Secrecy Rate Region of Wiretap Interference Channels with Energy Harvesting Receivers

Ali Kariminezhad, *Student Member, IEEE*, and Aydin Sezgin, *Senior Member, IEEE*

***Abstract*—The secrecy rate region of wiretap interference channels under receiver energy harvesting constraint is studied. The legitimate users are equipped with single transmit/receive antennas, while the passive eavesdropper has multiple antennas. To stay operational in the network, the legitimate receivers demand energy alongside information, which is fulfilled by power transmission and exploiting a power splitting receiver. In order to achieve the secrecy rate region frontier, smart tuning of the transmit power and receiver power splitting coefficient is required. In this paper, we propose an efficient algorithm to optimize these parameters jointly in polynomial time. The secrecy rate region characterization is formulated as a weighted max-min optimization problem. This problem turns to be a non-convex problem due to the non-convex constraint set. This set is lower-bounded by a convex set which in consequence results in an achievable suboptimal solution that is improved iteratively. Finally, we compare the achievable secrecy rate region of legitimate users with a weak and strong eavesdropper under legitimate users' energy harvesting constraints.**

I. Introduction

Secrecy is one of the main concerns for future communication networks. This includes wireless sensor networks (WSN) and Internet of Things (IoT) [1]. Moreover, due to an steadily increased number of connected devices, the scarce spectrum needs to be shared among multiple communication pairs. These two facts motivate the study of the wiretap interference channel [2]. In this channel, multiple communication pairs communicate simultaneously over a common spectrum, which imposes destructive interference at the receivers. Here, we assume that the receivers treat the incident interference as noise (TIN). Thus, the complexity of the receiver is kept low. Note that in certain cases TIN is optimal in terms of achievable rates [3], [4]. Further, a multi-antenna malicious eavesdropper overhears the transmit signals of the legitimate users with the goal of decoding the messages. This renders the communication to be insecure.

Alongside secure information transfer, legitimate receivers need to stay operational in the network as long as possible [5], [6]. For instance, consider a WSN with limited energy supply at the sensors. By deploying energy harvesting receivers, the energy buffer can be charged wirelessly from energy sources, e.g., solar energy. The main focus of this paper is to harvest RF signal energy. The sensors with scarce energy supplies face the trade-off in simultaneous information detection (ID) and energy harvesting (EH). By time sharing between ID chain and EH circuitry, information is extracted in one time instant, while the energy can be harvested in another time instant [7]. Exploiting multiple receive antennas at the sensors makes simultaneous ID and EH feasible in spatial domain by antenna switching. In a single antenna receiver, power splitting (PS) allows simultaneous ID and EH. By PS, one portion of received signal power undergoes the ID chain while the other portion passes through the EH circuitry. Utilizing power splitting receiver, the demanded energy is satisfied by power transmission. Hence, the legitimate transmitters convey energy alongside information. This concept is well-known as simultaneous wireless information and power transmission (SWIPT) [8]–[10].

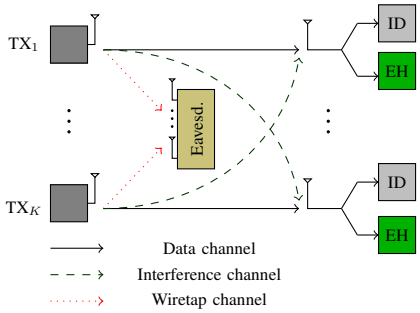


Fig. 1: K-user wiretap interference channel with power splitting structure at the legitimate receivers.

In order to identify secure communication rate tuples in multi-user networks, we need to characterize the achievable secrecy rate region frontier. Achievable secrecy rate region frontier of the wiretap interference channel with legitimate users' EH demands is a function of the transmit power and the receiver power splitting coefficients at the legitimate users. Therefore, for characterizing the secrecy rate region frontier, it is crucial to study the joint interaction between transmit power and splitting coefficients at multiple legitimate pairs. Thus, optimal design which captures the trade-off between those parameters needs to be investigated.

Contribution: In this letter, we investigate the secrecy rate region of the wiretap interference channel with a weak and strong multi-antenna eavesdropper, respectively, under legitimate user energy harvesting constraints. The transmit power and receiver power splitting coefficients are optimized jointly in order to capture the trade-off between secure communication rates and energy demands.

II. System Model

Consider a wiretap interference channel where the legitimate users are equipped with single antennas and the eavesdropper exploits multiple antennas as shown in Fig.1. The channel

A. Kariminezhad and A. Sezgin are with the Institute of Digital Communication Systems, Ruhr-Universität Bochum (RUB), Germany (emails: {ali.kariminezhad, aydin.sezgin}@rub.de).

input-output relationships at the legitimate users and eavesdropper are given as

$$y_k = h_{kk}x_k + \sum_{\substack{j=1 \\ j\neq k}}^{K} h_{kj}x_j + n_k, \quad \forall k \in \mathcal{K}, \tag{1}$$

$$\mathbf{y}_{\mathrm{E}} = \sum_{j=1}^{K} \mathbf{h}_{\mathrm{E}j}x_j + \mathbf{n}_{\mathrm{E}}, \tag{2}$$

where the set of legitimate users is denoted by $\mathcal{K} = \{1, ..., K\}$. The received signal at kth legitimate receiver and the eavesdropper with M antennas are represented by $y_k \in \mathbb{C}$ and $\mathbf{y}_{\mathrm{E}} \in \mathbb{C}^M$, respectively. The transmit signal from kth transmitter is assumed to be from a Gaussian codebook and is denoted by $x_k \in \mathbb{C}$. Moreover, zero-mean additive white Gaussian noise (AWGN) at the kth legitimate receives and at the eavesdropper are represented by $n_k \sim \mathcal{CN}\left(0, \sigma_k^2\right)$ and $\mathbf{n}_{\mathrm{E}} \sim \mathcal{CN}\left(\mathbf{0}, \sigma_{\mathrm{E}}^2\mathbf{I}_M\right)$, respectively. Channel realization from jth transmitter to kth receiver is represented by $h_{kj} \in \mathbb{C}$, and the channel from jth user to the eavesdropper is expressed by $\mathbf{h}_{\mathrm{E}j} \in \mathbb{C}^M$. These channels are assumed to be globally known. Legitimate receivers harvest the energy of the incident radio frequency (RF) signal by power splitting. Hence, a portion of received signal power undergoes the information detection (ID) chain and the other portion passes through the energy harvesting (EH) circuitry. Therefore, the achievable information rate (by treating interference as noise) and harvested energy are formulated as

$$R_k = \log_2\left(1 + \frac{\eta_k p_k |h_{kk}|^2}{\sigma^2 + \eta_k \sum_{\substack{j=1 \\ j\neq k}}^{K} p_j |h_{kj}|^2}\right), \quad \forall k \in \mathcal{K}, \tag{3}$$

$$E_k = (1-\eta_k)\sum_{j=1}^{K} p_j |h_{kj}|^2, \quad \forall k \in \mathcal{K}, \tag{4}$$

respectively, which guarantees reliable decoding with arbitrarily small decoding error. Notice that η_k is the power splitting coefficient at the kth legitimate receiver. Moreover, the transmit power from the kth transmitter is represented by p_k, i.e., $\mathbb{E}\{|x_k|^2\} = p_k$. Reliability is not the only concern in wiretap interference channels as the secrecy needs to be considered as well. The communication between kth pair of legitimate users is proved to be reliable and secure [11] if

$$R_k^{\mathrm{s}} = R_k - R_{\mathrm{E}_k} \geq 0, \quad \forall k \in \mathcal{K}, \tag{5}$$

where R_k is defined in (3) and

$$R_{\mathrm{E}k} = \log_2\left(1 + \frac{p_k \mathbf{u}_k^H \mathbf{h}_{\mathrm{E}_k}\mathbf{h}_{\mathrm{E}_k}^H \mathbf{u}_k}{\sigma_{\mathrm{E}}^2\|\mathbf{u}_k\|^2 + \sum_{\substack{j=1 \\ j\neq k}}^{K} p_j \mathbf{u}_k^H \mathbf{h}_{\mathrm{E}_j}\mathbf{h}_{\mathrm{E}_j}^H \mathbf{u}_k}\right), \ \forall k \in \mathcal{K}. \tag{6}$$

Notice that $\mathbf{u}_k^H$ is the signal post processing vector at the eavesdropper for obtaining the transmit signal from kth user. Now, by transmitting with the secrecy coding rate in (5), the legitimate receivers are able to decode the signals from the corresponding transmitters reliably and securely. That means, the eavesdropper fails in decoding the signals from the legitimate transmitters.

Here, we assume that the eavesdropper deploys two receive structures defined by its computational capabilities, namely

1) maximum ratio combining (MRC),
2) minimum mean-squared error and successive interference cancellation (MMSE-SIC).

Note that MMSE-SIC corresponds with the optimal linear reception at the eavesdropper. Hence, worst-case secrecy rates are associated with this type of reception at the eavesdropper.

Secrecy Rate Region: By defining kth user achievable secrecy rate in (5), the secrecy rate region of the wiretap interference channel is defined as

$$\mathcal{R}^{\mathrm{s}} \triangleq \bigcup_{\substack{p_k \leq p_{k_{\max}},\ \forall k\in\mathcal{K} \\ 0\leq\eta_k\leq 1,\ \forall k\in\mathcal{K}}} \{\mathbf{r} | \mathbf{0} \leq \mathbf{r} \leq \bar{\mathbf{r}}^{\mathrm{s}}\}, \tag{7}$$

where $p_{k_{\max}}$ is the available power budget at the kth legitimate transmitter and $\bar{\mathbf{r}}^{\mathrm{s}} = [R_1^{\mathrm{s}}, ..., R_K^{\mathrm{s}}]$ specifies the outermost achievable secrecy rate tuples. Notice that, the secrecy rate region can be uniquely characterized by determining the rate tuples on the boundary of the secrecy rate region. Determining these rates require optimal resource allocation at the transmitter alongside receivers power splitting optimization. In what follows, we present the achievable secrecy rate region of the wiretap interference channel under energy harvesting constraints of the legitimate users.

III. MRC at the Eavesdropper

In this section, we study the case that the eavesdropper uses maximum ratio combining as the post processing vector, $\mathbf{u}_k = \frac{\mathbf{h}_{\mathrm{E}_k}}{\|\mathbf{h}_{\mathrm{E}_k}\|}$. Then, (6) is reformulated as

$$R_{\mathrm{E}k} = \log_2\left(1 + \frac{p_k\|\mathbf{h}_{\mathrm{E}_k}\|^2}{\sigma_{\mathrm{E}}^2 + \mathbf{u}_k^H \sum_{\substack{j=1 \\ j\neq k}}^{K} p_j \mathbf{h}_{\mathrm{E}_j}\mathbf{h}_{\mathrm{E}_j}^H \mathbf{u}_k}\right), \quad \forall k \in \mathcal{K}. \tag{8}$$

By plugging (3) and (8) into (5), we obtain

$$R_k^{\mathrm{s}} = \log_2\left(\frac{\left(\sigma^2 + \eta_k \sum_{j=1}^{K} p_j |h_{kj}|^2\right)\left(\sigma_{\mathrm{E}}^2 + \mathbf{u}_k^H \sum_{\substack{j=1 \\ j\neq k}}^{K} p_j \mathbf{h}_{\mathrm{E}_j}\mathbf{h}_{\mathrm{E}_j}^H \mathbf{u}_k\right)}{\left(\sigma^2 + \eta_k \sum_{\substack{j=1 \\ j\neq k}}^{K} p_j |h_{kj}|^2\right)\left(\sigma_{\mathrm{E}}^2 + \mathbf{u}_k^H \sum_{j=1}^{K} p_j \mathbf{h}_{\mathrm{E}_j}\mathbf{h}_{\mathrm{E}_j}^H \mathbf{u}_k\right)}\right).$$

Now, the secrecy rate region can be characterized by formulating the following weighted max-min optimization problem

$$\max_{\boldsymbol{\eta},\mathbf{p}} \quad \min_k \frac{R_k^{\mathrm{s}}}{\alpha_k} \tag{9}$$

$$\text{subject to} \quad E_k \geq \psi_k, \tag{9a}$$

$$\mathbf{p} \leq \mathbf{p}_{\max}, [1] \tag{9b}$$

$$\mathbf{0} \leq \boldsymbol{\eta} \leq \mathbf{1}, \tag{9c}$$

where $\mathbf{p} = [p_1, ..., p_K]$ and $\boldsymbol{\eta} = [\eta_1, ..., \eta_K]$. Moreover, $\mathbf{p}_{\max} = [p_{1_{\max}}, ..., p_{K_{\max}}]$ is the power budget available at the users. The energy harvesting constraint is given by (9a), where

[1] $\mathbf{a} \leq \mathbf{b}$: vector $\mathbf{a}$ is less than or equal to vector $\mathbf{b}$, if each element in $\mathbf{a}$ is less than or equal to the corresponding element in $\mathbf{b}$.

the energy demand of the kth user is represented by ψ_k. The weight vector $\boldsymbol{\alpha} = [\alpha_1, ..., \alpha_K]$ is determined apriori with $0 \leq \alpha_k \leq 1,\ \forall k$ and $\|\boldsymbol{\alpha}\|_1 = 1$. Notice that, with each realization of $\boldsymbol{\alpha}$ we obtain a secure achievable rate on the rate region Pareto boundary. Hence, solving problem (9) for each realization of $\boldsymbol{\alpha} \in \mathbb{R}^K$ with a predefined resolution, delivers the secrecy rate region [12]. The Pareto boundary represents the outermost boundary of the achievable secrecy rate tuples, where by increasing the secrecy rate of one user, the secrecy rate of at least one other user is inevitably decreased. Problem (9) is a non-convex problem. This is due to the non-convexity of the objective function, which is the division of non-convex functions. By defining an auxiliary variable $\beta = \min_k \frac{R_k^{\mathrm{s}}}{\alpha_k}$, we transfer the objective function into the constraint set. Then we obtain,

$$\max_{\beta, \boldsymbol{\eta}, \mathbf{p}} \quad \beta \tag{10}$$

$$\text{subject to} \quad \beta\alpha_k \leq R_k^{\mathrm{s}}, \quad \forall k \in \mathcal{K}, \tag{10a}$$

$$(9a), (9b), (9c). \tag{10b}$$

We can reformulate constraints (10a) as

$$\frac{\lambda^{\alpha_k}\left(\sigma^2 + \eta_k \sum_{\substack{j=1 \\ j\neq k}}^{K} p_j |h_{kj}|^2\right)\left(\sigma_{\mathrm{E}}^2 + \mathbf{u}_k^H \sum_{j=1}^{K} p_j \mathbf{h}_{\mathrm{E}_j}\mathbf{h}_{\mathrm{E}_j}^H \mathbf{u}_k\right)}{\left(\sigma^2 + \eta_k \sum_{j=1}^{K} p_j |h_{kj}|^2\right)\left(\sigma_{\mathrm{E}}^2 + \mathbf{u}_k^H \sum_{\substack{j=1 \\ j\neq k}}^{K} p_j \mathbf{h}_{\mathrm{E}_j}\mathbf{h}_{\mathrm{E}_j}^H \mathbf{u}_k\right)} \leq 1, \tag{11}$$

where we defined $\lambda = 2^{\beta}$. Since λ is monotonically increasing as a function of β in optimization problem (10), we replace β with λ. The energy harvesting constraints in (9a) are reformulated as

$$\frac{\psi_k + \eta_k \sum_{j=1}^{K} p_j |h_{kj}|^2}{\sum_{j=1}^{K} p_j |h_{kj}|^2} \leq 1. \tag{12}$$

Hence, we obtain

$$\max_{\lambda, \boldsymbol{\eta}, \mathbf{p}} \quad \lambda \qquad \text{subject to} \quad (11), (12), (9b), (9c), \tag{13}$$

The constraints (11) and (12) are divisions of posynomials, which are not necessarily convex functions. This renders the weighted max-min optimization problem into a signomial program which is NP-hard problem [13]. Here, we approximate the denominator of the functions in (11) and (12) with a monomial function based on the single condensation method. This approximation is based on the relation between arithmetic and geometric means [14]. For instance, the denominator of constraint (12) can be approximated as

$$\sum_{j=1}^{K} p_j |h_{kj}|^2 \geq \prod_{j=1}^{K} \left(\frac{p_j |h_{kj}|^2}{c_{kj}}\right)^{c_{kj}}, \tag{14}$$

where $c_{kj},\ \forall j$, controls the approximation gap. Inequality (14) holds with equality with the optimal value of $c_{kj},\ \forall j$, which is

$$c_{kj}^{\star} = \frac{p_j |h_{kj}|^2}{\sum_{j=1}^{K} p_j |h_{kj}|^2}. \tag{15}$$

Similar approximation is applied for the denominator of (11). Utilizing $c_{kj}^{\star}$ as a function of $\mathbf{p}$ renders the problem to be non-convex, hence we resolve it iteratively. Here, we tighten the approximation gap by optimizing over p_j and $\eta_j,\ \forall j$ and using the solutions to obtain $c_{kj}^{\star}$. Notice that this $c_{kj}^{\star}$ is optimal only for the current iteration and suboptimal for the next iteration.

Lemma 1. *Exploiting MRC at the eavesdropper results in the worst-case achievable secrecy rates for any given* $\|\mathbf{h}_{E_k}\|^2,\ \forall k \in \mathcal{K}$*, if and only if* $M \geq K$ *and*

$$\mathbf{h}_{E_k} = \text{Null}\left(\mathbf{h}_{E_1}, ...\mathbf{h}_{E_{k-1}}, \mathbf{h}_{E_{k+1}}, \mathbf{h}_{E_K}\right),\ \forall k \in \mathcal{K}, \tag{16}$$

where $\text{Null}\left(\mathbf{h}_{E_1}, ...\mathbf{h}_{E_{k-1}}, \mathbf{h}_{E_{k+1}}, \mathbf{h}_{E_K}\right)$ *represents the null space of the subspace spanned by* $\mathbf{h}_{E_1}, ...\mathbf{h}_{E_{k-1}}, \mathbf{h}_{E_{k+1}}, \mathbf{h}_{E_K}$.

Proof. Having $M \geq K$, provides sufficient dimensions for the probability that the channels are orthogonal to each other. For orthogonal channels from the legitimate transmitters to the eavesdropper, MRC simultaneously nulls the interference and maximizes the signal-to-noise ratio (SNR). Therefore, $R_{\mathrm{E}_k},\ \forall k$ is maximized which in consequence minimizes $R_k^{\mathrm{s}},\ \forall k$. □

The occurrence of the orthogonal channels given in (16) is of measure zero (almost never happens) assuming limited number of antennas at the eavesdropper. Therefore, it is of importance to investigate the worst-case secrecy rate region for arbitrary channel realizations. For any given channel realization, among all linear receivers, utilizing MMSE-SIC at the eavesdropper delivers the secrecy rate region lower-bound which is going to be discussed in the following section.

IV. MMSE and SIC at the Eavesdropper

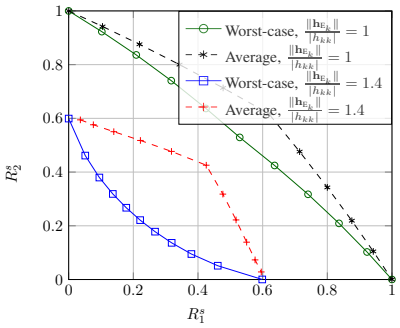
In this section, we assume that the eavesdropper is capable of performing MMSE-SIC at the signal combining stage. Thus, the signal combining vector $\mathbf{u}_k,\ \forall k$ that minimizes the mean of the squared-error is

$$\mathbf{u}_k^{\mathrm{mmse}} = \left(\sum_{j=k+1}^{K} p_j \mathbf{h}_{\mathrm{E}_j}\mathbf{h}_{\mathrm{E}_j}^H + \sigma_{\mathrm{E}}^2 \mathbf{I}\right)^{-1} \mathbf{h}_{\mathrm{E}_k}, \quad \forall k \in \mathcal{K}. \tag{17}$$

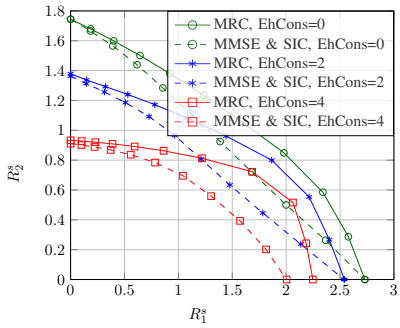
As can be seen from (17), the MMSE signal combining is a function of the power allocation performed at the legitimate receivers. Hence, we assume that the eavesdropper

1) knows neither the power budget nor the transmit power at the legitimate users: MMSE with $p_j = 1,\ \forall j$,
2) only knows the power budget at the legitimate users: MMSE with $p_j = p_{j_{\max}},\ \forall j$,
3) knows the actual transmit power at the legitimate users: MMSE with $p_j = p_j^{\star},\ \forall j$.

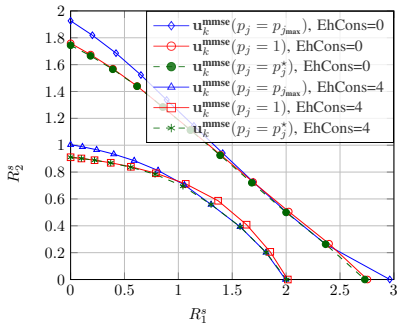
The first two assumptions are trivial and we only present the simulation results in section V. However, the last assumption provides the worst-case secrecy rate region, which is discussed in this section. By utilizing $\mathbf{u}_k^{\mathrm{mmse}},\ \forall k$ as a function of $p_j,\ \forall j$, and performing SIC, the kth legitimate user's achievable secrecy rate is formulated similar to (6). Now, we formulate the weighted max-min optimization problem



(a) Average vs. worst-case achievable secrecy rate region with MRC at the eavesdropper. $\frac{|h_{kj}|}{|h_{kk}|}=0.6,\ \forall j\neq k$.



(b) MRC vs. MMSE and SIC at the eavesdropper



(c) MMSE and SIC with suboptimal linear processings at the eavesdropper.

Fig. 2: Secrecy rate region of wiretap interference channel with weak and strong multi-antenna eavesdropper. The transmit signal budget to receiver AWGN variance is $\mathrm{SINR}_{\mathrm{T}_k}=5,\ \forall k\in\mathcal{K}$

similar to problem (13) to obtain the secrecy rate region. This problem becomes non-convex in the optimization variables, $\lambda, \mathbf{p}, \boldsymbol{\eta}$. Here, we propose an approach with inner and outer iterations to obtain a suboptimal solution, which is improved iteratively. In this approach, the transmit power $\mathbf{p}$, the receiver power splitting coefficients $\boldsymbol{\eta}$ and the auxiliary variable λ is optimized in an inner iteration loop. However, the MMSE signal combining vector is optimized in an outer iteration loop. This procedure in elaborated in Algorithm I in details. It is important to mention that the decoding order at the eavesdropper is not captured in the optimization framework. Here, we compare the solutions of all decoding order that is $K!$ combinations and the convex hull of all achievable rate tuples delivers the secrecy rate region.

Algorithm 1 Eavesdropper with MMSE and SIC

1: Set $\boldsymbol{\alpha}$, s.t. $\|\boldsymbol{\alpha}\|_1=1,\ \boldsymbol{\alpha}\geq\mathbf{0}$,
2: Initialize $\boldsymbol{\eta}^{(1)}=\mathbf{1}$
3: Initialize $\mathbf{p}^{(1)}=\mathbf{p}_{\max}$
4: Outer-iteration index $l=1$
5: **while** $A^{(l)}-A^{(l-1)}$ large **do**
6: Set $\mathbf{u}_k^{(l)}=\left(\sum_{\substack{j=k+1\\ j\neq k}}^{K} p_j^{(1)}\mathbf{h}_{\mathrm{E}_j}\mathbf{h}_{\mathrm{E}_j}^H+\sigma_{\mathrm{E}}^2\mathbf{I}\right)^{-1}\mathbf{h}_{\mathrm{E}_k},\ \forall k$
7: Inner-iteration index $q=1$
8: **while** $B^{(q)}-B^{(q-1)}$ large **do**
9: Formulate weighted max-min optimization problem similar to (13)
10: Utilize the approximation in (14)
11: Solve the weighted max-min problem (geometric program) and obtain $\left(\mathbf{p}^{\star(q)},\boldsymbol{\eta}^{\star(q)},\lambda^{\star(q)}\right)$
12: $q=q+1$
13: Calculate posynomial to monomial approximation gap $B^{(q)}=\mathrm{func}\left(\mathbf{p}^{\star(q)},\boldsymbol{\eta}^{\star(q)},\lambda^{\star(q)}\right)$
14: **end while**
15: $l=l+1$
16: $A^{(l)}=\lambda^{\star(q)}$
17: $p^{(l)}=p_j^{\star(q)}$
18: **end while**

V. Numerical Results

We consider two legitimate users that are wiretapped by an eavesdropper equipped with two antennas, i.e., $K=M=2$. The ratio between transmit signal power budget and receiver AWGN variance over legitimate and eavesdropper channels are assumed to be equal to 5, i.e., $\mathrm{SINR}_{\mathrm{T}_k}=\frac{p_{k_{\max}}}{\sigma^2}=\frac{p_{k_{\max}}}{\sigma_{\mathrm{E}}^2}=5,\ \forall k\in\mathcal{K}$. Secure communication should be guaranteed under energy harvesting constraints at the legitimate receivers. By solving optimization problem (13) with the proposed iterative method, we obtain the secrecy rate region with MRC at the eavesdropper. Assuming MMSE-SIC at the eavesdropper, the Pareto boundary of the achievable secrecy rate region is obtained by Algorithm 1. Notice that, these optimization problems need to be solved for $\boldsymbol{\alpha}\in\mathbb{A}=\{\boldsymbol{\alpha}\in\mathbb{R}^2|\boldsymbol{\alpha}\geq\mathbf{0},\|\boldsymbol{\alpha}\|_1=1\}$. In Fig. 2(a), the average achievable secrecy rate region assuming an eavesdropper with MRC capability is compared to the worst-case scenario from lemma 1. There, we observe the convexity of the worst-case secrecy rate region for the case that the legitimate users channel strength is equal to the eavesdropper channel strength. Furthermore we compare the secrecy rate region assuming MRC and MMSE-SIC at the eavesdropper in Fig. 2(b). In that figure, we observe the performance gap of MRC compared to MMSE-SIC from the secrecy rate perspective. Moreover, simultaneous transmission with power control at the transmitters and optimal power splitting tuning at the receiver outperforms time sharing between the users. This performance gap is enlarged with increasing energy harvesting demands. Furthermore, the shrinkage of the achievable secrecy rate region as a function of energy demands at the legitimate receivers is worth noting. Notice that, the worst-case scenario is only for performance comparison. That means higher secrecy rate tuples are always achievable due to the absence of optimal power allocation knowledge at the eavesdropper. This can be seen in Fig. 2(c), where eavesdropper does not access the legitimate users' transmit power, when decoding kth user's signal. Hence, MMSE is performed by assuming $p_j=1$ and $p_j=p_{j_{\max}},\ \forall j\in\{k+1,...,K\}$. Moreover, given the actual transmit power of the legitimate users at the eavesdropper as a side information, the secrecy rate region is not enlarged significantly.

REFERENCES

[1] R. Roman, J. Zhou, and J. Lopez, *On the Security of Wireless Sensor Networks*. Springer Berlin Heidelberg, 2005.

[2] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint Power Control in Wiretap Interference Channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3810–3823, July 2015.

[3] C. Geng, N. Naderializadeh, A. S. Avestimehr, and S. A. Jafar, "On the Optimality of Treating Interference as Noise," *IEEE Transactions on Information Theory*, vol. 61, no. 4, pp. 1753–1767, April 2015.

[4] S. Gherekhloo, A. Chaaban, C. Di, and A. Sezgin, "(Sub-)Optimality of Treating Interference as Noise in the Cellular Uplink With Weak Interference," *IEEE Transactions on Information Theory*, vol. 62, no. 1, pp. 322–356, Jan 2016.

[5] B. Li, Z. Fei, Z. Chu, and Y. Zhang, "Secure transmission for heterogeneous cellular networks with wireless information and power transfer," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–12, 2017.

[6] X. Chen, X. Chen, and T. Liu, "A unified performance optimization for secrecy wireless information and power transfer over interference channels," *IEEE Access*, vol. 5, pp. 12 726–12 736, 2017.

[7] Z. Ni and M. Motani, "Transmission schemes and performance analysis for time-switching energy harvesting receivers," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[8] G. Pan, H. Lei, Y. Yuan, and Z. Ding, "Performance Analysis and Optimization for SWIPT Wireless Sensor Networks," *IEEE Transactions on Communications*, vol. PP, no. 99, pp. 1–1, 2017.

[9] L. Liu, R. Zhang, and K. C. Chua, "Wireless Information and Power Transfer: A Dynamic Power Splitting Approach," *IEEE Transactions on Communications*, vol. 61, no. 9, pp. 3990–4001, September 2013.

[10] A. Kariminezhad, S. Gherekhloo, and A. Sezgin, "Optimal Power Splitting for Simultaneous Information Detection and Energy Harvesting," *IEEE Signal Processing Letters*, vol. 24, no. 7, pp. 963–967, July 2017.

[11] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, July 1978.

[12] E. Bjornson, E. Jorswieck, M. Debbah, and B. Ottersten, "Multiobjective Signal Processing Optimization: The way to balance conflicting metrics in 5G systems," *IEEE Signal Proc. Magazine*, vol. 31, no. 6, pp. 14–23, Nov 2014.

[13] M. Chiang, *Geometric Programming for Communication Systems*, ser. Foundations and trends in communications and information theory. Now Publishers.

[14] S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optimization and Engineering*, vol. 8, no. 1, pp. 67–127, Apr 2007.