Optimization of Secure Wireless Communications for IoT Networks in the Presence of Eavesdroppers

Sami Ahmed Haider, Muhammad Naeem Adil, MinJian Zhao

Abstract

The problem motivates this paper is that securing the critical data of 5G based wireless IoT network is of significant importance. Wireless 5G IoT systems consist of a large number of devices (low-cost legitimate users), which are of low complexity and under strict energy constraints. Physical layer security (PLS) schemes, along with energy harvesting, have emerged as a potential candidate that provides an effective solution to address this issue. During the data collection process of IoT, PHY security techniques can exploit the characteristics of the wireless channel to ensure secure communication. This paper focuses on optimizing the secrecy rate for simultaneous wireless information and power transfer (SWIPT) IoT system, considering that the malicious eavesdroppers can intercept the data. In particular, the main aim is to optimize the secrecy rate of the system under signal to interference noise ratio (SINR), energy harvesting (EH), and total transmits power constraints. We model our design as an optimization problem that advocates the use of additional noise to ensure secure communication and guarantees efficient wireless energy transfer. The primary problem is non-convex due to complex objective functions in terms of transmit beamforming matrix and power splitting ratios. We have considered both the perfect channel state information (CSI) and the imperfect CSI scenarios. To circumvent the non-convexity of the primary problem in perfect CSI case, we proposed a solution based on the concave-convex procedure (CCCP) iterative algorithm, which results in a maximum local solution for the secrecy rate. In the imperfect CSI scenario, we facilitate the use of S-procedure and present a solution based on the iterative successive convex approximation (SCA) approach. Simulation results present the validations of the proposed algorithms. The results provide an insightful view that the proposed iterative method based on the CCCP algorithm achieves higher secrecy rates and lower computational complexity in comparison to the other algorithms.

I. Introduction

IInternet of Things (IoT) has emerged as an integrated part of the present communication system and has tremendous applications in security, logistics, quality control agriculture, etc. [1]–[3]. Wireless communication (e.g., wireless sensor network) is one of the key enabling technologies of IoT as it plays a significant role in data collection at the nodes. Security of the wireless medium is a great concern for communication systems because of their susceptibility to eavesdropping due to the nature of the wireless medium and its inherent characteristics [4]. Traditionally, the wireless communication systems rely on the application layer cryptographic algorithms for secure communication, however, due to the complexity of the encryption and decryption algorithms and limited computational capabilities of the edge points, it might not be a suitable choice for IoT [5], [6]. In order to cover the computational complexity of the conventional higher layered cryptographic algorithms, physical layer security (PLS) algorithms have emerged as the potential solution. From the information theory perspective, PLS algorithms are capable of ensuring secure communication by exploiting the characteristics of the wireless channel.

Massive IoT in 5G is possible with the advancements in low power efficient communicating devices. Energy harvesting techniques, along with secrecy, will be a good choice for future IoT. Electromagnetic (EM) energy transfer techniques have emerged as one of the potential research areas over the energy crises. Simultaneous wireless information and power transfer (SWIPT) is a potential technique to overcome the bottleneck for providing sufficient power. In this method, the transmitter collectively transmits the energy signal along with the information signal [7]–[10]. SWIPT has been recognized as a promising technology to solve the energy scarcity problem in energy-constrained 5G wireless communication systems. The idea of SWIPT was first proposed by Varshney in [11], in which he characterizes the rate-energy trade-off in a discrete memory-less channel. Mainly there are two main techniques for the application of SWIPT, time switching (TS), and the power splitting (PS). In TS technique, the receiver switches between the information decoding (ID) and energy harvesting (EH) at any time [12], [13], while in the later the receiver splits the signal into two streams, such that a fraction ρ $(0 \leq \rho \leq 1)$ of the received signal power is used for information decoding while the remaining $(1-\rho)$ is used for energy harvesting, respectively [14], [15].

Focusing on this problem, secure communication in SWIPT systems has recently been pursued in a different context [16]. In SWIPT systems, we exploit the physical layer characteristics of the wireless channel such as fading and interference [17], to counter eavesdropping and ensure secure communication. Energy harvesting systems, specifically focus on beamforming with additional noise (AN) signal to ensure secure communication in wireless channels [18], [19]. Wyner first introduced the concept of secrecy capacity in [20], in which he defined secrecy as the difference of mutual information between the legitimate channel and the wire-tap channel. Most of the previous work done in secure beamforming SWIPT system broadcast channels (BC) consider perfect channel state information (CSI) for the eavesdroppers (ED) as well as the users in the system [21]–[24].

S.A Haider is with the Department of Computing, University of Worcester,e-mail: (s.ahmedhaider@worc.ac.uk).

M.N. Adil and M.J.Zhao are with the School of Information Science and Communication Engineering,Zhejiang Provincial key laboratory of Information Network Technology, Zhejiang University, Hangzhou, 310027, P.R.China

However, due to the practical limitations, such as the quantization errors, delay errors, and limited feedback channel capacity, the transmitter is unable to get the perfect CSI. Recently, some potential work have been done, keeping into consideration the imperfect CSI for eavesdroppers, for secure SWIPT beamforming system [25]–[29]. To be more specific, [28] maximize the secrecy rate of the system model for SWIPT in the nonregenerative multi-antenna relay network with one energy receiver (ER), one information receiver (IR) and one eavesdropper. The authors proposed a constrained convex-concave procedure (CCCP) based on an iterative algorithm to maximize the secrecy rate and achieve a local optimum. Moreover, they proposed non-iterative semidefinite programming (SDP) based suboptimal solution and closed-form suboptimal solution. In [30], the authors proposed a suboptimal Gaussian randomization solution based on semidefinite relaxation (SDR) upper and lower bounds with one IR, one ER, and one ED, respectively. The authors in [29] take channel errors into account and proposed a worst-case secrecy rate maximization problem via SDP programming. They also focused on the stochastic uncertainty model and proposed a suboptimal solution for outage probability secrecy rate maximization based robust design. In [31], AN aided secrecy rate for multiple-input single-output (MISO) channel in the presence of multiple antennas eavesdroppers was investigated under both perfect and imperfect CSI. The author in [25] studied the max-min fairness EH among multiple multi-antennas energy receivers with channel errors considering power splitting. In [32], a SWIPT system with multiple antennas at ER and ID with perfect and imperfect CSI in the presence of AN was studied. The authors proposed a novel bisection search based reformulation of secrecy rate maximization problem into an associated power minimization problem. SWIPT in two-tier heterogeneous networks was studied in [27], for perfect CSI case two-stage problem based on SDR and one-dimensional line search were proposed, and successive convex approximation (SCA) approach has been applied for robust beamforming.

To summarize, research on SWIPT mainly focuses on traditional architectures, and the research for secrecy rate maximization for the SWIPT system with multiple users and eavesdroppers is still an open problem. SWIPT communication system with multiple users in the presence of eavesdroppers brings new challenges for secure joint beamforming and power splitting (JBPS) design. To the best of our knowledge, the security issue in JBPS design is still an open problem. This paper focuses on optimizing the secrecy rate of the wireless communication system, which consist of multiple transmit antennas, with K single antenna legitimate receivers and L single antenna eavesdroppers The desired user is assumed to adopt PS scheme to decode information and harvest energy, while the idle receivers can harvest energy at the same time. We study the design of the joint transmit beamforming vector for the desired user, with a combination of additional noise and power splitting ratio to maximize the secrecy rate. The main contributions of this paper are summarized below.

- Assuming perfect CSI, we first investigate the secure transmission issue for the SWIPT MISO system. Particularly, the transmit beamforming vectors and AN are jointly designed to optimize the secrecy rate of the system. The original problem is a non-convex due to the coupling of the optimization variable and is a hard optimization problem. In order to solve this non-convexity issue, we proposed a CCCP based iterative algorithm. By the application of this proposed algorithm, the original problem can be decomposed into subproblems. Each sub-problem in the iterative CCCP algorithm can be transformed into a second-order cone programming (SOCP) problem. The problem is guaranteed to converge to a locally optimal point.
- Further, we extend the secure beamforming optimization problem to the case of imperfect CSI, while considering the worst-case based optimization framework for secure communication. In this case, the beamforming vectors and AN is jointly designed to maximize the worst-case secrecy rate under transmit power constraint while guaranteeing the data transmit constraint, the energy harvesting constraints, and the worst-case transmission security constraint for eavesdroppers. We model imperfect CSI cases based on the deterministic norm bounded error CSI model. The problem is non-convex due to intractable semi-infinite constraints and the complex objective function. We facilitate the use of S- procedure for transforming semi-infinite constraints to linear matrix inequalities (LMI). The SCA approximation is applied to solve the non-convexity of the remaining constraint. The approximation can be refined at each iteration, and the local optimum of the original problem can be obtained.

The remainder of this paper is organized as follows. Section II presents the multi-user MISO system model and problem formulation. In Section III, joint beamforming and AN designed is proposed with a perfect CSI scenario. Section IV discusses the optimization design for the robust case. Finally, in Section V simulation results are presented to verify the proposed algorithm and conclusions are drawn in Section VI.

Notation: Boldfaced lower case and upper case letters represent vectors and matrices, respectively. $(\mathbf{A})^H$, $\|\mathbf{A}\|$ and $Tr(\mathbf{A})$ denote hermitian, Eculidean norm and trace of matrix $\mathbf{A}$, respectively. $\mathbb{R}^{m\times n}$ denotes the space of $m \times n$ real matrices and $\mathbb{R}_+$ denotes the set of positive real numbers. $\mathbf{A} \succeq 0$ denotes that $\mathbf{A}$ is a positive semi-definite matrix and $Rank(\mathbf{A})$ is the rank of matrix $\mathbf{A}$. $\mathbf{I}_{N\times N}$ denotes an $N \times N$ identity matrix. The operator vec(.) stacks the elements of a matrix in one long column vector, invp(x) denotes the inverse of the positive portion.

II. System Model

In this paper, the system is modeled as the SWIPT wireless communication system, as shown by Fig. 1. The system has N_T transmit antennas can be considered as the source in terms of the IoT network model, the source or the transmit antenna

Notation	Definitation
N_T	The number of transmit antennas
K	The number of legitimate single antenna users
L	The number of single antenna eavesdroppers
$\mathbf{f}_k$	Beamforming vector for receiver k
$\mathbf{h}_k$	The channel between transmit antenna and k user
$\mathbf{g}_l$	The channel between transmit antenna and eavesdropper
s_k	The message intended for receiver k
n_s	The noise due to signal processing
$\mathbf{V}$	The noise covariance matrix
R_{sec}	The secrecy rate
E_k	The harvested energy of the k user
P_t	The total transmit power
ρ_k	The power splitting ratio
γ_k	The minimum target SINR at each receiver k
e_k	The required energy threshold at each receiver k
invp(a)	Inverse of a

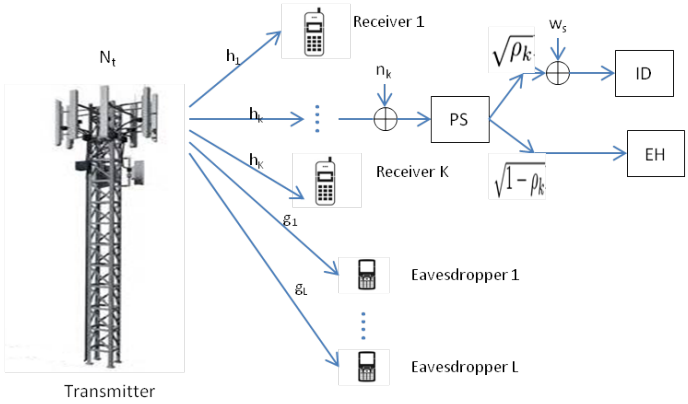

Fig. 1. System Model

is capable of transmitting K independent message to K single antennas legitimate receivers which can relay simultaneously. In addition, L single antenna passive eavesdroppers are also present in the system. The wireless system from the relay to the destination is not considered in this particular scenario, but the same algorithm can be applied in terms of a single-hop wireless network. The direct link between the source and the destination is unavailable due to strong fading effects. The K independent legitimate receivers will act as the relay to forward messages from the sinking node to the destination node.

III. Problem Formulation

The based band signal is expressed as

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{f}_k s_k + \mathbf{v} \tag{1}$$

where $s_k \in \mathbb{C}$ is the message intended for receiver k, $v \in \mathbb{C}^{N_T \times 1}$ denotes the additional noise vector and $\mathbf{f}_k \in \mathbb{C}^{N_T \times 1}$ is the corresponding beamforming vector for receiver k. The AN is modeled as $\mathbf{v} \sim \mathcal{CN}(0, \mathbf{V})$, where $\mathbf{V} = \mathbf{v}\mathbf{v}^H \succeq 0$ is the covariance matrix of $\mathbf{v}$. In the rest of the paper, we use $\mathcal{K} = 1, \ldots, K$ and $\mathcal{L} = 1, \ldots, L$, which denotes the index set of the receivers and the external eavesdroppers, respectively. Without loss of generality, we assume that $s_k \sim \mathcal{CN}(0, 1)$.

The received signal at the k^{th} receiver and l^{th} external eavesdropper are respectively given as

$$y_k = \mathbf{h}_k^H \mathbf{f}_k s_k + \mathbf{h}_k^H \sum_{j \neq k}^{K} \mathbf{f}_j s_j + \mathbf{h}_k^H \mathbf{v} + n_k \quad \forall k \in \{1, \ldots, K\} \tag{2}$$

$$y_l = \mathbf{g}_l^H \sum_{k=1}^{K} \mathbf{f}_k s_k + \mathbf{g}_l^H \mathbf{v} + n_l \quad \forall l \in \{1, \ldots, L\} \tag{3}$$

where $\mathbf{h}_k \in \mathbb{C}^{N_T \times 1}$ is the channel vector between the transmitter and the k^{th} user, $\mathbf{g}_l \in \mathbb{C}^{N_T \times 1}$ denotes the channel vector between the transmitter and the l_{th} passive eavesdropper. It is noted here that the variable $\mathbf{h}_k$ and $\mathbf{g}_l$ includes the effects of the multi path, fading and path loss of the associated channels, respectively. $n_k \sim \mathcal{CN}(0, \sigma_k^2)$ and $n_l \sim \mathcal{CN}(0, \sigma_l^2)$ are modeled as additive white Gaussian noise (AWGN), for k^{th} receiver and for l^{th} eavesdropper, respectively. In addition, we assume that

every receiver k exploits the power splitting scheme to handle the received signal i.e capable of denoting the information from the received signal and will harvest energy at the same time. Specifically, at receiver k, $\rho_k (0 \leq \rho_k \leq 1)$ portion of the signal power is consumed for information decoding and $1-\rho_k$ is used for energy harvesting.

Therefore, we can write Eq.(2) as

$$\begin{aligned} y_k^{ID} =& \sqrt{\rho_k}\Big(\mathbf{h}_k^H \mathbf{f}_k s_k + \mathbf{h}_k^H \sum_{j\neq k}^{K} \mathbf{f}_j s_j + \mathbf{h}_k^H \mathbf{v} + n_k\Big) \\ &+ n_s \quad \forall k \in \{1,\ldots,K\} \end{aligned} \tag{4}$$

where $n_s \sim \mathcal{CN}(0,\omega_s^2)$ is the additional noise caused by the signal processing.

The equivalent energy harvested signal at the receiver k can be expressed as

$$\begin{aligned} y_k^{ED} =& \sqrt{1-\rho_k}\Big(\mathbf{h}_k^H \mathbf{f}_k s_k + \mathbf{h}_k^H \sum_{j\neq k}^{K} \mathbf{f}_j s_j + \mathbf{h}_k^H \mathbf{v} + n_k\Big) \\ &\forall k \in \{1,\ldots,K\} \end{aligned} \tag{5}$$

The signal to noise interference ratio (SINR) between the transmitter and idle receivers (potential eavesdroppers) k is given as [31]

$$SINR_k = \frac{\mathbf{f_k}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_k}}{\sum\limits_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + Tr(\mathbf{h}_k \mathbf{h}_k^H \mathbf{V}) + \sigma_k^2 + \frac{\omega_s^2}{\rho_k}} \forall k \tag{6}$$

On the other hand, the EH efficiency at the receiver k can be expressed as [32]

$$E_k = (1-\rho_k)\eta\big(\sum_{k=1}^{K} |\mathbf{h_k^H w}|^2 + Tr(\mathbf{h}_k \mathbf{h}_k^H \mathbf{V}) + \sigma_k^2\big), \qquad \forall k \tag{7}$$

where $\eta \in (0,1]$ denotes the EH efficiency at the receivers in converting the received radio signals to the electrical signals.

IV. Secure Beamforming with perfect CSI

The main is to optimize the secrecy rate of the wireless system. In this section, assuming perfect CSI, the focus is on jointly designing the beamforming vectors subject to the users SINR, EH and the transmit power constraints, in order to optimize the secrecy rate of energy harvested system. To begin with, the secrecy rate considering the worst case scenario is given by [46]

$$R_{sec} = \Big[log(1+SINR_k) - \max_{l\in 1,\ldots,L} log(1+SINR_l)\Big]^+ \tag{8}$$

The optimal resource allocation policy,$\{\mathbf{f}_k^*, \rho_k^*\}$, for maximizing the secrecy rate can be obtained by solving

$$\max_{\mathbf{f_k},\mathbf{V},\rho_k} \quad \min_{l\in\{1,\ldots,L\}} log \frac{\left(1+\frac{\mathbf{f_k}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_k}}{\sum\limits_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \mathbf{h}_k^H \mathbf{V} \mathbf{h}_k + \sigma_k^2 + \frac{\omega_s^2}{\rho_k}}\right)}{\left(1+\frac{\mathbf{f_k}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_k}}{\sum\limits_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_j} + \mathbf{g}_l^H \mathbf{V} \mathbf{g}_l + \sigma_l^2}\right)} \tag{9a}$$

$$\text{s.t} \quad SINR_k \geq \gamma_k, \ \forall k \tag{9b}$$

$$E_k \geq e_k, \ \forall k \tag{9c}$$

$$\sum_{k=1}^{K} |\mathbf{f}_k|^2 + Tr(\mathbf{V}) \leq P_t \tag{9d}$$

$$0 \leq \rho_k \leq 1 \ \forall k \in K \tag{9e}$$

where constraint (9b) is due to quality of service (QoS) which require that minimum SINR at each receiver k should be greater than the target value γ_k, constraint (9c) ensures that the minimum harvested energy threshold e_k should be satisfied at each receiver, (9d) ensures that the total minimum transit power is minimized while maximizing the secrecy rate of the system. Maximizing the secrecy rate in problem (9) is a non convex due to the non-convexity of the objective function and the coupling of optimization variable $\mathbf{f}_k$ and ρ_k in constraints (9b), (9c) and (9d). Since logarithmic function is monotonically increasing, therefore, it can be dropped from the objective function (9a). Problem (9) can be reformulated as

$$\max_{\mathbf{f_k},\mathbf{V},p_k,q_k,y,x,z} \quad z \tag{10a}$$

$$\text{s.t} \quad xy \geq z \tag{10b}$$

$$\left(1+\frac{\mathbf{f_k}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_k}}{\sum\limits_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_j} + \mathbf{g}_l^H \mathbf{V} \mathbf{g}_l + \sigma_l^2}\right) \leq (\frac{1}{y}) \tag{10c}$$

$$\left(1+\frac{\mathbf{f_k}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_k}}{\sum\limits_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \mathbf{h}_k^H \mathbf{V} \mathbf{h}_k + \sigma_k^2 + \omega_s^2 \rho_k}\right) \geq (x) \tag{10d}$$

$$\frac{1}{\gamma_k} \mathbf{f_k}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_k} \geq \sum_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \mathbf{h}_k^H \mathbf{V} \mathbf{h}_k + \sigma_k^2 + \omega_s^2 p_k \tag{10e}$$

$$\sum_{k=1}^{K} |\mathbf{h_k^H w}|^2 + \mathbf{h}_k^H \mathbf{V} \mathbf{h}_k + \sigma_k^2 \geq \frac{e_k q_k}{\eta_k} \tag{10f}$$

$$\sum_{k=1}^{K} \mathbf{f}_k^H \mathbf{f}_k + Tr(\mathbf{V}) \leq P_t \tag{10g}$$

$$p_k \geq 1, q_k \geq 1, invp(p_k) + invp(q_k) \leq 1, \ \forall k, \quad x > 0, \quad y > 0 \tag{10h}$$

where $p_k = \frac{1}{\rho_k}$, $q_k = \frac{1}{1-\rho_k}$, x y and z in constraint (10a), (10b), (10c) and (10h) are the slack variables, y represents the mutual information at the l^{th} eavesdropper. In problem (10) it is easy to recognize the equivalence of problem (9) and (10) as the constraints in both of the problems will hold at equalities, when the optimal solution is obtained. A larger objective value can be obtained otherwise by increasing the values of the slack variables x , y and z. Therefore, we can deduce that the (10) is equivalent to the original problem (9). The formulated problem (10) is still non-convex. In order to circumvent the non-convexity issue, we proposed a solution that is motivated on the observation that problem (10) can be reformulated to a convex problem by the application of difference of convex (DC) programming. In DC programming, we make use of CCCP [33], [34] algorithm to achieve local optimal solution, iteratively.The detailed procedure is explained below. In order to further simplify the algorithm, we define the following vectors:

$$\begin{aligned} \mathbf{p} &= [p_1, \ldots, p_k]^T, \quad \mathbf{q} = [q_1, \ldots, q_k]^T \\ \mathbf{f} &= [\mathbf{f_1^T}, \ldots, \mathbf{f_k^T}]^T, \quad \mathbf{r} = [\mathbf{p}^T, \mathbf{q}^T, \mathbf{f}^T, x, y]^T, \end{aligned} \tag{11}$$

Applying the vectors formed in equation (11) and rearranging the constraints problem (10) can be reformulated as

$$\max_{\mathbf{f_k}, \mathbf{V}, \mathbf{r}} \quad z \tag{12a}$$

$$\text{s.t} \quad xy \geq z \tag{12b}$$

$$\sum_{j=1}^{K} \mathbf{f_j}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_j} + \mathbf{g}_l^H \mathbf{V} \mathbf{g}_l + \sigma_l^2 - v_l(\mathbf{r}, \mathbf{V}) \leq 0 \tag{12c}$$

$$\sum_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \mathbf{h}_k^H \mathbf{V} \mathbf{h}_k + \sigma_k^2 + \omega_s^2 p_k - x_k(\mathbf{r}, \mathbf{V}) \leq 0 \tag{12d}$$

$$\sum_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \mathbf{h}_k^H \mathbf{V} \mathbf{h}_k + \sigma_k^2 + \frac{\omega_s^2 (p_k+1)^2}{4} - y_k(\mathbf{r}) \leq 0 \tag{12e}$$

$$\frac{e_k (q_k+1)^2}{4} - \sigma_l^2 - z_k(\mathbf{r}, \mathbf{V}) \leq 0 \tag{12f}$$

$$\sum_{k=1}^{K} \mathbf{f}_k^H \mathbf{f}_k + Tr(\mathbf{V}) \leq P_t \tag{12g}$$

$$x > 0, \quad y > 0, \quad p_k \geq 1, q_k \geq 1, invp(p_k) + invp(q_k) \leq 1, \ \forall k \tag{12h}$$

where the last set of inequality constraint (12h) must be satisfied with equality at optimality, otherwise, the objective value can be further decreased by decreasing the p_k. $v_l(\mathbf{r},\mathbf{V})$, $x_k(\mathbf{r},\mathbf{V})$, $y_k(\mathbf{r})$ and $z_k(\mathbf{r},\mathbf{V})$ in constraint (12c),(12d),(12e) and (12f) , respectively can be given as

$$v_l(\mathbf{r},\mathbf{V}) \triangleq \frac{\sum\limits_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_j} + \mathbf{g}_l^H \mathbf{V} \mathbf{g}_l + \sigma_l^2}{y} \tag{13}$$

$$x_k(\mathbf{r},\mathbf{V}) \triangleq \frac{\sum\limits_{j=1}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \mathbf{h}_k^H \mathbf{V} \mathbf{h}_k + \sigma_k^2 + \omega_s^2 p_k}{x} \tag{14}$$

$$y_k(\mathbf{r}) \triangleq \frac{1}{\gamma_k} \mathbf{f_k}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_k} + \frac{\omega_s^2 (p_k-1)^2}{4} \tag{15}$$

$$z_k(\mathbf{r},\mathbf{V}) \triangleq \sum_{j=1}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \mathbf{h}_k^H \mathbf{V} \mathbf{h}_k + \frac{e_k (q_k-1)^2}{4} \tag{16}$$

We remark that (13), (14), (15) and (16) are all convex functions jointly with respect to the variable in $\mathbf{r} \in \mathbb{R}_+^K \times \mathbb{R}_+^K \times \mathbb{C}_+^{KN_t \times 1} \times \mathbb{R}_+ \times \mathbb{R}_+$ and $\mathbf{V}$.

Proposition 1: By using the concept of CCCP, problem (12) can be reformulated into the following DC problem (17).

Proof

Please refer to Appendix A.

Thus, after the application of the CCCP algorithm, the problem (12) in its ith iteration can be formulated into the following convex optimization problem.

$$\max_{\mathbf{r},\mathbf{V},z} \quad z \tag{17a}$$

$$\text{s.t} \quad xy \geq z \tag{17b}$$

$$\sum_{j=1}^{K} \mathbf{f_j}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_j} + \sigma_l^2 - \hat{v}_l(\mathbf{r}^{(i)},\mathbf{V}^{(i)},\mathbf{r},\mathbf{V}) \leq 0 \tag{17c}$$

$$\sum_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \sigma_k^2 + \omega_s^2 p_k - \hat{x}_k(\mathbf{r}^{(i)},\mathbf{V}^{(i)},\mathbf{r},\mathbf{V}) \leq 0 \tag{17d}$$

$$\sum_{j\neq k}^{K} \mathbf{f_j}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{f_j} + \sigma_k^2 + \frac{\omega_s^2 (p_k+1)^2}{4} - \hat{y}_k(\mathbf{r}^{(i)},\mathbf{r}) \leq 0 \tag{17e}$$

$$\frac{e_k (q_k+1)^2}{4} - \sigma_l^2 - \hat{z}_k(\mathbf{r}^{(i)},\mathbf{V}^{(i)},\mathbf{r},\mathbf{V}) \leq 0 \tag{17f}$$

$$\sum_{k=1}^{K} \mathbf{f}_k^H \mathbf{f}_k + Tr(\mathbf{V}) \leq P_t \tag{17g}$$

$$x>0, \quad y>0, \quad p_k \geq 1, q_k \geq 1, invp(p_k) + invp(q_k) \leq 1, \ \forall k \tag{17h}$$

whose solution is given by $\left(\mathbf{r}^{(i+1)},\mathbf{V}^{(i+1)}\right)$

Proposition 2: By introducing the new sets of variables $\tilde{a}_l$, a_l, $\tilde{b}_k$, b_k, $\tilde{c}_k$,c_k, $\tilde{d}_k$ and d_k, $l \in \mathcal{L}$, $k \in \mathcal{K}$, problem (17) can be reformulated into the following SOCP problem (18).

Proof

Proof is given in Appendix B.

It can also be proved that the proposed iterative based CCCP algorithm for optimizing the secrecy rate of $k \in \mathcal{K}$ users converges to a local optimal solution of (9). The proof is similar to that of Lemma 2 and Theorem 1 in [35] and is omitted for brevity. The proposed non-robust secrecy maximization algorithm is summarized in Algorithm 1.

$$\max_{\mathbf{r},\mathbf{V},z} \quad z \tag{18a}$$

$$\text{s.t} \quad \|[2z, x-y]\| \leq x+y \tag{18b}$$

$$\|[\mathbf{s}_l^T, \frac{\tilde{a}_l - a_l - 1}{2}]\| \leq \frac{\tilde{a}_l - a_l + 1}{2} \tag{18c}$$

$$\|[\mathbf{t}_k^T, \frac{\tilde{b}_k - b_k - 1}{2}]\| \leq \frac{\tilde{b}_k - b_k + 1}{2} \tag{18d}$$

$$\|[\mathbf{u}_k^T, \frac{\tilde{c}_k - c_k - 1}{2}]\| \leq \frac{\tilde{c}_k - c_k + 1}{2} \tag{18e}$$

$$\|[\sqrt{\frac{e_k}{4\eta_k}}, \frac{\tilde{d}_k - d_k - 1}{2}]\| \leq \frac{\tilde{d}_k - d_k + 1}{2} \tag{18f}$$

$$\|[\mathbf{f}_1^T, \ldots, \mathbf{f}_K^T]\| + Tr(\mathbf{V}) \leq P_t \tag{18g}$$

$$x > 0, \quad y > 0, \quad p_k \geq 1, q_k \geq 1, invp(p_k) + invp(q_k) \leq 1, \ \forall k \tag{18h}$$

Algorithm 1 The Proposed CCCP-Based Iterative Algorithm

Inputs: Total transmit power P_t, beamforming vector $\mathbf{f}_k$, energy harvesting ratio p_k and q_k, energy harvesting efficiency at each receiver η_k, maximum number of iterations N_{max} and equations (48),(49),(50) and (51).
Define the tolerance accuracy δ
Initialize the algorithm with a feasible point by solving problem (9) using SDP approach [25] to get $\mathbf{r}^{(0)}$, $\mathbf{V}^{(0)}$.
Set the iteration number $i = 0$

repeat
Compute th e affine approximation (13), (14), (15) and (16), respectively.
Solve problem (P5) and assign the solution to $\mathbf{r}^{(i+1)}$ and $\mathbf{V}^{(i+1)}$
Update the iteration number: $i = i + 1$
until Until convergence or max no if iteration is reached i.e $i > N_{max}$.
Outputs: Secrecy rate, slack variable z, vector $\mathbf{r}$ given by equation (11) and covariance matrix $\mathbf{V}$.

V. Robust secure beamforming with Imperfect CSI

Its worth noting that the problem (10) considers a secure SWIPT system under the assumption of perfect CSI. In practice, during the transmission the legitimate receivers send feedback information to the transmit antennas of successful transmission of data packets. As a result of which the transmit antennas are able to refine the channel estimate of the legitimate receivers. Therefore we can assume the perfect CSI for the legitimate receivers during the transmission. However, since there is no communication between the transmit antennas and the eavesdroppers that are present in the coverage area of the base station, the CSI of that particular eavesdroppers becomes outdated. To capture this effect, we consider a worst case imperfect CSI scenario for modeling the resulting CSI uncertainties. The erroneous channel model is based on the deterministic norm-bounded model [36]

Let $\hat{\mathbf{g}}_l$ denotes the estimated channel vector between the transmitter and the eavesdroppers l, respectively. The erroneous channel vector can be described as

$$\mathbf{g}_l = \hat{\mathbf{g}}_l + \Delta\mathbf{g}_l, \qquad \forall l \tag{19}$$

where $\Delta\mathbf{g}_l \in \mathcal{G}_l$ is the CSI error vectors unknown to the transmitter. We assume that the error vectors $\Delta\mathbf{g}_l$ is bounded in their Eculadien norm, that is $\|\Delta\mathbf{g}_l\| \leq \epsilon_l$. The error bounded sets corresponding to these error vectors are respectively defined as

$$\mathcal{G}_l = \{\mathbf{g}_l | \mathbf{g}_l = \hat{\mathbf{g}}_l + \Delta\mathbf{g}_l, \|\Delta\mathbf{g}_l\| \leq \epsilon_l\}, \qquad \forall k \tag{20}$$

The shape and size of $\mathcal{G}_l$ model the type of uncertainty on the estimated CSI, which is linked to the physical phenomena producing the CSI errors. It should be emphasized that the actual errors $\Delta\mathbf{g}_l$ is assumed to be unknown, while the corresponding upper bounds ϵ_l can be obtained using preliminary knowledge about the type of imperfections and/or coarse knowledge of the channel type and main characteristics. In this section, we will address the secure optimization problem by employing the channel error model described above.

The aim is to investigate the secrecy rate maximization problem considering the imperfect CSI for the eavesdroppers. To begin with, in the presence of channel errors for eavesdroppers, problem (10) can be equivalently written as

$$\max_{\mathbf{f}_k, \mathbf{V}, z, p_k, q_k, y, x} \quad z \tag{21a}$$

$$\text{s.t} \quad xy \geq z \tag{21b}$$

$$\max_{\epsilon_1} \left(1 + \frac{\mathbf{f_k}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_k}}{\sum\limits_{j \neq k}^{K} \mathbf{f_j}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{f_j} + \mathbf{g}_l^H \mathbf{V} \mathbf{g}_l + \sigma_l^2}\right) \leq (\frac{1}{y}) \tag{21c}$$

$$\left(1+\frac{\mathbf{f_k}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_k}}{\sum\limits_{j\neq k}^{K}\mathbf{f_j}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_j}+\mathbf{h}_k^H\mathbf{V}\mathbf{h}_k+\sigma_k^2+\frac{\omega_s^2}{\rho_k}}\right)\geq(x) \tag{21d}$$

$$frac1\gamma_k\mathbf{f_k}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_k}\geq\sum_{j\neq k}^{K}\mathbf{f_j}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_j}+\mathbf{h}_k^H\mathbf{V}\mathbf{h}_k+\sigma_k^2+\omega_s^2p_k \tag{21e}$$

$$\sum_{k=1}^{K}|\mathbf{h_k^H}\mathbf{w}|^2+\mathbf{h}_k^H\mathbf{V}\mathbf{h}_k+\sigma_k^2\geq\frac{e_kq_k}{\eta_k} \tag{21f}$$

$$\sum_{k=1}^{K}\mathbf{f}_k^H\mathbf{f}_k+Tr(\mathbf{V})\leq P_t \tag{21g}$$

$$x>0,\quad y>0,\quad p_k\geq1,q_k\geq1,invp(p_k)+invp(q_k)\leq1 \tag{21h}$$

The problem (21) is non-convex due to the infinite constraint in the CSI errors in $\mathbf{g}_l$ and the coupling of the optimization variable $\mathbf{f}_k$ and ρ_k. In order to solve the problem more efficiently, we introduce a slack variables u. The optimization problem can be reformulated as

$$\max_{\mathbf{f}_k,\mathbf{V},z,p_k,q_k,y,x,u,v}\quad z \tag{22a}$$

$$\text{s.t}\quad xy\geq z \tag{22b}$$

$$\min_{\epsilon_1}\sum_{j\neq k}^{K}\mathbf{g}_l^H\mathbf{f}_j\mathbf{f}_j^H\mathbf{g}_l+\mathbf{g}_l^H\mathbf{V}\mathbf{g}_l+\sigma_l^2\geq yu \tag{22c}$$

$$\max_{\epsilon_1}\sum_{j=1}^{K}\mathbf{g}_l^H\mathbf{f}_j\mathbf{f}_j^H\mathbf{g}_l+\mathbf{g}_l^H\mathbf{V}\mathbf{g}_l+\sigma_l^2\leq u \tag{22d}$$

$$\left(1+\frac{\mathbf{f_k}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_k}}{\sum\limits_{j\neq k}^{K}\mathbf{f_j}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_j}+\mathbf{h}_k^H\mathbf{V}\mathbf{h}_k+\sigma_k^2+\frac{\omega_s^2}{\rho_k}}\right)\geq(x) \tag{22e}$$

$$\frac{1}{\gamma_k}\mathbf{f_k}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_k}\geq\sum_{j\neq k}^{K}\mathbf{f_j}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_j}+\mathbf{h}_k^H\mathbf{V}\mathbf{h}_k+\sigma_k^2+\omega_s^2p_k \tag{22f}$$

$$\sum_{k=1}^{K}|\mathbf{h_k^H}\mathbf{w}|^2+\mathbf{h}_k^H\mathbf{V}\mathbf{h}_k+\sigma_k^2\geq\frac{e_kq_k}{\eta_k} \tag{22g}$$

$$\sum_{k=1}^{K}\mathbf{f}_k^H\mathbf{f}_k+Tr(\mathbf{V})\leq P_t \tag{22h}$$

$$x>0,\quad y>0\quad p_k\geq1,q_k\geq1,invp(p_k)+invp(q_k)\leq1 \tag{22i}$$

Now we will try to deal with the non-convex constraints in the problem (22). The function on the right hand side (RHS) of constraint (22c) is quasi convex. We will first deal with the quasi convex problem after that we will apply the S procedure [37] to deal with the infinite constraints for CSI errors. Inspired by the idea of successive convex approximation (SCA) [38], [39] technique as already been used in [27], we will approximate the terms in the right hand side with their convex upper estimates. Assuming $\theta\geq0$, we define the following function

$$c_\theta(a,b)=\frac{\theta}{2}a^2+\frac{1}{2\theta}b^2$$

is always convex and upper estimate of the function $c(a,b)=ab$ for a fixed θ. According to SCA, the RHS yu of constraint 2 can be written as $k_{\theta_1}(y^{(i)},u^{(i)})$, where $\theta_1=\frac{\tilde{u}}{\tilde{y}}$. It is pertinent to note here that initial values i.e $u^{(i)}$, and $x^{(i)}$ are to be selected at random and can be updated by the optimal solution at each iteration. Now we will focus on the infinite constraints, by applying the channel uncertainty model in (19), constraint (22c) and (22d) can be given as

$$\min_{\epsilon_1};\ (\hat{\mathbf{g}}_l+\Delta\mathbf{g}_l)^H\Big(\sum_{j\neq k}^{K}\mathbf{f}_j\mathbf{f}_j^H+\mathbf{V}\Big)(\hat{\mathbf{g}}_l+\Delta\mathbf{g}_l)+\sigma_l^2\geq k_{\theta_1}(y,u) \tag{23}$$

$$\max_{\epsilon_1}(\hat{\mathbf{g}}_l+\Delta\mathbf{g}_l)^H\Big(\sum_{j=1}^{K}\mathbf{f}_j\mathbf{f}_j^H+\mathbf{V}\Big)(\hat{\mathbf{g}}_l+\Delta\mathbf{g}_l)+\sigma_l^2\leq u \tag{24}$$

Since the left hand side of (23) and (24) contains ellipsoidal uncertainty regions, to make the problem more traceable, we introduce some more slack variables t_{1l} and t_{21}. The constraints in (23) and (24) can be transformed as

$$\min_{\epsilon_1}(\hat{\mathbf{g}}_l+\Delta\mathbf{g}_l)^H\Big(\sum_{j\neq k}^{K}\mathbf{F}_j+\mathbf{V}\Big)(\hat{\mathbf{g}}_l+\Delta\mathbf{g}_l)\geq t_{1l} \tag{25}$$

$$t_{1l}+\sigma_l^2\geq k_{\theta_1}(y,u) \tag{26}$$

$$\max_{\epsilon_1}(\hat{\mathbf{g}}_l+\Delta\mathbf{g}_l)^H\Big(\sum_{j=1}^{K}\mathbf{F}_j+\mathbf{V}\Big)(\hat{\mathbf{g}}_l+\Delta\mathbf{g}_l)\leq t_{2l} \tag{27}$$

$$t_{2l}+\sigma_l^2\leq u \tag{28}$$

By applying the S-procedure, we can rewrite (25) and (27) into linear matrix inequality form as

$$\begin{bmatrix}\boldsymbol{\Delta}_1+\lambda_l\mathbf{I}_{N_T} & \boldsymbol{\Delta}_1\hat{\mathbf{g}}_l\\ \hat{\mathbf{g}}_l^H\boldsymbol{\Delta}_1 & \hat{\mathbf{g}}_l^H\boldsymbol{\Delta}_1\hat{\mathbf{g}}_l-t_{1l}-\lambda_l\epsilon_l\end{bmatrix} \tag{29}$$

$$\begin{bmatrix}-\boldsymbol{\Delta}_2+\mu_l\mathbf{I}_{N_T} & -\boldsymbol{\Delta}_2\hat{\mathbf{g}}_l\\ -\hat{\mathbf{g}}_l^H\boldsymbol{\Delta}_2 & -\hat{\mathbf{g}}_l^H\boldsymbol{\Delta}_2\hat{\mathbf{g}}_l+t_{2l}-\mu_l\epsilon_l\end{bmatrix} \tag{30}$$

where $\boldsymbol{\Delta}_1=\sum_{j\neq k}^{K}\mathbf{f}_j\mathbf{f}_j^H+\mathbf{V}$ and $\boldsymbol{\Delta}_2=\sum_{j=1}^{K}\mathbf{f}_j\mathbf{f}_j^H+\mathbf{V}$, while $\lambda_l\geq 0$ and $\mu_l\geq 0$ are the slack variables. The remaining constraint can be solved by using the CCCP and SOCP method as explained in section III. With the transformation problem (22) is equivalently represented as

$$\max_{\mathbf{f}_k,\mathbf{V},z,p_k,q_k,y,u,t_{1l},t_{2l},\lambda_l,\mu_l} \quad z \tag{31a}$$

$$\text{s.t} \quad \|[2z,x-y]\|\leq x+y \tag{31b}$$

$$t_{1l}+\sigma_l^2\geq k_{\theta_1}(y,u) \tag{31c}$$

$$t_{2l}+\sigma_l^2\leq u \tag{31d}$$

$$(29)\text{ and }(30),\ \lambda_l\geq 0,\ \mu_l\geq 0 \tag{31e}$$

$$\|[\mathbf{t}_k^T,\frac{\tilde{b}_k-b_k-1}{2}]\|\leq\frac{\tilde{b}_k-b_k+1}{2} \tag{31f}$$

$$\|[\mathbf{u}_k^T,\frac{\tilde{c}_k-c_k-1}{2}]\|\leq\frac{\tilde{c}_k-c_k+1}{2} \tag{31g}$$

$$\|[\sqrt{\frac{e_k}{4\eta_k}},\frac{\tilde{d}_k-d_k-1}{2}]\|\leq\frac{\tilde{d}_k-d_k+1}{2} \tag{31h}$$

$$\|[\mathbf{f}_1^T,\ldots,\mathbf{f}_K^T]\|+Tr(\mathbf{V})\leq P_t \tag{31i}$$

$$x>0,\quad y>0y\geq 0,\ \mathbf{V}\succeq 0, \tag{31j}$$

$$p_k\geq 1,\ q_k\geq 1,\ invp(p_k)+invp(q_k)\leq k \tag{31k}$$

The constraint set of problem (31a) is convex and can be efficiently solved by using existing softwares, e.g., CVX [37]. Finally the robust algorithm is summarized in Algorithm 2. Let the optimal solution of problem (31a) is denoted by $\big(\mathbf{f}_k^*,\ \mathbf{V}^*,\ \rho_k^*\ \forall k\big)$.

We can show that the proposed CCCP based robust iterative algorithm for the beamforming design convergences to the local optimal solution of the problem (21). The proof is similar to the that of Lemma 3 and Theorem 1 in [35] and can also be found in [40], we therefore omit the details. We summarized the proposed robust case secrecy rate optimization algorithm in Algorithm 2.

Note: At each iteration, the values of the variables are updated. In particular the optimal value of the variables at n^{th} iteration is always a feasible solution to $(n+1)^{th}$ iteration. Since the optimal values at the $(n+1)^{th}$ iteration become greater or equal to the values at n^{th} iteration, therefore there will be a monotonically increase or decrease in the secrecy rate at each iteration. Due to the transmit power constraint, there is an upper bound on the secrecy rate, the convergence of the proposed algorithm is guaranteed, as verified by the simulation results.

Algorithm 2 Robust secure Iterative Algorithm

Inputs: Slack variable x, y and z, total transmit power P_t, noise covariance matrix $\mathbf{V}$, beamforming vector for each user $\mathbf{f}_k$, equations (48), (49), (50) and (51), energy harvesting ratios p_k and q_k, total number of iterations N_{max}, error bound for eavesdropper channel ϵ_l.
Define the tolerance accuracy δ
Initialize the algorithm with a feasible point [25], [27], $u^{(i)}$, $v^{(i)}$, $x^{(i)}$, $y^{(i)}$, $\mathbf{f}_k^{(i)}$ and $\mathbf{V}^{(i)}$.
Set the iteration number $i = 1$

repeat
Solve problem (P8) with initial values and assign the solution to $u^{(i+1)}$, $v^{(i+1)}$, $\mathbf{f}^{(i+1)}$, $\mathbf{V}^{(i+1)}$, $x^{(i+1)}$ and $y^{(i+1)}$
Update the iteration number: $i = i + 1$
until
The convergence or max no if iteration is reached i.e $i > N_{max}$.
Obtain the optimal solution $\mathbf{f}_k^*, \mathbf{V}^*, \rho_k^*, u^*$, v^*, x^* and y^*
Outputs: Noise covariance matirx $\mathbf{V}$, beamforming vector for each user $\mathbf{f}_k$, secrecy rate, maximized value of harvested energy ratios.

Proposed Algorithm	Complexity Order (suppressing the $\ln(1/\epsilon)$)
Non-robust SR	$AI_1(((KN+N^2+1)^2+2k(2K+3)^2+KL(KL+2)^2+(K+1)3^2+n_1^2))$, $n_1=\mathcal{O}(KN+N^2+2K+2)$
Robust SR	$AI_2((2KL(N+1)^3+2K(2K+3)^2+(K+1)3^2+(KN+N^2+1)^2+n_2^2))$, $n_2=\mathcal{O}(KN+N^2+2K+4L+2)$

VI. Complexity Analysis

In section III and IV, we have proposed the perfect and imperfect CSI case secrecy rate maximization problem. In this section we analyze the computational complexity analysis of the proposed algorithm. Moreover, we apply the same basic element of complexity analysis as in [41]. For ease of comparison, we assume that all transmitters are equipped with the same number of antennas i.e., $N_T = N$, $\forall k$. The complexity of the non-robust secrecy rate maximization is dominated by problem (18) AI_1 times, where I_1 is the iteration number. Since the complexity of solving $\hat{v}_l(\mathbf{r}^{(i)}, \mathbf{V}^{(i)}, \mathbf{r}, \mathbf{V})$, $\hat{x}_k(\mathbf{r}^{(i)}, \mathbf{V}^{(i)}, \mathbf{r}, \mathbf{V})$, $\hat{y}_k(\mathbf{r}^{(i)}, \mathbf{r})$ and $\hat{z}_k(\mathbf{r}^{(i)}, \mathbf{V}^{(i)}, \mathbf{r}, \mathbf{V})$ is negligible compared to solving problem (18). Problem (18) involves $KL+3K+2$ SOCs constraints, including $K+1$ SOCs of dimension 3, KL SOCs of dimensions $KL+2$, $2K$ SOCs of dimension $2K+3$ and 1 SOC of dimension $KN+N^2+1$. The number of decision variable is of the order of $\mathcal{O}(KN+N^2+2K+2)$.

The complexity of robust secrecy rate maximization is dominated by problem (31) AI_2 times, where I_2 is the iteration number. Algorithm II in problem (31) involves $KN+N^2+4K+2$ variables. Problem P8 involves $2KL$ linear matrix inequality constraints of size $N+1$ and $2K+3$ SOCs constraints, including $K+1$ SOCs contraints of dimension 3, $2K$ SOCs constraints of dimension $2K+3$ and 1 SOC of size $KN+N^2+1$.

VII. Simulation Results

In this section, in order to evaluate the performance of the proposed MISO secure energy harvesting system, numerical results have been obtained by performing computer simulations. In simulations, we assume that the channel vectors are randomly generated from independent and identical Rayleigh fading distribution with unity variance. The nominal system configuration is defined by the following choice of parameters: $N_T = 6$, $K = 3$, $L = 2$, $\eta = 1$, $\sigma^2 = \sigma_k^2 = \sigma_l^2$=-30 dBm, ω_s^2 =-20 dBm unless specified otherwise. In addition, the SINR of each receiver k is $\gamma_k = 10\ dB$ and the energy harvesting threshold e_k =-10 dBm. In the implementation of the algorithm, the tolerance parameter is chosen as $\delta = 2 \times 10^{-3}$ and the maximum number of iteration in $N_{max} = 20$. All the modeling and solution of the algorithms are performed using CVX [37] on a desktop Intel (i3-2100) CPU running at 3.1 GHz and 4GB RAM. The performance of our proposed algorithm has been compared with that of the SDR based optimal solution of the problem, for both perfect CSI and the robust case. We have also compared the performance with No-AN scheme, for No-AN algorithm, the same designed method has been used to that of our proposed algorithm except we set $\mathbf{V} = 0$.

Figure 2 presents the convergence of the proposed algorithm 1 and 2. The convergence behavior of the proposed CCCP and the robust algorithm is demonstrated for different values of the transmit power. It is obvious that as we increase the transmit power constraint there is an increase in the secrecy rate of the system. It can also been shown that the secrecy rate of the proposed algorithm, as discussed before increase monotonically in each iteration and it after few iterations converges to a certain value.

Figure 3 represents the performance comparison of the secrecy rate versus the total transmit power constraint with $N_t = 6$, $L = 2$ and $e_k = -10dBm$. As it can been seen from Figure 3, that our proposed CCCP and the robust algorithm outperforms SDR and No-AN schemes. The simulation results shows that proposed schemes achieves higher secrecy rates for all values

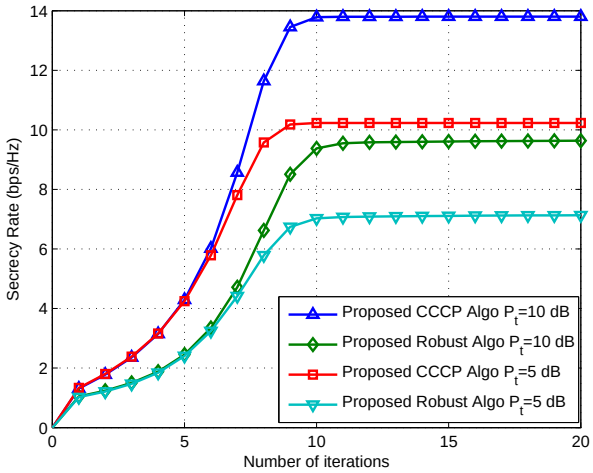

Fig. 2. Convergence property of the proposed algorithms according to different transmit power

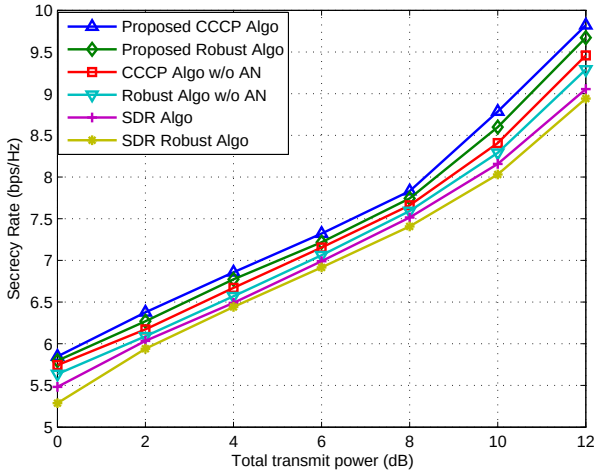

Fig. 3. Total transmit power versus secrecy rate with $N_T = 6$, $K = 3$, $L = 2$,$e_k = -10dBm$ and $\gamma_k = 10dB$

of total transmit power. Moreover we also note higher secrecy rates can be obtained by applying our proposed algorithms as compared to the SDR algorithm.

Figure 4 illustrates the normalized secrecy rate versus the transmitted total power constraint. It can be seen that as the total transmit power increases the performance gap between our proposed algorithm i.e CCCP for perfect CSI and robust algorithms increases as compared to the SDR based secrecy rate optimization method. Besides, it can be observed, that the CCCP and joint robust algorithm with even without additional noise performs better to the SDR approach for both robust and non-robust cases.

Figure 5 plots the secrecy rate versus the harvested energy threshold constraint of each receiver with $N_t = 6$, $L = 2$ and γ_k =-10 dBm. It is clear from figure 5 that the secrecy rate for different algorithms decrease monotonically with increasing harvested energy e_k. This is attributed to the fact that there exist a trade-off between the energy harvested constraint at each receiver versus the secrecy rate. As we increase the harvested energy more power is consumed for EH of the user which results in lower secrecy rates. Moreover, a significant reduction is witnessed in the secrecy rate of the system with increasing energy harvested constraint which is attributed to the limited energy rate region. The CCCP and proposed robust algorithm achieves better performance gain in terms of secrecy rate as compared to the No-AN and SDR based schemes for all tested range of e_k. Figure 6 depicts the total secrecy rate versus the number of transmit antennas with $L = 2$, $\gamma_k = 10\ dBm$ and $e_k = -10\ dBm$. It is observed that the total secrecy rate of the system for all the schemes improves with increasing number of transmit antennas. The reason behind this fact is that as we increase the number of transmit antennas the extra degree of freedom is exploited for designing beamforming. Thus secrecy rate is directly proportional to the number of transmit antennas. Moreover, the secrecy rate for the No-AN design approaches to that our proposed algorithm when the number of antennas is

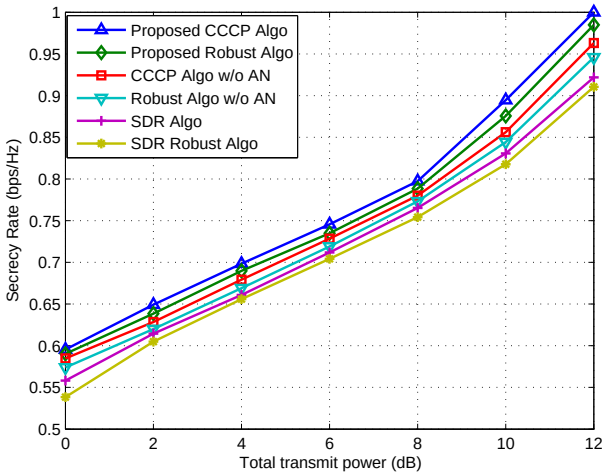

Fig. 4. Normalized transmit power versus secrecy rate with $N_T = 6$, $K = 3$, $L = 2$,$e_k = -10dBm$ and $\gamma_k = 10dB$

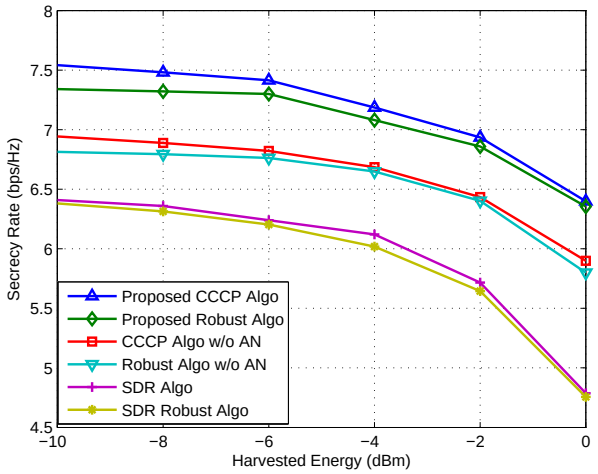

Fig. 5. Harvested energy e_k versus secrecy rate with $N_T = 6$, $K = 3$, $L = 2$,$P_t = 10dB$ and $\gamma_k = 10dB$

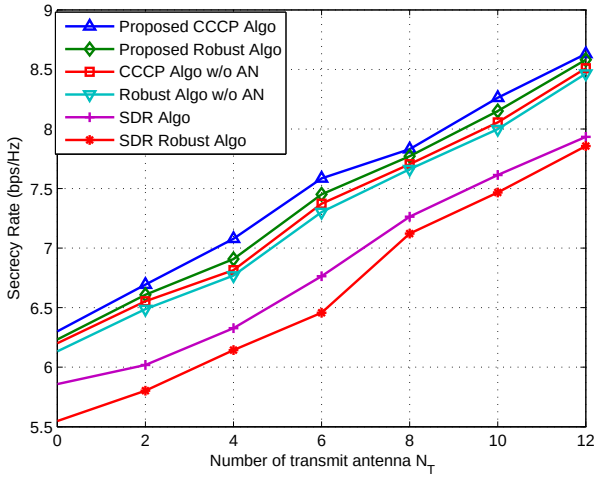

Fig. 6. Number of transmit antennas versus secrecy rate with $P_t = 10dB$, $K = 3$, $L = 2$,$e_k = -10dBm$ and $\gamma_k = 10dB$

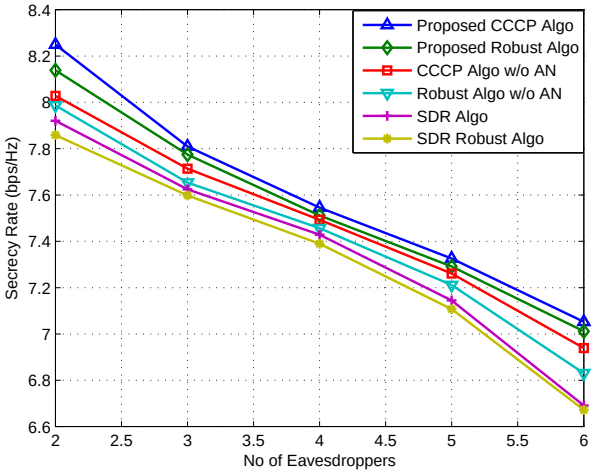

Fig. 7. No of eavesdroppers versus secrecy rate with $N_T = 6$, $K = 3$, $P_t = 10dB$,$e_k = -10dBm$ and $\gamma_k = 10dB$

large. The reason behind this interesting phenomena is that as degree of freedom increases the effect of additional noise is the system reduces.

Figure 7 examines the effect of increasing eavesdroppers L on the secrecy rate of the system. It is assumed that $N_T = 9$, $K = 3$, $\gamma_k = 10dBm$ and $e_k = -10dBm$. It is observed from figure 7 that the total secrecy rate of the system for all the schemes decreases with the increase of eavesdropper L in the system. This is because as the number of eavesdropper increases more transmit power should be allocated to energy harvesting receivers and to generate AN in order to guarantee the EH and SINR constraint of the users. Allocating more power for generating the AN for jamming the channels of eavesdropper is difficult to achieve with the increasing number of eavesdroppers due to the transmit power constraint of the system, which result in reduce secrecy rate. Moreover it is clear from the figure 7 that our proposed design outperform the benchmark and No-AN schemes for different number of EDs in the system.

VIII. Conclusion

This paper presents a novel algorithm to maximize the secrecy rate of the 5G wireless IoT system under both perfect and imperfect channel state information in the presence of malicious users. In order to maintain the QoS, the secrecy rate of the proposed algorithm is maximized, considering the SINR, energy harvesting, and the total transmits power constraints for each user. Additional noise is also added to prevent the system from malicious users. To address the nonconvexity issue of the secrecy rate maximization problem, we make use of the CCCP and SOCP algorithm fir the perfect CSI case. The proposed algorithm achieves a locally optimal solution to the problem. For a robust case, an iterative solution based on the SCA technique is proposed, which results in maximized secrecy. Simulation results are presented to validate the proposed algorithm.

IX. Future Work

In this section, we will be discussing future research directions. The channel error in this paper is only considered for eavesdroppers. In future work channels, errors will be considered for legitimate users as well. Feature of some emerging technologies in 5G wireless systems like directionality in mmWave communication and superimposed signal in non-orthogonal multiple access techniques (NOMA), can be integrated to enhance the PLS of the 5G IoT network and need to be investigated. One of the main features of IoT is the easiness in the mobility of the user. Physical layer security issues need to be addressed in mobile users.

Appendix A
The Proof of Proposition 1

To proceed, we show that the problem (17) can equivalently written as a DC program, by using the concept of CCCP. Therefore problem (17) is an equivalent DC program. According to the concept of CCCP, we approximate the functions $v_l(\mathbf{r}, \mathbf{V})$, $x_k(\mathbf{r}, \mathbf{V})$, $y_k(\mathbf{r})$ and $z_k(\mathbf{r}, \mathbf{V})$ in the ith iteration by their first order Taylor expansion around the current point $\mathbf{r}^{(i)}$, denoted as $\hat{v}_l(\mathbf{r}^{(i)}, \mathbf{V}^{(i)}, \mathbf{r}, \mathbf{V})$, $\hat{x}_l(\mathbf{r}^{(i)}, \mathbf{V}^{(i)}, \mathbf{r}, \mathbf{V})$, $\hat{y}_k(\mathbf{r}^{(i)}, \mathbf{r})$ and $\hat{z}_k(\mathbf{r}^{(i)}, \mathbf{V}^{(i)}, \mathbf{r}, \mathbf{V})$, respectively The approximated functions in (13),(14),(15) and (16) can be approximated by their taylor series expansion given as

$$\begin{aligned}\hat{v}_l(\mathbf{r}^{(i)}, \mathbf{V}^{(i)}, \mathbf{r}, \mathbf{V}) &= v_l(\mathbf{r}^{(i)}, \mathbf{V}^{(i)}) \\ &+ 2R\{\nabla v_l(\mathbf{r}^{(i)})^H(\mathbf{r} - \mathbf{r}^{(i)})\} + 2R\{\nabla v_l(\mathbf{V}^{(i)})^H(\mathbf{V} - \mathbf{V}^{(i)})\}\end{aligned} \tag{32}$$

$$\nabla v_l(\mathbf{r}^{(i)},\mathbf{V}^{(i)}) = \Big[\Big(0_{1\times(2K)}, \frac{(\mathbf{g}_l\mathbf{g}_l^H\mathbf{f}_{\mathbf{1}}^{(\mathbf{i})})^T}{y^{(i)}}, \ldots, \frac{(\mathbf{g}_l\mathbf{g}_l^H\mathbf{f}_{\mathbf{k-1}}^{(\mathbf{i})})^T}{y^{(i)}}, \frac{(\mathbf{g}_l\mathbf{g}_l^H\mathbf{f}_{\mathbf{k+1}}^{(\mathbf{i})})^T}{y^{(i)}}, \ldots, \frac{(\mathbf{g}_l\mathbf{g}_l^H\mathbf{f}_{\mathbf{K}}^{(\mathbf{i})})^T}{y^{(i)}}, 0_{1\times 1}, - \frac{\sum\limits_{j\neq k}^{K}\mathbf{f_j}^{(i)H}\mathbf{g}_l\mathbf{g}_l^H\mathbf{f_j^{(i)}} + \sigma_l^2}{2y^{(i)2}}\Big)^T, \mathbf{g}_l\mathbf{g}_l^H\Big] \tag{36}$$

$$\nabla x_k(\mathbf{r}^{(i)},\mathbf{V}^{(i)}) = \Big[\Big(0_{1\times(k-1)}, \frac{\omega_s^2}{2x^{(i)}}, 0_{1\times(2K-k)}, \frac{(\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_{\mathbf{1}}^{(\mathbf{i})})^T}{x^{(i)}}, \ldots, \frac{(\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_K^{(i)})^T}{x^{(i)}}, - \frac{\sum\limits_{j=1}^{K}\mathbf{f_j}^{(i)H}\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_j^{(i)}} + \sigma_k^2 + \omega_s^2 p_k^{(i)}}{2x^{(i)2}}, 0_{1\times 1}\Big)^T, \mathbf{h}_k\mathbf{h}_k^H\Big] \tag{37}$$

$$\nabla y_k(\mathbf{r}^{(i)}) = [0_{1\times(k-1)}, \frac{\omega_s^2(p_k^{(i)}-1)}{4}, 0_{1\times(2K-k)}, \frac{1}{\gamma_k}(\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_k^{(i)})^T, 0_{1\times 2}]^T \tag{38}$$

$$\nabla z_k(\mathbf{r}^{(i)},\mathbf{V}^{(i)}) = \Big[\Big(0_{1\times(k-1)}, \frac{e_k(q_k^{(i)}-1)}{4}, 0_{1\times(2K-k)}, (\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_1^{(i)})^T, \ldots, (\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_1^{(i)})^T, 0_{1\times 2}\Big)^T, \mathbf{h}_k\mathbf{h}_k^H\Big] \tag{39}$$

$$\hat{x}_k(\mathbf{r}^{(i)},\mathbf{V}^{(i)},\mathbf{r},\mathbf{V}) = x_k(\mathbf{r}^{(i)},\mathbf{V}^{(i)}) + 2R\{\nabla x_k(\mathbf{r}^{(i)})^H(\mathbf{r}-\mathbf{r}^{(i)})\} + 2R\{\nabla x_k(\mathbf{V}^{(i)})^H(\mathbf{V}-\mathbf{V}^{(i)})\} \tag{33}$$

$$\hat{y}_k(\mathbf{r}^{(i)},\mathbf{r}) = y_k(\mathbf{r}^{(i)}) + 2R\{\nabla y_k(\mathbf{r}^{(i)})^H(\mathbf{r}-\mathbf{r}^{(i)})\} \tag{34}$$

$$\hat{z}_k(\mathbf{r}^{(i)},\mathbf{V}^{(i)},\mathbf{r},\mathbf{V}) = z_k(\mathbf{r}^{(i)},\mathbf{V}^{(i)}) + 2R\{\nabla z_k(\mathbf{r}^{(i)})^H(\mathbf{r}-\mathbf{r}^{(i)})\} + 2R\{\nabla z_k(\mathbf{V}^{(i)})^H(\mathbf{V}-\mathbf{V}^{(i)})\} \tag{35}$$

where ∇ denotes the conjugate derivative of the respective function with respect to the complex vector $\mathbf{r}$ and $\mathbf{V}$. We note that $v_l(\mathbf{r},\mathbf{V})$, $x_k(\mathbf{r},\mathbf{V})$, $y_k(\mathbf{r})$ and $z_k(\mathbf{r},\mathbf{V})$, are all affine function of $\mathbf{r}$ and $\mathbf{V}$.

APPENDIX B
THE PROOF OF PROPOSITION B

We first introduce the eight set of auxiliary variables $\tilde{a}_l$, a_l, $\tilde{b}_k$, b_k, $\tilde{c}_k$,c_k, $\tilde{d}_k$ and d_k, $l\in\mathcal{L}$, $k\in\mathcal{K}$, which satisfy

$$\tilde{a}_l = 2\mathcal{R}\left(\frac{\sum\limits_{j\neq k}^{K}\mathbf{f_j}^{(i)H}\mathbf{g}_l\mathbf{g}_l^H\mathbf{f_j}}{y^{(i)}}\right) - \left(\frac{\sum\limits_{j\neq k}^{K}\mathbf{f_j}^{(i)H}\mathbf{g}_l\mathbf{g}_l^H\mathbf{f}_j^{(i)} + \sigma_l^2}{y^{(i)2}}\right)y + \frac{\mathbf{g}_l^H\mathbf{V}\mathbf{g}_l}{y^{(i)}} \tag{40}$$

$$a_l = \sigma_l^2 - 2\frac{\sigma_l^2}{y^{(i)}} - \frac{\mathbf{g}_l^H\mathbf{V}^{(i)}\mathbf{g}_l}{y^{(i)}} \tag{41}$$

$$\tilde{b}_k = 2\mathcal{R}\left(\frac{\sum\limits_{j=1}^{K}\mathbf{f_j}^{(i)H}\mathbf{h}_k\mathbf{h}_k^H\mathbf{f_j}}{x^{(i)}}\right) + \frac{\mathbf{h}_k^H\mathbf{V}\mathbf{h}_k}{x^{(i)}} - \left(\frac{\sum\limits_{j=1}^{K}\mathbf{f_j}^{(i)H}\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_j^{(i)} + \sigma_k^2 + \omega_s^2 p_k^{(i)}}{x^{(i)2}}\right)x + \frac{\omega_s^2 p_k}{x^{(i)}} - \omega_s^2 p_k \tag{42}$$

$$b_k = \sigma_k^2 - \frac{\omega_s^2 p_k^{(i)}}{x^{(i)}} - \frac{2\sigma_k^2}{x^{(i)}} \tag{43}$$

$$\tilde{c}_k = \frac{2}{\gamma_k}\mathcal{R}\{\mathbf{f_k}^{(i)H}\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_k\} + \frac{\omega_s^2 p_k(p_k^{(i)}-1)}{2} \tag{44}$$

$$c_k = \frac{1}{\gamma_k}\mathbf{f_k}^{(i)H}\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_k^{(i)} + \sigma_k^2 - \frac{\omega_s^2(p_k^{(i)}-1)^2}{4} + \frac{\omega_s^2(p_k^{(i)}-1)p_k^{(i)}}{2} \tag{45}$$

$$\tilde{d}_k = 2\mathcal{R}\{\sum_{j=1}^{K}\mathbf{f_j}^{(i)H}\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_j\} + \frac{e_k}{2\eta_k}(q_k^{(i)}-1)q_k + \mathbf{h}_k^H\mathbf{V}\mathbf{h}_k \tag{46}$$

$$d_k = \sum_{j=1}^{K}\mathbf{f_j}^{(i)H}\mathbf{h}_k\mathbf{h}_k^H\mathbf{f}_j^{(i)} + \frac{e_k}{2\eta_k}(q_k^{(i)}-1)q_k^{(i)} - \frac{e_k(q_k^{(i)}-1)^2}{4\eta_k} + \sigma_k^2 \tag{47}$$

where a_l, b_k, c_k and d_k are constant scalars and $\tilde{a}_l$, $\tilde{b}_k$, $\tilde{c}_k$ and $\tilde{d}_k$ are affine functions in $\mathbf{r}$. The constraint in problem (18) can be rewritten in SOCP form as

$$\|[\mathbf{s}_l^T, \frac{\tilde{a}_l - a_l - 1}{2}]\| \leq \frac{\tilde{a}_l - a_l + 1}{2} \tag{48}$$

$$\|[\mathbf{t}_k^T, \frac{\tilde{b}_k - b_k - 1}{2}]\| \leq \frac{\tilde{b}_k - b_k + 1}{2} \tag{49}$$

$$\|[\mathbf{u}_k^T, \frac{\tilde{c}_k - c_k - 1}{2}]\| \leq \frac{\tilde{c}_k - c_k + 1}{2} \tag{50}$$

$$\|[\sqrt{\frac{e_k}{4\eta_k}}, \frac{\tilde{d}_k - d_k - 1}{2}]\| \leq \frac{\tilde{d}_k - d_k + 1}{2} \tag{51}$$

where

$$\mathbf{s}_l^T = [\mathbf{g}_l^H\mathbf{f}_1, \ldots, \mathbf{g}_l^H\mathbf{f}_K]^T,$$
$$\mathbf{t}_k^T = [\mathbf{h}_k^H\mathbf{f}_1, \ldots, \mathbf{h}_k^H\mathbf{f}_{k-1}, \mathbf{h}_k^H\mathbf{h}_{k+1}, \ldots, \mathbf{h}_k^H\mathbf{f}_K]^T and$$
$$\mathbf{u}_k^T = [\mathbf{h}_k^H\mathbf{f}_1, \ldots, \mathbf{h}_k^H\mathbf{f}_{k-1}, \mathbf{h}_k^H\mathbf{h}_{k+1}, \ldots, \mathbf{h}_k^H\mathbf{f}_K, \frac{\omega_s(p_k+1)}{2}]^T$$

Therefore, (17) can be shown equivalent to the following SOCP problem

$$\begin{aligned} & \max_{\mathbf{r}} \quad z \\ \text{s.t} \quad & \|[2z, x-y]\| \leq x+y, \\ & (48), (49), (50), (51), \\ & \|[\mathbf{f}_1^T, \ldots, \mathbf{f}_K^T]\| + Tr(\mathbf{V}) \leq P_t, \quad x>0, \quad y>0 \\ & p_k \geq 1, q_k \geq 1, invp(p_k) + invp(q_k) \leq 1 \end{aligned}$$

REFERENCES

[1] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Networking Letters*, vol. 1, no. 2, pp. 68–71, 2019.

[2] S. Zafar, S. Jangsher, O. Bouachir, M. Aloqaily, and J. B. Othman, "Qos enhancement with deep learning-based interference prediction in mobile iot," *Computer Communications*, vol. 148, pp. 86–97, 2019.

[3] H. B. Salameh, S. Otoum, M. Aloqaily, R. Derbas, I. Al Ridhawi, and Y. Jararweh, "Intelligent jamming-aware routing in multi-hop iot-based opportunistic cognitive radio networks," *Ad Hoc Networks*, vol. 98, p. 102035, 2020.

[4] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5g wireless networks for iot: Challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[5] P. Chen, T. Li, and X. Fang, "Secure beamforming and artificial noise design in full-duplex wireless-powered relay networks," in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, pp. 789–794, IEEE, 2019.

[6] X. Da, L. Ni, H. Niu, H. Hu, S. Yue, and M. Zhang, "An-aided transmission design for secure mimo cognitive radio network with swipt," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 102, no. 8, pp. 946–952, 2019.

[7] A. A. Okandeji, M. R. A. Khandaker, and K. K. Wong, "Two-way beamforming optimization for full-duplex swipt systems," in *2016 24th European Signal Processing Conference (EUSIPCO)*, pp. 2375–2379, Aug 2016.

[8] J. Rubio, A. Pascual-Iserte, D. P. Palomar, and A. Goldsmith, "Swipt techniques for multiuser mimo broadcast systems," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–6, Sept 2016.

[9] Z. Deng, Q. Li, Q. Zhang, L. Yang, and J. Qin, "Beamforming design for physical layer security in a two-way cognitive radio iot network with swipt," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10786–10798, 2019.

[10] D. Xu and H. Zhu, "Secure transmission for swipt iot systems with full-duplex iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10915–10933, 2019.

[11] L. R. Varshney, "Transporting information and energy simultaneously," in *2008 IEEE International Symposium on Information Theory*, pp. 1612–1616, July 2008.

[12] J. Xu, L. Liu, and R. Zhang, "Multiuser miso beamforming for simultaneous wireless information and power transfer," *IEEE Transactions on Signal Processing*, vol. 62, pp. 4798–4810, Sept 2014.

[13] A. E. Shafie, K. Tourki, and N. Al-Dhahir, "An artificial-noise-aided hybrid ts/ps scheme for ofdm-based swipt systems," *IEEE Communications Letters*, vol. PP, no. 99, pp. 1–1, 2016.

[14] M. R. A. Khandaker and K. K. Wong, "Swipt in miso multicasting systems," *IEEE Wireless Communications Letters*, vol. 3, pp. 277–280, June 2014.

[15] Z. Chu, Z. Zhu, W. Xiang, and J. Hussein, "Robust beamforming and power splitting design in miso swipt downlink system," *IET Communications*, vol. 10, no. 6, pp. 691–698, 2016.

[16] M. R. Camana, P. V. Tuan, C. E. Garcia, and I. Koo, "Joint power allocation and power splitting for miso swipt rsma systems with energy-constrained users," *Wireless Networks*, pp. 1–14.

[17] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, pp. 1202–1216, March 2011.

[18] G. Pan, H. Lei, Y. Deng, L. Fan, J. Yang, Y. Chen, and Z. Ding, "On secrecy performance of miso swipt systems with tas and imperfect csi," *IEEE Transactions on Communications*, vol. 64, pp. 3831–3843, Sept 2016.

[19] J. Liao, M. R. A. Khandaker, and K. K. Wong, "Robust power-splitting swipt beamforming for broadcast channels," *IEEE Communications Letters*, vol. 20, pp. 181–184, Jan 2016.

[20] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct 1975.

[21] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, "Secure beamforming for mimo broadcasting with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 2841–2853, May 2015.

[22] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 180–190, Jan 2016.

[23] L. Liu, R. Zhang, and K. C. Chua, "Secrecy wireless information and power transfer with miso beamforming," *IEEE Transactions on Signal Processing*, vol. 62, pp. 1850–1863, April 2014.

[24] B. Zhu, J. Ge, Y. Huang, Y. Yang, and M. Lin, "Rank-two beamformed secure multicasting for wireless information and power transfer," *IEEE Signal Processing Letters*, vol. 21, pp. 199–203, Feb 2014.

[25] W. Wu and B. Wang, "Robust secrecy beamforming for wireless information and power transfer in multiuser miso communication system," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 161, 2015.

[26] M. R. A. Khandaker and K. K. Wong, "Robust secrecy beamforming with energy-harvesting eavesdroppers," *IEEE Wireless Communications Letters*, vol. 4, pp. 10–13, Feb 2015.

[27] Y. Ren, T. Lv, H. Gao, and Y. Li, "Secure wireless information and power transfer in heterogeneous networks," *IEEE Access*, vol. 5, pp. 4967–4979, 2017.

[28] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks," *IEEE Transactions on Vehicular Technology*, vol. 63, pp. 2462–2467, Jun 2014.

[29] Y. Tang, J. Xiong, D. Ma, and X. Zhang, "Robust artificial noise aided transmit design for miso wiretap channels with channel uncertainty," *IEEE Communications Letters*, vol. 17, pp. 2096–2099, November 2013.

[30] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure transmission in miso simultaneous wireless information and power transfer system," *IEEE Transactions on Vehicular Technology*, vol. 64, pp. 400–405, Jan 2015.

[31] Q. Shi, M. Razaviyayn, M. Hong, and Z.-Q. Luo, "Sinr constrained beamforming for a mimo multi-user downlink system: Algorithms and convergence analysis," *IEEE Transactions on Signal Processing*, vol. 64, no. 11, pp. 2920–2933, 2016.

[32] Q. Shi, C. Peng, W. Xu, M. Hong, and Y. Cai, "Energy efficiency optimization for miso swipt systems with zero-forcing beamforming," *IEEE Transactions on Signal Processing*, vol. 64, no. 4, pp. 842–854, 2015.

[33] A. L. Yuille and A. Rangarajan, "The concave-convex procedure," *Neural Computation*, vol. 15, pp. 915–936, April 2003.

[34] B. K. Sriperumbudur and G. R. Lanckriet, "On the convergence of the concave-convex procedure," in *Proceedings of the 22nd International Conference on Neural Information Processing Systems*, pp. 1759–1767, Curran Associates Inc., 2009.

[35] Y. Cheng and M. Pesavento, "Joint optimization of source power allocation and distributed relay beamforming in multiuser peer-to-peer relay networks," *IEEE Transactions on Signal Processing*, vol. 60, pp. 2962–2973, June 2012.

[36] P. Ubaidulla and A. Chockalingam, "Relay precoder optimization in mimo-relay networks with imperfect csi," *IEEE Transactions on Signal Processing*, vol. 59, pp. 5473–5484, Nov 2011.

[37] S.Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K: Cambridge, Univ. Press, 2004.

[38] A. Beck, A. Ben-Tal, and L. Tetruashvili, "A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *Journal of Global Optimization*, vol. 47, pp. 29–51, May 2010.

[39] L. N. Tran, M. F. Hanif, A. Tolli, and M. Juntti, "Fast converging algorithm for weighted sum rate maximization in multicell miso downlink," *IEEE Signal Processing Letters*, vol. 19, pp. 872–875, Dec 2012.

[40] G. R. Lanckriet and B. K. Sriperumbudur, "On the convergence of the concave-convex procedure," in *Advances in Neural Information Processing Systems 22* (Y. Bengio, D. Schuurmans, J. D. Lafferty, C. K. I. Williams, and A. Culotta, eds.), pp. 1759–1767, Curran Associates, Inc., 2009.

[41] K. Y. Wang, A. M. C. So, T. H. Chang, W. K. Ma, and C. Y. Chi, "Outage constrained robust transmit optimization for multiuser miso downlinks: Tractable approximations by conic optimization," *IEEE Transactions on Signal Processing*, vol. 62, pp. 5690–5705, Nov 2014.

[42] R. Zhang and C. Ho, "Mimo broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun*, vol. 12, 2013.

[43] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *11*, vol. 61, 2013.

[44] H. Zhang, Y. Huang, C. Li, and L. Yang, "Secure beamforming design for swipt in miso broadcast channel with confidential messages and external eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 7807–7819, Nov 2016.

[45] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 4599–4615, Aug 2014.

[46] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2180–2189, June 2008.

[47] N. D. Sidiropoulos, T. N. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Transactions on Signal Processing*, vol. 54, pp. 2239–2251, June 2006.

[48] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K: Cambridge, Univ. Press, 1985.

[49] Z. Chu, Z. Zhu, M. Johnston, and S. Y. L. Goff, "Simultaneous wireless information power transfer for miso secrecy channel," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 6913–6925, Sept 2016.

[50] Q. Li and W. K. Ma, "Spatially selective artificial-noise aided transmit optimization for miso multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, pp. 2704–2717, May 2013.

[51] J. Lei, Z. Han, M. Vazquez-Castro, and A. Hjorungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 661–671, Sept 2011.

[52] Z. q. Luo, W. k. Ma, A. M. c. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Processing Magazine*, vol. 27, pp. 20–34, May 2010.

[53] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," *IEEE access*, vol. 3, pp. 1206–1232, 2015.

[54] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[55] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.