Beamforming Design for Physical Layer Security in a Two-Way Cognitive Radio IoT Network with SWIPT

Zhishan Deng, Quanzhong Li, Qi Zhang, *Member, IEEE,* Liang Yang, and Jiayin Qin

***Abstract*—In this paper, we study the secure beamforming design for a two-way cognitive radio (CR) Internet of Things (IoT) network aided with simultaneous wireless information and power transfer (SWIPT). Located at the center of secondary network, the IoT controller helps to provide relay assistance and cooperative physical layer security (PLS) for two primary users (PUs) against an eavesdropper, while transmitting information and power to the other IoT devices (IoDs) with primary spectrum. To enhance the information security, we aim to maximize the secrecy sum rate for PUs by jointly designing the beamforming matrix and vectors at the central controller. To efficiently solve the non-convex problem, we first propose the branch-reduce-and-bound (BRB)-based algorithm to obtain an upper bound for the secrecy sum rate and offer a feasible solution by Gaussian randomization, which demands two-level iteration and thus has high complexity. To strike a balance between the complexity and the performance, we then propose iterative algorithm based on constrained-convex-concave programming (CCCP) and a zero forcing (ZF)-based non-iterative algorithm, the latter of which with lowest complexity is suitable for the central controller with limited-power supply. Simulation results are provided to demonstrate the effectiveness of our proposed optimization algorithms in comparison to the traditional schemes.**

***Index Terms*—Internet of Things (IoT), two-way cognitive radio, physical layer security (PLS), secrecy sum rate (SSR), secure beamforming design, optimization algorithms.**

I. Introduction

WITH the recent advancement of the fifth-generation (5G) technology, Internet of Things (IoT) is now emerging as an innovative paradigm, which enables various surrounding physical objects such as controllers, sensors and mobile phones to be connected through a communication network for information exchange [1], [2]. Moreover, the applications of future IoT become multi-functional and ubiquitous, which acts as a key enabler for smart cities, wearable electronics, smart grids, intelligent transportation and environmental monitoring, etc. In practice, the reliable IoT deployment is expected to face some fundamental challenges [3], [4], i.e., energy limitation, information security and spectrum scarcity, which we focus on and address in this paper.

IoT device (IoD) generally has a battery with limited capacity [5], which is not adequate to maintain the long-term operation. However, it's not sensible to frequently charge or replace the battery of IoD since it will lead to higher cost when the number of IoDs is massive. To overcome the limited battery life, researchers in [6]–[9] have introduced the simultaneous wireless information and power transfer (SWIPT) technology [10]–[12] into IoT networks. SWIPT is a promising energy harvesting (EH) technique, which enables the IoD to harvest energy from the received radio frequency (RF) signal and convert it into direct current form to store in the battery. Specifically, the sum rate maximization problem was studied in the downlink SWIPT-aided IoT network [6], [7], where multiple EH-enabled IoDs were involved. To further explore the energy issues in the SWIPT-aided IoT network, the energy efficiency (EE) maximization problem was investigated in [8] and [9] with consideration of different antenna configuration. However, these works merely concentrated on improving the performance of SWIPT-aided IoT in terms of different metrics, without focusing on the critical secrecy issues.

Communication security and privacy protection are significantly important for wireless network like IoT. Since the broadcast nature of electromagnetic propagation makes IoT communications vulnerable to eavesdropping attacks, the secrecy transmission schemes need to be specially considered when designing such systems [13]. Different from the conventional cryptographic techniques which have inherent difficulties in secret key management [14], physical layer security (PLS) exploits a promising solution for secure IoT communication by exploring physical properties of wireless channels [15]–[17]. The wire-tap channel was initiated by Wyner in 1975 [18], which laid the foundation for PLS techniques. In [15], the authors mainly proposed jamming

This work was supported in part by the National Natural Science Foundation of China under Grant 61802447, Grant 61671160 and Grant 61672549, in part by the Guangdong Natural Science Foundation under Grant 2014A030310374 and Grant 2018B0303110016, in part by the Department of Education of Guangdong Province under Grant 2016KZDXM050, in part by the Hunan Natural Science Foundation under Grant 2019JJ40043, in part by the Science and Technology Program of Guangzhou under Grant 201904010249 and Grant 201804010445, and in part by the Fundamental Research Funds for the Central Universities. *(Corresponding author: Quanzhong Li.)*

Z. Deng and Q. Zhang are with the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China (e-mail: dengzhsh3@mail2.sysu.edu.cn; zhqi26@mail.sysu.edu.cn).

Q. Li is with the School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China (e-mail: liquanzh@mail.sysu.edu.cn).

L. Yang is with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China (e-mail: liangyang.guangzhou@gmail.com).

J. Qin is with the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China, and also with the Xinhua College of Sun Yat-sen University, Guangzhou 510520, China (e-mail: issqjy@mail.sysu.edu.cn).

scheme to counteract eavesdropping considering perfect and imperfect channel state information (CSI). Furthermore, cooperative jamming (CJ) and harvest-and-jam relaying protocol were proposed in [16] to study PLS in wireless powered communication networks, where the secrecy rate maximization problem was formulated. Representative PLS techniques towards IoT applications presented in [17] include artificial noise (AN) injection [19], multi-antenna transmission [20] and cooperative secrecy scheme [21]. There have been a few works on IoT from the perspective of PLS [22]–[24]. To enhance the secrecy of uplink transmission in the cellular IoT, a full-duplex base station jamming scheme was proposed in [22], which required low power consumption at IoT terminals.

AN-aided beamforming scheme was combined with CJ to combat against eavesdroppers for downlink transmission, where the secrecy outage probability was investigated [23]. In [24], zero-forcing beamforming and AN technique were incorporated in a multi-user IoT downlink network, where the secrecy throughput was derived. Nevertheless, the above research towards secrecy issues in IoT mainly focused on the individual IoT system without considering the interaction between primary and secondary systems, which is a common scenario existing in the IoT networks and thus introduced as follows.

Radio spectrum is essential to support multilevel IoT networks. Deploying IoT networks in the industrial, scientific and medical (ISM) band is not a long-lasting solution since more and more IoDs are operating in such bands. Cognitive radio (CR) is proposed to solve the spectrum scarcity issue [25], [26] and recently introduced into IoT networks [27]–[29]. Traditionally, three strategies are adopted for enabling spectrum sharing in wireless systems, i.e., overlay, underlay and interweave [26]. From a general point of view, the authors in [27] presented an overview of CR-aided IoT, where the potential applications and architectures were introduced. In [28], the authors investigated an underlay CR IoT network and proposed a new leakage-based precoding scheme. In [29], an energy-efficient resource allocation scheme was proposed for SWIPT-enabled CR IoT network. Compared to the underlay technique with strict limits on the interference level and the interweave techniques suffering from traffic pattern error, overlay scheme with cooperative CR was assumed to be more suitable for enabling IoT [30]. At first, the authors in [31] have proposed a one-way cooperative CR network (CCRN) model to further improve the spectrum efficiency of CR system, where the primary and secondary systems can cooperate with each other. Afterwards, the authors in [32] extended CCRN into a two-way relay model, which investigated the optimal beamforming scheme for the multi-antenna secondary users (SUs). When it comes to IoT, the authors in [30] studied an overlay CR IoT network with SWIPT, where two IoDs as SUs sent information to each other and also provided relay cooperation to the primary users (PUs). Actually, the spectrum efficiency of IoT can benefit a lot from CCRN with the presence of multiple IoDs and other PUs. Especially when the relay node (controller) has multiple antenna, beamforming schemes to counteract eavesdropping are proved to be effective [33], which motivates us to study it.

In order to fill such gap, we propose a two-way CR IoT network with SWIPT to investigate the cooperative secrecy scheme against eavesdropping and meanwhile guarantee the quality of service (QoS) of IoDs. A CR-enabled controller located at the center of the secondary network offers relay assistance and cooperative security to a pair of PUs , while transmitting information and power to its corresponding IoDs by utilizing primary spectrum. Two-way amplify-and-forward (AF) relaying is adopted to enable CCRN. Moreover, the IoDs operating in the secondary network preform different functionalities, i.e., IoDs for information decoding (ID-IoDs) and IoDs for energy harvesting (EH-IoDs). In the presence of a potential eavesdropper existing in the secondary network, our objective is to design the secure beamforming at the central controller to maximize the secrecy sum rate of PUs under transmit power constraint, while maintaining the QoS requirements of the secondary IoDs. Our work is different from the previous works [6]–[9], [22]–[24], [28]–[30]. First, we address the secrecy problem for IoT networks while the other performance issues are considered in [6]–[9]. Second, we consider the energy limitation of IoT devices while the works [22]–[24] did not consider the energy-limited constraints. Third, we consider the cooperation between the primary and secondary CR networks to enhance the security of IoT, while no cooperation and no security are considered in [28]–[30]. The main contributions of our works are summarized as follows.

1) A two-way CR IoT network model with SWIPT is constructed to investigate the secrecy issue against eavesdropping. Considering different computing capabilities of IoT controller, we propose three secure beamforming schemes in order to maximize the secrecy capacity [18].
2) We firstly propose the branch-reduce-and-bound (BRB)-based [34] iterative algorithm to solve the secrecy sum rate maximization problem, which can serve as an upper bound benchmark of the objective and generate a feasible solution by Gaussian randomization [35].
3) To solve the problem with lower computational complexity, we further transform the original nonconvex problem into a difference-of-convex (DC) programming problem [36] and propose a constrained-convex-concave programming (CCCP)-based iterative algorithm [37], [38] to find a local optimum of the DC programming.
4) For the IoT network with limited power supply or weak computing capability at the controller, the aforementioned iterative optimization algorithms may not be applicable. Thus, we propose another zero forcing (ZF)-based non-iterative algorithm for the secrecy sum rate maximization problem.
5) Finally, simulation experiments are conducted to verify the effectiveness of our proposed algorithms and their superiority comparing to the conventional schemes.

The rest of this paper is organized as follows. In Section II, the system model is described and the secrecy sum rate maximization problem is formulated. In Section III, we proposed the BRB-based iterative algorithm. In Section IV, we transform the original optimization problem into a DC programming and proposed CCCP-based algorithm. In Section

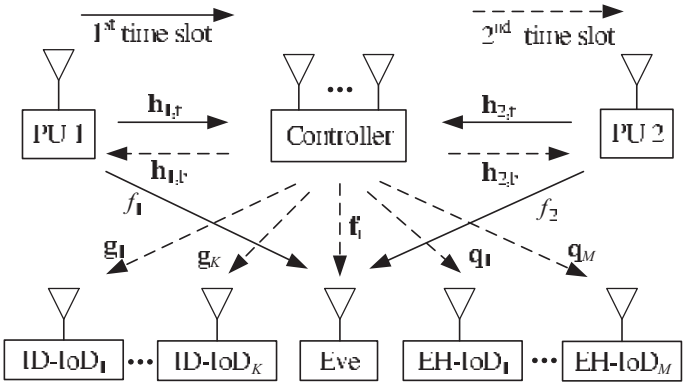

Fig. 1. The cooperative security model of a two-way CR IoT network with SWIPT.

V, we propose a ZF-based non-iterative algorithm. Simulation results are provided in Section VI and in Section VII we conclude our paper.

Notations: Scalars are denoted by lowercase letters like z. Bold lowercase letters like $\mathbf{a}$ denote column vectors. $\mathrm{Re}(z)$, $|z|$, and z^* denote the real part, norm, and conjugate of a complex number z, respectively. $||\mathbf{a}||$ denotes Euclidean norm of a complex vector $\mathbf{a}$. $\mathbf{a}(i)$ denotes the i-th element of the vector $\mathbf{a}$. $\mathbf{A}^\dagger$, $\|\mathbf{A}\|$ and $\mathrm{tr}(\mathbf{A})$ represent the conjugate transpose operation, Frobenius norm, and trace of the matrix $\mathbf{A}$, respectively. $\otimes$ denotes Kronecker product. $\mathrm{vec}(\mathbf{A})$ denotes to stack the columns of matrix $\mathbf{A}$ into a single vector. $\mathbf{A} \succeq \mathbf{0}$ denotes $\mathbf{A}$ is positive semidefinite. $\lambda_{max}(\mathbf{A})$ stands for the maximum eigenvalue of the matrix $\mathbf{A}$.

II. System Model and Problem Formulation

Fig.1 depicts a two-way CR IoT system, which consists of primary and secondary networks. Two single-antenna PUs (PU 1 and PU 2) in the primary network intend to exchange information to each other while an illegal eavesdropper (denoted as Eve) with single antenna is interested in PUs' information and attempts to wiretap it. The secondary network is composed of a CR-enabled controller and multiple IoDs[1]. Located at the center of the secondary network, the controller equipped with N antennas provides the PUs with cooperatively secure relay assistance and serves the secondary IoDs with primary spectrum. Particularly, multiple single-antenna IoDs operate for different functionalities, i.e., K ID-IoDs for decoding specific information (e.g., actuators) and M EH-IoDs for harvesting energy (e.g., sensors) [39]. One typical scenario is smart home application, where an IoT control center (e.g., WiFi access point or smart TV) simultaneously relays two-way information and provide cooperative secrecy for PUs (e.g., smartphone, laptop or controller in other IoT subsystem), meanwhile utilizing the primary spectrum to transmit downlink information to its multiple IoT clients. In this research, we focus on designing the secure beamforming scheme at the central controller.

In this paper, we focus on designing the beamforming schemes to safeguard the secure communication, whose motivation is due to the following facts. One is that according to the initial study of physical layer security in Wyner's work [18], if the main channel is better than the eavesdropping channel with respect to the signal quality, then it is possible to achieve secure transmission from an information theoretic point of view. Here the definition of secrecy channel capacity is the difference of the Shannon capacity of main channel to the one of eavesdropping channel. In this research, we aim at maximizing secrecy channel capacity by means of secure beamforming design. Especially when the relay node has multiple antennas, effective beamforming schemes are proved to exist [33], which constructs our motivation.

The secure information transmission and energy cooperation is divided into two consecutive time slots. In the first time slot, PU 1 and PU 2 simultaneously transmit symbols $x_1 \in \mathbb{C}^{1\times 1}$ and $x_2 \in \mathbb{C}^{1\times 1}$ to the controller with average transmit power $\mathbb{E}[|x_i|^2] = P_i$, $i \in \{1, 2\}$, respectively. We denote the forward channel response from PU i to the controller [2] as $\mathbf{h}_{i,f} \in \mathbb{C}^{N\times 1}$ and the one to the eavesdropper as $f_i \in \mathbb{C}^{1\times 1}, i \in \{1, 2\}$. Thus, the received signals at the controller and eavesdropper in the first time slot are expressed as

$$\mathbf{y}_r = \mathbf{h}_{1,f}x_1 + \mathbf{h}_{2,f}x_2 + \mathbf{n}_r, \tag{1}$$

$$y_{e,1} = f_1x_1 + f_2x_2 + n_{e,1}, \tag{2}$$

respectively, where $\mathbf{n}_r \sim \mathcal{CN}(0, \sigma^2\mathbf{I})$ and $n_{e,1} \sim \mathcal{CN}(0, \sigma^2)$ refer to the additive Gaussian noise at the controller and the eavesdropper, respectively.

In the second time slot, we denote the symbol intending to the ID-IoD j as $s_j \in \mathbb{C}^{1\times 1}, j \in \{1, 2, ..., K\}$. The received signal $\mathbf{y}_r$ and multiple ID-IoDs' symbol s_j are multiplied by beamforming matrix $\mathbf{F} \in \mathbb{C}^{N\times N}$ and corresponding beamforming vector $\mathbf{w}_j \in \mathbb{C}^{N\times 1}$, respectively. Therefore, these multiple products are integrated and sent by the central controller to PUs, ID-IoDs, EH-IoDs and eavesdropper. The transmit signal from the controller is expressed as

$$\mathbf{x}_r = \mathbf{F}\mathbf{y}_r + \sum_{j=1}^{K} \mathbf{w}_j s_j, \tag{3}$$

Assuming s_j with normalized power, i.e., $\mathbb{E}[|s_j|^2] = 1$, the transmit power can be equivalently transformed to the following form by employing $\mathrm{vec}(\mathbf{ABC}) = (\mathbf{C}^{\mathrm{T}} \otimes \mathbf{A})\mathrm{vec}(\mathbf{B})$

$$P_t = \mathbf{f}^\dagger\mathbf{A}\mathbf{f} + \sum_{j=1}^{K} \mathbf{w}_j^\dagger\mathbf{w}_j, \tag{4}$$

where $\mathbf{f} = \mathrm{vec}(\mathbf{F})$ and $\mathbf{A} = (P_1\mathbf{h}_{1,f}\mathbf{h}_{1,f}^\dagger + P_2\mathbf{h}_{2,f}\mathbf{h}_{2,f}^\dagger + \sigma^2\mathbf{I})^T \otimes \mathbf{I}$.

Since PU i knows its transmit symbol in (1), it can eliminate

[1]In the distributed-architecture mobile edge computing (MEC)-based network such as Internet of Vehicles (IoV), massive data generated by vehicles can be processed at the network edge servers instead of transmitting to the centralized cloud infrastructure due to efficiency and energy concerns [40], [41]. Here we consider the secondary network adopts a centralized manner among the whole distributed IoT networks with the benefits for data processing [23], [24], which is applicable in the small IoT subsystem such as smart home application.

[2]We assume that the global channel state information (CSI) of all the considered channels is available to the controller, therefore secure beamforming design can be performed at it. This assumption is reasonable when the eavesdropper is an active user in the IoT network [42], [43].

the self-interference when receiving the backward signal from the controller. Thus, the received signals at PU i and the eavesdropper in the second time slot are expressed as

$$y_{d,i} = \mathbf{h}_{i,b}^T(\mathbf{F}\mathbf{h}_{3-i,f}x_{3-i} + \sum_{j=1}^{K}\mathbf{w}_j s_j + \mathbf{F}\mathbf{n}_r) + n_{d,i}, \quad (5)$$

$$y_{e,2} = \mathbf{f}_r^T(\sum_{p=1}^{2}\mathbf{F}\mathbf{h}_{p,f}x_p + \sum_{j=1}^{K}\mathbf{w}_j s_j + \mathbf{F}\mathbf{n}_r + n_{e,2}, \quad (6)$$

where $\mathbf{h}_{i,b}, \mathbf{f}_r \in \mathbb{C}^{N\times 1}$ denote the backward channel response vectors from the controller to PU i and the eavesdropper; $n_{d,i}, n_{e,2} \sim \mathcal{CN}(0,\sigma^2)$ refer to the additive Gaussian noise at PU i and eavesdropper, respectively.

Based on (5), the received SINR at PU i can be expressed as fractional quadratic form as

$$\gamma_i = \frac{\mathbf{f}^\dagger \mathbf{B}_i \mathbf{f}}{\mathbf{f}^\dagger \mathbf{R}_i \mathbf{f} + \sum_{j=1}^{K}\mathbf{w}_j^\dagger \mathbf{C}_i \mathbf{w}_j + \sigma^2}, \quad (7)$$

where

$$\begin{aligned}
&\mathbf{B}_i = P_{3-i}[(\mathbf{h}_{3-i,f}\mathbf{h}_{3-i,f}^\dagger) \otimes (\mathbf{h}_{i,b}\mathbf{h}_{i,b}^\dagger)]^T,\\
&\mathbf{R}_i = [(\sigma^2\mathbf{I}) \otimes (\mathbf{h}_{i,b}\mathbf{h}_{i,b}^\dagger)]^T,\\
&\mathbf{C}_i = (\mathbf{h}_{i,b}\mathbf{h}_{i,b}^\dagger)^T, \quad i \in \{1,2\},
\end{aligned} \quad (8)$$

where $(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D}) = (\mathbf{AC})\otimes(\mathbf{BD})$ has been employed.

Meanwhile, the received signals at the ID-IoD k and EH-IoD m can be expressed respectively as

$$y_{ID,k} = \mathbf{g}_k^T(\sum_{p=1}^{2}\mathbf{F}\mathbf{h}_{p,f}x_p + \sum_{j=1}^{K}\mathbf{w}_j s_j + \mathbf{F}\mathbf{n}_r) + n_{ID,k}, \quad (9)$$

$$\begin{aligned}
y_{EH,m} = \mathbf{q}_m^T(\sum_{p=1}^{2}\mathbf{F}\mathbf{h}_{p,f}x_p + \sum_{j=1}^{K}\mathbf{w}_j s_j + \mathbf{F}\mathbf{n}_r),\\
k \in \{1,2,...,K\}, \quad m \in \{1,2,...,M\},
\end{aligned} \quad (10)$$

where $\mathbf{g}_k \in \mathbb{C}^{N\times 1}$ and $\mathbf{q}_m \in \mathbb{C}^{N\times 1}$ refer to the channel responses from the controller to the ID-IoD k and EH-IoD m, respectively, $n_{ID,k} \sim \mathcal{CN}(0,\sigma^2)$ is the corresponding additive gaussian noise at the ID-IoD k.

Based on (9) and (10), the received SINR at the ID-IoD k and the harvested energy at the EH-IoD m are given by

$$\gamma_k = \frac{\mathbf{w}_k^\dagger \mathbf{D}_k \mathbf{w}_k}{\mathbf{f}^\dagger \mathbf{E}_k \mathbf{f} + \sum_{j=1,j\neq k}^{K}\mathbf{w}_j^\dagger \mathbf{D}_k \mathbf{w}_j + \sigma^2}, \quad (11)$$

$$Q_m = \rho(\mathbf{f}^\dagger \mathbf{U}_m \mathbf{f} + \sum_{j=1}^{K}\mathbf{w}_j^\dagger \mathbf{V}_m \mathbf{w}_j), \quad (12)$$

respectively, where ρ denotes the EH efficiency factor and

$$\mathbf{D}_k = (\mathbf{g}_k\mathbf{g}_k^\dagger)^T, \mathbf{V}_m = (\mathbf{q}_m\mathbf{q}_m^\dagger)^T, \quad (13)$$

$$\mathbf{E}_k = (P_1\mathbf{h}_{1,f}\mathbf{h}_{1,f}^\dagger + P_2\mathbf{h}_{2,f}\mathbf{h}_{2,f}^\dagger + \sigma^2 I)^T \otimes \mathbf{D}_k, \quad (14)$$

$$\mathbf{U}_m = (P_1\mathbf{h}_{1,f}\mathbf{h}_{1,f}^\dagger + P_2\mathbf{h}_{2,f}\mathbf{h}_{2,f}^\dagger + \sigma^2 I)^T \otimes \mathbf{V}_m. \quad (15)$$

Without loss of generality, we assume the EH efficiency $\rho = 1$. The received signals at the eavesdropper are equivalent to a 2×2 MIMO system, which is expressed as

$$\begin{aligned}
\mathbf{y}_e = &\underbrace{\begin{bmatrix} f_1 & f_2 \\ \mathbf{f}_r^T\mathbf{F}\mathbf{h}_{1,f} & \mathbf{f}_r^T\mathbf{F}\mathbf{h}_{2,f}\end{bmatrix}}_{\mathbf{H}_e}\begin{bmatrix} x_1 \\ x_2\end{bmatrix}\\
&+\underbrace{\begin{bmatrix} n_{e,1} \\ \mathbf{f}_r^T(\mathbf{F}\mathbf{n}_r + \sum_{j=1}^{K}\mathbf{w}_j s_j) + n_{e,2}\end{bmatrix}}_{\mathbf{n}_e}.
\end{aligned} \quad (16)$$

Thus, the achievable information rate leaked to the eavesdropper can be expressed as

$$\begin{aligned}
r_e &= \frac{1}{2}\log_2\det(\mathbf{I} + \mathbf{H}_e\mathbf{P}\mathbf{H}_e^\dagger\mathbf{Z}^{-1})\\
&= \frac{1}{2}\log_2\frac{\mathbf{f}^\dagger\mathbf{R}_4\mathbf{f} + \sum_{j=1}^{K}\mathbf{w}_j^\dagger\mathbf{C}_4\mathbf{w}_j + \beta}{\sigma^4(1+\mathbf{f}^\dagger\mathbf{R}_3\mathbf{f}) + \sigma^2\sum_{j=1}^{K}\mathbf{w}_j^\dagger\mathbf{C}_3\mathbf{w}_j},
\end{aligned} \quad (17)$$

where $\mathbf{P} = \mathrm{diag}(P_1, P_2)$ and

$$\begin{aligned}
&\mathbf{Z} = \mathbb{E}\{\mathbf{n}_e\mathbf{n}_e^\dagger\} = \mathrm{diag}(\sigma^2, \sigma^2(1+\mathbf{f}^\dagger\mathbf{R}_3\mathbf{f}) + \sum_{j=1}^{K}\mathbf{w}_j^\dagger\mathbf{C}_3\mathbf{w}_j),\\
&\mathbf{C}_3 = (\mathbf{f}_r\mathbf{f}_r^\dagger)^T, \quad \mathbf{C}_4 = (P_1|f_1|^2 + P_2|f_2|^2 + \sigma^2)\mathbf{C}_3,\\
&\mathbf{Q}_i = (\mathbf{h}_{i,f}\mathbf{h}_{i,f}^\dagger)^T \otimes \mathbf{C}_3, \bar{\mathbf{Q}}_i = (\mathbf{h}_{3-i,f}\mathbf{h}_{i,f}^\dagger)^T \otimes \mathbf{C}_3, i = 1,2\\
&\mathbf{R}_3 = \mathbf{I}\otimes\mathbf{C}_3, \quad \beta = \sigma^2P_1|f_1|^2 + \sigma^2P_2|f_2|^2 + \sigma^4,\\
&\mathbf{R}_4 = (P_1P_2|f_2|^2 + P_1\sigma^2)\mathbf{Q}_1 + (P_1P_2|f_1|^2 + P_2\sigma^2)\mathbf{Q}_2\\
&\quad + \beta\mathbf{R}_3 - (P_1P_2f_1f_2^*)\bar{\mathbf{Q}}_1 - (P_1P_2f_1^*f_2)\bar{\mathbf{Q}}_2.
\end{aligned} \quad (18)$$

Based on (7) and (17), the secrecy sum rate for the PUs against eavesdropper is expressed as [18]

$$R_s = \frac{1}{2}(\sum_{i=1}^{2}\log_2(1+\gamma_i) - r_e)^+. \quad (19)$$

In this paper, our objective is to maximize the secrecy sum rate for PUs under the transmit power constraint at the controller and the SINR and EH requirements at each IoD, by optimizing the beamforming matrix $\mathbf{F}$ and a sequence of beamforming vectors $\mathbf{w}_j$. Based on (4), (11), (12) and (19), the optimization problem is formulated as

$$\begin{aligned}
\max_{\mathbf{f},\{\mathbf{w}_j\}_1^K} \quad & R_s\\
\text{s.t.} \quad & P_t = \mathbf{f}^\dagger\mathbf{A}\mathbf{f} + \sum_{j=1}^{K}\mathbf{w}_j^\dagger\mathbf{w}_j \le P_r,\\
& \gamma_k = \frac{\mathbf{w}_k^\dagger\mathbf{D}_k\mathbf{w}_k}{\mathbf{f}^\dagger\mathbf{E}_k\mathbf{f} + \sum_{j=1,j\neq k}^{K}\mathbf{w}_j^\dagger\mathbf{D}_k\mathbf{w}_j + \sigma^2} \ge \gamma_0,\\
& Q_m = \mathbf{f}^\dagger\mathbf{U}_m\mathbf{f} + \sum_{j=1}^{K}\mathbf{w}_j^\dagger\mathbf{V}_m\mathbf{w}_j \ge Q_0,\\
& k \in \{1,2,...,K\}, \quad m \in \{1,2,...,M\},
\end{aligned} \quad (20)$$

where P_r, γ_0 and Q_0 are the maximum transmit power at the controller, the SINR requirement at each ID-IoD and the harvested energy threshold at each EH-IoD, respectively.

III. BRB-Based Iterative Algorithm

The secrecy sum rate maximization problem (20) is a non-convex fractional quadratically constrained quadratic programming (FQCQP) problem and thus it is hard to obtain the

optimal solution via conventional convex methods. To provide a benchmark with an upper bound for evaluating the problem compared to other suboptimal algorithms, we will propose an iterative algorithm based on the BRB-based method [34] in this section for solving (20). The idea of the proposed BRB-based method is to recursively update a set of non-overlapping boxes and constantly minimize box size, which impel the objective value to approach the optimal one. More specifically, the proposed BRB-based algorithm includes three steps: branch, reduce and bound. To begin with, we introduce some useful definitions from [34] in the following.

A. Some Definitions of BRB Approach

Box: For given $\mathbf{a}, \mathbf{b} \in \mathcal{R}_+^n$ with $\mathbf{a} < \mathbf{b}$, the set of all $\mathbf{x}$ such that $\mathbf{a} \leq \mathbf{x} \leq \mathbf{b}$ is called a box and denoted as [**a**,**b**]. **a** and **b** denote the vertex of the box in this paper.

Branch: To select a box with a feasible vertex from the set $\mathcal{N}$ and divide it into multiple smaller boxes.

Reduce: To subtract some region in a box that cannot improve the lower bound f_{min}, which can avoid unnecessary feasibility evaluations.

Bound: To search for a feasible solution in one of the new boxes and use it to update the lower and upper bounds, i.e., f_{min}, f_{max}.

Throughout the whole algorithm, we maintain a set $\mathcal{N}$ of multiple non-overlapping boxes, where each box stands for the value of the variables in the problem (20). Each iteration of the algorithm executes the above three procedure, i.e. branch, reduce and bound, to narrow the solution space.

B. Proposed BRB-Based Iterative Algorithm for Solving SSR Maximization Problem (20)

Firstly, we initialize the box set $\mathcal{N} = \{\mathcal{M}_0\}$, which contains the original box $\mathcal{M}_0 = [\mathbf{a}_0, \mathbf{b}_0]$. In order to define the size of $\mathcal{M}_0$, the objective function of problem (20) can be simplified into a product form by discarding the logarithm term, that is, $\bar{R}_s = f(\boldsymbol{\gamma}) = \gamma_1\gamma_2\gamma_3$, where

$$\begin{aligned}\gamma_i =& 1 + \frac{\mathbf{f}^\dagger \mathbf{B}_i \mathbf{f}}{\mathbf{f}^\dagger \mathbf{R}_i \mathbf{f} + \sum_{j=1}^K \mathbf{w}_j^\dagger \mathbf{C}_i \mathbf{w}_j + \sigma^2}, \quad i \in \{1,2\} \\ \gamma_3 =& \frac{\sigma^4(1 + \mathbf{f}^\dagger \mathbf{R}_3 \mathbf{f}) + \sigma^2 \sum_{j=1}^K \mathbf{w}_j^\dagger \mathbf{C}_3 \mathbf{w}_j}{\mathbf{f}^\dagger \mathbf{R}_4 \mathbf{f} + \sum_{j=1}^K \mathbf{w}_j^\dagger \mathbf{C}_4 \mathbf{w}_j + \beta}. \end{aligned} \tag{21}$$

Particularly, $\mathbf{b}_0 = [\gamma_{1,max}, \gamma_{2,max}, \gamma_{3,max}]^T$ is the upper right vertex chosen as a vector consisting of the maximal values of $\gamma_1, \gamma_2, \gamma_3$, and $\mathbf{a}_0 = [\gamma_{1,min}, \gamma_{2,min}, \gamma_{3,min}]^T$ is the lower left vertex constructed by the minimum values of $\gamma_1, \gamma_2, \gamma_3$.

Based on the expressions in (21), γ_1, γ_2, and γ_3 are kinds of generalized Rayleigh quotients whose maximum values are the maximum eigenvalue of the generalized matrices. Therefore, the upper and lower bounds of $\gamma_1, \gamma_2, \gamma_3$ are listed below

$$\begin{aligned}&\gamma_{i,min} = 1, \gamma_{i,max} = 1 + P_r/\sigma^2 \lambda_{max}(\mathbf{A}^{-1}\mathbf{B}_i), i = 1,2 \\ &\gamma_{3,max} = \sigma^4/\beta + P_r/\beta \lambda_{max}(\mathbf{M}^{-1}\mathbf{X}), \\ &\gamma_{3,min} = 1/(\beta + P_r \lambda_{max}(\mathbf{M}^{-1}\mathbf{Y})), \end{aligned} \tag{22}$$

where $\mathbf{M} = \text{diag}(\underbrace{\mathbf{A}, \mathbf{I}, ..., \mathbf{I}}_{K+1})$, $\mathbf{X} = \sigma^2 \text{diag}(\underbrace{\sigma^2\mathbf{R}_3, \mathbf{C}_3, ..., \mathbf{C}_3}_{K+1})$, and $\mathbf{Y} = \text{diag}(\underbrace{\mathbf{R}_4, \mathbf{C}_4, ..., \mathbf{C}_4}_{K+1})$.

1. Branch

The initial upper bound is set as $f_{max} = f(\mathbf{b}_0)$ and the lower bound f_{min} is determined by one feasible vector. In the branching procedure, any box $\mathcal{M} = [\mathbf{a}, \mathbf{b}]$ selected from the set $\mathcal{N}$ should satisfy that the objective value obtained from the upper vertex **b** equals to the current upper bound, i.e., $f(\mathbf{b}) = f_{max}$. Besides, if the lower vertex **a** is an infeasible point to the problem, the box contains no feasible solutions and should be removed from the set $\mathcal{N}$, namely, $\mathcal{N} = \mathcal{N} \setminus \mathcal{M}$. Meanwhile, the current upper bound f_{max} will be reset as

$$f_{max} = \arg\max_{\mathcal{M} \in \mathcal{N}} f(\mathbf{b}). \tag{23}$$

This selecting procedure terminates until an appropriate box $\mathcal{M} = [\mathbf{a}, \mathbf{b}]$ with a feasible vertex **a** is found. Then, we assume the line l_{ab} connecting the vertices of $\mathcal{M}$ crosses through the hyperplane $\{\mathbf{r} | f(\mathbf{r}) = f_{min}\}$ and intersects at point **c**. In order to efficiently improve the lower bound f_{min}, we apply the bisection search and start with checking the feasibility of the intersection point **c**, which is given by

$$\mathbf{c} = \mathbf{a} + (\mathbf{b} - \mathbf{a}) \times (f_{min} - f(\mathbf{a}))/f(\mathbf{b} - \mathbf{a}). \tag{24}$$

If **c** is feasible, a bisection method is applied on l_{cb} to search for the intersection point **v** on the Pareto boundary. Given the accuracy δ, the bisection approach can return the result $[\mathbf{v}_{min}, \mathbf{v}_{max}]$ to improve the lower bound as $f_{min} = \max(f(\mathbf{v}_{min}), f_{min})$. If infeasible, such search procedure is abandoned since any point on l_{ac} cannot update f_{min}. Thus, we set $\mathbf{v} = \mathbf{c}$ to continue the branching procedure.

Now we turn to partition the selected box $\mathcal{M}$ into 3 non-overlapping smaller boxes to improve f_{max}. The upper vertices $\mathbf{b}^1, \mathbf{b}^2, \mathbf{b}^3$ of 3 new boxes are created based on the intersection point **v**, that is

$$\mathbf{b}^i = \mathbf{b} - (\mathbf{b}(i) - \mathbf{v}(i))\mathbf{e}_i, \tag{25}$$

where $\mathbf{e}_i$ is a column vector with its i-th element being 1 and others being 0. Next we calculate the objective value of each vertex as $f(\mathbf{b}^i)$ and reorganize the 3 upper vertices as $\{\mathbf{b}^{\kappa_1}, \mathbf{b}^{\kappa_2}, \mathbf{b}^{\kappa_3}\}$ based on $f(\mathbf{b}^{\kappa_3}) > f(\mathbf{b}^{\kappa_2}) > f(\mathbf{b}^{\kappa_1})$, where κ_i denotes the original index corresponding to the current i-th vertex. Then the corresponding lower vertices are given by

$$\mathbf{a}^{\kappa_1} = \mathbf{a}, \tag{26}$$

$$\mathbf{a}^{\kappa_2} = \mathbf{a}^{\kappa_1} + (\mathbf{v}(\kappa_1) - \mathbf{a}^{\kappa_1}(\kappa_1))\mathbf{e}_{\kappa_1}, \tag{27}$$

$$\mathbf{a}^{\kappa_3} = \mathbf{a}^{\kappa_2} + (\mathbf{v}(\kappa_2) - \mathbf{a}^{\kappa_2}(\kappa_2))\mathbf{e}_{\kappa_2}. \tag{28}$$

Therefore, new boxes are constructed as $\mathcal{M}_1 = [\mathbf{a}^{\kappa_1}, \mathbf{b}^{\kappa_1}]$, $\mathcal{M}_2 = [\mathbf{a}^{\kappa_2}, \mathbf{b}^{\kappa_2}]$, $\mathcal{M}_3 = [\mathbf{a}^{\kappa_3}, \mathbf{b}^{\kappa_3}]$.

2. Reduce

Actually, the boxes in $\mathcal{N}$ contain some parts that may not attain higher value than f_{min}, which should be optimized to avoid unnecessary feasibility evaluations in the following. Take box $[\mathbf{a}, \mathbf{b}]$ for example, if $f(\mathbf{b}) < f_{min}$, the whole box will be discarded from $\mathcal{N}$. Otherwise, the lower vertex **a** is

updated based on

$$\bar{\mathbf{a}}(i) = \mathbf{b}(i) - \min(\frac{f(\mathbf{b}) - f_{min}}{\mathbf{b}(i) - \mathbf{a}(i)}, 1) \times (\mathbf{b}(i) - \mathbf{a}(i)). \quad (29)$$

After all the aforementioned procedures applied on the chosen box $\mathcal{M} = [\mathbf{a}, \mathbf{b}]$, the box set $\mathcal{N}$ is updated as

$$\mathcal{N} = \mathcal{N} \setminus \mathcal{M} \cup \{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3\}. \quad (30)$$

3. Bound

At the end of each iteration, the upper bound is reduced according to (23). By setting the converge accuracy ε, the whole algorithm terminates and returns the objective value $[f_{min}, f_{max}]$, which is presented in Algorithm 1.

Algorithm 1 The Proposed BRB-based Iterative Algorithm

input the original box $\mathcal{M}_0 = [\mathbf{a}_0, \mathbf{b}_0]$, the box set $\mathcal{N} = \{\mathcal{M}_0\}$, accuracy ε and bisection line search accuracy δ;
Set initial f_{min} and f_{max};
while $f_{max} - f_{min} > \varepsilon$
  Choose the box $\mathcal{M} = [\mathbf{a}, \mathbf{b}]$ with feasible lower point $\mathbf{a}$ and $f(\mathbf{b}) = f_{max}$;
  while 1
    Select a box $[\mathbf{a}, \mathbf{b}]$ with $f(\mathbf{b}) = f_{max}$ from $\mathcal{N}$;
    Check the feasibility of $\mathbf{a} = [\mathbf{a}(1), \mathbf{a}(2), \mathbf{a}(3)]^T$;
    if feasible:box $[\mathbf{a}, \mathbf{b}]$ is chosen; **break**
    else: remove the box from the set $\mathcal{N} = \mathcal{N} \setminus [\mathbf{a}, \mathbf{b}]$ and update the upper bound f_{max} as $f_{max} = \arg\max_{[\mathbf{a},\mathbf{b}] \in \mathcal{N}} f(\mathbf{b})$; **end**
  end
  Set the intersection point $\mathbf{c}$ as $\mathbf{c} = \mathbf{a} + (\mathbf{b} - \mathbf{a}) \times (f_{min} - f(\mathbf{a}))/f(\mathbf{b} - \mathbf{a})$, set $\mathbf{v} = \mathbf{c}$;
  Check the feasibility of $\mathbf{c}$:
    if feasible: Apply **Bisection method** on line l_{cb} to search the interval $[\mathbf{v}_{min}, \mathbf{v}_{max}]$, update $\mathbf{v} = \mathbf{v}_{max}$ and improve the lower bound by $f_{min} = \max(f_{min}, f(\mathbf{v}_{min}))$; **end**
  Branch the box $\mathcal{M}_{max}$ into 3 new boxes based on $\mathbf{v}$;
  for any box $[\mathbf{a}, \mathbf{b}] \in \mathcal{N}$
    if $f(b) > f_{min}$: rewrite the vertex $\mathbf{a}$ according to (29)
    else: subtract this box from the box set; **end**
  end
  Update the box set $\mathcal{N} = \mathcal{N} \setminus \mathcal{M} \cup \{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3\}$ and the upper bound $f_{max} = \arg\max_{[\mathbf{a},\mathbf{b}] \in \mathcal{N}} f(\mathbf{b})$;
end
return the interval $[f_{min}, f_{max}]$ and feasible solution.

To finish the proposed Algorithm 1, the remaining challenge is to construct the feasibility problem. By letting $\mathbf{T} = \mathbf{f}\mathbf{f}^\dagger$ and $\mathbf{W}_j = \mathbf{w}_j\mathbf{w}_j^\dagger$ for all j, (20) can be reformulated into a semidefinite programming (SDP) problem. For a box $[\mathbf{a}, \mathbf{b}]$, the feasibility evaluation on vertex $\mathbf{a}$ can be written as

$$\begin{aligned}
&\text{find} \quad (\mathbf{T}, \{\mathbf{W}_j\}) \\
&\text{s.t.} \\
&\mathrm{tr}(\mathbf{B}_i\mathbf{T}) + (1 - \mathbf{a}(i))(\mathrm{tr}(\mathbf{R}_i\mathbf{T}) + \sum_{j=1}^{K} \mathrm{tr}(\mathbf{C}_i\mathbf{W}_j) + 1) \geq 0, \\
&\mathrm{tr}((\mathbf{R}_3 - \mathbf{a}(3)\mathbf{R}_4)\mathbf{T}) + \sum_{j=1}^{K} \mathrm{tr}((\mathbf{C}_3 - \mathbf{a}(3)\mathbf{C}_4)\mathbf{W}_j) + 1 \geq \mathbf{a}(3)\beta, \\
&\mathrm{tr}(\mathbf{E}_k\mathbf{T}) + \sum_{j=1, j\neq k}^{K} \mathrm{tr}(\mathbf{D}_k\mathbf{W}_j) + 1 - \mathrm{tr}(\mathbf{D}_k\mathbf{W}_k)/\gamma_0 \leqslant 0, \\
&Q_0 - \mathrm{tr}(\mathbf{U}_m\mathbf{T}) - \sum_{j=1}^{K} \mathrm{tr}(\mathbf{V}_m\mathbf{W}_j) \leqslant 0, \\
&i \in \{1, 2\}, \quad k \in \{1, 2...K\}, \quad m \in \{1, 2...M\}, \\
&\mathrm{tr}(\mathbf{A}\mathbf{T}) + \sum_{j=1}^{K} \mathrm{tr}(\mathbf{W}_j) - P_r \leqslant 0, \\
&\mathbf{T} \succeq 0, \quad \mathbf{W}_j \succeq 0, \quad \mathrm{rank}(\mathbf{T}) = 1, \quad \mathrm{rank}(\mathbf{W}_j) = 1. \qquad (31)
\end{aligned}$$

By discarding the rank-one constraint, such problem is convex and solvable using interior point method [44].

Another remaining task is to build up the bisection search in Algorithm 1. If the point $\mathbf{c}$ is feasible, the basic idea is to choose the middle point $\boldsymbol{\theta}$ on line l_{cb} to check its feasibility. Thus, the point $\mathbf{a}$ is substituted for $\boldsymbol{\theta}$ in (31) to evaluate it. The bisection method is summarized in Algorithm 2. We initialize the bisection bounds as $\varphi^l = 0$ and $\varphi^u = ||\mathbf{b} - \mathbf{c}||_1$. By constantly updating the two endpoints, we can approximate the optimal result in an interval range $[\mathbf{v}_{min}, \mathbf{v}_{max}]$, where $\mathbf{v}_{min}$ is calculated by the feasible point and used to update f_{min} in Algorithm 1, and $\mathbf{v}_{max}$ is used in the branching procedure.

Algorithm 2 Bisection Method Applied on l_{cb}

input accuracy δ, $\varphi^l = 0$ and $\varphi^u = ||\mathbf{b} - \mathbf{c}||_1$.
while $\varphi^u - \varphi^l > \delta$
  set $\varphi^{mid} = (\varphi^u + \varphi^l)/2$,
  set $\boldsymbol{\xi} = \frac{\mathbf{b}-\mathbf{c}}{||\mathbf{b}-\mathbf{c}||_1} = [\boldsymbol{\xi}(1), \boldsymbol{\xi}(2), \boldsymbol{\xi}(3)]^T$,
  set $\boldsymbol{\theta}(k) = \mathbf{c}(k) + \boldsymbol{\xi}(k)\varphi^{mid}, \quad k = 1, 2, 3.$
if problem (31) is feasible for given $\boldsymbol{\theta}$: set $\varphi^l = \varphi^{mid}$
else: set $\varphi^u = \varphi^{mid}$. **end**
end
return $[\varphi^l, \varphi^u]$, $[\mathbf{v}_{min}, \mathbf{v}_{max}]$ and the last feasible solution.

Remark 1 (Initial f_{min} for Algorithm 1): We have predefined the initial f_{max} as $f_{max} = f(\mathbf{b}_0)$ in the beginning of Algorithm 1. However, the value of the initial f_{min} will directly affect the location of the intersection point $\mathbf{c}$, which influences the convergence speed. In this regard, we propose to solve a SDP problem based on (31) whose constraints are (41e)-(41g) and the objective is $\max(\mathbf{B}_1 + \mathbf{B}_2)\mathbf{T}$. Then we use its feasible solution $\mathbf{T}, \mathbf{W}$ to calculate the initial f_{min}.

Remark 2 (Retaining feasible box in the reduce procedure): In the reduce procedure ,we update the lower left bounds of each box by using (29). Although it cuts off parts that cannot achieve function values between f_{min} and $f_{\mathbf{b}}$ in one box, it is likely to reduce the feasible region, which may cause the box set $\mathcal{N}$ contains no feasible regions. Thus, we propose to evaluate the feasibility of each new vertex $\mathbf{a}$ after (29). If infeasible, the original $\mathbf{a}$ is retained.

Remark 3 (Gaussian randomization): Since the feasibility problem (31) may not have a rank-one solution, we preserve the last feasible solution and apply Gaussian randomization

(GR) [35] to construct a feasible rank-one solution. Thus, the results obtained from Algorithm 1 is an upper bound for the original problem (20). Simulations with comparison of average secrecy sum rate obtained by the BRB-based proposed algorithm without GR and that with GR are presented in Section VI.

IV. CCCP-Based Iterative Algorithm

Although the proposed Algorithm 1 presented in the last section can serve as a benchmark by offering an upper bound, it has quite high computational complexity due to the double-tier iteration. Thus, we will propose a single-tier iterative algorithm in this section, which is based on constrained-convex-concave programming (CCCP). The main idea of CCCP-based iterative algorithm is to equivalently transform problem (20) into a difference-of-convex (DC) programming form, where the objective and constraints can be expressed as difference of convex functions. By replacing the latter convex functions with their approximately linear form, the resulting problem can be solved with iteratively updated variables until convergence.

For the ease of presentation, we normalize the variance of noise to be unit, i.e., $\sigma^2 = 1$ and the EH efficiency $\rho = 1$. Let $\mathbf{q} = [\mathbf{f}^\dagger, \mathbf{w}_1^\dagger, \mathbf{w}_2^\dagger, ..., \mathbf{w}_K^\dagger]^\dagger$. Given the monotonicity and concavity properties of logarithm function, problem (20) can be reformulated by omitting the logarithm term as

$$\begin{aligned}
\max_{\mathbf{q}} \quad & \prod_{i=1}^{2} \frac{\mathbf{q}^\dagger \mathbf{A}_i \mathbf{q} + 1}{\mathbf{q}^\dagger \mathbf{H}_i \mathbf{q} + 1} \cdot \frac{\mathbf{q}^\dagger \mathbf{H}_3 \mathbf{q} + 1}{\mathbf{q}^\dagger \mathbf{H}_4 \mathbf{q} + \beta} && \text{(32a)}\\
\text{s.t.} \quad & \mathbf{q}^\dagger \mathbf{M} \mathbf{q} - P_r \le 0, && \text{(32b)}\\
& \gamma_0(\mathbf{q}^\dagger \mathbf{G}_k \mathbf{q} + 1) - (\gamma_0 + 1)\mathbf{w}_k^\dagger \mathbf{D}_k \mathbf{w}_k \le 0, && \text{(32c)}\\
& Q_0 - \mathbf{q}^\dagger \mathbf{T}_m \mathbf{q} \le 0, && \text{(32d)}\\
& k \in \{1, 2, ..., K\}, \quad m \in \{1, 2, ..., M\},
\end{aligned}$$

where $\bar{\mathbf{B}}_i = \mathbf{B}_i + \mathbf{R}_i$, $\mathbf{A}_i = \text{diag}(\underbrace{\bar{\mathbf{B}}_i, \mathbf{C}_i, ..., \mathbf{C}_i}_{K+1}), i = 1, 2$, $\mathbf{H}_i = \text{diag}(\underbrace{\mathbf{R}_i, \mathbf{C}_i, ..., \mathbf{C}_i}_{K+1})$, $\mathbf{G}_k = \text{diag}(\underbrace{\mathbf{E}_k, \mathbf{D}_k, ..., \mathbf{D}_k}_{K+1})$, and $\mathbf{T}_m = \text{diag}(\underbrace{\mathbf{U}_m, \mathbf{V}_m, ..., \mathbf{V}_m}_{K+1})$.

By introducing three slack variables (t_1, t_2, t_3), the problem (32) can be equivalently recast as follows

$$\begin{aligned}
\max_{\mathbf{q}, \{t_i > 0\}_1^3} \quad & t_1 t_2 t_3 && \text{(33a)}\\
\text{s.t.} \quad & \mathbf{q}^\dagger \mathbf{H}_i \mathbf{q} + 1 - (\mathbf{q}^\dagger \mathbf{A}_i \mathbf{q} + 1)/t_i \le 0, i = 1, 2 && \text{(33b)}\\
& \mathbf{q}^\dagger \mathbf{H}_4 \mathbf{q} + \beta - (\mathbf{q}^\dagger \mathbf{H}_3 \mathbf{q} + 1)/t_3 \le 0, && \text{(33c)}\\
& \text{(32b)}, \quad \text{(32c)}, \quad \text{(32d)}. && \text{(33d)}
\end{aligned}$$

Then, we propose the CCCP-based iterative algorithm to solve DC programming problem (33), where we iteratively approximate the original nonconvex feasible set around the current point by a convex subset and then solve the resulting convex approximation in each iteration. To conduct the procedure, we define following functions and corresponding first-order Taylor expansions around points $\bar{t}$, $(\bar{\mathbf{f}}, \bar{x})$ and $\bar{\mathbf{f}}$ as

$$g(t) = 1/t, \qquad g(t, \bar{t}) = g(\bar{t}) + g'(\bar{t})(t - \bar{t}) = 2/\bar{t} - t/\bar{t}^2,$$

$$\begin{aligned}
&\xi_{\mathbf{Y}}(\mathbf{f}, x) = \mathbf{f}^\dagger \mathbf{Y} \mathbf{f}/x, \ \xi_{\mathbf{Y}}(\mathbf{f}, x, \bar{\mathbf{f}}, \bar{x}) = 2\text{Re}\{\bar{\mathbf{f}}^\dagger \mathbf{Y} \mathbf{f}\}/\bar{x} - \bar{\mathbf{f}}^\dagger \mathbf{Y} \bar{\mathbf{f}} x/\bar{x}^2,\\
&\varphi_{\mathbf{Y}}(\mathbf{f}) = \mathbf{f}^\dagger \mathbf{Y} \mathbf{f}, \quad \varphi_{\mathbf{Y}}(\mathbf{f}, \bar{\mathbf{f}}) = 2\text{Re}\{\bar{\mathbf{f}}^\dagger \mathbf{Y} \mathbf{f}\} - \bar{\mathbf{f}}^\dagger \mathbf{Y} \bar{\mathbf{f}}. \qquad \text{(34)}
\end{aligned}$$

In the (n+1)-th iteration of the algorithm, given the optimal set $\Theta^{(n)} = \{\mathbf{q}^{(n)} = [\mathbf{f}^{(n)\dagger}, \mathbf{w}_1^{(n)\dagger}, ...\mathbf{w}_K^{(n)\dagger}]^\dagger, t_1^{(n)}, t_2^{(n)}, t_3^{(n)}\}$ obtained in the n-th iteration, we solve the following convex optimization problem

$$\begin{aligned}
\max_{\mathbf{q}, \{t_i > 0\}_1^3} \quad & t_1 t_2 t_3\\
\text{s.t.} \quad & \mathbf{q}^\dagger \mathbf{H}_i \mathbf{q} + 1 - \xi_{\mathbf{A}_i}(\mathbf{q}, t_i, \mathbf{q}^{(n)}, t_i^{(n)}) - g(t_i, t_i^{(n)}) \le 0,\\
& \mathbf{q}^\dagger \mathbf{H}_4 \mathbf{q} + \beta - \xi_{\mathbf{H}_3}(\mathbf{q}, t_3, \mathbf{q}^{(n)}, t_3^{(n)}) - g(t_3, t_3^{(n)}) \le 0,\\
& \mathbf{q}^\dagger \mathbf{M} \mathbf{q} - P_r \le 0,\\
& \gamma_0(\mathbf{q}^\dagger \mathbf{G}_k \mathbf{q} + 1) - (\gamma_0 + 1)\varphi_{\mathbf{D}_k}(\mathbf{w}_k, \mathbf{w}_k^{(n)}) \le 0,\\
& Q_0 - \varphi_{\mathbf{T}_m}(\mathbf{q}, \mathbf{q}^{(n)}) \le 0,\\
& k \in \{1, 2, ..., K\}, \quad m \in \{1, 2, ..., M\}, \qquad \text{(35)}
\end{aligned}$$

which can be further transformed into an second-order cone programming (SOCP) problem to reduce the computational complexity.

By introducing the variables (α_1, α_2) and z, problem (35) is converted into the following convex SOCP

$$\begin{aligned}
\max_{\mathbf{q}, \{t_i > 0\}_1^3, \{\alpha_i > 0\}_1^2, z} \quad & z\\
\text{s.t.} \quad & |||[2\alpha_1, t_1 - t_2]||| \le t_1 + t_2,\\
& |||[2\alpha_2, t_3 - 1]||| \le t_3 + 1,\\
& |||[2z, \alpha_1 - \alpha_2]||| \le \alpha_1 + \alpha_2,\\
& \left\| \begin{bmatrix} 2\mathbf{H}_i^{\frac{1}{2}} \mathbf{q} \\ -\text{Re}\{\mathbf{b}_i^\dagger \mathbf{q}\} - r_i t_i - e_i - 1 \end{bmatrix} \right\| \le -\text{Re}\{\mathbf{b}_i^\dagger \mathbf{q}\} - r_i t_i\\
& - e_i + 1, \quad i = 1, 2\\
& \left\| \begin{bmatrix} 2\mathbf{H}_3^{\frac{1}{2}} \mathbf{q} \\ -\text{Re}\{\mathbf{b}_3^\dagger \mathbf{q}\} - r_3 t_3 - e_3 - 1 \end{bmatrix} \right\| \le -\text{Re}\{\mathbf{n}^\dagger \mathbf{q}\} - r_3 t_3\\
& - e_3 + 1,\\
& \left\| \begin{bmatrix} 2\mathbf{H}_k^{\frac{1}{2}} \mathbf{q} \\ -\text{Re}\{\mathbf{p}_k^\dagger \mathbf{w}_k\} - n_k - 1 \end{bmatrix} \right\| \le -\text{Re}\{\mathbf{p}_k^\dagger \mathbf{w}_k\} - n_k + 1,\\
& Q_0 + \text{Re}\{\mathbf{v}_m^\dagger \mathbf{q}\} + d_m \le 0,\\
& ||\mathbf{H}_4^{\frac{1}{2}} \mathbf{q}|| \le \sqrt{P_r}, \quad k \in \{1, 2, ..., K\}, m \in \{1, 2, ..., M\},
\end{aligned} \qquad \text{(36)}$$

where

$$\begin{aligned}
&\mathbf{b}_i = -2/t_i^{(n)}[(\bar{\mathbf{B}}_i \mathbf{f}^{(n)})^\dagger, (\mathbf{C}_i \mathbf{w}_1^{(n)})^\dagger, ...(\mathbf{C}_i \mathbf{w}_K^{(n)})^\dagger]^\dagger,\\
&r_i = (\mathbf{q}^{(n)\dagger} \mathbf{A}_i \mathbf{q}^{(n)} + 1)(t_i^{(n)})^2, \quad e_i = 1 - 2/t_i^{(n)}, i = 1, 2;\\
&\mathbf{b}_3 = -2/t_3^{(n)}[(\mathbf{R}_3 \mathbf{f}^{(n)})^\dagger, (\mathbf{C}_3 \mathbf{w}_1^{(n)})^\dagger, ...(\mathbf{C}_3 \mathbf{w}_K^{(n)})^\dagger]^\dagger,\\
&r_3 = (\mathbf{q}^{(n)\dagger} \mathbf{H}_3 \mathbf{q}^{(n)} + 1)(t_3^{(n)})^2, \quad e_3 = \beta - 2/t_3^{(n)};\\
&\mathbf{p}_k = -2(\gamma_0 + 1)\mathbf{D}_k \mathbf{w}_k^{(n)}, n_k = \gamma_0 + (\gamma_0 + 1)(\mathbf{w}_k^{(n)})^\dagger \mathbf{D}_k \mathbf{w}_k^{(n)};\\
&\mathbf{v}_m = -2[(\mathbf{U}_m \mathbf{f}^{(n)})^\dagger, (\mathbf{V}_m \mathbf{w}_1^{(n)})^\dagger, ...(\mathbf{V}_m \mathbf{w}_K^{(n)})^\dagger]^\dagger,\\
&d_m = \mathbf{q}^{(n)\dagger} \mathbf{T}_m \mathbf{q}^{(n)}. \qquad \text{(37)}
\end{aligned}$$

The CCCP-based algorithm for solving problem (32) is summarized in Algorithm 3.

Algorithm 3 The Proposed CCCP-based Iteration Algorithm

1: **Initialize**: Set $n=0$, given a feasible set $\Theta^{(0)}=\{\mathbf{q}^{(0)}=[\mathbf{f}^{(0)\dagger},\mathbf{w}_1^{(0)\dagger},...\mathbf{w}_K^{(0)\dagger}]^\dagger,t_1^{(0)},t_2^{(0)},t_3^{(0)}\}$ and accuracy ε;
2: **Repeat**:
Solve the SOCP problem (36) with $\Theta^{(n)}$ using interior method and assign the optimal solution Θ^* to $\Theta^{(n+1)}$;
$n:=n+1$;
3: **Until:** Convergence, i.e., $\mid z^{(n+1)}-z^{(n)}\mid\leq\varepsilon$.

Remark 4 (Initial Point for Algorithm 3): We choose the initial point for Algorithm 3 as that for Algorithm 1, where a feasible solution $\mathbf{T},\mathbf{W}$ is found. Then, by employing Gaussian randomization, the initial point $\{\mathbf{f}^{(0)},\mathbf{w}_1^{(0)},\mathbf{w}_2^{(0)},...\mathbf{w}_K^{(0)}\}$ are derived. Accordingly, slack variables $\{t_1^{(0)},t_2^{(0)},t_3^{(0)}\}$ can be determined when the slack inequalities become active.

V. ZF-Based Non-Iterative Suboptimal Solution

Although Algorithm 3 has much lower computation complexity than Algorithm 1, we still need to solve a sequence of SOCPs. To further reduce the complexity, we present a ZF-based non-iterative suboptimal solution in this section, where only one SDP is needed to be solved. In this section, we take the scenario $K=M$ for example. Firstly, we force the beamforming vector $\mathbf{f}$ at the controller to be in the null-space of the corresponding eavesdropping channels in the second time slot, which can be expressed as

$$[\mathbf{q}_1,\mathbf{q}_2]^T\mathbf{f}=[0,0]^T, \tag{38}$$

where $\mathbf{q}_1=\mathrm{vec}(\mathbf{f}_\mathrm{r}\mathbf{h}_{1,\mathrm{f}}^\mathrm{T})$ and $\mathbf{q}_2=\mathrm{vec}(\mathbf{f}_\mathrm{r}\mathbf{h}_{2,\mathrm{f}}^\mathrm{T})$. Accordingly, the beamforming vector $\mathbf{f}$ can be expressed as

$$\mathbf{f}=\mathbf{V}\mathbf{x}, \tag{39}$$

where $\mathbf{V}\in\mathbb{C}^{N^2\times(N^2-2)}$ consists of N^2-2 singular vectors of the matrix $[\mathbf{q}_1,\mathbf{q}_2]^T$, corresponding to zero singular values and $\mathbf{x}\in\mathbb{C}^{(N^2-2)\times1}$ denotes an arbitrary vector to be optimized.

By inserting (39) into problem (32), the third term of the objective, i.e, the SINR of the eavesdropper is a constant with respect to the channels, which can be discarded from the objective. Thus, we can obtain

$$\max_{\bar{\mathbf{q}}}\quad \frac{\bar{\mathbf{q}}^\dagger\bar{\mathbf{H}}_1\bar{\mathbf{q}}+1}{\bar{\mathbf{q}}^\dagger\bar{\mathbf{H}}_3\bar{\mathbf{q}}+1}\cdot\frac{\bar{\mathbf{q}}^\dagger\bar{\mathbf{H}}_2\bar{\mathbf{q}}+1}{\bar{\mathbf{q}}^\dagger\bar{\mathbf{H}}_4\bar{\mathbf{q}}+1} \tag{40a}$$
$$\text{s.t.}\quad \bar{\mathbf{q}}^\dagger\mathbf{H}_5^k\bar{\mathbf{q}}+\gamma_0\leq0, \tag{40b}$$
$$\bar{\mathbf{q}}^\dagger\mathbf{H}_6^k\bar{\mathbf{q}}\geq Q_0, \tag{40c}$$
$$\bar{\mathbf{q}}^\dagger\mathbf{H}_7\bar{\mathbf{q}}\leq P_r,\quad k\in\{1,2...K\}, \tag{40d}$$

where $\bar{\mathbf{q}}=[\mathbf{x}^\dagger,\mathbf{w}_1^\dagger,\mathbf{w}_2^\dagger,...\mathbf{w}_K^\dagger]^\dagger$ and

$$\bar{\mathbf{H}}_i=\mathrm{diag}(\mathbf{V}^\dagger\underbrace{\bar{\mathbf{B}}_i\mathbf{V},\mathbf{C}_i,...,\mathbf{C}_i}_{K+1}),\quad i=1,2$$
$$\bar{\mathbf{H}}_j=\mathrm{diag}(\mathbf{V}^\dagger\underbrace{\mathbf{R}_{j-2}\mathbf{V},\mathbf{C}_{j-2},...,\mathbf{C}_{j-2}}_{K+1}),\quad j=3,4$$
$$\mathbf{H}_5^k=\mathrm{diag}(\gamma_0\mathbf{V}^\dagger\underbrace{\mathbf{E}_k\mathbf{V},\gamma_0\mathbf{D}_k,...,-\mathbf{D}_k,...,\gamma_0\mathbf{D}_k}_{K+1}),$$
$$\mathbf{H}_6^k=\mathrm{diag}(\mathbf{V}^\dagger\underbrace{\mathbf{U}_k\mathbf{V},\mathbf{V}_k,...,\mathbf{V}_k}_{K+1}),$$
$$\mathbf{H}_7=\mathrm{diag}(\mathbf{V}^\dagger\underbrace{\mathbf{A}\mathbf{V},\mathbf{I},...,\mathbf{I}}_{K+1}). \tag{41}$$

Note that the matrix $-\mathbf{D}_k$ in the diagonal matrix $\mathbf{H}_5^k$ corresponds to the beamforming vector $\mathbf{w}_k$ for ID-IoD k. Actually, to achieve the optimum of the problem (40), the optimal solution $\bar{\mathbf{q}}$ should always satisfy that the transmit power constraint of the controller is active, i.e.,

$$\bar{\mathbf{q}}^\dagger\mathbf{H}_7\bar{\mathbf{q}}=P_r. \tag{42}$$

By substituting (42) into problem (40) and replacing $\bar{\mathbf{q}}\bar{\mathbf{q}}^\dagger$ by $P_r/n\cdot{\mathbf{H}_7}^{-1}$, we rewrite (40) as

$$\max_{\bar{\mathbf{q}}}\quad \frac{\bar{\mathbf{q}}^\dagger\mathbf{P}_1\mathbf{H}_7^{-1}\mathbf{P}_2\bar{\mathbf{q}}}{\bar{\mathbf{q}}^\dagger\mathbf{P}_3\mathbf{H}_7^{-1}\mathbf{P}_4\bar{\mathbf{q}}} \tag{43a}$$
$$\text{s.t.}\quad \bar{\mathbf{q}}^\dagger\mathbf{P}_5^k\bar{\mathbf{q}}\leq0, \tag{43b}$$
$$\bar{\mathbf{q}}^\dagger\mathbf{P}_6^k\bar{\mathbf{q}}\geq0,\quad k\in\{1,2,...,K\}, \tag{43c}$$

where $\mathbf{P}_i=\bar{\mathbf{H}}_i+P_r^{-1}\mathbf{H}_7, i\in\{1,2,3,4\}, \mathbf{P}_5^k=P_r\mathbf{H}_5^k+\gamma_0\mathbf{H}_7, \mathbf{P}_6^k=P_r\mathbf{H}_6^k-Q_0\mathbf{H}_7$.

Define $\mathbf{K}_1=\mathbf{P}_1\mathbf{H}_7^{-1}\mathbf{P}_2$, $\mathbf{K}_2=\mathbf{P}_3\mathbf{H}_7^{-1}\mathbf{P}_4$, and $\mathbf{S}=\bar{\mathbf{q}}\bar{\mathbf{q}}^\dagger$. Omitting the rank-one constraint $\mathrm{rank}(\mathbf{S})=1$ and applying Charnes-Cooper transformation [45], problem (43) can be transformed into the following SDP

$$\max_{\mathbf{S}\succeq0}\quad \mathrm{tr}(\mathbf{K}_1\mathbf{S}) \tag{44a}$$
$$\text{s.t.}\quad \mathrm{tr}(\mathbf{K}_2\mathbf{S})=1, \tag{44b}$$
$$\mathrm{tr}(\mathbf{P}_5^k\mathbf{S})\leq0, \tag{44c}$$
$$\mathrm{tr}(\mathbf{P}_6^k\mathbf{S})\geq0,\quad k\in\{1,2...K\}. \tag{44d}$$

Problem (44) is convex and can be efficiently solved via interior point method. Assume that $\mathbf{S}^o$ is the optimal solution to SDP (44). If the rank of $\mathbf{S}^o$ is one, denoted as $\mathbf{S}^o=\mathbf{s}^o\mathbf{s}^{o\dagger}$, the optimal solution to problem (43) is $\bar{\mathbf{q}}^o=\mathbf{s}^o$. If $\mathrm{rank}(\hat{\mathbf{S}}^\mathrm{o})\geq2$ and $k=1$, the number of trace condition in problem (43) is 4. The following rank-one decomposition theorem is employed.

Theorem 1 [46]: Let $\mathbf{A}_i\in\mathcal{C}^{n\times n}$, $i\in\mathcal{I}=[1,2,3,4]$, be a Hermitian matrix, and $\mathbf{Z}\in\mathcal{C}^{n\times n}$ be a nonzero Hermitian positive semidefinite matrix. Suppose that $n>3$ and for any nonzero Hermitian positive semidefinite matrix $\mathbf{Y}\in\mathcal{C}^{n\times n}$, $[\mathrm{tr}(\mathbf{A}_1\mathbf{Y}),\mathrm{tr}(\mathbf{A}_2\mathbf{Y}),\mathrm{tr}(\mathbf{A}_3\mathbf{Y}),\mathrm{tr}(\mathbf{A}_4\mathbf{Y})]\neq[0,0,0,0]$. If $\mathrm{rank}(\mathbf{Z})\geq2$, we can find a rank-one matrix $\mathbf{z}\mathbf{z}^\dagger$ such that $\mathrm{tr}(\mathbf{A_i}\mathbf{z}\mathbf{z}^\dagger)=\mathrm{tr}(\mathbf{A_i}\mathbf{Z}),\mathrm{i}\in\mathcal{I}$.

When $\mathrm{rank}(\mathbf{S}^\mathrm{o})\geq2$ and $k=1$, from Theorem 1, we can find a rank-one matrix $\mathbf{z}\mathbf{z}^\dagger$ such that $\mathrm{tr}(\mathbf{K}_1\mathbf{z}\mathbf{z}^\dagger)=\mathrm{tr}(\mathbf{K}_1\mathbf{S}^\mathrm{o})$, $\mathrm{tr}(\mathbf{K}_2\mathbf{z}\mathbf{z}^\dagger)=\mathrm{tr}(\mathbf{K}_2\mathbf{S}^\mathrm{o})$, $\mathrm{tr}(\mathbf{P}_5\mathbf{z}\mathbf{z}^\dagger)=\mathrm{tr}(\mathbf{P}_5\mathbf{S}^\mathrm{o})$, $\mathrm{tr}(\mathbf{P}_6\mathbf{z}\mathbf{z}^\dagger)=\mathrm{tr}(\mathbf{P}_6\mathbf{S}^\mathrm{o})$. Thus, the optimal solution to the FQCQP (43) is $\mathbf{q}^o=\mathbf{z}$. Otherwise, if $k\geq2$, we employ Gaussian randomization to obtain the approximate solution.

Remark 5 (Practical Implementation Issue): The application of the three proposed algorithms depends heavily on the processing capability of the central controller. For the scenario that the controller with much powerful computing ability and sufficient power supply, e.g., micro base station, it's more suitable to employ BRB-based algorithm at it. For the controller

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2941873, IEEE Internet of Things Journal

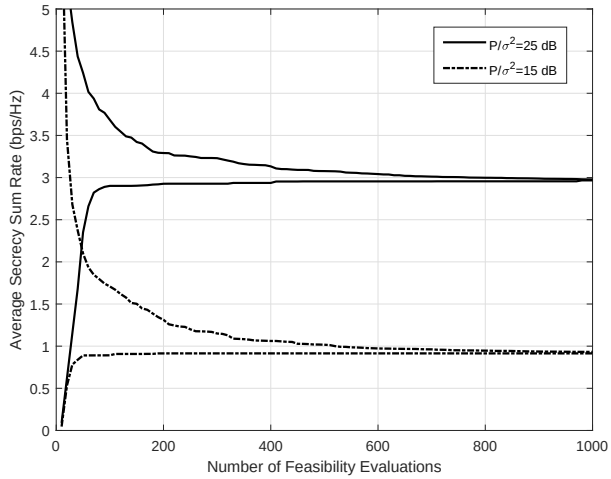

Fig. 2. Average secrecy sum rate versus the number of feasibility evaluations in the BRB-based iterative algorithm when the transmit power to noise power ratio and the number of antennas at the controller are $P_r/\sigma^2 = 25$ dB, $N = 3$ and the accuracy $\varepsilon = 0.1$, $\delta = 0.01$.

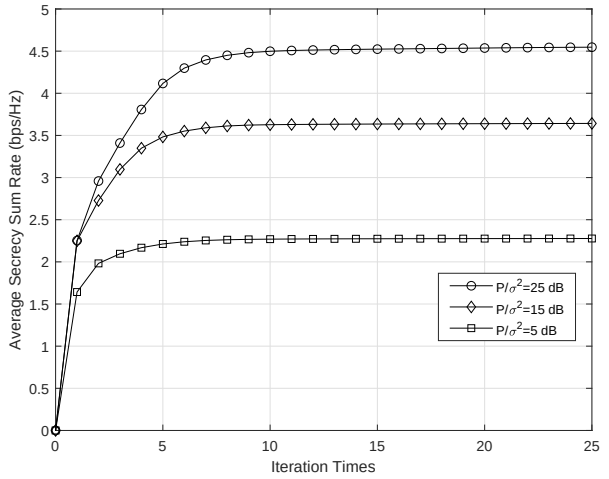

Fig. 3. Average secrecy sum rate versus the iteration times of the CCCP-based iterative algorithm when the transmit power to noise power ratio and the number of antennas at the controller are $P_r/\sigma^2 = 30$ dB and $N = 4$.

with limited computing power such as a WiFi access point or laptop, CCCP-based algorithm is a good choice that strikes a balance between lower complexity and better performance. However, for the IoT network with lower power supply at the controller, we suggest adopting ZF-based algorithm, which can obtain the solutions within a short period at the expense of relatively poor performances.

VI. Simulation Results

In this section, we will present computer simulation results of our proposed algorithms. In the proposed model, we assume that all the channel response vectors are independent and identically distributed (i.i.d.) complex Gaussian random variables with zero mean and unit variance. To solve the SOCPs and SDPs, we apply the CVX optimization solver based on MATLAB environment [47]. In all the simulations, the secrecy sum rate is an average value by using 500 randomly generated channel realizations. Besides, the transmit-power-to-noise-power ratios of the two PUs are set equal, i.e., $P_1/\sigma^2 = P_2/\sigma^2 = P/\sigma^2$. If not specified, the EH and SINR thresholds for secondary IoDs are $Q_0 = \gamma_0 = 5$ dB, and the numbers of ID-IoDs and EH-IoDs are identical, i.e., $K = M = 1$.

In the following simulations, comparisons of average secrecy sum rates for different algorithms are presented, including the BRB-based iterative algorithm without Gaussian randomization (denoted as "BRB" in the legend), the BRB-based iterative algorithm with Gaussian randomization (denoted as "BRB-GR" in the legend), the CCCP-based iterative algorithm (denoted as "CCCP" in the legend) and the ZF-based non-iterative algorithm (denoted as "ZF" in the legend). We also consider another algorithm as benchmark, i.e., the maximal-ratio reception and maximal-ratio transmission algorithm in [48] (denoted as "MRR-MRT" in the legend). To demonstrate the benefits of secure beamforming design, we include the scheme without beamforming (denoted as "No-BF" in the legend), where the elements of beamforming matrix and vectors are set equal to 1.

A. Convergence Performances of the Proposed Iterative Algorithms

In Fig. 2, we present the average secrecy sum rate achieved by the BRB-based iterative algorithm versus the total number of feasibility evaluations. The number of antennas at the controller is $N = 3$ and the transmit power to noise power ratio is $P_r/\sigma^2 = 25$ dB. The bisection method is applied with a line-search accuracy $\delta = 0.01$ and the accuracy for termination is $\varepsilon = 0.1$. As shown in Fig. 2, the convergence characteristics of two different transmit power scenarios are studied, where the upper bound and lower bound of the objective gradually converge into a straight line with the number of feasibility evaluations increase. It is also observed that it takes both approximately 800 times of feasibility evaluations to converge in these two scenarios.

In Fig. 3, we present the average secrecy sum rate achieved by the CCCP-based iterative algorithm for different transmit power of primary users, where the transmit power to noise power ratio of the controller is $P_r/\sigma^2 = 30$ dB and the number of antenna is 4. As shown in Fig. 3, the average secrecy sum rate is achieved steadily after about 5 iterations, regardless of P/σ^2. Compared to the convergence performance of the BRB-based algorithm shown in Fig. 2, it consumes less iteration times to converge in the CCCP-based algorithm.

B. Average Secrecy Sum Rate Versus the Transmit Power at PUs

In Fig. 4, we present the average sum rate comparisons of different secure beamforming algorithms for various transmit power to noise power ratios of primary users, P/σ^2. The number of antennas at the controller is $N = 3$ and its transmit power to noise power ratio is $P_r/\sigma^2 = 30$ dB. As shown in Fig. 4, the performance of the BRB algorithm outperforms

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2941873, IEEE Internet of Things Journal

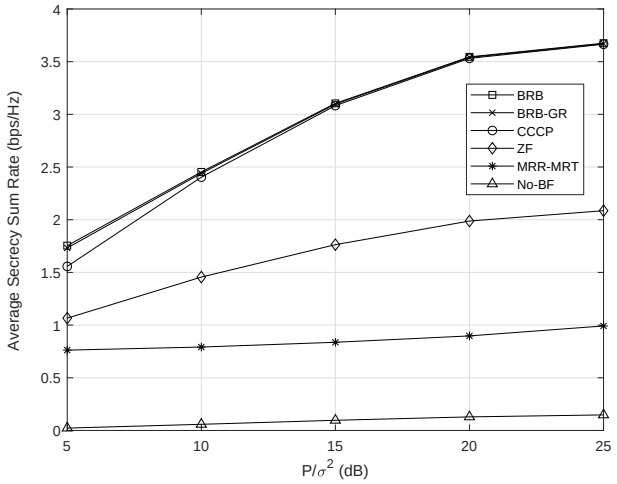

Fig. 4. Average secrecy sum rate versus P/σ^2; performance comparison of different algorithms when the transmit power and the number of antennas at the controller are $P_r/\sigma^2 = 30$ dB and $N = 3$.

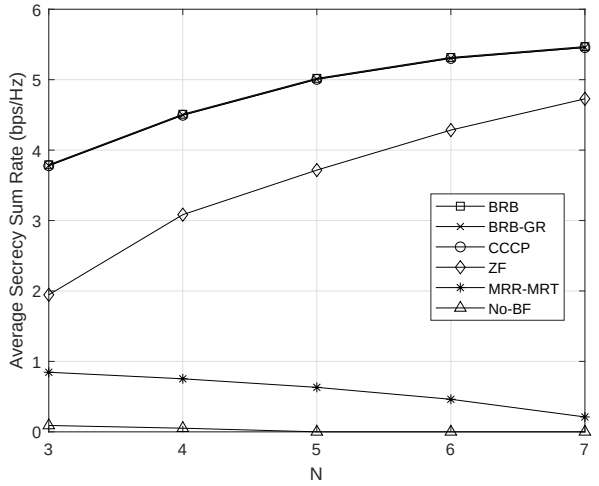

Fig. 6. Average sum rate versus N when the transmit power to noise power ratios of the controller and primary users are $P_r/\sigma^2 = 30$ dB and $P/\sigma^2 = 20$ dB.

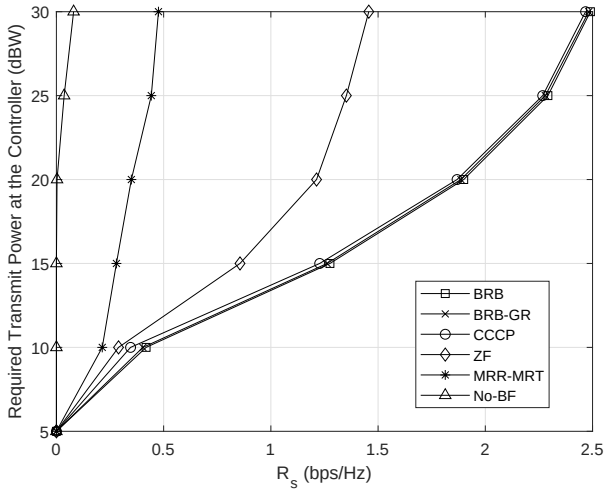

Fig. 5. Required transmit power at the controller versus R_s when the transmit power to noise power ratio of primary users is $P/\sigma^2 = 10$ dB and the number of antennas at the controller is $N = 3$.

the BRB-GR algorithm slightly, which results from that the Gaussian randomization procedure in BRB-GR requires rank-one solution. Besides, the two scheme based on BRB are superior to CCCP in lower P/σ^2 region and they achieve almost the same performance in high P/σ^2, which demonstrates that the suboptimal solution obtained by BRB schemes offers almost the upper bound among all schemes. With lower computational complexity, CCCP algorithm can achieve most of the performance of BRB algorithm, which is suitable for the IoT device with poor processing ability. Moreover, MRR-MRT and No-BF schemes with least computational complexity are left far behind by the proposed schemes, which verifies the effectiveness of our proposed schemes.

C. Required Transmit Power at the Controller Versus Average Secrecy Sum Rate

In this subsection, we further investigate the required transmit power at the controller, i.e., P_r for different secrecy sum rates, where the transmit power to noise power ratio at primary users is $P/\sigma^2 = 10$ dB and the number of antennas is 3. From Fig. 5, it is observed that higher transmit power at the controller is required when we want to improve the secrecy sum rate for all schemes. Furthermore, for the fixed secrecy sum rate, the required transmit power at the controller in CCCP scheme is larger than the one in BRB schemes, which demonstrates that the schemes based on BRB are more energy-efficient. Besides, to provide valid cooperative security, it consumes more power at controller in the ZF and MRR-MRT schemes. However, without the optimization on beamforming, the No-BF scheme can not guarantee secure communication when the transmit power at controller P_r is in the lower region.

D. Average Secrecy Sum Rate Versus the Number of Antennas at the Controller

In Fig. 6, we show the average secrecy sum rate for different number of transmit antennas at the controller when the transmit power to noise power ratio of the controller and primary users are $P_r/\sigma^2 = 30$ dB and $P/\sigma^2 = 20$ dB. As shown in Fig. 6, with the increase of N, the average secrecy sum rates of our proposed algorithms increase while the MRR-MRT scheme decreases. For the proposed algorithms, more transmit antennas at the controller can make full use of the space resources and enhance the transmission gain. While for the MRR-MRT algorithm, it is more likely to produce infeasible solutions when more antennas are used to construct larger transmit matrices. The No-BF scheme can not take advantage of multiple antennas, which accounts for its poor performance.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2941873, IEEE Internet of Things Journal

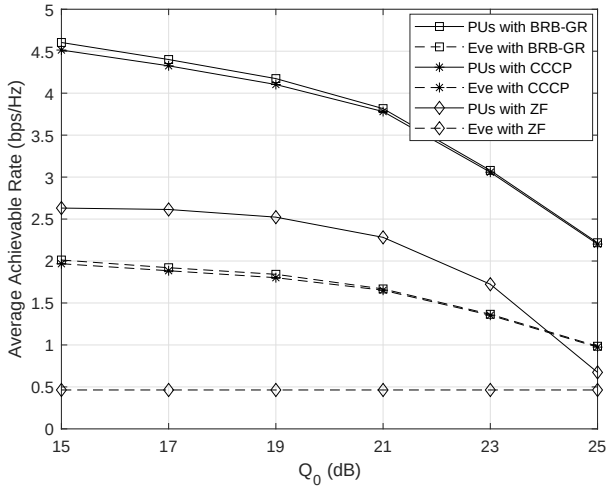

Fig. 7. Average achievable rates of primary users and eavesdropper versus Q_0 when the transmit power to noise power ratio and the number of antennas at the controller are $P_r/\sigma^2 = 20$ dB and $N = 4$, respectively.

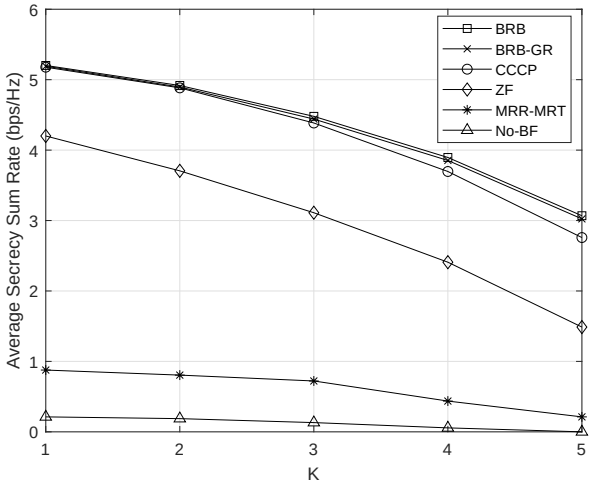

Fig. 8. Average secrecy sum rate versus K when the transmit power to noise power ratios of the controller and primary users are $P_r/\sigma^2 = 30$dB and $P/\sigma^2 = 20$dB, and the number of antennas at controller is $N = 6$.

E. Effect of the EH Threshold on Average Achievable Rates of PUs and Eavesdropper

In Fig. 7, we set the EH threshold Q_0 from 15 dB to 25 dB to investigate its effect on the achievable rates of primary users and eavesdropper with proposed algorithms, where the parameters are set as $P/\sigma^2 = 10$ dB, $P_r/\sigma^2 = 30$ dB and $N = 4$. Generally, the average achievable sum rates of primary users achieved by all algorithms decrease with the increase of EH thresholds on IoDs, which results from that higher QoS level demands more energy provided by controller and therefore lower the system performance. Compared to ZF scheme, BRB-GR and CCCP algorithms can obtain much better results and these two algorithms perform close with higher EH threshold, which is because the higher Q_0 leads to frequent occurrence of infeasible solutions when solving the problem. When it comes to the achievable rate of eavesdropper, the results achieved by BRB-GR and CCCP similarly reduce as the increase of Q_0. Besides, since the ZF scheme can force the beamforming vector to be in the null-space of the eavesdropping channel, the achievable rate of eavesdropper is a constant which is related to the random channel responses, regardless of Q_0.

F. Average Secrecy Sum Rate Versus the Number of ID-IoDs and EH-IoDs

In this subsection, we investigate the effect of the number of IoDs in the secondary network. The number of ID-IoDs and EH-IoDs are set identically, i.e., $K = M$, from 1 to 5, and the number of transmit antennas at the controller is $N = 6$. Theoretically, more IoDs to be served in the secondary network means more power needs to be consumed, which will lead to a decline on security performance of the whole system. From Fig. 8, we see that the average secrecy sum rates obtained by all the algorithms decrease with the increase number of IoDs, which verifies our assumptions. It is also found that when the number K is less than 3, the performances of the BRB and CCCP algorithms are close, and when $K > 3$, the difference between them becomes larger, which reveals the stability of BRB-based schemes as more IoDs are involved.

TABLE I
SECRECY SUM RATE (BPS/HZ) COMPARISON OF ALGORITHMS

Algorithm	P_r/σ^2=10dB	P_r/σ^2=20dB	P_r/σ^2=30dB
BRB-GR	0.7227	1.8346	2.1977
CCCP	0.5652	1.8128	2.1829
ZF	0.5091	1.1615	1.1719
MRR-MRT	0.3532	0.4625	0.4962
No-BF	0	0	0.0580

G. Numerical Results for One-time Channel Realization

To further clearly reveal the performances of different algorithms, we compare the secrecy sum rates obtained by the proposed algorithms in Table I for one-time channel realization under different transmit power to noise power ratios at the controller, where the transmit power to noise power ratio of primary users is $P/\sigma^2 = 10$ dB and the number of antenna at controller is 3. From TABLE I, it is observed the proposed BRB algorithm with Gaussian randomization obtains the upper bound of performance for all proposed schemes under different P_r/σ^2. Besides, the CCCP algorithm performs close to BRB-GR scheme only in the high value region of P_r/σ^2 and both of them outperform the ZF and MRR-MRT schemes. It is also found that without secure beamforming design, the benefits of multi-antenna technique can not be exploited, which leads to poor performance.

VII. CONCLUSIONS

In this paper, we have proposed the BRB-based iterative algorithm, CCCP-based iterative algorithm and the ZF-based non-iterative algorithm for secure information transmission in the two-way CR IoT network with SWIPT. Simulation results

have shown that the the BRB-based iterative algorithm with or without Gaussian randomization procedure achieve the best performances among the proposed schemes, which verifies that BRB offers almost the upper bound for the problem. The CCCP-based iterative algorithm with lower computational complexity performs close to the BRB scheme, which strikes a balance between complexity and performance. Moreover, the ZF-based non-iterative algorithm with the lowest complexity obtains relatively poor performances, which is suitable for the IoT network with limited power supply at the controller.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: a survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet of Things J.*, vol. 1, no. 1, pp. 22-32, Feb. 2014.

[3] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Thing J.*, vol. 3, no. 6, pp. 854-864, Jun. 2016.

[4] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi, and S. He, "Narrowband Internet of Things: Implementations and applications," *IEEE Internet of Things J.*, vol. 4, no. 6, pp. 2309-2314, Dec. 2017.

[5] E. Nilsson and C. Svensson, "Power consumption of integrated lowpower receivers," *IEEE J. Emerging Sel. Topics Circu. Syst.*, vol. 4, no. 3, pp. 273-283, Sep. 2014.

[6] Q. Qi and X. Chen, "Wireless powered massive access for cellular Internet of Things with imperfect sic and non-linear EH," *IEEE Internet of Things J.*, DOI 10.1109/JIOT.2018.2878860, 2018.

[7] Z. Na, J. Lv, F. Jiang, M. Xiong, and N. Zhao, "Joint subcarrier and subsymbol allocation based simultaneous wireless information and power transfer for multiuser GFDM in IoT," *IEEE Internet of Things J.*, DOI 10.1109/JIOT.2018.2865248, 2018.

[8] Y. Huang, M. Liu, and Y. Liu, "Energy-efficient SWIPT in IoT distributed antenna systems," *IEEE Internet of Things J.*, vol. 5, pp. 2646-2656, Jan. 2018.

[9] J. Tang, D. K. C. So, N. Zhao, A. Shojaeifard, and K. Wong, "Energy efficiency optimization with SWIPT in MIMO broadcast channels for Internet of Things," *IEEE Internet of Things J.*, vol. 5, pp. 972-978, Aug. 2018.

[10] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1612-1616, 2008.

[11] 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.

[12] J. Xu, L. Liu, and R. Zhang, "Multiuser MISO beamforming for simutaneous wireless information and power transfer," in *Proc. IEEE ICASSP*, pp. 4754-4758, 2013.

[13] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.* , vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

[14] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29-33, Sep. 1998.

[15] A. Jamalipour and Y. Bi, "Enhancing physical layer security in wireless powered communication networks", in *Wireless Powered Communication Networks*, pp. 25-70, Oct 2018.

[16] X. Hong, "Enhancing physical layer security in wireless powered communication networks: challenges and opportunities", *Ph.D thesis in King's College London*, 2016.

[17] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: challenges and solutions," *Entropy*, vol. 20, no. 10, 2018.

[18] A. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[20] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29-40, Sep. 2013.

[21] 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, March 2010.

[22] S. Zhang, X. Xu, H. Wang, D. Zhang, and K. Huang, "Enhancing the physical layer security of uplink non-orthogonal multiple access in cellular internet of things," *IEEE Access*, vol. 6, pp. 58405-58417, 2018.

[23] L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in internet of things ," *IEEE Internet of Things J.*, vol.5, Feb. 2018.

[24] J. Hu, N. Yang and Y. Cai, "Secure downlink transmission in the Internet of Things: How many antennas are needed?," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1622-1634, July 2018.

[25] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[26] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127-2159, 2006.

[27] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-radiobased internet of things: Applications, architectures, spectrum related functionalities, and future research directions," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 17-25, June 2017.

[28] R. Tian, Z. Wang, and X. Tan, "A new leakage-based precoding scheme in IoT oriented cognitive MIMO-OFDM systems," *IEEE Access*, vol. 6, pp. 41023-41033, 2018.

[29] A. Shahini, A. Kiani, and N. Ansari, "Energy efficient resource allocation in EH-enabled CR networks for IoT," *IEEE Internet of Things J.*, DOI 10.1109/JIOT.2018.2880190, 2018.

[30] D. S. Gurjar, Ha H. Nguyen, and H. D. Tuan, "Wireless information and power transfer for IoT applications in overlay cognitive radio networks," *IEEE Internet of Things J.*, DOI 10.1109/JIOT.2018.2882207, 2018.

[31] G. Zheng, Z. Ho, E. A. Jorswieck, and B. Ottersten, "Information and energy cooperation in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2290-2303, May, 2014.

[32] Q. Li and L. Yang, "Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Trans. Inf. Forensics and Security*, pp. 1-14, 2019.

[33] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532-3545, 2012.

[34] E. Bjornson, G. Zheng, M. Bengtsson, and B.Ottersten, "Robust monotonic optimisation framework for multicell MISO systems," *IEEE Trans. Signal Process.*, vol. 60, pp. 2508-2523, May 2012.

[35] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems", *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20-34, May 2010.

[36] R. Horst and N.V. Thoai, "DC programming: overview," *J. Optim. Theory Appl.,* vol.103, no.1, pp. 1-43, Oct. 1999.

[37] A. J. Smola, S.V.N.Vishwanathan, and T. Hofmann, "Kernel methods for missing variables," in *Proc. 10th Int. Workshop Artific. Intell. Stat.,* Mar. 2005, pp. 325-332.

[38] Q. Li and L. Yang, "Robust optimization for energy efficiency in MIMO two-way relay networks with SWIPT," *IEEE Syst. J.*, pp. 1-12, 2019.

[39] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747-1761, Oct. 2015.

[40] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of Vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356-5373, 2016.

[41] Y. Cao, O. Kaiwartya, C. Han, K. Wang, H. Song and N. Aslam, "Toward distributed battery switch based electro-mobility using publish/subscribe System," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10204-10217, Nov. 2018.

[42] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35-38, Jan, 2013.

[43] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014.

[44] S. Boyd and L. Vandenberghe, "Convex optimization", Cambridge, U.K. *Cambridge Univ. Press*, 2004.

[45] A. Charnes and W. W. Cooper, "Programming with linear fractional functions," *Naval Res. Logist. Quater,* vol. 9, no. 3/4, pp.181-186, Sep./Dec., 1962.

[46] W. Ai, Y. Huang, and S. Zhang, "New results on Hermitian matrix rank-one decomposition," *Math. Programm.,* vol. 128, no. 1/2, pp. 253-283, Jun. 2011.

[47] M. Grant and S. Boyd, CVX: Matlab Software for Disciplined Convex Programming. Available: http://cvxr.com/cvx.

[48] R. Zhang, Y.-C. Liang, C. C. Chai, and S. Cui, "Optimal beamforming for two-way multi-antenna relay channel with analogue network coding," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 699-712, Jun. 2009.

Zhishan Deng received the B.Eng. degree in communication engineering from Guangdong University of Technology, Guangzhou, China, in 2017. He is currently pursuing the M.S. degree with the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China. His research interests include wireless communications powered by energy harvesting, cognitive radio, cooperative communications, and multiple-input-multiple-output communications.

Quanzhong Li received the B.S. and Ph.D. degrees from Sun Yat-sen University (SYSU), Guangzhou, China, both in information and communications engineering, in 2009 and 2014, respectively.

He is currently an Associate Professor with the School of Data and Computer Science, SYSU. His research interests include UAV communications, non-orthogonal multiple access, wireless communications powered by energy harvesting, cognitive radio, cooperative communications, and multiple-input-multiple-output communications.

Qi Zhang (S'04-M'11) received the B.Eng. (Hons.) and M.S. degrees from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1999 and 2002, respectively. He received the Ph.D. degree in electrical and computer engineering from the National University of Singapore (NUS), Singapore, in 2007.

He is currently an Associate Professor with the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China. From 2007 to 2008, he was a Research Fellow with the Communications Lab, Department of Electrical and Computer Engineering, NUS. From 2008 to 2011, he was with the Center for Integrated Electronics, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China. His research interests include UAV communications, non-orthogonal multiple access, wireless communications powered by energy harvesting, cooperative communications, ultra-wideband communications.

Liang Yang was born in Hunan, China. He received the Ph.D. degree in electrical engineering from Sun Yat-sen University, Guangzhou, China, in 2006.

From 2006 to 2013, he was a Teacher at Jinan University, Guangzhou. He joined the Guangdong University of Technology in 2013. He is currently a Professor at Hunan University, Changsha, China. His current research interest includes the performance analysis of wireless communications systems.

Jiayin Qin received the M.S. degree in radio physics from the Huazhong Normal University, Wuhan, China, in 1992 and the Ph.D. degree in electronics from Sun Yat-sen University (SYSU), Guangzhou, China, in 1997.

He is currently a Professor with the School of Electronics and Information Technology, SYSU. From 2002 to 2004, he was the Head of the Department of Electronics and Communication Engineering, SYSU. From 2003 to 2008, he was the Vice Dean of the School of Information Science and Technology, SYSU. His research interests include wireless communications and submillimeter wave technology.

He was the recipient of the IEEE Communications Society Heinrich Hertz Award for Best Communications Letter in 2014, the Second Young Teacher Award of Higher Education Institutions, Ministry of Education (MOE), China in 2001, the Seventh Science and Technology Award for Chinese Youth in 2001, and the New Century Excellent Talent, MOE, China in 1999.