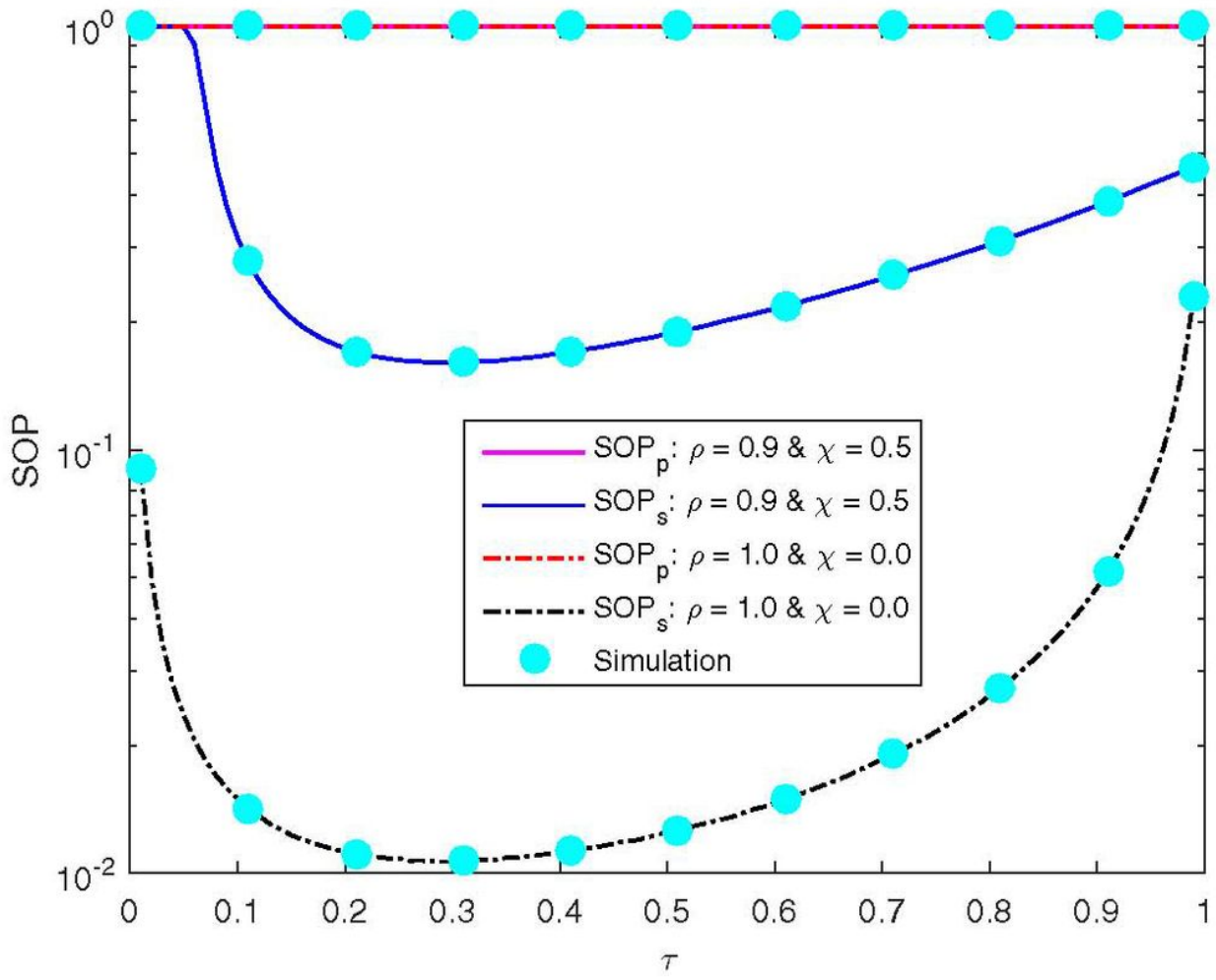

Figure 11

SOPs versus τ.

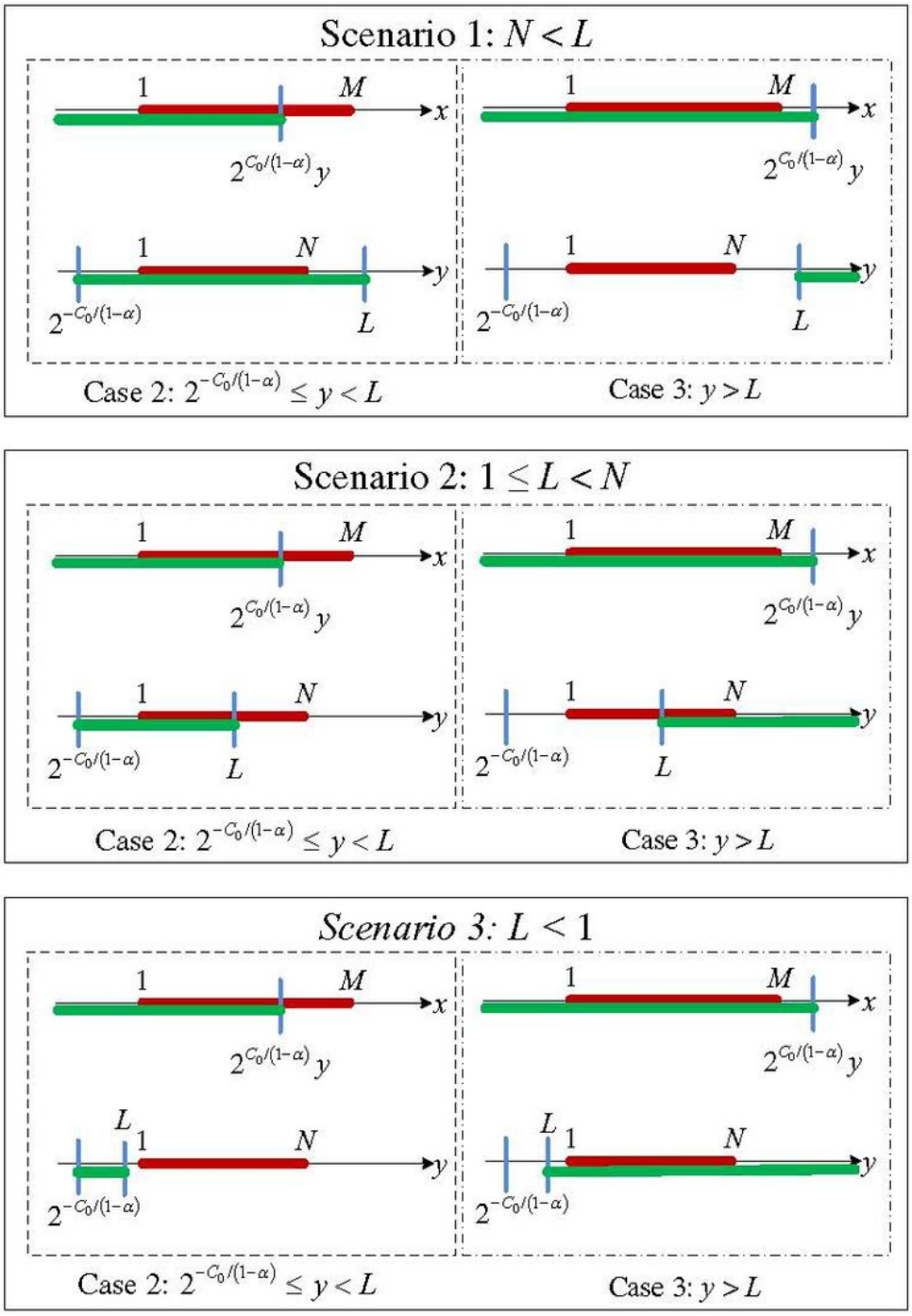

Figure 12

Scenarios for computing Y.