Impact of channel estimation-and-artificial noise cancellation imperfection on artificial noise-aided energy harvesting overlay networks

Khuong Ho-Van 1,2 · Thiem Do-Dac 1,2,3

Accepted: 6 June 2021 / Published online: 5 July 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

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.

Keywords Overlay · Secrecy outage probability · Energy harvesting · Channel estimation imperfection · Artificial noise cancellation

1 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 [1–4]. 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, ...) [5]. 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 [6].

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 improv-
ing spectral efficiency and mitigating spectrum scarcity issue [7]. 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 the 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 these solutions, RF (Radio Frequency) energy harvesting can be integrated into (5G/6G mobile or IoT) users to supply energy, extend the life-time of wireless devices, and improve energy efficiency since it requires simple energy harvesting circuits [8–10].

EHONs (Energy Harvesting Overlay Networks) can exploit simultaneously advantages of two feasible (energy harvesting and cognitive radio) technologies to meet several standards of advanced wireless networks requiring high energy-and-spectral efficiencies [11]. 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 [12]. 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 [13]. Therefore, this paper applies artificial noise in EHONs to secure primary/secondary communication.

Most references (e.g., [14–21]) 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 impacting 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 (Artificial Noise-aided EHONs). Therefore, this paper evaluates the effect of artificial noise cancellation-and-channel estimation imperfection on security performance of PUs/CRs in ANaEHON.

1.1 Prior works and motivations

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. Data 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 [14–21,23]. More specifically, [14] and [15] 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 [16], a dedicated jammer was employed to interfere the eavesdropper instead of the primary receiver as [14] and [15]. In addition, [16] differs [14] and [15] 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 [25], 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 [26]. To further secure primary transmission, [17] proposed to jam the eavesdropper by the primary receiver as well as the dedicated jammer. However, security performance of primary/secondary communication in terms of SOP (Secrecy Outage Probability) was not analyzed in [14–17]. In [23], the transmit antenna selection and the multi-user scheduling were proposed to secure EHONs. Moreover, the SOP of primary communication and the ergodic rate of secondary communication were derived in closed-form in [23]. Recently, [18] proposed a group of dedicated jammers to guarantee communication security for the secondary transmitter in EHONs. Moreover, the SOP of secondary/primary communication was analyzed in [18]. Nonetheless, different from [14–17], the secondary user relays the primary signal

1 [24] investigated the same system model as [14] and [15]. Nonetheless, the energy source which the secondary transmitter scavenges is not RF signals, significantly simplifying the analysis in [24]. Furthermore, [24] ignored artificial noise. Consequently, references such as [24] are not related works for survey.
and transmits its private signal separately in [18] and [23]. This significantly mitigates complexity in analyzing the SOP and hence, making the analysis in [18] and [23] tractable.

Although [18] proposed the SOP analysis for both primary and secondary communication and [23] analyzed the SOP/ergodic rate of primary/secondary 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 primary communication, Stage II: secondary communication to PU, Stage III: secondary communication to SU) to complete both secondary and primary communication, considerably reducing spectral efficiency. Recently, [19–21] proposed a two-stage transmission scheme with artificial noise generation in EHONs to enhance secrecy performance and spectral efficiency. More specifically, [19–21] suggested an ANaEHON where the secondary transmitter performed a superposition of artificial noise, secondary signal, and primary signal to transmit at once. Furthermore, [19–21] proposed the SOP analysis.

In summary, imperfect channel estimation and artificial noise cancellation are ineluctable in practical systems. Nonetheless, none of the prior works in [14–21,23] analyzed the SOP of both primary and secondary communication in ANaEHONs under their impact as summarized in Table 1. This motivates the current paper to study their impact on security performance of ANaEHON in [19–21] for the first time.

1.2 Contributions

The following are our contributions:

- Suggest a novel signal model for ANaEHONs accounting for channel estimation-and-artificial noise cancellation imperfection. In ANaEHONs under consideration, the secondary transmitter harvests energy in primary signals, decodes and forwards primary data, and generates a signal combination of primary data, secondary data, and artificial noise. Such an operation mechanism of the secondary transmitter 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 rating security metrics of primary/secondary 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 optimal secrecy capability and the best performance compromise between primary and secondary communication.

- Provide insightful results on security performance of primary/secondary communication in important system parameters.

1.3 Structure

Section 2 discusses the system model. Then, Section 3 derives the SOP of primary/secondary communication. Next, Section 4 provides illustrative results and ultimately, Section 5 closes the paper.

2 System description

2.1 System model

Figure 1 shows an ANaEHON in which direct communication between a primary transmitter-receiver pair, \( PT \rightarrow PR \), is not of good quality owing to uncertainties (e.g., long distance, severe 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 spends the scavenged energy for its communication operation. Additionally, the overlay mechanism is applied to \( ST \) in order for \( ST \) to relay the \( PT \)'s signal to \( PR \) as well as send 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 \( ST \).

2.2 Channel model

Table 2 summarizes main notations used throughout this paper. More specifically, as shown in Fig. 1, \( h_{ps}, h_{sp}, h_{sr} \) 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 \( h_{ps} \sim \mathcal{CN}(0, \mu_{ps}), h_{sp} \sim \mathcal{CN}(0, \mu_{sp}), h_{sr} \sim \mathcal{CN}(0, \mu_{sr}) \), and \( h_{sr} \sim \mathcal{CN}(0, \mu_{sr}) \), respectively. Such a channel model indicates Rayleigh fading. Path-loss can be incorporated into \( \mu_{uv} \) with \( u \in \{ p, s \} \) and \( v \in \{ s, p, r, e \} \) as \( \mu_{uv} = d_{uv}^{-\zeta} \) in which \( \zeta \) is the path-loss exponent and \( d_{uv} \) is the u-v distance. Then, the probability density function (PDF) and the cumulative distribution function (CDF) of \( |h_{uv}|^2 \) are correspondingly expressed as \( f_{|h_{uv}|^2}(x) = e^{-x/\mu_{uv}}/\mu_{uv} \) and \( F_{|h_{uv}|^2}(x) = 1 - e^{-x/\mu_{uv}} \), where \( x \geq 0 \).
Table 1  Summary of related references and comparison between our work and related references

| Reference | Analyze SOP of primary communication? | Analyze SOP of secondary communication? | Consider imperfect channel estimation and artificial noise cancellation? |
|-----------|--------------------------------------|----------------------------------------|---------------------------------------------------------------|
| [14–17]   | No                                   | No                                     | No                                                            |
| [23]      | Yes                                  | No                                     | No                                                            |
| [18–21]   | Yes                                  | Yes                                    | No                                                            |
| Our work  | Yes                                  | Yes                                    | Yes                                                           |

---

Fig. 1  System model

**2.3 Signal model**

In Fig. 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 $\alpha T$ with $\alpha \in (0, 1)$ being the time splitting factor is for $PT$ to send its private data $x_p$ in order for $ST$ to harvest energy with the power splitting technique and recover the $PT$’s information. Such a technique separates the received signal at $ST$, $y_s$, 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 as shown in the flow chart of Fig. 2. To be specific, if $ST$ successfully restores the $PT$’s information, it sends a combination of three signals $\sqrt{\theta}x_p x_p + \sqrt{\theta (1-\theta)} x_s + \sqrt{(1-\theta)} x_a$ ($x_p$, $\theta$ $\in (0, 1)$).}

---

$^2$ Decoding with infinitesimal power is assumed. This assumption is popularized in previous publications (e.g., [16,27–29]).

$^3$ In [16], Stage II allows $ST$ to always relay primary data, leading to error propagation for primary data. Nonetheless, the secondary/primary SOP analysis was dissembled in [16]. Consequently, error propagation was not considered in the SOP analysis.
Table 2  Summary of Symbols

| Symbol | Meaning |
|--------|---------|
| $C_t$  | Transmission rate required by $ST$ |
| $C_0$  | Required secrecy capacity |
| $d_{uv}$ | Distance between transmitter $u$ and receiver $v$ |
| $s_p$  | Transmit symbol of $PT$ |
| $s_t$  | Transmit symbol of $ST$ |
| $s_a$  | Artificial noise |
| $P_p$  | Transmit power of $PT$ |
| $P_r$  | 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 |
| $\mu_{ps}$ | Fading power of $PT$ − $ST$ channel |
| $\mu_{sp}$ | Fading power of $ST$ − $PR$ channel |
| $\mu_{se}$ | Fading power of $ST$ − $E$ channel |
| $\mu_{sr}$ | 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 |
| $Pr[Z]$ | Probability of the event $Z$ |
| $Z \sim CN(0, m)$ | Zero-mean $m$-variance circular symmetric complex Gaussian random variable |
| $\alpha$ | Time splitting factor |
| $\gamma_s$ | SNR at $ST$ |
| $\gamma_e$ | SINR at $E$ |
| $\gamma_r$ | SINR at $SR$ |
| $\gamma_p$ | SINR at $PR$ |
| $\theta$ | Power allocation factor for desired signals and artificial noise when $ST$ decodes successfully $PT$’s signal |
| $\tau$ | Power allocation factor for artificial noise and secondary signal as $ST$ decodes incorrectly $PT$’s signal |
| $\kappa$ | Power allocation factor for primary and secondary signals |
| $\zeta$ | Path-loss exponent |
| $\rho_{uv}$ | Correlation coefficient between true and estimated channels |
| $\chi$ | Artificial noise residue level |
| $\lambda$ | Power splitting factor |
| $\eta$  | Energy conversion efficiency |
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 xₚ, the ST’s private information xₛ, and the artificial noise xₐ. In the case that ST unsuccessfully decodes the primary data, it sends a combination of two signals \(\sqrt{\tau} Pₛ xₛ + \sqrt{(1-\tau)} Pₛ xₐ\) (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 xₛ and the artificial noise xₐ. 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

\[yₛ = hₚₛ \sqrt{Pₚ} xₚ + nₛ.\] (1)

In (1), the receive antenna at ST induces the noise \(nₛ \sim CN(0, \sigma^2ₛ)\) and PT transmits with power of \(Pₚ\).

Stage I in Fig. 1 offers ST the scavenged energy as

\[Eₛ = \eta \mathbb{E} \left( \left| \sqrt{\lambda} yₛ \right|^2 \right) \alpha T = \alpha \eta \lambda \left( Pₚ \mu_{ₚₛ} + \sigma^2ₛ \right) T.\] (2)

where \(\eta \in (0, 1)\) is the energy conversion efficiency and \(\mathbb{E}[-]\) is the expectation operator.

The scavenged energy \(Eₛ\) offers the transmit power of ST in Stage II as

\[Pₛ = \frac{Eₛ}{(1-\alpha)T} = \frac{\alpha \eta \lambda}{1-\alpha} \left( Pₚ \mu_{ₚₛ} + \sigma^2ₛ \right).\] (3)

Figure 1 shows that the signal used for decoding the PT’s information is \(\tilde{y}_ₛ = \sqrt{1-\lambda} yₛ + \bar{n}_ₛ\) where \(\bar{n}_ₛ \sim CN(0, \sigma^2ₛ)\) is the noise owing to the passband-to-baseband signal conversion. Inserting (1) into \(\tilde{y}_ₛ\) yields

\[\tilde{y}_ₛ = \sqrt{(1-\lambda)} Pₚ hₚₛ xₚ + \sqrt{1-\lambda} nₛ + \bar{n}_ₛ.\] (4)

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 \([22]\)

\[\hat{h}_{uv} = \rho_{uv} h_{uv} + \sqrt{1-\rho^2_{uv}} e_{uv}\] (5)
where $h_{uv}$ is the true channel, $\hat{h}_{uv}$ is the estimated channel, $\epsilon_{uv}$ is the estimation error; all random variables $h_{uv}$, $\hat{h}_{uv}$, $\epsilon_{uv}$ are modelled as $CN(0, \mu_{uv})$; the correlation coefficient $0 \leq \rho_{uv} \leq 1$ is a constant, representing the exactness of channel estimation.

Inserting (5) into (4), one obtains

$$y_p = \begin{cases} h_{sp} \left( \sqrt{\theta} P_s x_p + \sqrt{\theta (1-\kappa)} P_s x_s + \sqrt{(1-\theta)} P_s x_a \right) + n_p, & y_s \geq y_t \quad (9) \\ h_{sp} \left( \sqrt{\theta} P_s x_p + \sqrt{(1-\tau)} P_s x_a \right) + n_p, & y_s < y_t \end{cases}$$

$$y_r = \begin{cases} h_{sr} \left( \sqrt{\theta} P_s x_p + \sqrt{\theta (1-\kappa)} P_s x_s + \sqrt{(1-\theta)} P_s x_a \right) + n_r, & y_r \geq y_t \quad (10) \\ h_{sr} \left( \sqrt{\theta} P_s x_s + \sqrt{(1-\tau)} P_s x_a \right) + n_r, & y_r < y_t \end{cases}$$

$$y_e = \begin{cases} h_{se} \left( \sqrt{\theta} P_s x_p + \sqrt{\theta (1-\kappa)} P_s x_s + \sqrt{(1-\theta)} P_s x_a \right) + n_e, & y_e \geq y_t \quad (11) \\ h_{se} \left( \sqrt{\theta} P_s x_s + \sqrt{(1-\tau)} P_s x_a \right) + n_e, & y_e < y_t \end{cases}$$

$$\tilde{y}_s = \sqrt{(1-\chi)} P_p \left( \frac{\tilde{h}_{ps}}{\rho_{ps}} + \frac{1 - \rho_{ps}^2}{\rho_{ps}^2} \epsilon_{ps}^2 x_p \right) + \sqrt{1 - \lambda n_s + \tilde{n}_s}$$

$$= \sqrt{(1-\lambda)} P_p \left( \frac{(1-\rho_{ps}^2) \epsilon_{ps}^2 x_p}{\rho_{ps}} + \sqrt{(1-\lambda) n_s + \tilde{n}_s} \right). \quad (6)$$

It is inferred from (6) that the SNR (Signal-to-Noise Ratio) achievable for decoding the $PT$’s information is given by

$$\gamma_s = \mathbb{E} \left\{ \left( \frac{\sqrt{(1-\lambda)} P_p \tilde{h}_{ps} x_p}{\rho_{ps}} \right)^2 \right\}$$

$$= D \left( \tilde{h}_{ps} \right)^2, \quad (7)$$

where

$$D = \frac{P_p}{\mu_{ps} + \left( \sigma_s^2 + \frac{\tilde{n}_s^2}{1-\lambda} \right) \rho_{ps}^2}. \quad (8)$$

The channel capacity that $ST$ can obtain is $C_s = \alpha \log_2 (1 + \gamma_s)$ bps/Hz with the pre-logarithm factor $\alpha$ owing to Stage I of $\phi T$. The communication theory addressed that $ST$ decodes exactly the $PT$’s data merely if $C_s$ exceeds the required transmission rate $C_t$, i.e., $C_s \geq C_t$ (or $\gamma_s \geq \gamma_t$ 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

$$\sqrt{\theta} P_s x_p + \sqrt{\theta (1-\kappa)} P_s x_s + \sqrt{(1-\theta)} P_s x_a$$

in Stage II. Otherwise, it broadcasts the combination of solely two signals in the form of

$$\sqrt{\theta} P_s x_s + \sqrt{(1-\tau)} P_s x_a$$

in Stage II. Therefore, $PR, SR$, and $E$ receive signals in Stage II, correspondingly, as

$$\tilde{y}_p = \begin{cases} h_{sp} \left( \sqrt{\theta} P_s x_p + \sqrt{\theta (1-\kappa)} P_s x_s \right) + n_p, & y_s \geq y_t \quad (12) \\ h_{sp} \left( \sqrt{\theta} P_s x_s + \sqrt{(1-\tau)} P_s x_a \right) + n_p, & y_s < y_t \end{cases}$$

$$\tilde{y}_r = \begin{cases} h_{sr} \left( \sqrt{\theta} P_s x_p + \sqrt{(1-\theta)} P_s x_a \right) + n_r, & y_r \geq y_t \quad (13) \\ h_{sr} \left( \sqrt{\theta} P_s x_s + \sqrt{(1-\theta)} P_s x_a \right) + n_r, & y_r < y_t \end{cases}$$

Inserting (5) into (12), one obtains

$$\tilde{y}_p = \begin{cases} h_{sp} \left( \sqrt{\theta} P_s x_p + \sqrt{\theta (1-\kappa)} P_s x_s \right) + n_p, & y_s \geq y_t \quad (12) \\ h_{sp} \left( \sqrt{\theta} P_s x_s + \sqrt{(1-\tau)} P_s x_a \right) + n_p, & y_s < y_t \end{cases}$$

$$\tilde{y}_r = \begin{cases} h_{sr} \left( \sqrt{\theta} P_s x_p + \sqrt{(1-\theta)} P_s x_a \right) + n_r, & y_r \geq y_t \quad (13) \\ h_{sr} \left( \sqrt{\theta} P_s x_s + \sqrt{(1-\theta)} P_s x_a \right) + n_r, & y_r < y_t \end{cases}$$
Based on (16), SINR (Signal-to-Interference plus Noise Ratio) for decoding $x_p$ at $PR$ is represented as

$$
\gamma_p = \begin{cases} 
\mathbb{E}\left[ \frac{\sqrt{h_{p\!\!t}}^2}{||\hat{h}_{p\!\!p}\!_{x_p}||^2} \right], & \gamma_s \geq \gamma_t \\
\frac{\theta \kappa P_s}{\rho_{p\!\!t}} \frac{|\hat{h}_{p\!\!p}\!_{x_p}|^2}{\rho_{p\!\!t}} + \frac{\theta \kappa P_s}{\rho_{p\!\!t}} \frac{|\hat{h}_{p\!\!p}\!_{x_p}|^2}{\rho_{p\!\!t}} \left( \sqrt{h_{s\!\!t}}^2 x_p + \sqrt{h_{s\!\!s}}^2 x_s + \sqrt{h_{s\!\!a}}^2 x_a \right) + n_r, & \gamma_s < \gamma_t 
\end{cases}
$$

Similarly, inserting (5) into (13), one obtains

$$
\tilde{\gamma}_r = \begin{cases} 
\mathbb{E}\left[ \frac{\sqrt{h_{r\!\!t}}^2}{||\hat{h}_{r\!\!r}\!_{x_r}||^2} \right], & \gamma_s \geq \gamma_t \\
\frac{\theta \kappa P_s}{\rho_{r\!\!t}} \frac{|\hat{h}_{r\!\!r}\!_{x_r}|^2}{\rho_{r\!\!t}} + \frac{\theta \kappa P_s}{\rho_{r\!\!t}} \frac{|\hat{h}_{r\!\!r}\!_{x_r}|^2}{\rho_{r\!\!t}} \left( \sqrt{h_{s\!\!t}}^2 x_p + \sqrt{h_{s\!\!s}}^2 x_s + \sqrt{h_{s\!\!a}}^2 x_a \right) + n_r, & \gamma_s < \gamma_t 
\end{cases}
$$

Based on (16), SINR for decoding $x_s$ at $SR$ is given by

$$
\gamma_r = \begin{cases} 
\mathbb{E}\left[ \frac{\sqrt{h_{r\!\!t}}^2}{||\hat{h}_{r\!\!r}\!_{x_s}||^2} \right], & \gamma_s \geq \gamma_t \\
\frac{\theta \kappa P_s}{\rho_{r\!\!t}} \frac{|\hat{h}_{r\!\!r}\!_{x_s}|^2}{\rho_{r\!\!t}} + \frac{\theta \kappa P_s}{\rho_{r\!\!t}} \frac{|\hat{h}_{r\!\!r}\!_{x_s}|^2}{\rho_{r\!\!t}} \left( \sqrt{h_{s\!\!t}}^2 x_p + \sqrt{h_{s\!\!s}}^2 x_s + \sqrt{h_{s\!\!a}}^2 x_a \right) + n_r, & \gamma_s < \gamma_t 
\end{cases}
$$
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 (11). Inserting (5) into (11) results in

$$y_{e} = \left\{ \begin{array}{l} \left( \frac{h_{se}}{\rho_{se}} - \sqrt{\frac{1-\rho_{se}^{2}}{\rho_{se}}} \varepsilon_{se}\right) \left( \sqrt{\theta_{s} P_{s} x_{p} + \sqrt{\theta} (1-\kappa) P_{s} x_{s} + \sqrt{(1-\theta)} P_{s} x_{a}} + n_{e}, \quad \gamma_{s} \geq \gamma_{t} \right) \\
\left( \frac{h_{se}}{\rho_{se}} - \sqrt{\frac{1-\rho_{se}^{2}}{\rho_{se}}} \varepsilon_{se}\right) \left( \sqrt{\tau P_{s} x_{s} + \sqrt{(1-\tau)} P_{s} x_{a}} + n_{e}, \quad \gamma_{s} < \gamma_{t} \right) \end{array} \right. \tag{18}$$

from which the SINRs at $E$ for restoring $x_{s}$ and $x_{p}$ are respectively derived as

$$y_{Es} = \left\{ \begin{array}{l} \left( \frac{h_{se}}{\rho_{se}} - \sqrt{\frac{1-\rho_{se}^{2}}{\rho_{se}}} \varepsilon_{se} \right) \left( \frac{\sqrt{\theta_{s} P_{s} x_{s} + \sqrt{\theta} (1-\kappa) P_{s} x_{s} + \sqrt{(1-\theta)} P_{s} x_{a}} + n_{e}}{\sqrt{\tau P_{s} x_{s} + \sqrt{(1-\tau)} P_{s} x_{a}} + n_{e}}, \quad \gamma_{s} \geq \gamma_{t} \right) \\
\left( \frac{h_{se}}{\rho_{se}} - \sqrt{\frac{1-\rho_{se}^{2}}{\rho_{se}}} \varepsilon_{se} \right) \left( \frac{\sqrt{\theta_{s} P_{s} x_{s} + \sqrt{\theta} (1-\kappa) P_{s} x_{s} + \sqrt{(1-\theta)} P_{s} x_{a}} + n_{e}}{\sqrt{\tau P_{s} x_{s} + \sqrt{(1-\tau)} P_{s} x_{a}} + n_{e}}, \quad \gamma_{s} < \gamma_{t} \right) \end{array} \right. \tag{19}$$

$$y_{Ep} = \left\{ \begin{array}{l} \left( \frac{h_{se}}{\rho_{se}} - \sqrt{\frac{1-\rho_{se}^{2}}{\rho_{se}}} \varepsilon_{se} \right) \left( \frac{\sqrt{\theta_{s} P_{s} x_{s} + \sqrt{\theta} (1-\kappa) P_{s} x_{s} + \sqrt{(1-\theta)} P_{s} x_{a}} + n_{e}}{\sqrt{\tau P_{s} x_{s} + \sqrt{(1-\tau)} P_{s} x_{a}} + n_{e}}, \quad \gamma_{s} \geq \gamma_{t} \right) \\
\left( \frac{h_{se}}{\rho_{se}} - \sqrt{\frac{1-\rho_{se}^{2}}{\rho_{se}}} \varepsilon_{se} \right) \left( \frac{\sqrt{\theta_{s} P_{s} x_{s} + \sqrt{\theta} (1-\kappa) P_{s} x_{s} + \sqrt{(1-\theta)} P_{s} x_{a}} + n_{e}}{\sqrt{\tau P_{s} x_{s} + \sqrt{(1-\tau)} P_{s} x_{a}} + n_{e}}, \quad \gamma_{s} < \gamma_{t} \right) \end{array} \right. \tag{20}$$

It is worth emphasizing from (19) and (20) 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 (15), (17), (19), (20) weighted by $1 - \rho_{se}^{2}$, degrades the performance of all receivers ($PR, SR, E$).

2.4 Secrecy capacity

The channel capacities at $PR$ and $SR$ in Stage II are inferred from (15) and (17), correspondingly, as

$$C_{p} = (1 - \alpha) \log \left( 1 + y_{p} \right), \tag{21}$$

$$C_{r} = (1 - \alpha) \log \left( 1 + y_{r} \right), \tag{22}$$

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 (19) and (20), correspondingly, as

$$C_{Es} = (1 - \alpha) \log \left( 1 + y_{Es} \right), \tag{23}$$

$$C_{Ep} = (1 - \alpha) \log \left( 1 + y_{Ep} \right). \tag{24}$$

The substraction of the channel capacity at $E$ for restoring $x_{s}$ from that at $SR$ is the secrecy capacity for $x_{s}$:

$$\hat{C}_{s} = \left[ C_{r} - C_{Es} \right]^{+} = (1 - \alpha) \left[ \log \frac{1 + \gamma_{r}}{1 + y_{Es}} \right]^{+}, \tag{25}$$
where \([x]^+\) denotes \(\max(x, 0)\).

Similarly, the subtraction of the channel capacity at \(E\) for restoring \(x_p\) from that at \(PR\) is the secrecy capacity for \(x_p\):

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

(26)

### 3 SOP analysis

The SOP indicates the possibility that the secrecy capacity is below the preset security threshold \(C_0\). Therefore, it quantifies the secrecy performance of ANaEHON. This section suggests precise closed-form SOP formulas for quickly rating 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.

#### 3.1 SOP for primary information \(x_p\)

The SOP for primary information \(x_p\) is given by

\[
SOP_p(C_0) = \Pr \left\{ \hat{C}_p < C_0 \right\}.
\]  

(27)

\(SOP_p(C_0)\) is divided into two scenarios: \(i\) one corresponds to the \(ST\’s\) unsuccessful decoding primary data and \(ii\) another corresponds to the \(ST\’s\) successful decoding primary data, i.e.

\[
SOP_p(C_0) = \Pr \left\{ \hat{C}_p < C_0 \mid C_s < C_I \right\} \Pr \{ C_s < C_I \}
\]

\[
+ \Pr \left\{ \hat{C}_p < C_0 \mid C_s \geq C_I \right\} \Pr \{ C_s \geq C_I \}.
\]  

(28)

Substituting \(\hat{C}_p\) in (26) into (28), one has

\[
SOP_p(C_0) = \Pr \left\{ \gamma_s = D \left| \hat{h}_{ps} \right|^2 \geq \gamma_t \right\} = e^{-\gamma_t/(\eta_p D)}.
\]  

(30)

In ANaEHONs, if \(ST\) unsuccessfully decodes the \(PT\’s\) data, it doesn’t forward primary data, yielding the zero SINR at \(PR\) for restoring \(x_p\) (i.e., \(\gamma_p = 0\) for \(\gamma_s < \gamma_t\) as shown in (15)). Therefore, in this scenario, the secrecy capacity for \(x_p\) is also zero (i.e., \(\hat{C}_p = 0\) conditioned on \(\gamma_s < \gamma_t\)), resulting in \(\psi = 1\).

The term \(\Upsilon\) in (29) is rewritten after using (15) and (20) for the case of \(\gamma_s \geq \gamma_t\) as

\[
\Upsilon = \Pr \left\{ X < 2^{C_0/(1-\alpha)} y \right\},
\]  

(31)

where

\[
X = 1 + \frac{A \left| \hat{h}_{sp} \right|^2}{B \left| \hat{h}_{sp} \right|^2 + \tilde{\sigma}_p^2},
\]  

(32)

\[
Y = 1 + \frac{A \left| \hat{h}_{se} \right|^2}{C \left| \hat{h}_{se} \right|^2 + \tilde{\sigma}_e^2},
\]  

(33)

with

\[
A = \theta \kappa P_t,
\]  

(34)

\[
B = \left[ \theta (1 - \kappa) + \chi^2 (1 - \theta) \right] P_s,
\]  

(35)

\[
C = (1 - \theta \kappa) P_s,
\]  

(36)

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

(37)

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

(38)

By imitating the derivations in [21, Appendix C], one achieves a precise form of \(\Upsilon\) as

\[
\Upsilon = \begin{cases} 
1 - U e^{\eta_p A + \eta_{se} C} \Lambda, & N < L \\
1 - U e^{\eta_p A + \eta_{se} C} \varphi, & 1 \leq L < N \\
1, & L < 1
\end{cases}
\]  

(39)

where

\[
M = 1 + A/B.
\]  

(40)

\[
N = 1 + A/C.
\]  

(41)

\[
L = 2^{-C_0/(1-\alpha)} M.
\]  

(42)

\[
J = \frac{\tilde{\sigma}_p^2 A}{\mu_{sp} B^2} 2^{-C_0/(1-\alpha)}.
\]  

(43)

\[
U = \frac{\tilde{\sigma}_e^2 A}{\mu_{se} C^2}.
\]  

(44)

\[
\Lambda = \frac{J}{N-N-1} \left[ e^{-U/(N-1)} - U e^{U/(L-N)} (N-L)^2 Ei(-UV) + \sum_{q=1}^{\infty} \frac{J! (-U)^{q-1}}{(N-L)^2 (q-1)!} \left( e^{-U/(L-N)} - e^{-U/(N-N)} \right) \right].
\]  

(45)

\[
V = (N-1)^{-1} - (N-L)^{-1}.
\]  

(46)
the precise closed-form expression of \( x_s \) is given by

\[
SOP_s (C_0) = \Pr \left\{ \hat{C}_s < C_0 \right\}.
\]  

(48)

\( SOP_s \) is divided into two scenarios: \( i \) one corresponds to the ST’s unsuccessful decoding primary data and \( ii \) another corresponds to the ST’s successful decoding primary data, i.e.

\[
SOP_s (C_0) = \Pr \left\{ \hat{C}_s < C_0 \bigg| C_s < C_t \right\} \Pr \{ C_s < C_t \} + \Pr \left\{ \hat{C}_s < C_0 \bigg| C_s \geq C_t \right\} \Pr \{ C_s \geq C_t \}.
\]  

(49)

Substituting \( \hat{C}_s \) in (25) into (49), one has

\[
SOP_s (C_0) = \Pr \left\{ \hat{C}_s < C_0 \bigg| C_s < C_t \right\} \Pr \{ C_s < C_t \} + \Pr \left\{ \hat{C}_s < C_0 \bigg| C_s \geq C_t \right\} \Pr \{ C_s \geq C_t \}.
\]  

(50)

The term \( \Delta \) in (50) was already computed in (30) while the term \( Z_1 \) in (50) is rewritten after using (17) and (19) for the case of \( \gamma_s \geq \gamma_t \) as

\[
Z_1 = \Pr \left\{ \frac{A_1 \sigma^2}{B_1 \sigma^2} \left( 1 + \frac{A_1 \sigma^2}{B_1 \sigma^2} \right) < 2 \right\},
\]  

(51)

where

\[
A_1 = \theta (1 - \kappa) P_s,
\]  

(52)

\[
B_1 = \left( \theta \kappa + \chi^2 [1 - \theta] \right) P_s,
\]  

(53)

\[
C_1 = \left( \theta \kappa + 1 - \theta \right) P_s,
\]  

(54)

\[
\tilde{\sigma}_s^2 = \left( 1 - \rho_s^2 \right) P_s \left( \theta + \chi^2 [1 - \theta] \right) \mu_s + \rho_s^2 \sigma_s^2.
\]  

(55)

The quantity \( Z_1 \) has the same form as \( \Upsilon \) in (31). Therefore, by substituting variables appropriately into \( \Upsilon \) in (31), one can achieve the precise closed-form formula of \( Z_1 \). More specifically, \( Z_1 \) is computed by using \( \Upsilon \) in (39) with \( A_1 \rightarrow A \), \( B_1 \rightarrow B \), \( C_1 \rightarrow C \), \( \mu \rightarrow \mu_s \), \( \sigma^2 \rightarrow \sigma_s^2 \). As a result, the derivation of \( Z_1 \) is skipped here for compactness.

The term \( Z_2 \) in (50) is rewritten after using (17) and (19) for the case of \( \gamma_s < \gamma_t \) as

\[
Z_2 = \Pr \left\{ \frac{1 + \frac{A_1 \sigma^2}{B_1 \sigma^2} \left( 1 + \frac{A_1 \sigma^2}{B_1 \sigma^2} \right)}{C_1 \sigma^2} < 2 \right\}.
\]  

(56)

where

\[
A_2 = \tau P_s,
\]  

(57)

\[
B_2 = \chi^2 (1 - \tau) P_s,
\]  

(58)

\[
C_2 = (1 - \tau) P_s,
\]  

(59)

\[
\tilde{\sigma}_s^2 = \left( 1 - \rho_s^2 \right) P_s \left( \tau + \chi^2 [1 - \tau] \right) \mu_s + \rho_s^2 \sigma_s^2.
\]  

(60)

The quantity \( Z_2 \) has the same form as \( \Upsilon \) in (31). Therefore, by substituting variables appropriately into \( \Upsilon \) in (31), one can achieve the precise closed-form formula of \( Z_2 \). More specifically, \( Z_2 \) is computed by using \( \Upsilon \) in (39) with \( A_2 \rightarrow A \), \( B_2 \rightarrow B \), \( C_2 \rightarrow C \), \( \mu \rightarrow \mu_s \), \( \sigma^2 \rightarrow \sigma_s^2 \). As a result, the derivation of \( Z_2 \) is skipped here for compactness.

Inserting the above-proposed precise closed-form formulas of \( \Delta \), \( Z_1 \), and \( Z_2 \) into (50) yields the precise closed-form expression of \( SOP_s (C_0) \).

### 3.3 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. Upon our understanding, these formulas haven’t been reported yet. Moreover, they can be exploited to achieve the formulas for other pivotal security measures. To be more specific, the IP addresses the probability of negative secrecy capacity. Accordingly, the IP of secondary/primary communication is computed as

\[
IP_s = \Pr \{ \hat{C}_{ua} < 0 \} = SOP_p (0),
\]  

(61)
where \( u = s, p \).

PSCP indicates the probability of positive secrecy capacity. Consequently, the PSCP of secondary/primary communication is expressed as

\[
PSCP_u = \Pr \left( \hat{C}_u > 0 \right) = 1 - SOP_u(0) \tag{62}
\]

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

\[
STP_u = [1 - SOP_u(C_0)]C_0. \tag{63}
\]

4 Illustrative results

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 \((0.6, -0.1), \eta = 0.9, \sigma^2_e = \sigma^2_v = \sigma^2_i = \sigma^2_s = N_0, \rho_{uv} = \rho, \varsigma = 3, P_p/N_0 = 10 \text{ dB}, \alpha = \lambda = \tau = 0.6, \theta = 0.8, \kappa = 0.7, C_i = C_0 = 0.1 \text{ bps/Hz}. \) Figures 3–12 respectively denote “Sim.” and “Ana.” as the simulation and the analysis, and illustrate the match between the simulation and the analysis, ratifying the exactness of the analysis in (29) and (50).

Figure 3 illustrates the SOPs versus channel estimation imperfection reflected by \( \rho \). 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 \( \chi \)) 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 among the amount of the power \( \theta P_s \) reserved for transmitting legitimate data, \( ST \) allocates 70% \((\kappa = 0.7)\) of this amount to relay the primary data and 30% \((1 - \kappa = 0.3)\) of that to send the secondary data.

Figure 4 illustrates the SOPs versus imperfect artificial noise cancellation reflected by \( \chi \). This figure shows the increase of SOPs with increasing \( \chi \), 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 \( \rho \)) 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 \( \chi \) \((e.g., SOP_s \) at \( \rho = 1.0 \) is larger than \( SOP_s \) at \( \rho = 0.9 \) for any \( \chi)\). Furthermore, due to \( \kappa = 0.7 \) as Fig. 3, primary communication is more secure than secondary communication at the same levels of channel estimation error and artificial noise cancellation, as expected.

Figure 5 plots the SOPs versus \( P_p/N_0 \). Owing to \( \kappa = 0.7 \) as Fig. 3, primary communication is more secure than secondary communication at the same levels of 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 6 plots the SOPs versus \( \theta \). This figure demonstrates optimum values of \( \theta \), which minimize the SOP of primary/secondary communication. These optimum values balance the powers for sending the artificial noise and the legitimate (secondary and primary) data. 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 the \( ST \) to transmit the \( PT \)’s information than the \( ST \)’s information. Furthermore, better artificial noise cancellation and channel estimation improve secondary/primary security capability in a certain region of \( \theta \) \((e.g., SOP_s \) (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 7 plots the SOPs versus \( \kappa \). The results illustrate that increasing \( \kappa \) improves secrecy performance of primary communication (decreasing \( SOP_p \)) but mitigates that of secondary communication (increasing \( SOP_s \)), showing the security compromise between primary and secondary communication. This is obvious because \( \kappa \) interprets the percentage of the \( ST \)’s transmit power allotted for the primary data while \( 1 - \kappa \) interprets the percentage of the \( ST \)’s transmit power allotted for the secondary data. Therefore, increasing \( \kappa \) decreases \( SOP_p \) but increases \( SOP_s \). Due to the conflicting
Fig. 3  SOPs versus $\rho$

Fig. 4  SOPs versus $\chi$
Fig. 5  SOPs versus $P_p/N_0$

Fig. 6  SOPs versus $\theta$
Fig. 7 SOPs versus $\kappa$

The security performance trend of $SOP_p$ and $SOP_s$ with respect to $\kappa$, there exists a value of $\kappa$ where $SOP_p$ and $SOP_s$ are equal (e.g., $\kappa \approx 0.535$ for $(\rho = 0.9, \chi = 0.5)$ and $\kappa \approx 0.5$ for $(\rho = 1.0, \chi = 0.0)$ as shown in Fig. 7), 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 $\kappa$; for example, $SOP_s = 1$ 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 Fig. 7. Furthermore, better artificial noise cancellation and channel estimation improve secondary/primary security capability in a certain region of $\kappa$ (e.g., $SOP_s$ or $SOP_p$) at $(\rho = 1.0, \chi = 0.0)$ is smaller than $SOP_p$ (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., $SOP_p$ (or $SOP_p$) at $(\rho = 1.0, \chi = 0.0)$ is larger than $SOP_p$ (or $SOP_p$) at $(\rho = 0.9, \chi = 0.5)$ when $0.52 < \kappa < 0.7$ (or $0.2 < \theta < 0.48$)).

Figure 8 plots the SOPs versus $C_t$, which expose that increasing $C_t$ enhances secrecy capability of secondary communication but deteriorates that of primary communication. This is because the increase in $C_t$ (equivalently, the increase in the transmission rate demanded by the $PT$) reduces the probability 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, ultimately reducing the $SOP_s$. Two contradictory trends of primary and secondary security capabilities with respect to $C_t$ facilitate in balancing these security capabilities by setting the reasonable required primary transmission rate; for instance, $SOP_s = SOP_p$ at $C_t = 0.79 \text{ bps/Hz}$ for $(\rho = 0.9, \chi = 0.5)$ and at $C_t = 1.85 \text{ bps/Hz}$ for $(\rho = 1.0, \chi = 0.0)$. Moreover, better artificial noise cancellation and channel estimation improve primary data security but degrade secondary data security, i.e., $SOP_p$ (or $SOP_p$) at $(\rho = 1.0, \chi = 0.0)$ is smaller (or larger) than $SOP_p$ (or $SOP_p$) at $(\rho = 0.9, \chi = 0.5)$.

Figure 9 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. Interestingly, 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 $C_0 \leq 0.016 \text{ bps/Hz}$ but $SOP_s > SOP_p$ for $C_0 > 0.016 \text{ bps/Hz}$ when $\rho = 1.0$ and $\chi = 0.0$). Moreover, better artificial noise cancellation and channel estimation also improve secondary/primary security capability in a certain region of $C_0$; for instance, $SOP_p$ (or $SOP_p$) at $(\rho = 1.0, \chi = 0.0)$ is smaller than $SOP_p$ (or $SOP_p$) at $(\rho = 0.9, \chi = 0.5)$ when $C_0$ is smaller than $0.232$ (or $0.049$) bps/Hz.

Figure 10 demonstrates the SOPs versus $\alpha$, which expose that the security measure of secondary/primary communication is optimized with relevant selection of $\alpha$. The reason behind the optimum value of $\alpha$ that minimizes SOPs is as fol-
Fig. 8  SOPs versus $C_t$

![Graph showing SOPs versus $C_t$.](image)

Fig. 9  SOPs versus $C_0$

![Graph showing SOPs versus $C_0$.](image)
The increase in $\alpha$ 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 which is proportional to $1 - \alpha$. Accordingly, $\alpha$ can be controlled to balance gains in two stages. Moreover, security performance of primary/secondary communication at the optimal value of $\alpha$ is improved with better channel estimation and artificial noise cancellation, i.e., $SOP_p$ (or $SOP_s$) at the optimal value of $\alpha$ for $(\rho = 1.0, \chi = 0.0)$ is smaller than $SOP_p$ (or $SOP_s$) at the optimal value of $\alpha$ for $(\rho = 0.9, \chi = 0.5)$. Nonetheless, the optimum secondary data security is inferior to the optimum primary data security at channel estimation-and-artificial noise cancellation perfection (i.e., $SOP_p > SOP_s$ at the optimal value of $\alpha$ for $(\rho = 1.0, \chi = 0.0)$) but artificial noise cancellation-and-channel estimation 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 $\alpha$ for $(\rho = 0.9, \chi = 0.5)$).

Figure 11 plots the SOPs versus $\lambda$, which expose that security capability of the secondary communication is almost constant and only improved for high $\lambda$ (e.g., $\lambda \geq 0.95$). The reason is that large $\lambda$ allows ST to scavenge more energy from PT and reduces signal power at ST’s decoder (i.e., reduces the possibility of restoring correctly the PT’s information); thus, the power for transmitting the ST’s information is higher in Stage II, eventually declining $SOP_s$. Nevertheless, $\lambda$ can be selected appropriately to optimize secrecy performance of primary communication. The optimal value of $\lambda$ for the smallest $SOP_p$ is to balance between the possibility of restoring the primary data at the ST and the scavenged energy. Moreover, primary communication is more secure than secondary communication due to $\kappa = 0.7$, which is a similar comment observed from the previous figures. Furthermore, better artificial noise cancellation and channel estimation enhance security capability of primary communication but deteriorate that of secondary communication.

The power allocation factor for artificial noise and secondary signal as the ST decodes incorrectly the PT’s signal is specified by $\tau$. Therefore, to recognize the affect of $\tau$ plainly, we should investigate 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 12 demonstrates the SOPs versus $\tau$ for $C_t = 5$ 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 $\tau$ which maximizes secrecy performance of secondary communication. This optimum $\tau$ aims to balance the power allocation for the ST’s information and the artificial noise. Furthermore, better artificial noise cancellation and channel estimation enhance secondary
Fig. 11  SOPs versus $\lambda$

Fig. 12  SOPs versus $\tau$
data security capability, i.e., $SOP_x$ at $(\rho = 1.0, \chi = 0.0)$ is smaller than $SOP_x$ at $(\rho = 0.9, \chi = 0.5)$.

5 Conclusion

This paper implemented the overlay mechanism in cognitive radio networks where the secondary transmitter assists the data transmission of the primary transmitter as well as transmits its private data. The secondary transmitter is capable of harvesting radio frequency energy and generating the artificial noise to self-power its operation and secure primary/secondary communication against eavesdroppers. Secrecy capability of primary/secondary communication is measured in terms of primary/secondary secrecy outage probability under uncertainties of artificial noise cancellation-and-channel estimation imperfection, which was numerically rated by the suggested precise closed-form formulas. Various results are generated to validate such 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 relied on the recommended formulas that well guides system design. Furthermore, the secrecy performance compromise between secondary and primary communication can be managed by controlling system parameters appropriately.

Acknowledgements This research is funded by Vietnam National University HoChiMinh City (VNU-HCM) under Grant Number B2021-20-01. We would like to thank Ho Chi Minh City University of Technology (HCMUT), VNU-HCM for the support of time and facilities for this study.

References

1. Yu, L., Liu, Z., Wen, M., Cai, D., Dang, S., Wang, Y., & Xiao, P. (2021). Sparse code multiple access for 6G wireless communication networks: Recent advances and future directions. *IEEE Communications Standards Magazine*, 5(2), 92–99.

2. Li, W., Wang, N., Jiao, L., & Zeng, K. (2021). Physical layer spoofing attack detection in MmWave massive MIMO 5G networks. *IEEE Access*, 9, 60419–60432.

3. De Alwis, C., Kalla, A., Pham, Q. V., Kumar, P., Dev, K., Hwang, W. J., et al. (2021). Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. *IEEE OJCS*, 2, 836–886.

4. Motz, C., Paireder, T., & Huemer, M. (2021). Low-complex digital cancellation of transmitter harmonics in LTE-A/5G transceivers. *IEEE OJCS*, 2, 948–963.

5. Savic, M., Lukic, M., Danilovic, D., Bodroski, Z., Bajovic, D., Mezey, I., et al. (2021). Deep learning anomaly detection for cellular IoT with applications in smart logistics. *IEEE Access*, 9, 59406–59419.

6. Ali, M., Qaisar, S., Naem, M., Ejaz, W., & Kvedaraite, N. (2020). LTE-U WiFi HetNets: Enabling spectrum sharing for 5G beyon 5G systems. *IEEE Internet of Things Magazine*, 7(4), 60–65.

7. Tian, Z., Yi, S., Zhiwen, P., Nan, L., & Xiaohu, Y. (2021). Matching theory based physical layer secure transmission strategy for cognitive radio networks. *IEEE Access*, 9, 46201–46209.

8. Fakharian, M. M. (2021). RF energy harvesting using high impedance asymmetric antenna array without impedance matching network. *Radio Science*, 56(3), 1–10.

9. Eltrey, N. A., Abd Elhamid, M., Elsheakh, D. M., Elhenawy, H. M., & Abdallah, E. A. (2021). Silver sandwiched ITO based transparent antenna array for RF energy harvesting in 5G mid-range of frequencies. *IEEE Access*, 9, 49476–49486.

10. Gunasinghe, D., & Baduge, G. A. A. Performance analysis of SWIPT for intelligent reflective surfaces for wireless communication. *IEEE Communications Letters*. [https://ieeexplore.ieee.org/document/9404225](https://ieeexplore.ieee.org/document/9404225)

11. Le, Q. N., Yadav, A., Nguyen, N. P., Dobre, O. A., & Zhao, R. (2021). Full-duplex non-orthogonal multiple access cooperative overlay spectrum-sharing networks with SWIPT. *IEEE Transactions on Green Communications and Networking*, 5(1), 322–334.

12. Sadique, J. J., Ullah, S. E., Islam, M. R., Raad, R., Kouzani, A. Z., & Mahmud, M. P. (2021). Transceiver design for full-duplex UAV based zero-padded OFDM system with physical layer security. *IEEE Access*, 9, 59432–59445.

13. Shang, X., Yin, H., Wang, Y., Li, M., & Wang, Y. (2021). Secure multiuser scheduling for hybrid relay-assisted wireless powered cooperative communication networks with full-duplex destination-based jamming. *IEEE Access*, 9, 49774–49787.

14. Su, R., Wang, Y., & Sun, R. (2019). Secure cooperative transmission in cognitive AF relay systems with destination-aided jamming and energy harvesting. *Proc* (pp. 1–5). Turkey: IEEE PIMRC.

15. Su, R., Wang, Y., & Sun, R. (2018). Destination-aided jamming for physical-layer security in SWIPT cognitive radio systems. *Proc* (pp. 1–6). Spain: IEEE WCNC.

16. Wang, D., Zhou, F., & Leung, V. C. (2020). Primary privacy preserving with joint wireless power and information transfer for cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking*, 6(2), 683–693.

17. Xu, M., Jing, T., Fan, X., Wen, Y., & Huo, Y. (2018). Secure transmission solutions in energy harvesting enabled cooperative cognitive radio networks. *Proc* (pp. 1–6). Spain: IEEE WCNC.

18. Ho-Van, K., & Do-Dac, T. Overlay networks with jamming and energy harvesting: Security analysis. *Arabian Journal for Science and Engineering*. [https://doi.org/10.1007/s13369-021-05492-z](https://doi.org/10.1007/s13369-021-05492-z)

19. Dang-Ngoc, H., Ho-Quoc, B., & Ho-Van, K. (2020). Key secrecy performance metrics of overlay networks with energy scavenging and artificial noise. In *Proc. IEEE SigTelCom*, Vietnam, 28-29 Aug. (pp. 77–81).

20. Pham-Thi-Dan, N., Ho-Quoc, B., Ho-Van, K., Do-Dac, T., Nguyen-Huu, P., Vo-Que, S., Pham-Ngoc, S., & Pham-Hong, L. (2020). Secrecy throughput analysis of energy scavenging overlay networks with artificial noise. In *Proc. IEEE ICT*, Vietnam, 8-10 Aug (pp. 90–94).

21. Dang-Ngoc, H., Ho-Van, K., & Do-Dac, T. Secrecy analysis of overlay mechanism in radio frequency energy harvesting networks with jamming under Nakagami-m fading. *Wireless Personal Communications*. [https://doi.org/10.1007/s11277-021-08468-2](https://doi.org/10.1007/s11277-021-08468-2)

22. Wang, D., & Tellambura, C. (2020). Performance analysis of energy beamforming WPCN links with channel estimation errors. *IEEE OFS-C, J* 1153–1170.

23. Li, M., Yin, H., Huang, Y., Wang, Y., & Yu, R. (2018). Physical layer security in overlay cognitive radio networks with energy harvesting. *IEEE Transactions on Vehicular Technology*, 67, 11274–11279.

24. Chen, L., Huang, L., Xu, H., Yang, C., Sun, Z., & Wang, X. (2015). Primary secrecy is achievable: Optimal secrecy rate in overlay CRNs with an energy harvesting secondary transmitter. *Proc* (pp. 1–6). USA: ICCCN.
25. Kazmi, S. A. A., & Coleri, S. (2020). Optimization of full-duplex relaying system with non-linear energy harvester. *IEEE Access, 8*, 201566–201576.

26. Tran, T. N., Vo, T. P., Fazio, P., & Voznak, M. SWIPT model adopting a PS framework to Aid IoT networks inspired by the emerging cooperative NOMA technique. *IEEE Access*, accepted.

27. Ho-Van, K., & Do-Dac, T. (2019). Security analysis for underlay cognitive network with energy scavenging capable relay over Nakagami-m fading channels. *Wireless Communications and Mobile Computing*, 2019, 1–16.

28. Nguyen-Huu, P., Ho-Van, K., & Bao, V. N. Q. (2019). Secrecy outage analysis of energy harvesting two-way relaying networks with friendly jammer. *IET Communications, 13*(13), 1877–1885.

29. Ge, L., Chen, G., Zhang, Y., Tang, J., Wang, J., & Chambers, J. A. (2020). Performance analysis for multihop cognitive radio networks with energy harvesting by using stochastic geometry. *IEEE IoT Journal, 7*(2), 1154–1163.

30. Gradshteyn, I. S., & Ryzhik, I. M. (2000). *Table of integrals, series and products* (6th ed.). Academic.

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Khuong Ho-Van** received the B.E. (with the first-rank honor) and the M.S. degrees in Electronics and Telecommunications Engineering from HoChiMinh City University of Technology, Vietnam, in 2001 and 2003, respectively, and the Ph.D. degree in Electrical Engineering from University of Ulsan, Korea in 2007. During 2007–2011, he joined McGill University, Canada as a postdoctoral fellow. Currently, he is an Associate professor at Ho Chi Minh City University of Technology. His major research interests are modulation and coding techniques, diversity techniques, digital signal processing, energy harvesting, physical layer security, and cognitive radio.

**Thiem Do-Dac** received the B.E. degree in Electronic Engineering from University of Transport and Communication, Vietnam in 1998, and the Master’s degree in Electronic Engineering from Can Tho University, Vietnam in 2003. Currently, he is working towards a Ph.D degree in Ho Chi Minh City University of Technology, Vietnam. His research interests are physical layer security and cognitive radios.