Performance Analysis of Energy-Efficient Secure Transmission for Wireless Powered Cooperative Networks with Imperfect CSI

Yajun Zhang[1*], Jun Wu[1], Bing Wang[1], Hongkai Wang[1], and Xiaohui Shang[2]
[1] Army Academy of Artillery and Air Defense (Nanjing Campus)
Nanjing, 211113, China
[e-mail: yajun2000@foxmail.com, 4270771@qq.com, njpywbing@163.com, whongkay@sina.com]
[2] 361618 Troops of PLA
Beijing, 100094, China
[e-mail: shangxiaohui1214@126.com]
[*]Corresponding author: Yajun Zhang

Received May 10, 2023; revised July 28, 2023; revised August 10, 2023; accepted August 22, 2023; published September 30, 2023

Abstract

The paper focuses on investigating secure transmission in wireless powered communication networks (WPCN) that involve multiple energy-constrained relays and one energy-constrained source. The energy is harvested from a power beacon (PB) while operating in the presence of a passive eavesdropper. The study primarily aims to achieve energy-efficient secure communications by examining the impact of channel estimation on the secrecy performance of WPCN under both perfect and imperfect CSI scenarios. To obtain practical insights on improving security and energy efficiency, we propose closed-form expressions for secrecy outage probability (SOP) under the linear energy harvesting (LEH) model of WPCN. Furthermore, we suggest a search method to optimize the secure energy efficiency (SEE) with limited power from PB. The research emphasizes the significance of channel estimation in maintaining the desired performance levels in WPCN in real-world applications. The theoretical results are validated through simulations to ensure their accuracy and reliability.

Keywords: Internet of Things, physical layer security, secure energy efficiency, secrecy outage probability, wireless powered communication network

This research was supported by a research grant LJ20202C020087 from Compreshensive Research on Equipment.

http://doi.org/10.3837/tiis.2023.09.006 **ISSN : 1976-7277**

1. Introduction

The advent of fifth-generation (5G) mobile communications has paved the way for the Internet of Things (IoT), which has a broad range of potential applications such as industrial control, remote health monitoring, and traffic control [1]. However, IoT devices typically have limited resources in terms of energy and computing power. Thus, energy efficiency is a critical factor in IoT systems [2], particularly since many IoT devices are designed to operate for extended periods of time. Wireless powered communication networks (WPCN) are a practical solution for maintaining the long-term operation of IoT devices. WPCNs consist of both wireless information transfer (WIT) and wireless power transfer (WPT) methods [3, 4].

Compared to traditional charging methods, WPCNs can be powered by batteries or RF signals from the environment. This allows the wireless system to stay connected at all times, effectively extending its lifespan and significantly improving network throughput and reliability [5]. Although WPCNs have these advantages, security remains a concern due to potential eavesdropping threats [6, 7]. To enhance security in WPCNs, Physical Layer Security (PLS) methods use the unique characteristics of wireless channels for secure transmission [8-13]. It is worth noting that, unlike literature [13], which is key based, we mainly focus on how to improve physical layer security derectly.

Secrecy Outage Probability (SOP) is often used to measure the performance of PLS in wireless physical layer secure transmission. SOP represents the probability that the achievable secrecy rate falls below the target secrecy rate [14]. In recent years, numerous studies have investigated the SOP of WPCNs [11-15]. In [15], the authors consider three relay selection schemes that select the best Power Beacon (PB) by source, namely Best Relay by Source (BRS), Best Relay Randomly (BRR), and Best Relay by Best PB (BRBP), respectively. Another study analyzed the outage probability of SWIPT-WPCN networks with nonlinear EH models by using time-switched receiver architecture for information decoding and EH [16]. In [17], an EH jammer was employed to minimize the SOP in wiretap WPCN systems. Literature [18, 19] analyzed the SOP under imperfect Channel State Information (CSI) using Transmit Antenna Selection (TAS).

The above results consider all the scenarios under perfect CSI. However, it is worth noting that obtaining ideal CSI is difficult in practice due to the incomplete feedback and influence of channel estimation error. Recently, several works have investigated the scenarios under imperfect CSI. In [20], both SOP and connection outage probability (COP) are investigated under partial CSI. In [21], the authors obtained an analytical expression for SOP under the imperfect CSI in the wireless-powered multi-antenna relaying system. In [22], the authors examined the design of a power-splitting with relay selection scheme, and derived optimal power splitting ratios under both imperfect and perfect CSI. In [23], the problem of secure energy-efficient transmission was investigated in an artificial-noise (AN)-aided SWIPT system with imperfect CSI.

Many works has focused on the research of secure energy efficiency (SEE), [24] examined the SEE in a multirelay DF scenario. Another study, [25], investigated how resources could best be allocated to optimize SEE in a scenario with multiple antennas at the legitimate transmitter. The study considered various CSI assumptions. Afterwards, in [26], the authors aimed to maximize SEE in cooperative networks with partial secrecy requirements. Furthermore, in [15], the SEE was sought to be maximized under a constraint on transmit power by optimizing the transmit power in power beacons (PBs) and the time-switching factor for WPCN.

Our paper builds on these studies by focusing on the impact of imperfect CSI on Physical Layer Security (PLS) for Wireless Powered Communication Networks (WPCN). Specifically, our work takes into account imperfections present in practical communication environments, making it more closely aligned with practical scenarios. Additionally, we examine the impact of imperfect CSI on the secure performance of WPCN, which complements existing work that has largely focused on perfect CSI [15]. As such, the main contributions of our work are as follows:

- For the multiple relays-assisted WPCN, by means of the best relay selection strategy, the influence of channel estimation on the secure transmission has been explored, in which the scenario including perfect CSI and the imperfect CSI has been discussed, respectively.
- We infer the closed-form expressions of SOP for perfect CSI and imperfect CSI under the linear EH model of WPCN. Moreover, in order to provide more practical guidance, the search method is used for solving the problem of maximizing SEE under the limited power of PB.
- The correctness of our derivation is verified by simulation results. The dominating role of the channel estimation on secure WPCN has been revealed with the help of analyzing the effects of relevant parameters including the time-switching factor, the energy conversion efficiency, and channel correlation coefficient on secrecy performance. It is worth noting that the dominating role should be paid much attention in practice.

The rest of this paper is arranged as follows: Section II introduces the system model, followed by Section III, which derives explicit expressions of SOP and SEE. Then, Section IV presents numerical results. Finally, we conclude in Section V.

2. System Model

Fig. 1 illustrates a communication scenario where a source sensor S sends confidential information to the base station D with the help of several relay sensors $R_n, n \in \{1, 2 \cdots, N\}$. A passive eavesdropper E, with no restrictions on its ability to eavesdrop, and commonly assumed for information-theoretic security, is also present in the communication channel. Due to serious fading between S and D, there is no direct link from S to D [27, 28]. To overcome this limitation, both S and D obtain energy support from multiple power beacons via wireless power transfer (WPT) for wireless information transfer (WIT). All nodes in the system have a single antenna, and the wireless channels are assumed to be independently Rayleigh-distributed [2].

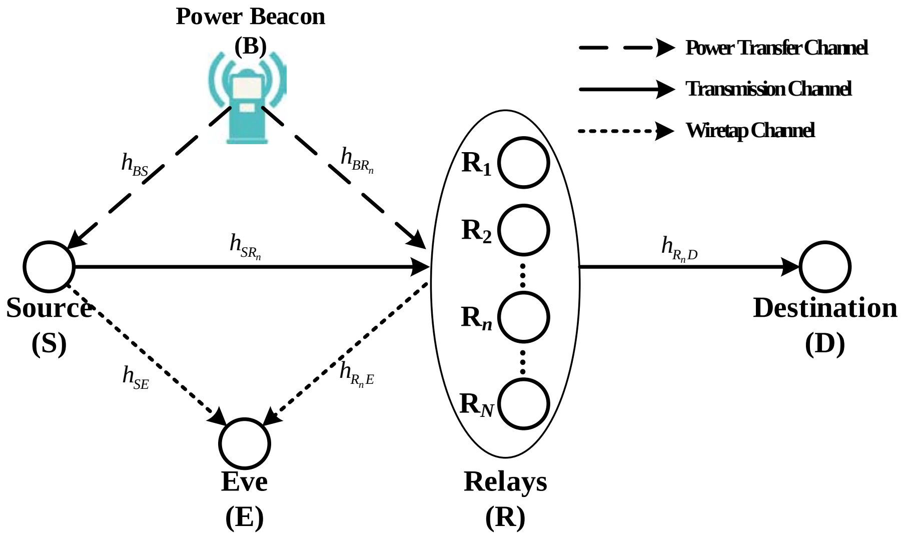

Fig. 1. System model

The power gain of each channel is exponentially distributed with parameter λ_{XY}, where $Y \in \{S, D, E, R_n\}$ and $X \in \{B, S, R_n\}$. Gaussian white noise is added to the channels at R_n and D with variance N_0 and zero mean. Similarly, the AWGN at E has variance N_E and zero mean. For the sake of mathematical modeling simplicity, $B \to S$, $S \to R_n$, $B \to R_n$, $S \to E$, $R_n \to D$, and $R_n \to E$ are denoted as h_{xy} .This assumption is commonly used in wireless-powered communication networks (WPCNs) due to the complexity and variability of the wireless communication environment (e.g. [29-31]). Although exact channel estimation on practical channels can be difficult, our assumption can simplify the analysis and lead to more intuitive conclusions, making it a suitable foundation for investigating real-world complex communication problems.

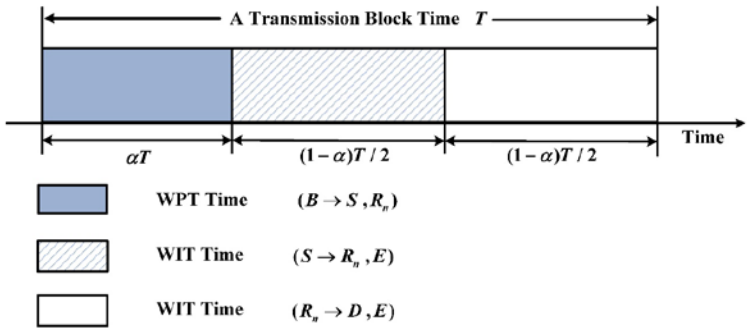
A Transmission Block Time T
Time
αT
$(1-\alpha)T/2$
$(1-\alpha)T/2$
WPT Time $(B \to S, R_n)$
WIT Time $(S \to R_n, E)$
WIT Time $(R_n \to D, E)$

Fig. 2. Time-switching relay protocol

1) As shown in Fig. 2, the time for WPT is αT and the time for WIT is $(1-\alpha)T$, where α is the time-switching factor and $\alpha \in (0,1)$. The energy harvested at sensors is fully consumed to send information in the WIT process [32]. Therefore, the energy harvested at R_n and S can be shown as:

$$E_{R_n} = \eta P_B \alpha T \left|h_{BR_n}\right|^2, \tag{1}$$

$$E_S = \eta P_B \alpha T \left|h_{BS}\right|^2, \tag{2}$$

where η is the energy efficiency coefficient and $10\% < \eta < 80\%$ [33], P_B is the transmission power at PB, $\left|h_{BS}\right|^2$ and $\left|h_{BR_n}\right|^2$ are power gains of the channels form PB to R_n and to S, respectively. Then, the received energy is used to transmit information in the rest time. As in [34], the harvested energy from noise is negligible. The reason is that the received power at sources contributed by PB is far more than the received noisy power.

2) In the second duration of $(1-\alpha)T/2$, the relays R_n get the information from the source. In this time, the channel fading coefficients remain constant [35]. Thus, the transmit power of S can be given by

$$P_S = \frac{2\eta\alpha}{1-\alpha} P_B \left|h_{BS}\right|^2, \tag{3}$$

3) In the last duration of $(1-\alpha)T/2$, the destination D receive information from the relays R_n. Similarly, the transmit power of R_n is

$$P_{R_n} = \frac{2\eta\alpha}{1-\alpha} P_B \left|h_{BR_n}\right|^2. \tag{4}$$

Form (3) and (4), we can get SNR of R and E in the second hop and SNR of D and E in the last hop e.g., γ_{SR_n}, γ_{SE}, γ_{R_nD} and γ_{R_nE} as

$$\begin{aligned}\gamma_{SR_n} &= \frac{P_S\left|h_{SR_n}\right|^2}{N_0} = \frac{2\eta\alpha}{N_0(1-\alpha)} P_B \left|h_{BS}\right|^2 \left|h_{SR_n}\right|^2 \\ &= \gamma_B \xi_0 \left|h_{BS}\right|^2 \left|h_{SR_n}\right|^2\end{aligned} \tag{5}$$

where $\gamma_B = \dfrac{P_B}{N_0}$, $\xi_0 = \dfrac{2\eta\alpha}{1-\alpha}$.

So the other SNRs can expressed as the same:

$$\gamma_{SE} = \gamma_E \xi_0 \left|h_{BS}\right|^2 \left|h_{SE}\right|^2 \tag{6}$$

$$\gamma_{R_nD} = \gamma_B \xi_0 \left|h_{BR_n}\right|^2 \left|h_{R_nD}\right|^2 \tag{7}$$

$$\gamma_{R_nE} = \gamma_E \xi_0 \left|h_{BR_n}\right|^2 \left|h_{R_nE}\right|^2 \tag{8}$$

Lemma 1: If X_k, $k \in \{1 \cdots K\}$, is a random variable that follows an independent and identically distributed exponential distribution, the probability density function (PDF) and the cumulative distribution function (CDF) of $X = \max_{k\in\{1\cdots K\}}\{X_k\}$ can be shown as [34]

$$f_X(x) = K\lambda_X e^{-\lambda_X x}(1-e^{-\lambda_X x})^{K-1} \tag{9}$$

$$F_X(x) = (1-e^{-\lambda_X x})^{K} \tag{10}$$

Here, using BRS scheme, the selected relay R_n^* is shown as:

$$R_n^* = \arg\max_{R_n\in(R_1\cdots R_N)}\{|h_{SR_n}|^2\} \tag{11}$$

Hence, the $|h_{SR_n^*}|^2$, $|h_{R_n^*E}|^2$, $|h_{R_n^*D}|^2$ are exponentially distributed with parameters λ_{SR} , λ_{RE} , λ_{RD} , respectively. From Lemma 1, the PDF of $|h_{SR_n^*}|^2$ can be derived as

$$f_{|h_{SR_n^*}|^2}(x) = N\lambda_{SR}e^{-\lambda_{SR}x}(1-e^{-\lambda_{SR}x})^{N-1} \tag{12}$$

It is worth noting that there is an inverse relationship between the exponential distribution parameter and the mean channel gain.

Obtaining accurate channel estimation is challenging due to the complex channel environments. Previous research [36, 37] has highlighted that there are bound to be errors between the estimated and actual channel values. To account for this, we can use the following mathematical model,

$$\bar{h}_{SR_n} = \sqrt{\varepsilon}h_{SR_n} + \sqrt{1-\varepsilon}\Delta h_{SR_n} \tag{13}$$

where $\varepsilon \in [0,1]$ represents the correlation coefficient between the actual channel value h_{SR_n} and the estimated channel value $\bar{h}_{SR_n}$, Δh_{SR_n} is a Gaussian random complex variable with the same distribution as h_{SR_n} . It is worth noting that a lower value of ε indicates a greater error in CSI estimation. Conversely, a value of $\varepsilon = 1$ corresponds to perfect CSI.

Remark 1: In reality, each communication channel has a situation where the CSI estimation is imperfect. In particular, we focus on the simple scenario of whether the estimation of the link relay selection is ideal or not. Despite its simplicity, this simplified scenario makes it easy to draw more obvious conclusions.

3. Secure Performance Analysis

The comprehensive secure performance analysis of WPCN with the perfect and imperfect CSI is provided in the section.

3.1 Secrecy Outage Probability

As shown in [38], the achievable secrecy rate of the dual-hop system in WIT is indicated as

$$R_S = min(R_{S_1}, R_{S_2}) \tag{14}$$

where R_{S_1} and R_{S_2} are the achievable secrecy rate of the second and the last hoop. Here, $(1-\alpha)T/2$ is the transmission duration of WIT, so R_{S_1} and R_{S_2} can be expressed as follows:

$$R_{S_1} = \frac{1-\alpha}{2}\left[\log_2\left(\frac{1+\gamma_{SR_n^*}}{1+\gamma_{SE}}\right)\right]^+ \tag{15}$$

$$R_{S_2} = \frac{1-\alpha}{2}\left[\log_2\left(\frac{1+\gamma_{R_n^*D}}{1+\gamma_{R_n^*E}}\right)\right]^+ \tag{16}$$

where $[x]^+ = max(x,0)$, then the achievable secrecy rate of R_S can be indicated as

$$R_S = \frac{1-\alpha}{2}\log_2\left(\min\left(\frac{1+\gamma_{SR_n^*}}{1+\gamma_{SE}}, \frac{1+\gamma_{R_n^*D}}{1+\gamma_{R_n^*E}}\right)\right) \tag{17}$$

As an important indicator for measuring the performance of secrecy, SOP is regarded as a kind of probability which the achievable security rate R_S is lower than the predetermined security rate threshold R_{th} .So the SOP under each scenario $P_{S_{out}}^{(\mathrm{sch})}$ can be express as

$$\begin{aligned} P_{S_{out}}^{(\mathrm{sch})} &= \Pr\left\{R_S < R_{th}\right\} \\ &= \Pr\left\{\frac{1-\alpha}{2}\log_2\left(\min\left(\frac{1+\gamma_{SR_n^*}}{1+\gamma_{SE}}, \frac{1+\gamma_{R_n^*D}}{1+\gamma_{R_n^*E}}\right)\right) < R_{th}\right\} \end{aligned} \tag{18}$$

where $\mathrm{sch} \in (\mathrm{p,ip})$, and p denotes the perfect CSI estimation, ip means the imperfect CSI estimation.

1) SOP under perfect CSI

According to (18), the exact SOP in the considered WPCN under perfect CSI can be formulated as

$$\begin{aligned} P_{S_{out}}^{\mathrm{p}} = 1 - \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n \frac{N\xi\lambda_{SR}\overline{\lambda}_{SE}}{\gamma_B\left(\lambda_{SR}(n+1)+\overline{\lambda}_{SE}\right)} \frac{\lambda_{RD}\overline{\lambda}_{RE}}{\lambda_{RD}+\overline{\lambda}_{RE}} 4\sqrt{\frac{\lambda_{BS}\lambda_{BR}}{\lambda_{SR}(n+1)\lambda_{RD}}} \\ \times K_1\left(2\sqrt{\frac{\lambda_{BS}\xi}{\gamma_B}\lambda_{SR}(n+1)}\right)K_1\left(2\sqrt{\frac{\lambda_{BR}\xi}{\gamma_B}\lambda_{RD}}\right) \end{aligned} \tag{19}$$

where $P_{S_{out}}^{\mathrm{p}}$ is the SOP when the WIT operate in the perfect CSI, $K_1(\cdot)$ is the modified Bessel function of second kind [39], $\beta = 2^{\frac{2R_{th}}{1-\alpha}}$, $\xi = \frac{(\beta-1)(1-\alpha)}{2\eta\alpha} = \frac{(\beta-1)}{\xi_0}$, $\gamma_B = \frac{P_B}{N_0}$, $\overline{\lambda}_{SE} = \frac{\lambda_{SE}}{\beta}$, $\overline{\lambda}_{RE} = \frac{\lambda_{RE}}{\beta}$.

Proof: The proof can be found in Appendix A. ■

2) SOP under imperfect CSI

Furthermore, according to (19), the exact SOP in the considered WPCN under imperfect CSI can be given as

$$\begin{aligned} P_{S_{out}}^{(\mathrm{ip})} = 1 - \sum_{n=0}^{N-1} \binom{N-1}{n} (-1)^n \frac{N\lambda_{SR}\overline{\lambda}_{SE}\xi}{\gamma_B\left[\lambda_{SR_n^*} + \overline{\lambda}_{SE}\left[1+(1-\varepsilon)n\right]\right]} \times \frac{\lambda_{RD}\overline{\lambda}_{RE}}{\lambda_{RD}+\overline{\lambda}_{RE}} 4\sqrt{\frac{\lambda_{BS}\lambda_{BR}\left[1+(1-\varepsilon)n\right]}{\lambda_{SR}(n+1)\lambda_{RD}}} \\ \times K_1\left(2\sqrt{\frac{\lambda_{BS}\xi}{\gamma_B}\frac{\lambda_{SR}(n+1)}{\left[1+(1-\varepsilon)n\right]}}\right) K_1\left(2\sqrt{\frac{\lambda_{BR}\xi}{\gamma_B}\lambda_{RD}}\right) \end{aligned} \tag{20}$$

where $P_{S_{out}}^{(\mathrm{ip})}$ is the SOP when the WIT operate in the imperfect CSI, $\varepsilon \in [0,1]$ is the correlation coefficient between the estimated channel coefficient $\overline{h}_{SR_n}$ and the real one h_{SR_n} in (12).

Proof: The proof can be found in Appendix B. ■

Remark 2: According to (19) and (20), the number of multiple relay sensors and the efficiency factor of EH have a beneficial impact on the SOP of the WPCN for two different channel estimation conditions. Meanwhile, we observe that the precision closed-expressions of SOP under perfect or imperfect CSI are the same. Basically, the single difference point is the correlation coefficient and the secrecy performance of imperfect CSI are superior if the correlation coefficient is higher. These discussion is analyzed and proved in the next subsection.

3.2 Secure Energy Efficiency Maximization

In general, more energy should be consumed to improve the transmission performance. For energy-constrained wireless sensor networks, the excessive pursuit of confidentiality would adversely affect network performance. As in [15], the SEE, which is regarded as a ratio between energy consumption and the secure performance, is used to be an effective way to evaluate the secrecy performance of WPCN. Hence, the SEE can be shown as

$$\eta_s^{(\mathrm{sch})} = \frac{R_{th}\left(1-P_{S_{out}}^{(\mathrm{sch})}\right)}{P_{total}} \tag{21}$$

where P_{total} is is power cost in all at PB and $P_{total} = \kappa P_B + P_B^0$, κ indicates the power coefficient, which is a ratio of the energy harvested by the source sensor in WIT to the transmission power of PB. P_B and P_B^0 represent the transmission power and static power of PB, respectively. It should be emphasized that it makes full use of the energy harvested by the source sensor in WIT, while ignoring the power cost of the circuit [40].

In order to get the best transmission power of PB, the maximum value of the SEE is expressed as

$$\begin{aligned} \max_{P_B,\alpha} \quad & \eta_s^{(\mathrm{sch})} = \frac{R_{th}(1-P_{S_{out}}^{(\mathrm{sch})})}{P_{total}} \\ s.t. \quad & 0 < P_B \le P_{\max}, \\ & 0 < \alpha < 1. \end{aligned} \tag{22}$$

On the basis of numerical analysis and simulation, the optimal value of P_B and α will be obtained by using the search method [15]. For the above optimization problem of the SEE, it can be used as a guide for actual implementation, which may be used in engineering decisions-making.

Remark 3: From (19) and (20), we find that the higher transmission power in PB, the better the performance of secrecy in the system. However, according to (22), the increased transmission power has an adverse effect on the SEE. In addition, the raised factor of time-switching can improve the SOP while lowering the performance of communication in system due to the fewer time of WIT. Therefore, it is more practical for the WPCN by optimizing the time-switching factor and transmission power in order to maximize the SEE.

4. Simulation Results

This section will verify our theoretical results via Monte Carlo simulations, and the discussions about the SOP and SEE of WPCN are provided. Specifically, both scenarios including perfect CSI and the imperfect CSI are considered for linear energy harvesting (LEH). The simulation parameters are set as follows: $N=3$, $R_{th}=0.1$ bits/s/Hz, $\eta=0.8$, $\varepsilon=0.8$, $\gamma_B=30$ dB. Meanwhile, $\lambda_{BS}=\lambda_{BR}=\lambda_{SR}=\lambda_{SD}=1$. Furthermore, $\lambda_{SE}=\lambda_{SR}I$, $\lambda_{RE}=\lambda_{RD}I$, the value of I is considered from -10dB to 50dB in this section. As in [15], we use $\tau=\lambda_{SE}/\lambda_{SD}$ to express the ratio of the primary channel to the eavesdropping channel. Obviously, It is evident from the following figures that the theoretical curves align closely with the simulation results, providing confirmation of our analysis.

Fig. 3 shows that the higher value of τ, the better performance of SOP. The reasons are as follows: with the increase of capacity difference between the main channel and eavesdropping channel, the secrecy capacity of system is enhanced. Additionally, we observe that the correlation coefficient ε has a positive impact on the SOP performance, where a higher value of ε corresponds to better SOP, because of the larger value of ε means that the imperfect channel is much more closer to the perfect channel, which brings less influence to the secrecy performance of WPCN. Therefore, it can be found that imperfect CSI has great influence on the security of WPCN.

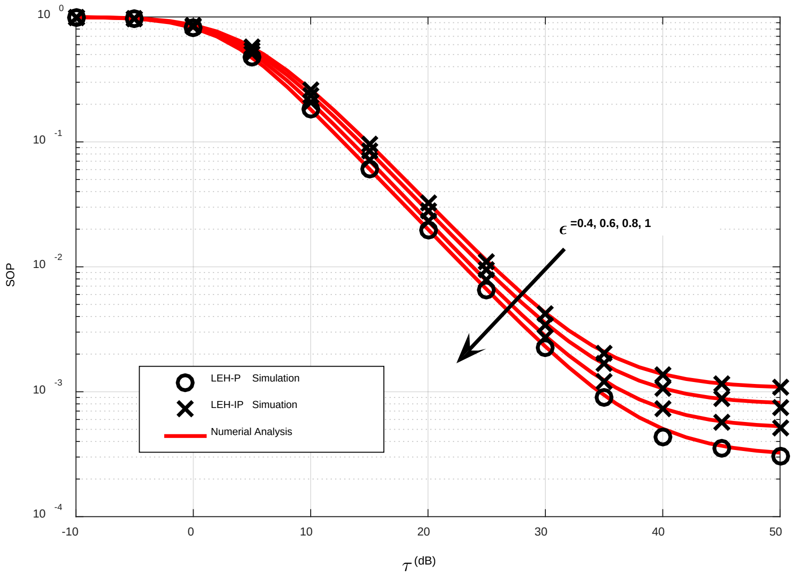

Fig. 3. SOP versus τ for various ε

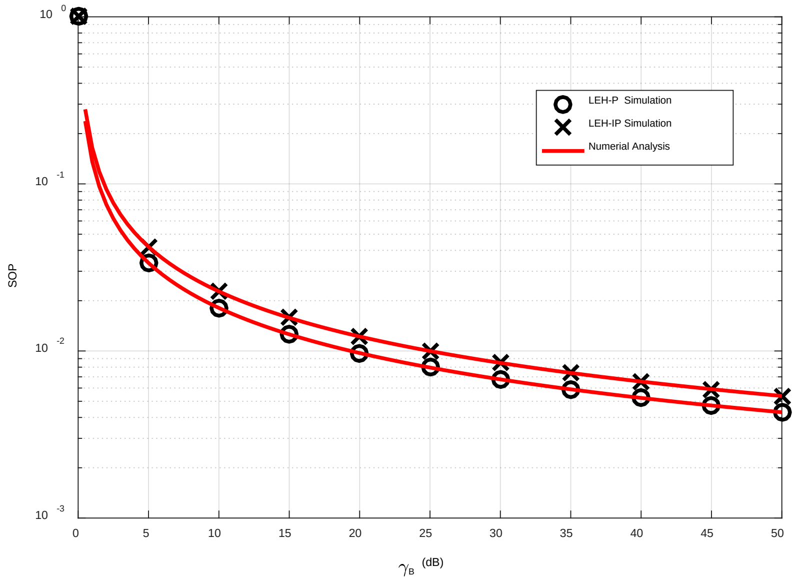

Fig. 4. SOP versus γ_{B}, where $\varepsilon = 0.8$

Fig. 4 plots the SOP performance with different various γ_{B} under perfect and imperfect CSI. We can see that the enhancement of SOP is attributed to the power of the PB, as higher power results in larger secrecy capacity. It is evident that perfect CSI outperforms imperfect CSI in terms of secure performance across the entire range of γ_{B}. In fact, $\varepsilon = 0.8$ means the channel estimation is not ideal, which reflects the gap of secrecy performance.

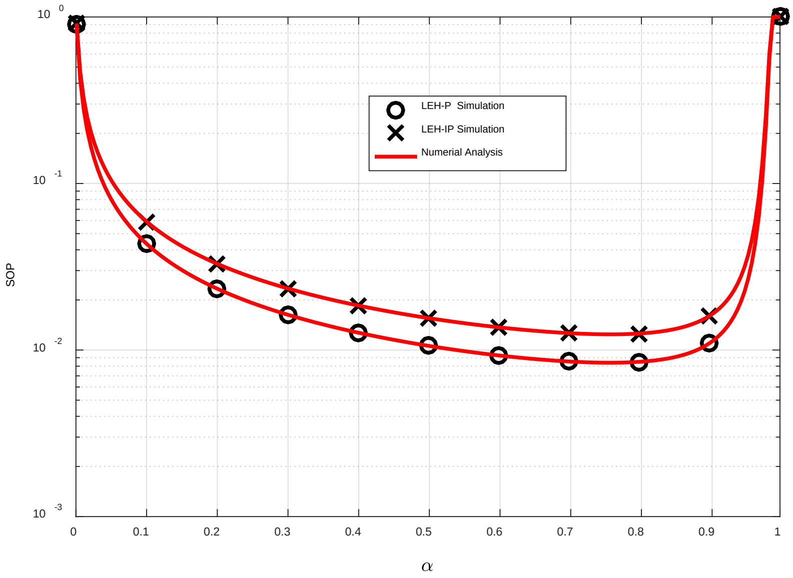

Fig. 5. SOP versus α

Fig. 5 shows the impact of the time-switching factor on SOP for different CSI. It can be observed that with the increasing of α , SOP decreases first and increases then. Specifically, when $\alpha = \alpha_{\text{optimal}}$, WPCN has the best security property ($\alpha_{\text{optimal}} \approx 0.75$ here). This is because when $\alpha < \alpha_{\text{optimal}}$, WPT dominates the secrecy performance of WPCN; by contrast, when $\alpha > \alpha_{\text{optimal}}$, which means the duration of WIT is shorter, the communication interruption probability will be increase. Meanwhile, the simulation results clearly show that the secrecy performance of the WPCN is better under full CSI than under imperfect CSI.

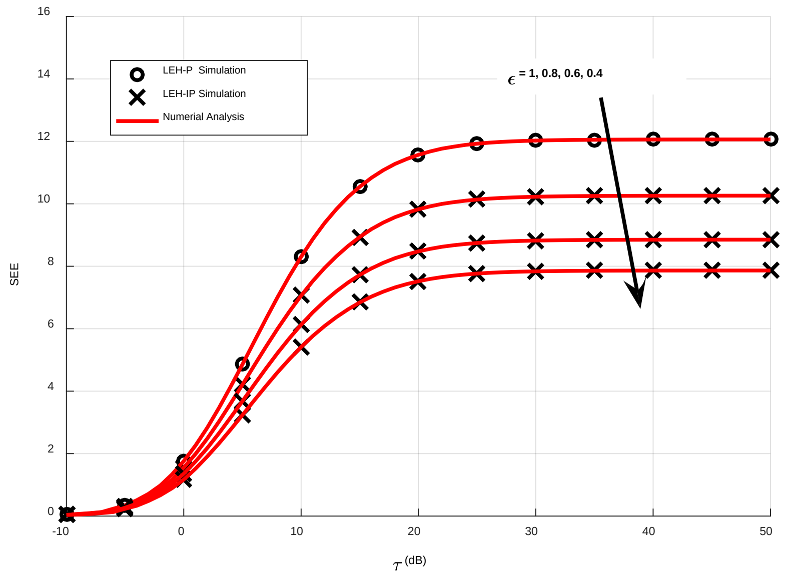

Fig. 6. SEE versus τ for various ε

Fig. 6 shows the impact of τ on the optimization of SEE by the exhaustive search method. First, SEE improves with the increase of τ and then it tends to be stable. This is because, when τ reaches a certain value, SEE is limited by other system parameters, like the transmit power of BP. Moreover, it can be easily observed that the better channel estimation, the better security performance of WPCN.

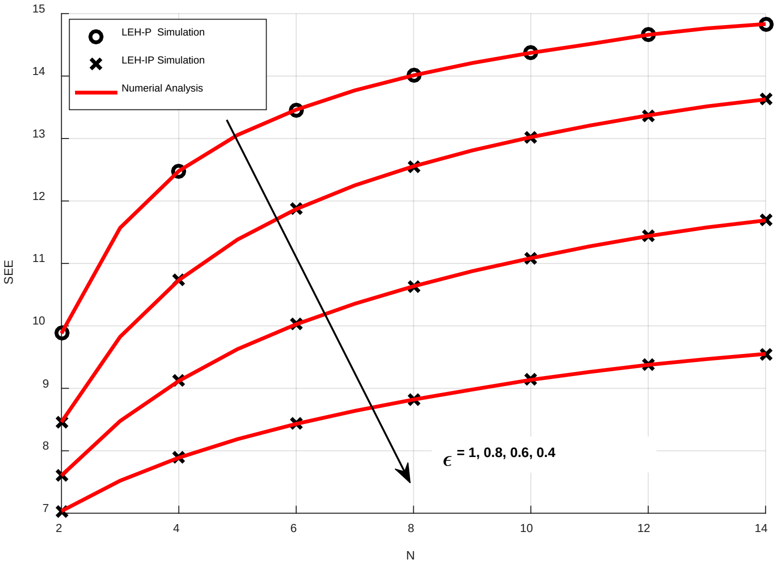

Fig. 7. SEE versus N for various ε

Fig. 7 shows the impact of the relays' number N on the SEE with $\tau = 20\text{dB}$. We can see that SEE improves with the increase of N. This is because, the larger number of relays, the higher secure performance can be obtained. Moreover, it can be easily observed that the better channel estimation, the better SEE performance of WPCN.

5. Conclusion

In this study, we investigate the performance of Physical Layer Security (PLS) for Wireless Powered Communication Networks (WPCN) under the linear Energy Harvesting (EH) model and imperfect Channel State Information (CSI). Specifically, we derive closed-form expressions of Secrecy Outage Probability (SOP) in the presence of passive eavesdroppers. Additionally, we solve the optimization problem of Secure Energy Efficiency (SEE) by utilizing a search algorithm while taking into account the constrained transmission power of Power Beacon (PB). Simulation results are provided to validate the accuracy of our derivations across all regions. Our findings demonstrate that imperfect CSI significantly impacts the PLS performance of WPCNs. In future work, we plan to analyze the impact of imperfect CSI under the nonlinear EH model.

Appendix A. Derivation of Eq. (19)

From(18), the $P_{S_{out}}^{\mathrm{p}}$ can be shown as

$$P_{S_{out}}^{\mathrm{p}} = 1 - P_r\left\{C_{S_1}^{\mathrm{p}} > R_{th}\right\} P_r\left\{C_{S_2}^{\mathrm{p}} > R_{th}\right\} \tag{23}$$

With the help of (4), (5), (6), the expansion can be derived as

$$\begin{aligned}
\Pr\left\{C_{S_1}^{\mathrm{p}} > R_{th}\right\} &= \Pr\left\{\frac{1-\alpha}{2}\log_2\frac{1+\gamma_{SR_{n^*}}}{1+\gamma_{SE}} > R_{th}\right\} \\
&= \Pr\left\{\gamma_{SR_{n^*}} > \beta\gamma_{SE} + \beta - 1\right\} \\
&= \Pr\left\{\frac{P_S\left|h_{SR_{n^*}}\right|^2}{N_0} > \beta\frac{P_S\left|h_{SE}\right|^2}{N_0} + (\beta-1)\right\} \\
&= \Pr\left\{\frac{2\eta\alpha}{1-\alpha}\frac{P_B\left|h_{BS}\right|^2}{N_0}\left(\left|h_{SR_{n^*}}\right|^2 - \beta\left|h_{SE}\right|^2 > (\beta-1)\right)\right\} \\
&= \Pr\left\{\left|h_{BS}\right|^2 > \frac{\xi}{z\gamma_B}\right\} = \int_0^{+\infty}\exp\left\{-\frac{\lambda_{BS}\xi}{\gamma_B}\Big/z\right\}f_z(z)\,dz
\end{aligned} \tag{24}$$

where $z = \left|h_{SR_{n^*}}\right|^2 - \beta\left|h_{SE}\right|^2$, $\xi = \frac{(\beta-1)(1-\alpha)}{2\eta\alpha}$, $\gamma_B = \frac{P_B}{N_0}$.

As result in [32, eq.(39)] and use (12), the PDF of z is further shown as

$$\begin{aligned}
f_z(z) &= \int_0^{+\infty} f_{\left|h_{SR_{n^*}}\right|^2}(z+y)\frac{1}{\beta}f_{\left|h_{SE}\right|^2}\left(\frac{y}{\beta}\right)dy \\
&= \int_0^{+\infty} N\lambda_{SR}e^{-\lambda_{SR}(z+y)}\left(1-e^{-\lambda_{SR}(z+y)}\right)^{N-1}\frac{1}{\beta}\left(1-e^{-\lambda_{SE}\frac{y}{\beta}}\right)dy \\
&= \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n\frac{N\lambda_{SR}\overline{\lambda}_{SE}}{\lambda_{SR}(n+1)+\overline{\lambda}_{SE}}\exp\left(-\lambda_{SR}(n+1)z\right)
\end{aligned} \tag{25}$$

where $\overline{\lambda}_{SE} = \frac{\lambda_{SE}}{\beta}$. Then replacing (25) with (24) and in the use of (3.324.1) in [39], we can get

$$\begin{aligned}
\Pr\left\{C_{S_1}^{\mathrm{p}} > R_{th}\right\} &= \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n\frac{N\lambda_{SR}\overline{\lambda}_{SE}}{\lambda_{SR}(n+1)+\overline{\lambda}_{SE}}\int_0^{+\infty}\exp\left(-\frac{4\frac{\lambda_{BS}\xi}{\gamma_B}}{4z} - \lambda_{SR}(n+1)z\right)dz \\
&= \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n\frac{N\lambda_{SR}\overline{\lambda}_{SE}}{\lambda_{SR}(n+1)+\overline{\lambda}_{SE}}2\sqrt{\frac{\lambda_{BS}\xi}{\gamma_B\lambda_{SR}(n+1)}}K_1\left(2\sqrt{\frac{\lambda_{BS}\xi}{\gamma_B}\lambda_{SR}(n+1)}\right)
\end{aligned} \tag{26}$$

In addition, we use the above mentioned method to get the refined expression of $P_r\left\{C_{S_2}^{(\mathrm{p})} > R_{th}\right\}$ as

$$\begin{aligned}\Pr\left\{C_{S_2}^{\mathrm{p}} > R_{th}\right\} &= \Pr\left\{\frac{1-\alpha}{2}\log_2\frac{1+\gamma_{R_n^*D}}{1+\gamma_{R_n^*E}} > R_{th}\right\} \\ &= \Pr\left\{\frac{2\eta\alpha}{1-\alpha}\frac{P_B\left|h_{BR_n^*}\right|^2}{N_0}\left(\left|h_{R_n^*D}\right|^2-\beta\left|h_{R_n^*E}\right|^2\right) > (\beta-1)\right\} \\ &= \Pr\left\{\left|h_{BR_n^*}\right|^2 > \frac{\xi}{\upsilon\gamma_B}\right\} = \int_0^{+\infty}\exp\left\{-\frac{\lambda_{BR}\xi}{\gamma_B}\Big/\upsilon\right\}f_\upsilon(\upsilon)\,d\upsilon\end{aligned} \tag{27}$$

where $\upsilon = \left|h_{R_n^*D}\right|^2-\beta\left|h_{R_n^*E}\right|^2$, $\xi = \frac{(\beta-1)(1-\alpha)}{2\eta\alpha}$, $\gamma_B = \frac{P_B}{N_0}$ and $f_\upsilon(\upsilon) = \frac{\lambda_{RD}\overline{\lambda}_{RE}}{\lambda_{RD}+\overline{\lambda}_{RE}}\exp(-\lambda_{RD}\upsilon)$. Consequently,

$$\begin{aligned}\Pr\left\{C_{S_2}^{\mathrm{p}} > R_{th}\right\} &= \frac{\lambda_{RD}\overline{\lambda}_{RE}}{\lambda_{RD}+\overline{\lambda}_{RE}}\int_0^{+\infty}\exp\left(-4\frac{\lambda_{BR}\xi}{\gamma_B}\Big/\upsilon-\lambda_{RD}\upsilon\right)d\upsilon \\ &= \frac{\lambda_{RD}\overline{\lambda}_{RE}}{\lambda_{RD}+\overline{\lambda}_{RE}}2\sqrt{\frac{\lambda_{BR}\xi}{\gamma_B\lambda_{RD}}}K_1\left(2\sqrt{\frac{\lambda_{BR}\xi}{\gamma_B}\lambda_{RD}}\right)\end{aligned} \tag{28}$$

By substituting the (26) and (28) into (18), after some mathematical manipulation, we have (19).

Appendix B. Derivation of Eq. (20)

Following the same line of derivation used for $P_{S_{out}}^{\mathrm{p}}$, from (18), $P_{S_{out}}^{\mathrm{ip}}$ can be expressed as

$$P_{S_{out}}^{\mathrm{ip}} = 1-P_r\left\{C_{S_1}^{\mathrm{ip}} > R_{th}\right\}P_r\left\{C_{S_2}^{\mathrm{ip}} > R_{th}\right\} \tag{29}$$

We can use the same way in Appendix A to get the $\Pr\left\{C_{S_1}^{\mathrm{ip}} > R_{th}\right\}$ and $\Pr\left\{C_{S_2}^{\mathrm{ip}} > R_{th}\right\}$, but there are some differences in this proof, which are pointed out in Remark 2. Moreover, it is necessary to use (13) for the expression of the imperfect CSI estimation. For the convenience of channel estimation, ε is only considered in first duration of WIT. The expansion can be derived as

$$\begin{aligned}\Pr\left\{C_{S_1}^{\mathrm{ip}} > R_{th}\right\} &= \Pr\left\{\frac{1-\alpha}{2}\log_2\frac{1+\overline{\lambda}_{SR_n^*}}{1+\gamma_{SE}} > R_{th}\right\} \\ &= \Pr\left\{\overline{\lambda}_{SR_n^*} > \beta\gamma_{SE}+\beta-1\right\} \\ &= \Pr\left\{\left|h_{BS}\right|^2 > \frac{\xi}{z\gamma_B}\right\} = \int_0^{+\infty}\exp\left\{-\frac{\lambda_{BS}\xi}{\gamma_B}\Big/ z\right\} f_z\left(z\right)dz\end{aligned} \tag{30}$$

where $z = \left|\overline{h}_{SR_n^*}\right|^2 - \beta\left|h_{SE}\right|^2$.

Firstly, the same as Appendix A, the PDF $f_z\left(z\right)$ in this process can be shown as

$$f_z\left(z\right) = \int_0^{+\infty} f_{\left|\overline{h}_{SR_n^*}\right|^2}\left(z+y\right)\frac{1}{\beta} f_{\left|h_{SE}\right|^2}\left(\frac{y}{\beta}\right)dy \tag{31}$$

where $f_{\left|\overline{h}_{SR_n^*}\right|^2}\left(y\right)$ and $f_{\left|h_{SE}\right|^2}\left(y\right)$, which are the PDFs of $\left|\overline{h}_{SR_n^*}\right|^2$ and $\left|h_{SE}\right|^2$, respectively, can be shown as

$$f_{\left|\overline{h}_{SR_n^*}\right|^2}\left(y\right) = \int_0^{+\infty} f_{\left|\overline{h}_{SR_n^*}\right|^2\left|\left|h_{SR_n^*}\right|^2\right.}\left(y\middle|x\right) f_{\left|h_{SR_n^*}\right|^2}\left(x\right)dx \tag{32}$$

$$f_{\left|h_{SE}\right|^2}\left(y\right) = \lambda_{SE}e^{-\lambda_{SE}y} \tag{33}$$

Correspondingly, the joint PDF $f_{\left|\overline{h}_{SR_n^*}\right|^2\left|h_{SR_n^*}\right|^2}\left(y,x\right)$ of $\left|\overline{h}_{SR_n^*}\right|^2$ and $\left|h_{SR_n^*}\right|^2$ is given by [41], and the conditional PDF can be obtained as

$$f_{\left|\overline{h}_{SR_n^*}\right|^2\left|\left|h_{SR_n^*}\right|^2\right.}\left(y\middle|x\right) = \frac{\lambda_{SR}}{\left(1-\varepsilon\right)}\exp\left(\frac{-\lambda_{SR}\left(y+\varepsilon x\right)}{\left(1-\varepsilon\right)}\right)\mathrm{I}_0\left(\frac{2\lambda_{SR}\sqrt{\varepsilon yx}}{\left(1-\varepsilon\right)}\right) \tag{34}$$

Hence, the PDF $f_{\left|\overline{h}_{SR_n^*}\right|^2}\left(y\right)$ can be obtained as

$$
\begin{aligned}
f_{\left|\bar{h}_{SR_{n^*}}\right|^2}(y) &= \int_0^{+\infty} f_{\left|\bar{h}_{SR_{n^*}}\right|^2 \left\|h_{SR_{n^*}}\right|^2}(y|x)\, f_{\left|h_{SR_{n^*}}\right|^2}(x)\,dx \\
&= \int_0^{+\infty} \frac{\lambda_{SR}}{(1-\varepsilon)} \exp\left(\frac{-\lambda_{SR}(y+\varepsilon x)}{(1-\varepsilon)}\right) \mathrm{I}_0\left(\frac{2\lambda_{SR}\sqrt{\varepsilon yx}}{(1-\varepsilon)}\right) \bullet N\lambda_{SR} e^{-\lambda_{SR}x}\left(1-e^{-\lambda_{SR}x}\right)^{N-1} dx \\
&\overset{\text{power series},(1+x)^N=\sum_{n=0}^{N}\binom{N}{n}x^n}{=} \frac{N\lambda_{SR}{}^2}{(1-\varepsilon)} \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n \exp\left(-\frac{\lambda_{SR}y}{(1-\varepsilon)}\right) \\
&\quad \times \int_0^{+\infty} \exp\left(-\frac{\lambda_{SR}\varepsilon x}{(1-\varepsilon)} - (n+1)\lambda_{SR}x\right) \mathrm{I}_0\left(\frac{2\lambda_{SR}\sqrt{\varepsilon yx}}{(1-\varepsilon)}\right) dx \\
&\overset{\int_0^{+\infty} \mathrm{e}^{-\alpha x}\mathrm{I}_0\left(2\sqrt{\beta x}\right)dx=\frac{1}{\alpha}\exp\left(\frac{\beta}{\alpha}\right)}{=} N\sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n \frac{\lambda_{SR}}{1+(1-\varepsilon)n} \exp\left(-\frac{\lambda_{SR}(n+1)y}{1+(1-\varepsilon)n}\right)
\end{aligned} \tag{35}
$$

By substituting the (35) and (33) into (31), after some mathematical manipulation, we have $f_z(z)$ as follows.

$$
f_z(z) = \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n \frac{N\lambda_{SR}\bar{\lambda}_{SE}}{\lambda_{SR}(n+1)+\bar{\lambda}_{SE}\left[1+(1-\varepsilon)n\right]} \exp\left(\frac{-\lambda_{SR}(n+1)z}{1+(1-\varepsilon)n}\right) \tag{36}
$$

Hence, by substituting the (36) into (30), after some mathematical manipulation, the $\Pr\left\{C_{S_1}^{\mathrm{ip}} > R_{th}\right\}$ can be obtained as

$$
\begin{aligned}
\Pr\left\{C_{S_1}^{\mathrm{ip}} > R_{th}\right\} &= \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n \frac{N\lambda_{SR}\bar{\lambda}_{SE}}{\lambda_{SR}(n+1)+\bar{\lambda}_{SE}+[1+(1-\varepsilon)n]} \times \int_0^{+\infty} \exp(-\frac{\frac{4\lambda_{BS}\xi}{\gamma_B}}{4z} - \frac{\lambda_{SR}(n+1)z}{1+(1-\varepsilon)n})dz \\
&= \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n \frac{N\lambda_{SR}\bar{\lambda}_{SE}}{\lambda_{SR}(n+1)+\bar{\lambda}_{SE}\left[1+(1-\varepsilon)n\right]} \\
&\quad \times 2\sqrt{\frac{\lambda_{BS}\xi\left[1+(1-\varepsilon)n\right]}{\gamma_B\lambda_{SR}(n+1)}} K_1\left(2\sqrt{\frac{\lambda_{BS}\xi}{\gamma_B}\frac{\lambda_{SR}(n+1)}{\left[1+(1-\varepsilon)n\right]}}\right)
\end{aligned} \tag{37}
$$

We can easily get that

$$
\Pr\left\{C_{S_2}^{\mathrm{ip}} > R_{th}\right\} = \Pr\left\{C_{S_2}^{\mathrm{p}} > R_{th}\right\} \tag{38}
$$

With the help of (37) and (38), we have $P_{S_{out}}^{\mathrm{ip}}$ in (20).

Acknowledgement

The authors would like to thank the reviewers and the guest editor for their comments and suggestions.

References

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619-3647, 2018. Article (CrossRef Link).

[2] H. Chen, Y. Li, J. Luiz Rebelatto, B. F. Uchôa-Filho and B. Vucetic, "Harvest-Then-Cooperate: Wireless-Powered Cooperative Communications," *IEEE Transactions on Signal Processing*, vol. 63, no. 7, pp. 1700-1711, April1, 2015. Article (CrossRef Link).

[3] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Communications Magazine*, vol. 52, no. 11, pp. 104-110, Nov. 2014. Article (CrossRef Link).

[4] Y. Zeng and R. Zhang, "Optimized Training Design for Wireless Energy Transfer," *IEEE Transactions on Communications*, vol. 63, no. 2, pp. 536-550, Feb. 2015. Article (CrossRef Link).

[5] H. Ju and R. Zhang, "Throughput Maximization in Wireless Powered Communication Networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 1, pp. 418-428, January 2014. Article (CrossRef Link).

[6] L. Tang and Q. Li, "Wireless Power Transfer and Cooperative Jamming for Secrecy Throughput Maximization," *IEEE Wireless Communications Letters*, vol. 5, no. 5, pp. 556-559, Oct. 2016. Article (CrossRef Link).

[7] Y. Feng, Z. Yang, W. -P. Zhu, Q. Li and B. Lv, "Robust Cooperative Secure Beamforming for Simultaneous Wireless Information and Power Transfer in Amplify-and-Forward Relay Networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2354-2366, March 2017. Article (CrossRef Link).

[8] Y. Liu, H. -H. Chen and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347-376, Firstquarter 2017. Article (CrossRef Link).

[9] X. Chen, D. W. K. Ng, W. H. Gerstacker and H. -H. Chen, "A Survey on Multiple-Antenna Techniques for Physical Layer Security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027-1053, Secondquarter 2017. Article (CrossRef Link).

[10] Y. Huang, P. Zhang, Q. Wu and J. Wang, "Secrecy Performance of Wireless Powered Communication Networks With Multiple Eavesdroppers and Outdated CSI," *IEEE Access*, vol. 6, pp. 33774-33788, 2018. Article (CrossRef Link).

[11] E. Boshkovska, D. W. K. Ng, L. Dai and R. Schober, "Power-Efficient and Secure WPCNs With Hardware Impairments and Non-Linear EH Circuit," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2642-2657, June 2018. Article (CrossRef Link).

[12] B. Li, Z. Fei, C. Zhou and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33-52, Jan. 2020. Article (CrossRef Link).

[13] G. Li, H. Luo, J. Yu, A. Hu and J. Wang, "Information-Theoretic Secure Key Sharing for Wide-Area Mobile Applications," *IEEE Wireless Communications*, pp. 1-8, 2023. Article (CrossRef Link).

[14] Biao He, Xiangyun Zhou, and Thushara D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Communications*, vol. 11, no. 3, pp.11-19, september 2013. Article (CrossRef Link).

[15] Y. Wang, W. Yang, X. Shang, J. Hu, Y. Huang and Y. Cai, "Energy-Efficient Secure Transmission for Wireless Powered Internet of Things With Multiple Power Beacons," *IEEE Access*, vol. 6, pp. 75086-75098, 2018. Article (CrossRef Link).

[16] R. Jiang, K. Xiong, P. Fan, L. Zhou and Z. Zhong, "Outage Probability and Throughput of Multirelay SWIPT-WPCN Networks With Nonlinear EH Model and Imperfect CSI," *IEEE Systems Journal*, vol. 14, no. 1, pp. 1206-1217, March 2020. Article (CrossRef Link).

[17] J. Moon, H. Lee, C. Song and I. Lee, "Secrecy Performance Optimization for Wireless Powered Communication Networks With an Energy Harvesting Jammer," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 764-774, Feb. 2017. Article (CrossRef Link).

[18] G. Pan, C. Tang, T. Li and Y. Chen, "Secrecy Performance Analysis for SIMO Simultaneous Wireless Information and Power Transfer Systems," *IEEE Transactions on Communications*, vol. 63, no. 9, pp. 3423-3433, Sept. 2015. Article (CrossRef Link).

[19] Y. Huang, F. S. Al-Qahtani, T. Q. Duong and J. Wang, "Secure Transmission in MIMO Wiretap Channels Using General-Order Transmit Antenna Selection With Outdated CSI," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2959-2971, Aug. 2015. Article (CrossRef Link).

[20] Z. Chen, L. Hadley, Z. Ding and X. Dai, "Improving Secrecy Performance of a Wirelessly Powered Network," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 4996-5008, Nov. 2017. Article (CrossRef Link).

[21] K. Wang, Y. Li, Y. Ye and H. Zhang, "Dynamic Power Splitting Schemes for Non-Linear EH Relaying Networks: Perfect and Imperfect CSI," in *Proc. of 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Toronto, ON, Canada, pp. 1-5, 2017. Article (CrossRef Link).

[22] J. Zhang, G. Pan and Y. Xie, "Secrecy Analysis of Wireless-Powered Multi-Antenna Relaying System With Nonlinear Energy Harvesters and Imperfect CSI," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 2, pp. 460-470, June 2018. Article (CrossRef Link).

[23] C. Meng, G. Wang and X. Dai, "Secure Energy-Efficient Transmission for SWIPT Intelligent Connected Vehicles With Imperfect CSI," *IEEE Access*, vol. 7, pp. 154649-154658, 2019. Article (CrossRef Link).

[24] D. Wang, B. Bai, W. Chen and Z. Han, "Energy Efficient Secure Communication Over Decode-and-Forward Relay Channels," *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 892-905, March 2015. Article (CrossRef Link).

[25] A. Zappone, P. -H. Lin and E. A. Jorswieck, "Energy-efficient secure communications in MISO-SE systems," in *Proc. of 2014 48th Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, pp. 1001-1005, 2014. Article (CrossRef Link).

[26] J. Farhat, G. Brante, R. D. Souza and J. L. Rebelatto, "Energy Efficiency of Repetition Coding and Parallel Coding Relaying Under Partial Secrecy Regime," *IEEE Access*, vol. 4, pp. 7275-7288, 2016. Article (CrossRef Link).

[27] X. Shang, H. Yin, Y. Wang, M. Li and Y. Wang, "Secure Multiuser Scheduling for Hybrid Relay-Assisted Wireless Powered Cooperative Communication Networks With Full-Duplex Destination-Based Jamming," *IEEE Access*, vol. 9, pp. 49774-49787, 2021. Article (CrossRef Link).

[28] Y. Wang, H. Yin, T. Zhang, W. Yang, X. Shang and Y. Shen, "Secure Transmission for Energy-Harvesting Sensor Networks With a Buffer-Aided Sink Node," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6703-6718, 1 May, 2022. Article (CrossRef Link).

[29] A. -N. Nguyen, V. Nhan Vo, C. So-In, D. -B. Ha, S. Sanguanpong and Z. A. Baig, "On Secure Wireless Sensor Networks With Cooperative Energy Harvesting Relaying," *IEEE Access*, vol. 7, pp. 139212-139225, 2019. Article (CrossRef Link).

[30] Z. Zhu, N. Wang, W. Hao, Z. Wang and I. Lee, "Robust Beamforming Designs in Secure MIMO SWIPT IoT Networks With a Nonlinear Channel Model," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1702-1715, 1 Feb.1, 2021. Article (CrossRef Link).

[31] J. Ren, X. Lei, P. D. Diamantoulakis, Q. Chen and G. K. Karagiannidis, "Buffer-Aided Secure Relay Networks With SWIPT," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6485-6499, June 2020. Article (CrossRef Link).

[32] X. Kang, Y. -C. Liang and J. Yang, "Riding on the Primary: A New Spectrum Sharing Paradigm for Wireless-Powered IoT Devices," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6335-6347, Sept. 2018. Article (CrossRef Link).

[33] T. M. Hoang, T. Q. Duong, N. -S. Vo and C. Kundu, "Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 174-177, April 2017. Article (CrossRef Link).

[34] V. Nhan Vo, T. G. Nguyen, C. So-In, Z. A. Baig and S. Sanguanpong, "Secrecy Outage Performance Analysis for Energy Harvesting Sensor Networks With a Jammer Using Relay Selection Strategy," *IEEE Access*, vol. 6, pp. 23406-23419, 2018. Article (CrossRef Link).

[35] H. Chen, C. Zhai, Y. Li and B. Vucetic, "Cooperative Strategies for Wireless-Powered Communications: An Overview," *IEEE Wireless Communications*, vol. 25, no. 4, pp. 112-119, AUGUST 2018. Article (CrossRef Link).

[36] C. Meng, G. Wang and X. Dai, "Secure Energy-Efficient Transmission for SWIPT Intelligent Connected Vehicles With Imperfect CSI," *IEEE Access*, vol. 7, pp. 154649-154658, 2019. Article (CrossRef Link).

[37] M. Li, H. Yin, Y. Huang, Y. Wang and R. Yu, "Physical Layer Security of WPCNs With Imperfect CSI and Full-Duplex Receiver Aided Jamming," *IEEE Access*, vol. 7, pp. 55318-55328, 2019. Article (CrossRef Link).

[38] O. O. Koyluoglu, C. E. Koksal and H. E. Gamal, "On Secrecy Capacity Scaling in Wireless Networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000-3015, May 2012. Article (CrossRef Link).

[39] Gradshteyn I. S., Ryzhik I. M., *Table of integrals, series, and products*, 7th ed., New York, USA: Academic, 2007. Article (CrossRef Link).

[40] M. Xia and S. Aissa, "On the Efficiency of Far-Field Wireless Power Transfer," *IEEE Transactions on Signal Processing*, vol. 63, no. 11, pp. 2835-2847, June1, 2015. Article (CrossRef Link).

[41] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2st ed., New York, USA: John Wiley and Sons, 2005, pp. 170-171. Article (CrossRef Link).

Yajun Zhang received his B.S. degree from Institute of Communications Engineering of Chongqing University, Chongqing, China, in 2009, M.S. and Ph.D. degree from Institute of Communications Engineering, PLA University of Science and Technology (PLAUST), Nanjing, China, in 2012 and 2016, respectively. Since 2016, he has been a lecturer with the Army Academy of Artillery and Air Defense (Nanjing Campus). His current research interest includes cooperative communications, physical layer security, and wireless powered communication.

Jun Wu received his B.S. degree from Nanjing Institute of Technology, Nanjing, China, in 2004, M.S. degree in the army artillery college of PLA, in 2007 and received PhD degree in the army military academy of PLAc, Hefei China in 2021. He has been a associate Professor with the Army Academy of Artillery and Air Defense (Nanjing Campus). His current research interest includes command and control communications, signal processing, and performance evaluation.

Bing Wang received his B.S. degree from the army artillery college of PLA, Nanjing, China, in 2005. He has been a Professor with the Army Academy of Artillery and Air Defense (Nanjing Campus). His current research interest includes information assurance, Intelligence, and Reconnaissance.

Hongkai Wang received his B.S. degree from Institute of Mechanical Engineering of Jilin University, Changchun, China, in 2009, M.S. and Ph.D. degree from Dept. of Artillery Engineering, Ordnance Engineering College, ShijiaZhuang, China, in 2012 and 2016, respectively. Since 2016, he has been a lecturer with the Army Academy of Artillery and Air Defense (Nanjing Campus). His current research interest includes artificial intelligence, efficiency analysis, and dynamic simulation.

Xiaohui Shang received his B.S. degree in communication engineering from Harbin Institute of Technology (HIT) in 2009, M.S. degree in communication and information system from PLA University of Science and Technology (PLAUST), in 2012 and received PhD degree in communication and information system from the College of Communications Engineering, Army Engineering University of PLA, Nanjing China in 2021. His research interests are focus on physical layer security, cooperative communications, wireless powered communication networks, energy harvesting etc.