Hindawi
Security and Communication Networks
Volume 2021, Article ID 5599334, 16 pages
https://doi.org/10.1155/2021/5599334

Research Article

Security-Reliability Tradeoff for Friendly Jammer Aided Multiuser Scheduling in Energy Harvesting Communications

Xiao Jiang,[1,2] Peng Li,[1,2] Bin Li,[3] Yulong Zou,[3] and Ruchuan Wang[1,2]

[1]*School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*
[2]*Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210023, Jiangsu Province, China*
[3]*School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, Jiangsu, China*

Correspondence should be addressed to Peng Li; lipeng@njupt.edu.cn

Received 10 January 2021; Revised 3 March 2021; Accepted 23 March 2021; Published 5 April 2021

Academic Editor: Savio Sciancalepore

In this paper, we investigate the physical-layer security in an energy-harvesting (EH) multiuser network with the help of a friendly jammer (J), where multiple eavesdroppers are considered to tap the information transmission from users (Us) to base station (BS). In this system, a power beacon (PB) transmits radio frequency (RF) signals to Us for charging. In order to enhance the security of wireless transmission, we propose non-energy-aware multiuser scheduling (NEAMUS) scheme and energy-aware multiuser scheduling (EAMUS) scheme. For the purpose of comparison, we introduce conventional round robin multiuser scheduling (CRRMUS) scheme. The closed-form outage probability (OP) and intercept probability (IP) expressions of NEAMUS, EAMUS, and CRRMUS schemes are derived over Rayleigh fading channels. Additionally, we analyze the security-reliability tradeoff (SRT) of NEAMUS, EAMUS, and CRRMUS schemes in terms of OP and IP. Numerical results show that the proposed EAMUS scheme is superior to the CRRMUS scheme and NEAMUS scheme in terms of SRT, demonstrating the advantage of the proposed EAMUS scheme in improving the physical-layer security and reliability. Moreover, SRT performance of NEAMUS and EAMUS schemes can also be improved by increasing the number of users.

1. Introduction

1.1. Background. With the rapid development of IOT and wireless communications [1–4], the energy supply of devices will face great challenges. Since mobile terminals are generally powered by the energy limited batteries instead of fixed power sources. Energy harvesting (EH), which can capture energy from surrounding environments such as wind energy, solar energy, and radio frequency (RF) energy, is regarded as a promising technology to enhance energy efficiency of mobile terminals and has been widely used in wireless communications [5–7]. Simultaneous wireless information and power transfer (SWIPT) transmits both message and energy to destinations [8]. Typically, there are two widely adopted SWIPT protocols, namely, time-switching protocol (TSP) and power-splitting protocol (PSP) [9]. Specifically, TSP divides the transmission timeslot into two phases. The devices harvest energy from received RF signals in the first phase and the harvested energy is used for information transmission in the remaining phase. By contrast, in PSP, the power splitter is used to divide the received RF signal power into two parts, one for information processing and the remaining for energy harvesting [10].

Wireless security has attracted more and more attention of researchers in recent years [11–13]. Due to the broadcast characteristics of wireless links, legitimate transmission is more vulnerable to eavesdropping attacks. Traditional wireless security protocol is based on cryptographic technologies, which use the public-private key pair to encrypt the data in the network layer. However, traditional cryptographic technologies impose extra computational overhead and additional system complexity. As an alternative, physical-layer security [14–17], which relies on utilizing the characteristics of wireless links to against eavesdropping

attacks, is a promising technology to improve wireless transmission security. In [18], Wyner proposed the concept of secrecy capacity, which refers to the difference between the main link capacity (spanning from sources to destinations) and the wiretap link capacity (spanning from sources to eavesdroppers). Furthermore, Wyner also proved that an eavesdropping event happens when the secrecy capacity is lower than zero, which will lead to the insecure transmission of information.

1.2. Related Works. For the past few years, various signal processing methods have been introduced to improve physical-layer security. In [19, 20], multiple-input-multiple-output (MIMO) scheme was presented to enhance secrecy capacity of the wireless network. Relay selection technologies [21, 22] were invoked for the sake of enhancing wireless security against eavesdropping attack by selecting an optimal relay to forward information. User scheduling schemes [23, 24] were conceived for achieving high security of wireless transmission. Additionally, jamming technologies [25, 26] were introduced to improve the secrecy performance against eavesdropping attacks by transmitting artificial noise to eavesdroppers. In [27], a user scheduling scheme based on optimal friendly jammer selection is proposed in the multiuser uplink network by combining jamming technology with user scheduling technology. Moreover, the simulated results showed that the combination of jamming and user scheduling technologies indeed enhances the physical-layer security. Additionally, Yan et al. proposed optimal and suboptimal antenna selection schemes in [28] for improving the wireless transmission security in MIMO networks. The results indicated that the antenna selection schemes can improve secrecy performance in MIMO networks.

As a further development, the combination of physical-layer security and EH networks has been drawing an increasing attention [29–35]. In [29], the authors studied wireless security of multiuser scheduling aided EH cognitive radio system. Security and reliability tradeoff of proposed user scheduling schemes was analyzed in terms of outage probability and intercept probability. Additionally, in [30], multiantenna transmission schemes were proposed to protect the secure transmission between legitimate user and base station. Furthermore, the secrecy outage probability and average secrecy rate expressions of both proposed schemes were obtained. Differing from [29, 30], where friendly jammers were not used against eavesdropping attacks, [31–34] investigated the physical-layer security with the aid of friendly jammers. Specifically, in [31], EH jammer selection schemes were investigated in uplink non-orthogonal multiple access (NOMA) networks. In order to enhance physical-layer security, the authors proposed random EH jammer selection (REJS), maximal EH jammer selection (MEJS), and optimal EH jammer selection (OEJS) schemes. Numerical results showed that the proposed OEJS scheme is better than conventional scheme without a jammer. In [32], a communication protocol was presented in EH jammer aided wireless networks to enable secure communication. Under the constraint of secrecy outage probability, the authors optimized the rate parameters to obtain the best throughput. For improving the security of EH wireless system, [33] selected a pair of intermediate nodes as a jammer and a relay to send jamming and legitimate messages to the eavesdropper and legitimate user, respectively. The secrecy outage probability was derived over Rayleigh fading channels. And in [34], the authors proposed an optimal sensor scheduling scheme to improve the security in energy harvesting wireless sensor networks.

In this paper, we study the physical-layer security for a multiuser EH wireless network consisting of multiple EH users (Us) in the face of multiple eavesdroppers (Es), where the Us, powered by a dedicated power beacon (PB), communicate with a base station (BS) with the help of a friendly jammer (J). In contrast to [29–34], we consider multiple users, multiple eavesdroppers, and a friendly jammer in this paper. Moreover, the Es and BS are equipped with multiple antennas. The main contributions of this paper can be summarized as follows:

(i) We propose the non-energy-aware multiuser scheduling (NEAMUS) scheme and energy-aware multiuser scheduling (EAMUS) scheme in EH wireless network to protect the secure transmission of information from Us to BS. Specifically, in the NEAMUS scheme, the user maximizing the main link gain of Us-BS will be selected to transmit signals. By contrast, the user maximizing the capacity of main link spanning from Us to BS will be chosen for information transmission in EAMUS scheme, which relies on both the main channel gain of Us-BS and the harvested energy.

(ii) We derive the closed-form outage probability (OP) and intercept probability (IP) expressions of NEAMUS and EAMUS schemes. For the purpose of comparison, we examine the OP and IP of the conventional round robin multiuser scheduling (CRRMUS) scheme. We further analysis the security-reliability tradeoff (SRT) of EAMUS, NEAMUS, and CRRMUS schemes. It is shown that the EAMUS scheme is better than NEAMUS and CRRMUS schemes in terms of SRT.

(iii) In [34], the authors have been proposed the best-node scheduling scheme, which corresponds to the NEAMUS scheme as introduced in this paper. Differing from [34], we propose EAMUS scheme, which significantly performs better than NEAMUS scheme in terms of SRT. Moreover, we consider the Es and BS are equipped with multiple antennas, which is much more challenging and more practical to analyze the secrecy performance. Additionally, [34] have assumed that the eavesdroppers work independently, but colluding eavesdroppers are considered in our paper.

The rest of this paper is organized as follows. In Section 2, we introduce the system model of an EH multiuser wireless network in the face of multiple eavesdroppers.

Section 3 analyzes the SRT performance of the CRRMUS, NEAMUS, and EAMUS schemes in terms of IP versus OP over Rayleigh fading channels. In Section 4, we provide the numerical results and discussions. Finally, we conclude this paper in Section 5.

2. System Model and Problem Formulation

2.1. System Model. As shown in Figure 1, we present an EH wireless network where M Us, denoted by U_m, $m \in \{1, \ldots, M\}$, communicate with a BS in the face of N Es, denoted by E_n, $n \in \{1, \ldots, N\}$, with the help of a friendly jammer (J). Each U_m is equipped with an energy harvester to harvest energy from a PB in the EH phase. The system model shown in Figure 1 can be applied to the scenarios such as mobile communications networks and wireless sensor networks with energy harvesting. We assume that the BS and Es are equipped with N_B and N_E receiving antennas, respectively, while PB and each U_m only have a single antenna. Additionally, all wireless channels are subject to independent quasi-static Rayleigh fading [32], where the black solid lines, the black dashed lines, the black dot dashed lines, and red dot dashed lines denote the main links (spanning from Us to BS), wiretap links (spanning from Us to Es), energy links (spanning from PB to Us), and artificial-noise links (spanning from J to BS and Es), respectively. Let h_{pm}, h_{mB_j}, $h_{mE_{n_e}}$ and $h_{JE_{n_e}}$, $m \in \{1, \ldots, M\}$, $j \in \{1, \ldots, N_B\}$, $n \in \{1, \ldots, N\}$, and $e \in \{1, \ldots, N_E\}$, respectively, represent the frequency non-selective Rayleigh fading channel coefficients of the $(\mathrm{PB} - U_m)$, $(U_m - B_j)$, $(U_m - E_{n_e})$, and $(J - E_{n_e})$ links, and B_j and E_{n_e} denote the jth antenna of the BS and eth antenna of E_n, respectively. The $|h_{pm}|^2$, $|h_{mB_j}|^2$, $|h_{mE_{n_e}}|^2$, and $|h_{JE_{n_e}}|^2$ obey the exponentially distribution with the means of σ^2_{pm}, $\sigma^2_{mB_j}$, $\sigma^2_{mE_{n_e}}$, and $\sigma^2_{JE_{n_e}}$, respectively. Additionally, we assume that the noise for any receiver of Figure 1 is an additive white Gaussian noise (AWGN) with a zero-mean and N_0 variance.

The total transmission timeslot T can be divided into two phases according to the time-switching ratio α, $0 \le \alpha \le 1$. In the first phase αT, the PB transmit signals to Us, and all Us harvest energy from received RF signals. In the remaining phase $(1 - \alpha)T$, the user who is selected will send message to BS and the J will transmit jamming signal to Es at the same time. Hence, the harvested energy of user node U_m can be expressed as

$$E_m = \eta \alpha T P_p \left| h_{pm} \right|^2, \tag{1}$$

where P_p represents the transmit power of the PB and η is the energy conversion efficiency of the energy harvester, $0 \le \eta \le 1$. The EH model is often assumed along with the perfect CSI and the hardware impairment is neglected for the purpose of tractability, which has been widely adopted in the existing literature [9, 10, 16, 17, 28–34]. It is indeed interesting to explore a general scenario with imperfect CSI and hardware impairment, which is out of the scope of this paper and considered for future work. From (1), the transmit power of U_m can be obtained as

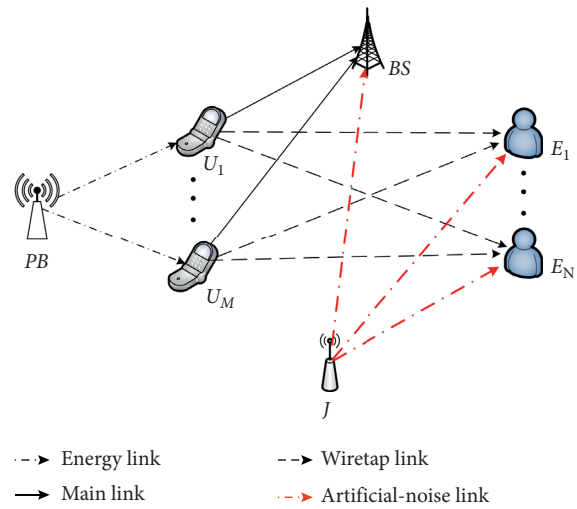

FIGURE 1: An EH wireless network consisting of a power beacon (PB), M users (Us), a base station (BS), and a friendly jammer (J) in the face of N eavesdroppers (Es).

$$P_m = a P_p \left| h_{pm} \right|^2, \tag{2}$$

where $a = (\eta\alpha/1 - \alpha)$. In the remaining $(1 - \alpha)T$, a user is chosen to send message to the BS and BS receives the signals with N_B antennas. Without loss of generality, we assume that the U_m is chosen to transmit signal x_s $(E[|x_s|^2] = 1)$ with the power of P_m to BS. Hence, we can express the signal received at BS with N_B antennas as

$$\mathbf{y}_{mB} = \sqrt{P_m}\mathbf{h}_{mB} x_s + \mathbf{n}_B, \tag{3}$$

where $\mathbf{h}_{mB} = [h_{mB_1}, h_{mB_2}, \ldots, h_{mB_{N_B}}]^T$ and $\mathbf{n}_B \sim CN(0, N_0\mathbf{I})$ is an N-dimensional AWGN vector at BS. Adopting MRC at BS, the channel capacity from U_m to BS can be expressed as

$$C_{mB} = (1 - \alpha)T \log_2 \left(1 + a\gamma_p \left| h_{pm} \right|^2 \sum_{j=1}^{N_B} \left| h_{mB_j} \right|^2 \right), \tag{4}$$

where $\gamma_p = (P_p/N_0)$.

Meanwhile, due to the broadcast nature of the wireless channel, the eavesdroppers attempt to tap the information transmission between Us and BS. Friendly jammer can help to improve security of U_m-BS links against eavesdropping attacks. As described in [36], the friendly jammer emits artificial noise using pseudo-random sequences, which are known to BS and not available to Es. Therefore, the artificial noise can be canceled at BS but cannot be removed at the Es [27, 31, 34, 36]. Assuming that the J transmits an artificial noise x_J with the power of P_J, therefore, the received signal at E_n can be obtained as

$$\mathbf{y}_{mE_n} = \sqrt{P_m}\mathbf{h}_{mE_n} x_s + \sqrt{P_J}\mathbf{h}_{JE_n} x_J + \mathbf{n}_E, \tag{5}$$

where $\mathbf{h}_{mE_n} = [h_{mE_1}, h_{mE_2}, \ldots, h_{mE_{N_E}}]^T$, $\mathbf{h}_{JE_n} = [h_{JE_1}, h_{JE_2}, \ldots, h_{JE_{N_E}}]^T$, and $\mathbf{n}_E \sim CN(0, N_0\mathbf{I})$ is an N-dimensional AWGN vector at E. The channel capacity of MRC from U_m to E_n with the assistance of the J can be obtained as

$$C_{mE_n} = (1-\alpha)T\log_2\left(1+\frac{a\gamma_p\left|h_{pm}\right|^2\sum_{e=1}^{N_e}\left|h_{mE_{n_e}}\right|^2}{\gamma_J\sum_{e=1}^{N_e}\left|h_{JE_{n_e}}\right|^2+1}\right), \quad (6)$$

where $\gamma_J = (P_J/N_0)$.

In this paper, we assume that Es wiretap the transmission between Us and BS cooperatively by MRC. Therefore, the channel capacity of the wiretap link can be expressed as

$$C_{mE} = (1-\alpha)T\log_2\left(1+\frac{a\gamma_p\left|h_{pm}\right|^2\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{mE_{n_e}}\right|^2}{\gamma_J\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{JE_{n_e}}\right|^2+1}\right). \quad (7)$$

2.2. Non-Energy-Aware Multiuser Scheduling. Here, we present the non-energy-aware multiuser scheduling (NEAMUS) scheme, in which the user maximizing CSI of the main link will be selected to send messages. Therefore, the multiuser scheduling criterion of the NEAMUS scheme can be defined as

$$u = \arg\max_m \sum_{j=1}^{N_B}\left|h_{mB_j}\right|^2. \quad (8)$$

Combining (8) and (4), we can obtain the channel capacity of U_u-BS as

$$C_{uB} = (1-\alpha)T\log_2\left(1+a\gamma_p\left|h_{pu}\right|^2\sum_{j=1}^{N_B}\left|h_{uB_j}\right|^2\right), \quad (9)$$

where h_{pu} and h_{uB_j}, respectively, denote the wireless channel fading coefficients of PB-U_u and U_u-BS. Meanwhile, the capacity of wiretap link is rewritten as

$$C_{uE} = (1-\alpha)T\log_2\left(1+\frac{a\gamma_p\left|h_{pu}\right|^2\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{uE_{n_e}}\right|^2}{\gamma_J\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{JE_{n_e}}\right|^2+1}\right), \quad (10)$$

where $h_{uE_{n_e}}$ represents the Rayleigh fading coefficient of wiretap link.

2.3. Energy-Aware Multiuser Scheduling. This subsection proposes the energy-aware multiuser scheduling (EAMUS) scheme. In EAMUS scheme, the user maximizing the channel capacity of U_m-BS is chosen to transmit data. This differs from NEAMUS scheme which only relies on the main link gain. Therefore, the multiuser scheduling criterion of EAMUS scheme can be defined as

$$o = \arg\max_m C_{mB} = \arg\max_m \left|h_{pm}\right|^2\sum_{j=1}^{N_B}\left|h_{mB_j}\right|^2. \quad (11)$$

Combining (11) and (4), we can obtain the channel capacity of U_o-BS as

$$C_{oB} = (1-\alpha)T\log_2\left(1+a\gamma_p\left|h_{po}\right|^2\sum_{j=1}^{N_B}\left|h_{oB_j}\right|^2\right), \quad (12)$$

where h_{po} and h_{oB_j}, respectively, denote the fading coefficients of PB-U_o and U_o-BS. Meanwhile, the capacity of wiretap link can be expressed as

$$C_{oE} = (1-\alpha)T\log_2\left(1+\frac{a\gamma_p\left|h_{po}\right|^2\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{oE_{n_e}}\right|^2}{\gamma_J\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{JE_{n_e}}\right|^2+1}\right), \quad (13)$$

where $h_{oE_{n_e}}$ represents the wireless channel fading coefficient of wiretap link.

3. Security and Reliability Analysis over Rayleigh Fading Channels

This section provides the SRT performance analysis for NEAMUS and EAMUS schemes in terms of OP versus IP. For the purpose of comparison, the SRT performance analysis for CRRMUS scheme is presented.

3.1. CRRMUS Scheme. In this section, we present the SRT performance analysis of the CRRMUS scheme as a benchmark. In the CRRMUS scheme, each user has the equal chance to be chosen to transmit its message. Without loss of generality, we assume the user U_b is selected. Following the literature [37], an outage event happens when the main channel capacity drops below the data rate of the main link R_0. Therefore, we can express the definition of OP for the CRRMUS scheme as

$$P_{\text{out}}^{\text{CRRMUS}} = \Pr\left(C_{bB} < R_0\right), \quad (14)$$

where b denotes the user who is chosen. According to the theory of total probability [37], the OP of CRRMUS scheme can be obtained as

$$P_{\text{out}}^{\text{CRRMUS}} = \sum_{m=1}^{M}\Pr\left(C_{mB} < R_0, b = m\right). \quad (15)$$

In the CRRMUS scheme, each user has the equal chance to be selected to transmit its data. Therefore, (15) can be rewritten as

$$P_{\text{out}}^{\text{CRRMUS}} = \sum_{m=1}^{M}\frac{1}{M}I_{0\_m}, \quad (16)$$

where I_{0_m} is given by

$$I_{0\_m} = \Pr\left(C_{mB} < R_0\right). \quad (17)$$

Substituting (4) into (17) yields

$$I_{0\_m} = \Pr\left(a\gamma_p \left| h_{pm} \right|^2 \sum_{j=1}^{N_B} \left| h_{mB_j} \right|^2 < \Delta \right) = \Pr\left(\sum_{j=1}^{N_B} \left| h_{mB_j} \right|^2 < \frac{\Delta}{a\gamma_p \left| h_{pm} \right|^2} \right), \tag{18}$$

where $\Delta = 2^{(R_0/(1-\alpha)T)} - 1$.

Based on Appendix A, I_{0_m} can be expressed as

$$I_{0\_m} = 1 - \sum_{k=0}^{N_B-1} \frac{\Delta^k}{k!\gamma_p^k a^k \sigma_{pm}^2 \sigma_{mB}^{2k}} \times 2\left(\frac{\Delta\sigma_{pm}^2}{\sigma_{mB}^2 a\gamma_p} \right)^{(1-k/2)} K_{1-k}\left(2\sqrt{\frac{\Delta}{\sigma_{pm}^2 \sigma_{mB}^2 a\gamma_p}} \right), \tag{19}$$

where $K_m(x)$ is the modified Bessel function of order m [38]. Substituting I_{0_m} from (19) into (16), $P_{\text{out}}^{\text{CRRMUS}}$ can be obtained.

Based on [37], an intercept event happens when the capacity of wiretap link is higher than $R_0 - R_s$, where R_s is a secrecy rate. Thus, the IP of the CRRMUS scheme can be defined as

$$P_{\text{int}}^{\text{CRRMUS}} = \Pr\left(C_{bE} > R_e \right), \tag{20}$$

where $R_e = R_0 - R_s$.

According to the theory of total probability [37], (20) can be expressed as

$$P_{\text{int}}^{\text{CRRMUS}} = \sum_{m=1}^{M} \Pr\left(C_{mE} > R_e, b = m \right). \tag{21}$$

Similarly to (16), we can rewritten $P_{\text{int}}^{\text{CRRMUS}}$ as

$$P_{\text{int}}^{\text{CRRMUS}} = \sum_{m=1}^{M} \frac{1}{M} I_{1\_m}, \tag{22}$$

where

$$I_{1\_m} = \Pr\left(C_{mE} > R_e \right). \tag{23}$$

Substituting (7) into (23), I_{1_m} can be rewritten as

$$I_{1\_m} = \Pr\left(\sum_{n=1}^{M} \sum_{e=1}^{N_e} \left| h_{JE_{n_e}} \right|^2 < \beta \left| h_{pm} \right|^2 \sum_{n=1}^{N} \sum_{e=1}^{N_e} \left| h_{mE_{n_e}} \right|^2 - \frac{1}{\gamma_J} \right), \tag{24}$$

where $\beta = (a\gamma_p / (2^{(R_s/(1-\alpha)T)} - 1)\gamma_J)$.

Based on Appendix B, I_{1_m} can be expressed as (25), shown at the top of this page, where $\zeta = (1/\sigma_{pU}^2 (NN_E - 1)!\sigma_{UE}^{2NN_E}) \exp(1/\sigma_{JE}^2\gamma_J)$, $h = NN_E - 1 + k - l$ and $f = l - k - 1 + h - t$. Substituting I_{1_m} from (25) into (22), the intercept probability of CRRMUS scheme can be obtained.

$$I_{1\_m} = 1 - \zeta \sum_{k=0}^{NN_E-1} \sum_{l=0}^{k} \sum_{t=0}^{h} \frac{(-1)^{l+t} \beta^{k-l-h-1} \sigma_{JE}^{2(h+1-k)} h!}{l!\gamma_J^l (h-t)! t! \sigma_{pU}^{2t}} \exp\left(\frac{\sigma_{JE}^2}{\beta\sigma_{pU}^2\sigma_{UE}^2} \right) \times \begin{cases} \left(\frac{\sigma_{JE}^2}{\beta\sigma_{UE}^2} \right)^{-f-1} \Gamma\left(f+1, \frac{\sigma_{JE}^2}{\beta\sigma_{UE}^2\sigma_{pU}^2} \right), & f \geq 0, \\ -Ei\left(-\frac{\sigma_{JE}^2}{\beta\sigma_{UE}^2\sigma_{pU}^2} \right), & f = -1, \\ (-1)^{-f} \frac{\left(\sigma_{JE}^2/\beta\sigma_{UE}^2 \right)^{-f-1} Ei\left(-\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\sigma_{pU}^2 \right) \right)}{(-f-1)!} + \sigma_{pU}^{2(-f-1)} e^{-\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\sigma_{pU}^2 \right)} \sum_{q=0}^{-f-2} \frac{(-1)^q \left(\sigma_{JE}^2/\beta\sigma_{UE}^2\sigma_{pU}^2 \right)^q}{(-f-1)(-f-2)\cdots(-f-1-q)}, & f < -1. \end{cases} \tag{25}$$

3.2. NEAMUS Scheme. In this subsection, we propose the SRT analysis of NEAMUS scheme over Rayleigh fading channels. As mentioned above, a user maximizing the main link gain will be selected in the NEAMUS scheme. Similarly to (14), we can obtain the OP of NEAMUS scheme as

$$P_{\text{out}}^{\text{NEAMUS}} = \Pr\left(C_{uB} < R_0 \right), \tag{26}$$

where C_{uB} is given by (9).

According to the theory of total probability [37], combining (9) and (26) yields

$$P_{\text{out}}^{\text{NEAMUS}} = \sum_{m=1}^{M} T_{0\_m}, \tag{27}$$

where T_{0_m} can be expressed as

$$T_{0\_m} = \Pr\left(\left| h_{pm} \right|^2 < \frac{\Delta}{a\gamma_p \sum_{j=1}^{N_B} \left| h_{mB_j} \right|^2}, \max_{g \in D, g \neq m} \sum_{j=1}^{N_B} \left| h_{gB_j} \right|^2 < \sum_{j=1}^{N_B} \left| h_{mB_j} \right|^2 \right), \tag{28}$$

where D represents the set of users.

According to Appendix C, T_{0_m} can be obtained as

$$T_{0\_m} = \frac{\sum_{i=1}^{M-1} \cup_{i'} (-1)^i A_{i'} B_{i'}}{(N_B - 1)! \sigma_{UB}^{2N_B}} \times \left[(\bar{i} + N_B - 1)! \left(\frac{1+i}{\sigma_{UB}^2} \right)^{-\bar{i} - N_B} - 2 \left(\frac{\Delta \sigma_{UB}^2}{a \gamma_p \sigma_{pU}^2 (1+i)} \right)^{\bar{i} + N_B/2} K_{\bar{i}+N_B} \left(2 \sqrt{\frac{\Delta(1+i)}{a \gamma_p \sigma_{pU}^2 \sigma_{UB}^2}} \right) \right], \tag{29}$$

where $\cup_{i'} = \Sigma_{i_1=0}^{i} \Sigma_{i_2=0}^{i-i_1} \cdots \Sigma_{i_{N_B-1}=0}^{i-i_1-\cdots i_{N_B-2}}$,

$\bar{i} = (N_B - 1)(i - i_1) - (N_B - 2) i_2 - (N_B - 3) i_3 - \cdots i_{N_B - 1}$,

$$A_{i'} = \binom{M-1}{i} \binom{i}{i_1} \binom{i - i_1}{i_2} \times \cdots \binom{i - i_1 - \cdots i_{N_B-2}}{i_{N_B-1}},$$

$$B_{i'} = \left(\frac{1}{(N_B - 1)! \sigma_{UB}^{2(N_B-1)}} \right)^{i - i_1 - \cdots i_{N_B-1}} \prod_{k=0}^{N_B-2} \left(\frac{1}{k! \sigma_{UB}^{2k}} \right)^{i_{k+1}}. \tag{30}$$

Substituting (29) into (27), the OP of NEAMUS scheme $P_{\text{out}}^{\text{NEAMUS}}$ can be obtained.

Similarly to (20), we can obtain the IP of NEAMUS scheme as

$$P_{\text{int}}^{\text{NEAMUS}} = \Pr(C_{uE} > R_e), \tag{31}$$

where C_{uE} is given by (10).

Combining (10) and (31), $P_{\text{int}}^{\text{NEAMUS}}$ can be expressed as

$$P_{\text{int}}^{\text{NEAMUS}} = \sum_{m=1}^{M} T_{1\_m}, \tag{32}$$

where T_{1_m} is given by

$$T_{1\_m} = \Pr\left(\sum_{n=1}^{N} \sum_{e=1}^{N_e} \left| h_{JE_{n_e}} \right|^2 < \beta \left| h_{pm} \right|^2 \sum_{n=1}^{N} \sum_{e=1}^{N_e} \left| h_{mE_{n_e}} \right|^2 - \frac{1}{\gamma_J}, \max_{g \in D, g \neq m} \sum_{j=1}^{N_B} \left| h_{gB_j} \right|^2 < \sum_{j=1}^{N_B} \left| h_{mB_j} \right|^2 \right). \tag{33}$$

Based on Appendix D, T_{1_m} can be formulated as

$$T_{1\_m} = \frac{\sum_{i=1}^{M-1} \cup_{i'} (-1)^i A_{i'} B_{i'}}{(N_B - 1)! \sigma_{UB}^{2N_B}} \times (\bar{i} + N_B - 1)! \left(\frac{1+i}{\sigma_{UB}^2} \right)^{-\bar{i} - N_B} I_{1\_m}, \tag{34}$$

where I_{1_m} is given by (25). Substituting (34) into (32), $P_{\text{int}}^{\text{NEAMUS}}$ can be obtained.

3.3. EAMUS Scheme. This section presents EAMUS scheme to improve the physical-layer security in terms of SRT performance. As mentioned above, a user maximizing the channel capacity of U_m-BS is chosen. Therefore, the OP of EAMUS scheme can be defined as

$$P_{\text{out}}^{\text{EAMUS}} = \Pr(C_{oB} < R_0), \tag{35}$$

where C_{oB} is given by (12).

Substituting (12) into (35) yields

$$P_{\text{out}}^{\text{EAMUS}} = \Pr\left(\max_m \left| h_{pm} \right|^2 \sum_{j=1}^{N_B} \left| h_{mB_j} \right|^2 < \frac{\Delta}{a \gamma_p} \right) = \prod_{m=1}^{M} \Pr\left(\left| h_{pm} \right|^2 \sum_{j=1}^{N_B} \left| h_{mB_j} \right|^2 < \frac{\Delta}{a \gamma_p} \right) = \prod_{m=1}^{M} I_{0\_m}, \tag{36}$$

where I_{0_m} is given by (19).

Relying on the definition of IP in (20), we can obtain the IP of EAMUS scheme as

$$P_{\text{int}}^{\text{EAMUS}} = \Pr(C_{oE} > R_e), \tag{37}$$

where C_{oE} is given by (13).

According to the theory of total probability [37], we can rewrite (37) as

$$P_{\text{int}}^{\text{EAMUS}} = \sum_{m=1}^{M} T_{2\_m}, \tag{38}$$

where T_{2_m} can be expressed as

$$T_{2\_m} = \Pr\left(\frac{\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{JE_{n_e}}\right|^2 + \left(1/\gamma_J\right)}{\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{mE_{n_e}}\right|^2} < \beta\left|h_{pm}\right|^2, \max_{g\in D, g\neq m}\left|h_{pg}\right|^2 \sum_{j=1}^{N_B}\left|h_{gB_j}\right|^2 < \left|h_{pm}\right|^2 \sum_{j=1}^{N_B}\left|h_{mB_j}\right|^2 \right), \tag{39}$$

With our existing knowledge, it is very challenging to derive the closed-form expression of T_{2_m} of Appendix E. For simplicity, as discussed in [32, 39], since the optimal user selection does not rely on the CSI of wiretap link, the best user scheduling for BS can be regarded as equivalent to random user scheduling for eavesdroppers. Therefore, the PDF of random variables of $\sum_{n=1}^{N}\sum_{e=1}^{N_e}|h_{oE_{n_e}}|^2$ is the same as $\sum_{n=1}^{N}\sum_{e=1}^{N_e}|h_{mE_{n_e}}|^2$. Hence, we can rewrite (37) as

$$P_{\text{int}_1}^{\text{EAMUS}} = \Pr\left(\sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{JE_{n_e}}\right|^2 < \beta\left|h_{po}\right|^2 \sum_{n=1}^{N}\sum_{e=1}^{N_e}\left|h_{mE_{n_e}}\right|^2 - \frac{1}{\gamma_J} \right). \tag{40}$$

After further manipulations, (40) can be expressed as (41) shown at the top of this page, where $\theta = (1/\sigma_{po}^2 (NN_E - 1)!\sigma_{UE}^{2NN_E})\exp(1/\sigma_{JE}^2\gamma_J)$.

$$P_{\text{int}_1}^{\text{EAMUS}} = 1 - \theta \sum_{k=0}^{NN_E-1}\sum_{l=0}^{k}\sum_{t=0}^{h} \frac{(-1)^{l+t}\beta^{k-l-h-1}\sigma_{JE}^{2(h+1-k)}h!}{l!\gamma_J^l (h-t)!t!\sigma_{po}^{2t}} \exp\left(\frac{\sigma_{JE}^2}{\beta\sigma_{po}^2\sigma_{UE}^2}\right) \times \begin{cases} \left(\dfrac{\sigma_{JE}^2}{\beta\sigma_{UE}^2}\right)^{-f-1}\Gamma\left(f+1, \dfrac{\sigma_{JE}^2}{\beta\sigma_{UE}^2\sigma_{po}^2}\right), & f \geq 0, \\ -Ei\left(-\dfrac{\sigma_{JE}^2}{\beta\sigma_{UE}^2\sigma_{po}^2}\right), & f = -1, \\ (-1)^{-f}\dfrac{\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\right)^{-f-1}Ei\left(-\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\sigma_{po}^2\right)\right)}{(-f-1)!} + \sigma_{po}^{2(-f-1)}e^{-\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\sigma_{po}^2\right)}\displaystyle\sum_{q=0}^{-f-2}\frac{(-1)^q\left(\sigma_{JE}^2/\beta\sigma_{po}^2\sigma_{UE}^2\right)^q}{(-f-1)(-f-2)\cdots(-f-1-q)}, & f < -1. \end{cases} \tag{41}$$

4. Numerical Results and Discussion

In this section, we present the numerical results and discussions for the CRRMUS, NEAMUS, and EAMUS schemes. The OP and IP of CRRMUS, NEAMUS, and EAMUS schemes are evaluated by using (16), (22), (27), (34), (38), and (40). In our analysis model, we assume that the transmission links between any two nodes of Figure 1 are Rayleigh fading channels. Following the existing literature [26–28, 36, 39], the average channel gains of $\sigma_{mB}^2 = \sigma_{UB}^2 = 1$, $\sigma_{mE}^2 = \sigma_{UE}^2 = \sigma_{JE}^2 = 1$, $\sigma_{pm}^2 = \sigma_{pU}^2 = 0.3$, $T = 1$ ms, $R_0 = 1$ bit/s/Hz, $R_s = 0.6$ bit/s/Hz, $N_B = N_E = 2$ are used for both the analysis and the simulation, unless otherwise stated. For simplicity, let "T" denote the theoretical result and "S" represent the simulated result.

As shown in Figure 2, we present the OP and IP versus γ_p of the CRRMUS, NEAMUS, and EAMUS schemes. In Figure 2, the theoretical results match well with the simulated results, which demonstrates the correctness of our analysis. Figure 2 shows that, with the increase of γ_p, the OP of CRRMUS, NEAMUS, and EAMUS schemes are significantly reduced, whereas the IP of three schemes increase, implying that a security and reliability tradeoff between the IP and OP exists in our proposed EH network. Figure 2 also demonstrates that the EAMUS scheme performs better than CRRMUS and NEAMUS schemes in terms of OP. Meanwhile, the IP of the EAMUS scheme is almost identical to that of the NEAMUS and CRRMUS schemes. This is due to the fact that the best user scheduling for BS can be regarded as equivalent to random user scheduling for eavesdroppers [32, 39]. However, the following SRT analysis shows that the physical-layer security can still be enhanced, because the improvement of reliability can be translated into the enhancement of security.

Figure 3 shows IP and OP versus energy conversion efficiency η of the CRRMUS, NEAMUS, and EAMUS schemes. As shown in Figure 3, as the energy conversion efficiency η increases, the OP of all CRRMUS, NEAMUS, and EAMUS schemes decreases, while the IP of CRRMUS, NEAMUS, and EAMUS schemes increases accordingly. This is due to the fact that, with the increase of energy conversion efficiency η, the users convert more energy from received RF signals for information transmission, which leads to a lower OP. Meanwhile, the increase of user transmission power is beneficial not only for BS but also for Es, which causes a higher IP.

Figure 4 shows IP versus OP of the CRRMUS, NEAMUS, and EAMUS schemes for different number of users M. It can be seen from Figure 4 that the EAMUS scheme is better than the NEAMUS scheme and CRRMUS scheme in terms of SRT, and the CRRMUS scheme is the worst of the three schemes. That means the proposed NEAMUS and EAMUS

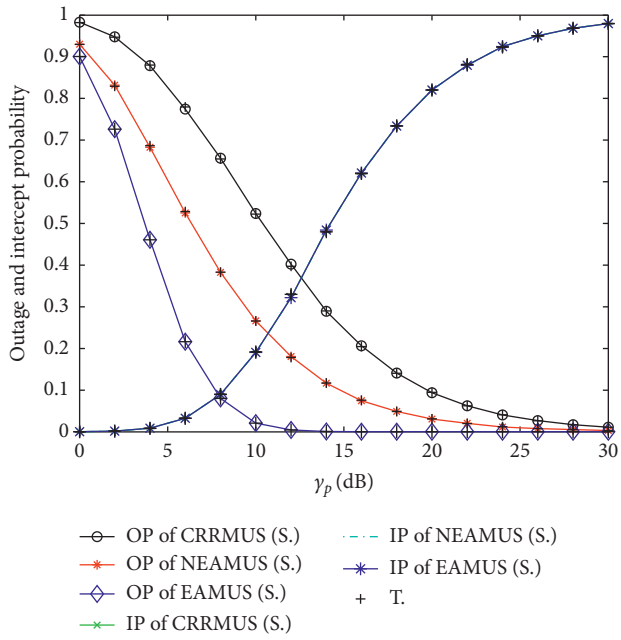

FIGURE 2: OP and IP versus γ_p (dB) of the CRRMUS, NEAMUS and EAMUS schemes with $\alpha = 0.5$, $\eta = 0.6$, $T = 1$ ms, $N = 4, M = 6$, $R_0 = 1$ bit/s/Hz, $R_s = 0.6$ bit/s/Hz, $N_B = N_E = 2$, and $\gamma_J = 10$ dB.

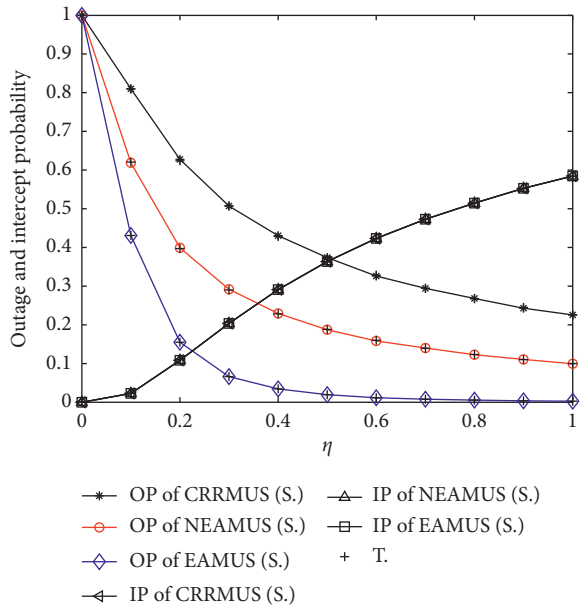

FIGURE 3: IP and OP versus energy conversion efficiency η of the CRRMUS, NEAMUS, and EAMUS schemes with $\alpha = 0.5$, $T = 1$ ms, $M = 6$, $N = 4$, $R_0 = 1$ bit/s/Hz, $R_s = 0.6$ bit/s/Hz, $N_B = N_E = 2$, $\gamma_J = 10$ dB, and $\gamma_p = 10$ dB.

schemes can achieve the benefit of wireless security. One can also observe from Figure 4 that as the number of users M increases from $M = 2$ to $M = 6$, the SRT performances of NEAMUS and EAMUS schemes improve, illustrating that increasing the number of users can effectively improve the physical-layer security performance. Moreover, as the number of users increases from 2 to 6, the SRT performance gap of EAMUS scheme is more significant than that of NEAMUS scheme, which also further shows the superiority of the proposed EAMUS scheme in terms of SRT. However, as M increases from 2 to 6, the SRT of CRRMUS scheme has not changed, due to the fact that the CRRMUS scheme randomly selects user without cooperation between users.

Figure 5 depicts IP versus OP of the CRRMUS, NEAMUS, and EAMUS schemes for different γ_J. As seen from Figure 5, for both $\gamma_J = 5$ dB and $\gamma_J = 10$ dB, the SRT performance of EAMUS scheme is always better than that of NEAMUS and CRRMUS schemes in the whole γ_p region. Additionally, with the γ_J increases from 5 dB to 10 dB, the SRT performances of CRRMUS, NEAMUS, and EAMUS

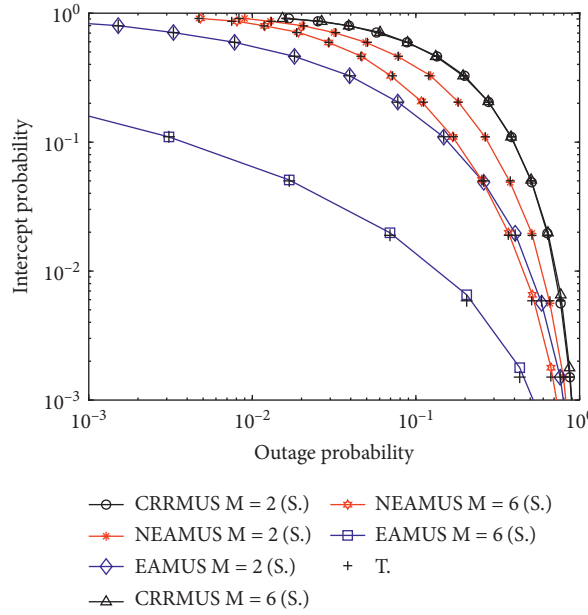

FIGURE 4: IP versus OP of the CRRMUS, NEAMUS, and EAMUS schemes for different number of users M with $\eta = 0.6$, $T = 1$ ms, $N = 4$, $R_0 = 1$ bit/s/Hz, $R_s = 0.6$ bit/s/Hz, $N_B = N_E = 2$, $\gamma_J = 10$ dB, and $\gamma_p = [0, 30]$ dB.

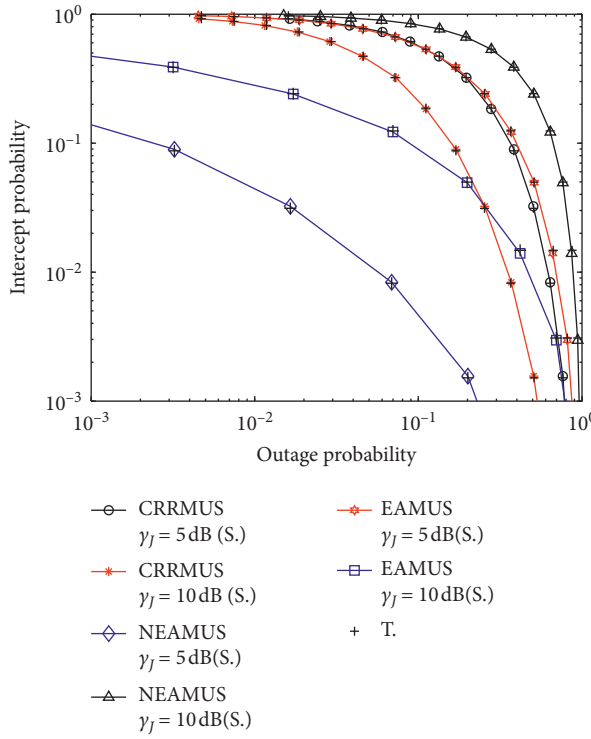

FIGURE 5: IP versus OP of the CRRMUS, NEAMUS, and EAMUS schemes for different γ_J with $\eta = 0.6$, $T = 1$ ms, $M = 6$, $N = 4$, $R_0 = 1$ bit/s/Hz, $R_s = 0.6$ bit/s/Hz, $N_B = N_E = 2$, and $\gamma_p = [0, 30]$ dB.

schemes all have been improved, implying significant SRT benefit achieved with the increases of γ_J. That is to say, the wireless transmission security of the proposed EH network can be improved by increasing the transmission power of the jammer for all three user scheduling schemes.

In Figure 6, we show IP versus OP of the CRRMUS, NEAMUS, and EAMUS schemes for different MER, where MER $= \sigma_{mB}^2/\sigma_{mE}^2$ represents the main-to-eavesdropping ratio [27, 28]. As shown in Figure 6, with the increasing of MER from -5 dB to 5 dB, the SRT performances of

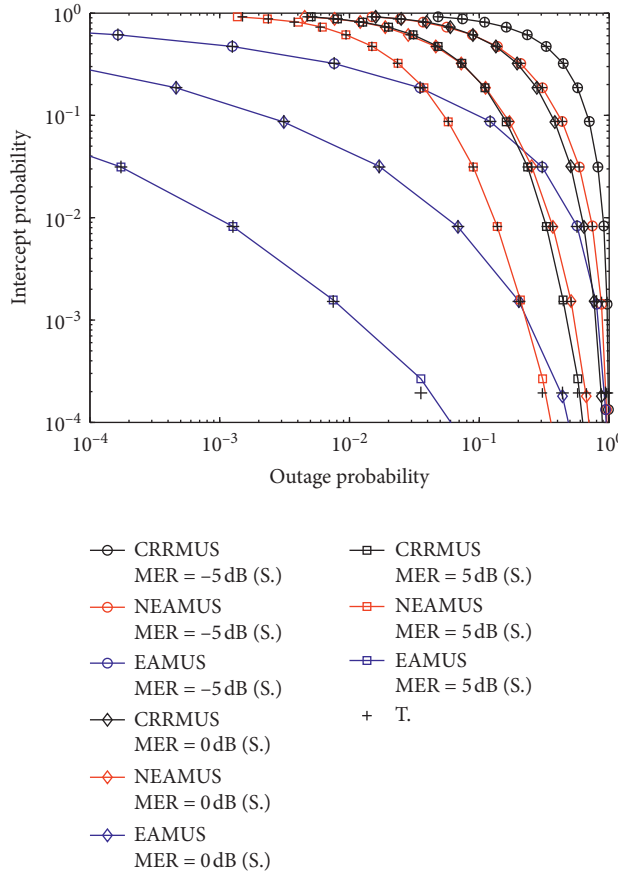

FIGURE 6: IP versus OP of the CRRMUS, NEAMUS, and EAMUS schemes for different MER with $\eta = 0.6$, $T = 1$ ms, $M = 6$, $N = 4$, $R_0 = 1$ bit/s/Hz, $R_s = 0.6$ bit/s/Hz, $N_B = N_E = 2$, $\gamma_J = 10$ dB, and $\gamma_p = [0, 30]$ dB.

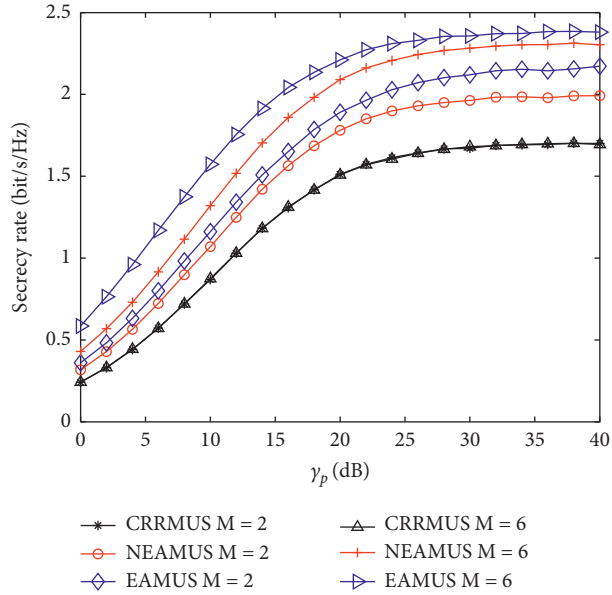

FIGURE 7: Secrecy rate versus γ_p of the CRRMUS, NEAMUS, and EAMUS schemes for different number of users M with $\eta = 0.6$, $T = 1$ ms, $N = 4$, $R_0 = 1$ bit/s/Hz, $R_s = 0.6$ bit/s/Hz, $N_B = N_E = 2$, and $\gamma_J = 10$ dB.

CRRMUS, NEAMUS, and EAMUS schemes all improve, accordingly. Specifically, given a special OP value, the IP of the CRRMUS, NEAMUS, and EAMUS schemes decreases with the increase of MER. That is to say, the physical-layer security of the proposed EH network can be effectively improved by increasing MER.

Figure 7 depicts the secrecy rate versus γ_p of the CRRMUS, NEAMUS, and EAMUS schemes for different number of users M. As shown in Figure 7, as the increase of γ_p, the secrecy rate of CRRMUS, NEAMUS, and EAMUS schemes improves, accordingly, and then the secrecy rates of the three schemes all keep in a stable state. It can also be observed from Figure 7 that, with the increase of the number of users from $M = 2$ to $M = 6$, the secrecy rate of both NEAMUS and EAMUS schemes improves, implying that the wireless transmission security of NEAMUS and EAMUS schemes can be improved by increasing the number of users. Additionally, Figure 7 also shows that the EAMUS scheme has the largest secrecy rate among the three schemes, demonstrating that the proposed EAMUS scheme can improve the physical-layer security significantly.

5. Conclusion

This paper investigated the physical-layer security for an EH wireless network consisting of multiple EH users, a base station, a friendly jammer, and multiple eavesdroppers. In order to improve the physical-layer security, we proposed energy-aware multiuser scheduling (EAMUS) scheme and non-energy-aware multiuser scheduling (NEAMUS) scheme depending on whether the CSI of energy link is available or not. Also, the conventional round Robin multiuser scheduling (CRRMUS) scheme is considered as a benchmark. Closed-form expressions of OP and IP for EAMUS, NEAMUS, and CRRMUS schemes are derived to evaluate the reliability and security achieved by the proposed schemes. Additionally, we presented the SRT performance analysis for CRRMUS, NEAMUS, and EAMUS schemes. Numerical results showed that the proposed EAMUS scheme is superior to the NEAMUS and CRRMUS schemes in terms of SRT. That is to say, the proposed EAMUS scheme can significantly improve the physical-layer security in the EH multiuser network. Additionally, the SRT performance of NEAMUS and EAMUS schemes can also be improved by increasing the number of users.

Appendix

A. Derivation of (19)

Assume that the fading coefficients of $|h_{pm}|^2$ and $|h_{mB_j}|^2$ are independent and identical distributed (i.i.d.) random variables with means of σ_{pm}^2 and σ_{mB}^2, respectively. Denote $X = \sum_{j=1}^{N_B} |h_{mB_j}|^2$ and $Y = |h_{pm}|^2$. Therefore, the probability density functions (PDFs) of X and Y can be written as

$$f_X(x) = \frac{x^{N_B-1}}{(N_B-1)!\sigma_{mB}^{2N_B}} \exp\left(-\frac{x}{\sigma_{mB}^2}\right),$$
$$f_Y(y) = \frac{1}{\sigma_{pm}^2} \exp\left(-\frac{y}{\sigma_{pm}^2}\right). \tag{A.1}$$

The cumulative distribution function (CDF) of X can be obtained as

$$F_X(x) = \int_0^x f_X(x)\mathrm{d}x = 1 - \exp\left(-\frac{x}{\sigma_{mB}^2}\right) \sum_{k=0}^{N_B-1} \frac{1}{k!}\left(\frac{x}{\sigma_{mB}^2}\right)^k. \tag{A.2}$$

Therefore, I_{0_m} can be rewritten as

$$\begin{aligned} I_{0\_m} &= \int_0^\infty F_X\left(\frac{\Delta}{a\gamma_p y}\right) f_Y(y)\mathrm{d}y = 1 - \sum_{k=0}^{N_B-1} \frac{\Delta^k}{k!\, a^k \gamma_p^k \sigma_{pm}^2 \sigma_{mB}^{2k}} \\ &\quad \times \int_0^\infty \exp\left(-\frac{\Delta}{\sigma_{mB}^2 a\gamma_p y} - \frac{y}{\sigma_{pm}^2}\right) y^{-k}\mathrm{d}y \\ &= 1 - \sum_{k=0}^{N_B-1} \frac{\Delta^k}{k!\gamma_p^k a^k \sigma_{pm}^2 \sigma_{mB}^{2k}} \\ &\quad \times 2\left(\frac{\Delta\sigma_{pm}^2}{\sigma_{mB}^2 a\gamma_p}\right)^{1-k/2} K_{1-k}\left(2\sqrt{\frac{\Delta}{\sigma_{pm}^2\sigma_{mB}^2 a\gamma_p}}\right). \end{aligned} \tag{A.3}$$

B. Derivation of (25)

For simplicity, we assume that the fading coefficients of $|h_{pm}|^2$, $|h_{mE_{n_e}}|^2$, and $|h_{JE_{n_e}}|^2$, $m \in \{1, \ldots, M\}$, $n \in \{1, \ldots, N\}$, and $e \in \{1, \ldots, N_E\}$, are independent and identical distributed (i.i.d.) random variables with the means of σ_{pU}^2, σ_{UE}^2, and σ_{JE}^2, respectively. Denote $X = \sum_{n=1}^{N}\sum_{e=1}^{N_e} |h_{JE_{n_e}}|^2$, $Y = |h_{pm}|^2$, and $Z = \sum_{n=1}^{N}\sum_{e=1}^{N_e} |h_{mE_{n_e}}|^2$. Therefore, we can express the PDFs of X, Y, and Z as

$$f_X(x) = \frac{x^{NN_E-1}}{(NN_E-1)!\sigma_{JE}^{2NN_E}} \exp\left(-\frac{x}{\sigma_{JE}^2}\right), \tag{B.1}$$

$$f_Y(y) = \frac{1}{\sigma_{pU}^2} \exp\left(-\frac{y}{\sigma_{pU}^2}\right), \tag{B.2}$$

$$f_Z(z) = \frac{z^{NN_E-1}}{(NN_E-1)!\sigma_{UE}^{2NN_E}} \exp\left(-\frac{z}{\sigma_{UE}^2}\right). \tag{B.3}$$

The CDF of X can be obtained as

$$F_X(x) = 1 - \exp\left(-\frac{x}{\sigma_{JE}^2}\right)\sum_{k=0}^{NN_E-1}\frac{1}{k!}\left(\frac{x}{\sigma_{JE}^2}\right)^k. \tag{B.4}$$

Therefore, (25) can be rewritten as

$$I_{1\_m} = \int_0^\infty\int_0^\infty F_X\left(\beta yz - \frac{1}{\gamma_J}\right) f_Y(y)\, f_Z(z)\mathrm{d}y\mathrm{d}z. \tag{B.5}$$

Using (B.4), $F_X(\beta yz - (1/\gamma_J))$ can be expressed as

$$F_X\left(\beta yz - \frac{1}{\gamma_J}\right) = 1 - \exp\left[-\frac{1}{\sigma_{JE}^2}\left(\beta yz - \frac{1}{\gamma_J}\right)\right]\sum_{k=0}^{NN_E-1}\frac{1}{k!\sigma_{JE}^{2k}}\left(\beta yz - \frac{1}{\gamma_J}\right)^k, \tag{B.6}$$

wherein $(\beta yz - (1/\gamma_J))^k$ can be expanded as

$$\left(\beta yz - \frac{1}{\gamma_J}\right)^k = \sum_{l=0}^{k}\frac{k!\beta^{k-l}(-1)^l}{l!\,(k-l)!\gamma_J^l}\, y^{k-l}\, z^{k-l}. \tag{B.7}$$

Combining (B.5), (B.6), and (B.7), I_{1_m} can be expressed as

$$I_{1\_m} = 1 - \zeta\sum_{k=0}^{NN_E-1}\sum_{l=0}^{k}\frac{(-1)^l\beta^{k-l}}{l!\,(k-l)!\gamma_J^l\sigma_{JE}^{2k}}\Phi_1, \tag{B.8}$$

where $\zeta = (1/\sigma_{pU}^2(NN_E-1)!\sigma_{UE}^{2NN_E})\exp(1/\sigma_{JE}^2\gamma_J)$ and

$$\begin{aligned}\Phi_1 &= \int_0^\infty\int_0^\infty y^{k-l}\exp\left(-\frac{\beta yz}{\sigma_{JE}^2} - \frac{y}{\sigma_{pU}^2} - \frac{z}{\sigma_{UE}^2}\right) z^h\mathrm{d}y\mathrm{d}z \\ &= (k-l)!\int_0^\infty\left(\frac{\beta z}{\sigma_{JE}^2} + \frac{1}{\sigma_{pU}^2}\right)^{l-k-1} z^h\exp\left(-\frac{z}{\sigma_{UE}^2}\right)\mathrm{d}z,\end{aligned} \tag{B.9}$$

where $h = NN_E - 1 + k - l$. Letting $w = (\beta z/\sigma_{JE}^2) + (1/\sigma_{pU}^2)$, we can rewrite Φ_1 as

$$\Phi_1 = \frac{(k-l)!\sigma_{JE}^{2(h+1)}}{\beta^{h+1}}\exp\left(\frac{\sigma_{JE}^2}{\beta\sigma_{pU}^2\sigma_{UE}^2}\right)\Phi_2, \tag{B.10}$$

where

$$\Phi_2 = \int_{\left(1/\sigma_{pU}^2\right)}^\infty w^{l-k-1}\left(w - \frac{1}{\sigma_{pU}^2}\right)^h\exp\left(-\frac{\sigma_{JE}^2 w}{\beta\sigma_{UE}^2}\right)\mathrm{d}w. \tag{B.11}$$

Similarly to (B.7), $(w - (1/\sigma_{pU}^2))^h$ can be expanded as

$$\left(w - \frac{1}{\sigma_{pU}^2}\right)^h = \sum_{t=0}^{h}\frac{h!\,(-1)^t}{(h-t)!t!\sigma_{pU}^{2t}}w^{h-t}. \tag{B.12}$$

Substituting (B.12) into (B.11) yields

$$\Phi_2 = \sum_{t=0}^{h}\frac{h!\,(-1)^t}{(h-t)!t!\sigma_{pU}^{2t}}\times\int_{\left(1/\sigma_{pU}^2\right)}^\infty w^{l-k-1+h-t}\exp\left(-\frac{\sigma_{JE}^2 w}{\beta\sigma_{UE}^2}\right)\mathrm{d}w. \tag{B.13}$$

Letting $f = l - k - 1 + h - t$, when $f \geq 0$, Φ_2 can be derived as

$$\Phi_2 = \sum_{t=0}^{h}\frac{h!\,(-1)^t}{(h-t)!t!\sigma_{pU}^{2t}}\left(\frac{\sigma_{JE}^2}{\beta\sigma_{UE}^2}\right)^{-f-1}\times\Gamma\left(f+1, \frac{\sigma_{JE}^2}{\beta\sigma_{UE}^2\sigma_{pU}^2}\right). \tag{B.14}$$

When $f = -1$, Φ_2 can be calculated as

$$\Phi_2 = -\sum_{t=0}^{h}\frac{h!\,(-1)^t}{(h-t)!t!\sigma_{pU}^{2t}}Ei\left(-\frac{\sigma_{JE}^2}{\beta\sigma_{UE}^2\sigma_{pU}^2}\right). \tag{B.15}$$

When $f < -1$, Φ_2 can be obtained as

$$\begin{aligned}\Phi_2 = \sum_{t=0}^{h}\frac{h!\,(-1)^t}{(h-t)!t!\sigma_{pU}^{2t}}\Bigg[&(-1)^f\frac{\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\right)^{-f-1}Ei\left(-\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\sigma_{pU}^2\right)\right)}{(-f-1)!} \\ &+\sigma_{pU}^{2(-f-1)}e^{-\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\sigma_{pU}^2\right)}\sum_{q=0}^{-f-2}\frac{(-1)^q\left(\sigma_{JE}^2/\beta\sigma_{UE}^2\sigma_{pU}^2\right)^q}{(-f-1)(-f-2)\cdots(-f-1-q)}\Bigg].\end{aligned} \tag{B.16}$$

Finally, by substituting (B.10) and the results of Φ_2 into (B.8), I_{1_m} can be expressed as (B.17), shown at the top of the following page.

$$I_{1\_m} = 1 - \zeta \sum_{k=0}^{NN_E-1} \sum_{l=0}^{k} \sum_{t=0}^{h} \frac{(-1)^{l+t} \beta^{k-l-h-1} \sigma_{JE}^{2(h+1-k)} h!}{l! \gamma_J^l (h-t)! t! \sigma_{pU}^{2t}} \exp\left(\frac{\sigma_{JE}^2}{\beta \sigma_{pU}^2 \sigma_{UE}^2}\right)$$

$$\times \begin{cases} \left(\frac{\sigma_{JE}^2}{\beta \sigma_{UE}^2}\right)^{-f-1} \Gamma\left(f+1, \frac{\sigma_{JE}^2}{\beta \sigma_{UE}^2 \sigma_{pU}^2}\right), & f \geq 0, \\ -Ei\left(-\frac{\sigma_{JE}^2}{\beta \sigma_{UE}^2 \sigma_{pU}^2}\right), & f = -1, \\ (-1)^{-f} \frac{\left(\sigma_{JE}^2/\beta \sigma_{UE}^2\right)^{-f-1} Ei\left(-\left(\sigma_{JE}^2/\beta \sigma_{UE}^2 \sigma_{pU}^2\right)\right)}{(-f-1)!} + \sigma_{pU}^{2(-f-1)} e^{-\left(\sigma_{JE}^2/\beta \sigma_{UE}^2 \sigma_{pU}^2\right)} \sum_{q=0}^{-f-2} \frac{(-1)^q \left(\sigma_{JE}^2/\beta \sigma_{UE}^2 \sigma_{pU}^2\right)^q}{(-f-1)(-f-2)\cdots(-f-1-q)}, & f < -1. \end{cases} \tag{B.17}$$

C. Derivation of (29)

Assume that the fading coefficients of $|h_{pm}|^2$ and $|h_{mB_j}|^2$, $m \in \{1, \ldots, M\}$ and $j \in \{1, \ldots, N_B\}$, are i.i.d. random variables with the means of σ_{pU}^2 and σ_{UB}^2, respectively. Denote $U = \sum_{j=1}^{N_B} |h_{mB_j}|^2$ and $V = |h_{pm}|^2$. Similarly to (B.1), the PDF of U can be expressed as

$$f_U(u) = \frac{u^{N_B-1}}{(N_B-1)! \sigma_{UB}^{2N_B}} \exp\left(-\frac{u}{\sigma_{UB}^2}\right). \tag{C.1}$$

T_{0_m} can be rewritten as

$$T_{0\_m} = \int_0^\infty \prod_{g \in D, g \neq m} \Pr\left(\sum_{j=1}^{N_B} \left|h_{gB_j}\right|^2 < u\right) \times F_V\left(\frac{\Delta}{a \gamma_p u}\right) f_U(u) \mathrm{d}u, \tag{C.2}$$

wherein $\prod_{g \in D, g \neq m} \Pr(\sum_{j=1}^{N_B} |h_{gB_j}|^2 < u)$ can be expressed as

$$\prod_{g \in D, g \neq m} \Pr\left(\sum_{j=1}^{N_B} \left|h_{gB_j}\right|^2 < u\right) = \underbrace{\left[1 - \exp\left(-\frac{u}{\sigma_{UB}^2}\right) \sum_{k=0}^{N_B-1} \frac{1}{k!} \left(\frac{u}{\sigma_{UB}^2}\right)^k\right]^{M-1}}_{\Phi_3}. \tag{C.3}$$

Applying successive binomial expansion on Φ_3, we have

$$\Phi_3 = \sum_{i=1}^{M-1} \bigcup_{i'} (-1)^i A_{i'} B_{i'} u^{\bar{i}} \exp\left(-\frac{ui}{\sigma_{UB}^2}\right), \tag{C.4}$$

where $\cup_{i'} = \Sigma_{i_1=0}^{i} \Sigma_{i_2=0}^{i-i_1} \cdots \Sigma_{i_{N_B-1}=0}^{i-i_1-\cdots i_{N_B-2}}$,

$$\begin{aligned} \bar{i} &= (N_B-1)(i-i_1) - (N_B-2)i_2 - (N_B-3)i_3 - \cdots i_{N_B-1}, \\ A_{i'} &= \binom{M-1}{i} \binom{i}{i_1} \binom{i-i_1}{i_2} \times \cdots \binom{i-i_1-\cdots i_{N_B-2}}{i_{N_B-1}}, \\ B_{i'} &= \left(\frac{1}{(N_B-1)! \sigma_{UB}^{2(N_B-1)}}\right)^{i-i_1-\cdots i_{N_B-1}} \prod_{k=0}^{N_B-2} \left(\frac{1}{k! \sigma_{UB}^{2k}}\right)^{i_{k+1}}. \end{aligned} \tag{C.5}$$

Substituting (C.4) into (C.2), T_{0_m} can be expressed as

$$T_{0\_m} = \frac{\sum_{i=1}^{M-1} \cup_{i'} (-1)^i A_{i'} B_{i'}}{(N_B - 1)! \sigma_{UB}^{2N_B}} (\Phi_4 - \Phi_5), \tag{C.6}$$

where Φ_4 and Φ_5 can be given by

$$\begin{aligned} \Phi_4 &= \int_0^\infty u^{\bar{i}+N_B-1} \exp\left(-\frac{ui}{\sigma_{UB}^2} - \frac{u}{\sigma_{UB}^2}\right) \mathrm{d}u \\ &= (\bar{i} + N_B - 1)! \left(\frac{1+i}{\sigma_{UB}^2}\right)^{-\bar{i}-N_B}, \end{aligned} \tag{C.7}$$

$$\begin{aligned} \Phi_5 &= \int_0^\infty u^{\bar{i}+N_B-1} \exp\left(-\frac{\Delta}{a\gamma_p \sigma_{pU}^2 u} - \frac{ui}{\sigma_{UB}^2} - \frac{u}{\sigma_{UB}^2}\right) \mathrm{d}u \\ &= 2\left(\frac{\Delta\sigma_{UB}^2}{a\gamma_p \sigma_{pU}^2 (1+i)}\right)^{\bar{i}+N_B/2} K_{\bar{i}+N_B}\left(2\sqrt{\frac{\Delta(1+i)}{a\gamma_p \sigma_{pU}^2 \sigma_{UB}^2}}\right). \end{aligned} \tag{C.8}$$

Substituting (C.7) and (C.8) into (C.6), we can obtain T_{0_m} as

$$\begin{aligned} T_{0\_m} = \frac{\sum_{i=1}^{M-1} \cup_{i'} (-1)^i A_{i'} B_{i'}}{(N_B - 1)! \sigma_{UB}^{2N_B}} \times \Bigg[&(\bar{i} + N_B - 1)! \left(\frac{1+i}{\sigma_{UB}^2}\right)^{-\bar{i}-N_B} \\ &- 2\left(\frac{\Delta\sigma_{UB}^2}{a\gamma_p \sigma_{pU}^2 (1+i)}\right)^{(\bar{i}+N_B/2)} K_{\bar{i}+N_B}\left(2\sqrt{\frac{\Delta(1+i)}{a\gamma_p \sigma_{pU}^2 \sigma_{UB}^2}}\right)\Bigg]. \end{aligned} \tag{C.9}$$

D. Derivation of (34)

Denote $U = \sum_{n=1}^{N} \sum_{e=1}^{N_e} |h_{JE_{n_e}}|^2$, $V = |h_{pm}|^2$ and $W = \sum_{n=1}^{N} \sum_{e=1}^{N_e} |h_{mE_{n_e}}|^2$, and all random variables are independent of each other. Therefore, T_{1_m} can be rewritten as

$$T_{1\_m} = \int_0^\infty \int_0^\infty \underbrace{\Pr\left(\max_{g\in D, g\neq m} \sum_{j=1}^{N_B} \left|h_{gB_j}\right|^2 < \sum_{j=1}^{N_B} \left|h_{mB_j}\right|^2\right)}_{T_{1\_m\_0}} \times F_U\left(\beta v w - \frac{1}{\gamma_J}\right) f_V(v) f_W(w) \mathrm{d}v \mathrm{d}w. \tag{D.1}$$

Letting $X = \sum_{j=1}^{N_B} |h_{mB_j}|^2$, similarly to (B.3) and (B.4), $T_{1\_m\_0}$ can be expressed as

$$\begin{aligned} T_{1\_m\_0} &= \int_0^\infty \sum_{i=1}^{M-1} \bigcup_{i'} (-1)^i A_{i'} B_{i'} x^{\bar{i}} \exp\left(-\frac{xi}{\sigma_{UB}^2}\right) \frac{x^{N_B-1}}{(N_B-1)! \sigma_{UB}^{2N_B}} \exp\left(-\frac{x}{\sigma_{UB}^2}\right) \mathrm{d}x \\ &= \frac{\sum_{i=1}^{M-1} \cup_{i'} (-1)^i A_{i'} B_{i'}}{(N_B - 1)! \sigma_{UB}^{2N_B}} \times \int_0^\infty x^{\bar{i}+N_B-1} \exp\left(-\frac{xi}{\sigma_{UB}^2} - \frac{x}{\sigma_{UB}^2}\right) \mathrm{d}x \\ &= \frac{\sum_{i=1}^{M-1} \cup_{i'} (-1)^i A_{i'} B_{i'}}{(N_B - 1)! \sigma_{UB}^{2N_B}} (\bar{i} + N_B - 1)! \left(\frac{1+i}{\sigma_{UB}^2}\right)^{-\bar{i}-N_B}. \end{aligned} \tag{D.2}$$

Combining (D.2) and (B.6), we can obtain T_{1_m} as

$$T_{1\_m} = \frac{\sum_{i=1}^{M-1} \cup_{i'} (-1)^i A_{i'} B_{i'}}{(N_B - 1)! \sigma_{UB}^{2N_B}} \times (\bar{i} + N_B - 1)! \left(\frac{1+i}{\sigma_{UB}^2}\right)^{-\bar{i}-N_B} I_{1\_m}, \tag{D.3}$$

which complete the proof of (34).

E

Let $X = |h_{pm}|^2$, $Y = \sum_{j=1}^{N_B} |h_{mB_j}|^2$, $Z = XY$, $U = \sum_{n=1}^{N} \sum_{e=1}^{N_e} |h_{JE_{n_e}}|^2$, $V = \sum_{n=1}^{N} \sum_{e=1}^{N_e} |h_{mE_{n_e}}|^2$, and $W = (U + (1/\gamma_J)/V)$. For simplicity, we assume that the fading coefficients of $|h_{pm}|^2$, $|h_{mB_j}|^2$, $|h_{JE_{n_e}}|^2$, and $|h_{mE_{n_e}}|^2$, $m \in \{1, \ldots, M\}$, $j \in \{1, \ldots, N_B\}$, $n \in \{1, \ldots, N\}$ and $e \in \{1, \ldots, N_E\}$, are i.i.d.

random variables with the means of σ_{pU}^2, σ_{UB}^2, σ_{JE}^2, and σ_{UE}^2, respectively. Therefore, the CDFs of Z and W can be expressed as

$$\begin{aligned} F_Z(z) &= \Pr\left(x < \frac{z}{y}\right) = \int_0^\infty F_X\left(\frac{z}{y}\right) f_Y(y)\mathrm{d}y \\ &= 1 - \frac{1}{(N_B-1)!\sigma_{UB}^{2N_B}} \int_0^\infty y^{N_B-1} \exp\left(-\frac{y}{\sigma_{UB}^2} - \frac{z}{\sigma_{pU}^2 y}\right)\mathrm{d}y \\ &= 1 - \frac{2}{(N_B-1)!\sigma_{UB}^{2N_B}} \left(\frac{z\sigma_{UB}^2}{\sigma_{pU}^2}\right)^{N_B/2} K_{N_B}\left(2\sqrt{\frac{z}{\sigma_{pU}^2\sigma_{UB}^2}}\right), \end{aligned} \tag{E.1}$$

$$F_W(w) = \Pr\left(u < wv - \frac{1}{\gamma_J}\right) = \int_0^\infty F_U\left(wv - \frac{1}{\gamma_J}\right) f_V(v)\mathrm{d}v. \tag{E.2}$$

Similarly to (B.6), $F_U(wv - (1/\gamma_J))$ can be obtained as

$$\begin{aligned} F_X\left(wv - \frac{1}{\gamma_J}\right) = 1 - \exp\left[-\frac{1}{\sigma_{JE}^2}\left(wv - \frac{1}{\gamma_J}\right)\right] \\ \sum_{k=0}^{NN_E-1} \frac{1}{k!\sigma_{JE}^{2k}}\left(wv - \frac{1}{\gamma_J}\right)^k, \end{aligned} \tag{E.3}$$

wherein $(wv - (1/\gamma_J))^k$ can be expressed as

$$\left(wv - \frac{1}{\gamma_J}\right)^k = \sum_{l=0}^{k} \frac{k!w^{k-l}(-1)^l}{l!(k-l)!\gamma_J^l} v^{k-l}. \tag{E.4}$$

Substituting (E.3) into (E.2) yields

$$F_W(w) = 1 - \tau \sum_{k=0}^{NN_E-1} \sum_{l=0}^{k} \frac{(-1)^l w^{k-l}}{l!(k-l)!\gamma_J^l \sigma_{JE}^{2k}} T_3, \tag{E.5}$$

where $\tau = (1/(N_B-1)!\sigma_{UE}^{2NN_E})\exp(1/\sigma_{JE}^2\gamma_J)$, and

$$\begin{aligned} T_3 &= \int_0^\infty v^{k-l+NN_E-1} \exp\left(-\frac{wv}{\sigma_{JE}^2} - \frac{v}{\sigma_{UE}^2}\right)\mathrm{d}v \\ &= (k-l+NN_E-1)!\left(\frac{w}{\sigma_{JE}^2} + \frac{1}{\sigma_{UE}^2}\right)^{l-k-NN_E}. \end{aligned} \tag{E.6}$$

Therefore, T_{2_m} can be rewritten as

$$T_{2\_m} = \int_0^\infty \int_0^\infty F_W(\beta x) \times \prod_{g\in D, g\neq m} \Theta(x,y) f_X(x) f_Y(y)\mathrm{d}x\mathrm{d}y, \tag{E.7}$$

where $F_W(w)$ is given by (E.5), and $\Theta(x,y)$ can be computed as

$$\begin{aligned} \Theta(x,y) = 1 - \frac{2}{(N_B-1)!\sigma_{UB}^{2N_B}} \left(\frac{xy\sigma_{UB}^2}{\sigma_{pU}^2}\right)^{N_B/2} \\ K_{N_B}\left(2\sqrt{\frac{xy}{\sigma_{pU}^2\sigma_{UB}^2}}\right). \end{aligned} \tag{E.8}$$

Data Availability

The data that support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was sponsored in part by the National Key R&D Program of China (no. 2018YFB1003201), the National Natural Science Foundation of P. R. China (nos. 61672296, 61872196, 61872194, and 61902196), Scientific and Technological Support Project of Jiangsu Province (nos. BE2017166 and BE2019740), Major Natural Science Research Projects in Colleges and Universities of Jiangsu Province (no. 18KJA520008), and Six Talent Peaks Project of Jiangsu Province (RJFW-111).

References

[1] Y. Zou, J. Zhu, and X. Jiang, "Joint power splitting and relay selection in energy-harvesting communications for IoT networks," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 584–597, 2020.

[2] W. Sun and J. Liu, "2-to-*M* coordinated multipoint-based uplink transmission in ultra-dense cellular networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8342–8356, 2018.

[3] J. Ren, J. Hu, D. Zhang, H. Guo, Y. Zhang, and X. Shen, "RF energy harvesting and transfer in cognitive radio sensor networks: opportunities and challenges," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 104–110, 2018.

[4] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 74–80, 2004.

[5] T. Li, P. Fan, and K. B. Letaief, "Outage probability of energy harvesting relay-aided cooperative networks over Rayleigh fading channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 972–978, 2016.

[6] S. Wang, M. Xia, K. Huang, and Y.-C. Wu, "Wirelessly powered two-way communication with nonlinear energy harvesting model: rate regions under fixed and mobile relay," *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 8190–8204, 2017.

[7] D. Mishra, S. De, and D. Krishnaswamy, "Dilemma at RF energy harvesting relay: downlink energy relaying or uplink information transfer?" *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 4939–4955, 2017.

[8] L. R. Varshney, "Transporting information and energy simultaneously," in *Procedings of the 2008 IEEE International*

Symposium on Information Theory, pp. 1612–1616, Toronto, Canada, August 2008.

[9] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 1989–2001, 2013.

[10] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4754–4767, 2013.

[11] L. Lv, F. Zhou, J. Chen, and N. Al-Dhahir, "Secure cooperative communications with an untrusted relay: a NOMA-inspired jamming and relaying approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3191–3205, 2019.

[12] P. Mukherjee and S. Ulukus, "Secrecy in MIMO networks with no eavesdropper CSIT," *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4382–4391, 2017.

[13] M. T. Mamaghani and Y. Hong, "On the performance of low-altitude UAV-enabled secure AF relaying with cooperative jamming and SWIPT," *IEEE Access*, vol. 7, pp. 153060–153073, 2019.

[14] J. Zhu, Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Security-reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5825–5831, 2016.

[15] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[16] M. T. Mamaghani and R. Abbas, "Security and reliability performance analysis for two-way wireless energy harvesting based untrusted relaying with cooperative jamming," *IET Communications*, vol. 13, no. 4, pp. 449–459, 2018.

[17] M. T. Mamaghani, A. Mohammadi, P. L. Yeoh, and A. Kuhestani, "Secure two-way communication via a wireless powered untrusted relay and friendly jammer," in *Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–6, Singapore, December 2017.

[18] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[19] X. Chen and Y. Zhang, "Mode selection in MU-MIMO downlink networks: a physical-layer security perspective," *IEEE Systems Journal*, vol. 11, no. 2, pp. 1128–1136, 2017.

[20] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3880–3900, 2016.

[21] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[22] L. Yang, J. Chen, H. Jiang, S. A. Vorobyov, and H. Zhang, "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 26–42, 2017.

[23] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5189–5202, 2016.

[24] H. Deng, H.-M. Wang, J. Yuan, W. Wang, and Q. Yin, "Secure communication in uplink transmissions: user selection and multiuser secrecy gain," *IEEE Transactions on Communications*, vol. 64, no. 8, pp. 3492–3506, 2016.

[25] L. Hu, H. Wen, B. Wu et al., "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, 2018.

[26] W. Tang, S. Feng, Y. Ding, and Y. Liu, "Physical layer security in heterogeneous networks with jammer selection and full-duplex users," *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 7982–7995, 2017.

[27] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y.-D. Yao, "Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks," *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3482–3495, 2019.

[28] P. Yan, J. Yang, M. Liu, J. Sun, and G. Gui, "Secrecy outage analysis of transmit antenna selection assisted with wireless power beacon," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7473–7482, 2020.

[29] X. Ding, Y. Zou, G. Zhang, X. Chen, X. Wang, and L. Hanzo, "The security-reliability tradeoff of multiuser scheduling-aided energy harvesting cognitive radio networks," *IEEE Transactions on Communications*, vol. 67, no. 6, pp. 3890–3904, 2019.

[30] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis, and Z. Zhang, "Secrecy performance of wirelessly powered wiretap channels," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3858–3871, 2016.

[31] K. Cao, B. Wang, H. Ding et al., "Improving physical layer security of uplink NOMA via energy harvesting jammers," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 786–799, 2021.

[32] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 401–415, 2016.

[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, 2017.

[34] V. N. Vo, T. G. Nguyen, and C. So-In, D.-B. Ha, Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer," *IEEE Access*, vol. 5, pp. 25196–25206, 2017.

[35] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Security in energy harvesting networks: a survey of current solutions and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2658–2693, 2020.

[36] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1319–1329, 2017.

[37] Y. Zou, "Intelligent interference exploitation for heterogeneous cellular networks against eavesdropping," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1453–1464, 2018.

[38] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, Academic Press, New York, NY, USA, 7th edition, 2007.

[39] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M.-S. Alouini, "On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 2, pp. 192–203, Jun. 2017.