ASM Sc. J., 13, Special Issue 2, 2020 for ICSCC2019, 58-64

Secure SWIPT MISO with Imperfect Channel State Information

Tiong Teck Chai

Electrical and Computer Engineering, Curtin University Malaysia,
CDT 250 Miri 98009 Sarawak Malaysia

Physical security techniques can improve secure wireless information transmission by generating more interference to potential eavesdroppers. This paper studies the secure transmission issue for simultaneous wireless information and power transfer (SWIPT) in a multiuser system with multiple eavesdroppers, where the base station transmitter broadcasts confidential message to legitimate multiple single-antenna information receivers (IRs) and multiple single-antenna energy–harvesting receivers (ERs). Our objective is to maximize the secrecy rate of the IRs subject to individual harvested energy constraints of the ERs for the case where the ERs can form eavesdropping party to carry out joint decoding in an attempt to illicitly decode the secret message intended for the IRs. The initial non-convex problem is converted to convex problem through semi-definite programming (SDP) relaxation for both perfect CSI and imperfect CSI. Numerical simulations are presented to demonstrate the performance under different scenarios.

Keywords: simultaneous wireless information and power transfer (SWIPT); energy harvesting; masked beamforming; secure beamforming; MISO downlink

I. INTRODUCTION

Multicasting through wireless channel is increasing important for video broadcasting and streaming media (Gopal *et al.*, 2017). Simultaneous wireless information and power transfer (SWIPT) promising technology to solve the energy scarcity problem in energy-constrained wireless networks by integrating the radio frequency (RF) energy harvesting capability into wireless devices (Zhang *et al.,* 2013).

Physical security techniques can improve secure wireless information transmission by generating more interference to potential eavesdroppers. By adding artificial noise (AN) and projecting it onto the null space of information user channels in information transmit beamforming, the potential eavesdroppers would experience a higher noise floor and thus obtain less information about the messages transmitted to the legitimate receivers (Li & Ma 2013). In SWIPT systems, AN injection can increase information transmission secrecy capacity while not downgrading simultaneous power transfer (Shi *et al.,* 2015). SWIPT multicasting in multiple-input-single-output (MISO) has been studied in (Khandaker & Wong 2014).

The total transmission power was minimized while satisfying the secrecy rate and energy harvesting constraints at each receiver in multiuser SWIPT MISO systems (Zhang *et al.,* 2015). However, this work assumes that the transmitter has perfect CSI, which may not be possible in some applications.

In this paper, we consider a secure MISO SWIPT system comprising one multi-antenna transmitter, two single antenna IRs, and multiple single-antenna ERs. Our aim is to design jointly the information and energy transmit beamforming in order to maximize the secrecy rate of the IRs subject to individual harvested energy constraints of the ERs whereas the ERs may collude to perform eavesdropping party for joint decoding. Worst-case robust beamforming is designed to deal with channel CSI uncertainty.

This initial non-convex problem is formulated to two stage maximization problem. The inner problem is recast to a

*Corresponding author's e-mail: tiong.teck.chai@curtin.edu.my

convex SDP (Semidefinite Programming) problem. The outer problem can be solved by one dimensional line search.

The rest of this paper is organized as follows. In section II, A MISO SWIPT with colluding eavesdroppers is modelled in section III, masked beamforming for perfect CSI is designed. In section IV, worst-case based robust secure beamforming is designed. In section V, Matlab simulations present the optimal solution. Finally, conclusions are drawn in the last section.

II. SYSTEM MODEL

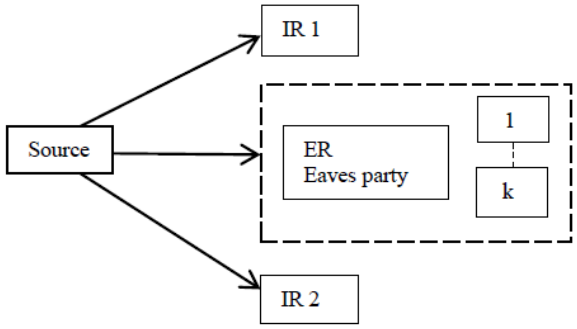

Figure 1. A MISO SWIPT with colluding eavesdroppers

We consider a SWIPT MISO downlink system as shown in Figure 1. The source or transmitter has $N_s > 1$ transmitting antennas and each receiver has single receiving antenna. Some of the receivers are information receiver (IR) while other receivers are energy receivers (ER). The source applies linear transmit beamforming to send secret information multicasting to the IRs. The ERs are supposed only to harvest energy.

Let be the transmit signal vector, the received signals at the mth IR and the kth ER can be expressed as

$$\mathbf{y}_{I,m} = \mathbf{h}_{I,m}\mathbf{x} + \mathbf{n}_{I,m} \quad (1)$$

$$\mathbf{y}_{E,k} = \mathbf{h}_{E,k}\mathbf{x} + \mathbf{n}_{E,k}, \quad \text{for k = 1 to K} \quad (2)$$

where $h_{I,m}$ are complex channel vector between the source and the mth IR. $h_{e,k}$ are complex channel vector between the source and the kth ER respectively.

The noise $\mathbf{n}_{I,m} \sim CN(0,\sigma_I^2)$ and $\mathbf{n}_{E,k} \sim CN(0,\sigma_e^2)$ are additive white Gaussian noise at the mth IR and kth ER respectively.

The source signal $\mathbf{x}$ is

$$\mathbf{x} = \mathbf{b}_I s_I + \mathbf{b}_E \quad (3)$$

$\mathbf{b}_I s_I$ is information beamforming vector and $\mathbf{b}_E$ is the energy-carrying artificial noise (AN) vector. $s_I \sim CN(0,1)$ is the confidential information bearing signal for the IR. $\mathbf{b}_E = \sum_{i=1}^{k} \mathbf{b}_{E,i} s_{E,i}$ is the sum of energy beams, where $\mathbf{b}_E$ is the ith energy beamforming vector and $s_{E,i} \sim CN(0,1)$ is the ith energy-carrying noise signal.

The ERs may become eavesdroppers. All the eavesdroppers are colluding i.e., cooperate and form a joint decoder. They perform joint maximum signal to interference noise ratio (SINR) receive beamforming. Let $\mathbf{Q}_I$ be the transmit covariance and $\mathbf{Q}_E = \sum_{i=1}^{k} \mathbf{b}_{E,i}\mathbf{b}_{E,i}^H$ is the energy covariance. The mutual information (MI) between the source and the IR is given by

$$C_I(\mathbf{Q}_I, \mathbf{Q}_E) = \log\left(1 + \frac{\mathbf{h}_I^H \mathbf{Q}_I^H \mathbf{h}_I}{\sigma_I^2 + \mathbf{h}_I^H \mathbf{Q}_E^H \mathbf{h}_I}\right) \quad (4)$$

and the mutual information between the source and ER is

$$C_E(\mathbf{Q}_I, \mathbf{Q}_E) = \log\det\left(\mathbf{I}_k + \left(\sigma_E^2 \mathbf{I}_k + \mathbf{H}_E^H \mathbf{Q}_E \mathbf{H}_E\right)^{-1} \times \mathbf{H}_E^H \mathbf{Q}_I \mathbf{H}_E\right) \quad (5)$$

The colluded channel matrix $\mathbf{H}_E$ is formed as $\mathbf{H}_E = [\mathbf{h}_{e,1}, \ldots, \mathbf{h}_{e,k}]$. The achievable secrecy rate is

$$\mathbf{C}_s = C_I(\mathbf{Q}_I, \mathbf{Q}_E) - C_E(\mathbf{Q}_I, \mathbf{Q}_E) \quad (6)$$

This is perfect secrecy rate when the IR can decode the confidential information correctly at $\mathbf{C}_s$ bits per channel use, while the ER can almost decode nothing about the secret message (Goel & Negi 2008).

The objective is to design transmit and covariance matrix $(\mathbf{Q}_I, \mathbf{Q}_E)$ in such a way that maximum information secrecy can be obtained under power constraints.

The secrecy rate maximization problem is expressed as

$$\max_{\mathbf{Q}_I,\mathbf{Q}_E} \; C_I(\mathbf{Q}_I,\mathbf{Q}_E)-C_E(\mathbf{Q}_I,\mathbf{Q}_E) \tag{7a}$$

$$\text{s.t. } \operatorname{tr}(\mathbf{Q}_I+\mathbf{Q}_E)\le P_T \tag{7b}$$

$$\zeta_k\left(\mathbf{h}_{E,k}^H(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_{E,k}\right)\ge \eta_k \tag{7c}$$

$$\mathbf{Q}_I\succeq 0,\ \mathbf{Q}_E\succeq 0 \tag{7d}$$

where $\xi_k \in (0,1]$ denotes the energy conversion efficiency of the kth ER. The minimum required harvested power at kth ER is η_k. tr is trace. P_T is transmission power budget. $\zeta_k = 0.5$ in this paper.

III. MASKED BEAMFORMING FOR FERFECT CSI

CSI for the IRs and ERs are available at the source. Possible eavesdropping by ERs can be prevented much more effectively by generating spatially selective AN, rather than applying AN isotropic (Li & Ma 2013).

Reformulate Problem (7) as

$$\max_{\mathbf{Q}_I,\mathbf{Q}_E,\phi} \; C_I(\mathbf{Q}_I,\mathbf{Q}_E)-\log\phi \tag{8a}$$

$$\text{s.t. } C_E(\mathbf{Q}_I,\mathbf{Q}_E)\le \phi \tag{8b}$$

$$\operatorname{tr}(\mathbf{Q}_I+\mathbf{Q}_E)\le P_T \tag{8c}$$

$$\left(\mathbf{h}_{E,k}^H(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_{E,k}\right)\ge \eta_k \tag{8d}$$

$$\mathbf{Q}_I\succeq 0,\ \mathbf{Q}_E\succeq 0,\ \phi\ge 1 \tag{8e}$$

where ϕ is a slack variable used to simplify the objective function. Without loss of generality, assume that $\sigma_I^2=\sigma_E^2=1$. Substitute (4) and (5) into (8), the problem can be expressed as

$$\max_{\mathbf{Q}_I,\mathbf{Q}_E,\phi} \; \log\left(\frac{1+\mathbf{h}_I^h(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_I}{\phi\left(1+\mathbf{h}_E^H\mathbf{Q}_E\mathbf{h}_I\right)}\right) \tag{9a}$$

$$\text{s.t. } \log\det\left(\mathbf{I}_k+\left(\mathbf{I}_k+\mathbf{H}_E^H\mathbf{Q}_E\mathbf{H}_E\right)^{-1}\mathbf{H}_E^H\mathbf{Q}_I\mathbf{H}_E\right)$$

$$\le \log\phi \tag{9b}$$

$$\operatorname{tr}(\mathbf{Q}_I+\mathbf{Q}_E)\le P_T \tag{9c}$$

$$\left(\mathbf{h}_{E,k}^H(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_{E,k}\right)\ge \eta_k \tag{9d}$$

$$\mathbf{Q}_I\succeq 0,\ \mathbf{Q}_E\succeq 0,\ \phi\ge 1 \tag{9e}$$

Using lemma from [8], constraints (9b) can be reformulated and problem expressed as

$$\min_m \max_{\mathbf{Q}_I,\mathbf{Q}_E,\phi} \sum_{i=1}^{m} \log\left(\frac{1+\mathbf{h}_I^h(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_I}{\phi\left(1+\mathbf{h}_E^H\mathbf{Q}_E\mathbf{h}_I\right)}\right) \tag{10a}$$

$$\text{s.t.} \quad (\phi-1)\left(\mathbf{I}_k+\mathbf{H}_E^H\mathbf{Q}_E\mathbf{H}_E\right)\succeq \mathbf{H}_E^H\mathbf{Q}_I\mathbf{H}_E \tag{10b}$$

$$\operatorname{tr}(\mathbf{Q}_I+\mathbf{Q}_E)\le P_T \tag{10c}$$

$$\left(\mathbf{h}_{E,k}^H(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_{E,k}\right)\ge \eta_k \tag{10d}$$

$$\mathbf{Q}_I\succeq 0,\ \mathbf{Q}_E\succeq 0,\ \phi\ge 1 \tag{10e}$$

Problem (11) can be reformulated as a two-stage problem:

$$\min_m \max_{\phi} \left\{ \begin{array}{ll} \max\limits_{\mathbf{Q}_I,\mathbf{Q}_E} \log\left(\frac{1+\mathbf{h}_I^h(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_I}{\phi\left(1+\mathbf{h}_E^H\mathbf{Q}_E\mathbf{h}_I\right)}\right) & (11a) \\ (\phi-1)\left(\mathbf{I}_k+\mathbf{H}_E^H\mathbf{Q}_E\mathbf{H}_E\right)\succeq \mathbf{H}_E^H\mathbf{Q}_I\mathbf{H}_E & (11b) \\ tr(\mathbf{Q}_I+\mathbf{Q}_E)\le P_T & (11c) \\ \left(\mathbf{h}_{E,k}^H(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_{E,k}\right)\ge \eta_k & (11d) \\ \mathbf{Q}_I\succeq 0,\ \mathbf{Q}_E\succeq 0,\ \phi\ge 1 & (11e) \end{array} \right\}$$

Given the optimal objective value C_I^* of the inner maximization problem, the corresponding secrecy rate constrained power minimization problem can be expressed as;

$$\min_{\mathbf{Q}_I,\mathbf{Q}_E} tr\sum_{i=1}^{m}(\mathbf{Q}_I+\mathbf{Q}_E) \tag{12a}$$

$$s.t. \;\; \log\left(\frac{1+\mathbf{h}_I^h(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{h}_I}{\phi\left(1+\mathbf{h}_E^H\mathbf{Q}_E\mathbf{h}_I\right)}\right)\ge C_I^* \tag{12b}$$

$$(\phi-1)\left(\mathbf{I}_k+\mathbf{H}_E^H\mathbf{Q}_E\mathbf{H}_E\right)\succeq \mathbf{H}_E^H\mathbf{Q}_I\mathbf{H}_E \tag{12c}$$

where $\mathbf{H}_{E,k}=\mathbf{h}_{E,k}\mathbf{h}_{E,k}^H$. Let $\beta=1-\phi 2^{C_I^*}$, problem (12) can be reformulated into a semi-definite program (SDP) as

$$\min_{\mathbf{Q}_I,\mathbf{Q}_E} tr\sum_{i=1}^{m} (\mathbf{Q}_I+\mathbf{Q}_E) \quad (13a)$$

$$\text{s.t.} \quad \text{tr}\left(\mathbf{h}_I\mathbf{h}_I^H(\mathbf{Q}_I+\beta\mathbf{Q}_E)\right)+\beta\geq 0 \quad (13b)$$

$$(\phi-1)\left(\mathbf{I}_k+\mathbf{H}_E^H\mathbf{Q}_E\mathbf{H}_E\right)\succeq \mathbf{H}_E^H\mathbf{Q}_I\mathbf{H}_E \quad (13c)$$

$$\left(\mathbf{H}_{E,k}^H(\mathbf{Q}_I+\mathbf{Q}_E)\mathbf{H}_{E,k}\right)\geq \eta_k \quad (13d)$$

$$\mathbf{Q}_I\succeq 0,\ \mathbf{Q}_E\succeq 0,\ \phi\geq 1 \quad (13e)$$

Problem (13) is convex and can be efficiently solved by convex optimization software tools such as CVX (Grant & Boyd 2014).

IV. WORST-CASE BASED ROBUST DESIGN FOR SECURE SWIPT

Consider the case that source has imperfect CSI for the eavesdroppers channels while having perfect CSI for the IRs.

Now, we adopt imperfect CSI based on the deterministic model (Mohammadkhani *et al.,* 2014). The actual channels between the transmitter and the kth ER, are modelled as

$$\mathbf{h}_{E,k} = \hat{\mathbf{h}}_{E,k}+\delta_k \quad \text{, for } k = 1 \text{ to K,} \quad (14)$$

where $\hat{\mathbf{h}}_{E,k}$ denote the estimated channel vector, while δ_k denote the CSI error vector. δ_k is bounded in its Euclidean norm, that is

$$\|\delta_k\|_2 = \left\|\mathbf{h}_{E,k}-\hat{\mathbf{h}}_{E,k}\right\|_2 \leq \varepsilon \quad (15)$$

The colluding eavesdroppers channel becomes $\mathbf{H}_E=\hat{\mathbf{H}}_E+\mathbf{\Delta}$ and $\|\Delta\|_F = \left\|\mathbf{H}_E-\hat{\mathbf{H}}_E\right\|_F \leq \varepsilon$.

The robust formulation of (8) becomes

$$\max_{\mathbf{Q}_I,\mathbf{Q}_E,\phi,\lambda_k,\lambda_{ce}} C_I(\mathbf{Q}_I,\mathbf{Q}_E)-\log\phi \quad (16a)$$

$$\text{s.t.} \quad \Phi_{ce}(\phi,\mathbf{Q}_I,\mathbf{Q}_E,\lambda_{ce})\succeq \mathbf{0} \quad (16b)$$

$$\text{tr}\left(\mathbf{Q}_I+\mathbf{Q}_E\right)\leq P_T \quad (16c)$$

$$\Omega(\mathbf{Q}_I,\mathbf{Q}_E,\lambda_k)\succeq \mathbf{0} \quad (16d)$$

$$\mathbf{Q}_I\succeq 0,\ \mathbf{Q}_E\succeq 0,\ \phi\geq 1 \quad (16e)$$

$$\phi\geq 1,\ \lambda_{ce}\geq 0,\ \lambda_k\geq 0,\ \forall k. \quad (16f)$$

where Φ_{ce} and Ω are defined at the bottom of the page (Tiong 2019).

Similar to the problem (13) for perfect CSI case, the optimal $(\mathbf{Q}_I,\mathbf{Q}_E)$ for the problem (16) can be obtained for given ϕ through solving the following robust secrecy rate constrained problem :

$$\min_{\mathbf{Q}_I,\mathbf{Q}_E} tr\sum_{i=1}^{m} (\mathbf{Q}_I+\mathbf{Q}_E) \quad (19a)$$

$$\text{s.t.} \quad \text{tr}\left(\mathbf{h}_I\mathbf{h}_I^H(\mathbf{Q}_I+\beta\mathbf{Q}_E)\right)+\beta\geq 0 \quad (19b)$$

$$\Phi_{ce}(\phi,\mathbf{Q}_I,\mathbf{Q}_E,\lambda_{ce})\succeq \mathbf{0} \quad (19c)$$

$$\Omega(\mathbf{Q}_I,\mathbf{Q}_E,\lambda_k)\succeq \mathbf{0} \quad (19d)$$

$$\mathbf{Q}_I\succeq 0,\ \mathbf{Q}_E\succeq 0,\ \phi\geq 1 \quad (19e)$$

$$\phi\geq 1,\ \lambda_{ce}\geq 0,\ \lambda_k\geq 0,\ \forall k. \quad (19f)$$

V. SIMULATION RESULTS

The transmitter is set with $N_s = 4$ antennas, 2 IRs and 3 EH receivers. The signal attenuation from source station to all mobile receivers is 30 dB corresponding to an equivalent distance of 5 meters.

$$\Phi_{ce}(\phi,\mathbf{Q}_I,\mathbf{Q}_E,\lambda_{ce}) \triangleq \begin{bmatrix} (\phi-1-\lambda_{ce})\mathbf{I}_k+\hat{\mathbf{H}}_E^H(\phi-1)\mathbf{Q}_E-\mathbf{Q}_I)\mathbf{H}_E & \hat{\mathbf{H}}_E^H(\phi-1)\mathbf{Q}_E-\mathbf{Q}_I) \\ (\phi-1)\mathbf{Q}_E-\mathbf{Q}_I)\hat{\mathbf{H}}_E & (\phi-1)\mathbf{Q}_E-\mathbf{Q}_I+\frac{\lambda_{ce}}{\varepsilon^2}\mathbf{I}_{Ns} \end{bmatrix}\succeq \mathbf{0} \quad (17)$$

$$\Omega(\mathbf{Q}_I,\mathbf{Q}_E,\lambda_k) \triangleq \begin{bmatrix} \lambda_k\mathbf{I}_{Ns}+\mathbf{Q}_I+\mathbf{Q}_E & (\mathbf{Q}_I+\mathbf{Q}_E)\hat{\mathbf{h}}_{E,k} \\ \hat{\mathbf{h}}_{E,k}^H(\mathbf{Q}_I+\mathbf{Q}_E) & \hat{\mathbf{h}}_{E,k}^H(\mathbf{Q}_I+\mathbf{Q}_E)\hat{\mathbf{h}}_{E,k}-\eta_k-\lambda_k\varepsilon^2 \end{bmatrix}\succeq \mathbf{0} \quad (18)$$

The source is broadcasting to all IRs. Each IR and ER is equipped with a single antenna. The environment is flat Rayleigh fading environment where the channel vectors have zero mean and unit variance. The system is set with energy harvesting threshold $\eta_k = \eta = -10\,dBm, \forall k$, and noise power $\sigma_m^2 = \sigma_k^2 = -30dBm$. The channel error vectors are uniformly and randomly generated in a sphere cantered at zero with $\varepsilon = 0.2$.

In Figure 2, we study these secrecy rate performances for different transmission power. We compare the achievable secrecy rates for the robust and non-robust algorithms with $(\eta = -10\,dBm)$ and without energy harvesting constraints. Figure 2 shows that the achievable secrecy rate increases when transmission powers increase for all cases. The achievable secrecy rate is lower with EH constraint compared to without EH constraint. This is due to transmission power is prioritized to satisfy EH constraint before improving secrecy rate. The achievable secrecy rate for robust algorithm is also lower compared to perfect CSI with zero channel estimation error. This is due to more transmission power is required to steer beamforming towards IR and EH in robust case. The achievable secrecy rate gap between without and with EH constraint for perfect CSI case remain constant when transmission power increase whereas the gap for robust case narrows. The latter is due to after initial transmission power is prioritized for satisfying EH constraint, the percentage for remaining power utilized for improving achievable secrecy rate increase with the increase in transmission power.

In Figure 3, We set transmit antenna number to be 6 and 7 respectively, with EH constraint $(\eta = -10dBm)$ and channel estimation error $\varepsilon = 0.2$. Figure 3 shows that more transmit antennas can achieve higher secrecy rate. This is due to more transmit antennas can provide more degree of freedom to steer beamforming towards IR and ER.

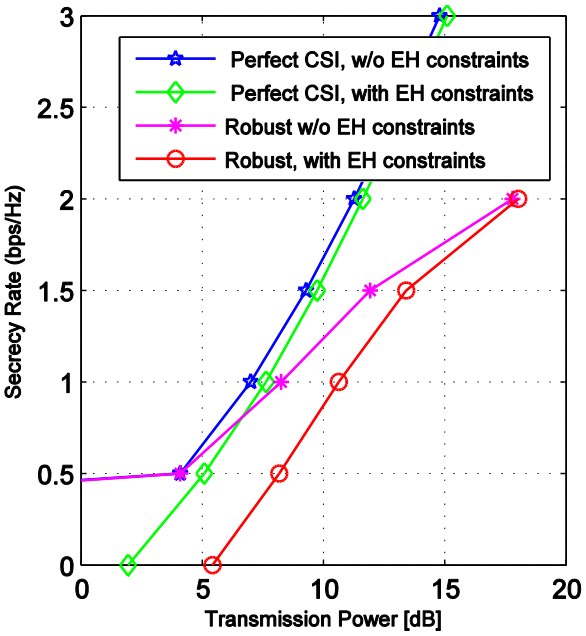

Figure 2. Secrecy rate versus transmision power

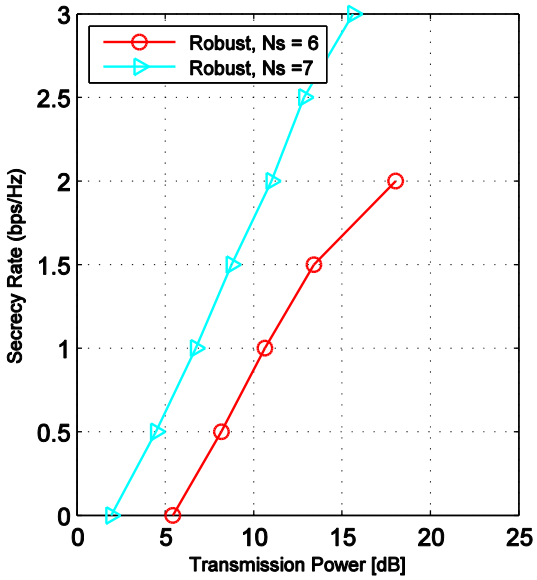

Figure 3. Secrecy rate versus transmission power with varying transmit antennas

In Figure 4, we set robust with energy harvesting constraint (R-EH), with $(\eta = -10dBm)$ and different channel estimation error variance. Figure 4 shows that the secrecy rate decreases with the increase in channel estimation error variance.

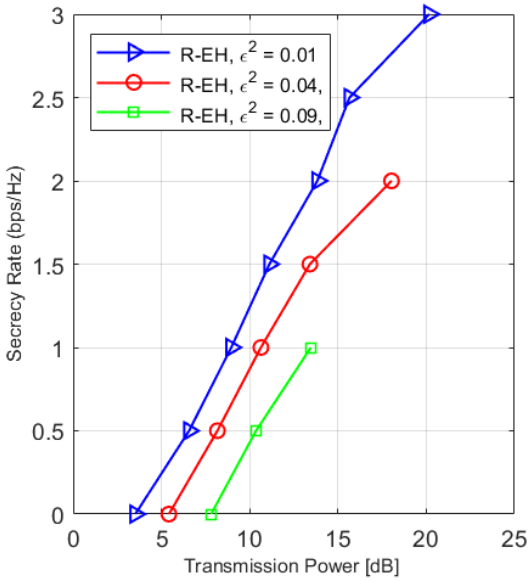

Figure 4. Secrecy rate versus transmission power with varying channel estimation variance

This is due to more transmission power is required to steer beamforming towards IR in higher channel estimation error variance.

In Figure 5, we set EH constraint (η=−10dBm), channel estimation error $\varepsilon = 0.2$ and vary the number of eavesdroppers. Figure 5 shows that secrecy rate decreases with increasing number of eavesdroppers. This is due to larger number of colluding eavesdroppers can more effectively eavesdrop IR secret message.

In Figure 6, we set channel estimation error $\varepsilon = 0.2$, 3 ERs (eavesdroppers) and vary the EH constraint. Figure 6 shows that secrecy rate decreases with increasing energy harvesting threshold. This is due to transmission power is prioritized to satisfy EH constraint before improving secrecy rate.

Figure 6, we set channel estimation error $\varepsilon = 0.2$, 3 ERs (eavesdroppers), EH constraint (η=−10dBm) and vary the IRs distance from the source. Figure 7 shows that secrecy rate decreases with increasing IRs distance from the source. This is due to more transmission power is required to steer beamforming directional towards IRs when the IRs are further away from the source.

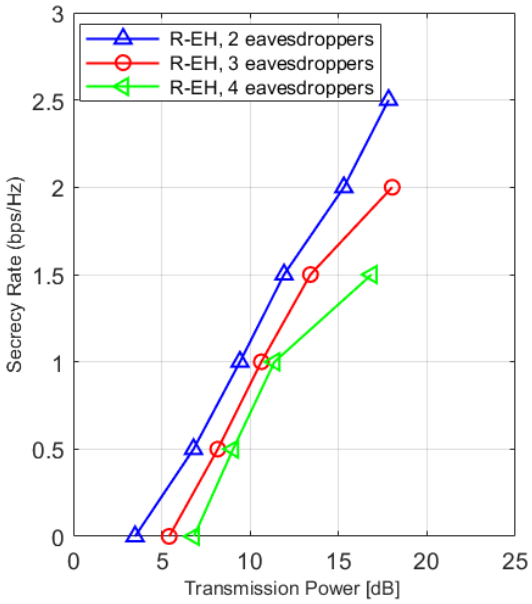

Figure 5. Secrecy rate versus transmission power with varying number of eavesdroppers

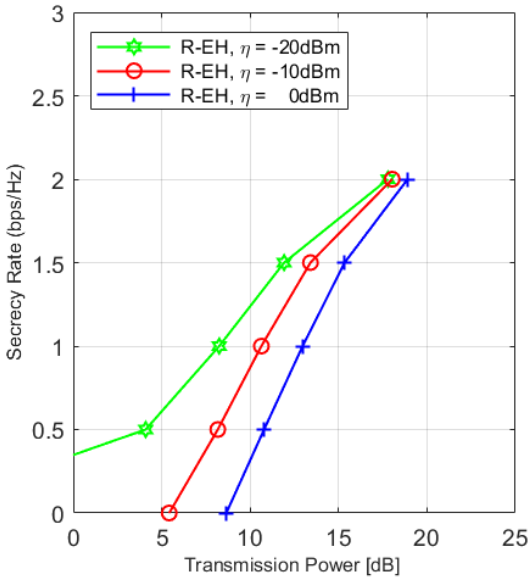

Figure 6. Secrecy rate versus transmission power with varying energy harvesting thresholds

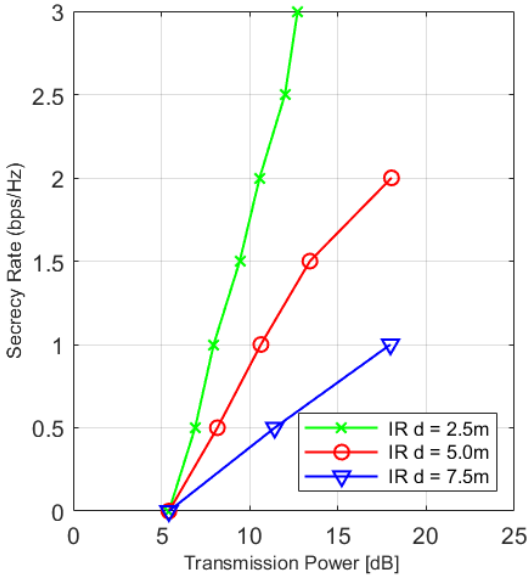

Figure 7. Secrecy rate versus transmission power with varying information receiver distances

VI. CONCLUSION

This paper has studied the secure beamforming design for SWIPT MISO system under both perfect CSI and imperfect CSI cases. Our design objective is to maximize the secrecy rate to the information receivers in the presence of colluding eavesdroppers while satisfying minimum transmission power to energy receivers.

VII. REFERENCES

Goel, S. & Negi, R. 2008, 'Guaranteeing secrecy using artificial noise', *IEEE Trans. Wireless Commun.,* vol. 7, no. 6, pp. 2180–2189.

Gopal, L., Rong, Y. & Zang, Z. 2017, 'Robust MMSE transceiver design for nonregenerative multicasting MIMO relay system', *IEEE Trans. Veh. Technol.,* vol. 66, no. 10, pp. 8979-8989.

Grant, M. & Boyd, S. 2014, *The CVX users guide*, viewed 1 March 2019, http://web.cvxr.com/cvx/doc/CVX.pdf.

Khandaker, M.R.A. & Wong, K.K. 2014, 'SWIPT in MISO multicasting systems', *IEEE Wireless Commun. Lett.,* vol. 3, no. 3, pp. 277–280.

Li, Q. & Ma, W.K. 2013, 'Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization', *IEEE Trans. Signal Process.,* vol. 61, no. 10, pp. 2704–2717.

Mohammadkhani, S., Razavizadeh, S.M. & Lee, I. 2014, 'Robust filter and forward relay beamforming with spherical channel state information uncertainties', in *2014 IEEE International Conference on Communications* (ICC), 10-14 June 2014, Sydney, NSW, Australia.

Shi, Q., Xu, W., Wu, J., Song, E. & Wang, Y., 2015, 'Secure beamforming for MIMO broadcasting with wireless information and power transfer', *IEEE Trans. Wireless Commun.,* vol. 14, no. 5, pp. 2841–2853.

Tiong, T.C. 2019, 'Robust secure SWIPT MISO', in *IEEE 2019 7th International Conference on Smart Computing & Communications,* 28-30 June 2019, Miri, Malaysia.

Zhang, H., Li, C., Huang, Y. & Yang, Y. 2015, 'Secure beamforming for SWIPT in multiuser MISO broadcast channel with confidential messages', IEEE *Commun. Lett.,* vol. 19, no. 8, pp. 1347 -1350.

Zhang, R. & Ho, C.K. 2013, 'MIMO broadcasting for simultaneous wireless information and power transfer', *IEEE Trans. Wireless Commun.,* vol. 12, no. 5, pp. 1989–2001.