Achievable Rate Region of Energy-Harvesting Based Secure Two-Way Buffer-Aided Relay Networks

Yulong Nie, Xiaolong Lan, *Member, IEEE,* Yong Liu, *Member, IEEE,* Qingchun Chen, *Senior Member, IEEE,* Gaojie Chen, *Senior Member, IEEE,* Lisheng Fan, and Dong Tang

***Abstract*—This paper considered an energy-harvesting based secure two-way relay (EH-STWR) network, where two users exchanged information with the assistance of one buffer-aided relay that harvested energy from two users. To realize the confidential message exchange between two users in the presence of a potential eavesdropper, a secure bidirectional relaying scheme based on time division broadcast (TDBC) was proposed, where one user sent artificial noise to suppress the eavesdropper and another user transmitted data to the relay. A secure sum-rate maximization problem was formulated subject to average and peak transmit power constraints, data buffer and energy storage causality, and transmission mode constraints. By employing the Lyapunov optimization framework, a security-aware adaptive transmission scheme was proposed to jointly adapt transmission mode selection, power allocation, and security rate allocation according to channel/buffer/energy state information (CSI/BSI/ESI). Analysis results showed that the average achievable secrecy rate region can be significantly improved and there exists an inherent trade-off among transmission delay, requirement of transmit power consumption, and achievable secure sum-rate. Moreover, the channel condition between the energy-constrained relay and the potential eavesdropper is a critical factor on the achievable long-term average secrecy rate performance.**

***Index Terms*—Energy harvesting, two-way secure relaying, buffer-aided relaying, achievable secrecy rate region.**

I. Introduction

With the rapid development of wireless communication technology, sensitive information has been delivered through wireless networks. Due to its broadcasting nature, wireless data transmission always encounters information disclosure to unwanted receivers, *i.e.*, the eavesdroppers. Thus, it is highly desirable to devise a secure communication paradigm [1]. Physical layer security has been recognized as an important approach to guarantee the security in wireless networks by using the inherent randomness of wireless channels and noise [2], [3]. Cooperative relaying technology is widely used in the research area of physical layer security due to the advantage of improving network throughput [4] and extending communication coverage [5]. In [6], physical layer security of multiple-input multiple-output (MIMO)-aided relaying networks was proposed to improve secrecy capacity. A class of relaying channels with orthogonal components was studied in [7] to obtain an enhanced channel in terms of secrecy capacity, even if the relay was untrusted. Achievable rates of the general Gaussian multiple-access and two-way wiretap channels were analyzed in [8]. To enhance physical-layer security, a cooperative jamming scheme was proposed to allow users who are prevented from data transmission to jam an eavesdropper. A cooperative jamming scheme was proposed in [9] for MIMO relaying network to unveil the significant improvement of the achieved secrecy rate. Later, cooperative jamming schemes were extended in [10] to bidirectional secrecy communications with an amplify-and-forward-based untrusted relay. It is shown in [11] that secure bidirectional relaying communications can be realized with a cooperative jamming design, as long as there are sufficient intermediate relays. In [12], an artificial noise-aided two-way opportunistic relay selection scheme was proposed to enhance the security performance between two source nodes with the assistance of multiple two-way relays. In most of the existing research efforts towards secure two-way relaying networks, the data received from the source will be immediately forwarded by the relay to the destination, even though the channel quality of the link between the relay and the destination is weak, which may cause an undesired loss in the realized spectral and energy efficiency. To maintain a reasonable spectral and energy efficiency, buffer-aided techniques were proposed for two-way relaying [13], cooperative non-orthogonal multiple access (NOMA) relaying network [14], wireless powered communication network [15], and amplify-and-forward relaying network [16]. Moreover, it is disclosed in [17] that a slow-fading channel can be converted into a fast-fading channel with some cost of the increased transmission delay in the buffer-aided relaying network. In fact, data buffer at the relay can create a new degree of freedom to schedule the relay transmission/reception mechanism. The results in [18]-[25] showed that secure buffer-aided relaying design can be scheduled to temporarily store the data in the buffer when the

The work of Yulong Nie and Qingchun Chen was jointly supported by the National Natural Science Foundation of China (NSFC) under Grant No.61771406 and the International Collaborative Research Program of Guangdong Science and Technology Department under Grant No.2020A0505100061. The work of Yong Liu was supported by the National Natural Science Foundation of China (NSFC) under Grant No.61901180. (*Corresponding author: Qingchun Chen.*)

Yulong Nie and Qingchun Chen are with the Research Center of Intelligent Communication Engineering, Huangpu Research & Graduate School of Guangzhou University, and they are also with the School of Electronics and Communication Engineering, Guangzhou University, Guangzhou, 510006, China. Xiaolong Lan is with the College of Cybersecurity, Sichuan University, Chengdu 610065, China. Yong Liu is with the School of Physics and Telecommunication Engineering, South China Normal University, Guangzhou, 510006, China. Gaojie Chen is with the Department of Engineering, University of Leicester, Leicester, UK. Lisheng Fan is with the School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou, 510006, China. Dong Tang is with the School of Electronics and Communication Engineering, Guangzhou University, Guangzhou, 510006, China.

corresponding link quality is not good enough, which can not only guarantee the secure transmission but also can improve the spectral efficiency of wireless networks.

In general, energy-constrained wireless devices impose a critical challenge on wireless network design. As an emerging technique to convert the received radio frequency (RF) signal into electricity for powering devices, an RF-based energy-harvesting technique provides a promising method to prolong the lifetime of wireless network and improve network performance [26]- [31]. In particular, a simultaneous wireless information and power transfer (SWIPT) technique developed in [26] has been recognized as a sustainable energy solution for future wireless network design [27]- [30]. In [13] and [31], Lyapunov optimization framework and an RF-based energy harvesting technique were combined to improve the transmission performance of a two-way relaying network. In SWIPT relaying network, time-switching-based relaying (TSR) and power-splitting-based relaying (PSR) [32], [33] protocols divide the received signal at the relay for energy harvesting (EH) and data delivery in the time and power domains, respectively. A secure cooperative relaying network with RF-based energy-harvesting capability has recently attracted much research attention. In [34], a secure two-way relaying network was investigated, where the influence of different PS and TS factors on the achieved performance was analyzed. The secrecy performance of a three-node relaying network with an EH-based untrusted relay was analyzed in [35], where both the signal transmitted by the source and the jamming signal by the destination were utilized for energy harvesting. In [36], an EH-based secure relaying network design with one amplify-and-forward (AF) relay was studied. A novel artificial noise (AN)-aided transmission scheme was proposed in [37] for an EH-based multi-antenna AF relaying network. Then, a secrecy capacity analysis was presented to explicitly show the impacts of system parameters, such as EH time, relay location, AN power, and number of relay antennas, on system performance. In [38], a wireless EH mechanism was utilized to transform the jamming signal into energy supply to improve the realized security performance in a secure AF relaying system. An EH-based buffer-aided relaying protocol can realize the benefit of both EH and buffer-aided relaying techniques, and the first motivation of this paper was to focus on EH-based secure two-way buffer-aided relaying networks.

Although there are already some research results about two-way relaying design, few efforts are devoted to disclosing the achievable security rate region of secure buffer-aided two-way relay network. The achievable rate region of the buffer-aided two-way relaying network with RF energy-harvesting was studied in [13], and it was shown that there is a great potential of exploring data buffer and energy storage at the relay to realize efficient energy-harvesting-based two-way relaying network. However, the achieved security performance in the presence of an eavesdropper has not been explored yet. Recently, the optimal power-splitting and time-switching energy harvesting schemes have been studied to optimize the physical layer security performance of a two-way relaying network in [39]. Nonetheless, the influence of buffers was not explored. The achievable secrecy rate region of energy-harvesting-based secure two-way buffer-aided relay networks is still unknown, which motivated us to conduct investigation in this regard. The primary contributions of this paper can be briefly summarized as follows:

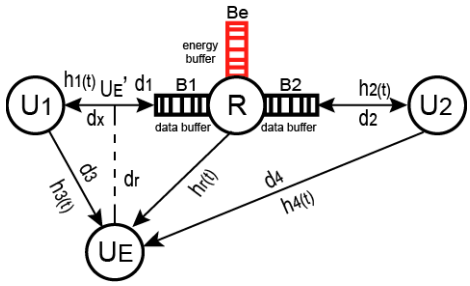


Fig. 1. A buffer-aided EH-based two-way secure relay (TWSR) network, consisting of two users U_1, U_2, one eavesdropper U_e and one half-duplex DF relay R.

- A secure bidirectional relaying scheme based on time division broadcast (TDBC) was proposed for EH-based secure two-way buffer-aided relay network, where two users exchanged confidential messages with the assistance of one intermediate relay in the presence of one potential eavesdropper. The weighted secure sum-rate maximization problem was formulated to derive the average achievable secrecy rate region, where transmission mode selection, transmit power allocation, and secrecy rate allocation were jointly optimized subject to average and peak transmit power constraints, data buffer and energy storage causality, and transmission mode constraints. It is disclosed that the achievable secrecy rate region of EH-based secure buffer-aided two-way relay network can be notably improved by fully exploiting data buffer-aided transmission mechanism.
- In order to realize the benefit of EH-based secure two-way buffer-aided relaying protocol, by employing the Lyapunov optimization framework, a security-aware adaptive transmission scheme was proposed to jointly adapt transmission mode selection, power allocation, and security rate allocation according to channel/buffer/energy state information (CSI/BSI/ESI). Results showed that there exists an inherent tradeoff among transmission delay, requirement of transmit power consumption, and achievable secrecy sum-rate. In addition, the channel condition between energy-constrained relay and eavesdropper is a critical factor that affects the achievable long-term average secrecy rate performance.

The remainder of this paper was organized as follows: In Section II, the system model and the problem formulation of EH-based secure two-way buffer-aided relaying scheme was introduced. The achievable secrecy rate region analysis and the security-aware adaptive transmission scheme were presented in Section III. The numerical results were presented in Section IV. Finally, the conclusion was in Section V.

II. System Model and Problem Formulation

A. System Model

As shown in Fig. 1, an energy-harvesting-based secure two-way relaying (EH-STWR) network is considered, where two users U_1 and U_2 exchange confidential information with the assistance of one half-duplex decode-and-forward (DF) relay R in the presence of one potential eavesdropper node U_e. It is assumed that there is no direct link between U_1 and U_2. Two users and the relay are assumed to be provisioned with single antenna. The relay R is assumed to be an energy-constrained device that harvests energy from signals transmitted by U_1 and U_2. Meanwhile, R is assumed to be provisioned with one energy storage B_e and two data buffers B_1 and B_2, where B_e is used to store the harvested energy while B_1 and B_2 are utilized to temporarily store the received data from U_1 and U_2, respectively. The status of energy storage B_e and the states of two data buffers B_1 and B_2 in the tth time slot are denoted by $E(t)$, $Q_1(t)$, and $Q_2(t)$, respectively. B_e, B_1, and B_2 are assumed to be large enough such that there are no harvested energy waste and data overflows with reasonable scheduling design [40]. The untrusted user U_e who might be a potential eavesdropper is assumed to be deployed with a single antenna as well. To suppress the eavesdropper and to enhance the secrecy performance, when one user transmits data to the relay, another user will simultaneously transmit artificial noise (AN) to confuse the eavesdropper [12]. The AN signals transmitted by both users are pre-designed pseudo-random signals that are known to the relay and can be perfectly eliminated at the relay [41], [12].

In this paper, R is assumed to be located in the connection line of U_1 and U_2, and d_i stands for the distance between U_i and the relay. d_3 (d_4) is the distance between U_1 (U_2) and U_e. Let $U_E^{'}$ denotes the closest point to U_E in the connecting line between two users, d_r is the closet distance between U_e and the connecting line between U_1 and U_2, and d_x represents the distance between U_1 and $U_E^{'}$. All the links are assumed to be quasi-static Rayleigh fading channels, and the channel coefficients are assumed to remain unchanged in each time slot but may vary independently from one slot to another. Let $h_1(t)$, $h_2(t)$, $h_3(t)$, $h_4(t)$, and $h_r(t)$ denote the channel coefficients of links $U_1 \leftrightarrow R$, $U_2 \leftrightarrow R$, $U_1 \leftrightarrow U_e$, $U_2 \leftrightarrow U_e$, and $R \rightarrow U_e$ in the tth time slot, respectively. In this paper, the centralized scheduling scheme is assumed, where the relay plays the role of the central node that is supposed to obtain channel state information (CSI) of all the involved links[1] by using appropriate channel estimation techniques.[2] Besides, in each time slot, the relay is supposed to make up decision according to the current CSIs as well as the status of energy storage, and data buffers, and to inform both users how to adjust their energy transfer, confidential message transmission, and artificial noise transmission.

[1]The potential eavesdropper U_e is a legitimate user who needs the assistance by the relay as well [42].

[2]The CSI acquisition requires proper insertion of channel estimation pilots at transmitters and appropriate channel estimation design at receivers. As for the practical channel estimate design issue in the decode-and-forward relaying system, the readers may refer to [46] and other related literature for the details.

B. Transmission Modes

In this paper, the confidential message exchange between two users can be completed via four transmission modes: (1) *energy transmission mode*, where the relay harvests energy from radio frequency signals transmitted by two users; (2) *data transmission mode from U_1 to R*, where U_1 transmits the confidential message to the relay while U_2 simultaneously transmits the artificial noise to confuse the eavesdropper U_e; (3) *data transmission mode from U_2 to R*, where U_2 and U_1 transmit the secret message and artificial noise to the relay simultaneously; and (4) *broadcasting mode*, where the relay forwards the multiplexed data extracted from the data buffers B_1 and B_2 to two users by using the harvested energy. Binary variable $\{q_i(t) \in \{0,1\}, i \in \{1,2,3,4\}\}$ is denoted as the selection decision of the ith transmission modes in the tth time slot. $q_i(t) = 1$ implies that the corresponding ith transmission mode is selected, otherwise $q_i(t) = 0$. Besides, only one mode can be activated in each time slot, namely, $q_1(t) + q_2(t) + q_3(t) + q_4(t) = 1$. Due to the potential eavesdropper U_e, let $R_{ir}^{sec}(t)$ and $R_{ri}^{sec}(t), i \in \{1,2\}$ denote the secrecy transmission rate from U_i to R and from R to U_i in time slot t, respectively. The four transmission modes can be explicated as follows:

(1) $\mathcal{M}_1$ (*energy-harvesting mode*): In this mode, the received signal at R is utilized for energy harvesting. The corresponding received signal and the amount of harvested energy can be given as follows:

$$y_r^{M_1}(t) = \sqrt{\frac{P_1(t)}{d_1^m}} h_1(t) x_1(t) + \sqrt{\frac{P_2(t)}{d_2^m}} h_2(t) x_2(t) + n(t), \quad (1)$$

$$E_h(t) = q_1(t) \Big(\frac{P_1(t) \left| h_1(t) \right|^2}{d_1^m} + \frac{P_2(t) \left| h_2(t) \right|^2}{d_2^m} \Big) \eta T, \quad (2)$$

where $P_1(t)$ and $P_2(t)$ represent the transmit power of U_1 and U_2, respectively. $x_i(t)$ $(i = 1, 2)$ is the transmitted signal of U_i and $\mathbb{E}[|x_i(t)|^2] = 1$. m is the path loss exponent, $\eta \in [0, 1]$ is the energy conversion efficiency, T is the time duration of one slot, and $n(t)$ is the additive white Gaussian noise (AWGN) at R with zero mean and variance σ^2, *i.e.*, $n(t) \sim \mathcal{CN}(0, \sigma^2)$. The harvested energy is stored in B_e and the energy queue $E(t)$ can be updated as follows:

$$E(t) = E(t-1) + E_h(t). \quad (3)$$

(2) $\mathcal{M}_2$ (*data transmission mode from U_1 to R*): In this mode, U_1 is scheduled to transmit the confidential message to R. To efficiently improve the secrecy rate, U_2 is assumed to generate an AN signal to confuse the potential eavesdropper U_e when U_1 transmits the confidential message to R. Moreover, the transmitted AN signal by U_2 is assumed as a pre-designed pseudo-random signal, which is known to R [12]. Thus, R can perfectly eliminate the artificial noise, and the received signals at R and eavesdropper in the tth time slot can be given as follows:

$$y_r^{M_2}(t) = \sqrt{\frac{P_1(t)}{d_1^m}} h_1(t) x_1(t) + n(t), \quad (4)$$

$$y_e^{M_2}(t) = \sqrt{\frac{P_1(t)}{d_3^m}} h_3(t) x_1(t) + \sqrt{\frac{P_2(t)}{d_4^m}} h_4(t) x_2(t) + n_e(t), \quad (5)$$

where $n_e(t)$ is the AWGN noise at U_e with zero mean and variance σ^2. Therefore, the secure transmission rate $R_{1r}^{sec}(t)$ from U_1 to R satisfies

$$R_{1r}^{sec}(t) \le q_2(t)\Big[\log_2\Big(1+P_1(t)H_1(t)\Big) - \log_2\Big(1+\frac{P_1(t)H_3(t)}{1+P_2(t)H_4(t)}\Big)\Big]^+, \tag{6}$$

where $H_i(t)=\frac{|h_i(t)|^2}{d_i^m\sigma^2}, i\in\{1,2,3,4\}$ and $[\cdot]^+=\max\{\cdot,0\}$. When the relay successfully decodes the data from U_1, the queue length of the data buffer B_1 will be updated as follows:

$$Q_1(t)=Q_1(t-1)+R_{1r}^{sec}(t). \tag{7}$$

(3) $\mathcal{M}_3$ (*data transmission mode from U_2 to R*): In this mode, U_2 and U_1 transmit the confidential message and AN signal to R, respectively, and the received signals at R and U_e are given below:

$$y_r^{M_3}(t)=\sqrt{\frac{P_2(t)}{d_2^m}}h_2(t)x_2(t)+n(t), \tag{8}$$

$$y_e^{M_3}(t)=\sqrt{\frac{P_2(t)}{d_4^m}}h_4(t)x_2(t)+\sqrt{\frac{P_1(t)}{d_3^m}}h_3(t)x_1(t)+n_e(t). \tag{9}$$

Thus, the secure transmission rate $R_{2r}^{sec}(t)$ satisfies

$$R_{2r}^{sec}(t) \le q_3(t)\Big[\log_2\Big(1+P_2(t)H_2(t)\Big) - \log_2\Big(1+\frac{P_2(t)H_4(t)}{1+P_1(t)H_3(t)}\Big)\Big]^+. \tag{10}$$

(4) $\mathcal{M}_4$ (*broadcast mode*): In this mode, R firstly extracts confidential messages from data buffers B_1 and B_2. Then, R generates the multiplexing signal $x_r(t)=\sqrt{P_{r1}(t)}x_2(t)+\sqrt{P_{r2}(t)}x_1(t)$ and broadcasts it back to two users by using the energy stored in B_e, where $P_{r1}(t)$ and $P_{r2}(t)$ represent the transmit power allocated to $x_2(t)$ and $x_1(t)$ at the relay, respectively. Thus, the total power consumption of R in this mode is $P_r(t)=P_{r1}(t)+P_{r2}(t)$. Since user U_i $(i=1,2)$ knows its own data and CSI between the relay and itself, it can perform self-interference cancellation to obtain its desired signal. Therefore, the received signals at U_i $(i=1,2)$ and U_e can be given as follows [34]:

$$y_1^{M_4}(t)=\sqrt{\frac{P_{r1}(t)}{d_1^m}}h_1(t)x_2(t)+n_1(t), \tag{11}$$

$$y_2^{M_4}(t)=\sqrt{\frac{P_{r2}(t)}{d_2^m}}h_2(t)x_1(t)+n_2(t), \tag{12}$$

$$y_e^{M_4}(t)=\sqrt{\frac{P_{r1}(t)}{d_r^m}}h_r(t)x_2(t)+\sqrt{\frac{P_{r2}(t)}{d_r^m}}h_r(t)x_1(t)+n_e(t), \tag{13}$$

where $n_1(t)$ and $n_2(t)$ represent the AWGN noise with zero mean and variance σ^2 at U_1 and U_2, respectively. Therefore, the secure transmission rates on $R\to U_1$ and $R\to U_2$ links can be given below:

$$R_{r1}^{sec}(t)\le q_4(t)\min\{C_{r1}^{sec}(t),Q_2(t-1)\}, \tag{14}$$

$$R_{r2}^{sec}(t)\le q_4(t)\min\{C_{r2}^{sec}(t),Q_1(t-1)\}, \tag{15}$$

where $C_{r1}^{sec}(t)$ and $C_{r2}^{sec}(t)$ stand for the maximum allowed transmission rate of $R\to U_1$ and $R\to U_2$ links, respectively. If a randomize-and-forward relaying strategy is assumed such that U_e treats $x_2(t)$ (or $x_1(t)$) as noise when decoding $x_1(t)$ (or $x_2(t)$), $C_{r1}^{sec}(t)$ and $C_{r2}^{sec}(t)$ can be given as follows:

$$C_{r1}^{sec}(t)=\Big[\log_2\Big(1+P_{r1}(t)H_1(t)\Big) - \log_2\Big(1+\frac{P_{r1}(t)H_r(t)}{1+P_{r2}(t)H_r(t)}\Big)\Big]^+, \tag{16}$$

$$C_{r2}^{sec}(t)=\Big[\log_2\Big(1+P_{r2}(t)H_2(t)\Big) - \log_2\Big(1+\frac{P_{r2}(t)H_r(t)}{1+P_{r1}(t)H_r(t)}\Big)\Big]^+, \tag{17}$$

where $H_r(t)=\frac{|h_r(t)|^2}{d_r^m\sigma^2}$.

C. Problem Formulation

Unlike the existing works in secure two-way relaying (STWR) networks [19], [34], the goal is to maximize the average achievable secrecy rate region subject to long-term average and peak transmit power constraints. In addition, power allocations, secrecy rate allocations, and transmission mode selection are jointly optimized according to CSI, buffer state information (BSI), and energy state information (ESI). The peak transmit power constraints at U_1, U_2, and R in each time slot can be given below:

$$0\le P_i(t)\le \widehat{P}_i, i\in\{1,2,r\},\forall t, \tag{18}$$

where $\widehat{P}_i$ is the peak transmit power at node $i\in\{1,2,r\}$. The long-term transmit power constraint at U_1 and U_2 is as follows:

$$\overline{P}_i=\lim_{N\to\infty}\frac{1}{N}\sum_{t=0}^{N-1}\sum_{m=1}^{3}q_m(t)P_i(t)\le \overline{P}_i^{\max}, i\in\{1,2\}, \tag{19}$$

where N is the total number of transmission time slots, t represents the time slot index, and $\overline{P}_i$ and $\overline{P}_i^{\max}$ stand for the average transmit power and the maximum allowed long-term average transmit power of node i $(i\in\{1,2\})$, respectively. The average consumed energy at R can not exceed its harvested energy, *i.e.,*

$$\overline{P}_r=\lim_{N\to\infty}\frac{1}{N}\sum_{t=0}^{N-1}q_4(t)P_r(t)\le\lim_{N\to\infty}\frac{1}{N}\sum_{t=1}^{N}\frac{E_h(t)}{T}. \tag{20}$$

Let $\overline{R}_{1r}^{sec}$, $\overline{R}_{r2}^{sec}$, $\overline{R}_{2r}^{sec}$, and $\overline{R}_{r1}^{sec}$ denote the long-term average secrecy rates of the links $U_1\to R, R\to U_2, U_2\to R$, and $R\to U_1$, respectively, and we have

$$\overline{R}_i^{sec}=\lim_{N\to\infty}\frac{1}{N}\sum_{t=0}^{N-1}R_i^{sec}(t), i\in\{1r,r2,2r,r1\}. \tag{21}$$

Let $\overline{R}_{12}^{sec}$, $\overline{R}_{21}^{sec}$ denote the average end-to-end secrecy rates of links $U_1\to U_2$ and $U_2\to U_1$, respectively, $\overline{R}_{12}^{sec}=\min\{\overline{R}_{1r}^{sec},\overline{R}_{r2}^{sec}\}$, and $\overline{R}_{21}^{sec}=\min\{\overline{R}_{2r}^{sec},\overline{R}_{r1}^{sec}\}$. Meanwhile, the maximum average secrecy rate can be obtained when two data queues are in a non-absorption state [44], namely, the average arrival rate is equal to the average departure rate, $i.e.$,

$$\overline{R}_{1r}^{sec}=\overline{R}_{r2}^{sec},\quad \overline{R}_{2r}^{sec}=\overline{R}_{r1}^{sec}. \tag{22}$$

The average achievable secrecy rate region can be obtained by maximizing the following weighted long-term secrecy sum-rate problem $\mathbf{P_1}$:

$$\begin{aligned}\mathbf{P_1}: \max_{\mathbf{q(t)},\mathbf{P(t)},\mathbf{R(t)}}\ & \theta\overline{R}_{1r}^{sec}+(1-\theta)\overline{R}_{2r}^{sec}\\ \text{s.t.}\ & (2),(6),(10),(14)-(22),\\ & q_1(t)+q_2(t)+q_3(t)+q_4(t)=1,\forall t,\\ & q_i(t)(q_i(t)-1)=0,,\forall i\in\{1,2,3,4\},\forall t,\end{aligned} \tag{23}$$

where $\theta \in [0,1]$ is the weighting coefficient associated with U_1, and the optimization variables include mode selection decision $\mathbf{q(t)} = \big(q_1(t), q_2(t), q_3(t), q_4(t)\big)$, power allocation policy $\mathbf{P(t)} = \big(P_1(t), P_2(t), P_r(t)\big)$, and rate allocation $\mathbf{R(t)} = \big(R_{1r}^{sec}(t), R_{r2}^{sec}(t), R_{2r}^{sec}(t), R_{r1}^{sec}(t)\big)$. Unfortunately, the above optimization problem $\mathbf{P_1}$ is a mixed-integer non-convex problem. In order to address this issue, in the next section, the use of Lyapunov optimization framework to transform the time average optimization problem $\mathbf{P_1}$ into a real-time problem is proposed, which can be further decomposed into multiple subproblems in Section III.

III. Security-Aware-Adaptive Transmission Design

A. Dynamic Characteristics of the EH-STWR Network

In this paper, since the relay is provisioned with the energy storage and two data buffers, R is able to temporarily store the harvested energy and to cache the received confidential messages from two users. When the energy-harvesting mode is scheduled, R stores the harvested energy into the energy storage. If either of the transmission mode $\mathcal{M}_2$ or $\mathcal{M}_3$ is selected, R stores the restored confidential message into the corresponding data buffers. While if the broadcast mode $\mathcal{M}_4$ is selected, R first extracts confidential messages from both data buffers, and then forwards the multiplexing signal to two users by using the energy stored in the energy storage. Hence, the dynamic updates of the energy storage $E(t)$ and two data buffers $Q_1(t), Q_2(t)$ can be summarized as follows:

$$E(t+1) = \max\{E(t) + E_h(t) - q_4(t)P_r(t)T, 0\}, \tag{24}$$

$$Q_1(t+1) = \max\{Q_1(t) + R_{1r}^{sec}(t) - R_{r2}^{sec}(t), 0\}, \tag{25}$$

$$Q_2(t+1) = \max\{Q_2(t) + R_{2r}^{sec}(t) - R_{r1}^{sec}(t), 0\}. \tag{26}$$

$Z_i(t)$ $(i = 1, 2)$ is defined as the virtual average power consumption queue of U_i, which is given below:

$$Z_i(t+1) = \max\Big\{Z_i(t) + \sum_{m=1}^{3} q_m(t)P_i(t) - \overline{P}_i^{\max}, 0\Big\}. \tag{27}$$

Then, we have

$$Z_i(t+1) \geq Z_i(t) + \sum_{m=1}^{3} q_m(t)P_i(t) - \overline{P}_i^{\max}. \tag{28}$$

Adding up the total power consumption of U_i in t successive time slots, and then dividing by t, it yields the following relation:

$$\frac{Z_i(t) - Z_i(0)}{t} \geq \frac{1}{t}\sum_{\tau=0}^{t-1}\sum_{m=1}^{3} q_m(\tau)P_i(\tau) - \overline{P}_i^{\max}. \tag{29}$$

Without loss of generality, $Z(0) = 0$ is assumed. Taking the expectation of both sides, we have

$$\lim_{t\to\infty} \frac{\mathbb{E}\{Z_i(t)\}}{t} \geq \overline{P}_i - \overline{P}_i^{\max}. \tag{30}$$

where $\mathbb{E}\{\cdot\}$ denotes the expectation. Thus, according to the above analysis, if the virtual queue is mean rate stable, *i.e.,* $\lim_{t\to\infty} \frac{\mathbb{E}\{Z_i(t)\}}{t} = 0$, the average power consumption constraint can be guaranteed, *i.e.*, $\overline{P}_i \leq \overline{P}_i^{\max}$, which means that the average power consumption constraint can be converted into the stable virtual power consumption queue constraint.

B. Security-Aware Adaptive Transmission Scheme

According to the above analysis, the status of energy queues, two data buffer queues and two virtual power consumption queues are jointly considered and the following quadratic Lyapunov function can be defined:

$$L(\Theta(t)) = \frac{\psi}{2}(\phi - E(t))^2 + \frac{1}{2}\sum_{i=1}^{2}\big(Q_i^2(t) + Z_i^2(t)\big), \tag{31}$$

where $\Theta(t) = [E(t), Q_1(t), Q_2(t), Z_1(t), Z_2(t)]$ represents all queue states, ψ is a nonnegative constant used to guarantee the same order of magnitude in (31), and ϕ is a positive perturbation value of the energy storage at the relay. In general, the energy queue size will not exceed ϕ. In order to characterize the expected increment of all queues between two consecutive time slots, the following *Lyapunov drift* is defined:

$$\Delta(\Theta(t)) = \mathbb{E}\big[L(\Theta(t+1)) - L(\Theta(t))|\Theta(t)\big]. \tag{32}$$

To ensure the stability of all queues, the transmission policy can be devised to minimize the *Lyapunov drift* $\Delta(\Theta(t))$. At the same time, since the goal is to maximize the achievable secrecy rate region, the transmission scheme can be derived by minimizing the following *Lyapunov drift-plus-penalty*:

$$\Delta\big(\Theta(t)\big) - V\mathbb{E}\big[R_{sum}(t)|\Theta(t)\big], \tag{33}$$

where $R_{sum}(t) = \theta R_{1r}^{sec}(t) + (1-\theta)R_{2r}^{sec}(t)$, and V is a nonnegative control parameter that is chosen to unveil the tradeoff between the average queue length and the average achievable secrecy rate. The upper bound of the *Lyapunov drift-plus-penalty* can be given in *Lemma* 1.

Lemma 1: In each time slot, with any control policy, the *Lyapunov drift-plus-penalty* can be upper bounded as below:

$$\begin{aligned}\Delta(\Theta(t)) - V\mathbb{E}\big[R_{sum}(t)|\Theta(t)\big] \leq\ & B - V\mathbb{E}\big[R_{sum}(t)|\Theta(t)\big] \\ & + \psi\big(\phi - E(t)\big)\mathbb{E}\big[q_4(t)P_r(t)T - E_h(t)|\Theta(t)\big] \\ & + \sum_{i=1}^{2} Z_i(t)\mathbb{E}\big[(q_1(t)+q_2(t)+q_3(t))P_i(t) - \overline{P}_i^{\max}|\Theta(t)\big] \\ & + Q_1(t)\mathbb{E}\big[R_{1r}^{sec}(t) - R_{r2}^{sec}(t)|\Theta(t)\big] \\ & + Q_2(t)\mathbb{E}\big[R_{2r}^{sec}(t) - R_{r1}^{sec}(t)|\Theta(t)\big],\end{aligned} \tag{34}$$

where B is a positive constant independent of V that satisfies the following constraint

$$\begin{aligned}B \geq\ & \frac{\psi}{2}\mathbb{E}\big[\big(q_4(t)P_r(t)T\big)^2 + E_h(t)^2|\Theta(t)\big] \\ & + \frac{1}{2}\sum_{i=1}^{2}\mathbb{E}\big[\big((q_1(t)+q_2(t)+q_3(t))P_i(t)\big)^2 + \big(\overline{P}_i^{\max}\big)^2|\Theta(t)\big] \\ & + \frac{1}{2}\sum_{i=1}^{2}\mathbb{E}\big[R_{ir}^{sec}(t)^2 + R_{ri}^{sec}(t)^2|\Theta(r)\big].\end{aligned} \tag{35}$$

Proof: See Appendix A.

According to Lemma 1, instead of directly minimizing the *Lyapunov drift-plus-penalty*, our transmission scheme is to minimize its upper bound, which can not only guarantee the queue stability but also maximize the achievable secrecy rate region. Hence, based on the current queue states $\Theta(t)$ and channel state information, the following optimization problem

can be formulated to derive transmit power allocation, secrecy rate allocations, and mode selection policies:

$$\begin{aligned}\min_{\mathbf{q(t)},\mathbf{P(t)},\mathbf{R(t)}} \quad & -\Delta_1(t)R_{1r}^{sec}(t)-\Delta_2(t)R_{2r}^{sec}(t)\\ & +\sum_{i=1}^{2}Z_i(t)\big(q_1(t)+q_2(t)+q_3(t)\big)P_i(t)\\ & +\psi(\phi-E(t))\big(q_4(t)P_r(t)T-E_h(t)\big)\\ & -Q_2(t)R_{r1}^{sec}(t)-Q_1(t)R_{r2}^{sec}(t)\\ \text{s.t.} \quad & (2),(6),(10),(14)-(18)\\ & q_1(t)+q_2(t)+q_3(t)+q_4(t)=1,\\ & q_i(t)\big(q_i(t)-1\big)=0, i=1,2,3,4,\ \forall t,\end{aligned} \tag{36}$$

where $\Delta_1(t)=\theta V-Q_1(t)$ and $\Delta_2(t)=(1-\theta)V-Q_2(t)$. Due to the binary optimization vector $\mathbf{q(t)}$, there is only one mode that can be selected in each time slot. Therefore, the above optimization problem can be analyzed in four cases.

Case 1. $\mathcal{M}_1$ (*energy harvesting mode*): In this case, the relay harvests energy from two users, $q_1(t)=1$ and $q_2(t)=q_3(t)=q_4(t)=0$. Therefore, the problem (36) can be rewritten as

$$\begin{aligned}\min_{P_1(t),P_2(t)} \quad & -\psi\big(\phi-E(t)\big)E_h(t)+Z_1(t)P_1(t)+Z_2(t)P_2(t)\\ \text{s.t.} \quad & 0\le P_i(t)\le \widehat{P}_i, i=1,2.\end{aligned} \tag{37}$$

Obviously, the objective function and all constraints are linear. The solutions can be obtained in *Lemma* 2.

Lemma 2: In the energy-harvesting mode, the optimal transmit power of U_1 and U_2 is either the peak or zero, *i.e.,*

$$P_i(t)=\begin{cases}\widehat{P}_i, & Z_i(t)\le\psi(\phi-E(t))\left|h_i(t)\right|^2T\eta,\\ 0, & \text{otherwise.}\end{cases} \tag{38}$$

Lemma 2 implies that the on/off energy allocation policy is optimal in the energy-harvesting mode, where $\psi(\phi-E(t))\left|h_i(t)\right|^2T\eta$ corresponds to the threshold value.

Case 2. $\mathcal{M}_2$ (*data transmission mode from U_1 to R*): In this mode, $q_2(t)=1$ and $q_1(t)=q_3(t)=q_4(t)=0$, and the problem (36) can be rewritten as follows:

$$\begin{aligned}\min_{P_1(t),P_2(t),R_{1r}^{sec}(t)} \quad & -\Delta_1(t)R_{1r}^{sec}(t)+\sum_{i=1}^{2}Z_i(t)P_i(t)\\ \text{s.t.} \quad & (6),(18).\end{aligned} \tag{39}$$

The optimal solutions can be derived by using the Karush-Kuhn-Tucker (KKT) conditions. The optimization problem (39) can be solved in two cases:

(1) $\Delta_1(t)\le 0$. In this case, the objective function increases with $P_1(t),P_2(t)$ and $R_{1r}^{sec}(t)$, so the optimal power allocation and the optimal secrecy rate results are $P_1(t)=P_2(t)=0$ and $R_{1r}^{sec}(t)=0$.

(2) $\Delta_1(t)>0$. In this case, based on the KKT conditions, the optimal secrecy rate allocation is given as follows:

$$\begin{aligned}R_{1r}^{sec}(t)=\Big[&\log_2\Big(1+P_1(t)H_1(t)\Big)\\ &-\log_2\Big(1+\frac{P_1(t)H_3(t)}{1+P_2(t)H_4(t)}\Big)\Big]^+.\end{aligned} \tag{40}$$

The optimal power allocation $(P_1(t),P_2(t))$ are presented in (41), which can also be illustrated in Fig. 2. A larger $\Delta_1(t)$ will result in a larger transmit power of U_1 and in a larger AN power of U_2 to confuse U_e, respectively. Therefore, a decrease in $Q_1(t)$ will lead to a larger transmit power and a larger AN power. When $\Delta_1(t)\le 0$, U_1 will not transmit any data to the relay and U_2 will not transmit AN to confuse U_e either, which means θV is the threshold value of the queue size $Q_1(t)$. Thus, the maximum data queue size can be determined by adjusting the value of V. Moreover, when the data queue size $Q_1(t)$ is large enough, U_1 will reduce the transmit power until it keeps silent to guarantee the stability of the data queue at the relay, and U_2 will keep silent for energy conservation accordingly. When the data queue size $Q_1(t)$ is small, U_1 will try to transmit and U_2 should try to transmit the AN signal to confuse U_e to maximize the security transmission rate.

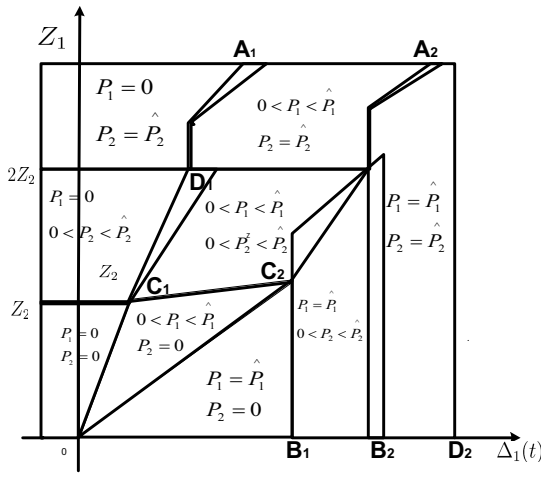


Fig. 2. The optimal transmit power allocation of U_1 in the mode $\mathcal{M}_2$.

Case 3. $\mathcal{M}_3$ (*data transmission mode from U_2 to R*): In this mode, $q_3(t)=1$, $q_1(t)=q_2(t)=q_4(t)=0$, and the optimization problem (36) can be rewritten as follows:

$$\begin{aligned}\min_{P_1(t),P_2(t),R_{2r}^{sec}(t)} \quad & -\Delta_2(t)R_{2r}^{sec}(t)+\sum_{i=1}^{2}Z_i(t)P_i(t)\\ \text{s.t.} \quad & (10),(18).\end{aligned} \tag{44}$$

Similar to the analysis of $\mathcal{M}_2$, the optimal solutions to the optimization problem (44) can also be derived by using the KKT conditions in two cases:

(1) $\Delta_2(t)\le 0$. In this case, the objective function increases with $P_1(t),P_2(t)$ and $R_{2r}^{sec}(t)$, so the optimal secrecy rate and the power allocation results in this mode are $P_1(t)=P_2(t)=0$ and $R_{2r}^{sec}(t)=0$.

(2)$\Delta_2(t)>0$. In this case, by using the KKT conditions, the optimal secrecy rate allocation can be derived as follows:

$$\begin{aligned}R_{2r}^{sec}(t)=\Big[&\log_2\Big(1+P_2(t)H_2(t)\Big)\\ &-\log_2\Big(1+\frac{P_2(t)H_4(t)}{1+P_1(t)H_3(t)}\Big)\Big]^+.\end{aligned} \tag{45}$$

Meanwhile, the optimal power allocation can be similarly derived like the mode $\mathcal{M}_2$.

Case 4. $\mathcal{M}_4$ (*broadcast mode*): In the broadcasting mode, the relay is selected for forwarding confidential messages to U_1 and U_2, and the eavesdropper will eavesdrop on the relay. Then, $q_4(t)=1$ and $q_1(t)=q_2(t)=q_3(t)=0$. Thus, the optimization problem (36) can be rewritten as follows:

$$\begin{aligned}\min_{P_r(t),R_{r1}^{sec}(t),R_{r2}^{sec}(t)} \quad & \psi(\phi-E(t))P_r(t)T-Q_1(t)R_{r2}^{sec}(t)\\ & -Q_2(t)R_{r1}^{sec}(t)\\ \text{s.t.} \quad & (14)-(18).\end{aligned} \tag{46}$$

$$(P_1(t),P_2(t))=\begin{cases}(0,0), & \text{if } f_1(t)\le 0\wedge f_2(t)\ge 0\\ \Big(0,\frac{H_3(t)\Delta_1(t)}{(H_1(t)\Delta_1(t)-Z_1\ln 2)H_4(t)}-\frac{1}{H_4(t)}\Big), & \text{if } f_1(t)<0\wedge f_4(t)>0\wedge f_2(t)>0\\ \Big(\frac{-b_1+\sqrt{b_1^2-4a_1c_1}}{2a_1},0\Big), & \text{if } f_3(t)<0\wedge f_1(t)>0\wedge f_5(t)>0\\ (P_1^*,P_2^*), & \text{if } f_1(t)>0\wedge f_6(t)<0\wedge f_7(t)<0\wedge f_5(t)>0\\ (0,\widehat{P}_2), & \text{if } f_1(t)>0\wedge f_4(t)\le 0\wedge f_2(t)>0\\ (\widehat{P}_1,0), & \text{if } f_3(t)\ge 0\wedge f_5(t)\le 0\\ \Big(\widehat{P}_1,\frac{-b_2+\sqrt{b_2^2-4a_2c_2}}{2a_2}\Big), & \text{if } f_3(t)<0\wedge f_6(t)>0\wedge f_5(t)>0\wedge f_7(t)<0\\ \Big(\frac{-b_3+\sqrt{b_3^2-4a_3c_3}}{2a_3},\widehat{P}_2\Big), & \text{if } f_7(t)>0\wedge f_4(t)>0\wedge f_6(t)<0\\ (\widehat{P}_1,\widehat{P}_2), & \text{if } f_6(t)\ge 0\wedge f_7(t)\ge 0\end{cases}\tag{41}$$

where $f_1(t)=\Delta_1(t)(H_1(t)-H_3(t))-Z_1\ln 2$ $\quad f_2(t)=Z_2$ $\quad f_3(t)=\Delta_1(t)(H_1(t)-H_3(t))-(1+\widehat{P}_1H_1(t))(1+\widehat{P}_1H_3)Z_1\ln 2$

$f_4(t)=\Delta_1(t)((1+\widehat{P}_2H_4(t))H_1(t)-H_3(t))-(1+\widehat{P}_2H_4(t))Z_1\ln 2$ $\quad f_5(t)=\Delta_1(t)-\dfrac{(1+\widehat{P}_1H_3(t))Z_1\ln 2}{\widehat{P}_1H_3(t)H_4(t)}$

$f_6(t)=\Delta_1(t)((1+\widehat{P}_2H_4(t))H_1(t)-H_3(t))-(1+\widehat{P}_1H_1(t))(1+\widehat{P}_1H_3(t)+\widehat{P}_2H_4(t))Z_2\ln 2$

$f_7(t)=\Delta_1(t)-\dfrac{(1+\widehat{P}_2H_4(t))(1+\widehat{P}_1H_3(t)+\widehat{P}_2H_4(t))Z_2\ln 2}{\widehat{P}_1H_3(t)H_4(t)}$

$a_1=H_1(t)H_3(t)$ $\quad b_1=H_1(t)+H_3(t)$ $\quad c_1=1-\dfrac{(H_1(t)-H_3(t))\Delta_1(t)}{Z_1\ln 2}$

$a_2=H_4^2(t)$ $\quad b_2=\widehat{P}_1H_3(t)H_4(t)+2H_4(t)$ $\quad c_2=1+\widehat{P}_1H_3(t)-\dfrac{\widehat{P}_2H_3(t)H_4(t)\Delta_1(t)}{Z_2\ln 2}$

$a_3=H_1(t)H_3(t)$ $\quad b_3=H_1(t)+H_3(t)+\widehat{P}_1H_1(t)H_4(t)$ $\quad c_3=1+\widehat{P}_2H_4(t)-\dfrac{(H_1(t)-H_3(t)+\widehat{P}_1H_3(t)H_4(t))\Delta_1(t)}{Z_1\ln 2}$ (42)

and (P_1^*,P_2^*) is the solution of the following equations

$$\begin{cases}f(P_1,P_2)=\Delta_1(t)(\frac{H_1(t)}{1+P_1H_1(t)}-\frac{H_3(t)}{1+P_2H_4(t)+P_1H_3(t)})-Z_1\ln 2=0,\\ f(P_1,P_2)=\Delta_1(t)(\frac{H_3(t)}{1+P_2H_3(t)}-\frac{H_3(t)}{1+P_1H_3(t)+P_2H_4(t)})-Z_2\ln 2=0.\end{cases}\tag{43}$$

$A_1,A_2,B_1,B_2,C_1,C_2,D_1,D_2$ in Fig. 2 are given as below

$$\begin{cases}A_1=\frac{(1+\widehat{P}_2H_4(t))\ln 2}{(1+\widehat{P}_2H_4(t))H_1(t)-H_3(t)}, A_2=\frac{(1+\widehat{P}_2H_4(t))(1+\widehat{P}_1H_3(t)+\widehat{P}_2H_4(t))\ln 2}{(1+\widehat{P}_2H_4(t))H_1(t)-H_3(t)},\\ B_1=\frac{(1+\widehat{P}_1H_3(t))Z_2\ln 2}{1+\widehat{P}_1H_3(t)H_4(t)}, \quad B_2=\frac{(1+\widehat{P}_1H_3(t))(1+\widehat{P}_1H_3(t)+\widehat{P}_2H_4(t))Z_2\ln 2}{1+\widehat{P}_1H_3(t)H_4(t)},\\ C_1=\big(\frac{Z_2\ln 2}{H_1(t)-H_3(t)},Z_2\big), \quad C_2=\big(\frac{(1+\widehat{P}_1H_3(t))Z_2\ln 2}{1+\widehat{P}_1H_3(t)H_4(t)},\frac{\widehat{P}_1H_3(t)H_4(t)Z_2}{(1+\widehat{P}_1H_3(t)H_4(t))\ln 2}\big),\\ D_1=\big(\frac{(1+\widehat{P}_2H_4(t))Z_2\ln 2}{(1+\widehat{P}_2H_4)H_1(t)Z_2\ln 2},2Z_2\big),\\ D_2=\frac{(1+\widehat{P}_1H_3(t))((1+\widehat{P}_2H_4(t))H_1(t)+\widehat{P}_1H_3(t))Z_2\ln 2}{1+\widehat{P}_1H_3(t)H_4(t)}.\end{cases}$$

By using the KKT conditions, the optimal power allocation and the secrecy rate allocation can be derived in *Lemma* 3.

Lemma 3: In the broadcast transmission mode, the optimal power allocation $(P_{r1}(t),P_{r2}(t))$ at the relay is presented in (47).

The optimal secrecy rate is given below:

$$R_{r1}^{sec}(t)=\min\{C_{r1}^{sec}(t),Q_2(t-1)\}.\tag{49}$$

$$R_{r2}^{sec}(t)=\min\{C_{r2}^{sec}(t),Q_1(t-1)\},\tag{50}$$

$$C_{r1}^{sec}(t)=\Big[\log_2\Big(1+P_{r1}(t)H_1(t)\Big)-\log_2\Big(1+\frac{P_{r1}(t)H_r(t)}{1+P_{r2}(t)H_r(t)}\Big)\Big]^+,\tag{51}$$

$$C_{r2}^{sec}(t)=\Big[\log_2\Big(1+P_{r2}(t)H_2(t)\Big)-\log_2\Big(1+\frac{P_{r2}(t)H_r(t)}{1+P_{r1}(t)H_r(t)}\Big)\Big]^+.\tag{52}$$

The optimal power allocation in the broadcast transmission mode can be illustrated in Fig. 3. Combined with (47), when

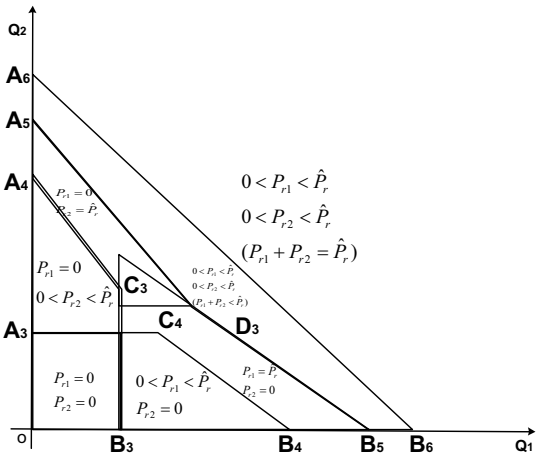


Fig. 3. The optimal transmit power allocation in broadcast transmission mode.

$$(P_{r1}(t),P_{r2}(t))=\begin{cases}(0,0), & \text{if } g_1(t)\geq 0\wedge g_2(t)\geq 0\\ (0,\widehat{P}_r), & \text{if } g_3(t)\leq 0\wedge g_4(t)\geq 0\wedge g_7(t)>0\wedge g_{10}(t)<0\\ (\widehat{P}_r,0), & \text{if } g_5(t)\leq 0\wedge g_6(t)\geq 0\wedge g_8(t)>0\wedge g_9(t)<0\\ \Big(0,\frac{-b_4+\sqrt{b_4^2-4a_4c_4}}{2a_4}\Big), & \text{if } g_1(t)\geq 0\wedge g_3(t)>0\wedge g_7(t)\leq 0\\ \Big(\frac{-b_5+\sqrt{b_5^2-4a_5c_5}}{2a_5},0\Big), & \text{if } g_2(t)\geq 0\wedge g_5(t)>0\wedge g_8(t)\leq 0\\ \Big(\frac{-b_6+\sqrt{b_6^2-4a_6c_6}}{2a_6},\frac{-b_7+\sqrt{b_7^2-4a_7c_7}}{2a_7}\Big)(P_{r1}(t)+P_{r2}(t)=\widehat{P}_r), & \text{if } g_9(t)\geq 0\wedge g_{10}(t)\geq 0\wedge g_{11}(t)\leq 0\\ (P_{r1}^*,P_{r2}^*)(P_{r1}(t)+P_{r2}(t)<\widehat{P}_r)), & \text{otherwise.}\end{cases} \tag{47}$$

where $g_1(t)=\psi(\phi-E(t))T\ln 2-Q_2(t)(H_1(t)-H_r(t)),\qquad g_2(t)=\psi(\phi-E(t))T\ln 2-Q_1(t)(H_2(t)-H_r(t)),$

$$g_3(t)=\psi(\phi-E(t))T\ln 2-Q_1(t)\Big(\frac{H_2(t)}{1+\widehat{P}_rH_2(t)}-\frac{H_r(t)}{1+\widehat{P}_rH_r(t)}\Big),\ g_4(t)=Q_1(t)\Big(\frac{H_2(t)}{1+\widehat{P}_rH_2(t)}-H_r(t)\Big)-Q_2(t)\Big(H_1(t)-\frac{H_r(t)}{1+\widehat{P}_rH_r(t)}\Big),$$

$$g_5(t)=\psi(\phi-E(t))T\ln 2-Q_2(t)\Big(\frac{H_1(t)}{1+\widehat{P}_rH_1(t)}-\frac{H_r(t)}{1+\widehat{P}_rH_r(t)}\Big),\ g_6(t)=Q_2(t)\Big(\frac{H_1(t)}{1+\widehat{P}_rH_1(t)}-H_r(t)\Big)-Q_1(t)\Big(H_2(t)-\frac{H_r(t)}{1+\widehat{P}_rH_r(t)}\Big),$$

$$g_7(t)=\psi(\phi-E(t))T\ln 2-\frac{Q_2(t)(H_1(t)-H_r(t))+\widehat{P}_rH_r(t)(Q_1(t)H_r(t)+Q_2(t)H_1(t))}{1+\widehat{P}_rH_r(t)},$$

$$g_8(t)=\psi(\phi-E(t))T\ln 2-\frac{Q_1(t)(H_2(t)-H_r(t))+\widehat{P}_rH_r(t)(Q_2(t)H_r(t)+Q_1(t)H_2(t))}{1+\widehat{P}_rH_r(t)},$$

$$g_9(t)=\psi(\phi-E(t))T\ln 2-\frac{H_r(t)(Q_1(t)+Q_2(t))(\widehat{P}_rH_1(t)H_r(t)-H_r(t))}{(H_1(t)+H_r(t))(1+\widehat{P}_rH_r(t))},$$

$$g_{10}(t)=\psi(\phi-E(t))T\ln 2-\frac{H_r(t)(Q_1(t)+Q_2(t))(\widehat{P}_rH_2(t)H_r(t)-H_r(t))}{(H_2(t)+H_r(t))(1+\widehat{P}_rH_r(t))},$$

$$g_{11}(t)=\psi(\phi-E(t))T\ln 2-\frac{H_r(t)(Q_1(t)(H_1(t)+H_r(t))+Q_2(t)(H_2(t)+H_r(t)))(\widehat{P}_rH_1(t)H_r(t)-H_r(t))}{(H_1(t)+H_r(t))(H_2(t)+H_r(t))(1+\widehat{P}_rH_r(t))},$$

$$a_4=H_2(t)H_r(t)\psi(\phi-E(t))T\ln 2,\quad b_4=\psi(\phi-E(t))(H_2(t)+H_r(t))T\ln 2,\quad c_4=\psi(\phi-E(t))T\ln 2-Q_1(t)(H_2(t)-H_r(t)),$$

$$a_5=H_1(t)H_r(t)\psi(\phi-E(t))T\ln 2,\quad b_5=\psi(\phi-E(t))(H_1(t)+H_r(t))T\ln 2,\quad c_5=\psi(\phi-E(t))T\ln 2-Q_2(t)(H_1(t)-H_r(t)),$$

$$a_6=H_1(t)H_r(t)(1+\widehat{P}_rH_r(t))\psi(\phi-E(t))T\ln 2+H_1(t)(H_r(t))^2(Q_1(t)+Q_2(t)),$$

$$b_6=(H_1(t)+H_r(t))(1+\widehat{P}_rH_r(t))\psi(\phi-E(t))T\ln 2-H_r(t)(Q_1(t)+Q_2(t))(\widehat{P}_rH_1(t)H_r(t)-H_r(t)),$$

$$c_6=(1+\widehat{P}_rH_r(t))\psi(\phi-E(t))T\ln 2-\widehat{P}_rH_r(t)(Q_1(t)H_r(t)+Q_2(t)H_1(t))+Q_2(t)(H_1(t)-H_r(t)),$$

$$a_7=H_2(t)H_r(t)(1+\widehat{P}_rH_r(t))\psi(\phi-E(t))T\ln 2+H_2(t)(H_r(t))^2(Q_1(t)+Q_2(t)),$$

$$b_7=(H_2(t)+H_r(t))(1+\widehat{P}_rH_r(t))\psi(\phi-E(t))T\ln 2-H_r(t)(Q_1(t)+Q_2(t))(\widehat{P}_rH_2(t)H_r(t)-H_r(t)),$$

$$c_7=(1+\widehat{P}_rH_r(t))\psi(\phi-E(t))T\ln 2-\widehat{P}_rH_r(t)(Q_2(t)H_r(t)+Q_1(t)H_2(t))+Q_1(t)(H_2(t)-H_r(t)),$$

and (P_{r1}^*,P_{r2}^*) is the solution of the following equations

$$\begin{cases}f(P_{r1},P_{r2})=\psi(\phi-E(t))T\ln 2-Q_1(t)(\frac{H_r(t)}{1+P_{r1}H_r(t)}-\frac{H_r(t)}{1+P_{r1}H_r(t)+P_{r2}H_r(t)})-Q_2(t)(\frac{H_1(t)}{1+P_{r1}H_1(t)}-\frac{H_r(t)}{1+P_{r1}H_r(t)+P_{r2}H_r(t)})=0,\\ f(P_{r1},P_{r2})=\psi(\phi-E(t))T\ln 2-Q_1(t)(\frac{H_2(t)}{1+P_{r2}H_2(t)}-\frac{H_r(t)}{1+P_{r1}H_r(t)+P_{r2}H_r(t)})-Q_2(t)(\frac{H_r(t)}{1+P_{r2}H_r(t)}-\frac{H_r(t)}{1+P_{r1}H_r(t)+P_{r2}H_r(t)})=0.\end{cases} \tag{48}$$

$A_3,A_4,A_5,A_6,B_3,B_4,B_5,B_6,C_3,C_4,D_3$ in Fig. 3 are given as below

$$\begin{cases}A_3=\frac{\psi(\phi-E(t))T\ln 2}{H_1(t)-H_r(t)}, & A_4=\frac{\psi(\phi-E(t))(1+\widehat{P}_rH_r(t))T\ln 2}{P_r(H_r(t))^2},\\ A_5=\frac{\psi(\phi-E(t))(1+\widehat{P}_rH_2(t))(1+\widehat{P}_rH_r(t))T\ln 2}{H_1(t)-H_r(t)}, & A_6=\frac{\psi(\phi-E(t))(1+\widehat{P}_rH_r(t))(H_1(t)+H_r(t))T\ln 2}{P_rH_1(t)H_r(t)-H_r(t)},\\ B_3=\frac{\psi(\phi-E(t))T\ln 2}{H_2(t)-H_r(t)}, & B_4=\frac{\psi(\phi-E(t))(1+\widehat{P}_rH_r(t))T\ln 2}{P_r(H_r(t))^2},\\ B_5=\frac{\psi(\phi-E(t))(1+\widehat{P}_rH_1(t))(1+\widehat{P}_rH_r(t))T\ln 2}{H_2(t)-H_r(t)}, & B_6=\frac{\psi(\phi-E(t))(1+\widehat{P}_rH_r(t))(H_2(t)+H_r(t))T\ln 2}{P_rH_2(t)H_r(t)-H_r(t)},\\ C_3=\frac{\psi(\phi-E(t))(1+\widehat{P}_r(H_1(t)-H_r(t)))T\ln 2}{P_rH_r(t)(H_1(t)-H_r(t))}, & C_4=\frac{\psi(\phi-E(t))(1+\widehat{P}_r(H_2(t)-H_r(t)))T\ln 2}{P_rH_r(t)(H_2(t)-H_r(t))},\\ D_3=\big(\frac{\psi(\phi-E(t))(1+\widehat{P}_rH_r(t))T\ln 2}{\widehat{P}_rH_r(t)+H_2(t)-H_r(t)},\frac{\psi(\phi-E(t))(1+\widehat{P}_rH_r(t))T\ln 2}{\widehat{P}_rH_r(t)+H_1(t)-H_r(t)}\big).\end{cases}$$

both data queue sizes $Q_1(t)$ and $Q_2(t)$ get larger, the transmit power at relay will be larger.

Based on the above analysis, the optimal power allocation and the secrecy rate allocation can be obtained according to the optimization problem in the corresponding transmission mode. Therefore, the optimal mode selection can be presented in *Lemma* 4.

Lemma 4: The optimal mode selection is to choose the transmission mode with the minimum scheduling cost, *i.e.,*

$$q_i^*(t)=\begin{cases}1, & \text{if } \Omega_m(t)=\arg\min\limits_{i=1,2,3,4}\Omega_i(t),\\ 0, & \text{otherwise,}\end{cases} \tag{53}$$

where the scheduling costs $\Omega_1(t)$, $\Omega_2(t)$, $\Omega_3(t)$, and $\Omega_4(t)$ stand for the sum of the weighted power consumption and the secure transmission rate, which are given as follows:

$$\Omega_1(t)=-\psi(\phi-E(t))E_h(t)+Z_1(t)P_1(t)+Z_2(t)P_2(t), \tag{54a}$$
$$\Omega_2(t)=-\Delta_1(t)R_{1r}^{sec}(t)+Z_1(t)P_1(t)+Z_2(t)P_2(t), \tag{54b}$$
$$\Omega_3(t)=-\Delta_2(t)R_{2r}^{sec}(t)+Z_1(t)P_1(t)+Z_2(t)P_2(t), \tag{54c}$$
$$\Omega_4(t)=\psi(\phi-E(t))P_r(t)T-Q_1(t)R_{r2}^{sec}(t)-Q_2(t)R_{r1}^{sec}(t). \tag{54d}$$

From the above mode selection policy, the larger data buffer queue length of $Q_1(t)$ is expected when the mode $\mathcal{M}_2$ is activated, which leads to an increase in $\Omega_2(t)$ and a decrease in $\Omega_4(t)$, such that the security-aware adaptive transmission scheme will prefer to choosing the mode $\mathcal{M}_4$. Similarly, the data queue size of $Q_2(t)$ will become larger when the mode $\mathcal{M}_3$ is selected, and the transmission mode $\mathcal{M}_4$ will be selected with high probability. The data buffer queue size and the energy storage size will be decreased when the mode $\mathcal{M}_4$ is selected, such that the security-aware adaptive transmission scheme will prefer to choosing the transmission mode either $\mathcal{M}_2/\mathcal{M}_3$ or the energy-harvesting mode $\mathcal{M}_1$. Therefore, the security-aware adaptive transmission scheme can guarantee the stability of the data buffers of $Q_1(t), Q_2(t)$ and the energy storage.

C. Performance Analysis

In this subsection, the performance of the proposed security-aware-adaptive policy scheme is presented in *Theorem* 1, which analyzes the upper bound of the weighted long-term average secure sum-rate and the average data queue length.

Theorem 1: For any $V>0$, $\epsilon>0$, all queues are stable, and the security transmission rate constraints are guaranteed. Meanwhile, the average secure sum-rate and the average data buffer queue length satisfy the following equations:

$$R_{sum}^*-\tfrac{B}{V}\le\lim_{N\to\infty}\tfrac{1}{N}\sum_{t=0}^{N-1}\mathbb{E}\big[R_{sum}(t)\big]\le R_{sum}^*, \tag{55}$$

$$\lim_{N\to\infty}\tfrac{1}{N}\sum_{t=0}^{N-1}\mathbb{E}\big[Q_1(t)+Q_2(t)\big]\le\tfrac{B+V[R_{sum}^*-\Psi(\epsilon)]}{\epsilon}, \tag{56}$$

where R_{sum}^* is the theoretically optimal weighted long-term average secure sum-rate, and $\Psi(\epsilon)$ is less than R_{sum}^*.

Proof: See Appendix B.

Theorem 1 indicates that the average queue length is linearly proportional to V, and the achieved secure sum-rate gap between $R_{sum}(t)$ and R_{sum}^* is inversely proportional to V, which implies a tradeoff of $[O(\frac{1}{V}), O(V)]$ between the achieved secrecy rates and the length of buffer queue.

IV. Numerical Analysis

In this section, the performance of the proposed energy-harvesting-based buffer-aided secure two-way relaying (TWR) scheduling scheme through the Monte-Carlo simulations is evaluated. In all simulations, unless otherwise stated, the path loss exponent is set to $m=2.7$, the noise variance of all nodes are $\sigma^2=-90$ dBm, and the energy conversion efficiency $\eta=0.5$. Meanwhile, the average transmit power at $U_i,(i=1,2)$ is $\overline{P}_i^{\max}=30$ dBm, and the peak transmit power at U_i is $\widehat{P}_i=3\overline{P}_i^{\max}$. The peak transmit power at relay is set as $\widehat{P}_r=\frac{E(t)}{T}$, which guarantees that the consumed energy of the relay can not exceed the energy stored in the energy storage in any time slot. Unless otherwise stated, the distance between U_1 and U_2 is equal to 10 m, namely, $d_1+d_2=10$ m, and $d_r=10$ m. All simulation results are obtained from one million time slots.

A. Benchmark Scheme

Because there is no existing EH-based secure two-way buffer-aided relaying network design for fair comparison, in order to highlight the influence of the data buffer and the energy storage on the mechanism design and the realized security transmission performance, a benchmark scheme is considered, where the two-way relaying is not provisioned with data buffers and energy storage. In the benchmark scheme, each time slot T is sub-divided into four sub-slots of αT, $\frac{(1-\alpha)T}{3}$, $\frac{(1-\alpha)T}{3}$ and $\frac{(1-\alpha)T}{3}$ as well, where $\alpha\in(0,1)$ is the time slot allocation factor. The relay first harvests energy in the first αT sub-slots from both users and then uses the collected energy for information transmission immediately, namely, *Harvest-Use* energy management policy is assumed. The remaining three sub-slots are utilized for the wireless information transmission from U_1 to the relay, U_2 to the relay, and the relay to both users, namely, transmission modes $\mathcal{M}_2, \mathcal{M}_3$, and $\mathcal{M}_4$, respectively. Since no data buffers are assumed at the relay, the relay must firstly decode the data from two users and then immediately forwards them to two users in the last $\frac{(1-\alpha)T}{3}$ sub-slots. Let E_1 and E_2 denote the total energy consumption at U_1 and U_2. Hence, the transmit power at U_i is $P_i=\frac{3E_i}{(\alpha+2)T}$. The harvested energy in the energy-harvesting phase is $E_h=\frac{3\alpha\eta(E_1|h_1|^2d_2^m+E_2|h_1|^2d_1^m)}{(\alpha+2)d_1^m d_2^m}$. In the modes $\mathcal{M}_2$ and $\mathcal{M}_3$, the achievable secrecy rate must satisfy the capacity limit. In the broadcast mode, the average transmit power of relay is $P_r=P_{r1}+P_{r2}=\frac{9\alpha\eta(E_1|h_1|^2d_2^m+E_2|h_2|^2d_1^m)}{(1-\alpha)(\alpha+2)d_1^m d_2^m T}$. Denote R_{12} and R_{21} as the secure transmission rate from U_1 to U_2 and that from U_2 to U_1. For the benchmark scheme, the achievable secrecy rate maximization problem can be formulated as follows:

$$\begin{aligned}
&\min_{R_{12},R_{21},\alpha,P_{r1},P_{r2}} -\theta R_{12}^{sec}-(1-\theta)R_{21}^{sec}\\
\text{s.t.}\quad & R_{12}^{sec}\le\tfrac{1-\alpha}{3}\Big[\log_2\Big(1+P_1H_1\Big)-\log_2\Big(1+\frac{P_1H_3}{1+P_2H_4}\Big)\Big]^+,\\
& R_{21}^{sec}\le\tfrac{1-\alpha}{3}\Big[\log_2\Big(1+P_2H_2\Big)-\log_2\Big(1+\frac{P_2H_4}{1+P_1H_3}\Big)\Big]^+,\\
& R_{21}^{sec}\le\tfrac{1-\alpha}{3}\Big[\log_2\Big(1+P_{r1}H_1\Big)-\log_2\Big(1+\frac{P_{r1}H_r}{1+P_{r2}H_r}\Big)\Big]^+,\\
& R_{12}^{sec}\le\tfrac{1-\alpha}{3}\Big[\log_2\Big(1+P_{r2}H_2\Big)-\log_2\Big(1+\frac{P_{r2}H_r}{1+P_{r1}H_r}\Big)\Big]^+,\\
& P_{r1}+P_{r2}\le P_r,\\
& 0<\alpha<1,
\end{aligned}$$

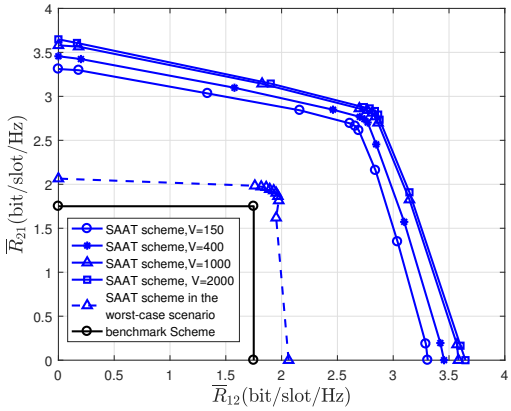


Fig. 4. The achievable average secrecy rate region, $P_1^{\max} = P_2^{\max} = 30$ dBm, $d_1 = d_2 = 5$ m, $d_x = 5$ m and $d_r = 10$ m.

where the first and second constraints correspond to the secure transmission rate limit when U_1 and U_2 transmit data to the relay, respectively. Similarly, the third and fourth constraints represent the secrecy rate limits when the relay broadcasts data to U_1 and U_2 simultaneously. The fifth constraint stands for the energy consumption constraint at the relay, and the last constraint indicates the time allocation policy. Since the first four constraints do not specify convex set, the problem is thus non-convex. One may resort to numerical solution by using the particle swarm optimization (PSO) algorithm [45].

Let us consider a worst-case scenario, where the eavesdropper U_e can eliminate the AN interference by using the successive interference cancellation [43] in the broadcast mode. In this worst-case scenario, $C_{r1}^{sec}(t)$ and $C_{r2}^{sec}(t)$ can be rewritten as follows:

$$C_{r1}^{sec}(t) = \left[\log_2\left(1 + P_{r1}(t)H_1(t)\right) - \log_2\left(1 + P_{r1}(t)H_r(t)\right)\right]^+, \tag{57}$$

$$C_{r2}^{sec}(t) = \left[\log_2\left(1 + P_{r2}(t)H_2(t)\right) - \log_2\left(1 + P_{r2}(t)H_r(t)\right)\right]^+. \tag{58}$$

Meanwhile, both data buffers and energy storage will be updated as below

$$Q_1(t) = Q_1(t-1) - q_4(t)C_{r2}^{sec}(t), \tag{59}$$

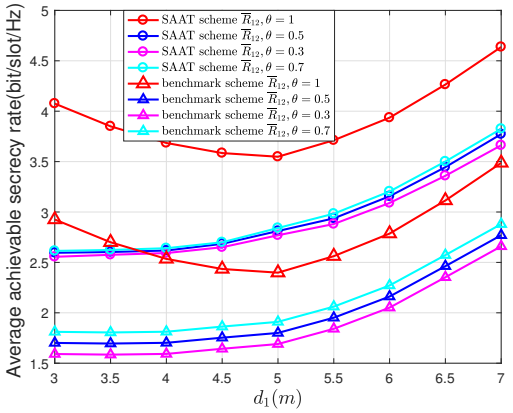
$$Q_2(t) = Q_2(t-1) - q_4(t)C_{r1}^{sec}(t), \tag{60}$$

$$E(t) = E(t-1) - q_4(t)P_r(t)T. \tag{61}$$

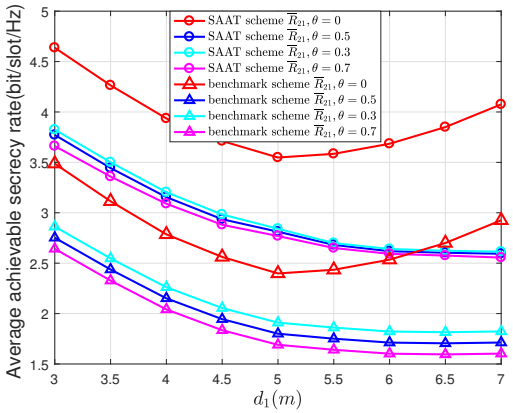
Based on (57)-(61), a similar analysis in Section III can be applied to derive the secure sum-rate performance of the worst-case scenario, which will be included in the following performance evaluation as well. For brevity, it is referred as the security-aware adaptive transmission scheme in the worst-case scenario in the following discussion.

B. Performance Evaluation

The achievable secrecy rate regions of the proposed scheme and the benchmark scheme are presented in Fig. 4, where d_1 = d_2 = 5 m, d_x = 5 m, and d_r = 10 m are assumed. As shown in Fig. 4, the larger V will lead to a larger achievable secrecy rate region of the proposed scheme. One may readily observe that the achievable secrecy rate region of the security-aware adaptive transmission scheme (SAAT) is noticeably superior to



(a) The achievable average secrecy rate in different relay positions.

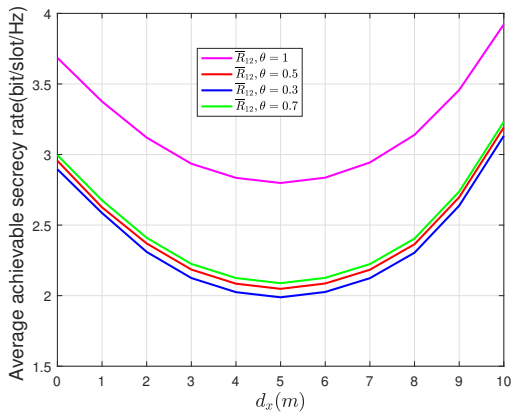


(b) The achievable average secrecy rate in different relay positions.

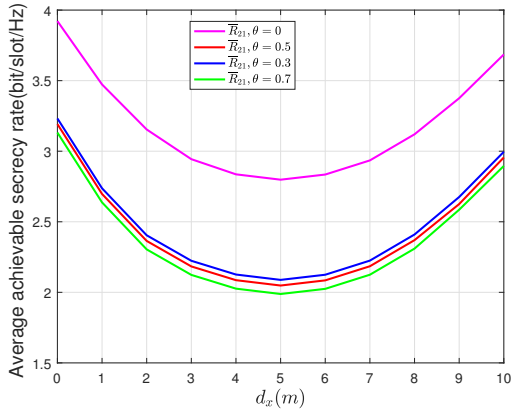
Fig. 5. The impact of different relay positions on the achievable average secrecy rate, $d_x = 5$ m, $d_r = 10$ m.

that of the benchmark scheme. Moreover, even the achievable rate region of the security-aware adaptive transmission scheme in the worst-case scenario is still better than the benchmark scheme, which confirms the benefit of deploying the data buffer and the energy storage at the relay.

In Fig. 5, the effect of the relay position (by varying d_1) on the achievable secrecy rate is illustrated, where $d_x = 5$ m and $d_r = 10$ m are assumed. When $\theta = 1$, the two-way relay network becomes one-way relay from U_1 to U_2. It can be observed from Fig. 5(a) that, with the increase of d_1 from 3 to 7 m, the achievable average secrecy rate $\overline{R}_{12}$ firstly decreases till the minimum value when $d_1 = 5$ m, and $\overline{R}_{12}$ then increases with a further increase in d_1 when $\theta = 1$. The numerical results in Fig. 5(a) can be interpreted as follows: Since the harvested energy $E_h(t)$ by the relay is limited by the large-scale fading of RF signals, which decays exponentially with the charging distance, the transmit power of the relay R is basically much less than that of the two users U_1 and U_2. Thus, the instantaneous secrecy rate from the relay to the users is generally smaller than the instantaneous secrecy rate from two users to the relay. Because of the fixed location of the eavesdropper, the distance between two users U_1, U_2 and the eavesdropper will be fixed. Hence, both the channel power gain $|h_i(t)|^2, i \in \{3, 4\}$ and the effective channel power gain



(a) The achievable average secrecy rate in different eavesdropper positions.



(b) The achievable average secrecy rate in different eavesdropper positions.

Fig. 6. The impact of different eavesdropper positions on the achievable average secrecy rate, $d_1 = d_2 = 5$ m, $d_r = 10$ m.

$H_i(t) = \frac{|h_i(t)|^2}{d_i^m \sigma^2}, i \in \{3, 4\}$ are also fixed. When the relay moves towards U_2 in the range of $[3, 5]$ m, an increase in $H_r(t)$ will become a critical factor that degrades the secrecy transmission rate $R_{r2}^{sec}(t)$ from R to U_2, which accounts for the decrease in the achieved security performance of $\overline{R}_{12}$ in the range of $[3, 5]$ m. Similarly, when the relay moves further towards U_2 in the range of $[5, 7]$ m, a decrease in $H_r(t)$ will be beneficial for the improved secrecy transmission rate $R_{r2}^{sec}(t)$ from R to U_2, which accounts for an increase in the achieved security performance of $\overline{R}_{12}$ in the range of $[5, 7]$ m. In a nutshell, when the eavesdropper location is fixed, because the transmit power of the relay is completely supplied via the energy harvesting from U_1 and U_2, the variations in $R \to U_E$ channel conditions will become a critical factor that affects the variations in the realized secrecy transmission rate of $\overline{R}_{12}$. Interestingly, a larger $\overline{R}_{12}$ can be realized when the relay is placed closer to U_2, because there will be a better effective channel power gain $H_2(t)$ of the second hop as well as the inferior eavesdropper channel power gain $H_r(t)$, which leads to a better secrecy transmission rate of the second hop when the relay is closer to U_2. Similarly, a symmetric secrecy transmission rate performance when $\theta = 0$ can be observed.

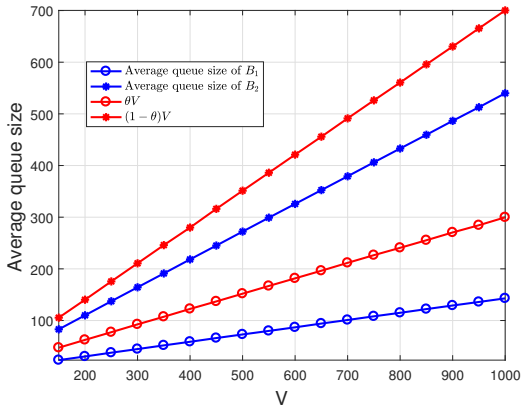


Fig. 7. The average queue size of B_1 and B_2 with different V, $d_1 = d_2 = 5$ m, $d_x = 5$ m. and $d_r = 10$ m.

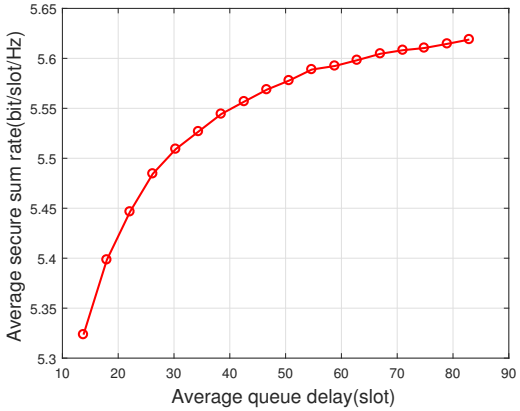
In addition to the two extreme cases of $\theta = 1$ and $\theta = 0$, the weighting coefficient θ can be regarded as a priority request by U_1 and U_2. A larger (smaller) θ indicates that U_1 has a higher (smaller) priority, and larger (smaller) average achievable secrecy rate $\overline{R}_{12}$ from U_1 to U_2 can be realized as expected. Meanwhile, one may also observe that, compared to the benchmark scheme, a notable secrecy transmission rate improvement can be realized by using the proposed security-aware adaptive transmission scheme in all settings.

In order to show the effect of the eavesdropper position (by varying d_x) on the achievable secrecy sum-rate, $d_1 = d_2 = 5$ m, and $d_r = 10$ m are assumed. Now, the position of U_E can be adjusted by adjusting the value of d_x. The achievable secrecy sum-rate can be illustrated in Fig. 6(a) and Fig. 6(b), respectively.In the same way, the variations in the relay to eavesdropper channel conditions dominate the variations in the achieved secrecy performance of $\overline{R}_{12}$ and $\overline{R}_{21}$. Meanwhile, the different choice of the weighting coefficient θ affects the realized secrecy transmission rate performance. A larger θ indicates that U_1 has a higher priority, thus a larger average achievable secrecy rate $\overline{R}_{12}$ from U_1 to U_2, as expected.

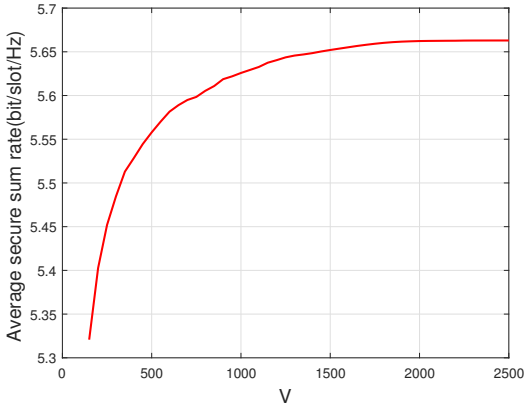
The relationship between the average queue size and V is illustrated in Fig. 7. The average queue size of the data buffers B_1 and B_2 is linearly proportional to V, and the average queue size in this case is less than the corresponding average queue size of θV and $(1-\theta)V$. The relationship between the average achievable secrecy rate and the average delay is shown in Fig. 8(a), where the average queueing delay can be calculated, according to Little's law, by dividing the average queue size with the average arrival rate, as follows:

$$T_{delay} = \lim_{N\to\infty} \frac{1}{N} \sum_{t=0}^{N-1} \frac{\mathbb{E}\big[Q_1(t) + Q_2(t)\big]}{\mathbb{E}\big[R_{sum}(t)\big]}. \tag{62}$$

As expected, when the proposed security-aware adaptive transmission scheme is employed, a larger average achievable secrecy sum-rate can be obtained when a larger delay is tolerated. The relationship between the average achievable secrecy sum-rate and V is shown in Fig. 8(b), where the achievable secrecy sum-rate by the proposed security-aware adaptive transmission scheme first increases with an increase of V until it tends to a stable value. In Theorem 1, the average



(a) The relationship between the average secrecy sum-rate and the average queue delay.

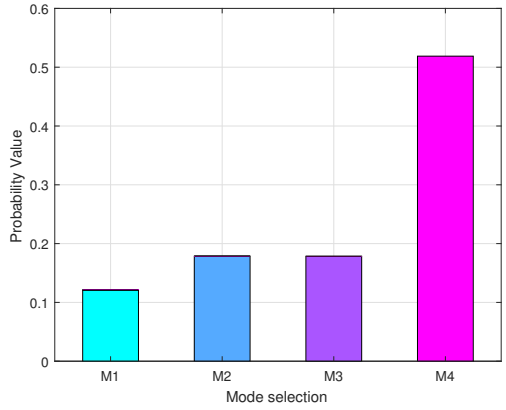


(b) The relationship between the secure average sum rate and V.

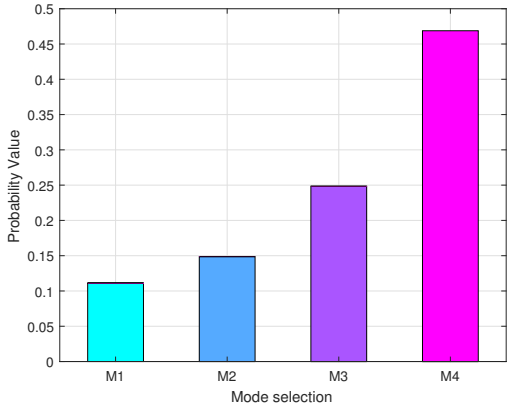
Fig. 8. The impact of V on the realized average secrecy sum-rate, $d_1 = d_2 = 5$ m, $d_x = 5$ m. and $d_r = 10$ m.

data queue size grows linearly with the control parameter V, and the achievable secrecy sum-rate gap between the theoretically optimal value and the proposed scheme is inversely proportional to V. Therefore, as long as the delay is tolerable, with a gradual increase in V, the achieved average secrecy sum-rate by using the proposed scheme can be arbitrarily close to the optimal value. In other words, the proposed security-aware adaptive transmission scheme provides an asymptotically optimal solution.

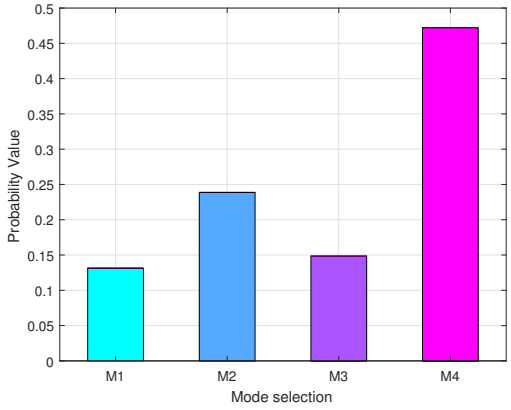
The probability of selecting the modes $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$, and $\mathcal{M}_4$ and the power consumption of U_1 and U_2 in the mode $\mathcal{M}_1, \mathcal{M}_2$, and $\mathcal{M}_3$ are illustrated in Figs. 9 and 10, respectively. Here the fixed eavesdropper location is assumed to be at $d_x = 5$ m, $d_r = 10$ m, and three different locations of the relay at $d_1 = d_2 = 5$ m, $d_1 = 3$ m, $d_2 = 7$ m, and $d_1 = 7$ m, $d_2 = 3$ m are considered. One can readily observe that, the broadcast mode $\mathcal{M}_4$ will be selected with the highest probability, as illustrated in Fig. 9. This can be explained by the fact that, the relay is an energy-constrained node, which has energy that is completely supplied by two users in the energy transmission mode $\mathcal{M}_1$. Basically, the collected energy by the relay is limited, because the large-scale fading of RF signals exponentially decays with distance.



(a) The probability of selecting each mode at $d_1 = d_2 = 5$ m, $\theta = 0.5$.



(b) The probability of selecting each mode at $d_1 = 3$ m, $d_2 = 7$ m, $\theta = 0.5$.

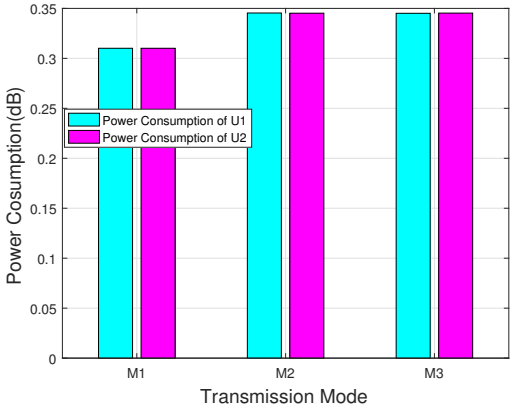


(c) The probability of selecting each mode at $d_1 = 7$ m,$d_2 = 3$ m, $\theta = 0.5$.

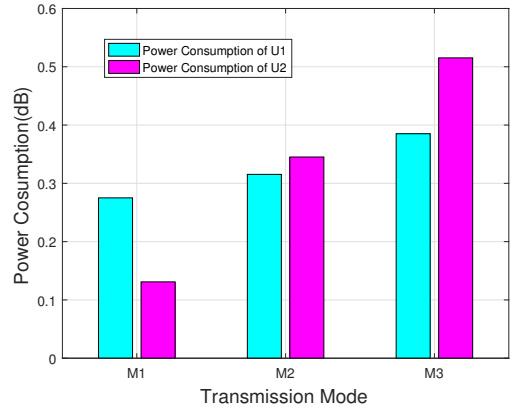
Fig. 9. The probability of selecting each mode in proposed scheme, $d_x = 5$ m, $d_r = 10$ m.

Hence, the transmission performance in the broadcast mode $\mathcal{M}_4$ will become the bottleneck of the whole system. In order to accomplish the two-way confidential message exchange, the relay needs more transmission opportunity.

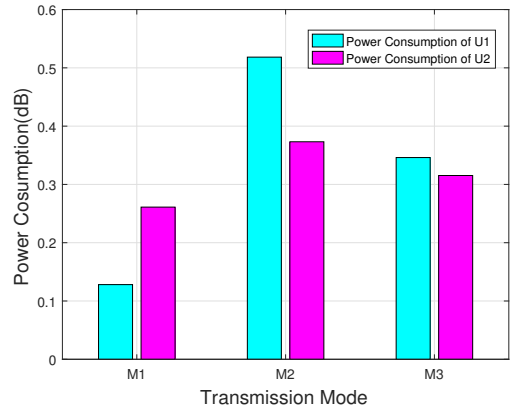
From Figs. 9(a) and 10(a), when $d_1 = d_2 = 5$ m, the power consumption of two users is equal and the probability of selecting the mode $\mathcal{M}_2$ and $\mathcal{M}_3$ is also equal. When the



(a) The transmit power consumption of U_1 and U_2 at $d_1 = d_2 = 5$ m, $\theta = 0.5$.



(b) The transmit power consumption of U_1 and U_2 at $d_1 = 3$m, $d_2 = 7$ m, $\theta = 0.5$.



(c) The transmit power consumption of U_1 and U_2 at $d_1 = 7$ m,$d_2 = 3$ m, $\theta = 0.5$.

Fig. 10. The transmit power consumption of U_1 and U_2 in different mode, $d_x = 5$ m, $d_r = 10$ m

relay is closer to U_1, *i.e.*, $d_1 = 3$ m, $d_2 = 7$ m, we can see from Fig. 9(b) that, the probability of selecting the mode $\mathcal{M}_3$ is higher than that of selecting the mode $\mathcal{M}_2$. This can be explicated by the fact that, when the relay is closer to U_1, $R_{1r}^{sec} > R_{r2}^{sec}$. The mode $\mathcal{M}_3$ will be activated with higher probability in order to guarantee the balance of the two-way

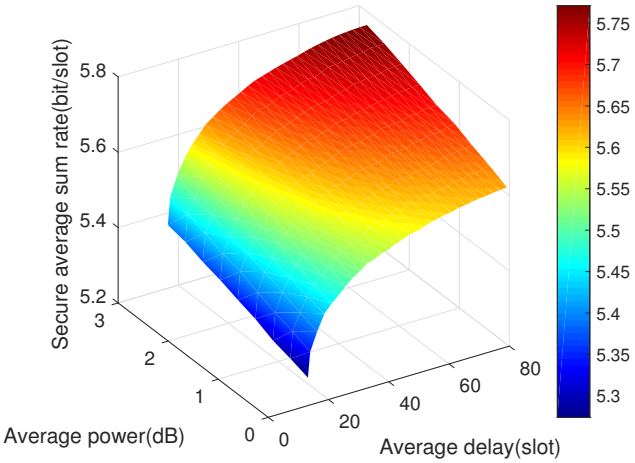


Fig. 11. The tradeoff of transmission delay, transmit power consumption and the secrecy sum-rate, $d_1 = d_2 = 5$ m, $d_x = 5$ m, $d_r = 10$ m.

confidential message exchange. On the other hand, since U_1 is closer to the relay, U_1 needs less energy to accomplish the confidential message transmission in the mode $\mathcal{M}_2$ and less energy to confuse the eavesdropper in the mode $\mathcal{M}_3$, but the relay tends to harvest more energy from U_1 in the mode $\mathcal{M}_1$. In this case, U_2 is farther from the relay and U_2 needs more energy to accomplish the confidential message transmission in the mode $\mathcal{M}_3$ and more energy to confuse the eavesdropper in the mode $\mathcal{M}_2$, but the relay tends to harvest less energy from U_2 in the mode $\mathcal{M}_1$, as illustrated in Fig. 10(b). As expected, symmetric phenomena can be observed in Fig. 10(c), where the relay is closer to U_2, *i.e.*, $d_1 = 7$ m, $d_2 = 3$ m.

The tradeoff among average transmission delay, average power consumption, and average achievable secrecy sum-rate of the proposed security-aware adaptive transmission scheme is illustrated in Fig. 11. When the relay is provisioned with data buffer and energy storage for the EH-based secure two-way relay network, not only a higher average transmit power consumption but also a larger tolerable transmission delay will lead to a larger average achievable secrecy sum-rate. Thus, a larger achievable secrecy sum-rate can be obtained for a predefined transmit power, or less power consumption is needed to achieve a target achievable secrecy sum-rate, when some increase in transmission delay is tolerable. This may provide useful guidance on the practical EH-based secure two-way buffer-aided relay network design.

V. Conclusions

In this paper, an EH-STWR network was studied, where two users exchanged confidential message with the assistance of one credible buffer-aided relay that harvested energy from two users. A secure bidirectional buffer-aided relaying scheme was proposed to realize the confidential message exchange between two users in the presence of a potential eavesdropper. A security-aware adaptive transmission scheme was proposed to jointly adapt transmission mode selection, power allocation, and rate allocation according to the underlying CSI,

BSI and ESI subject to average and peak transmit power constraints, data buffer and energy storage causality, as well as transmission mode constraints. Analysis results showed that, the average achievable secrecy sum-rate region can be significantly improved, and there exists an inherent trade-off among transmission delay, required transmit power consumption, and realized secure achievable sum-rate. Furthermore, the realized achievable security transmission performance is sensitive to the channel condition between the relay and the eavesdropper. The energy-harvesting-based secure two-way buffer-aided relay network provides an effective candidate to realize the energy sustainable secure two-way relaying design. When imperfections, such as the imperfect CSIs as well as the outdated CSIs, are taken into consideration, a robust security-aware adaptive transmission scheme that is capable of approaching the secrecy rate region derived in this paper will be left for exploration in our future work.

APPENDIX A
PROOF OF *Lemma* 1

According to the dynamic update expression of energy queue (24), it is worth noting that

$$\begin{aligned}&(\phi-\max\{E(t)+E_h(t)-q_4(t)P_r(t)T,0\})^2\\&\qquad\le(\phi-E(t)-E_h(t)+q_4(t)P_r(t)T)^2.\end{aligned}\tag{63}$$

By the similar operation to the dynamic update expressions of data buffer queue (25) and (26), we have

$$\begin{aligned}\Delta(\Theta(t))\le{}&B+\psi(\phi-E(t))\mathbb{E}\big[q_4(t)P_r(t)T-E_h(t)|\Theta(t)\big]\\&+\sum_{i=1}^{2}Z_i(t)\mathbb{E}\big[(q_1(t)+q_2(t)+q_3(t))P_i(t)-\overline{P}_i^{\max}|\Theta(t)\big]\\&+Q_1(t)\mathbb{E}\big[R_{1r}^{sec}(t)-R_{r2}^{sec}(t)|\Theta(t)\big]\\&+Q_2(T)\mathbb{E}\big[R_{2r}^{sec}(t)-R_{r1}^{sec}(t)|\Theta(t)\big],\end{aligned}\tag{64}$$

After adding the penalty item to both sides of the above inequality, the *Lemma* 1 can be derived.

APPENDIX B
PROOF OF *Theorem* 1

Assume that all the channel states are independent and identically distributed (i.i.d) at each time slot, so there exits a stationary randomized transmit power allocation, achievable secrecy rate allocation, and mode selection policy independent of data buffer states, energy buffer states and power consumption states, which satisfies

$$\mathbb{E}\big[R_{sum}(t)|\Theta(t)\big]=\mathbb{E}\big[R_{sum}(t)\big]=\Psi(\epsilon),\tag{65}$$

$$\mathbb{E}\big[q_4(t)P_r(t)T-E_h(t)|\Theta(t)\big]=\mathbb{E}\big[q_4(t)P_r(t)T-E_h(t)\big]\le-\epsilon,\tag{66}$$

$$\begin{aligned}&\mathbb{E}\big[(q_1(t)+q_2(t)+q_3(t))P_i(t)-\overline{P}_i^{\max}|\Theta(t)\big]\\&\quad=\mathbb{E}\big(q_1(t)+q_2(t)+q_3(t))P_i(t)-\overline{P}_i^{\max}\big]\le-\epsilon,\end{aligned}\tag{67}$$

$$\mathbb{E}\big[R_{ir}^{sec}(t)-R_{rj}^{sec}(t)|\Theta(t)\big]=\mathbb{E}\big[R_{ir}^{sec}(t)-R_{rj}^{sec}(t)\big]\le-\epsilon.\tag{68}$$

After substituting the above expressions into (34), it yields

$$\begin{aligned}&\Delta(\Theta(t))-V\mathbb{E}\big[R_{sum}(t)|\Theta(t)\big]\\&\qquad\le B-V\Psi(\epsilon)-\psi(\phi-E(t))\epsilon-\sum_{i=1}^{2}(Q_i(t)+Z_i(t))\epsilon.\end{aligned}\tag{69}$$

By using iterations of conditional expectations in (69), we have

$$\begin{aligned}&\mathbb{E}\big[L(\Theta(t+1))-L(\Theta(t))\big]-V\mathbb{E}\big[R_{sum}(t)\big]\\&\qquad\le B-V\Psi(\epsilon)-\psi(\phi-\mathbb{E}[E(t)])\epsilon-\sum_{i=1}^{2}\mathbb{E}\big[Q_i(t)+Z_i(t)\big]\epsilon.\end{aligned}\tag{70}$$

Dividing (70) with N and summing over each time slot, thus we have

$$\begin{aligned}&\frac{\mathbb{E}\big[L(\Theta(N))-L(\Theta(0))\big]}{N}-\frac{V}{N}\sum_{t=0}^{N-1}\mathbb{E}\big[R_{sum}(t)\big]\le B-V\Psi(\epsilon)\\&\qquad-\frac{\epsilon}{N}\sum_{t=0}^{N-1}(\psi(\phi-\mathbb{E}[E(t)])+\sum_{i=1}^{2}\mathbb{E}\big[Q_i(t)+Z_i(t)\big]).\end{aligned}\tag{71}$$

Based on the following inequalities as

$$\begin{cases}\lim\limits_{N\to\infty}\frac{1}{N}\sum\limits_{t=0}^{N-1}\mathbb{E}\big[R_{sum}(t)\big]\le R_{sum}^*,\\L\big(\Theta(N)\big)\ge0, L(\Theta(0))=0,\\Q_i(t)\ge0, Z_i(t)\ge0, \phi-E(t)\ge0\end{cases}$$

Taking a limit as $N\to\infty$ and $\Psi(\epsilon)\to R_{sum}^*$ as $\epsilon\to0$, we have

$$\frac{1}{N}\sum_{t=0}^{N-1}\mathbb{E}\big[Q_1(t)+Q_2(t)\big]\le\frac{B+V[R^*-\Psi(\epsilon)]}{\epsilon},\tag{72}$$

$$\Psi(\epsilon)-\frac{B}{V}\le\frac{1}{N}\sum_{t=0}^{N-1}\mathbb{E}\big[R_{sum}(t)\big].\tag{73}$$

Thus, the *Theorem* 1 is proved.

REFERENCES

[1] T. Karygiannis, and L. Owens, Wireless Network Security, *NIST Special Publication*, vol. 800, p. 48, Nov. 2002.

[2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[4] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[5] L. Lai, and H. E. Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Trans. Inform. Theory.*, vol. 54, no. 9, pp. 4005-4019, Sept. 2008.

[6] A. Mukherjee, and A. L. Swindlehurst, "Securing Multi-Antenna Two-way Relay Channels with Analog Network Coding against Eavesdroppers," in *Proc. IEEE 11th Int. Workshop Signal Process. Adv. Wireless Commun.*, Jun. 2010, pp. 1-5.

[7] X. He, and A. Yener, "The Role of an Untrusted Relay in Secret Communication," in *Proc. IEEE Int. Symp. Inf. Theory,* Toronto, Canda, pp. 2212-2216, Jul. 2008.

[8] E. Tekin, and A. Yener, "The general Gaussian Multiple-Access and Two-way Wiretap Channels: Achievable Rates and Cooperative Jamming," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

[9] J. Huang, and A. L. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[10] H. Long, W. Xiang, J. Wang, Y. Y. Zhang, and W. B. Wang, "Cooperative Jamming and Power Allocation with Untrusty Two-way Relay Nodes," *IET Commun.*, vol. 8, no. 13, pp. 2290-2297, Sept. 2014.

[11] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving Wireless Security for Bidirectional Communication Scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842-2848, Jul. 2012.

[12] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, "Security-Reliability Tradeoff Analysis of Artificial Noise Aided Two-way Opportunistic Relay Selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930-3941, May. 2017.

[13] X. Lan, Q. Chen, X. Tang, and L. Cai, "Achievable Rate Region of the Buffer-aided Two-way Energy Harvesting Relay Network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11127-11142, Nov. 2018.

[14] X. Lan, Y. Zhang, Q. Chen, and L. Cai, "Energy Efficient Buffer-aided Transmission Scheme in Wireless Powered Cooperative NOMA Relay Network," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1432-1447, 2020.

[15] X. Lan, Q. Chen, and L. Cai, "Buffer-aided Adaptive Wireless Powered Communication Network with Finite Energy Storage and Data Buffer," *IEEE Trans. Wireless Commun.*, vol.18, no. 12, pp. 5764-5779, Dec. 2019.

[16] Z. Tian, G. Chen, Y. Gong, Z. Chen, and J. A. Chambers, "Buffer-aided Max-Link Relay Selection in Amplify-and-Forward Cooperative Networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 553-565, Feb. 2015.

[17] B. Xia, Y. Fan, J. Thomphson, and H.V. Poor, "Buffering in a Three-node Relay Network," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4492-4496, Nov. 2008.

[18] A. E. Shafie, A. Sultan, and N. Al-Dhahir, "Physical-layer Security of a Buffer-aided Full-duplex Relaying System," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1856-1859, Sept. 2016.

[19] J. Huang, and A. L. Swindlehurst, "Buffer-aided Relaying for Two-hop Secure Communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152-164, Jan. 2015.

[20] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy Outage Analysis of Buffer-aided Multi-antenna Relay Systems without Eavesdroppers CSI," in *Proc. of IEEE ICC*, Paris, France, 2017, pp. 1-6.

[21] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Enhancing the PHY-layer Security of MIMO Buffer-aided Relay Networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 400-403, Aug. 2016.

[22] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio Relay Selection in Secure Buffer-aided Cooperative Wireless Networks," *IEEE Trans. Inf. Forensics Security,* vol. 9, no. 4, pp. 719-729, Apr. 2014.

[23] D. Wang, P. Ren, and J. Cheng, "Cooperative Secure Communication in Two-hop Buffer-Aided Networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 972-985, Mar. 2018.

[24] J. Wan, D. Qiao, H. Wang, and H. Qian, "Buffer-Aided Two-Hop Secure Communications with Power Control and Link Selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7635-7647, Nov 2018.

[25] X. Liao, Y. Zhang, Z. Wu, Y. Shen, X. Jiang, and H. Inamura, "On Security Delay Trade-off in Two-hop Wireless Networks with Buffer-aided Relay Selection," *IEEE Trans. Wireless Commun.,* vol. 17, no. 3, pp. 1893-1906, Mar. 2018.

[26] X. Zhou, R. Zhang, and C. K. Ho, "Wireless Information and Power Transfer: Architecture Design and Rate-Energy Tradeoff," *IEEE Trans. Commun.,* vol. 61, no. 11, pp. 4754-4767, Nov. 2012.

[27] G. Chen, P. Xiao, J. R. Kelly, B. Li, and R. Tafazolli, "Full-duplex Wireless-Powered Relay in Two Way Cooperative Networks," *IEEE Access*, vol. 5, pp. 1548-1558, Mar. 2017.

[28] R. Zhang, and C. K. Ho, "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989-2001, May. 2013.

[29] L. R. Varshney, "Transporting Information and Energy Simultaneously," in *Proc. of IEEE ISIT*, Toronto, ON, Canada, pp. 1612-1616, Jul. 2008.

[30] Z. Ding, I. Krikidis, B. Sharif, and H. V. Poor, "Wireless Information and Power Transfer in Cooperative Networks with Spatially Random Relays," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4440-4453, Aug. 2014.

[31] Y. Hu, C. Qiu, and Y. Chen, "Lyapunov-Optimized Two-Way Relay Networks With Stochastic Energy Harvesting," *IEEE Trans. Wireless Commun.*, vol. 17, no.9, pp. 6280-6292, Sept. 2018.

[32] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying Protocols for Wireless Energy Harvesting and Information Processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622-3636, Jul. 2013.

[33] L. Liu, R. Zhang, and K. C. Chua, "Wireless Information Transfer with Opportunistic Energy Harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288-300, Jan. 2013.

[34] F. Jameel, S. Wyne, and Z. Ding, "Secure Communications in Three-step Two-way Energy Harvesting DF Relaying," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 308-311, Feb. 2018.

[35] S. S. Kalamkar, A. Banerjee, "Secure Communication via a Wireless Energy Harvesting Untrusted Relay," *IEEE Trans. Veh. Technol.*, 2017, vol. 66, no. 3, pp. 2199-2213, Mar. 2017.

[36] H. Xing, K.-K. Wong, and A. Nallanathan, "Secure Wireless Energy Harvesting-Enabled AF-Relaying SWIPT Networks," *IEEE Int. Conf. Commun. (ICC)*, London, U.K., pp. 2307-2312, Jun. 2015.

[37] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical Layer Security with RF Energy Harvesting in AF Multi-antenna Relaying Networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025-3038, Jul. 2016,

[38] H. Xing, K.-K. Wong, Z. Chu, and A. Nallanathan, "To Harvest and Jam: A Paradigm of Self-Sustaining Friendly Jammers for Secure AF Relaying," *IEEE Trans. Signal Process*, vol. 63, no. 24, pp. 6616-6631, Dec. 2015.

[39] K. Lee, J.-P. Hong, H.-H. Choi, and T. Q. S. Quek, "Wireless-Powered Two-Way Relaying Protocols for Optimizing Physical Layer Security," *IEEE Trans. Inform. Forensics Security*, vol. 14, no. 1, pp. 162-174, Jan. 2019.

[40] Y. Liu, Q. Chen, X. Tang, and L. X. Cai, "On the Buffer Energy Aware Adaptive Relaying in Multiple Relay Networks," *IEEE Trans. Wireless Commun.,* vol. 16, no. 9, pp. 6248-6263, Sept. 2017.

[41] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical Layer Network Security in the Full-Duplex Relay System," *IEEE Trans. Inform. Forensics Security.*, vol. 10, no.3, pp. 574-583, Mar. 2015.

[42] A. E. Shafie, T. Q. Duong, and N. Al-Dhahir, "QoS-aware Enhanced Security for TDMA Transmissions from Buffered Source Nodes," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1051-1065, Feb. 2017.

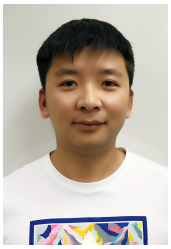
[43] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "MIMO Multi-user Secrecy Rate Analysis," in *IEEE ICC*, Sydney, NSW, Australia, pp. 1023-1028, Jun. 2014.

[44] V. Jamali, N. Zlatanov, A. Ikhlef, and R. Schobert, "Adaptive Mode Selection and Power Allocation in Bidirectional Buffer-aided Relay Networks," in *IEEE GLOBECOM*, Atlanta, GA, USA, pp. 1933-1938, Dec. 2013.

[45] J. Kennedy, Particle swarm optimization, in: *Encyclopedia of Machine Learning*, Springer, US, 2010, pp. 760-766.

[46] F. Gao, T. Cui, and A. Nallanathan, "Maximum likelihood channel estimation in decode-and-forward relay networks," in *Proc. IEEE Int. Symp. Inform. Theory*, Toronto, ON, Canada, pp. 1233-1237, Jul. 2008.

Yulong Nie received his M.S. degree with the department of electronic and communication engineering, Guangzhou University, Guangzhou, China, in 2020. His current research interests include buffer-aided physical layer security, wireless communication



Xiaolong Lan received the B. S. degree in mathematics and applied mathematics from Chengdu University of Technology and the Ph.D. degree in information and communication engineering from Southwest Jiaotong University, China, in 2012 and 2019, respectively. From 2017 to 2019, he was a visiting Ph.D. student with the University of Victoria, BC, Canada. He is currently an Associate Researcher with the College of Cybersecurity, Sichuan University, Chengdu, China. His current research interests include physical layer security, buffer-aided communication, energy-harvesting wireless communication, and mobile edge computing.

Yong Liu (Member, IEEE) received the Ph.D degree in information and communication engineering from the School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China, in 2019. He was a Visiting Stu-dent with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, USA, from October 2017 to April 2019. He has been an Assistant Professor with the School of Physics and Telecommunication Engineering, South China Normal University, Guangzhou, China, since 2019. His current research interests include green communication, buffer/cache-aided communication, massive MIMO, and wireless sensor networks. He was a recipient of the 2016 IEEE GLOBECOM Best Paper Award.

Qingchun Chen (SM'14) received his B.Sc degree and M.Sc degree with honor from Chongqing University, P.R. China, in 1994 and 1997, respectively. He received his Ph.D. degree from Southwest Jiaotong University, P.R. China in 2004. He was with Southwest Jiaotong University from 2004 to 2018, now he is a professor at Guangzhou University, Guangzhou, P.R. China. Dr. Qingchun Chen is the director of the Research Center of Intelligent Communication Engineering, Huangpu Research & Graduate School, Guangzhou University. Dr. Chen has authored and coauthored over 100 research papers, two book chapters and 40 patents. Dr. Chen received the 2016 IEEE GLOBECOM Best Paper Award. His research interest includes wireless communication, wireless network, information coding and signal processing.

Gaojie Chen (S'09 – M'12 – SM'18) received the B.Eng. and B.Ec. degrees in electrical information engineering and international economics and trade from Northwest University, China, in 2006, and the M.Sc. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Loughborough University, Loughborough, U.K., in 2008 and 2012, respectively. From 2008 to 2009, he was a Software Engineer with DT Mobile, Beijing, China. From 2012 to 2013, he was a Research Associate with the School of Electronic, Electrical and Systems Engineering, Loughborough University. He was a Research Fellow with 5GIC, Faculty of Engineering and Physical Sciences, University of Surrey, U.K., from 2014 to 2015. He was also a Research Associate with the Department of Engineering Science, University of Oxford, U.K., from 2015 to 2018. He is currently a Lecturer with the School of Engineering, University of Leicester, U.K. His current research interests include information theory, wireless communications, cooperative communications, cognitive radio, the Internet of Things, secrecy communications, and random geometric networks. He received the Exemplary Reviewer Certificates of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2018 and the IEEE TRANSACTIONS ON COMMUNICATIONS in 2019. He serves as an Associate Editor for the IEEE COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS LETTERS and *Electronics Letters* (IET).

Lisheng Fan received the bachelor and master degrees from Fudan University and Tsinghua University, China, in 2002 and 2005, respectively, both from the Department of Electronic Engineering. He received the Ph.D degree from the Department of Communications and Integrated Systems of Tokyo Institute of Technology, Japan, in 2008. He is now a Professor with GuangZhou University. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. Lisheng Fan has published many papers in international journals such as IEEE Transactions on Wireless Communications, IEEE Transactions on Communications, IEEE Transactions on Information Theory, as well as papers in conferences such as IEEE ICC, IEEE Globecom, and IEEE WCNC. He is a guest editor of EURASIP Journal on Wireless Communications and Networking, and served as the chair of Wireless Communications and Networking Symposium for Chinacom 2014. He has also served as a member of Technical Program Committees for IEEE conferences such as Globecom, ICC, WCNC, and VTC.

Dong Tang received the B.S. degree from the Nanhua University, Hengyang, China, in 1989, the M.S. degree from the Hunan University, Changsha, China, in 1999, and the Ph.D. degree in communications and information systems from Sun Yat-sen University, Guangzhou, in 2006. From 2014 to 2015, he was a Research Fellow with the University of California, Irvine, Irvine, U.S. He was an Associate Professor with the School of Electrical Engineering, Nanhua University, Hengyang, China, from 2005 to 2007. In 2007, he joined the Department of Electronics Engineering, Guangzhou University, Guangzhou, China, where he is currently a Professor. His main research interests include 5G/6G technologies, statistics and optimization for wireless communicationintelligent network system and green communications.