Secure Transmission Scheme Design for SWIPT in Buffer-aided Relay Networks

Juanjuan Ren*, Xianfu Lei*, Panagiotis D. Diamantoulakis*†, Qingchun Chen‡, and George K. Karagiannidis†
*School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China
†Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Thessaloniki, Greece
‡School of Mechanical and Electric Engineering, Guangzhou University, Guangzhou 510006, China
e-mails: juanjuanren@foxmail.com, xflei81@gmail.com, padiaman@ieee.org, geokarag@auth.gr, qingchunchen@foxmail.com

***Abstract*—In this paper, we investigate a secure relaying network with simultaneous wireless information and power transfer (SWIPT). It is assumed that Alice wants to send confidential information to Bob under the existence of a passive eavesdropper (Eve), while the relay is equipped with a data buffer and an energy storage device. More specifically, we aim at achieving higher secrecy throughput, while retaining the stability of the data and energy queues. To achieve this with acceptable complexity, we transform the original long-term stochastic optimization problem into a series of online subproblems using the framework of Lyapunov optimization. The proposed scheme shows that the optimal time switching factor is 0 or 1, which is different from the conventional secure relaying network with SWIPT. In addition, simulation results verify that the proposed scheme can improve the secrecy throughput compared with the baseline scheme.**

I. Introduction

Recently, physical layer security (PLS) which makes use of the randomness nature of wireless propagation channel to guarantee secure has received considerable attention. In general, higher secrecy rate can be achieved by increasing the rate of legitimate users and reducing the quality of eavesdropping channels by jamming. A case of special interest is the application of PLS in cooperative relaying networks [1]–[3]. For instance, in order to improve the security rate, a scenario where the helper acted as a relay or a jammer in a four-node cooperative network was studied in [1]. Moreover, optimal beamforming and power allocation have been considered as candidate solutions to improve the achievable secrecy rate in relaying networks by [3] and [2], respectively.

However, the relaying performance in the above works is bottlenecked by the link with the worst channel conditions. To this end, buffering-aided relaying is a promising solution [4], according to which the confidential messages can be firstly stored at the relay and retransmitted when the channel state conditions of the second hop are improved. The secrecy outage probability and secrecy throughput in buffer-aided secure half-duplex trust relay system were studied in [5]. In order to improve the security of the legitimate user, a hybrid half-duplex (HD)/full-duplex (FD) relaying scheme was proposed in [6]. Moreover, in [7] power allocation and link selection in buffer-aided secure communication were considered.

Another challenging issue in cooperative networks is how to prolong the lifetime of energy-constrained nodes. To this direction, simultaneous wireless information and power transfer (SWIPT) which harvests energy and receives data from the same radio frequency (RF) signal is a useful technology. It needs to be noted that security is an important challenge when SWIPT is used, mainly due to the stochastic nature of the harvested energy and its limited availability, which reduces the achievable rate of the legitimate user. To this end, several schemes had been proposed. For instance, time switching and beamforming design in SWIPT full-duplex secure relay network was studied in [8]. [9] studied an energy-harvesting buffer-aided secure relay network and proposed two secure cooperative protocols.

However, the design of scheduling schemes to improve the secrecy performance in relaying networks with SWIPT, taking advantage of the data buffer and energy storage, has not been considered yet in existing literature. To this end, we first formulate an optimization problem which maximizes the long-term average secrecy throughput, considering the stability of the queues. Next, in order to solve this multivariable stochastic optimization problem, we propose an online adaptive time and power allocation scheme based on the Lyapunov optimization theory. In addition, we mathematically prove that each time slot should be used either for energy transfer or information transmission. Finally, simulations results are provided to validate the effectiveness of the proposed scheme.

II. System Model

As illustrated in Fig.1, Alice transmits confidential information to Bob via a trust randomize-and-forward relay (R), under the existence of a passive eavesdropper (Eve) in the network. R is an energy-constrained node that operates by solely using the harvested energy from the RF signal transmitted by Alice. When the existence of a data buffer and an energy storage device is assumed, $Q(t)$ and $E_{\mathrm{r}}(t)$ are used to denote the amount of data and energy that is available in the corresponding data and energy buffers, respectively, in the t-th time slot. We also assume that Eve eavesdrops both the links of Alice-R and R-Bob. Each node is equipped with a single antenna and there's no direct link between Alice and Bob due to the deep fading. Also, time-division duplex (TDD) is assumed, i.e., the relay cannot receive and transmit information simultaneously.

A. Channel Model

All channels $\tilde{h}_{jk}(t)$ between nodes j and k are assumed to undergo large-scale fading with path loss parameter α and small-

978-1-7281-5207-3/20/$31.00 ©2020 IEEE

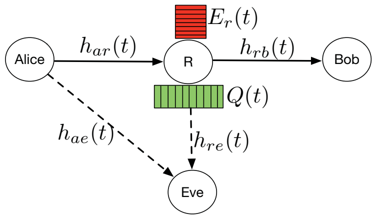


Fig. 1: Network model

scale block Rayleigh fading, i.e., $\widetilde{h}_{jk}(t) = h_{jk}(t)/\sqrt{d_{jk}^{\alpha}}$, $jk \in \{\text{ar, ae, rb, re}\}$, where $h_{jk}(t)$ and d_{jk} denote the small-scale fading channel coefficient of all links at time slot t and the transmission distance, respectively. Also, the channel gains remain constant during a time slot, but change independently between consecutive time slots. A centralized scheduling scheme is assumed, according to which a central control node makes control decisions, taking into account the data and energy buffer states, as well as the channel state information (CSI) of all involved links. It is further assumed that Eve is a legitimate user that also uses the relay to transmit information [10]. Thus, it is reasonable to assume that CSI for all links is perfectly obtained by the central control node using dedicated feedback links.

B. Communication Protocol

The duration T of each time slot is divided into three subslots durations, also, $m_1(t)T$, $m_2(t)T$ and $m_3(t)T$ are used to denote the time duration that is dedicated to energy harvesting, information transmission by Alice, and information transmission by the relay, respectively. Accordingly, it holds that

$$m_1(t) + m_2(t) + m_3(t) = 1, m_i(t) \in (0,1), i \in \{1,2,3\}. \quad (1)$$

More information about the three phases are provided below.

Phase 1: The relay harvests energy from the RF signal transmitted by Alice. The harvested energy at R is

$$E_{\mathrm{h}}(t) = m_1(t) T \eta P_{\mathrm{a}}(t) |\widetilde{h}_{\mathrm{ar}}(t)|^2, \quad (2)$$

where $P_{\mathrm{a}}(t)$ and η denote the transmitting power of Alice and the energy conversion efficiency, respectively.

Phase 2: Alice transmits information to the relay. The received information signal can be expressed as

$$y_{\mathrm{a}j}(t) = \sqrt{P_{\mathrm{a}}(t)}\widetilde{h}_{\mathrm{a}j}(t) x(t) + n_j(t), \quad (3)$$

where $y_{\mathrm{a}j}(t)$ corresponds to the received signal by node $j \in \{\mathrm{r}, \mathrm{e}\}$ during the first hop, $x(t)$ is the normalized information symbols from Alice, i.e., $\mathbb{E}[|x(t)|^2] = 1$. Also, $n_j(t) \sim \mathcal{CN}(0, \sigma^2)$ denotes the additive white Gaussian noise (AWGN) at the corresponding node. The instantaneous secrecy capacity of this hop normalized by the time that is dedicated to this phase is given by

$$C_{\mathrm{ar}}(t) = \left[\log_2\left(1 + \Gamma_{\mathrm{ar}}(t)\right) - \log_2\left(1 + \Gamma_{\mathrm{ae}}(t)\right)\right]^+, \quad (4)$$

where $\Gamma_{\mathrm{ar}}(t) = \frac{P_{\mathrm{a}}(t)|\widetilde{h}_{\mathrm{ar}}(t)|^2}{\sigma^2}$, $\Gamma_{\mathrm{ae}}(t) = \frac{P_{\mathrm{a}}(t)|\widetilde{h}_{\mathrm{ae}}(t)|^2}{\sigma^2}$, and $[x]^+ \triangleq \max(x,0)$. Thus, the secrecy rate from Alice to R during T is constrained by $R_{\mathrm{ar}}(t) \le m_2(t) C_{\mathrm{ar}}(t) T$.

Phase 3: The relay transmits information to Bob. In this time duration, R transmits the confidential messages by using the energy from its energy storage. The received signal by node k during the second hop can be expressed as

$$y_{\mathrm{r}k}(t) = \sqrt{P_{\mathrm{r}}(t)}\widetilde{h}_{\mathrm{r}k}(t) s(t) + n_k(t), \quad (5)$$

where $s(t)$ is the normalized information symbols from R, i.e., $\mathbb{E}[|s(t)|^2] = 1$. $P_{\mathrm{r}}(t)$ and $n_k(t), k \in \{\mathrm{b}, \mathrm{e}\}$ correspond to the transmitting power at R and additive white Gaussian noise (AWGN) at the k-th node, respectively. The instantaneous secrecy capacity of this hop is given by

$$C_{\mathrm{rb}}(t) = \left[\log_2\left(1 + \Gamma_{\mathrm{rb}}(t)\right) - \log_2\left(1 + \Gamma_{\mathrm{re}}(t)\right)\right]^+, \quad (6)$$

where $\Gamma_{\mathrm{rb}}(t) = \frac{P_{\mathrm{r}}(t)|\widetilde{h}_{\mathrm{rb}}(t)|^2}{\sigma^2}$ and $\Gamma_{\mathrm{re}}(t) = \frac{P_{\mathrm{r}}(t)|\widetilde{h}_{\mathrm{re}}(t)|^2}{\sigma^2}$. Thus, the secrecy rate from R to Bob during T is constrained by

$$R_{\mathrm{rb}}(t) \le m_3(t) C_{\mathrm{rb}}(t) T. \quad (7)$$

III. Optimization Framework

We assume that R is equipped with a data buffer and an energy storage device. Therefore, the optimal resource allocation policy depends not only on the CSI but also on the extra degrees-of freedom offered by the buffers, as well as their states. For example, if the link between Alice and the relay is secure while the link between the relay and Bob is insecure, Alice can still transmit information to the relay. This is because the corresponding information can be stored to the data buffer and be forwarded when the link between the relay and Bob becomes secure. Also, the use of the energy buffer allows the relay to harvest energy when both links are not secure, so that no time slot is wasted. In the sequel, the goal is to maximize the average secrecy throughput by designing an online adaptive transmission policy, optimizing both the time and power allocation.

A. Problem Formulation

Assuming that the size of data buffer and energy storage are sufficiently large, and, thus, the overflow probability is negligible [4], [7], which is verified by simulation in Section IV, the state of the data and energy queue at each time slot can be updated according to [7]

$$Q(t+1) = \left[Q(t) + R_{\mathrm{ar}}(t) - R_{\mathrm{rb}}(t)\right]^+, \quad (8)$$

$$E_{\mathrm{r}}(t+1) = \left[E_{\mathrm{r}}(t) - m_3(t) T P_{\mathrm{r}}(t)\right]^+ + E_{\mathrm{h}}(t). \quad (9)$$

Also, the average secrecy rate is

$$\bar{C}_{\mathrm{sec}} = \min\left\{\bar{C}_{\mathrm{ar}}, \bar{C}_{\mathrm{rb}}\right\}, \quad (10)$$

where $\bar{C}_{\mathrm{ar}} = \lim\limits_{N \to +\infty} \frac{1}{N} \sum\limits_{t=0}^{N-1} R_{\mathrm{ar}}(t)$ and $\bar{C}_{\mathrm{rb}} = \lim\limits_{N \to +\infty} \frac{1}{N} \sum\limits_{t=0}^{N-1} R_{\mathrm{rb}}(t)$. Thus, the optimization problem that aims at the maximization of the average secrecy rate can be expressed as

$$
\begin{aligned}
\max_{\mathbf{P(t)},\,\mathbf{R(t)},\,\mathbf{m(t)}} \quad & \bar{C}_{\mathrm{ar}} \\
\text{s.t.} \quad & \mathrm{C}_1: \bar{C}_{\mathrm{ar}} \leq \bar{C}_{\mathrm{rb}}, \\
& \mathrm{C}_2: \lim_{N\to\infty} \frac{1}{N} \sum_{t=0}^{N-1} m_3(t) P_{\mathrm{r}}(t) T \leq \lim_{N\to\infty} \frac{1}{N} \sum_{t=0}^{N} E_{\mathrm{h}}(t), \\
& \mathrm{C}_3: \lim_{N\to\infty} \frac{1}{N} \sum_{t=0}^{N-1} \left(m_1(t)+m_2(t)\right) P_{\mathrm{a}}(t) T \leq \bar{P}_{\mathrm{a}} T, \\
& \mathrm{C}_4: 0 \leq P_{\mathrm{a}}(t) \leq \hat{P}_{\mathrm{a}}, \forall t, \\
& \mathrm{C}_5: 0 \leq P_{\mathrm{r}}(t) \leq \hat{P}_{\mathrm{r}}, \forall t, \\
& \mathrm{C}_6: R_{\mathrm{ar}}(t) \leq m_2(t) C_{\mathrm{ar}}(t) T, \forall t, \\
& \mathrm{C}_7: R_{\mathrm{rb}}(t) \leq m_3(t) C_{\mathrm{rb}}(t) T, \forall t, \\
& \mathrm{C}_8: m_i(t) \geq 0, i \in \{1,2,3\}, \forall t, \\
& \mathrm{C}_9: \sum_{i=1}^{3} m_i(t) = 1, \forall t,
\end{aligned}
\tag{11}
$$

where $\mathbf{P(t)} = [P_{\mathrm{a}}(t), P_{\mathrm{r}}(t)]$, $\mathbf{R(t)} = [R_{\mathrm{ar}}(t), R_{\mathrm{rb}}(t)]$. In addition, $\bar{P}_{\mathrm{a}}$ is the maximum average transmit power at Alice, while $\hat{P}_{\mathrm{a}}$ and $\hat{P}_{\mathrm{r}}$ are the peak transmit power at Alice and the relay, respectively. The stability of data and energy queues at relay are guaranteed by C_1 and C_2, respectively. Also, C_3 represents the average power constraint. Moreover, C_4 and C_5 are imposed to constrain the peak power at Alice and R, respectively, C_6 and C_7 stand for the constraint of the arrival and departure secure rate, respectively, while C_8 guarantees that the time allocation factor is non-negative. Finally, C_9 indicates that the length of T is divided into three parts.

B. Problem Transformation using Lyapunov Optimization

The average energy consumption of Alice is considered in C_3 of (11), which can be described as the energy status at Alice. Let $E_{\mathrm{a}}(t)$ represent the energy state of Alice, the dynamic characteristics of which can be given by

$$
E_{\mathrm{a}}(t+1) = \left[E_{\mathrm{a}}(t) + \left(m_1(t)+m_2(t)\right) P_{\mathrm{a}}(t) T - \bar{P}_{\mathrm{a}} T\right]^{+}. \tag{12}
$$

It can be easily proved that the average power constraint C_3 is equivalent to the energy queue stability problem (12). Moreover, the update equations of queue and energy queues at R, which correspond to (8) and (9), respectively, are in similar form with (12). Thus, we can also transform the constraints C_1 and C_2 into data and energy queue stability problems, respectively. Therefore, the optimization problem (11) can be transformed into an equivalent one that aims at the maximization of the average secrecy rate while keeping the stability of all data and energy queues.

To efficiently solve the equivalent optimization problem, Lyapunov optimization framework can be applied [11]. We define $\boldsymbol{\Theta}(t) = [Q(t), E_{\mathrm{r}}(t), E_{\mathrm{a}}(t)]$ as the actual and virtual queues backlog vector, the "size" of which can be described as follows:

$$
L(\boldsymbol{\Theta}(t)) = \frac{1}{2} Q^2(t) + \frac{\mu_1}{2} E_{\mathrm{a}}^2(t) + \frac{\mu_2}{2} \left(\phi - E_{\mathrm{r}}(t)\right)^2, \tag{13}
$$

where μ_1, μ_2 are non-negative weights, which can keep the stability of the three queues. In order to ensure that the energy queue always has sufficient energy for transmission, ϕ is introduced as a perturbation value of the energy queue, while it is assumed that $E_{\mathrm{r}}(t) \leq \phi$. Thus the energy queue update equation can be modified as

$$
E_{\mathrm{r}}(t+1) = \min\left\{\left[E_{\mathrm{r}}(t) - m_3(t) T P_{\mathrm{r}}(t)\right]^{+} + E_{\mathrm{h}}(t), \phi\right\}. \tag{14}
$$

According to [11], we further define the one-slot conditional Lyapunov drift as

$$
\Delta(\boldsymbol{\Theta}(t)) \triangleq \mathbb{E}\left\{L(\boldsymbol{\Theta}(t+1)) - L(\boldsymbol{\Theta}(t)) \,|\, \boldsymbol{\Theta}(t)\right\}, \tag{15}
$$

where the expectation is taken over the randomness of the CSIs and the control decisions (power and time allocations). $\Delta(\boldsymbol{\Theta}(t))$ reflects the increment characteristics of the queue $\boldsymbol{\Theta}(t)$, and we can ensure the stability of queues by minimizing it. At the same time, our goal is to maximize the average secrecy rate. To this end, we only need to minimize the drift-plus-penalty function

$$
\Delta(\boldsymbol{\Theta}(t)) - V \mathbb{E}\left\{R_{\mathrm{ar}}(t) | \boldsymbol{\Theta}(t)\right\}, \tag{16}
$$

where the parameter $V \geq 0$ is a penalty weight, which is used to control the tradeoff between the long-term average secrecy rate and the average data queue length. It is worth mentioning that according to Little's law, the average data queue length is proportional to the average queue delay. Thus, the selection V affects the tradeoff between the average secrecy rate and the average queue delay.

Lemma 1: (Drift-Plus-Penalty Bound): For given $\boldsymbol{\Theta}(t)$ and $\forall V \geq 0$, the Lyapunov drift-plus-penaly function has the following bound, $\forall t$:

$$
\begin{aligned}
& \Delta(\boldsymbol{\Theta}(t)) - V \mathbb{E}\left\{R_{\mathrm{ar}}(t) | \boldsymbol{\Theta}(t)\right\} \\
\leq & B - V \mathbb{E}\{R_{\mathrm{ar}}(t) | \boldsymbol{\Theta}(t)\}\} + Q(t) \mathbb{E}\{R_{\mathrm{ar}}(t) - R_{\mathrm{rb}}(t) | \boldsymbol{\Theta}(t)\} + \\
& \mu_1 E_{\mathrm{a}}(t) \mathbb{E}\left\{\left(m_1(t)+m_2(t)\right) P_{\mathrm{a}}(t) T - \bar{P}_{\mathrm{a}} T | \boldsymbol{\Theta}(t)\right\} + \\
& \mu_2 (\phi - E_{\mathrm{r}}(t)) \mathbb{E}\{m_3(t) P_{\mathrm{r}}(t) T - E_{\mathrm{h}}(t) | \boldsymbol{\Theta}(t)\},
\end{aligned}
\tag{17}
$$

where

$$
\begin{aligned}
B \geq & \frac{1}{2} \mathbb{E}\{\hat{R}_{\mathrm{ar}}^2 + \hat{R}_{\mathrm{rb}}^2 | \boldsymbol{\Theta}(t)\} + \frac{\mu_1}{2} \mathbb{E}\{(\hat{P}_{\mathrm{a}}^2 + \bar{P}_{\mathrm{a}}^2) | \boldsymbol{\Theta}(t)\} \\
& + \frac{\mu_2}{2} \mathbb{E}\{(\hat{P}_{\mathrm{r}}^2 + \hat{E}_{\mathrm{h}}^2) | \boldsymbol{\Theta}(t)\},
\end{aligned}
\tag{18}
$$

in which B is a constant, $\hat{R}_{\mathrm{ar}}$ and $\hat{R}_{\mathrm{rd}}$ denote the maximum secure transmission rate of the corresponding link. $\hat{E}_{\mathrm{h}}$ is the maximum harvested energy of the relay.

Lemma 1 can be easily proved. One can note that Lemma 1 provides an upper bound on the Lyapunov drift-plus-penalty given in the right-hand-side of (17), the minimization of which is equivalent to directly minimizing the Lyapunov drift-plus-penalty. Since the channels are independent and identically distributed (i.i.d.) random variables over different time slots and we consider the statistical expectation over the the channels' realizations and scheduling decisions, at each time slot t, we can dynamically optimize the power and time allocation by observing the current queue state $\boldsymbol{\Theta}(t)$ and the current channel state. Thus, the optimization problem of (11) is transformed as

$$\mathcal{L}(R_{\mathrm{ar}}(t),R_{\mathrm{rb}}(t),\mathbf{E}(\mathbf{t}),\mathbf{m}(\mathbf{t}),\mathbf{l},\lambda,\mathbf{v}(\mathbf{t}),\mathbf{s}(\mathbf{t}),\mathbf{w}(\mathbf{t}))=-VR_{\mathrm{ar}}(t)+Q(t)\left(R_{\mathrm{ar}}(t)-R_{\mathrm{rb}}(t)\right)+\mu_1E_{\mathrm{a}}(t)\left(E_{\mathrm{m}}^1(t)+E_{\mathrm{m}}^2(t)\right)T$$
$$+\mu_2\left(\phi-E_{\mathrm{r}}(t)\right)\left(E_{\mathrm{m}}^3(t)T-\eta m_1(t)E_{\mathrm{m}}^1(t)|\widetilde{h}_{\mathrm{ar}}(t)|^2T\right)-\sum_{i=1}^{2}\left(l^i(t)E_{\mathrm{m}}^i(t)-\lambda^i(t)\left(E_{\mathrm{m}}^i(t)-\hat{P}_{\mathrm{a}}m_i(t)\right)\right)+\lambda^3(t)(E_{\mathrm{m}}^3(t)-\hat{P}_{\mathrm{r}}m_3(t)))$$
$$-\sum_{i=1}^{3}v_i(t)m_i(t)+\sum_{t=1}^{N}v(t)\left(\sum_{i=1}^{3}m_i(t)-1\right)-\sum_{j\in J}s_j(t)R_j(t)+\sum_{j\in J}\sum_{t=1}^{N}w_j(t)\left(R_j(t)-\tilde{C}_j(t)\right). \qquad (20)$$

follows:

$$\begin{aligned}\min_{\mathbf{P(t)},\,\mathbf{R(t)},\,\mathbf{m(t)}}\quad & -VR_{\mathrm{ar}}(t)+Q(t)(R_{\mathrm{ar}}(t)-R_{\mathrm{rb}}(t))\\ & +\mu_1E_{\mathrm{a}}(t)(m_1(t)+m_2(t))P_{\mathrm{a}}(t)T\\ & +\mu_2(\phi-E_{\mathrm{r}}(t))(m_3(t)P_{\mathrm{r}}(t)T-E_{\mathrm{h}}(t))\\ \mathbf{s.t.}\quad & \mathrm{C}_4,\mathrm{C}_5,\mathrm{C}_6,\mathrm{C}_7,\mathrm{C}_8,\mathrm{C}_9.\end{aligned} \qquad (19)$$

C. Solution of the Transformed Problem

It should be noted that (19) is non-convex, thus, it cannot be directly solved with acceptable complexity. However, in the following Lemma we will show that (19) can be transformed into a standard convex optimization problem by introducing some new auxiliary optimization variables.

Lemma 2: The optimization problem in (19) can be transformed into the following convex optimization problem:

$$\begin{aligned}\min_{\mathbf{R(t)},\,\mathbf{E(t)},\,\mathbf{m(t)}}\quad & -VR_{\mathrm{ar}}(t)+Q(t)(R_{\mathrm{ar}}(t)-R_{\mathrm{rb}}(t))+\mu_1E_{\mathrm{a}}(t)\times\\ & (E_{\mathrm{m}}^1(t)+E_{\mathrm{m}}^2(t))T+\mu_2(\phi-E_{\mathrm{r}}(t))\times\\ & (E_{\mathrm{m}}^3(t)T-\eta E_{\mathrm{m}}^1(t)|\widetilde{h}_{\mathrm{ar}}(t)|^2T)\\ \mathbf{s.t.}\quad & \mathrm{C}_1:0\le E_{\mathrm{m}}^1(t)\le\hat{P}_{\mathrm{a}}m_1(t),\\ & \mathrm{C}_2:0\le E_{\mathrm{m}}^2(t)\le\hat{P}_{\mathrm{a}}m_2(t),\\ & \mathrm{C}_3:0\le E_{\mathrm{m}}^3(t)\le\hat{P}_{\mathrm{r}}m_3(t),\\ & \mathrm{C}_4:0\le R_{\mathrm{ar}}(t)\le\widetilde{C}_{\mathrm{ar}}(t)T,\\ & \mathrm{C}_5:0\le R_{\mathrm{rb}}(t)\le\widetilde{C}_{\mathrm{rb}}(t)T,\\ & \mathrm{C}_6:m_i(t)\ge0,i\in\{1,2,3\},\\ & \mathrm{C}_7:\sum_{i=1}^{3}m_i(t)=1,\end{aligned} \qquad (21)$$

where $\widetilde{C}_{\mathrm{ar}}(t)=m_2(t)C_{\mathrm{ar}}(t)$, $\widetilde{C}_{\mathrm{rb}}(t)=m_3(t)C_{\mathrm{rb}}(t)$, $\mathbf{E}(\mathbf{t})=\left[E_{\mathrm{m}}^1(t),E_{\mathrm{m}}^2(t),E_{\mathrm{m}}^3(t)\right]$, $E_{\mathrm{m}}^1(t)=m_1(t)P_{\mathrm{a}}(t)$, $E_{\mathrm{m}}^2(t)=m_2(t)P_{\mathrm{a}}(t)$, and $E_{\mathrm{m}}^3(t)=m_3(t)P_{\mathrm{r}}(t)$.

Proof: By considering the expressions of $E_{\mathrm{m}}^1(t)$, $E_{\mathrm{m}}^2(t)$ and $E_{\mathrm{m}}^3(t)$, the constraints C_4 and C_5 of (19) can be rewritten as $0\le E_{\mathrm{m}}^1(t)\le\hat{P}_{\mathrm{a}}m_1(t)$, $0\le E_{\mathrm{m}}^2(t)\le\hat{P}_{\mathrm{a}}m_2(t)$, and $0\le E_{\mathrm{m}}^3(t)\le\hat{P}_{\mathrm{r}}m_3(t)$. Besides, it holds that

$$C_{\mathrm{ar}}(t)=\left[\log_2\left(1+c_1(t)\frac{E_{\mathrm{m}}^2(t)}{m_2(t)}\right)-\log_2\left(1+c_2(t)\frac{E_{\mathrm{m}}^2(t)}{m_2(t)}\right)\right]^+, \qquad (22)$$

and

$$C_{\mathrm{rb}}(t)=\left[\log_2\left(1+c_3(t)\frac{E_{\mathrm{m}}^3(t)}{m_3(t)}\right)-\log_2\left(1+c_4(t)\frac{E_{\mathrm{m}}^3(t)}{m_3(t)}\right)\right]^+, \qquad (23)$$

where $c_1(t)=\frac{|\widetilde{h}_{\mathrm{ar}}(t)|^2}{\sigma^2}$, $c_2(t)=\frac{|\widetilde{h}_{\mathrm{ae}}(t)|^2}{\sigma^2}$, $c_3(t)=\frac{|\widetilde{h}_{\mathrm{rb}}(t)|^2}{\sigma^2}$ and $c_4(t)=\frac{|\widetilde{h}_{\mathrm{re}}(t)|^2}{\sigma^2}$, respectively. Both of $\widetilde{C}_{\mathrm{ar}}(t)=m_2(t)C_{\mathrm{ar}}(t)$ and $\widetilde{C}_{\mathrm{rb}}(t)=m_3(t)C_{\mathrm{rb}}(t)$ are in the form of $G(x,t)=tF\left(\frac{x}{t}\right)$, where $F(x)=[\log_2(1+c_3(t)x)-\log_2(1+c_4(t)x)]^+$. It is noticed that if $c_3(t)\le c_4(t)$, $F(x)=0$; if $c_3(t)>c_4(t)$, $F(x)$ is a concave function. Since $G(x,t)=tF\left(\frac{x}{t}\right)$ retains concavity, it can be concluded that both $R_{\mathrm{ar}}(t)$ and $R_{\mathrm{rb}}(t)$ are concave functions. Thus, (21) is a standard convex optimization problem. ■

Theorem 1: The optimal time allocation ratio $m_i(t),i\in\{1,2,3\}$ at time slot t is either equal to 0 or 1, i.e., the system will choose only one of the three phases at the t-th time slot.

Proof: The optimization problem (21) is a convex problem with respect to variables $R_{\mathrm{ar}}(t),R_{\mathrm{rb}}(t),\mathbf{E}(\mathbf{t})$ and $\mathbf{m}(\mathbf{t})$. First, let us define the dual variables $\boldsymbol{l},\boldsymbol{\lambda},\mathbf{v}(\mathbf{t}),\mathbf{s}(\mathbf{t}),\mathbf{w}(\mathbf{t})$ associated with the corresponding constraints and write the Lagrange function as (20). By setting the derivative of the Lagrangian function with respect to $m_i(t)$ equal to zero, we can get

$$\frac{\partial\mathcal{L}}{\partial m_1(t)}=-\lambda^1(t)\hat{P}_{\mathrm{a}}-v_1(t)+v(t)=0, \qquad (24)$$

$$\begin{aligned}\frac{\partial\mathcal{L}}{\partial m_2(t)}&=-\lambda^2(t)\hat{P}_{\mathrm{a}}-v_2(t)+v(t)-\frac{w_{\mathrm{ar}}(t)E_{\mathrm{m}}^2(t)c_2(t)}{\ln2(m_2(t)+E_{\mathrm{m}}^2(t)c_2(t))}\\ &\quad-w_{\mathrm{ar}}(t)\frac{C_{\mathrm{ar}}(t)}{m_2(t)}+\frac{w_{\mathrm{ar}}(t)E_{\mathrm{m}}^2(t)c_1(t)}{\ln2(m_2(t)+E_{\mathrm{m}}^2(t)c_1(t))}=0,\end{aligned} \qquad (25)$$

and

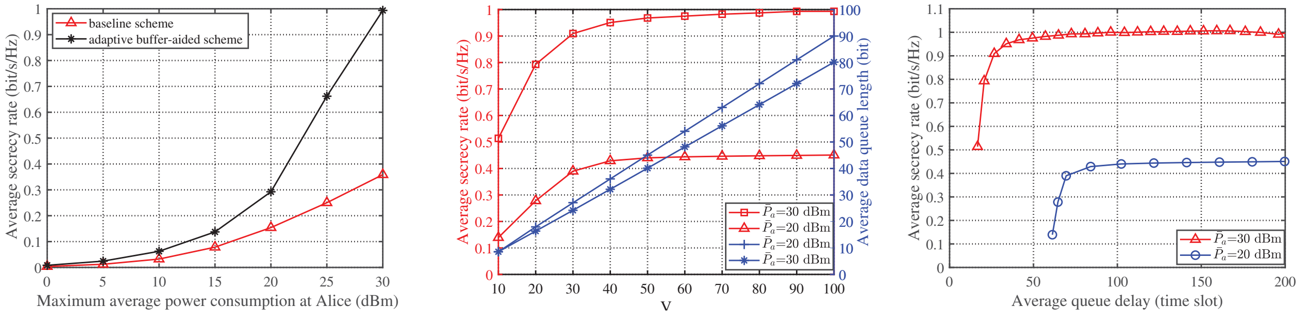
$$\begin{aligned}\frac{\partial\mathcal{L}}{\partial m_3(t)}&=-\lambda^3(t)\hat{P}_{\mathrm{r}}-v_3(t)+v(t)-\frac{w_{\mathrm{rb}}(t)E_{\mathrm{m}}^3(t)c_4(t)}{\ln2(m_3(t)+E_{\mathrm{m}}^3(t)c_4(t))}\\ &\quad-w_{\mathrm{rb}}(t)\frac{C_{\mathrm{rb}}(t)}{m_3(t)}+\frac{w_{\mathrm{rb}}(t)E_{\mathrm{m}}^3(t)c_3(t)}{\ln2(m_3(t)+E_{\mathrm{m}}^3(t)c_3(t))}=0.\end{aligned} \qquad (26)$$

If one of the optimal mode selection variables $m_i(t)\in(0,1)$, then according to $\sum_{i=1}^{3}m_i(t)=1$, we can infer that there should be $j\ne i$, for which $m_j(t)\in(0,1)$. Without loss of generality, we assume that $m_1(t)\in(0,1)$ and $m_2(t)\in(0,1)$. According to the complementary slackness of the KKT conditions, we get that $v_1(t)=v_2(t)=0$. Accordingly, (24) and (25) can be rewritten as

$$v(t)=\lambda^1(t)\hat{P}_{\mathrm{a}}, \qquad (27)$$

and

$$\begin{aligned}v(t)=&\lambda^2(t)\hat{P}_{\mathrm{a}}+\frac{1}{\ln2}\frac{w_{\mathrm{ar}}(t)E_{\mathrm{m(t)}}^2c_2(t)}{m_2(t)+E_{\mathrm{m(t)}}^2c_2(t)}\\ &+w_{\mathrm{ar}}(t)\frac{C_{\mathrm{ar}}(t)}{m_2(t)}-\frac{w_{\mathrm{ar}}(t)E_{\mathrm{m(t)}}^2c_1(t)}{\ln2\left(m_2(t)+E_{\mathrm{m(t)}}^2c_1(t)\right)},\end{aligned} \qquad (28)$$



(a) Secrecy throughput of the considered schemes versus the transmit power of Alice (b) Average data queue length and secrecy rate v.s. V. (c) Average secrecy rate v.s. average queueing delay.

Fig. 2

respectively.

The channel gains are assumed to have continuous probability density functions. Therefore, we can hardly find a $v(t)$ to satisfy both of the above two equations, which completes the proof. ■

Thus, (21) can be solved by considering two different cases i.e., by considering $m(t) = 0$ and $m(t) = 1$, respectively. Then, the corresponding problems can be efficiently solved by using conventional convex optimization methods.

IV. Simulation Results

In this section, we evaluate the performance of the proposed schemes through Monte-Carlo simulations. We set the path loss exponent $m = 2$, the distances $d_{\mathrm{ar}} = 4$ m, $d_{\mathrm{rb}} = 5$ m, $d_{\mathrm{ae}} = 9$ m, $d_{\mathrm{re}} = 8$ m, and the duration of each time slot $T = 1$ s. The energy harvesting efficiency is $\eta = 0.5$, and the maximum transmit power of Alice is $\hat{P}_{\mathrm{a}} = 3\bar{P}_{\mathrm{a}}$, $\bar{P}_{\mathrm{a}} = 30$ dBm. The noise variances of all receivers are set to 0 dBm. The perturbation value of energy queue is assumed to be $\phi = 10$ J. Moreover, all figures are obtained for 10^6 time slots.

In Fig. 2(a), a conventional secure relaying network with SWIPT is considered as a baseline scheme, in which the relay is neither equipped with a data buffer nor with an energy storage device. It can be seen that the proposed buffer-aided scheme has a considerable improvement of the average secrecy rate, since it enables the disjoint exploitation of the two links, without being constrained by the worse link. Rather than this, when both links are not reliable, the relay can still harvest energy, eliminating the waste of time and energy resources.

The average data queue length and average secrecy rate under different V are presented in Fig. 2(b). We can observe that the average data queue length grows linearly with V and the average secrecy throughput increases with the increase in V, which is consistent with Theorem 1. The tradeoff between the average secrecy throughout and the average queueing delay is shown in Fig. 2(c). As one can observe, a larger average secrecy throughput can be achieved if a large delay is tolerable.

V. Conclusion

In this paper, a buffer-aided secure relaying network with SWIPT has been investigated. Based on the Lyapunov optimization approach, we proposed an online adaptive transmission policy to maximize the long-term average secrecy rate. Moreover, we have proved that each time slot should be used either for energy transfer of information transmission. In addition, an interesting tradeoff between the secrecy throughput and the average queue delay has been revealed.

VI. Acknowledgment

This work was supported by the Sichuan Science and Technology Program under Grant 2017HH0035, the NSFC project under Grants 61971360/61771406, and the Fundamental Research Funds for the Central Universities under Grant 2682018CX27. (Xianfu Lei is the corresponding author of this paper.)

References

[1] H. Deng, H. Wang, W. Guo, and W. Wang, “Secrecy transmission with a helper: To relay or to jam.” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[2] T. Q. Duong, T. M. Hoang, C. Kundu, M. Elkashlan, and A. Nallanathan, “Optimal power allocation for multiuser secure communication in cooperative relaying networks,” *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 516–519, Oct. 2016.

[3] C. Wang, H.-M. Wang, D. W. K. Ng, X.-G. Xia, and C. Liu, “Joint beamforming and power allocation for secrecy in peer-to-peer relay networks,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280–3293, Jun. 2015.

[4] B. Xia, Y. Fan, J. Thompson, and H. V. Poor, “Buffering in a three-node relay network,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4492–4496, Nov. 2008.

[5] J. He, Y. Zhang, Y. Shen, and X. Jiang, “Link selection for secure two-hop transmissions in buffer-aided relay wireless networks,” in *Proc. Int. Conf. Netw. Netw. Appl.*, Jul. 2016, pp. 64–68.

[6] A. El Shafie, A. Sultan, and N. Al-Dhahir, “Physical-layer security of a buffer-aided full-duplex relaying system,” *IEEE Wireless Commun. Lett.*, vol. 20, no. 9, pp. 1856–1859, Sep. 2016.

[7] J. Wan, D. Qiao, H.-M. 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.

[8] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, “Joint beamforming and time switching design for secrecy rate maximization in wireless-powered fd relay systems,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 567–579, Jan. 2018.

[9] A. El Shafie and N. Al-Dhahir, “Secure communications in the presence of a buffer-aided wireless-powered relay with self-energy recycling,” *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 32–35, Feb 2016.

[10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[11] M. J. Neely, “Stochastic network optimization with application to communication and queueing systems,” *Synthesis Lectures on Communication Networks*, vol. 3, no. 1, pp. 1–211, 2010.