Security and Communication Networks

Secure Information Transmissions in Wireless-powered Cognitive Radio Networks for Internet of Medical Things

K. Tang,[1,3] W. Tang,[2] E. Luo,[3] Z. Tan[4], W. Meng[5], L. Qi[6]

[1] Guangdong Provincial Key Laboratory of Millimeter-Wave and Terahertz, School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China.

[2] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China.

[3] School of Electronics and Information Engineering, Hunan University of Science and Engineering, Yongzhou 425000, China.

[4] School of Computing, Edinburgh Napier University, Edinburgh EH11 4BN, United Kingdom.

[5] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Lyngby 2800 Kgs., Denmark.

[6] School of Information Science and Engineering, Qufu Normal University, Rizhao 276826, China.

Correspondence should be addressed to E. Luo; luoentao_huse@163.com

Abstract

In this paper, we consider the issue of the secure transmissions for the cognitive radio-based Internet of Medical Things (IoMT) with wireless energy harvesting. In these systems, a primary transmitter (PT) will transmit its sensitive medical information to a primary receiver (PR) by a multi-antenna-based secondary transmitter (ST), where we consider that a potential eavesdropper may listen the PT's sensitive information. In the meanwhile, the ST also transmits its own information concurrently by utilizing spectrum sharing. We aim to propose a novel scheme for jointly designing the optimal parameters, i.e., energy harvesting (EH) time ratio and secure beamforming vectors, for maximizing the primary secrecy transmission rate while guaranteeing secondary transmission requirement. For solving the non-convex optimization problem, we transfer the problem into convex optimization form by adopting the semi-definite relaxation (SDR) method and Charnes-Cooper transformation technique. Then, the optimal secure beamforming vectors and energy harvesting duration can be obtain easily by utilizing the CVX tools. According to the simulation results of secrecy transmission rate, i.e., secrecy capacity, we can observe that the proposed protocol for the considered system model can effectively promote the primary secrecy transmission rate when compared with

traditional zero-forcing (ZF) scheme, while ensuring the transmission rate of the secondary system.

I. Introduction

With the rapid development of wireless communication and networking technologies, an increasing number of devices need to be connected globally and communicate automatically. Therefore, the emerging of the Internet of Things (IoT) as a promising paradigm can achieve a fusing of the various technologies in 5G communication systems, which have been widely applied in smart cities, agriculture, and environment monitoring [1-6]. Moreover, the medical care and health care have becoming one of the most popular applications based on the IoT [7,8], named the Internet of Medical Things (IoMT), which can collect the data from the medical devices and applications to improve the treatment effect, disease diagnosis, and patient experience, while reduce decrease misdiagnosis rate and treatment cost. According to the investigation of relevant organizations, the market share of IoMT will reach to roughly 117 billion dollars by the end of 2020 [9]. However, with the increasing use of IoMT equipment, the huge demand for radio spectrum has become a serious problem. In addition, the allocated radio spectrums are often underutilized due to the inflexible spectrum policies [10]. In order to facilitate an effective utilization of spectrum resources, cognitive radio technology was introduced in which unlicensed nodes could communicate with each other in an opportunistic manner over a licensed frequency band without interrupting the primary transmissions [11-13].

Yet, power supply is another key constraint on the development of IoMT. In general, an IoMT system usually contains a large number of small-size devices that are battery-powered and difficult to be replaced. In order to solve this problem, wireless-powered technology has been paid high attention. The devices with EH capabilities can convert energy from the surrounding environment into electricity for data transmission, such as solar, wind, or RF signals [14]. Especially with the synchronous development of antenna and circuit designs, wireless EH based on RF signals has attracted more attention due to its advantages of wireless, low cost and small form implementation [15-17]. Furthermore, the amount of harvested energy is in milliwatts, which is enough to power small-size IoMT devices, such as medical data sensors for short-distance transmissions. Therefore, the combination of cognitive radio and EH in medical wireless sensor networks can greatly improve both the spectrum and energy efficiencies.

Although adopting cognitive radio technology with EH can effectively improve the transfer efficiency for IoMT, the variety of medical devices in healthcare fields will introduce several security problems [18]. Since the energy-constraint sensors need to perform energy harvesting and then forward the sensitive patient data wirelessly, the other illegal sensors may be the potential eavesdropper to listen such confidential messages [19]. As an emerging field, a large number of healthcare manufacturers are rushing to utilize the IoT solutions in some applications without considering security. As a result, there will bring new security problems related to confidentiality, integrity, and availability. Furthermore, due to the limited capabilities, such as lack of effective computation and sufficient power supply, many sensors in IoMT cannot embed encryption algorithm. Therefore, these lack of strong encryption across medical sensors make themselves to be discovered and exploited by malicious users easily.

A. Related work

To take the full advantage of the potential gains for wireless EH, the researchers developed simultaneous wireless information and power transmission (SWIPT) schemes in wireless networks that utilize RF signals to transmit energy and information to receivers. Authors in [20] applied the SWPIT in relay interference channels for multiple source-destination pairs communication system, where each pair of link has a dedicated EH relay serving for relaying transmission. On this basis, the optimal power allocation ratio for each relay was deduced by adopting the distributed power allocation framework of game theory. A SWIPT scheme for amplify-and-forward (AF) bidirectional relaying network based on OFDM was proposed in [21], where a wireless-powered relay performed information processing and EH by utilizing two disjoint subcarriers groups, respectively. Based on the decode-and-forward (DF) mode, the authors in [22] designed an optimal resource allocation strategy to maximize the energy efficiency with non-linear SWIPT model under a two-way relay network. For cognitive radio networks with energy harvesting in IoT systems, the authors in [23] analyzed the outage probability of a random underlay cognitive network with EH-based assistant relay. The two main challenges for cognitive radio sensor networks in IoT systems were considered in [24], where the authors developed an architecture and proposed an energy management strategy for achieving balance between the transmission performance of the networks and operational life. In [25], the authors considered the insecure characteristic of electronic medical records based on eHealth systems, and then proposed a corresponding secure encrypted scheme to ensure the data security. In [26], the authors investigated an overlaid spectrum sharing network with SWIPT for IoT systems, where a pair of SWIPT-based devices as the relays to assist the transmission of the primary signals. Considering information security in cognitive radio-based IoT systems, the authors in [27] presented a novel algorithm for channel allocation with time-sensitive data under the scenario of jamming attacks. A secure relay selection scheme based on channel state information and battery state information was proposed for energy harvesting-based cognitive radio networks in IoT networks [28].

B. Motivation and Contributions

Unlike the mentioned literates [27] and [28] in above, we consider an actual application scenarios for sanatorium or hospital under the cognitive radio-based IoTM networks to protect the patients' sensitive medical information. Considering an indoor environment for sanatorium or hospital, where the PT intends to transmit its sensitive medical data to the PR, while the ST performs data monitoring and transfer to the SR. In this scenario, the node ST has lack of energy supply and need to scavenge energy from the primary transmitter, while ST can be regarded as the relay to opportunistically access the licensed primary channel. Meanwhile, we assume that an attacker is located near the PR to eavesdrop the PT's medical data. Thus, to enable the secure transmission of the PT's signal, we investigate a typical cognitive radio network with wireless-powered relay (CRN-WPR) and jointly design the optimal EH time ratio and secure beamforming vectors to maximize the secrecy transmission rate of the primary system, while effectively guarantee the secondary transmission rate. The main contributions are summarized as follows:

- We propose a corresponding protocol for EH and secrecy information transmission for a cognitive radio-based IoMT system, where the relay node ST is equipped with multiple-antenna to perform EH at first and then transfers the sensitively primary signal with DF processing to the destination in security with its own signal.

- In order to protect the sensitive medical data sending from the PT, we formulate the optimization problem based on maximizing the secrecy transmission rate of the primary system while ensuring the transmission requirement of the secondary system. We adopt SDR and Charnes-Cooper transformation to transform the non-convex optimization problem into a convex optimization problem to find a solution for the optimization problem. A corresponding algorithm is then developed. In addition, the zero-forcing (ZF) scheme is also applied to solve the optimization problem as a benchmark.
- The numerical results of the influence for the secrecy transmission rate on the primary system under different system parameters are given, such as primary transmission power, number of antennas, and transmission distance, etc. The results demonstrate excellent secure transmission performance with proposed scheme than ZF scheme.

The rest of this paper is organized as follows. The section II introduces the system model and transmission protocol. Section III formulates the optimization problem and proposes the corresponding solution with secure beamforming. Furthermore, the ZF scheme is also adopted to solve the optimization as a benchmark. The section IV presents the simulation results and corresponding analyses. The section V summarizes this paper.

Notations: Throughout this paper, let $(\cdot)^H$ denote the conjugate transpose. $\mathbf{I}$ presents the identity matrix with appropriate dimension. $[x]^+$ represents the maximum value between x and 0, while x^* denotes the optimal value of x. $\prod_x^{\perp}$ denotes the orthogonal projection onto the orthogonal complement of the column space of x. $\|\cdot\|$ denotes the Euclidean norm of a vector or a matrix and $|\cdot|$ denotes the magnitude of a channel or the absolute value of a complex number. Table I lists the fundamental notations and parameters.

Table 1: List of parameters and their physical meaning/expression.

Parameter	Meaning/Expression
$\mathbf{h}_{PST}, \mathbf{h}_{SS}, \mathbf{h}_{SME}, \mathbf{h}_{SPR}$	$N \times 1$ complex channel vectors of the PT-ST, ST-SR, ST-ME, and ST-PR, respectively
h_{PP}, h_{PME}	Channel coefficients of the PT-PR and the PT-ME
α	Duration of energy harvesting
T	Total block time
x_e, x_P	Transmit dedicated energy signal and confidential signal at PT
$\hat{x}_P, x_S$	Decoded primary signal and secondary signal at ST
P_P	PT’s transmission power
$\mathbf{n}_{ST}, n_{PR}, n_{ME}, n_{SR}$	Received AWGN at ST, PR, ME, and SR
η	Energy conversion efficiency from signal power to circuit power
$R_{ST}, R_{PR}, R_{ME}, R_{SR}$	Achievable rate at ST, PR, ME, and SR, respectively
$\tilde{R}_{PR}, \tilde{R}_{ME}$	Overall transmission rates at PR and ME
R_{SEC}	Secrecy rate of the primary system
$\mathbf{v}_P, \mathbf{v}_S$	Relaying beamforming vector and cognitive beamforming vector
E_{ST0}	Initial power at the ST
r_S	Minimal transmission rate requirement for the secondary system

Γ	An auxiliary optimization variable to bound the achievable rate of the eavesdropper ME
β	Power allocation coefficient

II. System Model and Transmission Protocol

A. System Model

We consider a cognitive radio network with wireless-powered relay (CRN-WPR) as shown in Fig. 1. The primary system is composed of a primary transmitter (PT) and a primary receiver (PR), while the secondary system consists of a secondary transmitter (ST) and a secondary receiver (SR). There also exists an eavesdropper (ME) whose purpose is to intercept the PT's confidential data in the range of the primary system, where PT intends to send a confidential data to PR. The primary system may be regard as the uplink of the transmission system with poor channel quality or lower rate. Therefore, the ST is willing to act as the relay for assisting the primary transmission while delivering its own data. We assume that the PT has a fixed power supply, while the ST may have limited battery storage, so it needs to obtain energy from the received RF signal. The ST is equipped with N antennas and other nodes operates in half-duplex mode with single antenna.

All channels undergo the flat block Rayleigh fading channel, which is characterized by quasi-static state of the channel in one transmission-slot and independent change in different transmission-slots. Let $\mathbf{h}_{PST}$, $\mathbf{h}_{SS}$, $\mathbf{h}_{SME}$, and $\mathbf{h}_{SPR}$ be the $N \times 1$ complex channel vectors of the PT-ST, ST-SR, ST-ME, and ST-PR, respectively. The channel coefficients of the PT-PR and the PT-ME links are denoted by h_{PP} and h_{PME}. The global channel state information is available for the system, which is a common assumption in physical-layer security literatures [29,30].

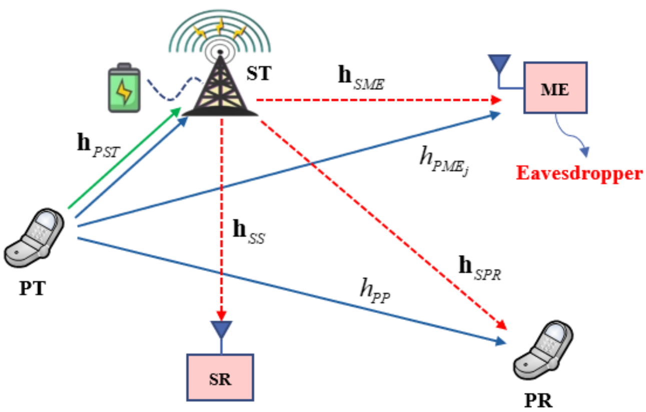

Figure 1: System model of a CRN-WPR. The green line denotes the first phase for energy harvesting, the blue lines and red lines represent the second and third information transmission phases from the PT and ST, respectively.

B. Energy Harvesting and Information Transmission

As depicted in Fig. 1, the EH and information transmission in one transmission-slot includes three phases. In the first phase, the PT uses a portion of time $\alpha\left(\alpha \in (0,1)\right)$ of the total block time T to transmit the dedicated energy signal x_e to ST for EH. Thus, the received signal at the ST can be expressed as

$$y_{ST}^{\mathrm{I}} = \sqrt{P_P}\mathbf{h}_{PST}x_e + \mathbf{n}_{ST}, \quad (1)$$

where P_P represents the transmission power of the node PT, x_e denotes the unit-power energy signal, $\mathbf{n}_{ST} \sim \mathcal{CN}\left(0, \delta_{ST}\mathbf{I}\right)$ is the received additive Gaussian white noise (AWGN) with variance of δ_{ST}. For definiteness and without loss of generality, we assume $T = 1$. Thus, the amount of harvested energy at the ST can be calculated as

$$E_{ST} = \alpha\eta P_P \left\|\mathbf{h}_{PST}\right\|^2, \quad (2)$$

where $\eta \in [0,1]$ is energy conversion efficiency. Note that the amount of scavenged energy from noise is neglected because the harvested energy from the thermal noise can be negligible compared to the energy signal.

At the second phase of duration $(1-\alpha)T/2$, the PT transmits confidential signal x_P with power P_P, the received signal at the ST is thus given as

$$y_{ST}^{\mathrm{II}} = \sqrt{P_P}\mathbf{h}_{PST}x_P + \mathbf{n}_{ST}. \quad (3)$$

The achievable rate R_{ST} can be derived as

$$R_{ST} = \frac{(1-\alpha)T}{2}\log_2\left(1 + \frac{P_P\left\|\mathbf{h}_{PST}\right\|^2}{\delta_{ST}}\right). \quad (4)$$

Due to the nature of the information broadcast, the PR and eavesdropper ME can also receive the signal x_P, the received signals at the PR and ME are given as

$$\begin{aligned} y_{PR}^{\mathrm{II}} &= \sqrt{P_P}h_{PP}x_P + n_{PR}, \\ y_{ME}^{\mathrm{II}} &= \sqrt{P_P}h_{PME}x_P + n_{ME}, \end{aligned} \quad (5)$$

respectively. Here, $n_{PR} \sim \mathcal{CN}\left(0, \delta_{PR}\right)$ and $n_{ME} \sim \mathcal{CN}\left(0, \delta_{ME}\right)$ denote AWGN at PR and ME, respectively.

During the third phase $(1-\alpha)T/2$, the node ST first decodes the received primary confidential signal $\hat{x}_P$ based on DF processing, and then simultaneously forwards $\hat{x}_P$ and its own signal x_S by utilizing the beamforming vectors $\mathbf{v}_P \in \mathbb{C}^{N\times1}$ and $\mathbf{v}_S \in \mathbb{C}^{N\times1}$, respectively. Therefore, the corresponding received signal at the PR and eavesdropper ME are expressed as

$$y_{PR}^{\text{III}} = \mathbf{h}_{SPR}^{H}\mathbf{v}_{P}\hat{x}_{P} + \mathbf{h}_{SPR}^{H}\mathbf{v}_{S}x_{S} + \mathbf{n}_{PR},$$
$$y_{ME}^{\text{III}} = \mathbf{h}_{SME}^{H}\mathbf{v}_{P}\hat{x}_{P} + \mathbf{h}_{SME}^{H}\mathbf{v}_{S}x_{S} + \mathbf{n}_{PR}, \tag{6}$$

respectively. The PR attempts to retrieve $\hat{x}_P$ from y_{PR}^{III} in the presence of the secondary signal x_S. In the meanwhile, the eavesdropper also intends to intercept signal $\hat{x}_P$. Thus, the achievable rates at the PR and ME in last two phases can be expressed as

$$R_{PR} = \frac{(1-\alpha)T}{2}\log_2\left(1+\frac{P_P\left|h_{PP}\right|^2}{\delta_{PR}}+\frac{\left|\mathbf{h}_{SPR}^{H}\mathbf{v}_{P}\right|^2}{\left|\mathbf{h}_{SPR}^{H}\mathbf{v}_{S}\right|^2+\delta_{PR}}\right),$$
$$R_{ME} = \frac{(1-\alpha)T}{2}\log_2\left(1+\frac{P_P\left|h_{PME}\right|^2}{\delta_{ME}}+\frac{\left|\mathbf{h}_{SME}^{H}\mathbf{v}_{P}\right|^2}{\left|\mathbf{h}_{SME}^{H}\mathbf{v}_{S}\right|^2+\delta_{ME}}\right). \tag{7}$$

At the SR, the received signal is given by

$$y_{SR} = \mathbf{h}_{SS}^{H}\mathbf{v}_{S}x_{S} + \mathbf{h}_{SS}^{H}\mathbf{v}_{P}\hat{x}_{P} + \mathbf{n}_{SR}. \tag{8}$$

Similar to the PR, the SR treats $\hat{x}_P$ as interference and then detects the desired secondary signal x_S. The achievable rate at the SR is given by

$$R_{SR} = \frac{(1-\alpha)T}{2}\log_2\left(1+\frac{\left|\mathbf{h}_{SS}^{H}\mathbf{v}_{S}\right|^2}{\left|\mathbf{h}_{SS}^{H}\mathbf{v}_{P}\right|^2+\delta_{SR}}\right). \tag{9}$$

III. Problem Formulation and Secure Beamforming

In this section, we first define the secrecy rate of the primary system, which is a critical performance index to illustrate the transmission security of the sensitive data [31, 32], and then formulate the optimization problem with maximizing the primary secrecy rate aiming to satisfy the minimum achievable rate for the secondary system and power constraint of the relay node ST. In order to effectively obtain the optimal parameters to keep data in safety, we also propose a mathematically efficient optimization scheme to solve the problem with two-stage procedure.

A. Problem Formulation

Based on the DF cooperative communication scheme, the overall transmission rates at PR and ME equal to the minimum rate of the two-hop transmissions, respectively [32], i.e.,

$$\tilde{R}_{PR} = \min\left\{R_{ST}, R_{PR}\right\},$$
$$\tilde{R}_{ME} = \min\left\{R_{ST}, R_{ME}\right\}. \tag{10}$$

Based on the definition of [33], the secrecy rate of the primary system for the considered secrecy CRN-WPR can be expressed as

$$R_{SEC} = \left[\tilde{R}_{PR} - \tilde{R}_{ME} \right]^{+}. \tag{11}$$

Substituting the results of Equation (8) into Equation (9), the overall primary secrecy rate is then given as

$$R_{SEC} = \left[\min\left\{ R_{ST}, R_{PR} \right\} - R_{ME} \right]^{+}. \tag{12}$$

In the following, the EH ratio and secure beamforming vectors are jointly designed by maximizing the primary secrecy rate subject to the minimum achievable rate for the SR and power constraint of the ST. Mathematically, the considered optimization problem can be represent as (P1):

$$\begin{aligned}
&\max_{\alpha, \mathbf{v}_P, \mathbf{v}_S} \left[\min\left\{ R_{ST}, R_{PR} \right\} - R_{ME} \right]^{+} \\
&s.t. \\
&\mathrm{C1}: R_{SR} \ge r_S, \\
&\mathrm{C2}: \left\| \mathbf{v}_P \right\|^2 + \left\| \mathbf{v}_S \right\|^2 \le \frac{2\left(\alpha \eta P_P \left\| \mathbf{h}_{PST} \right\|^2 + E_{ST0} \right)}{1-\alpha}, \\
&\mathrm{C3}: 0 < \alpha < 1.
\end{aligned} \tag{13}$$

In (13), C1 means that the achievable rate of SR should be larger than or equal to minimum rate r_S. C2 denotes the transmission power constraint at the ST with E_{ST0} representing the initial power at the ST.

B. Optimal Secure Beamforming Design

According to the analysis of formula (13), we can observe that (P1) is a non-convex function, which is difficult to derive three optimal variables $\left(\alpha, \mathbf{v}_P, \mathbf{v}_S \right)$ concurrently. In the followings, this section proposes a mathematically efficient optimization scheme with two-stage procedure for solving the (P1):

- In the stage I, we obtain the optimal secure beamforming $\left(\mathbf{v}_P^*, \mathbf{v}_S^* \right)$ for any given energy harvesting duration α;
- In the stage II, the global optimal solution $\left(\alpha^*, \mathbf{v}_P^*, \mathbf{v}_S^* \right)$ can be found based on one-dimension search over α.

In the stage I, the maximization of the primary secrecy rate is equivalent to maximizing the achievable rate of the PR subject to an alternative upper bound on the achievable rate of ME. Thus, for a given $\alpha = \alpha_0$, $R_{ST}\left(\alpha_0 \right)$ is the constant value and the problem (P1) can be transformed into follows problem (P2):

$$\begin{aligned}
&\max_{\mathbf{v}_P,\mathbf{v}_S} \frac{(1-\alpha_0)T}{2}\log_2\left(1+\frac{P_P\left|h_{PP}\right|^2}{\delta_{PR}}+\frac{\left|\mathbf{h}_{SPR}^H\mathbf{v}_P\right|^2}{\left|\mathbf{h}_{SPR}^H\mathbf{v}_S\right|^2+\delta_{PR}}\right)\\
&s.t.\\
&\mathrm{C1}: \frac{(1-\alpha_0)T}{2}\log_2\left(1+\frac{\left|\mathbf{h}_{SS}^H\mathbf{v}_S\right|^2}{\left|\mathbf{h}_{SS}^H\mathbf{v}_P\right|^2+\delta_{SR}}\right)\geq r_S,\\
&\mathrm{C2}: \left\|\mathbf{v}_P\right\|^2+\left\|\mathbf{v}_S\right\|^2\leq\frac{2\left(\alpha_0\eta P_P\left\|\mathbf{h}_{PST}\right\|^2+E_{ST0}\right)}{1-\alpha_0},\\
&\mathrm{C3}: \frac{(1-\alpha_0)T}{2}\log_2\left(1+\frac{P_P\left|h_{PME}\right|^2}{\delta_{ME}}+\frac{\left|\mathbf{h}_{SME}^H\mathbf{v}_P\right|^2}{\left|\mathbf{h}_{SME}^H\mathbf{v}_S\right|^2+\delta_{ME}}\right)\leq\Gamma,
\end{aligned} \tag{14}$$

where Γ represents an auxiliary optimization variable to bound the achievable rate of the eavesdropper ME, thus the maximum primary secure rate can be obtained by adjusting value of Γ. The optimal value of Γ^* can be founded by one-dimension search since it is a non-negative value. Note that the optimization problem (P2) is still non-convex concerning with beamforming vectors $\mathbf{v}_P$ and $\mathbf{v}_S$.

Considering $\log_2(x)$ is monotonically increasing function of x and defining $\mathbf{H}_{SPR}=h_{SPR}h_{SPR}^H$, $\mathbf{H}_{SME}=h_{SME}h_{SME}^H$, $\mathbf{H}_{SS}=h_{SS}h_{SS}^H$, $\mathbf{V}_P=\mathbf{v}_P\mathbf{v}_P^H$, and $\mathbf{V}_S=\mathbf{v}_S\mathbf{v}_S^H$, the problem (P2) can be denoted as a fractional programming problem, but the objective function is still non-convex since two optimization variables $\mathbf{V}_P$ and $\mathbf{V}_S$ are existed in numerator and denominator of objective function, respectively. To solve the problem (P2) more effectively, the fractional programming problem can be equivalently reformulated to a convex SDR problem by utilizing Charnes-Cooper transformation [34]. Thus, we let

$$\lambda=\frac{1}{\mathrm{tr}\left(\mathbf{H}_{SPR}\mathbf{V}_S\right)+\delta_{SR}}, \tag{15}$$

while defining $\tilde{\mathbf{V}}_P=\lambda\mathbf{V}_P$ and $\tilde{\mathbf{V}}_S=\lambda\mathbf{V}_S$, the corresponding SDR of problem (P2) can be rewritten as (P3)

$$\begin{aligned}
&\max_{\mathbf{v}_P,\mathbf{v}_S,\lambda} \operatorname{tr}\left(\mathbf{H}_{SPR}\tilde{\mathbf{V}}_P\right)\\
&s.t.\\
&\text{C1}: \operatorname{tr}\left(\mathbf{H}_{SPR}\tilde{\mathbf{V}}_S\right)+\lambda\delta_{SR}=1,\\
&\text{C2}: \operatorname{tr}\left(\mathbf{H}_{SS}\tilde{\mathbf{V}}_S\right)-\Gamma_S\operatorname{tr}\left(\mathbf{H}_{SS}\tilde{\mathbf{V}}_P\right)\geq\lambda\Gamma_S\delta_{SR},\\
&\text{C3}: \operatorname{tr}\left(\tilde{\mathbf{V}}_P\right)+\operatorname{tr}\left(\tilde{\mathbf{V}}_S\right)\leq\frac{2\lambda\left(\alpha_0\eta P_P\left\|\mathbf{h}_{PST}\right\|^2+E_{ST0}\right)}{1-\alpha_0}\\
&\text{C4}: \operatorname{tr}\left(\mathbf{H}_{SME}\tilde{\mathbf{V}}_P\right)-\Gamma_e\operatorname{tr}\left(\mathbf{H}_{SME}\tilde{\mathbf{V}}_S\right)\leq\lambda\Gamma_e\delta_{ME},\\
&\text{C5}: \tilde{\mathbf{V}}_P\succeq 0,\tilde{\mathbf{V}}_S\succeq 0,\lambda>0,
\end{aligned} \tag{16}$$

where $\Gamma_S=2^{\frac{2r_S}{1-\alpha_0}}-1$ and $\Gamma_e=2^{\frac{2\Gamma}{1-\alpha_0}}-\frac{P_P\left|h_{PME}\right|^2}{\delta_{ME}}-1$.

It must be noted that SDR cannot guarantee to derive the optimal solution $\left(\mathbf{v}_P^*,\mathbf{v}_S^*\right)$ with rank-one. In the followings, the first step is to prove that the rank of optimal $\tilde{\mathbf{V}}_P^*$ equals to one, then we propose a method to structure the optimal $\tilde{\mathbf{V}}_S^*$ with rank-one when the rank of $\tilde{\mathbf{V}}_S$ is greater than one.

Let θ_1, θ_2, θ_3, and θ_4 represents the Lagrange multipliers, i.e., dual variables, related to constraints C1 to C4 in Equation (16), respectively. Thus, the corresponding Lagrange function of problem (P3) can be expressed as

$$\mathcal{L}\left(\tilde{\mathbf{V}}_P,\tilde{\mathbf{V}}_S,\theta_1,\theta_2,\theta_3,\theta_4\right)=\operatorname{tr}\left(\xi\tilde{\mathbf{V}}_P\right)+\operatorname{tr}\left(\psi\tilde{\mathbf{V}}_P\right)+\rho, \tag{17}$$

where

$$\xi=\mathbf{H}_{SPR}-\theta_2\Gamma_S\mathrm{H}_{SS}-\theta_3\mathbf{I}-\theta_4\mathbf{H}_{SME}, \tag{18}$$

$$\psi=-\theta_1\mathbf{H}_{SPR}+\theta_2\mathrm{H}_{SS}-\theta_3\mathbf{I}+\theta_4\Gamma_e\mathbf{H}_{SME}, \tag{19}$$

and ρ denotes the residual information that is not related for the proof. According to the definition of Karush-Kuhn-Tucker conditions and Lagrange function of problem (P3), we thus have

$$\xi^*\tilde{\mathbf{V}}_P^*=0,\psi^*\tilde{\mathbf{V}}_S^*=0. \tag{20}$$

Assuming the harvested energy and initial energy are all used for secure beamforming transmission in the third phase, the power constraint C3 in Equation (16) is activated with equality, thus the dual variable $\theta_3^*>0$. Since the transmission channel vectors $\mathbf{H}_{SS}\succeq 0$ and $\mathbf{H}_{SME}\succeq 0$, we can derive that $\operatorname{rank}\left(-\theta_2^*\Gamma_S\mathbf{H}_{SS}-\theta_3^*\mathbf{I}-\theta_4^*\mathbf{H}_{SME}\right)=N$. Furthermore, since

$\mathrm{rank}\left(\mathbf{H}_{SPR}\right) \le 1$, it follows that $\mathrm{rank}\left(\xi^*\right) \ge N-1$. Based on Equation (20), we thus obtain $\mathrm{rank}\left(\tilde{\mathbf{V}}_P^*\right)=1$.

Define $\kappa^* = -\theta_1^* \mathbf{H}_{SPR} - \theta_2^* \mathbf{H}_{SS} - \theta_3^* \mathbf{I} + \theta_4^* \mathbf{H}_{SME}$, thus we have

$$\psi^* = \kappa^* + 2\theta_2^* \mathbf{H}_{SS}. \tag{21}$$

Since $\mathbf{H}_{SPR} \succeq 0$, $\mathbf{H}_{SS} \succeq 0$, and $\mathbf{H}_{SME} \succeq 0$, we can obtain that $\mathrm{rank}\left(-\theta_1^* \mathbf{H}_{SPR} - \theta_2^* \mathbf{H}_{SS} - \theta_3^* \mathbf{I}\right) = N$. Moreover, since $\mathrm{rank}\left(\mathbf{H}_{SME}\right) \le 1$, it can be derived that $\mathrm{rank}\left(\kappa^*\right) \ge N-1$.

- If $\mathrm{rank}\left(\kappa^*\right)=N$, we can obtain that $\mathrm{rank}\left(\psi^*\right)=N-1$, thus it follows from Equation (20) that $\mathrm{rank}\left(\tilde{\mathbf{V}}_S^*\right)=1$ and $\tilde{\mathbf{V}}_S^*$ is equal to aww^H, where $w \in \mathbb{C}^{N\times 1}$ denotes the spanning null space of ψ^* and $a>0$. Thus, the corresponding optimal value of (P3) is $\left(\tilde{\mathbf{V}}_P^*/\lambda^*, \tilde{\mathbf{V}}_S^*/\lambda^*\right)$;
- If $\mathrm{rank}\left(\kappa^*\right)=N-1$, we can observe that $\mathrm{rank}\left(\tilde{\mathbf{V}}_S^*\right)>1$ and thus it requires constructing a new solution with rank-one. First, we obtain the orthonormal basis $u \in \mathbb{C}^{N\times 1}$ of the null base of κ^*, which is defined as $\kappa^* u=0$ and $\mathrm{rank}\left(u\right)=1$. Then, based on the expression of κ^*, we can further derive that $\mathbf{H}_{SS} u = 0$. Thus, the optimal solution of $\tilde{\mathbf{V}}_S^*$ is given by

$$\tilde{\mathbf{V}}_S^* = buu^H + aww^H, \tag{22}$$

where $b \ge 0$, $\|w\|=1$, and $w^H u=0$. Finally, the optimal result of $\hat{\mathbf{V}}_S^*$ with rank-one can be rewritten as $\hat{\mathbf{V}}_S^* = \tilde{\mathbf{V}}_S^* - buu^H$. Thus, the reconstructed optimal solution for (P3) is $\left(\tilde{\mathbf{V}}_P^*/\lambda^*, \hat{\mathbf{V}}_S^*/\lambda^*\right)$.

For fixed $\alpha=\alpha_0$, the optimal solutions $\left(\Gamma^*, \tilde{\mathbf{V}}_P^*, \tilde{\mathbf{V}}_S^*\right)$ can be obtained through one-dimension search Γ based on the following equation

$$\left(\Gamma^*, \mathbf{V}_P^*, \mathbf{V}_S^*\right) = \arg\max_{\alpha=\alpha_0} \mathrm{problem}\left(\mathrm{P3}\right), \tag{23}$$

thus the optimal secure beamforming vectors $\left(\mathbf{v}_P^*, \mathbf{v}_S^*\right)$ can be obtained by adopting eigenvalue decomposition (EVD) of $\tilde{\mathbf{V}}_P^*/\lambda^*$ and $\tilde{\mathbf{V}}_S^*/\lambda^*$.

In order to obtain the global optimal solution for problem (P1) in the second stage, one-dimension search related to α is then utilized. The optimal solution is chosen from the following equation

$$\left(\alpha^*, \Gamma^*, \mathbf{v}_P^*, \mathbf{v}_S^*\right) = \arg\max_{\alpha\in(0,1)} \mathrm{problem}\left(\mathrm{P1}\right). \tag{24}$$

The whole algorithm process can be described as follows:

Algorithm 1 Optimal Secure Beamforming Design

Initialize $\alpha = \alpha_0$ and $\Gamma = \Gamma_0$; Define $\Gamma_{\max}$ as a large positive real number, $\Delta\alpha$ and $\Delta\tau$ are all small positive real numbers as the iterative steps for one-dimension search.

1: **for** a given $\alpha = \alpha_0$ **do** S1-S4

2: S1: Given $\Gamma = \Gamma_0$, then solve problem (P3) and derive the optimal solution $\left(\tilde{\mathbf{V}}_P^*, \tilde{\mathbf{V}}_S^*, \lambda^*\right)$ by utilizing CVX tools;

3: S2: Obtain optimal $\left(\tilde{\mathbf{V}}_P^*, \tilde{\mathbf{V}}_S^*\right)$ through the following procedures;

4: **if** $\text{rank}\left(\tilde{\mathbf{V}}_P^*\right) = 1$ and $\text{rank}\left(\tilde{\mathbf{V}}_S^*\right) = 1$, **then**

5: The optimal solution for problem (P3) is $\left(\tilde{\mathbf{V}}_P^* / \lambda^*, \tilde{\mathbf{V}}_S^* / \lambda^*\right)$;

6: **else**

7: Reconstruct an optimal solution $\left(\tilde{\mathbf{V}}_P^* / \lambda^*, \hat{\mathbf{V}}_S^* / \lambda^*\right)$ for problem (P3) with $\text{rank}\left(\tilde{\mathbf{V}}_P^*\right) = 1$ and $\text{rank}\left(\hat{\mathbf{V}}_S^*\right) = 1$ based on Equation (22);

8: **end if**

9: S3: **Let** $\Gamma = \Gamma + \Delta\tau$ when $\Gamma < \Gamma_{\max}$ and then go to S1-S2;

10: S4: **Choose** the optimal solution $\left(\Gamma^*, \mathbf{V}_P^*, \mathbf{V}_S^*\right)$ from Equation (23) and derive optimal secure beamforming vectors $\left(\mathbf{V}_P^*, \mathbf{V}_S^*\right)$ by performing EVD.

11: **end for**

12: **Update** $\alpha = \alpha + \Delta\alpha$ and S1-S4;

Choose the optimal solution $\left(\alpha^*, \Gamma^*, \mathbf{v}_P^*, \mathbf{v}_S^*\right)$ based on Equation (24).

C. Secure Beamforming based on Zero-forcing Rule

This section investigates another secure beamforming solution based on Zero-forcing (ZF) rule as a benchmark, which the primary transmission will not be interfered by other transmissions. Therefore, based on the criterion of ZF rule [35], the beamforming vectors $\mathbf{v}_{S,ZF}$ and $\mathbf{v}_{P,ZF}$ for the primary and secondary systems should be in the null space of $\mathbf{h}_{SPR}^{\perp}$ and $\mathbf{h}_{SS}^{\perp}$, respectively, i.e., $\mathbf{h}_{SPR}^H \mathbf{v}_{S,ZF} = 0$ and $\mathbf{h}_{SS}^H \mathbf{v}_{P,ZF} = 0$. Since there exists an eavesdropper in the system to listen the primary's confidential information, so that the beamforming $\mathbf{v}_{P,ZF}$ should also be in the null space of $\mathbf{h}_{SME}^{\perp}$, i.e., $\mathbf{h}_{SME}^H \mathbf{v}_{P,ZF} = 0$. In order to be fair in secondary transmission power, we further define $\mathbf{v}_{P,ZF} = \sqrt{\beta P_{ST}}\, \hat{\mathbf{v}}_{P,ZF}$ and $\mathbf{v}_{S,ZF} = \sqrt{(1-\beta) P_{ST}}\, \hat{\mathbf{v}}_{S,ZF}$ with $\hat{\mathbf{v}}_{P,ZF}^H \hat{\mathbf{v}}_{P,ZF} = 1$ and $\hat{\mathbf{v}}_{S,ZF}^H \hat{\mathbf{v}}_{S,ZF} = 1$, where β represents the power allocation coefficient and $P_{ST}=2\left(\alpha\eta P_P\left\|\mathbf{h}_{PST}\right\|^2+E_{ST0}\right)\big/\left(1-\alpha\right)$ denotes the secondary transmission power. Based on Equations (13) and (14), the optimization problem based on ZF rule can be formulated as (P4):

$$\begin{aligned}
&\max_{\hat{\mathbf{v}}_{P,ZF},\hat{\mathbf{v}}_{S,ZF}} \frac{(1-\alpha)T}{2}\log_2\left(1+\frac{P_P\left|h_{PP}\right|^2+\beta P_{ST}\left|\mathbf{h}_{SPR}^H\hat{\mathbf{v}}_{P,ZF}\right|^2}{\delta_{PR}}\right)\\
&s.t.\\
&\mathrm{C1}: \frac{(1-\alpha)T}{2}\log_2\left(1+\frac{(1-\beta)P_{ST}\left|\mathbf{h}_{SS}^H\hat{\mathbf{v}}_{S,ZF}\right|^2}{\delta_{SR}}\right)\geq r_S,\\
&\mathrm{C2}: \frac{(1-\alpha)T}{2}\log_2\left(1+\frac{P_P\left|h_{PME}\right|^2}{\delta_{ME}}\right)\leq\Gamma,\\
&\mathrm{C3}: \mathbf{h}_{SPR}^H\hat{\mathbf{v}}_{S,ZF}=0, \mathbf{h}_{SS}^H\hat{\mathbf{v}}_{P,ZF}=0, \mathbf{h}_{SME}^H\hat{\mathbf{v}}_{P,ZF}=0,\\
&\mathrm{C4}: 0<\alpha<1.
\end{aligned} \tag{25}$$

Based on the objective function of the optimization problem (P4), we can observe that the optimal $\hat{\mathbf{v}}_{P,ZF}$ should maximize the primary transmission rate under the constraint C3. Thus, the optimal $\mathbf{v}_{P,ZF}$ can be obtained by utilizing the following optimization problem:

$$\begin{aligned}
&\max_{\mathbf{v}_{P,ZF}}\left|\mathbf{h}_{SPR}^H\hat{\mathbf{v}}_{P,ZF}\right|^2\\
&s.t.\quad \mathbf{h}_{SS}^H\hat{\mathbf{v}}_{P,ZF}=0, \mathbf{h}_{SME}^H\hat{\mathbf{v}}_{P,ZF}=0,
\end{aligned} \tag{26}$$

Since both the constraint functions in Equation (26) include $\hat{\mathbf{v}}_{P,ZF}$, we thus can define a new matrix $\mathbf{H}_S=\left[\mathbf{h}_{SS}^H;\mathbf{h}_{SME}^H\right]$ and the constraint function can be rewritten as $\mathbf{H}_S\hat{\mathbf{v}}_{P,ZF}=0$. To satisfy the new constraint, $\hat{\mathbf{v}}_{P,ZF}$ can be obtained by solving the orthogonal value of $\mathbf{H}_S$, which means that $\hat{\mathbf{v}}_{P,ZF}$ should be the null space of $\mathbf{H}_S$. To obtain the maximization of $\left|\mathbf{h}_{SPR}^H\hat{\mathbf{v}}_{P,ZF}\right|^2$, the optimal $\hat{\mathbf{v}}_{P,ZF}^*$ should be chosen the one which is in the direction of the orthogonal projection of $\mathbf{h}_{SPR}^H$ on to the subspace $\mathbf{H}_S^\perp$, where the optimal $\hat{\mathbf{v}}_{P,ZF}^*$ is given by

$$\hat{\mathbf{v}}_{P,ZF}^*=\frac{\left(\mathbf{I}-\dfrac{\mathbf{H}_S\mathbf{H}_S^H}{\left\|\mathbf{H}_S\right\|^2}\right)\mathbf{h}_{SPR}}{\left\|\left(\mathbf{I}-\dfrac{\mathbf{H}_S\mathbf{H}_S^H}{\left\|\mathbf{H}_S\right\|^2}\right)\mathbf{h}_{SPR}\right\|}. \tag{27}$$

Similarly, the optimal $\hat{\mathbf{v}}_{S,ZF}^*$ can be derived by analyzing the constraint function $\mathbf{h}_{SPR}^H\hat{\mathbf{v}}_{S,ZF}=0$ in Equation (25), where the $\hat{\mathbf{v}}_{S,ZF}^*$ should be the null space of $\mathbf{h}_{SPR}^\perp$, i.e., $\hat{\mathbf{v}}_{S,ZF}^*$

belongs to the subspace $\mathbf{h}_{SPR}^{\perp}$. Here, we try to maximize the $\left|\mathbf{h}_{SS}^{H}\hat{\mathbf{v}}_{S,ZF}\right|^{2}$ so that more ST's transmission power can be used to transfer primary data to effectively ensure the secure transmission of information in the primary system. Therefore, the optimal $\hat{\mathbf{v}}_{S,ZF}^{*}$ can be derived as

$$\hat{\mathbf{v}}_{S,ZF}^{*}=\frac{\left(\mathbf{I}-\frac{\mathbf{h}_{SPR}\mathbf{h}_{SPR}^{H}}{\left\|\mathbf{h}_{SPR}\right\|^{2}}\right)\mathbf{h}_{SS}}{\left\|\left(\mathbf{I}-\frac{\mathbf{h}_{SPR}\mathbf{h}_{SPR}^{H}}{\left\|\mathbf{h}_{SPR}\right\|^{2}}\right)\mathbf{h}_{SS}\right\|}. \tag{28}$$

According to (25), we can find that the objective function is an increasing function while C1 is a decreasing function with the increase of β, we can obtain the optimal β^{*} through deriving the upper-bound of β. Therefore, the optimal β^{*} can be expressed as

$$\beta^{*}=1-\delta_{SR}\left(\frac{2^{\frac{2r_S}{(1-\alpha)T}}-1}{P_{ST}\left|\mathbf{h}_{SS}^{H}\hat{\mathbf{v}}_{S,ZF}^{*}\right|^{2}}\right). \tag{29}$$

Then, the optimal energy harvesting duration α^{*} and Γ^{*} can be derived by adopting one-dimension search.

IV. Simulations and Analyses of Security Transmission Performance

In this section, we will verify security transmission performance of the primary and transmission efficiency of secondary system by comparing the proposed scheme and ZF-based scheme. Unless stated otherwise, we assume that all noise power are normalized to unity, i.e., $\delta_{PR}=\delta_{SR}=\delta_{ME}=1$. We also consider a scenario where the transmission distance between the PT and PR is 8 m, while the distance between the ST and SR is 3 m. Moreover, the ST is equipped with 4 antennas and the energy harvesting efficiency is set as η=0.5 . The transmission channel can be modeled as $h=d^{-\frac{\varpi}{2}}e^{jw}$ with d and ϖ=3.5 denoting the distance and path loss exponent, respectively [36]. The minimum transmission rate of the secondary system and maximal auxiliary optimization variable are set to be r_S=0.5 bit/s/Hz and $\Gamma_{\max}$=1.0 bit/s/Hz, respectively.

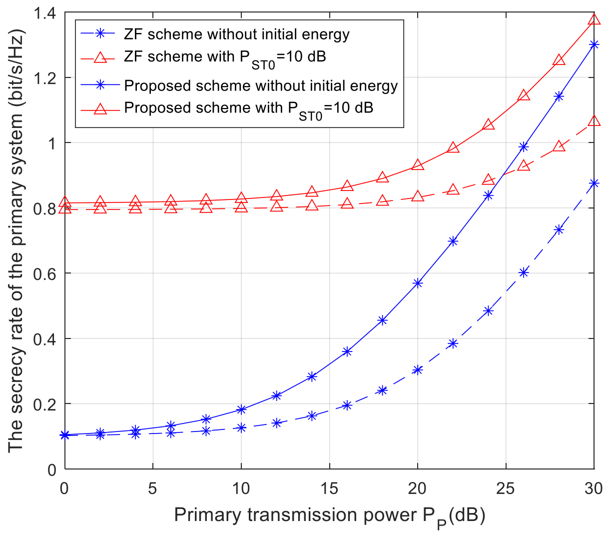

Figure 2: The secrecy rate of the primary system with respect to the primary transmission power P_P for different initial energy at the ST. The antenna number N=4, d_{PST}=4 m, d_{SPR}=d_{PP}-d_{PST}, d_{PME}=d_{PP}.

Figure 2 illustrates the secrecy rate of the primary system with respect to the primary transmission power for different initial energy at the ST. In this figure, both the secrecy rates of the primary system with proposed scheme and ZF scheme are improved with the increase of primary transmission power, respectively. Moreover, the proposed scheme outperforms the ZF scheme in terms of the primary's secrecy rate. With the lower primary transmission power, the superiority of the proposed scheme is obviously and the primary secrecy rates with both schemes are close in high primary transmission power. With the increase of the initial energy at the ST, the secrecy rate gets better as shown in Figure 2 since the more transmission power will be utilized to assist the transmission of the primary signals.

Figure 3 compares the secrecy rates of the primary system with proposed scheme and ZF scheme against the antenna number at the ST. Obviously, with the increase of the antenna number, the secrecy rates gets better continually since more antenna will result in a higher spatial reuse efficiency. Similarly, the primary secrecy rate is always high for the proposed scheme.

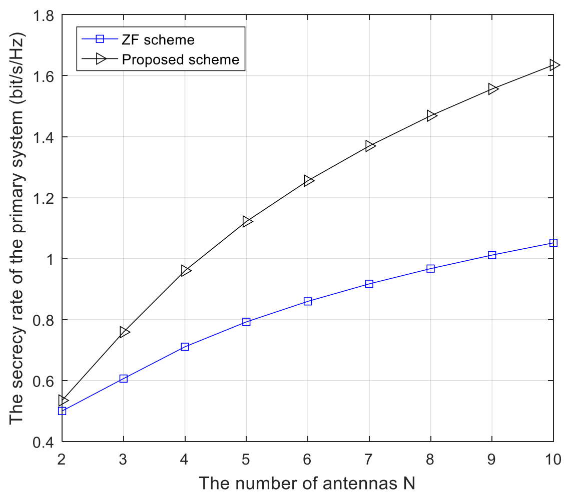

Figure. 3: The secrecy rate of the primary system with respect to the number of antenna at the ST. P_P=10dB, P_{ST0}=0dB. d_{PST}=4 m, d_{SS}=2 m, d_{SPR}=d_{PP}-d_{PST}, d_{SME}=d_{SPR}, d_{PME}=d_{PP}.

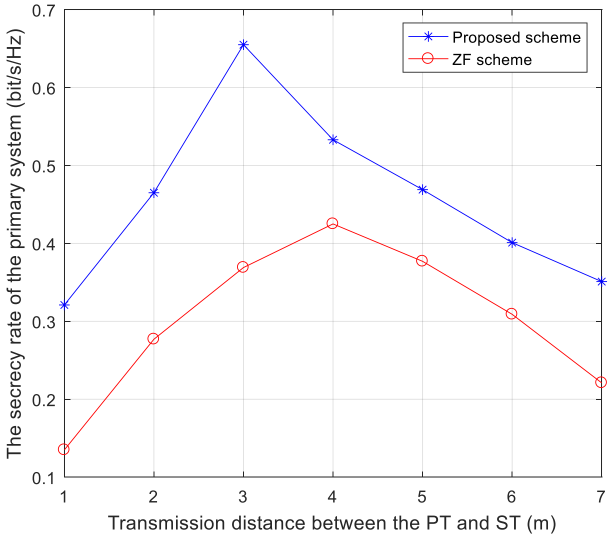

Figure. 4: The secrecy rate of the primary system with respect to the distance between the PT and ST. P_P=10dB, P_{ST0}=0dB, d_{SS}=2 m, d_{SPR}=d_{PP}-d_{PST}, d_{SME}=d_{SPR}, d_{PME}=d_{PP}. The antenna number N=4.

Figure 4 shows the primary secrecy rates with the proposed scheme and ZF scheme against the transmission distance between the PT and ST. From this figure, we can observe that the proposed scheme is superiority to the ZF scheme in term of the primary secrecy rate, regardless the position of the ST. With the increase of the d_{PST}, the primary secrecy rates first become better and then become worse. When the transmission distance d_{PST} is short, the secrecy rates get better with the increase of the d_{PST} because the more energy will be harvested for signal transmission and shorter distance for primary signal transferring. However, when the distance d_{PST} is longer, the secrecy rates get worse since the amount of harvested energy will be decreased and more path-loss will result in a negative effect for the ST to process the PT's signal. Furthermore, we can obtain that the optimal positions of the ST are roughly 3m and 4m for the proposed scheme and ZF scheme, respectively.

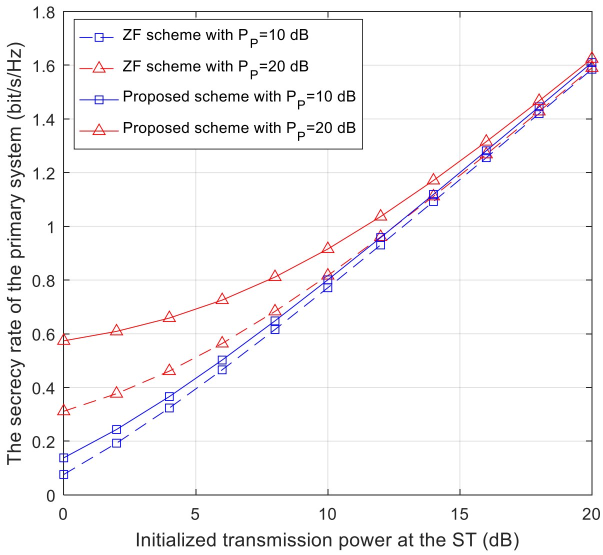

Figure. 5: The secrecy rate of the primary system with respect to the initialized transmission power P_{ST0} at the ST for different primary transmission power P_P. d_{PST}=4 m, d_{SS}=2 m, d_{SPR}=d_{PP}-d_{PST}, d_{SME}=d_{SPR}, d_{PME}=d_{PP}. The antenna number N=4.

The Figure 5 shows the secrecy rate of the primary system corresponding to the ST's initial energy for different primary transmission power. In this figure, we can observe that the secrecy rates of the primary system with both the schemes are close with the increase of the ST's initial energy, which further illustrates the proposed scheme is superior to the ZF scheme. Specifically, the proposed scheme outperforms the ZF scheme in a lower primary power range. However, in the higher initial primary power range, the gap of the secrecy rates of the primary system between the proposed scheme and the ZF scheme gets small. Therefore, the proposed scheme in this paper is more effective when the initial energy is small.

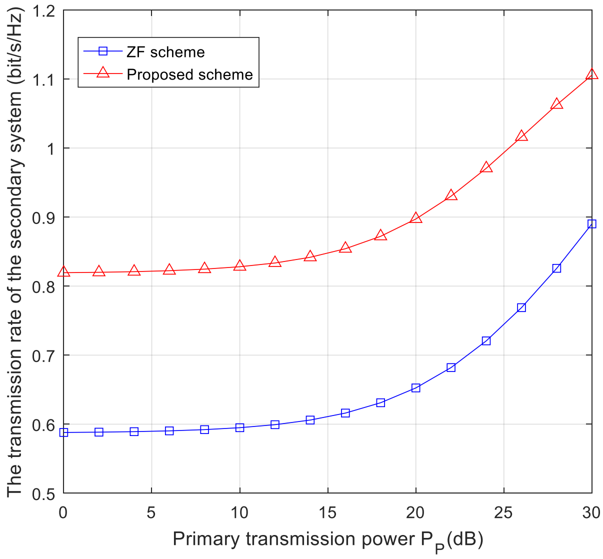

Figure. 6: The transmission rate of the secondary system with respect to the primary transmission power P_P. P_{ST0}=10dB. d_{PST}=4 m, d_{SS}=2 m, $d_{SPR}=d_{PP}-d_{PST}$, $d_{SME}=d_{SPR}$, $d_{PME}=d_{PP}$. The antenna number N=4.

Figure 6 shows the achievable rate of the secondary system with respect to the primary transmission power. From the figure, the throughput of the secondary system with both the scheme are enhanced with the increase of the primary transmission power, which because of more energy will be harvested for the signal transmission. In the meanwhile, the propose scheme outperforms the ZF scheme, which verifies the effectiveness of the proposed scheme.

V. Conclusions

This paper studied the secure transmission problem for the cognitive radio-based IoMT with energy harvesting when the sensitive medical data send from the PT can be listened by a malicious eavesdropper. For the sake of protecting the security of the sensitive data, we formula the corresponding optimization problem and propose a novel algorithm for jointly designing optimal EH duration and secure beamforming vectors to maximizing the primary secrecy transmission rate while ensuring the transmission requirement of the secondary system. In fact, the number of eavesdroppers may usually more than one, the proposed scheme still can be utilized to obtain optimized beamforming vectors. The numerical results presents excellent secure transmission performance with proposed scheme than zero-forcing scheme, which can be implemented into the IoMT devices to effectively protect the security of the sensitive data.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

The authors thank the Research Foundation of China Postdoctoral Science Foundation under Grant No.2019M652895, in part by the Research Foundation of Education Department of Hunan Province under Grant No.18B517, and in part by the Teaching Reform Research Project of Hunan University of Science and Engineering under Grant No.XKYJ2018023, and in part by the Construct Program of Applied Characteristic Discipline in Hunan University of Science and Engineering.

Acknowledgements

Not applicable

References

[1] C. Zhu, V.C.M. Leung, L. Shu, et al., "Green Internet of Things for smart world," *IEEE Access*, vol. 3, pp. 2151–2162, 2015.

[2] K. Zhang, J. Ni, K. Yang, et al., "Security and privacy for smart city applications: Challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[3] J. Ni, K. Zhang, X. Lin, et al., "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[4] F. Montori, L. Bedogni, and L. Bononi, "A collaborative Internet of Things architecture for smart cities and environmental monitoring," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 592–605, 2018.

[5] S. Dhingra, R.B. Madda, A.H. Gandomi, et al., "Internet of Things Mobile-Air pollution monitoring system," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5577–5584, 2019.

[6] W. Tang, J. Ren, and Y. Zhang, "Enabling trusted and privacy-preserving healthcare services in social media health networks", *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 579–590, 2019.

[7] W. Tang, J. Ren, K. Deng, et al.,: Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives, *IEEE Internet of Things Journal*, accepted, 2019.

[8] W. Tang, J. Ren, K. Zhang, et al.,: Efficient and privacy-preserving fog-assisted health data sharing scheme, *ACM Transactions on Intelligent Systems and Technology*, accepted, 2019.

[9] F. Alsubaei, S. Shiva, and A. Abuhussein, "Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment," *42nd IEEE Conference on Local Computer Networks Workshops*, pp. 112–120, 2015.

[10] Federal Communications Comission, "In the Matter of Unlicensed Operation in the TV Broadcast Bands: Second Report and Order and Memorandum Opinion and Order", FCC 08-260, Nov. 2008.

[11] M. Sharma and A. Sahoo, "Stochastic model based opportunistic channel access in dynamic spectrum access networks", *IEEE Transactions on Mobile Computing*, vol. 13, no. 7, pp. 1625–1639, 2014.

[12] N. Zhang, H. Liang, N. Chen, et al., "Dynamic spectrum access in multichannel cognitive radio networks", *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2053–2064, 2014.

[13] D. Jiang, Y. Wang, C. Yao, et al., "An effective dynamic spectrum access algorithm for multi-hop cognitive wireless networks", *Computer Networks*, vol. 84, pp. 1–16, 2015.

[14] C. Wang, J. Li, Y. Yang, et al., "Combing solar energy harvesting with wireless charging for hybrid wireless sensor networks", *IEEE Transactions on Mobile Computing*, vol. 17, no. 3, pp. 560–576, 2018.

[15] I. Ahmed, M.M. Butt., C. Psomas, et al., "Survey on energy harvesting wireless communications: Challenges and opportunities for radio resource allocation", *Computer Networks*, vol. 88 , pp. 234–248, 2015.

[16] H. Chen, C. Zhai, Y. Li, et al., "Cooperative strategies for wireless-powered communications: An overview", *IEEE Wireless Communications*, vol. 25, no. 4, pp. 112–119, 2018.

[17] K. Tang, R. Shi, and J. Dong, "Throughput analysis of cognitive wireless acoustic sensor networks with energy harvesting", *Future Generation Computer Networks*, vol. 86, pp. 1218–1227, 2018.

[18] Y. Zhang, C. Xu, X. Lin, et al., "Blockchain-based public integrity verification for cloud storage against procrastinating auditors", IEEE Transactions on Cloud Computing, early access, 2019.

[19] Mamta and S. Prakash, "An overview of healthcare perspective based security issues in wireless sensor networks", *3rd International Conference on Computing for Sustainable Global Development*, pp. 870–875, 2016.

[20] H. Chen, Y. Li, Y. Jiang, et al., "Distributed power splitting for SWIPT in relay interference channels using game theory", *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 410–420, 2015.

[21] W. Lu, W. Zhao, S. Hu, et al., "OFDM based SWIPT for two-way AF relaying network", *IEEE Access*, vol. 6, pp. 73223–73231, 2018.

[22] L.Shi, Y. Ye, R-Q. Hu, et al., "Energy efficiency maximization for SWIPT enabled two-way DF relaying", *IEEE Signal Processing Letters*, vol. 26, no. 5, pp. 755–759, 2019.

[23] Z. Yan, S. Chen, X. Zhang, et al., "Outage performance analysis of wireless energy harvesting relay-assisted random underlay cognitive networks", *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2691–2699, 2018.

[24] S. Aslam, W. Ejaz, and M. Ibnkahla, "Energy and spectral efficient cognitive radio sensor networks for Internet of Things", *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3220–3233, 2018.

[25] Y. Zhang, C. Xu, H. Li, et al., "HealthDep: An efficient and secure deduplication scheme for cloud-assisted eHealth systems", IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 4101-4112, 2018.

[26] D.S. Gurjar, H.H. Nguyen, and H.D. Tuan, "Wireless information and power transfer for IoT applications in overlay cognitive radio networks", *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3257–3270, 2019.

[27] H.A.B. Salameh, S. Almajali, M. Ayyash, et al., "Spectrum assignment in cognitive radio networks for Internet-of-Things delay-sensitive applications under jamming attacks", *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1904–1913, 2018.

[28] Y. Huo, M. Xu, X. Fan, et al., "A novel secure relay selection strategy for energy-harvesting-enabled Internet of things", *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, pp. 1–18, 2018.

[29] Z. Wang, Z. Chen, B. Xia, et al., "Cognitive relay networks with energy harvesting and information transfer: Design, analysis, and optimization", *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2562–2576, 2016.

[30] A. Mukherjee, T. Acharya, and M.R.A. Khandaker, "Outage analysis for SWIPT-enabled two-way cognitive cooperative communications", *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 9032–9036, 2018.

[31] C. Zhai, J. Liu, and L. Zheng, "Relay-based spectrum sharing with secondary users powered by wireless energy harvesting", *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 1875–1887, 2016.

[32] C. Tang, G. Pan, and T. Li, “Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels”, *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 609–612, 2014.

[33] X. Chen, J. Chen, and T. Liu, “Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization”, *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8025–8035, 2016.

[34] Wu. W, B. Wang, Y. Zeng, et al., “Robust secure beamforming for wireless powered full-duplex systems with self-energy recycling”, *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10055–10069, 2017.

[35] G. Zhang, I. Krikidis, and B. Ottersten, “Full-duplex cooperative cognitive radio with transmit imperfections”, *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2498–2511, 2013.

[36] G. Zhang, H.Z. Jorswieck, and B. Ottersten, “Information and energy cooperation in cognitive radio networks”, IEEE Transactions on Signal Processing, vol. 62, no. 9, pp. 2290–2303, 2014.