Feasibility of Positive Secrecy Rate in Wiretap Interference Channels

Ashkan Kalantari*, Sina Maleki*, Gan Zheng† *, Symeon Chatzinotas*, and Björn Ottersten*
*SnT, University of Luxembourg. Emails: {ashkan.kalantari, gan.zheng, bjorn.ottersten}@uni.lu
†School of Computer Science and Electronic Engineering, University of Essex, UK. E-mail: ganzheng@essex.ac.uk

***Abstract*—Interference usually is an adverse phenomenon in wireless networks. However, the interference can potentially be used to boost the secrecy rate in wireless interference channels. This work studies the secrecy rate in a two-user interference network where unintended user may overhear one of the users, namely user 1. User 1 tunes its transmission power in order to maximize its secrecy rate as well as to maintain the quality of service at the other user's destination, user 2, while both user's power limits are considered. It is demonstrated that achieving a positive secrecy rate for user 1 only depends on the channel conditions and user 2's transmission power. Consequently, depending on the channel conditions, the exact threshold for user 2's transmission power which leads to a positive secrecy rate for user 1 is derived.**

Keywords*—Physical-layer security, wireless interference channel, power control, secrecy rate.

I. Introduction

Sending information through wireless channels is a common way to communicate in networks. However, transmitting information over the same frequency band results in interference among users. Furthermore, more and more frequency bands are allocated to wireless communication technology which makes the spectrum scarce. As a solution, the spectrum can be shared which in turn results in interference. For instance, standards such as WiFi, Zigbee and Bluetooth that transmit information over the same frequency band, known as the industrial, scientific and medical (ISM) band, may interfere with each other [1]. In addition, wireless transmission exposes data to wiretappers. Here, "wiretapper", or "eavesdropper" indicate the unintended users. By employing physical layer security techniques, a specific secure rate using a proper coding schemes [2] can be defined for a user. As a result, the unintended agents can be prevented from overhearing the information [3].

The physical layer security in the interference channel to provide perfect secure transmission has recently attracted some attention. The authors of [4] consider a two-user interference channel with an external eavesdropper. It is shown that the structured transmission based on information theory security leads to a higher secrecy rate compared to randomly generated Gaussian codebooks. In [5], noise injection along with data and joint codebook design is investigated in order to enhance the secrecy capacity region in a two-user interference channel, while an external wiretapper is present. In [6], the secrecy capacity region for Gaussian and discrete memoryless channels is investigated in a two-user network with an external eavesdropper. One user, receives constructive interference from the other user to improve its security.

A. Contributions and main results

We study achieving a positive secrecy rate in a two-user wireless interference network in the presence of an unintended user. Users transmit in a manner to maximize the secrecy rate of the first user, user 1, and sustain the quality of service (QoS) at the destination of the second user, user 2. Here, the eavesdropper only tries to wiretap user 1.

As shall be shown later, the motivations for user 2 to cooperate can be justified as: 1) sometimes user 1 cannot achieve a positive secrecy rate and stops its transmission. As a result, user 2 can enjoy an interference-free transmission, 2) user 2 tunes its transmission power so that the QoS at user 2's destination is held equal or above the threshold. We demonstrate that user 2's transmission power as well as the channel conditions are the only parameters which define the feasibility of a positive secrecy rate for user 1. Based on the channel conditions, the amount of transmission power for the second user is specified to preserve a positive secrecy rate for user 1.

B. Related Work

The secrecy capacity in a two-user interference network is investigated in [7]–[11]. The authors of [12] study the secrecy capacity when a number of nodes are employed to suppress eavesdropping by intentional interference. Beamforming weights of antennas are jointly designed for a two-user interference network in [13] in order to enhance the secrecy rate. Further, the concept of interference exploitation to improve the secrecy is also investigated in cognitive radio networks. In [14], the secrecy rate is optimized for a multiple-antenna secondary user in the presence of a wiretapper while sustaining the QoS at the primary receiver. A scenario where the primary user tries to increase its secrecy rate by getting help from the secondary user is considered in [15]. The achievable rate region for both primary and secondary users is derived when secondary user causes interference to both primary and eavesdropper. A network comprised of single-antenna nodes is considered in [16] where a transceiver pair need to keep the transmission secret from an eavesdropper. Game theory is used to analyze the interaction between this pair and other nodes which act as cooperative jammers. Nodes which cooperate as jammers are permitted to use a part of the primary user's spectrum in exchange of the jamming service that they have provided.

The underlaying problem formulation in the mentioned works is different from the one in our work. Also, none of these papers provide an exact analytical insight in the required feasibility conditions in order to achieve a positive secrecy rate in a wiretap interference channel network.

The rest of the paper is organized as follows. The network structure and signal model are introduced in Section II. In Section III, the optimization problem is defined and the feasibility of a positive secrecy rate is investigated. Numerical results are presented in Section IV, and Section V concludes our paper.

II. System Model

A. Signal Model

A wireless interference model comprised of two users denoted by U_1 and U_2, two destinations denoted by D_1 and D_2, and one user as a potential eavesdropper denoted by E is considered. All nodes are considered to be equipped with one antenna. The same frequency band is used by U_1 and U_2 to send data to their corresponding destinations, D_1 and D_2, respectively. Using the same frequency band by the users leads to cross-interference. The network model is depicted in Fig. 1. The wiretapper, E, overhears the users. In our model, E can only decode the signal transmitted by U_1, and thus is not able to decode U_2's signal. Hence, x_2 is the signal which generates interference on both D_1 and E.

In the considered network, U_1 requires maintaining a positive secrecy rate, so the fair procedure would be that U_1 affords all the computational and transmission cost for calculating and distributing the optimal transmission powers. The intended destinations as well as the eavesdropper send pilots to the transmitters which enables them to estimate the required CSIs. Then, U_2 forwards the estimated CSIs to U_1. U_1 uses the estimated CSIs received from U_2 as well as the CSIs estimated by itself to derive the optimal values for the users' transmission powers. Consequently, U_2 receives the value of its optimal transmission power from U_1. When the eavesdropper is completely passive, it is difficult to get its CSI. However, in our scenario, as the eavesdropper is an unintended user which is part of the network of U_1, its channel can be estimated by receiving pilots during the estimation period.

The received signals by D_1 and D_2 are as follows

$$y_{D_1} = \sqrt{P_1} h_{U_1,D_1} x_1 + \sqrt{P_2} h_{U_2,D_1} x_2 + n_{D_1}, \tag{1}$$
$$y_{D_2} = \sqrt{P_2} h_{U_2,D_2} x_2 + \sqrt{P_1} h_{U_1,D_2} x_1 + n_{D_2}, \tag{2}$$

where P_1 and P_2 are the power of the transmitted signals by U_1 and U_2, and h_{U_i,D_j} is the channel gain from each user to the corresponding destination for $i = 1, 2$ and $j = 1, 2$. $\sqrt{P_i}x_i$ and n_{D_i} are the transmit signal from the i-th user, and the additive white Gaussian noise at the i-th destination for $i = 1, 2$, respectively. The random variables x_i and n_{D_i} are independent and identically distributed (i.i.d.) with $x_i \sim \mathcal{CN}(0, 1)$ and $n_{D_i} \sim \mathcal{CN}(0, \sigma_n^2)$, respectively. The overheard signal by E is given by

$$y_E = \sqrt{P_1} h_{U_1,E} x_1 + \sqrt{P_2} h_{U_2,E} x_2 + n_E, \tag{3}$$

where $h_{U_i,E}$ is the channel coefficient from the i-th user to the eavesdropper for $i = 1, 2$, and n_E is the additive white Gaussian noise at the eavesdropper with the same distribution as n_{D_i}. The additive white Gaussian noise at different receivers are assumed to be mutually independent.

B. Users' transmission rates

The transmission rate for each user to the corresponding destination is derived using (1) and (2) as

$$R_{U_1-D_1} = \log_2\left(1 + \frac{P_1 |h_{U_1,D_1}|^2}{P_2 |h_{U_2,D_1}|^2 + \sigma_n^2}\right), \tag{4}$$

$$R_{U_2-D_2} = \log_2\left(1 + \frac{P_2 |h_{U_2,D_2}|^2}{P_1 |h_{U_1,D_2}|^2 + \sigma_n^2}\right). \tag{5}$$

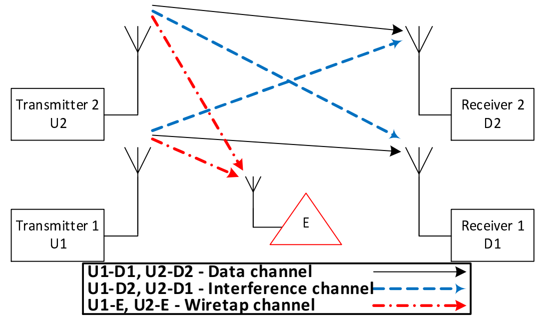

Fig. 1: Two-user wireless interference network.

C. Eavesdropper's reception rate

Since the eavesdropper is part of the U_1's network, its receiver is similar to the one for the other users of the network. As a result, similar to the works [7], [12], [17], [18], it is assumed that the eavesdropper is not capable of decoding and thus canceling the U_2's signal; hence, the instantaneous reception rate from U_1 toward E is obtained as

$$R_{U_1-E} = \log_2\left(1 + \frac{P_1 |h_{U_1,E}|^2}{P_2 |h_{U_2,E}|^2 + \sigma_n^2}\right). \tag{6}$$

The optimization problem to maximize U_1's secrecy rate is defined in the next section. Furthermore, the conditions in order to achieve a positive secrecy rate for U_1 are also studied there.

III. Problem Formulation

In this section, an optimization problem is defined in order to maximize U_1's secrecy rate subject to the peak power limits of the users as well as the quality of service (QoS) at D_2. Furthermore, according to the channel CSIs, we derive the required condition on U_2's transmission power in order to guarantee a positive secrecy rate for U_1.

As a metric to measure the number of bits which can be transmitted securely by U_1, we obtain the secrecy rate as [3],

$$R_S = \max_x \left[R_{U_1-D_1} - R_{U_1-E}\right]^+ \tag{7}$$

where $[\cdot]^+ \triangleq \max(\cdot, 0)$ and x is the message bearing signal. It is shown in [6], [8], [19] that using an input with Gaussian distribution maximizes the mutual information between a transmitter and the corresponding receiver in a one-sided interference channel. For the sake of simplicity, we drop the operator $[\cdot]^+$ in rest of the paper. Employing the secrecy rate in (7) and considering the peak power limits of the users and the QoS at D_2, optimal P_1 and P_2 can be obtained by solving the following optimization problem

$$\begin{aligned} \max_{P_1,P_2} \quad & R_S \\ \text{s.t.} \quad & P_1 \le P_{\max_1}, \\ & P_2 \le P_{\max_2}, \\ & R_{U_2-D_2} \ge \beta, \end{aligned} \tag{8}$$

where β is the minimum data rate for U_2. Inserting (4), (5) and (6) in (8), and considering the fact that log is a monotonic increasing function of its argument, we obtain

$$\begin{aligned}
\max_{P_1,P_2} \quad & \frac{1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}}{1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}} \\
\text{s.t.} \quad & P_1 \le P_{\max_1}, \\
& P_2 \le P_{\max_2}, \\
& \frac{P_2|h_{U_2,D_2}|^2}{P_1|h_{U_1,D_2}|^2+\sigma_n^2} \ge \gamma.
\end{aligned} \tag{9}$$

where γ is $2^\beta - 1$.

To derive the necessary condition on U_2's transmission power in order to achieve a positive secrecy rate for U_1, we try to optimize P_1 for a given P_2 in (9). For this case, (9) is reduced to

$$\begin{aligned}
\max_{P_1} \quad & \frac{1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}}{1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}} \\
\text{s.t.} \quad & P_1 \le P_{\max_1}, \\
& P_1 \le \frac{P_2|h_{U_2,D_2}|^2-\gamma\sigma_n^2}{\gamma|h_{U_1,D_2}|^2}.
\end{aligned} \tag{10}$$

In Theorem 1, the bounds on P_2 to preserve a positive secrecy rate for U_1 are obtained.

Theorem 1: In order to achieve a positive secrecy rate for user 1, i.e., having a grater or equal to one objective in (10), P_2 should satisfy the following bounds:

$$P_2 > \frac{A}{B} \qquad \text{if} \qquad A>0, B>0, \tag{11a}$$

$$P_2 > 0 \qquad \text{if} \qquad A<0, B>0, \tag{11b}$$

$$P_2 < \frac{A}{B} \qquad \text{if} \qquad A<0, B<0, \tag{11c}$$

where $A = \sigma_n^2\left(|h_{U_1,E}|^2 - |h_{U_1,D_1}|^2\right)$ and $B = |h_{U_1,D_1}|^2|h_{U_2,E}|^2 - |h_{U_2,D_1}|^2|h_{U_1,E}|^2$. Note that beside each condition above, it is assumed that the QoS at the destination of U_2 is feasible, i.e., $P_2 \ge \frac{\gamma\sigma_n^2}{|h_{U_2,D_2}|^2}$. Further, for $A>0, B<0$, irrespective of the value of P_2, no positive secrecy rate can be obtained for U_1.

Proof: For the objective function in (10) to be greater or equal to one, the following condition must hold

$$\begin{aligned}
& \log_2\left(1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}\right) \\
& -\log_2\left(1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}\right) > 0 \\
& \Rightarrow \frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2} > \frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2} \\
& \Rightarrow \begin{cases} P_2 > \frac{\sigma_n^2\left(|h_{U_1,E}|^2-|h_{U_1,D_1}|^2\right)}{B} & B>0 \\ P_2 < \frac{\sigma_n^2\left(|h_{U_1,E}|^2-|h_{U_1,D_1}|^2\right)}{B} & B<0 \end{cases}
\end{aligned} \tag{12}$$

where $B = |h_{U_1,D_1}|^2|h_{U_2,E}|^2 - |h_{U_2,D_1}|^2|h_{U_1,E}|^2$. ■

One explicit result of Theorem 1 is given in Corollary 3.1.

Corollary 3.1: In a wiretap interference channel as mentioned in Theorem 1, the possibility of achieving a positive secrecy rate for user 1 is independent from user 1's transmitting power, P_1, and only depends on the channel conditions as well as the value of P_2.

In Theorem 1, A shows the difference between U_1's data and wiretap channel gains. To clarify, B can be rewritten as $B = \frac{|h_{U_1,D_1}|^2}{|h_{U_1,E}|^2} - \frac{|h_{U_2,D_1}|^2}{|h_{U_2,E}|^2} = B_1 - B_2$. The new form of B compares U_1's self channel to its wiretap channel gain ratio, B_1, with respect to U_2's cross channel toward U_1 to U_2's cross channel toward eavesdropper gain ratio, B_2. We name the former ratio as the "security ratio", and the latter as the "security interference ratio". For a constant security interference ratio, a higher secrecy ratio enhances the secrecy rate. On the other hand, given a constant security ratio, a higher security interference ratio yields a lower secrecy rate. Results of Theorem 1 can be summarized as follows

1) When U_1's wiretap channel gain is higher than its own channel gain, but the security ratio is higher than the security interference ratio, U_2 can grant a positive secrecy rate to U_1 by a transmission power higher than $\frac{A}{B}$. In other words, the interference from U_2 on E can compensate for U_1's weak data channel gain and grant a positive secrecy rate to U_1.
2) If U_1's wiretap channel gain is higher than its data channel gain, but the security ratio is lower than the security interference ratio, any transmitting power by U_2 is not capable of providing U_1 with a positive secrecy rate. This implies that the interference from U_2 on E cannot contribute to U_1's secrecy rate. Consequently, U_1 is better not to transmit.
3) When U_1's data channel gain is higher than its wiretap channel gain, and the security ratio is higher than the security interference ratio, U_1 can obtain a positive secrecy rate with any transmission power from U_2. In other words, since U_1 has already a positive secrecy rate, and the security ratio is higher than the security interference ratio, any transmission power from U_2 results in a positive secrecy rate.
4) If U_1's data channel gain is higher than its wiretap channel gain but the security ratio is lower than the security interference ratio, U_2 can provide U_1 with a positive secrecy rate by a transmitting power less than $\frac{A}{B}$.

IV. Numerical Results

In this section, we present different scenarios for numerical evaluations. As a benchmark, we consider a single-user scenario where only one user is present in an interference-free environment [3]. In all simulation scenarios, we assume that the noise power is equal to one, i.e., $\sigma_n^2 = 1$. All the the channel coefficients are modeled as i.i.d. complex normal random variables with real and imaginary parts following a distribution as $\mathcal{N}(0,1)$. The channel coefficients are normalized to have a unit variance as $\mathcal{CN}(0,1)$.

In Fig. 2, different cases of Theorem 1 are verified with respect to the maximum available power of the first user, $P_{\max_1}$, using separate random channel generations. Examples for the Case 11a and Case 11c of Theorem (1) are plotted for two different values of the maximum available power to the second user, $P_{\max_2}$. As we can see in Fig. 2, a slight deviation from the power thresholds of U_2 obtained in Theorem 1 leads to a negative secrecy rate.

Different cases of Theorem 1 are plotted in Fig. 3 with respect to the mximum available power for user 2, $P_{\max_2}$, in order to further

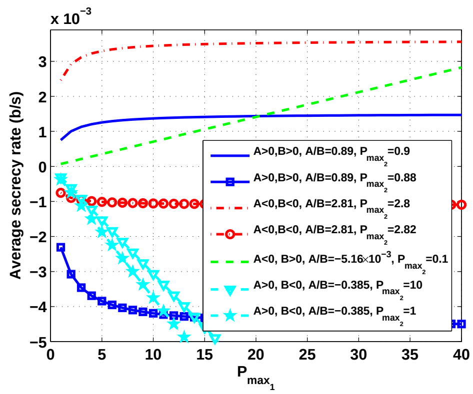

Fig. 2: Examples of Theorem 1 when $P_{\max_1}$ is variable.

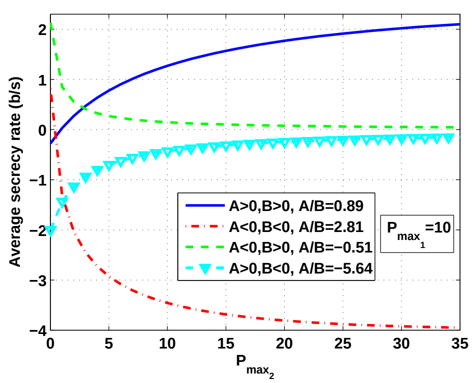

Fig. 3: Examples of Theorem 1 when $P_{\max_2}$ is variable.

investigate the results of Theorem 1. For the curve related to the Case 11a of Theorem (1), it is seen as $P_{\max_2}$ passes the defined power threshold, the value of the secrecy rate moves from a negative one to a positive one. On the contrary, for the curve related to the Case 11c of Theorem (1), when $P_{\max_2}$ passes the defined power threshold, the secrecy rate deteriorates and becomes negative. Finally, we see that for the Case 11b of Theorem (1), the positive secrecy rate can be maintained for all the transmit powers from U_2.

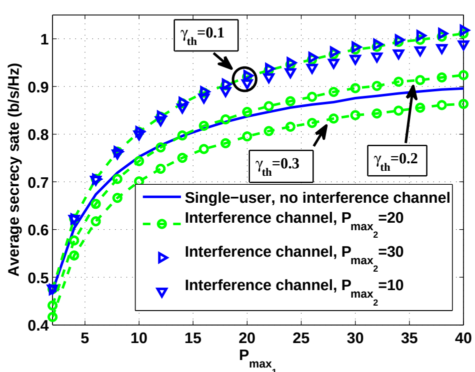

Fig. 4: Average secrecy rate versus $P_{\max_1}$.

The comparison of the secrecy rate in the single-user benchmark and the interference channel scenarios is presented in Fig. 4 with respect to the maximum available power of the first user. Note that to solve (8) analytically, we follow the algorithms provided in [20]. Following points can be implied from Fig. 4:

1) According to the required SINR at D_2, the secrecy rate of the interference channel can be higher or lower than the one of the single-user case. When the data channel is stronger than the wiretap channel in the single-user case, the user can transmit with the maximum available power. On the other hand, U_1 is not able to transmit with the maximum available power in the interference channel since it has to take care of the QoS at D_2.
2) When the required SINR at D_2, γ_{th}, falls below a specific level, the performance of the interference channel becomes better than the single-user case. Because the interference from U_1 decreases the QoS at D_2, U_1 cannot transmit with the maximum available power. On the other hand, as the QoS constraint limit, γ_{th}, decreases, U_1 can transmit with a higher power. In other words, U_1 takes advantage of the interference form U_2 and transmits with a higher power. As a result, with lower power consumption, the secrecy rate in the interference channel is superior to the one of the single-user case.
3) Increasing $P_{\max_2}$ enhances the average secrecy rate much less compared to increasing the $P_{\max_1}$. By increasing $P_{\max_2}$, U_2 creates more interference not only on E, but also on D_1.

V. Conclusion

The role of interference on enhancing the secrecy rate in a two-user wireless interference network was studied in this paper. The appropriate range of transmission power for the interfering user, namely user 2, in order to obtain a positive secrecy rate for the other user, namely user 1, was determined according to the channel qualities. We showed that below a specific required QoS at the destination of user 2, the secrecy rate in the interference channel becomes higher than the one in the single-user case.

Considering the case where a multiple-antenna eavesdropper can perform joint decoding and get access to messages of both users is the subject of the future work.

References

[1] C. Chiasserini and R. Rao, "Coexistence mechanisms for interference mitigation in the 2.4-GHz ISM band," *IEEE Trans. Wireless Commun.*, vol. 2, no. 5, pp. 964–975, Sept. 2003.

[2] Physical layer wireless security. Seventh framework programme (FP7). [Online]. Available: http://www.phylaws-ict.org

[3] A. D. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[4] S. Agrawal and S. Vishwanath, "On the secrecy rate of interference networks using structured codes," in *IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, Jun. 2009, pp. 2091–2095.

[5] O. Koyluoglu and H. El-Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sept. 2011.

[6] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[7] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[8] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, Jul. 2008, pp. 379–383.

[9] X. He and A. Yener, "A new outer bound for the gaussian interference channel with confidential messages," in *43rd Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, Maryland, Mar. 2009, pp. 318–323.

[10] J. Xie and S. Ulukus, "Secrecy games on the one-sided interference channel," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, St. Petersburg, Russia, Jul. 2011, pp. 1245–1249.

[11] S. Bross, Y. Steinberg, and S. Tinguely, "The discrete memoryless interference channel with one-sided generalized feedback," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4171–4191, Jul. 2013.

[12] A. Rabbachin, A. Conti, and M. Win, "Intentional network interference for denial of wireless eavesdropping," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Houston, Texas, Dec. 2011, pp. 1–6.

[13] J. Ni, K.-K. Wong, Z. Fei, C. Xing, H. Chen, K.-F. Tong, and J. Kuang, "Secrecy-rate balancing for two-user MISO interference channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 1, pp. 6–9, Feb. 2014.

[14] Y. Pei, Y.-C. Liang, L. Zhang, K. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[15] Y. Wu and K. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sept. 2011.

[16] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[17] E. Jorswieck and E. Larsson, "The MISO interference channel from a game-theoretic perspective: A combination of selfishness and altruism achieves pareto optimality," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Las Vegas, Nevada, Apr.-Mar. 2008, pp. 5364–5367.

[18] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 885–887, Oct. 2010.

[19] S. A. A. Fakoorian and A. L. Swindlehurst, "Competing for secrecy in the MISO interference channel," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 170–181, Jan. 2013.

[20] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten. (2014, Mar.) Joint power control in wiretap interference channels. [Online]. Available: http://arxiv.org/abs/1403.2079