Secure Energy Efficiency Optimization for MISO Cognitive Radio Network with Energy Harvesting

Miao Zhang, Kanapathippillai Cumanan and Alister Burr

Department of Electronic Engineering, University of York, York, YO10 5DD, United Kingdom Email: {mz1022, kanapathippillai.cumanan, alister.burr}@york.ac.uk

Abstract—This paper investigates a secure energy efficiency (SEE) optimization problem in a multiple-input single-output (MISO) underlay cognitive radio (CR) network. In particular, a multi-antenna secondary transmitter (SU-Tx) simultaneously sends secured information and energy to a secondary receiver (SU-Rx) and an energy receiver (ER), respectively, in the presence of a primary receiver (PU-Rx). It is assumed that the SU-Rx, ER and PU-Rx are each equipped with a single antenna. In addition, the SU-Tx should satisfy constraints on maximum interference leakage to the PU-Rx and minimum harvested energy at the ER. In this CR network, we consider the transmit covariance matrix design with the assumption of perfect channel state information (CSI) at the SU-Tx. In addition, it is assumed that the ER is a potential passive eavesdropper due to broadcast nature of wireless transmission. On the other hand, we consider the worst-case scenario that ER's energy harvesting requirement is only satisfied when it performs only energy harvesting without intercepting or eavesdropping information intended for the SU-Rx. We formulate this transmit covariance matrix design as a SEE maximization problem which is a non-convex problem due the non-linear fractional objective function. To realize the solution for this non-convex problem, we utilize the non-linear fractional programming and difference of concave (DC) functions approaches to reformulate into a tractable form. Based on these techniques and the Dinkelbach's method, we propose iterative algorithms to determine the solution for the original SEE maximization problem. Numerical simulation results are provided to demonstrate the performance of the proposed transmit covariance matrix design and convergence of the proposed algorithms.

Index Terms—Secure energy efficiency (SEE), energy harvesting, MISO, convex optimization.

I. INTRODUCTION

Without doubt, information security is one of the most critical issues of wireless communications due to the open nature of transmission over the wireless medium. Traditionally, information security techniques are implemented at the application layer based on cryptographic techniques which mainly rely on the computational complexity of difficult mathematical problems [1]. On the other hand, the broadcast nature of wireless communications introduces different challenges in terms of key exchange and distribution [2]-[4]. Information theoretic studies have proven that if the signal to noise ratio (SNR) of the legitimate channel is larger than that of the eavesdropper's channel, secure communication can be guaranteed [5], which is known as physical layer security in the literature. This approach was first theoretically proposed by Shannon [5] and then the secrecy capacity of wiretap and related channels were developed by Wyner [6] and Csiszar [7]. Physical layer security exploits physical layer characteristics of wireless channels including randomness to achieve secure communication between legitimate parties in the presence of eavesdroppers [8], [9]. In contrast to conventional security techniques, physical layer security has lower computational complexity for practical implementation [10], [11].

Achieving higher data rate, energy efficiency and information security are the essential requirements of future wireless communications, including fifth generation (5G) wireless networks. However, with the exponential growth of the number of wireless devices with high data rate and security requirements, energy consumption has become one of the critical issues in terms of both environmental and economic aspects [12]. In addition, wireless communications consume two percent of the entire world energy [13], and this percentage will grow rapidly with the increasing number of wireless devices and the development of new communication technologies. This growth in energy consumption will result in more carbon emission and electromagnetic pollution to the environment. In addition, due to the limited battery life of mobile devices and slow development of energy storage technologies, energy efficient communications have recently become a promising approach to address these issues.

Most work on physical layer security in the literature is either secrecy rate maximization with a total transmit power constraint [14]–[17] or power minimization to meet the secrecy rate requirements [18]–[20]. However, the solutions for the above mentioned optimization problems might not be able to achieve the optimal SEE, as the objective functions of these problems are optimized while satisfying the constraints. Therefore, we consider the SEE based resource allocation problem in this paper to measure efficient utilization of transmit power in a secure communication system. The SEE is defined as the ratio between the achievable secrecy rate and the total transmit power consumption.

Wireless energy harvesting (EH) is a newly emerging technique to harvest energy from the information carrying radio frequency signals radiated from transmitters [21], [22]. Conventional EH methods usually collect energy from the external natural sources, like wind, solar, etc [23], [24]. However, these external energy resources are not constantly stable and are difficult to apply to mobile devices, for example, the size of harvesting devices and the geographical limitations. In comparison to other renewable energy sources such as solar and wind, wireless EH is easier to implement and design for mobile devices [25].

Motivated by the aforementioned aspects, we investigate the

SEE maximization problem for an underlay MISO CR network with EH requirement. In particular, a multi-antenna SU-Tx simultaneously sends secured information and energy to a SU-Tx and ER, respectively, in the presence of a PU-Rx as shown in Fig. 1. We consider transmit covariance matrix design to maximize the achievable SEE with secrecy rate on the SU-Rx, interference leakage [26] and EH requirement. On the other hand, the ER is considered to be a potential passive eavesdropper due to broadcast nature of wireless transmission. With the perfect channel state information (CSI) assumption, we formulate the transmit covariance matrix design problem to maximize SEE under these constraints. The original SEE maximization problem is not convex due to its non-linear fractional objective function and it introduces some challenges in realizing the solution. To circumvent this issue, we reformulate this problem into a tractable form by exploiting non-linear fractional programming [27] and difference of concave (DC) functions programming [28]. Though the reformulated problem is still non-convex, we show that the optimal solution can be obtained by iteratively solving the problem with the help of non-linear fractional programming and DC programming. The remainder of this paper is organized as follows. The system model is presented in Section II, and the SEE maximization problem with the perfect CSI assumption is formulated and iterative algorithms are proposed to solve it in section III. Section IV provides simulation results to validate the performance of the proposed algorithms and finally Section V concludes this paper.

A. Notations

We use upper and lower case boldface letters for matrices and vectors, respectively. $(\cdot)^{-1}$, $(\cdot)^T$ and $(\cdot)^H$ stand for the inverse, transpose and conjugate transpose operations, respectively. $\mathbf{A} \succeq \mathbf{0}$ means that \mathbf{A} is a positive semidefinite matrix. rank(\mathbf{A}) denotes the rank of a matrix, and tr(\mathbf{A}) represents the trace of matrix \mathbf{A} . The circularly symmetric complex Gaussian (CSCG) distribution is represented by $\mathcal{CN}(\mu, \sigma^2)$ with mean μ and variance σ^2 . \mathbb{H}^N denotes the set of all $N \times N$ Hermitian matrices.

II. SYSTEM MODEL

We consider a MISO CR network with four terminals: one SU-Tx, one SU-Rx, one PU-Rx and one ER. The SU-Tx intends to send confidential message to the SU-Rx while the interference leakage to the PU-Rx should not exceed a predefined threshold. The ER harvests energy from the SU-Tx through wireless power transfer. However, a potential issue might arise that the ER might turn out to be a potential eavesdropper and attempts to intercept the message sent to the SU-Rx. Therefore, it is assumed that the ER is a passive eavesdropper in this CR network. We focus on the worst-case scenario that the SU-Tx guarantees the EH requirement only when the ER does not attempt to decode the message [29]. The SU-Tx is equipped with N_t antennas, while the ER, the



Fig. 1: An underlay CR network with a multi-antenna SU-Tx and PU-Rx, SU-Rx and ER are equipped with single antenna.

SU-Rx and the PU-Rx each have only a single antenna. The channel coefficients between the SU-Tx and the PU-Rx, the SU-Rx and the ER are denoted by $\mathbf{h}_p \in \mathcal{C}^{N_T \times 1}$, $\mathbf{h}_s \in \mathcal{C}^{N_T \times 1}$ and $\mathbf{h}_e \in \mathcal{C}^{N_T \times 1}$, respectively. Thus, the received signal at SU-Rx and ER can be written as

$$y_s = \mathbf{h}_s^H \mathbf{x} + n_s, \tag{1}$$

$$y_e = \mathbf{h}_e^H \mathbf{x} + n_e, \tag{2}$$

where $\mathbf{x} \in \mathcal{C}^{N_T \times 1}$ denotes the transmitted signal from the SU-Tx, whose transmit covariance matrix is defined as $\mathbf{Q}_s(\succeq 0) = E(\mathbf{x}\mathbf{x}^H) \in \mathcal{C}^{N_T \times N_T}$. $n_s \sim \mathcal{CN}(0, 1)$ and $n_e \sim \mathcal{CN}(0, 1)$ denote the additive white Gaussian noise (AWGN) at the SU-Rx and the ER, respectively. For guaranteeing communication security, we consider the worst-case scenario that the ER can only harvest energy when it does not attempt to eavesdrop the SU-Rx message. Denote R_s as the achievable secrecy rate of SU-Rx:

$$R_s = \log_2(1 + \mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) - \log_2(1 + \mathbf{h}_e^H \mathbf{Q}_s \mathbf{h}_e).$$
(3)

The total transmit power consumption at SU-Tx is given by:

$$P_t = \frac{\operatorname{tr}(\mathbf{Q}_s) + P_c}{\xi},\tag{4}$$

where P_c is the circuit power consumption of the transmitter and $\xi \in (0, 1]$ is the power amplifier efficiency, which is assumed to be one ($\xi = 1$) without loss of generality in this paper. The SEE is defined as the ratio between the achievable secrecy rate and the total transmit power consumption, which can be written as

$$\eta = \frac{R_s}{P_t} = \frac{\log_2(1 + \mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) - \log_2(1 + \mathbf{h}_e^H \mathbf{Q}_s \mathbf{h}_e)}{\operatorname{tr}(\mathbf{Q}_s) + P_c}.$$
 (5)

The harvested energy at ER can be defined as

$$E_{eh} = \eta_{eh} (\mathbf{h}_e^H \mathbf{Q}_s \mathbf{h}_e + 1), \tag{6}$$

where $\eta_{eh} \in (0, 1]$ is the energy conversion ratio at the ER.

III. PROBLEM FOMULATION

In this section, we solve a SEE maximization problem with the constraints on the minimum harvested energy at ER and the maximum interference leakage at the PU-Rx. This SEE maximization problem can be formulated as

$$\max_{\mathbf{Q}_s} \eta = \frac{\log_2(1 + \mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) - \log_2(1 + \mathbf{h}_e^H \mathbf{Q}_s \mathbf{h}_e)}{\operatorname{tr}(\mathbf{Q}_s) + P_c}, \quad (7a)$$

s.t.
$$R_s = \log_2(1 + \mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) - \log_2(1 + \mathbf{h}_e^H \mathbf{Q}_s \mathbf{h}_e) \ge R_d$$
(7b)

$$E_{eh} = \eta_{eh} (\mathbf{h}_e^H \mathbf{Q}_s \mathbf{h}_e + 1) \ge E_s, \tag{7c}$$

$$\mathbf{h}_{p}^{H}\mathbf{Q}_{s}\mathbf{h}_{p} \leq P_{f}, \operatorname{tr}(\mathbf{Q}_{s}) \leq P_{\mathrm{tx}}, \mathbf{Q}_{s} \succeq 0.$$
(7d)

The physical meaning of the constraint in (7c) is that the transmitter should satisfy the minimum harvest energy requirement at the ER if it is only interested in EH and not in eavesdropping the SU-Rx signal. This problem is not a convex problem due to the fractional objective function, and we convert this problem into a convex one through non-linear fractional and DC programming in the following subsections.

A. Non-linear fractional programming

The objective function in (7a) is a fractional programming problem with non-linear as well as linear terms in the numerator and denominator, therefore the problem in (7) is known as a non-linear fractional problem in literature [27]. The original problem can be converted into a parametric programming problem [27]. Denote

$$\lambda^* = \frac{R_s^*}{P_t^*},\tag{8}$$

where R_s^* and P_t^* are the optimal secrecy rate and power consumption of problem (7), respectively. The maximum SEE

$$\lambda^* = \frac{R_s^*}{P_t^*} = \max_{\mathbf{Q}_s} \frac{R_s}{P_t} \tag{9}$$

can be achieved only when λ^* , R_s^* and P_t^* satisfy the following condition [27]

$$\max_{\mathbf{Q}_{s}} \ [R_{s} - \lambda^{*} P_{t}] = R_{s}^{*} - \lambda^{*} P_{t}^{*} = 0,$$
(10)

for $R_s \ge 0$ and $P_t > 0$. The parametric programming problem with parameter λ is defined as

$$\max_{\mathbf{Q}_s} [R_s - \lambda P_t] = \max_{\mathbf{Q}_s} \{ \log_2(1 + \mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) - \log_2(1 + \mathbf{h}_e^H \mathbf{Q}_s \mathbf{h}_e) - \lambda [\operatorname{tr}(\mathbf{Q}_s) + P_c] \}$$

s.t. (7b)-(7d). (11)

It can be seen that the original problem (7) is transformed into a parameterized polynomial subtractive form. As a result, the original problem is reformulated to find λ^* and \mathbf{Q}_s^* to satisfy the condition in (10). By utilizing Dinkelbach's method [27] with an initial value λ_0 of λ , the optimal solutions of (11) can be obtained iteratively by solving

$$\max_{\mathbf{Q}_s} [R_s - \lambda_i P_t]$$

s.t. (7b)-(7d). (12)

with a given λ_i at the *i*th iteration, where *i* is the iteration index. λ_i can be considered as the SEE obtained at the previous iteration. At each iteration, λ_i should be updated as

$$\lambda_{i+1} = \frac{R_s^i}{P_t^i},\tag{13}$$

where R_s^i and P_t^i denote the solution of (12) for the given λ_i . This iterative process will be terminated when the condition in (10) is satisfied. However, in practice the iterative process will be repeated until the following inequality is satisfied:

$$\Delta F = |R_s^i - \lambda_i P_t^i| \le \varepsilon, \tag{14}$$

with a small convergence tolerance $\varepsilon > 0$. The proposed algorithm of non-linear fractional programming is summized in Algorithm 1.

Algorithm 1 Non-linear fractional programming		
1:	Initial $i = 0$ and choose an initial value λ_0 ;	
2:	repeat	
3:	For the given λ_i , find the optimal R_s^i and P_t^i of (12)	
	(DC programming);	
4:	Update $\lambda_{i+1} = \frac{R_s^i}{P^i}$ to obtain λ_{i+1}	
5:	i = i + 1;	
6:	until (14) satisfied;	
7:	Return $\lambda^* = \lambda_i, P_t^* = P_t^{i-1}, R_s^* = R_s^{i-1}.$	

B. DC programming

DC programming is an optimization approach to solve nonconvex problems. In particular, this technique can be applied for an optimization problem with an objective function, which is a difference of two concave functions. Since, the objective function in (12) falls into this category, DC programming can be utilized to solve this problem.

The fundamental idea of DC programming [28] is to locally linearize the non-concave functions at a feasible point \mathbf{Q}_s^k and then iteratively solve the linearized problem. We define the following function to approximate the second term of the objective function in (12)

$$f(\mathbf{Q}_s, \mathbf{Q}_s^k) = \log_2(1 + \mathbf{h}_e^H \mathbf{Q}_s^k \mathbf{h}_e) + \frac{\mathbf{h}_e^H (\mathbf{Q}_s - \mathbf{Q}_s^k) \mathbf{h}_e}{(1 + \mathbf{h}_e^H \mathbf{Q}_s^k \mathbf{h}_e) \ln 2}.$$
(15)

Based on this approximation, the problem (12) can be converted into the following equivalent problem:

$$\begin{aligned} \max_{\mathbf{Q}_{s}} & \{ \log_{2}(1 + \mathbf{h}_{s}^{H}\mathbf{Q}_{s}\mathbf{h}_{s}) - f(\mathbf{Q}_{s}, \mathbf{Q}_{s}^{k}) - \lambda_{i}[\operatorname{tr}(\mathbf{Q}_{s}) + P_{c}] \} \\ s.t. & 1 + \mathbf{h}_{s}^{H}\mathbf{Q}_{s}\mathbf{h}_{s} \geq 2^{R_{d}}(1 + \mathbf{h}_{e}^{H}\mathbf{Q}_{s}\mathbf{h}_{e}), \\ & \eta_{eh}(\mathbf{h}_{e}^{H}\mathbf{Q}_{s}\mathbf{h}_{e} + 1) \geq E_{s}, \\ & \mathbf{h}_{p}^{H}\mathbf{Q}_{s}\mathbf{h}_{p} \leq P_{f}, \operatorname{tr}(\mathbf{Q}_{s}) \leq P_{\mathrm{tx}}, \mathbf{Q}_{s} \succeq 0. \end{aligned}$$
(16)

This approximated problem is convex in terms of (\mathbf{Q}_s) and hence \mathbf{Q}_s^* can be obtained through iteratively solving problem (16) and iteratively updating \mathbf{Q}_s^k . The algorithm based on DC programming is provided in Algorithm 2.

Algorithm 2 DC Programming

1:	Initial $k = 0$, choose an initial value $\mathbf{Q}_s^k = 0$ and $\eta^{i,k} = 0$;
2:	repeat
3:	Solve the problem (16) with $\lambda = \lambda_i$ from Algorithm
	1 and obtain \mathbf{Q}_s^{k+1} ;
4:	Compute $\eta^{i,k+1} = \log_2(1 + \mathbf{h}_s^H \mathbf{Q}_s^{k+1} \mathbf{h}_s) - \log_2(1 + \mathbf{h}_s^H \mathbf{Q}_s^{k+1} \mathbf{h}_s)$
	$\mathbf{h}_{e}^{H}\mathbf{Q}_{s}^{k+1}\mathbf{h}_{e}) - \lambda_{i}[\mathrm{tr}(\mathbf{Q}_{s}^{k+1}) + P_{c}];$
5:	$\Delta \eta = \eta^{i,k+1} - \eta^{i,k};$

- 6: Update k = k + 1;
- 7: **until** $|\Delta \eta| \leq \zeta$;
- 8: Return $R_s^i = \log_2(1 + \mathbf{h}_s^H \mathbf{Q}_s^k \mathbf{h}_s) \log_2(1 + \mathbf{h}_e^H \mathbf{Q}_s^k \mathbf{h}_e)$ and $P_t^i = \operatorname{tr}(\mathbf{Q}_s^k) + P_c$ to Algorithm 1 for updating λ_{i+1} .

Proposition 1: Provided that the problem (11) is feasible, the optimal solution will be always rank-one.

Proof: Please refer to Appendix.

IV. SIMULATION RESULTS

In this section, we provide numerical simulation results to validate the performance of the proposed schemes. The SU-Tx is equipped with three ($N_t = 3$) antennas, while the PU-Rx, SU-Rx and ER each use a single antenna. All the channel coefficients are generated by CSCG with zero mean and unit variance. The maximum interference leakage to the PU-Rx is assumed to be 0 dB. In addition, the energy conversion ratio is assumed to be 0.5. The convergence tolerances ε and ζ are set to be 10^{-3} .

First, we evaluate the convergence of the proposed algorithms in Fig. 2 for the target secrecy rate $R_d = 0.5$ bps/Hz, the power consumption for transmission $P_{\text{tx}} = 13$ dB and the EH requirement $E_s = 0$ dB, respectively. Fig. 2(a) shows the convergence of achieved SEE with Algorithm 1. Fig. 2(b) and 2(c) illustrate the convergence of parameter ΔF in Algorithm 1 and parameter $\Delta \eta$ in Algorithm 2, respectively. These two parameters control the termination of the iterative processes in both algorithms. As seen in these numerical results, the maximum SEE and the convergence of both algorithms can be achieved with a limited number of iterations.

Fig. 3 illustrates the achieved SEE with different target secrecy rates and EH requirements. As seen in Fig. 3, the optimal SEE decreases as the target rate increases. Note that the zero SEE means that problem is not feasible with a given target secrecy rate constraint. On the other hand, the SEE can achieve a better performance with a smaller EH requirement. In addition, if the problem is feasible with a given target secrecy rate constraint with small transmit power consumption, it would be able to achieve the same SEE with larger transmit power consumption. Increasing the transmit power consumption cannot yield a better SEE, however, it should be able to achieve a higher target secrecy rate.



Fig. 2: Convergence results of our proposed algorithms by these assumptions: $P_{\text{tx}} = 13 \text{ dB}$, $E_s = 0 \text{ dB}$ and $R_d = 0.5 \text{ bps/Hz}$



Fig. 3: Achieved SEE with different target secrecy rates and transmit power constraints and harvest energy requirements

Fig. 4 compares the achievable SEE of three schemes: SEE maximization, power minimization and secrecy rate maximization. In these simulation results, the transmit power constraint is assumed to be 20 dB and the EH requirement is -20dB. As expected, the proposed scheme for SEE maximization achieves the best SEE of all the three schemes. As can be seen in this figure, the achievable SEE performance obtained from secrecy rate maximization is not affected by the target secrecy rate values in its feasible domain. This can be explained as follows. The power and energy limitations become major concerns in secrecy rate maximization problems, and therefore the limited power is used fully to maximize the secrecy rate. Hence, the ratio of secrecy rate and transmit power consumption does not change with a fixed transmit power constraint. Furthermore, the zero SEE means the target secrecy rate cannot be achieved with the available transmit power.



Fig. 4: Achieved SEE for different schemes: SEE maximization, power minimization and secrecy rate maximization

V. CONCLUSION

In this paper, we have considered the SEE maximization problem for an underlay MISO CR network. In particular, the transmit covariance matrix was designed to provide the required secrecy rate at the SU-Rx while satisfying the interference leakage constraint on the PU-Rx and the EH requirement on the ER. The original problem was not convex due to the non-linear fractional objective function. To overcome this non-convexity issue, we converted the original problem into a convex one by exploiting non-linear fractional and DC programming. Simulation results were provided to validate the convergence of the proposed algorithms and the performance of the proposed SEE based resource allocation technique. In addition, the achievable SEE in the developed scheme was compared with two alternative schemes.

APPENDIX

Proof of Proposition 1

First, we consider the Langrange function of problem (11): which completes the proof of proposition 1.

$$\mathcal{L}(\mathbf{Q}_{s}, \mathbf{Z}, \alpha, \beta, \gamma, \mu) = -\{\log_{2}(1 + \mathbf{h}_{s}^{H}\mathbf{Q}_{s}\mathbf{h}_{s}) - \log_{2}(1 + \mathbf{h}_{e}^{H}\mathbf{Q}_{s}\mathbf{h}_{e}) - \lambda[\operatorname{tr}(\mathbf{Q}_{s}) + P_{c}]\} - \operatorname{tr}(\mathbf{Z}\mathbf{Q}_{s}) - \alpha[\log_{2}(1 + \mathbf{h}_{s}^{H}\mathbf{Q}_{s}\mathbf{h}_{s}) - \log_{2}(1 + \mathbf{h}_{e}^{H}\mathbf{Q}_{s}\mathbf{h}_{e}) - R_{d}] - \beta[\eta_{eh}[\mathbf{h}_{e}\mathbf{Q}_{s}\mathbf{h}_{e} + 1] - E_{s}] + \gamma[\mathbf{h}_{p}^{H}\mathbf{Q}_{s}\mathbf{h}_{p} - P_{f}] + \mu[\operatorname{tr}(\mathbf{Q}_{s}) - P_{\mathrm{tx}}]$$
(17)

where $\mathbf{Q}_s \in \mathbb{H}^{N_t}_+$, $\mathbf{Z} \in \mathbb{H}^{N_t}_+$, $\alpha \in \mathbb{R}_+$, $\beta \in \mathbb{R}_+$, $\gamma \in \mathbb{R}_+$, $\mu \in$ \mathbb{R}_+ are the Lagrangian multipliers associated with problem (11). Then we derive the corresponding Karush-Kuhn-Tucker (KKT) conditions [30]:

$$\frac{\partial \mathcal{L}}{\partial \mathbf{Q}_s} = -(\alpha + 1) \left[\frac{\mathbf{h}_s^H \mathbf{h}_s}{(1 + \mathbf{h}_s^H \mathbf{Q}_s \mathbf{h}_s) \ln 2} \right] + (1 - \alpha - \beta \eta_{eh})$$

$$\left[\frac{\mathbf{h}_e^H \mathbf{h}_e}{(1 + \mathbf{h}_e^H \mathbf{Q}_s \mathbf{h}_e) \ln 2} \right] + (\lambda + \mu) \mathbf{I} - \mathbf{Z} - \gamma \frac{\mathbf{h}_p^H \mathbf{h}_p}{(1 + \mathbf{h}_p^H \mathbf{Q}_s \mathbf{h}_p) \ln 2}$$

$$= 0 \tag{18}$$

$$\mathbf{Z}\mathbf{Q}_s = 0, \mathbf{Z} \succeq 0 \tag{19}$$

The following equality holds:

$$- (\alpha + 1) \left[\frac{\mathbf{h}_{s}^{H} \mathbf{h}_{s}}{(1 + \mathbf{h}_{s}^{H} \mathbf{Q}_{s} \mathbf{h}_{s}) \ln 2} \right] + (1 - \alpha - \beta \eta_{eh}) \\ \left[\frac{\mathbf{h}_{e}^{H} \mathbf{h}_{e}}{(1 + \mathbf{h}_{e}^{H} \mathbf{Q}_{s} \mathbf{h}_{e}) \ln 2} \right] + (\lambda + \mu) \mathbf{I} - \gamma \frac{\mathbf{h}_{p}^{H} \mathbf{h}_{p}}{(1 + \mathbf{h}_{p}^{H} \mathbf{Q}_{s} \mathbf{h}_{p}) \ln 2} = \mathbf{Z}$$

$$(20)$$

$$\Rightarrow \{-(\alpha+1)[\frac{\mathbf{h}_{s}^{H}\mathbf{h}_{s}}{(1+\mathbf{h}_{s}^{H}\mathbf{Q}_{s}\mathbf{h}_{s})\ln 2}] + (1-\alpha-\beta\eta_{eh}) \\ [\frac{\mathbf{h}_{e}^{H}\mathbf{h}_{e}}{(1+\mathbf{h}_{e}^{H}\mathbf{Q}_{s}\mathbf{h}_{e})\ln 2}] + (\lambda+\mu)\mathbf{I} - \gamma\frac{\mathbf{h}_{p}^{H}\mathbf{h}_{p}}{(1+\mathbf{h}_{p}^{H}\mathbf{Q}_{s}\mathbf{h}_{p})\ln 2}\}\mathbf{Q}_{s} \\ = 0$$
(21)

$$\Rightarrow \{(1 - \alpha - \beta \eta_{eh}) [\frac{\mathbf{h}_{e}^{H} \mathbf{h}_{e}}{(1 + \mathbf{h}_{e}^{H} \mathbf{Q}_{s} \mathbf{h}_{e}) \ln 2}] + (\lambda + \mu) \mathbf{I} - \frac{\mathbf{h}_{p}^{H} \mathbf{h}_{p}}{(1 + \mathbf{h}_{p}^{H} \mathbf{Q}_{s} \mathbf{h}_{p}) \ln 2} \} \mathbf{Q}_{s} = \{(\alpha + 1) [\frac{\mathbf{h}_{s}^{H} \mathbf{h}_{s}}{(1 + \mathbf{h}_{s}^{H} \mathbf{Q}_{s} \mathbf{h}_{s}) \ln 2}] \} \mathbf{Q}_{s}$$

$$(22)$$

$$\Rightarrow \mathbf{Q}_{s} = \{(\alpha+1)[\frac{\mathbf{h}_{s}^{H}\mathbf{h}_{s}}{(1+\mathbf{h}_{s}^{H}\mathbf{Q}_{s}\mathbf{h}_{s})\ln 2}]\}\{(1-\alpha-\beta\eta_{eh})$$
$$[\frac{\mathbf{h}_{e}^{H}\mathbf{h}_{e}}{(1+\mathbf{h}_{e}^{H}\mathbf{Q}_{s}\mathbf{h}_{e})\ln 2}]+(\lambda+\mu)\mathbf{I}-\gamma\frac{\mathbf{h}_{p}^{H}\mathbf{h}_{p}}{(1+\mathbf{h}_{p}^{H}\mathbf{Q}_{s}\mathbf{h}_{p})\ln 2}\}^{-1}\mathbf{Q}_{s}$$
(23)

Hence, the following rank relation holds:

$$\operatorname{rank}(\mathbf{Q}_{s}) = \operatorname{rank}\left\{\left\{(\alpha+1)\left[\frac{\mathbf{h}_{s}^{H}\mathbf{h}_{s}}{(1+\mathbf{h}_{s}^{H}\mathbf{Q}_{s}\mathbf{h}_{s})\ln 2}\right]\right\}\left\{(1-\alpha-\beta\eta_{eh}\right)\right\}$$
$$\left[\frac{\mathbf{h}_{e}^{H}\mathbf{h}_{e}}{(1+\mathbf{h}_{e}^{H}\mathbf{Q}_{s}\mathbf{h}_{e})\ln 2}\right] + (\lambda+\mu)\mathbf{I} - \gamma\frac{\mathbf{h}_{p}^{H}\mathbf{h}_{p}}{(1+\mathbf{h}_{p}^{H}\mathbf{Q}_{s}\mathbf{h}_{p})\ln 2}\right\}^{-1}\mathbf{Q}_{s}\right\}$$
$$\leq \operatorname{rank}\left[\frac{\mathbf{h}_{s}^{H}\mathbf{h}_{s}}{(1+\mathbf{h}_{s}^{H}\mathbf{Q}_{s}\mathbf{h}_{s})\ln 2}\right] \leq 1.$$
(24)

REFERENCES

- [1] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Trans. Inf. Theory., vol. 54, no. 6, pp. 2470-2492, Jun. 2008
- [2] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," IEEE Trans. Veh. Technol., vol. 64, no. 5, pp. 1833-1847, May 2015.
- [3] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," IEEE Trans. Veh. Technol., vol. 63, no. 4, pp. 1678-1690, May 2014.
- [4] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," IEEE J. Sel. Topics Signal Process., vol. 10, no. 8, pp. 1417-1432, Dec. 2016.
- [5] C. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656-715, Oct. 1949.
- [6] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.
- [7] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory., vol. 24, no. 3, pp. 339-348, May 1978.
- [8] B. Li, Z. Fei, and Z. Chu, "Optimal transmit beamforming for secure SWIPT in a two-tier hetnet," IEEE Commun. Lett., Aug. 2017.

- [9] K. Cumanan, R. Krishna, Z. Xiong, and S. Lambotharan, "Multiuser spatial multiplexing techniques with constraints on interference temperature for cognitive radio networks," *IET Signal Process.*, vol. 4, no. 6, pp. 666–672, Dec 2010.
- [10] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, Dec. 2016.
- [11] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, Jul. 2016.
- [12] J. Hu, G. Zhang, W. Heng, and X. Li, "Optimal energy-efficient transmission in multiuser systems with hybrid energy harvesting transmitter," in *Proc. IEEE GLOBECOM*, Washington, Dec. 2016, pp. 1–5.
- [13] A. Zappone, P.-H. Lin, and E. A. Jorswieck, "Energy-efficient secure communications in miso-se systems," in *Proc. IEEE ICASSP*, Pacific Grove, Nov. 2014, pp. 1001–1005.
- [14] M. Zhang, K. Cumanan, and A. Burr, "Secrecy rate maximization for MISO multicasting SWIPT system with power splitting scheme," in *Proc. IEEE SPAWC*, Edinburgh, Jul. 2016, pp. 1–5.
- [15] Y. Yuan, Z. Chu, Z. Ding, K. Cumanan, and M. Johnston, "Joint relay beamforming and power splitting ratio optimization in a multi-antenna relay network," in *IEEE WCSP*, Hefei, Dec. 2014, pp. 1–5.
- [16] Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multi-antenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283– 297, Jan. 2016.
- [17] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy rate optimization for a MIMO secrecy channel based on stackelberg game," in *IEEE EUSIPCO*, Lisbon, Nov. 2014, pp. 126–130.
- [18] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
- [19] Z. Chu, Z. Zhu, M. Johnston, and S. Y. Le Goff, "Simultaneous wireless information power transfer for MISO secrecy channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 6913–6925, Nov 2016.
- [20] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Robust outage secrecy rate optimizations for a MIMO secrecy channel," *IEEE Wireless Commun Lett.*, vol. 4, no. 1, pp. 86–89, Feb 2015.
- [21] L. R. Varshney, "Transporting information and energy simultaneously," in Proc. IEEE Int. Symp. Inf. Theory, Toronto, Jul. 2008, pp. 1612–1616.
- [22] P. Grover and A. Sahai, "Shannon meets tesla: Wireless information and power transfer." in *Proc. IEEE Int. Symp. Inf. Theory.*, Austin, Jun. 2010, pp. 2363–2367.
- [23] E. Hossain, M. Rasti, H. Tabassum, and A. Abdelnasser, "Evolution toward 5G multi-tier cellular wireless networks: An interference management perspective," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 118– 127, Jun. 2014.
- [24] V. Raghunathan, S. Ganeriwal, and M. Srivastava, "Emerging techniques for long lived wireless sensor networks," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 108–114, May 2006.
- [25] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, Oct. 2013.
- [26] K. Cumanan, R. Krishna, Z. Xiong, and S. Lambotharan, "SINR balancing technique and its comparison to semidefinite programming based qos provision for cognitive radios," in *Proc. IEEE VTC*. IEEE, Barcelona, Apr. 2009, pp. 1–5.
- [27] W. Dinkelbach, "On nonlinear fractional programming," Manag. Sci., vol. 13, no. 7, pp. 492–498, Mar. 1967.
- [28] T. P. Dinh and H. A. Le Thi, "Recent advances in DC programming and DCA," in *Trans. Comput. Intell. XIII.* Springer, 2014, pp. 1–37.
- [29] S. Leng, D. W. K. Ng, and R. Schober, "Power efficient and secure multiuser communication systems with wireless information and power transfer," in *Proc. IEEE ICC*, Sydney, Jun. 2014.
- [30] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University press, 2004.