Secrecy outage probability analysis of energy-aware relay selection for energy-harvesting cooperative systems

Yujie Zhang 1,2 | Peng Li 1 | Weibei Fan 1 | Ruchuan Wang 2

1 School of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (Email: zhangyujie@njupt.edu.cn; wbfan@njupt.edu.cn)
2 Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Jiangsu Province, Nanjing 210003, China

Abstract
The secrecy outage performance for a cooperative cognitive radio energy-harvesting network is analyzed. The cognitive network is composed of an energy-constrained cognitive source (CS), multiple energy-constrained cognitive relays (CRs) and a cognitive destination (CD) as well as an eavesdropper (E) coexists with a primary network consisting of a primary transmitter (PT) and a primary receiver (PR). The CS and CRs are equipped with energy harvesters for collecting energy from the radio frequency signal from PT and their transmit powers are limited by the interference threshold at PR. To prevent confidential information leaking to E, an optimal relay selection (ORS) scheme and a suboptimal relay selection (SRS) scheme are proposed. In ORS scheme, the whole channels state information (CSI) of wireless links is available to CRs while SRS only needs to know the CSI of main channels from CRs to CD. Moreover, the closed-form expressions of secrecy outage probabilities for both ORS and SRS schemes are derived. For the purpose of comparison, the classical round-robin relay selection (RRRS) is also analyzed in terms of secrecy outage probability. Furthermore, the numerical results show that ORS achieves the best performance and RRRS performs the worst in terms of secrecy outage probability.

1 | INTRODUCTION

1.1 | Background

Energy efficiency and management of the fifth generation wireless networks have attracted much attention from academia and industry. Energy-harvesting technique can effectively improve energy efficiency [1–3]. Simultaneous wireless information and power transfer (SWIPT) [4–6] is one of the energy-harvesting technology, which delivers information and energy by utilizing the same electromagnetic wave. There are two different types in relaying SWIPT, namely time-switching relaying (TSR) protocol [7, 8] and power-splitting relaying (PSR) protocol [9, 10]. In TSR protocol, the relay collects energy from the radio frequency signal during the energy-harvesting phase, and the harvested energy is exploited to handle the received information and forward it to destination in the information transmission phase [7, 8]. Differing from TSR, the received energy is divided into two different parts, which are employed to transmit private information and energy storage [9, 10]. Cognitive radio (CR) [11, 12] can effectively solve the scarcity of spectrum resources. To elaborate, CR allows secondary users to dynamically share the licensed spectrum with primary users, providing the quality-of-service of primary communications can be guaranteed. However, the confidential information of SWIPT and CR still face the information leakage threat due to the broadcast nature of wireless communications.

1.2 | Related works

Physical-layer security [13, 14] has emerged as an effective method to prevent eavesdropping attackers, which utilizes the physical characteristics of wireless mediums. In [15], the secrecy capacity which is the difference between the capacity of source to destination and the source to vicious eavesdroppers that...
is introduced for the first time. Moreover, the research findings illustrated that the perfectly secure can be guaranteed if the secrecy capacity is bigger than zero. However, the secrecy capacity is limited by the wireless fading effects [16, 17]. To combat with fading effects and increase the secrecy capacity, multiple-input multiple-output (MIMO) [13, 14, 18–20], cooperative communication [21, 22] and artificial noise [23, 24] were exploited. Specifically, Yan et al. [19] studied the secret cognitive transmission in a MIMO system and the analysis of secrecy diversity was carried out over Rayleigh fading channels. In [22], the authors employed relay selection to improve the secrecy capacity and the closed-form expressions of secrecy outage probabilities for optimal relay selection and suboptimal relay selection were derived. In [24], the artificial noise was generated to enhance physical-layer security. Moreover, the effect of system parameters on secrecy rate was theoretically discussed.

Presently, physical-layer security based on energy harvesting technique [25–34] is a hot topic. In [35], the authors employed the best relay with either amplify-and-forward or decode-and-forward to assist the communication between source and destination. The results shown that decode-and-forward protocol outperforms amplify-and-forward protocol in terms of secrecy outage performance. Differing from [35], the authors in [27, 31, 36] considered two-way relaying protocol. To elaborate, Li et al. [27] maximized the achievable secrecy rate under the two different scenarios where the channel state information (CSI) of wiretap is available and unavailable. Due to the non-convexity of this problem, the 2D search was utilized to obtain the secrecy rate. In [31], the secrecy performance was investigated for a two-way untrusted relay system with amplify-and-forward protocol. The secure time-switching relay and power-splitting relay were proposed to enhance the performance in terms of secrecy energy efficiency.

However, the works on physical-layer security combining with energy-harvesting technique [25–31, 35] merely discussed on non-cognitive radio systems, while [37–42] examined the private cognitive transmission. In [37], the multiuser scheduling was exploited to fight against eavesdroppers. Basing on the CSI of energy-harvesting links known or unknown for cognitive users, energy-aware multiuser scheduling (EARTH) and conventional multiuser scheduling (CMUS) are proposed to improve the security-reliability tradeoff performance. In [38], the authors theoretically analyzed the secrecy outage performance of optimal antenna selection (OAS) and suboptimal antenna selection (SAS). Additionally, the analysis of secrecy diversity was carried out to show an intuitive insight into the effect of number of antennas on the secrecy outage performance [40], jointly considered the QoS of both primary users and secondary users. More specifically, the transmit beamforming vector was designed to maximize the security of primary users while ensuring the reliability of secondary users.

Additionally, the cooperative relaying technique with energy-harvesting technology was widely employed in physical-layer security for cognitive radio systems [41, 43]. For example, the optimal relay selection (ORS) with EH was proposed to ameliorate the wireless physical layer security [41]. The results indicated that the ORS with EH outperforms ORS without EH in terms of the tradeoff between secrecy outage probability of primary transmission and ergodic rate of cognitive transmission. In [43], the authors designed the beam-forming vectors to protect the information leakage for a two-way internet of things system. Specifically, branch-reduce-and-bound (BRB)-based algorithm was proposed to derive the expression of secrecy sum rate for primary users. In [44], authors proposed a mobile relay based system model for high-speed trains wireless communications, and derived novel exact closed-form expressions for the corresponding outage probability. In [45], the authors presented novel routing policies that make use of mobility information from the relays to reduce energy consumption. Furthermore, the iterative algorithm constrained-convex concave programming (CCCP) and a non-iterative algorithm based on zero forcing were used to reduce the computational complexity of BRB, and the effectiveness of CCCP and ZF were verified by the simulation results.

\subsection{1.3 Motivation and contributions}

To the best of our knowledge, less existing literatures focused on the secrecy outage performance for a cooperative cognitive radio system with energy-harvesting technique (CCR-EH). Consequently, we examine the physical-layer security for a CCR-EH system, where a secondary system consisting of a energy-constrained cognitive source (CS) and multiple energy-constrained cognitive fixed relays (CRs) as well as a cognitive destination (CD) coexists with a primary system. The main contributions are described as follows.

First, we explore physical-layer security for an energy harvesting underlay cognitive radio system and propose optimal relay selection (ORS) and suboptimal relay selection (SAS) to enhance the secrecy performance for our considered CCR-EH system. In the SAS scheme, only the CSI of main channels of CRs-CD is available. However, the ORS scheme needs to know the whole CSI of wireless channels including wiretap channels of CRs-E. We derive closed-form expressions of outage probability (OP) and intercept probability (IP) for the SRS scheme and our proposed ORS scheme over Rayleigh fading channels. For the purpose of comparison, we also present the analysis of the secrecy outage performance for classical round-robin relay selection (RRRS) scheme. The research findings indicate that ORS scheme is the best and RRRS scheme performs the worst in view of the secrecy outage performance.

Second, it needs to be pointed out that we examine the secrecy outage performance in a CCR-EH system, while [30, 35] merely considered physical-layer security for an energy-harvesting cooperative system without cognitive radio, differing from [4, 5], which only studied the reliable transmission between source and destination with the help of relay. The security is also an important metric of cognitive transmission. Thus, we analyze the secrecy performance for a CCR-EH system.

The rest of this paper is organized as follows. We provide the system model for a CCR-EH system in Section 2. In Section 3, we present the theoretical analysis of secrecy outage performance for RRRS, SRS and ORS scheme over Rayleigh fading.
and CR, can be given by
\[ E_i = \alpha \eta T P_i |h_i|^2, \]  
and
\[ E_i = \alpha \eta T P_i |h_i|^2. \]

To guarantee the quality-of-service (QoS) of primary communications, the transmit powers of CS and CR, can be written as
\[ P_i = \min \left( \frac{2\alpha \eta}{1 - \alpha} P_i |h_i|^2, \frac{|I|}{|h_i|^2} \right), \]
and
\[ P_i = \min \left( \frac{2\alpha \eta}{1 - \alpha} P_i |h_i|^2, \frac{|I|}{|h_i|^2} \right), \]
where \( \eta (0 \leq \eta \leq 1) \) is the energy conversion efficiency and \( P_p \) is the transmit power of PT.

In the second phase \((1 - \alpha)T/2, \) CS transmits confidential information to CR. Consequently, the wireless channel capacity of CS-CR, can be expressed as
\[ C_{\alpha} = \frac{(1 - \alpha)T}{2} \log_2 \left( 1 + \frac{P_i |h_i|^2}{N_0} \right), \]
where \( P_i \) is the transmit power of CR. Due to the openness and broadcast nature of wireless communications, the wireless channel capacity of CR, to E can be written as
\[ C_{\alpha} = \frac{(1 - \alpha)T}{2} \log_2 \left( 1 + \frac{P_i |h_i|^2}{N_0} \right). \]

Basing on [46, 47], we consider all relays in our paper employ DF to decode the received signal. To elaborate, the results in [46] indicated that DF protocol has a higher probability of successful decoding and flawless retransmission from a shorter distance than AF protocol if the relay is closer to the source. Additionally, the analysis illustrated that DF performs better than AF in terms of secrecy outage performance, and provided a low and medium signal-to-noise ratio (SNR) at destination [47]. Hence, we employ DF relaying protocol to decode the source signal. Specifically, only the relay succeeding in recovering the received signal can participate in forwarding the source signal to CD. For
similarly, let \( D \) to be a set where the elements mean that CRs who can succeed in decoding the signal from CS. Therefore, the sample space of \( D \) can be given by

\[
\mathcal{w} = \{ \phi, D_1, D_2, \ldots, D_{2^N-1} \},
\]

where \( \phi \) means that all CRs fail to decode received signal, and \( D_i \) is the \( i \)-th null set. Using the Shannon theory, the case \( D = \phi \) and \( D = D_i \) can be respectively represented as

\[
D = \phi, \{ C_{ij} < R | i = 1, 2, 3, \ldots, N_i \},
\]

and

\[
D = D_a, \left\{ C_{ij} > R, C_{ij} < R | i \in D_a, j \in \overline{D}_a \right\},
\]

where

\[
C_{ij} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{P_iR | b_{ij} |^2}{N_0} \right)
\]

and \( \overline{D}_a \) denotes the complementary set of \( D_a \).

3  SECRECY OUTAGE PROBABILITY OVER RAYLEIGH FADING CHANNELS

3.1  Round-Robin relay selection

This subsection provides the analysis of RRRS scheme in terms of secrecy outage probability. Rayleigh fading model is the basis of the wireless channel model, which is widely used in the study of the physical layer security of cognitive radio systems\cite{39},\cite{19}. We propose RRRS scheme over Rayleigh fading channels, and all CRs in set \( D_a \) have an equal chance to access the licensed spectrum to transmit its data information. Moreover, the secrecy outage event will happen when the secrecy capacity of wireless transmission is less than the data rate \( R \), yielding

\[
P_{\text{out},i}^{\text{RRRS}} = \Pr(C_{id} < R, D = \phi) + \Pr(C_{id} - C_{id} < R, D = D_i),
\]

where \( C_{id} \) and \( C_{id} \) are given by (6) and (7). Combining (9) with (12), we can further simplify the secrecy outage probability of RRRS scheme to

\[
P_{\text{out},i}^{\text{RRRS}} = \Pr(D = \phi) + \Pr(C_{id} - C_{id} < R, D = D_i).
\]

By substituting (5) and (6) as well as (7) into (13), we can further obtain

\[
P_{\text{out},i}^{\text{RRRS}} = \prod_{i=1}^{N} \vartheta_i + \sum_{a=1}^{2^N-1} \prod_{i \in D_a} (1 - \vartheta_i) \prod_{j \in \overline{D}_a} \vartheta_{i,j} P_{\text{out},i}^{\text{RRRS}},
\]

where \( \vartheta_i \) and \( \vartheta_{i,j} \) can be separately written as

\[
\vartheta_i = \Pr \left[ \min(\delta \gamma_j | b_{ji} |^2, \frac{\gamma_j}{| b_{ji} |^2}) | b_{ij} |^2 < \gamma \right],
\]

\[
\vartheta_{i,j} = \Pr \left[ \min(\delta \gamma_j | b_{ji} |^2, \frac{\gamma_j}{| b_{ji} |^2}) | b_{ij} |^2 < \gamma \right],
\]

and

\[
P_{\text{out},i}^{\text{RRRS}} = \frac{1}{|D_a|} \sum_{j=1}^{D_1} \Pr \left[ \min(\delta \gamma_j | b_{ji} |^2, \frac{\gamma_j}{| b_{ji} |^2}) | b_{ij} |^2 < \gamma \right.
\]

\[
+ (\gamma + 1) \min(\delta \gamma_j | b_{ji} |^2, \frac{\gamma_j}{| b_{ji} |^2}) | b_{ij} |^2 \right],
\]

where \( \gamma_i = P_i/N_0, \gamma_j = I_j/N_0, \delta = 2\alpha \eta / (1 - \alpha), \gamma = 2\beta \eta / (\gamma - \alpha) - 1 \) and \( |D_a| \) represents the number of set. It is clear for us to see that the closed-form expressions of \( \vartheta_i, \vartheta_{i,j} \) and \( P_{\text{out},i}^{\text{RRRS}} \) are important to derive the theoretical results for \( P_{\text{out},i}^{\text{RRRS}} \). Using the results of Appendix A and Appendix B, we can readily get

\[
\vartheta_i = 1 - \frac{\gamma_j}{\sigma_j^2} \sqrt{\sum_k K_k (\sqrt{\sum_i s_i})}
\]

\[
+ \sqrt{\sum_i s_i} K_k (\sqrt{\sum_i s_i}) - \sqrt{\sum_j s_j} K_k (\sqrt{\sum_j s_j})
\]

\[
\vartheta_{i,j} = 1 - \frac{\gamma_j}{\sigma_j^2} \sqrt{\sum_k K_k (\sqrt{\sum_i s_i})}
\]

\[
+ \sqrt{\sum_i s_i} K_k (\sqrt{\sum_i s_i}) - \sqrt{\sum_j s_j} K_k (\sqrt{\sum_j s_j})
\]

(18)

(19)

where \( K_i(x) \) is the first order modified Bessel function of the second kind \cite{48}, \( s_1 = 4(\delta \gamma_j | b_{ki} |^2) \) and \( s_2 = \gamma | b_{ij} |^2 + \gamma | b_{ij} |^2 \). Moreover, the expression of \( \vartheta_{i,j} \) is similar to \( \vartheta_i \). Thus, \( \vartheta_i \) can be obtained by replacing \( \sigma_j^2 \) in (18) with \( \sigma_j^2 \), yielding

\[
\vartheta_{i,j} = 1 - \frac{\gamma_j}{\sigma_j^2} \sqrt{\sum_k K_k (\sqrt{\sum_i s_i})}
\]

\[
+ \sqrt{\sum_i s_i} K_k (\sqrt{\sum_i s_i}) - \sqrt{\sum_j s_j} K_k (\sqrt{\sum_j s_j})
\]

In addition, relying on the results of Appendix B, we can rewrite \( P_{\text{out},i}^{\text{RRRS}} \) as

\[
P_{\text{out},i}^{\text{RRRS}} = \frac{1}{|D_a|} \sum_{j=1}^{D_1} \left[ \frac{\gamma_j}{\sigma_j^2} + \frac{\gamma_j}{\sigma_j^2} + \sqrt{\sum_k K_k (\sqrt{\sum_i s_i})} + \sqrt{\sum_i s_i} K_k (\sqrt{\sum_i s_i}) \right]
\]

(20)
Let us substitute (18), (19) and (20) into (14); we can compute the closed-form expression of $P_{\text{out}}^{\text{ORS}}$ as (21) at the top of the following page.

$$
P_{\text{out}}^{\text{ORS}} = \prod_{i=1}^{N} (1 - \frac{P_i}{N_0}) \left[ \frac{1}{K_i(\sqrt{s_i^2(\gamma_j^2)})} \right] \prod_{m=1}^{2^{N-1}} \prod_{i=1}^{N} \left[ \frac{1}{K_i(\sqrt{s_i^2(\gamma_j^2)})} \right] \prod_{i=1}^{N} \sum_{m=1}^{D_n} \left[ \frac{1}{K_i(\sqrt{s_i^2(\gamma_j^2)})} \right],
$$

(21)

wherein, $p_{\text{ORS}}^{\text{out},b}$ can be given by

$$
p_{\text{ORS}}^{\text{out},b} = \Pr[\min(\delta y_j^2, b_{\text{pd}}^2, \frac{r_j}{|b_{\text{pd}}|^2}) < \gamma] + (\gamma + 1) \min(\delta y_j^2, b_{\text{pd}}^2, \frac{r_j}{|b_{\text{pd}}|^2}),
$$

(27)

where $b_{\text{pd}}$ and $b_{\text{pd}}^2$ respectively, represent the channel gains from PT to CR$_b$ and CR$_d$ to PD. Using the law of total probability and denoting $z = \min(\delta y_j^2, b_{\text{pd}}^2, \frac{r_j}{|b_{\text{pd}}|^2})$, $p_{\text{ORS}}^{\text{out},b}$ can be reformulated as

$$
p_{\text{ORS}}^{\text{out},b} = \sum_{m=1}^{2^{D_n}} \Pr[|b_{\text{pd}}|^2 < \gamma] + (\gamma + 1) \frac{\max_{k \in \{1, \ldots, D_n\}} |b_{\text{pd}}|^2}{|b_{\text{pd}}|^2},
$$

(28)

However, the best relay in SRS scheme merely depends on the CSIs of wireless channels from CRs to CD, thereby causing the random relay selection for E, and the probability density function (PDF) of $|b_{\text{pd}}|^2$ is the same as $|b_{\text{pd}}|^2$. Similarly, the PDFs of $|b_{\text{pd}}|^2$ and $|b_{\text{pd}}|^2$ are the same as $|b_{\text{pd}}|^2$ and $|b_{\text{pd}}|^2$. Basing on the results of Appendix C and substituting (15), (16) and (23) into (22), the closed-form expressions of secrecy outage probability can be obtained as

$$
p_{\text{ORS}}^{\text{out},b} = 1 + \sum_{m=1}^{2^{D_n}-1} \kappa(m) \left[ \kappa^2 \sum_{i=0}^{D_n} \left( \sqrt{\frac{r_j}{\sigma_i^2}} K_i(\sqrt{\frac{r_j}{\sigma_i^2}}) \right) \right],
$$

(29)

where $\kappa(m) = (-1)^{|D_n(n)|}/\left(1 + \sigma_i^2(y + 1) \sum_{i \in D_n} \sigma_i^{-2}\right)$. Therefore, the closed-form expression of secrecy outage probability of SRS scheme can be given by (30) at the following page.

$$
p_{\text{ORS}}^{\text{out},b} = \prod_{i=1}^{N} (1 - \frac{P_i}{N_0}) \sum_{i=1}^{2^{N-1}} \prod_{m=1}^{N} (1 - \delta_t) \prod_{i \in D_n} \delta_t p_{\text{ORS}}^{\text{out},b},
$$

(26)

3.2 Suboptimal relay selection scheme

In this section, we propose SRS scheme to enhance the physical layer security for cognitive communications with energy-harvesting technique, which only relies on the CSI of main channels from CRs to CD. To be more specific, the CR$_b$ maximizing the wireless channel capacity of CR$_b$-CD can be selected as an optimal relay to help the cognitive transmission from CS to CD. As a consequence, the selection criterion can be described as

$$
b = \arg \max_{i \in D_n} |b_{id}|^2,
$$

(22)

where $D_n$ is described as (10). Therefore, the corresponding wireless channel capacity of CR$_b$-CD can be written as

$$
C_{bd} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{P_i|b_{id}|^2}{N_0} \right),
$$

(23)

where $P_i$ means the transmit power of CR$_b$ and $b_{id}$ is the channel gain of the optimal CR to CD. Additionally, the wireless channel capacity of CR$_b$-E can be given by

$$
C_{be} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{P_i|b_{be}|^2}{N_0} \right),
$$

(24)

where $b_{be}$ is the channel gain of the optimal CR to E. Basing on (23) and (24), the secrecy outage probability of SAS scheme can be formulated as

$$
P_{\text{ORS}}^{\text{out},b} = \Pr(C_{bd} < R, D = \phi) + \Pr(C_{bd} - C_{be} < R, D = D_n),
$$

(25)

which is similar to (13). Hence, $p_{\text{ORS}}^{\text{out},b}$ can be further expressed as

$$
p_{\text{ORS}}^{\text{out},b} = \prod_{i=1}^{N} \delta_t + \sum_{m=1}^{2^{N-1}} \prod_{i \in D_n} (1 - \delta_t) \prod_{i \in D_n} \kappa \delta_t p_{\text{ORS}}^{\text{out},b},
$$

(26)

3.3 Optimal relay selection scheme

This section provides our proposed ORS scheme to improve the secrecy outage performance for cognitive communications.
Differing from SRS scheme, ORS scheme chooses an optimal relay which maximizes the secrecy capacity basing on the whole CSI of all wireless links. Therefore, the ORS relay selection criterion can be defined as

$$O = \max_{\mathcal{A} \in D_s} \left[ \frac{1 + \min(\delta r_p|b_{id}|^2, y_r|b_{id}|^2)}{1 + \min(\delta r_p|b_{id}|^2, y_r|b_{id}|^2)} \right].$$

(31)

Thus, we can obtain the wireless channel capacity of $\text{CR}_s$-CD as

$$C_{\text{cd}} = \frac{(1 - \alpha)T}{2} \log_2(1 + \frac{P|h_{cd}|^2}{N_0}),$$

(32)

where $P$ and $h_{cd}$ mean the transmit power of $\text{CR}_s$ and the channel gain of $\text{CR}_s$-CD. Additionally, the wireless capacity of wiretap channel is obtained as

$$C_{\text{we}} = \frac{(1 - \alpha)T}{2} \log_2(1 + \frac{P|h_{we}|^2}{N_0}),$$

(33)

where $h_{we}$ represents the channel gain of channel from $\text{CR}_s$ to $E$. As a consequence, the secrecy outage probability of ORS scheme can be written as

$$P_{\text{out}}^{\text{ORS}} = \Pr(C_{\text{cd}} < R, D = \phi) + \Pr(C_{\text{cd}} - C_{\text{we}} < R, D = N_s),$$

(34)

which is similar to (12) and (26). Therefore, $P_{\text{out}}^{\text{ORS}}$ can be further simplified to

$$P_{\text{out}}^{\text{ORS}} = \prod_{n=1}^{N_s} \sum_{a=1}^{2^{N_s-1}} \prod_{i \in D_s} (1 - \bar{\delta}_i) \prod_{j \in D_s} \bar{\delta}_j P_{\text{out},a}^{\text{ORS}},$$

(35)

wherein, $P_{\text{out},a}$ can be represented by

$$P_{\text{out},a}^{\text{ORS}} = \Pr[|b_{id}|^2 < \gamma + (\gamma + \epsilon)|\gamma|b_{id}|^2]$$

$$= \prod_{i \in D_s} \Pr[|b_{id}|^2 < \gamma + (\gamma + \epsilon)|\gamma|b_{id}|^2]$$

(36)

where $\epsilon = \min(\delta r_p|b_{id}|^2, y_r|b_{id}|^2)$ and $s$ have been given in (27). Consequently, comparing $P_{\text{out},a}^{\text{ORS}}$ with (17), we can compute (36) as

$$P_{\text{out},a}^{\text{ORS}} = \prod_{i \in D_s} \left[ \frac{s^2}{s^2 + (\gamma + \epsilon)s^2} \left( \sqrt{\frac{s^2}{\sigma^2_{id}}} K_i\left(\sqrt{\frac{s^2}{\sigma^2_{id}}}\right) + \sqrt{\frac{s^2}{\sigma^2_{id}}} \right) \times K_i\left(\sqrt{\frac{s^2}{\sigma^2_{id}}}\right) \right] \left(\frac{\gamma_i}{\sigma^2_{id}} \right)^{\frac{1}{2}} \sqrt{\frac{\gamma_i}{\sigma^2_{id}}} K_i\left(\sqrt{\frac{\gamma_i}{\sigma^2_{id}}}\right) \right].$$

(37)

Thus, the closed-form expression of $P_{\text{out}}^{\text{ORS}}$ can be computed as (38) at the top of next page.

FIGURE 2 Secrecy outage probabilities of RRRS and SRS as well as ORS scheme versus $\gamma_p$ with $\alpha = 0.4, \gamma_r = 10$ dB, $\sigma^2_r = \sigma^2_p = 1, \sigma^2_{id} = \sigma^2_{ip} = \sigma^2_{ps} = 0.1$, $T = 1$ s, $N_s = 10$ and $R = 0.4$bit/s/Hz for different $\eta$

4 | NUMERICAL RESULTS AND DISCUSSIONS

In this section, we realize numerical simulation through MATLAB and provide the theoretical and simulated results to highlight the impact of different related values of cooperative cognitive radio systems with energy-harvesting The correctness of our closed-form expressions of secrecy outage probabilities of RRRS and SRS as well as ORS scheme are verified by Monte-Carlo simulations. In addition, data rate is set as $R = 0.4$bit/s/Hz, total communication time $T = 1$ s and $\sigma^2_i = \sigma^2_{id} = 1$. The specific values assigned to system parameters are referred to in [37] and [39]. Moreover, “$T$” represents the theoretical result and “Simulation” denotes the simulated results.

In Figure 2, we plot the curves of secrecy outage probabilities of RRRS and SRS as well as our proposed ORS scheme versus $\gamma_p$ for different $\eta$. It is clear for us to see that our theoretical results match well with the simulated results, which shows the correctness of our theoretical analysis in terms of secrecy outage probabilities for RRRS, SRS and ORS scheme. From

Figure 2, as the power of primary transmitter $\gamma_p$ increases, the secrecy outage probabilities of RRRS and SRS as well as proposed ORS scheme decrease accordingly. This phenomenon can be explained such that an increasing power $\gamma_p$ causes cognitive users to harvest more energy and transmit data information with higher power, resulting in significantly improved secrecy outage performance of all schemes. Figure 2 also illustrates that the physical-layer security of cognitive communications is greatly enhanced by an increasing $\eta$ from 0.2 to 0.8, which results from the fact that more energy can be exploited to transmit private information. Moreover, ORS scheme and SRS scheme outperform the classical RRRS scheme in terms of secrecy outage probability, implying the security benefits of our proposed scheme.

Figure 3 shows the secrecy outage probabilities of RRRS, SRS and ORS scheme versus $\gamma_p$ for different $N_r$. It is shown from Figure 3 that the classical RRRS scheme fails to achieve the secrecy benefits with an increasing number of CRs. This means that the number of CRs has no obvious effect on the secrecy outage performance, which can be explained by the fact that all relays succeeding in recovering the source signal have an equal chance to access the licensed spectrum to assist the transmission from CS to CD. By contrast, as the number of CRs increases from $N_r = 2$ to $N_r = 8$, the secrecy outage probabilities of SRS scheme and our proposed ORS scheme significantly decrease. Moreover, the performance superiority of our ORS and SRS will become increasingly apparent with an increasing number of CRs.

Figure 4 depicts the secrecy outage probabilities of RRRS, SRS and ORS scheme versus energy harvesting time allocation ratio $\alpha$. The secrecy outage performance of ORS scheme performs the best and that of RRRS scheme is the worst among three schemes. It is clear for one to observe that the secrecy outage probabilities of RRRS, SRS and our proposed ORS scheme can arrive at the minimum by choosing an appropriate $\alpha$. In other words, we can achieve the best performance by performing the energy harvesting time allocation between energy collection and cognitive transmission. Figure 5 shows the secrecy outage probabilities of the classical RRRS, SRS and ORS schemes versus $\gamma_p$ for different MER ($\sigma_i^2/\sigma_e^2$). One can clearly observe that the secrecy outage performance of ORS scheme and SRS scheme as well as the classical RRRS scheme significantly enhances result from MER increases from $-10$ to 10.
5 | CONCLUSION

This paper has employed relay selection to improve the physical-layer security for a CCR-EH system consisting of a CS, multiple CRs and a CD in the face of an E. The CS and CRs have energy harvesters to collect energy from the radio frequency signal of PT. To elaborate, ORS scheme basing on the whole CSI of wireless links and SRS scheme merely depending on the CSI of main links from CRs to CD have been proposed to prevent an E overhearing the confidential information. Moreover, in order to achieve the purpose of comparison, the secrecy outage performance of classical RRRS scheme was carried out. The numerical results show that both our proposed ORS scheme and SRS scheme outperform RRRS in terms of secrecy outage probability. Furthermore, when relays are mobile, the time-varying nature of fading channels renders the provision of accurate CSI challenging; our future research will focus on the secrecy outage performance optimization with mobile relays.

ORCID
Yujie Zhang https://orcid.org/0000-0001-5511-9373

REFERENCES
1. Abedi, M., Masoumi, H., Emadi, M.J.: A Survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE Wireless Commun. Lett. 8(2), 432–435 (2019)
2. Lim, D., Kang, J., Kim, H.: Adaptive power control for D2D communications in downlink SWIPT networks with partial CSI. IEEE Wireless Commun. Lett. 8(5), 1333–1336 (2019)
3. Jang, S., et al.: Energy efficient SWIPT systems in multi-cell MISO networks. IEEE Trans.Wireless Commun. 17(12), 8180–8194 (2018)
4. Liu, Y., et al.: Wireless energy harvesting in a cognitive relay network. IEEE Trans.Wireless Commun. 15(4), 2498C2508 (2016)
5. Chen, Z., et al.: Cooperative transmission in simultaneous wireless information and power transfer networks. IEEE Trans. Veh. Technol. 65(10), 8710–8715 (2016)
6. Ng, D.W.K., Lo, E.S., Schober, R.: Multiojective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer. IEEE Trans. Veh. Technol. 65(5), 3166C3184 (2016)
7. Liu, Y., et al.: Wireless energy harvesting in a cognitive relay network. IEEE Trans. Wireless Commun. 15(4), 2498–2508 (2016)
8. Xu, C., et al.: Outage performance of underlay multihop cognitive relay networks with energy harvesting. in IEEE Commun. Lett. 20(6), 1148–1151 (2016)
9. Liu, H., et al.: Power splitting-based SWIPT with decode-and-forward full-duplex relaying. IEEE Trans. Wireless Commun. 15(11), 7561–7577 (2016)
10. Cheng, Y. et al.: Optimal power splitting and censoring strategies for SWIPT-Enabled DF relay systems with relay censoring. In: Proceedings of the IEEE International Conference on Communications, May 2018, Kansas City, pp. 1–6
11. Goldsmith, A., et al.: Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. Proc. IEEE 97(5), 894C914 (2009)
12. Hattab, G., Ibnkahla, M.: Multiband spectrum access: great promises for future cognitive radio networks. Proc. IEEE 102(3), 282–306 (2014)
13. Alves, H., et al.: Performance of transmit antenna selection physical layer security schemes. IEEE Signal Process. Lett. 19(6), 372C375 (2012)
14. Yang, N., et al.: Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Trans. Commun. 61(1), 144–154 (2013)
15. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. 54(8), 1355–1387 (1975).
16. Bloch, M., et al.: Wireless information-theoretic security. IEEE Trans. Inf. Theory 54(6), 2515C2534 (2008)
17. Gopala, P.K., Lai, L., Gamal, H.: On the secrecy capacity of fading channels. IEEE Trans. Inf. Theory 54(10), 4687CA608 (2008)
18. Lei, H., et al.: Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels. IEEE Trans. Veh. Technol. 66(3), 2237–2250 (2017)
19. Yan, P., Zou, Y., Zhu, J.: Secrecy outage performance of transmit antenna selection for cognitive radio systems. IET Commun. 11(13), 1998–2004 (2017)
20. Lei, H., et al.: Secrecy outage analysis for SIMO underlay cognitive radio networks over generalized-K fading channels. IEEE Signal Process. Lett. 23(8), 1106–1110 (2016)
21. Zhang, H. et al.: Secrecy performance analysis with optimal DF relay selection of underlay CR networks over Nakagami-m fading channels. In: Proceedings of the IEEE International Conference on Communications, May 2017, Paris, pp. 1–6
22. Lei, H., et al.: On secrecy outage of relay selection in underlay cognitive radio networks over nakagami-m fading channels. IEEE Trans. Cogn. Commun. Netw. 3(4), 614–627 (2017)
23. Gu, Y. et al.: The secrecy capacity optimization artificial noise: a new type of artificial noise for secure communication in MIMO systems. IEEE ACCESS 7, 58353–58360 (2019).
24. Yun, S., et al.: On the secrecy rate and optimal power allocation for artificial noise assisted MIMOME channels. IEEE Trans. Veh. Technol. 67(4), 3098–3113 (2018)
25. Khandaker, M.R.A., Wong, K.: Robust secrecy beamforming with energy-harvesting eavesdroppers. IEEE Wireless Commun. Lett. 4(1), 10–13 (2015)
26. Wang, Z., et al.: Secrecy analysis in SWIPT systems over generalized-K fading channels. IEEE Commun. Lett. 23(5), 834–837 (2019)
27. Li, Q., Zhang, Q., Qin, J.: Secure relay beamforming for SWIPT in amplify-and-forward two-way relay networks. IEEE Trans. Veh. Technol. 65(11), 9006–9019 (2016)
28. Tang, X., et al.: Energy-constrained SWIPT networks: enhancing physical layer security with FD self-jamming. IEEE Trans. Inf. Forensics Security 14(1), 212–222 (2019)
29. Dong, Y., et al.: Robust energy efficient beamforming in MISOME-SWIPT systems with proportional secrecy rate. IEEE J. Sel. Areas Commun. 37(1), 202–215 (2019)
30. Liu, X., Li, Z., Wang, C.: Secure decode-and-forward relay SWIPT systems with power splitting scheme. IEEE Trans. Veh. Technol. 67(8), 7341–7354 (2018)
31. Zhang, J. et al.: Secure transmission in SWIPT-powered two-way untrusted relay networks. IEEE ACCESS 6, 10508–10519 2018.
32. Yan, P., Zou, Y., Zhu, J.: Energy-aware multiuser scheduling for physical-layer security in energy-harvesting underlay cognitive radio systems. IEEE Trans. Veh. Technol. 67(3), 2084–2096 (2018)
33. Yan, P., et al.: Energy-aware relay selection improves security-reliability tradeoff in energy harvesting cooperative cognitive radio systems. IEEE Trans. Veh. Technol. 69(5), 5115–5128 (2020)
34. Yan, P., et al.: Secrecy outage analysis of transmit antenna selection assisted with wireless power beacon. IEEE Trans. Veh. Technol. 69(7), 7473–7482 (2020)
35. Sun, P.N., Kong, H.Y.: Cooperative communication with energy-harvesting relays under physical layer security. IET Commun. 9(17), 2113–2139 (2015)
36. Zhang, Y., Zhao, X., Xie, Y.: Secure communications in SWIPT-enabled two-way relay networks. IEEE ACCESS 7, 111890–111896 (2019)
37. Yan, P., Zou, Y., Zhu, J.: Energy-aware multiuser scheduling for physical-layer security in energy-harvesting underlay cognitive radio systems. IEEE Trans. Veh. Technol. 67(3), 2084–2096 (2018)
38. Lei, H., et al.: On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection. IEEE Trans. Green Commun. Netw. 3(4), 202–215 (2019)
39. ZHANG ET AL.
APPENDIX A: DERIVATIONS OF (17)

For the convenience of notation, let us denote \( X = |b_{p1}|^2 \) and \( Y = |b_{p2}|^2 \). Additionally, we assume that \( X \) and \( Y \) are independently and exponentially distributed with respective means \( \sigma_{p1}^2 \) and \( \sigma_{p2}^2 \). Therefore, we can write the PDFs of \( X \) and \( Y \) as

\[
f_X(x) = \frac{1}{\sigma_{p1}^2} \exp\left(-\frac{x}{\sigma_{p1}^2}\right), \quad (A.1)
\]

and

\[
f_Y(y) = \frac{1}{\sigma_{p2}^2} \exp\left(-\frac{y}{\sigma_{p2}^2}\right). \quad (A.2)
\]

Additionally, we can rewrite (14) as

\[
\Delta_1 = \text{Pr}\left(\frac{|b_{p1}|^2}{Y_1^2} < \frac{Y_1}{\sigma_{p1}^2} \right)
\]

\[
= \int_0^\infty \text{Pr}\left(\frac{|b_{p1}|^2}{y} < \frac{y}{\sigma_{p1}^2} \right) f_Y(y) \, dy
\]

\[
= \int_0^\infty \left[1 - \exp\left(-\frac{y}{\sigma_{p2}^2}\right)\right] f_Y(y) \, dy
\]

\[
= 1 - \sqrt{\frac{\bar{\Gamma}_{\zeta_1}}{\bar{\Gamma}_{\zeta_2}}} K_1\left(\sqrt{\frac{\bar{\Gamma}_{\zeta_1}}{\bar{\Gamma}_{\zeta_2}}}\right) - \sqrt{\frac{\bar{\Gamma}_{\zeta_2}}{\bar{\Gamma}_{\zeta_1}}} K_1\left(\sqrt{\frac{\bar{\Gamma}_{\zeta_2}}{\bar{\Gamma}_{\zeta_1}}}\right)
\]

\[
\Delta_2 = \text{Pr}\left(\frac{|b_{p2}|^2}{Y_2^2} > \frac{Y_2}{\sigma_{p2}^2} \right)
\]

\[
= \int_0^\infty \text{Pr}\left(\frac{|b_{p2}|^2}{y} > \frac{y}{\sigma_{p2}^2} \right) f_Y(y) \, dy
\]

\[
= \int_0^\infty \left[1 - \exp\left(-\frac{y}{\sigma_{p2}^2}\right)\right] f_Y(y) \, dy
\]

\[
= \sqrt{\frac{\bar{\Gamma}_{\zeta_2}}{\bar{\Gamma}_{\zeta_1}}} K_1\left(\sqrt{\frac{\bar{\Gamma}_{\zeta_2}}{\bar{\Gamma}_{\zeta_1}}}\right) - \frac{\bar{\Gamma}_{\zeta_2}^{\frac{\bar{\Gamma}_{\zeta_1}}{\bar{\Gamma}_{\zeta_2}}}}{\bar{\Gamma}_{\zeta_1}^{\frac{\bar{\Gamma}_{\zeta_2}}{\bar{\Gamma}_{\zeta_1}}}} K_1\left(\sqrt{\frac{\bar{\Gamma}_{\zeta_2}}{\bar{\Gamma}_{\zeta_1}}}\right)
\]

where \( \zeta_1 = \frac{4}{\sigma_{p1}^2} \) and \( \zeta_2 = \frac{\sigma_{p2}^2 + \sigma_{p1}^2}{\sigma_{p2}^2} \). Therefore, we can easily obtain the theoretical result for (14) by substituting (A.4) and (A.5) into (14).

APPENDIX B: DERIVATIONS OF (19)

For the convenience of notation, let us consider \( X_i = |b_{pi}|^2 \), \( Y_i = |b_{pi}|^2 \) and \( Z_i = |b_{pi}|^2 \) to be independently and exponentially distributed random variables with respective means \( \sigma_{pi}^2 \), \( \sigma_{p}\) and \( \sigma_{p2}^2 \). Thus, the joint PDF of \((X_i, Y_i)\) and \((Y_i, Z_i)\) can be written as

\[
f_{(X_i, Y_i, Z_i)}(x_i, y_i, z_i) = \frac{1}{\sigma_{p1}^2 \sigma_{p2}^2} \exp\left(-\frac{x_i}{\sigma_{p1}^2} - \frac{y_i}{\sigma_{p2}^2} - \frac{z_i}{\sigma_{p2}^2}\right). \quad (B.1)
\]
and

\[ f(y_1, z_1)(y_1, z_1) = \frac{1}{\sigma_{y_{1, p}}^2 \sigma_{z_{1, p}}^2} \exp\left(-\frac{y_1}{\sigma_{y_{1, p}}^2} - \frac{z_1}{\sigma_{z_{1, p}}^2}\right). \]  

(B.2)

Hence, the expression (16) can be rewritten as

\[ p_{\text{out,} j}^{\text{RRS}} = \frac{1}{|D_n|} \sum_{i=1}^{2|D_n|} (P_1 + P_2). \]  

(B.3)

where \( P_1 \) and \( P_2 \) can be, respectively, given by

\[ P_1 = \int_{x_1 \geq 0, y_1 > 0} \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, p}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right] \times \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, p}}^2}\right) \right] f(x_1, y_1)(x_1, y_1) \, dx_1 \, dy_1, \]

and

\[ P_2 = \int_{y_1 > 0, z_1 > 0} \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, p}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right] \times \exp\left(-\frac{y_1}{\sigma_{y_{1, p}}^2}\right) f(y_1, z_1)(y_1, z_1) \, dy_1 \, dz_1. \]

(B.4)

(B.5)

According to the \( f(x_1, y_1)(x_1, y_1) \) and \( f(y_1, z_1)(y_1, z_1) \), we can compute \( P_1 \) and \( P_2 \) as

\[ P_1 = 1 - \sqrt{\frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2}} \left( \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} \right) + \frac{\sigma_y^2}{\sigma_{y_{i, f}}^2} \left[ \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} + (y_1 + 1) \sigma_y^2 \right], \]

\[ \times \left( \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} \right) + \frac{\sigma_y^2}{\sigma_{y_{i, f}}^2} \left[ \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} + (y_1 + 1) \sigma_y^2 \right], \]

(B.6)

and

\[ P_2 = \sqrt{\frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2}} \left( \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} \right) + \frac{\sigma_y^2}{\sigma_{y_{i, f}}^2} \left[ \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} + (y_1 + 1) \sigma_y^2 \right], \]

where the abbreviations \( \zeta_4 \) and \( \zeta_5 \) represent \( \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} \) and \( \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} \), respectively. Finally, substituting (B.6) and (B.7) into (B.3), the closed-form expression of (B.3) can be reformulated as

\[ p_{\text{out,} j}^{\text{RRS}} = \frac{1}{|D_n|} \sum_{i=1}^{2|D_n|} \left\{ \frac{\sigma_y^2}{\sigma_{y_{i, f}}^2} \left[ \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} + (y_1 + 1) \sigma_y^2 \right], \right. \]

\[ \left. \times \left( \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} \right) + \frac{\sigma_y^2}{\sigma_{y_{i, f}}^2} \left[ \frac{\gamma_{i, f} \sigma_{y_{i, f}}}{\sigma_y^2} + (y_1 + 1) \sigma_y^2 \right], \right\}. \]

(B.8)

**APPENDIX C: DERIVATIONS OF (28)**

For simplicity, the best relay in SRS scheme merely depends on the CSI of wireless channels from CRs to CD, thereby causing the random relay selection for E, PT and PD. Thus, the PDFs of \( |b_{i1}|^2 \), \( |b_{i2}|^2 \) and \( |b_{i3}|^2 \) is the same as \( |b_{i1}|^2 \), \( |b_{i2}|^2 \) and \( |b_{i3}|^2 \). In this way, (27) can be further simplified to

\[ p_{\text{out,} b}^{\text{RRSWEH}} = \text{Pr} \left[ \min(\delta \gamma)|b_{i1}|^2 \left\{ \frac{y_1}{\gamma_1} \right\} \max |b_{i3}|^2 \right] \]

\[ < y + (y + 1) \min(\delta \gamma)|b_{i1}|^2 \left\{ \frac{y_1}{\gamma_1} \right\} |b_{i3}|^2 \right]. \]

(C.1)

Depending on the joint PDFs of \((X_1, Y_1)\) and \((Y_1, Z_1)\), (C.2) can be further written as

\[ p_{\text{out,} b}^{\text{RRSWEH}} = P_3 + P_4, \]

where \( P_3 \) and \( P_4 \) are

\[ P_3 = \int_{x_1 \geq 0, y_1 > 0} \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right] \times \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2}\right) \right] f(x_1, y_1)(x_1, y_1) \, dx_1 \, dy_1, \]

\[ \times \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2}\right) f(y_1, z_1)(y_1, z_1) \, dy_1 \, dz_1. \]

(B.4)

(B.5)

Basing on the binomial theorem, \( \prod_{\gamma \in D_n} \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right] \) and \( \prod_{\gamma \in D_n} \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right] \) can be expanded as

\[ \prod_{\gamma \in D_n} \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right] = 1 + \sum_{m=1}^{2|D_n|} (-1)^m \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right], \]

(C.5)

and

\[ \prod_{\gamma \in D_n} \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right] = 1 + \sum_{m=1}^{2|D_n|} (-1)^m \left[ 1 - \exp\left(-\frac{y_1}{\sigma_{y_{1, f}}^2} - \frac{(y_1+1)\gamma_1}{\sigma_{u}^2}\right) \right]. \]

(C.6)

Combining (A.1) and (C.5) with (C.3), we can reformulate (C.3) as (C.7) at the top of next page.
Similarly, substituting (C.5) into (C.4), we can rewrite (C.4) as

\[ P_4 = \sqrt{\frac{\delta}{\sigma_0^2}} K_1(\sqrt{\frac{\delta}{\sigma_0^2}}) - 2 \sum_{m=1}^{2^{\rho a_{L-1}}} \frac{\sigma_{\rho}^2 (-1)^{|\rho a_{h}|}}{1 + \sigma_{\rho}^2 (y+1)} \sum_{\rho \in D_{\rho}(m)} \sqrt{\frac{\delta}{\rho}} K_1(\sqrt{\frac{\delta}{\rho}}). \]  

(C.8)

where \( \rho a_{L} = \sum_{i \in D_{\rho}(m)} \frac{y}{\sigma_{\rho}^2} + \frac{y_f}{\sigma_{\rho}^2} \). Hence, the final expression of \( P_{\text{out}} \) can be got as (48) using the results of (C.7) and (C.8).