

Joint Power Control in Wiretap Interference Channels

Ashkan Kalantari *Student Member, IEEE*, Sina Maleki *Member, IEEE*,
Gan Zheng *Senior Member, IEEE*, Symeon Chatzinotas *Senior Member, IEEE*,
and Björn Ottersten, *Fellow, IEEE*

Abstract—Interference in wireless networks degrades the signal quality at the terminals. However, it can potentially enhance the secrecy rate. This paper investigates the secrecy rate in a two-user interference network where one of the users, namely user 1, requires to establish a confidential connection. User 1 wants to prevent an unintended user of the network to decode its transmission. User 1 has to transmit such that its secrecy rate is maximized while the quality of service at the destination of the other user, user 2, is satisfied, and both user's power limits are taken into account. We consider two scenarios: 1) user 2 changes its power in favor of user 1, an altruistic scenario, 2) user 2 is selfish and only aims to maintain the minimum quality of service at its destination, an egoistic scenario. It is shown that there is a threshold for user 2's transmission power that only below or above which, depending on the channel qualities, user 1 can achieve a positive secrecy rate. Closed-form solutions are obtained in order to perform joint optimal power control. Further, a new metric called secrecy energy efficiency is introduced. We show that in general, the secrecy energy efficiency of user 1 in an interference channel scenario is higher than that of an interference-free channel.

Index Terms—Physical-layer security, interference channel, power control, secrecy rate, secrecy energy efficiency.

I. INTRODUCTION

Broadcasting information over the same frequency band in wireless networks leads to interference among users. Even in the systems where the spatial dimension is used to concentrate the signal towards the intended destination, the destination may receive interfering signals from other transmitters operating in the same frequency band. Also, due to the expansion and deployment of wireless services, the spectrum is getting scarce [1]. As one possible solution, devices can share the same spectrum which results in interference and degradation of the signal quality. For instance, IEEE standards such as WiFi, Zigbee and Bluetooth share the same frequency band named the industrial, scientific and medical (ISM) band and they may interfere with each other [2]. Furthermore, the wireless medium leaves the information vulnerable to unintended users who can potentially decode the message which was meant for other users. Throughout this paper, the words “wiretapper”, or “eavesdropper” refer to the unintended users. While there are higher layer cryptography techniques to secure the data, it is

yet possible that a malicious agent breaks into the encryption and gets access to the data [3]. By intelligently tuning the system parameters using physical layer security techniques, we can prevent the wiretappers from getting access to the information and this way, and further improve the system security along other techniques. Consequently, a specific rate can be perfectly secured for the users to transmit their data, so that the wiretapper is not able to decode the message. There are efficient coding schemes which can achieve this rate. However, this area is still in its infancy, and the research effort at the moment is inclined in implementing practical codes [4].

Potentially, the interference can improve the secrecy rate by introducing extra interference at the eavesdropper. The possibility of secure transmission in a multi-user interference channel using interference alignment and secrecy pre-coding is investigated in [5]. The authors of [6] investigate the secrecy rate in a two-user interference channel with an external eavesdropper. They show structured transmission results in a better secrecy rate compared to randomly generated Gaussian codebooks. The authors of [7] study the secrecy capacity region for a two-user interference channel in the presence of an external eavesdropper. The users jointly design randomized codebooks and inject noise along with data transmission to improve the secrecy rate. The authors of [8] consider a user who gets helping interference in order to increase its confidentiality against an eavesdropper. The achievable secrecy rate for both discrete memoryless and Gaussian channels is derived. A two-user interference network with an unintended user is considered in [9]. Depending on the channel conditions, bounds on the transmission power of the interfering user is derived such that a positive secrecy rate is sustained for the other user.

As an example of the interference channel, the effect of interference on the secrecy rate is also investigated in cognitive radio systems. In cognitive radios, secondary user transmits in the primary user's operating frequency band when it is not in use. Stochastic geometry is used in [10] to analyze physical layer secrecy in a multiple node cognitive radio network where an eavesdropper is present. The secrecy outage probability and the secrecy rate of the primary user is derived while secondary user produces interference. The authors of [11] maximize the secrecy rate for a multiple-antenna secondary user in the presence of an external eavesdropper while considering the quality of service (QoS) at the primary receiver. Similar problems to maximize the secrecy rate through beamforming design in cognitive radio are studied in [12]–[14].

This work is supported by national Luxembourg projects AFR reference 5798109 and SeMIGod. Ashkan Kalantari, Sina Maleki, Symeon Chatzinotas and Björn Ottersten are with SnT, The University of Luxembourg, Luxembourg (E-mail: ashkan.kalantari, sina.maleki, symeon.chatzinotas, and bjorn.ottersten@uni.lu). Gan Zheng is with University of Essex, UK, (E-mail: ganzheng@essex.ac.uk). He is also affiliated with SnT.

A. Contributions and main results

In this work, we investigate the secrecy rate in a two-user wireless interference network. Apart from the two users, one of the idle users (unintended user) in this network is a potential eavesdropper. Both nodes transmit in a way so that the secrecy rate is maximized for the first user (user 1), and the second user (user 2) maintains the QoS at its intended destination. Only user 1 needs to establish a secure connection and to keep its data secure. For example, in a network with ISM band users, user 1 and user 2 can be WiFi and ZigBee transmitters. The ZigBee can be used to send measurement data, which is one of its applications, so its data may not be necessarily important to the potential eavesdropper who is interested in WiFi messages.

We study the effect of interference from user 2 on the secrecy rate of user 1 in two scenarios, namely altruistic and egoistic scenarios. In the altruistic scenario, we jointly optimize the transmission powers of both users in order to maximize the secrecy rate of user 1, while maintaining the QoS at user 2's destination equal or above a specific threshold. The incentives for user 2 to cooperate are twofold: 1) when positive secrecy rate cannot be granted for user 1, it can enjoy an interference-free transmission, 2) user 1 adjusts its transmission power to maintain the QoS of user 2's destination equal or above the threshold. In the egoistic scenario, the users' powers are still jointly optimized. However, user 2 is selfish and only tries to maintain the minimum QoS at the corresponding destination. The contributions of our work are as follows. It is shown that by appropriate control of user 1's power, we can make sure that the eavesdropper cannot decode the signal of user 2, and thus cannot employ successive interference cancellation (SIC). Also, it is shown that the transmitted power from user 2 has a crucial role in achieving a positive secrecy rate for user 1. According to the channel conditions, we define the proper power transmission for user 2 to maintain a positive secrecy rate for user 1. We develop closed-form expressions to implement joint optimal power control for both users in both altruistic and egoistic scenarios. Finally, a new metric called "secrecy energy efficiency" is defined, which is the secrecy rate over the consumed power ratio. Using the new metric, it is shown that the interference channel can outperform the single-user channel for specific values of QoS requirements.

B. Related Work

Inner and outer bounds for the secrecy capacity regions in a two-user interference channel with destinations as eavesdroppers are investigated in [15]. They showed that the secrecy capacity can be enhanced when one user transmits signal with artificial noise. Later, [15] was extended to the case when both users transmit artificial noise along with data in [16]. As a result, they achieve a larger secrecy rate region when one or both destinations are considered as eavesdropper. In [17], an outer bound for secrecy capacity region is calculated for a two-user one-sided interference channel. Outer bounds on sum rate of a two-user Gaussian interference channel are studied in [18] where message confidentiality is important for users. Secrecy capacity region for a two-user MIMO Gaussian interference channel is investigated in [19] where

each receiver is a potential eavesdropper. A two-user symmetric linear deterministic interference channel is investigated in [20]. The achievable secrecy rate is investigated when interference cancelation, cooperation, time sharing, and transmission of random bits are used. It is shown that sharing random bits achieves a better secrecy rate compared to sharing data bits. A two-user MISO interference channel is considered in [21] where beamforming is performed to maintain fair secrecy rate. The work in [22] analyzes a two-user interference channel with one-sided noisy feedback. Rate-equivocation region is derived when the second user's message needs to be kept secret. The secrecy rate constrained to secrecy rate outage probability and power is maximized by designing robust beamformer in [23] where a transceiver pair and multiple eavesdroppers constitute a network.

A multiple-user interference channel where only one user as a potential eavesdropper receives interference is considered in [24]. The sum secrecy rate is derived using nested lattice codes. The authors in [25] consider a wireless network comprised of users, eavesdroppers and interfering nodes. It is shown that interference can improve secrecy rate. A communication network comprised of multiple-antenna base stations and single-antenna users is considered in [26]. The total transmit power is minimized while the signal-to-interference plus noise ratio and equivocation rate for each user is satisfied.

In [27], a two-user network with one-sided-interference where each destination is a potential eavesdropper for the other one is studied. Using game theory, it is concluded that depending on the objective of each pair, the equilibrium can include or exclude the self-jamming strategy. The authors of [28] analyze a two-user MISO Gaussian interference channel where each destination is a potential eavesdropper. Game theory is used to tackle the scenario where each user tries to maximize the difference between its secrecy rate and the secrecy rate of the other user. Beamformers under full and limited channel information are designed at each transmitter to achieve this goal.

A transceiver pair is studied in [29] where they try to increase the secrecy rate using an external interferer when a passive eavesdropper is present. The authors of [30] consider a user and an eavesdropper where known interference which only degrades the decoding ability at the eavesdropper is used to enhance the secrecy capacity. The secrecy capacity and secrecy outage capacity when closest interfering node and multiple interfering nodes are separately employed to prevent eavesdropping is studied in [31]. It is demonstrated that multiple interferes method is superior to the closet interfering method. The exact secure degrees of freedom for different types of Gaussian wiretap channels are discussed in [32] where cooperative jamming from helpers is used.

The equivocation-rate for a cognitive interference network is considered in [33] where the primary receiver is a potential eavesdropper and should not decode the secondary message. A MISO transceiver along with multiple single-antenna eavesdroppers are considered in [34]. The relationship of the mentioned network with interference cognitive radio network is used to design the transmit covariance matrix. In [35], the secondary user causes interferes to both primary

destination and eavesdropper. Primary user tries to maintain its secrecy rate while the secondary aims to increase its rate. The achievable pair rate for both users is derived.

C. Paper Organization

The remainder of the paper is organized as follows. In Section II, we introduce the network topology as well as the signal model. The optimization problems for the altruistic and egoistic scenarios are defined and analyzed in Section III and Section IV, respectively. In Section VI, we evaluate the optimal achievable secrecy rate and compare the two-user wiretap interference channel scheme with the single-user wiretap channel as the benchmark. Finally, the conclusions are drawn in Section VII.

D. Notation

$A \stackrel{(1)}{\geq} 0$ means that $A > 0$ when the conditions of Case 1 hold and $A < 0$ when the conditions of Case 2 hold. $|\cdot|$ represents the absolute value.

II. SYSTEM MODEL

A. Signal Model

We consider a wireless interference network consisting of two users denoted by U_1 and U_2 , two destinations denoted by D_1 and D_2 , and one user as the eavesdropper denoted by E . E is assumed to be passive during U_1 and U_2 transmission and active outside the mentioned period. All nodes employ one antenna for data communication. We denote by x_1 and x_2 , the messages which are sent over the same frequency band from U_1 and U_2 to D_1 and D_2 , respectively. Sharing the same frequency band by the users leads to cross-interference. While the users send data, their signals are wiretapped by the eavesdropper, E . The network setup is depicted in Fig. 1. Here, we consider a scenario where E is only interested in the data sent by one of the users, namely U_1 . As a result, x_2 is considered as an interfering signal at both D_1 and E .

There are two ways in order to carry out the joint power allocation: 1) users send their channel information to a fusion center. At the fusion center, the optimal power values are calculated and sent back to the users separately, 2) one of the users sends its channel information to the other user who calculates the optimal power values and sends the optimal power value to the corresponding user. It can be seen that the first approach consumes more time and number of transmissions compared to the second one. Since U_1 is interested in sustaining a positive secrecy rate, it is fair if this user pays the computational cost. Hence, we assume that U_2 sends the channels data to U_1 and then U_1 calculates the optimal power values and sends back the related optimal power value to U_2 . To perform channel estimation in the network, one approach is that the destinations, including the unintended user, send pilots and the transmitters are then able to estimate the required CSIs. After estimating the channels, U_2 forwards the required CSIs to U_1 . U_1 is then responsible to perform the power control and inform U_2 of the optimal power that it can

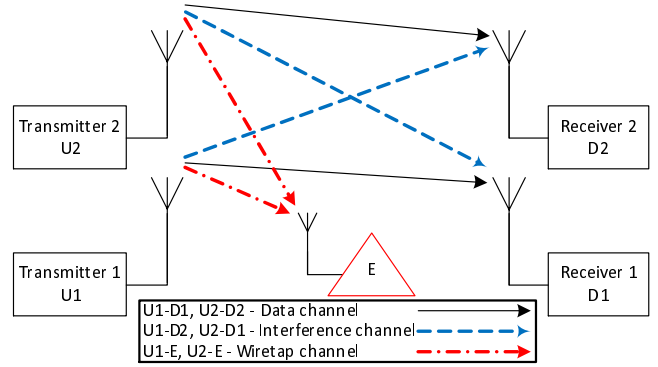


Fig. 1: Two-user wireless interference network.

transmit. Note that in practice, it is often optimistic to have such a model, as the eavesdroppers are often totally passive. But here, we assume that the eavesdropper is momentarily active, and thus its channel can be estimated and remains unchanged for the optimal power control usage. One practical example of such a scenario is when the eavesdropper is a known user in a network such that U_1 's messages should be kept confidential from it.

The received signals at D_1 and D_2 are as follows

$$y_{D_1} = \sqrt{P_1}h_{U_1,D_1}x_1 + \sqrt{P_2}h_{U_2,D_1}x_2 + n_{D_1}, \quad (1)$$

$$y_{D_2} = \sqrt{P_2}h_{U_2,D_2}x_2 + \sqrt{P_1}h_{U_1,D_2}x_1 + n_{D_2}, \quad (2)$$

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 $j = 1, 2$. The transmission signal from the i -th user, and the additive white Gaussian noise at the i -th destination are shown by $\sqrt{P_i}x_i$ and n_{D_i} 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, where \mathcal{CN} denotes the complex normal random variable. In practice, some signals follow Gaussian distribution such as the amplitude of sample distributions of OFDM signal [36]. Using a Gaussian distributed signal may not always be optimal, however, our focus is on maximizing the secrecy rate by designing joint optimal power allocation in a specific system model. The wiretapped signal at E is

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

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. Secrecy rate of U_1

In order to calculate the secrecy rate of U_1 , we need to first find the rate of U_1 without considering the secrecy, and then the rate in which the eavesdropper wiretaps U_1 . In this paper, we assume that U_1 and U_2 do not employ SIC. Therefore, using (1) and (2), the rates for each user to the corresponding

destination can be calculated as

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

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

The eavesdropper simultaneously receives signals from U_1 and U_2 which are transmitting in the same frequency band. Hence, the channel from users towards the eavesdropper can be modeled by a multiple-access channel. Assume that the transmission powers of U_1 and U_2 in a specific time slot are P_1 and P_2 . Then, considering that users employ Gaussian codebooks and the eavesdropper tends to achieve the maximum wiretapping rate from U_1 , the rate pairs achieved at the eavesdropper are shown in Fig. 2 [37] which lie on the line from point “A” to point “D”. To wiretap U_1 with the maximum achievable rate, the eavesdropper can employ the SIC method [38]. Using SIC, the eavesdropper first decodes the signal from U_2 while considering U_1 's signal as interference. Then, considering the fact that the signal from U_2 is decoded and known, eavesdropper deducts U_2 's signal from the received signal and gets an interference-free signal from U_1 . In this approach, the rate pairs on the line “CD” are achieved at the eavesdropper if the transmission rate of U_2 , defined by R_2 , is lower than the decode-able rate defined at point “G”. To prevent the eavesdropper from achieving the maximal wiretapping rate, U_2 's transmission rate needs to be higher than the decode-able rate at point “G”. Since users do not coordinate in order to implement time-sharing or rate-splitting, U_1 's signal cannot be decoded with the rates which are on the line “DE”, and thus it needs to decode U_1 considering U_2 as the interference with a rate equal to the rate at point “E”. Therefore, to disable the eavesdropper from performing SIC (i.e., achieving rate at point “D”), the following condition needs to hold:

$$\begin{aligned} R_2 &= \log_2 \left(1 + \frac{P_2 |h_{U_2,D_2}|^2}{P_1 |h_{U_1,D_2}|^2 + \sigma_n^2} \right) \\ &> \log_2 \left(1 + \frac{P_2 |h_{U_2,E}|^2}{P_1 |h_{U_1,E}|^2 + \sigma_n^2} \right). \end{aligned} \quad (6)$$

In (6), the left-hand side is the actual transmission rate of U_2 which is equal to the decode-able rate at its destination, D_2 . If condition (6) is satisfied, the eavesdropper has to decode U_1 's signal by considering U_2 's signal as interference. Interestingly, satisfying condition (2) just needs U_1 to adjust its transmission power and is independent from P_2 . The condition on P_1 to satisfy (6) is derived as:

$$P_1 > \frac{A''}{B''} \quad \text{if} \quad A'' > 0, B'' > 0, \quad (7a)$$

$$P_1 > 0 \quad \text{if} \quad A'' < 0, B'' > 0, \quad (7b)$$

$$P_1 < \frac{A''}{B''} \quad \text{if} \quad A'' < 0, B'' < 0, \quad (7c)$$

$$P_1 < 0 \text{ (not feasible)} \quad \text{if} \quad A'' > 0, B'' < 0, \quad (7d)$$

where $A'' = \sigma_n^2 (|h_{U_2,E}|^2 - |h_{U_2,D_2}|^2)$ and $B'' = |h_{U_2,D_2}|^2 |h_{U_1,E}|^2 - |h_{U_1,D_2}|^2 |h_{U_2,E}|^2$. As we can see, the

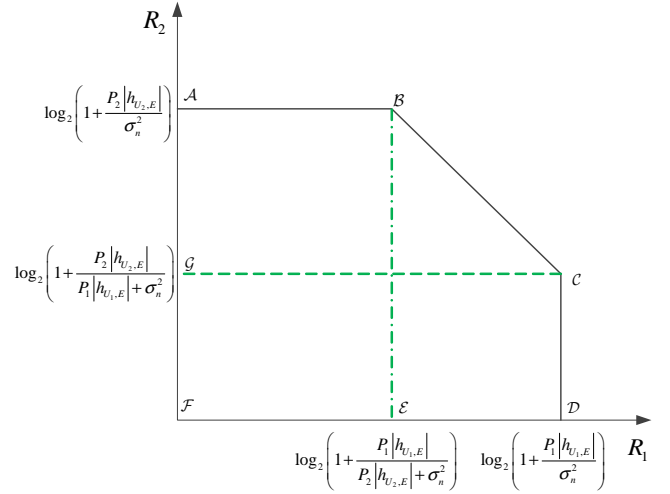


Fig. 2: Maximum achievable rate pairs of a two-user multiple-access fading channel.

channel conditions define whether U_1 can block the eavesdropper by adjusting its power. For the Cases 7a, 7b, and 7c, the instantaneous wiretap rate from U_1 toward E is obtained by $I_{U_1-E} = \log_2 \left(1 + \frac{P_1 |h_{U_1,E}|^2}{P_2 |h_{U_2,E}|^2 + \sigma_n^2} \right)$, and thus the secrecy rate of U_1 in this case is as follows

$$\begin{aligned} C_{S_{U_1}} &= I_{U_1-D_1} - I_{U_1-E} = \log_2 \left(1 + \frac{P_1 |h_{U_1,D_1}|^2}{P_2 |h_{U_2,D_1}|^2 + \sigma_n^2} \right) \\ &\quad - \log_2 \left(1 + \frac{P_1 |h_{U_1,E}|^2}{P_2 |h_{U_2,E}|^2 + \sigma_n^2} \right). \end{aligned} \quad (8)$$

For Case 7d, no power from U_1 is capable of preventing the eavesdropper from applying the SIC technique and deriving an interference-free version of U_1 's signal and thus $I_{U_1-E} = \log_2 \left(1 + \frac{P_1 |h_{U_1,E}|^2}{\sigma_n^2} \right)$. This results in the following secrecy rate

$$\begin{aligned} C_{S_{U_2}} &= I_{U_1-D_1} - I_{U_1-E} = \log_2 \left(1 + \frac{P_1 |h_{U_1,D_1}|^2}{P_2 |h_{U_2,D_1}|^2 + \sigma_n^2} \right) \\ &\quad - \log_2 \left(1 + \frac{P_1 |h_{U_1,E}|^2}{\sigma_n^2} \right). \end{aligned} \quad (9)$$

In the next two sections, we formulate and solve the underlying problems so as to find the optimal P_1 and P_2 .

III. PROBLEM FORMULATION: ALTRUISTIC SCENARIO

In this section, we maximize the secrecy rate of U_1 subject to the peak power limits of the users as well as the quality of service (QoS) at D_2 . If one of the cases 7a, 7b, or 7c holds, using (8), the following secrecy rate optimization is solved:

$$\begin{aligned} &\max_{P_1, P_2} C_{S_{U_1}} \\ &\text{s.t.} \quad P_1 \leq P_{\max,1}, P_1 \underset{(7c)}{\gtrless} \omega, P_2 \leq P_{\max,2}, I_{U_2-D_2} \geq \beta, \end{aligned} \quad (10)$$

where β is the minimum required data rate for U_2 and $\omega = \frac{A''}{B''}$. In Case 7b, any P_1 ensures that the eavesdropper cannot employ SIC. Therefore, no additional constraint over P_1 is necessary. For Case 7d, using (9), the following secrecy rate optimization problem should be solved

$$\begin{aligned} & \max_{P_1, P_2} C_{S_{U_2}} \\ & \text{s. t. } P_1 \leq P_{\max_1}, P_2 \leq P_{\max_2}, I_{U_2-D_2} \geq \beta. \end{aligned} \quad (11)$$

We first solve (10) and then (11). By inserting (8) into (10), we obtain

$$\begin{aligned} & \max_{P_1, P_2} \log_2 \left(\frac{1 + \frac{P_1 |h_{U_1, D_1}|^2}{P_2 |h_{U_2, D_1}|^2 + \sigma_n^2}}{1 + \frac{P_1 |h_{U_1, E}|^2}{P_2 |h_{U_2, E}|^2 + \sigma_n^2}} \right) \\ & \text{s. t. } P_1 \leq P_{\max_1}, P_1 \stackrel{(7a)}{\geq} \omega, P_2 \leq P_{\max_2}, \\ & \quad \frac{P_2 |h_{U_2, D_2}|^2}{P_1 |h_{U_1, D_2}|^2 + \sigma_n^2} \geq \gamma, \end{aligned} \quad (12)$$

where γ is $2^\beta - 1$. Since \log is a monotonic increasing function of its argument, we can just maximize the argument and thus we rewrite (12) as

$$\begin{aligned} & \max_{P_1, P_2} \frac{1 + \frac{P_1 |h_{U_1, D_1}|^2}{P_2 |h_{U_2, D_1}|^2 + \sigma_n^2}}{1 + \frac{P_1 |h_{U_1, E}|^2}{P_2 |h_{U_2, E}|^2 + \sigma_n^2}} \\ & \text{s. t. } P_1 \leq P_{\max_1}, P_1 \stackrel{(7a)}{\geq} \omega, P_2 \leq P_{\max_2}, \\ & \quad \frac{P_2 |h_{U_2, D_2}|^2}{P_1 |h_{U_1, D_2}|^2 + \sigma_n^2} \geq \gamma. \end{aligned} \quad (13)$$

Considering that the objective function is neither convex, nor concave, solving problem (13) is difficult. As a result, we shall adopt a two-step approach in order to solve (13). First, we consider P_2 to be fixed and derive the optimal value for P_1 , and then we replace the obtained P_1 in (13) and solve the optimization problem for P_2 .

A. Optimizing P_1 for a Given P_2

For this case, (13) is reduced to

$$\begin{aligned} & \max_{P_1} \frac{1 + \frac{P_1 |h_{U_1, D_1}|^2}{P_2 |h_{U_2, D_1}|^2 + \sigma_n^2}}{1 + \frac{P_1 |h_{U_1, E}|^2}{P_2 |h_{U_2, E}|^2 + \sigma_n^2}} \\ & \text{s. t. } P_1 \leq P_{\max_1}, P_1 \stackrel{(7a)}{\geq} \omega, P_1 \leq \frac{P_2 |h_{U_2, D_2}|^2 - \gamma \sigma_n^2}{\gamma |h_{U_1, D_2}|^2}. \end{aligned} \quad (14)$$

In order to solve (14), first, we find the range of P_2 for which the objective function in (14) is always positive, i.e., a positive secrecy rate can be achieved. In the following theorem, we outline the related bounds on P_2 where the positive secrecy rate is obtained.

Theorem 1: Assume an interference network similar to the one mentioned in Fig. 1 along with the assumptions on power

limits and the QoS. In order to achieve a positive secrecy rate, P_2 should satisfy the following bounds:

$$P_2 > \frac{A}{B} \quad \text{if } A > 0, B > 0, \quad (15a)$$

$$P_2 > 0 \quad \text{if } A < 0, B > 0, \quad (15b)$$

$$P_2 < \frac{A}{B} \quad \text{if } A < 0, B < 0, \quad (15c)$$

where $A = \sigma_n^2 (|h_{U_1, E}|^2 - |h_{U_1, D_1}|^2)$ and $B = |h_{U_1, D_1}|^2 |h_{U_2, E}|^2 - |h_{U_2, D_1}|^2 |h_{U_1, E}|^2$. Further, for $A > 0, B < 0$, irrespective of the value of P_2 , no positive secrecy rate can be obtained for U_1 .

Proof: The proof is given in Appendix A. ■

One immediate conclusion of Theorem 1 is given by the following corollary which can be considered as the most important result of this paper.

Corollary 3.1: In a wiretap interference channel as in Fig. 1, where the goal is to obtain a positive secrecy rate for U_1 , the possibility of achieving a positive secrecy rate is independent from the value of P_1 , and depends on the value of P_2 and the conditions of the channels.

Now that we have defined the required conditions for P_2 to achieve a positive secrecy rate, we investigate the optimal value of P_1 , denoted by P_1^* for a given P_2 . If we take the derivative of the objective function in (14) with respect to P_1 , we see that the conditions on P_2 to have a monotonically increasing, referred to as Case 1, or decreasing, referred to as Case 2, are the same as the conditions to have a positive or negative secrecy rate, respectively. These conditions are summarized as follows

$$\begin{aligned} P_{2(1)} > \frac{A}{B}, P_{2(2)} < \frac{A}{B} & \quad \text{if } A > 0, B > 0, \\ P_{2(1)} = \emptyset, P_{2(2)} > 0 & \quad \text{if } A > 0, B < 0, \\ P_{2(1)} > 0, P_{2(2)} = \emptyset & \quad \text{if } A < 0, B > 0, \\ P_{2(1)} < \frac{A}{B}, P_{2(2)} > \frac{A}{B} & \quad \text{if } A < 0, B < 0, \end{aligned} \quad (16)$$

where $P_{2(1)}$ refers to the required power in Case 1, $P_{2(2)}$ refers to the required power in Case 2 and \emptyset denotes the empty set. According to Theorem 1, and the conditions in (16), the global optimal values for P_1 in Cases 1 and 2 are defined as

- 1) If the objective function in (10) is monotonically increasing, then

$$P_1^* = \min \left\{ \chi, \frac{P_2 |h_{U_2, D_2}|^2 - \gamma \sigma_n^2}{\gamma |h_{U_1, D_2}|^2} \right\}. \quad (17)$$

where $\chi = P_{\max_1}$ for Cases 7a and 7b, $\chi = \min \{P_{\max_1}, \omega\}$ for Case 7c.

- 2) If the objective function in (10) is monotonically decreasing, then $P_1^* = 0$. This could also be concluded from the fact that when a positive secrecy rate cannot be granted, U_1 should be turned off.

B. Optimizing P_2 for a Given P_1

We insert the P_1^* obtained in Subsection III-A into (14), and try to obtain the optimal value for P_2 . First, we decompose

the optimal answer of P_1 in (17) into two different answers as follows

$$P_1^* = \begin{cases} \chi & P_2 \geq \frac{\gamma(\chi|h_{U_1,D_2}|^2 + \sigma_n^2)}{|h_{U_2,D_2}|^2}, \\ \frac{P_2|h_{U_2,D_2}|^2 - \gamma\sigma_n^2}{\gamma|h_{U_1,D_2}|^2} & P_2 < \frac{\gamma(\chi|h_{U_1,D_2}|^2 + \sigma_n^2)}{|h_{U_2,D_2}|^2}. \end{cases} \quad (18)$$

Using Theorem 1 and according to the two resulting cases in (18), we can break (13) into two problems in order to optimize P_2 , respectively, as follows

$$\begin{aligned} \max_{P_2} & \frac{1 + \frac{P_{\max_1}|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2 + \sigma_n^2}}{1 + \frac{P_{\max_1}|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2 + \sigma_n^2}} \\ \text{s. t. } & P_2 \leq P_{\max_2}, \quad P_2 \geq \frac{\gamma(\chi|h_{U_1,D_2}|^2 + \sigma_n^2)}{|h_{U_2,D_2}|^2} = \lambda_1, \\ & P_2 \stackrel{(15a)}{\geq} \frac{\sigma_n^2(|h_{U_1,E}|^2 - |h_{U_1,D_1}|^2)}{|h_{U_1,D_1}|^2|h_{U_2,E}|^2 - |h_{U_2,D_1}|^2|h_{U_1,E}|^2} = \varphi_1, \\ & P_2 \stackrel{(15c)}{\geq} \frac{\sigma_n^2(|h_{U_1,E}|^2 - |h_{U_1,D_1}|^2)}{|h_{U_1,D_1}|^2|h_{U_2,E}|^2 - |h_{U_2,D_1}|^2|h_{U_1,E}|^2} = \varphi_1, \end{aligned} \quad (19)$$

and

$$\begin{aligned} \max_{P_2} & \frac{1 + \frac{(P_2|h_{U_2,D_2}|^2 - \gamma\sigma_n^2)|h_{U_1,D_1}|^2}{\gamma|h_{U_1,D_2}|^2(P_2|h_{U_2,D_1}|^2 + \sigma_n^2)}}{1 + \frac{(P_2|h_{U_2,D_2}|^2 - \gamma\sigma_n^2)|h_{U_1,E}|^2}{\gamma|h_{U_1,D_2}|^2(P_2|h_{U_2,E}|^2 + \sigma_n^2)}} \\ \text{s. t. } & P_2 \leq P_{\max_2}, \quad P_2 < \frac{\gamma(\chi|h_{U_1,D_2}|^2 + \sigma_n^2)}{|h_{U_2,D_2}|^2} = \lambda_1, \\ & P_2 \geq \frac{\gamma\sigma_n^2}{|h_{U_2,D_2}|^2} = \lambda_2, \\ & P_2 \stackrel{(15a)}{\geq} \frac{\sigma_n^2(|h_{U_1,E}|^2 - |h_{U_1,D_1}|^2)}{|h_{U_1,D_1}|^2|h_{U_2,E}|^2 - |h_{U_2,D_1}|^2|h_{U_1,E}|^2} = \varphi_1, \\ & P_2 \stackrel{(15c)}{\geq} \frac{\sigma_n^2(|h_{U_1,E}|^2 - |h_{U_1,D_1}|^2)}{|h_{U_1,D_1}|^2|h_{U_2,E}|^2 - |h_{U_2,D_1}|^2|h_{U_1,E}|^2} = \varphi_1, \end{aligned} \quad (20)$$

for $A \stackrel{(15a)}{\geq} 0$ and $B \stackrel{(15a)}{\geq} 0$. For the case $A < 0$ and $B > 0$ which is represented by (15b), the last constraint in (19) and (20) is removed from the problem since with any positive value for P_2 , U_1 can have a positive secrecy rate. Also for $A > 0$ and $B < 0$, the secrecy rate is simply zero since $P_1 = 0$. Furthermore, the numerator and denominator in (20) have the possibility to become less than unit and this leads to a negative rate. The constraint in (20) which is placed one to the last, ensures that the data and wiretap rates do not go below zero.

We discuss the feasibility conditions of (19) and (20) to derive the feasibility domain, p_2 , in Proposition 3.2.

Proposition 3.2: The feasibility domain for the problems (19) and (20) denoted by p_2 is defined as follows

- 1) Problem (19): For case (15a), we should have $\max\{\lambda_1, \sup \varphi_1\} \leq P_{\max_2}$ which leads to $p_2 = [\max\{\lambda_1, \sup \varphi_1\}, P_{\max_2}]$. For case (15c), we should have $\min\{\inf \varphi_1, P_{\max_2}\} \geq \lambda_1$ which leads to $p_2 = [\lambda_1, \min\{\inf \varphi_1, P_{\max_2}\}]$.

- 2) Problem (20): For case (15a), we should have $\max\{\sup \varphi_1, \lambda_2\} \leq \min\{\inf \lambda_1, P_{\max_2}\}$ which leads to $[\max\{\sup \varphi_1, \lambda_2\}, \min\{\inf \lambda_1, P_{\max_2}\}]$. For case (15c), we should have $\min\{\inf \varphi_1, \inf \lambda_1, P_{\max_2}\} \geq \lambda_2$ which leads to $p_2 = [\min\{\inf \varphi_1, \inf \lambda_1, P_{\max_2}\}, \lambda_2]$.

Proof: The proof is straightforward, thus was omitted. ■

If both (19) and (20) are feasible at the same time, we select the P_2^* and the corresponding secrecy rate from the problem which results in a higher secrecy rate. Here, we provide a generic closed-form solution depending on the channels' conditions in Theorems 2 and 3 for (19) and (20), respectively.

Theorem 2: Assume $a = P_{\max_1}|h_{U_1,D_1}|^2$, $b = |h_{U_2,D_1}|^2$, $c = P_{\max_1}|h_{U_1,E}|^2$, $d = |h_{U_2,E}|^2$, $C = b - d$, $D = b(c + \sigma_n^2) - d(a + \sigma_n^2)$, $E = -BP_{\max_1} = bc - ad$, $F = cd\sigma_n^2 - a(b(c + \sigma_n^2) - cd)$, $G = \frac{AP_{\max_1}}{\sigma_n^2} = c - a$, $\alpha = \min(\inf \varphi_1, P_{\max_2})$, and $\beta = \max\{\lambda_1, \sup \varphi_1\}$. Also, suppose that (19) is feasible. Then, (19) is solved as follows:

- 1) If $CD < 0$
 - a) If $A < 0$ and $E > 0$

$$P_2^* = \alpha \quad (21)$$

- b) If $E < 0$

$$P_2^* = \begin{cases} \beta & A > 0 \\ \lambda_1 & A < 0 \end{cases} \quad (22)$$

- 2) If $CD > 0$
 - a) If $A < 0$, $E > 0$ and $F < 0$

$$P_2^* = \arg \max_{P_2, P_2 \in \{\lambda_1, \alpha\}} C_s \quad (23)$$

- b) If $E < 0$ and $F > 0$

$$P_2^* = \begin{cases} P_{2C} & P_{2C} \in p_2 \\ \arg \max_{P_2, P_2 \in \{\beta, P_{\max_2}\}} C_s & A > 0, P_{2C} \notin p_2 \\ \arg \max_{P_2, P_2 \in \{\lambda_1, P_{\max_2}\}} C_s & A < 0, P_{2C} \notin p_2 \end{cases} \quad (24)$$

- c) If $E > 0$, $F > 0$ and $G < 0$

$$P_2^* = \begin{cases} \arg \max_{P_2, P_2 \in \{P_{2C}, \lambda_1, \alpha\}} C_s & P_{2C} \in p_2 \\ \arg \max_{P_2, P_2 \in \{\lambda_1, \alpha\}} C_s & P_{2C} \notin p_2 \end{cases} \quad (25)$$

- d) If $E < 0$, $F < 0$ and $G > 0$

$$P_2^* = \begin{cases} \arg \max_{P_2, P_2 \in \{P_{2C}, \beta, P_{\max_2}\}} C_s & P_{2C} \in p_2 \\ \arg \max_{P_2, P_2 \in \{\beta, P_{\max_2}\}} C_s & P_{2C} \notin p_2 \end{cases} \quad (26)$$

- e) If $E < 0$, $F < 0$ and $G < 0$

$$P_2^* = \lambda_1 \quad (27)$$

where C_s is the objective function in (19), $P_{2C} = \frac{-2bdG\sigma_n^2 - \sqrt{\Delta}}{2bdE}$, and $\Delta = 4abcdCD\sigma_n^2$.

Proof: The proof is given in Appendix B. ■

Theorem 3: Assume $e = |h_{U_1,D_1}|^2$, $f = |h_{U_2,D_2}|^2$, $g = |h_{U_1,D_2}|^2$, $h = |h_{U_2,D_1}|^2$, $i = |h_{U_1,E}|^2$,

$$\begin{aligned}
j &= |h_{U_2,E}|^2, H = h - j, \delta = \min(\inf \lambda_1, P_{\max_2}), \\
\kappa &= \min\{\inf \lambda_1, \inf \varphi_1, P_{\max_2}\}, \mu = \max\{\sup \varphi_1, \lambda_2\}, \\
I &= -fi + gh\gamma - (hi + gj)\gamma + e(f + j\gamma), \\
J &= -gh^2i\gamma(f + j\gamma) + e(f^2i(-h + j) + fgj^2\gamma + ghj^2\gamma^2), \\
K &= -gi(f + j\gamma) + e(fg + gh\gamma - hi\gamma + ij\gamma), \\
L &= -ghi(f + j\gamma) + e(fhi + fgj - fij + ghj\gamma).
\end{aligned}$$

Also, suppose that (20) is feasible. Then, (20) can be solved as follows

1) If $HI < 0$

a) If $J > 0$

$$P_2^* = \begin{cases} \delta & A > 0, B > 0 \\ \delta & A < 0, B > 0 \\ \kappa & A < 0, B < 0 \end{cases} \quad (28)$$

b) If $J < 0$

$$P_2^* = \begin{cases} \mu & A > 0, B > 0 \\ \lambda_2 & A < 0, B > 0 \\ \lambda_2 & A < 0, B < 0 \end{cases} \quad (29)$$

2) If $HI > 0$

a) If $J > 0$ and $K < 0$

$$P_2^* = \begin{cases} \arg \max_{P_2 \in \{\mu, \delta\}} C_s & A > 0, B > 0 \\ \arg \max_{P_2 \in \{\lambda_2, \delta\}} C_s & A < 0, B > 0 \\ \arg \max_{P_2 \in \{\lambda_2, \kappa\}} C_s & A < 0, B < 0 \end{cases} \quad (30)$$

b) If $J < 0$ and $K > 0$

$$P_2^* = \begin{cases} P_{2C} & P_{2C} \in p_2 \\ \arg \max_{P_2 \in \{\mu, \delta\}} C_s & A > 0, B > 0, P_{2C} \notin p_2 \\ \arg \max_{P_2 \in \{\lambda_2, \delta\}} C_s & A < 0, B > 0, P_{2C} \notin p_2 \\ \arg \max_{P_2 \in \{\lambda_2, \kappa\}} C_s & A < 0, B < 0, P_{2C} \notin p_2 \end{cases} \quad (31)$$

c) If $J > 0, K > 0$ and $L < 0$ or $J < 0, K < 0$ and $L > 0$

$$P_2^* = \begin{cases} \arg \max_{P_2 \in \{P_{2C}, \mu, \delta\}} C_s & A > 0, B > 0, P_{2C} \in p_2 \\ \arg \max_{P_2 \in \{P_{2C}, \lambda_2, \delta\}} C_s & A < 0, B > 0, P_{2C} \in p_2 \\ \arg \max_{P_2 \in \{P_{2C}, \lambda_2, \kappa\}} C_s & A < 0, B < 0, P_{2C} \in p_2 \\ \arg \max_{P_2 \in \{\mu, \delta\}} C_s & A > 0, B > 0, P_{2C} \notin p_2 \\ \arg \max_{P_2 \in \{\lambda_2, \delta\}} C_s & A < 0, B > 0, P_{2C} \notin p_2 \\ \arg \max_{P_2 \in \{\lambda_2, \kappa\}} C_s & A < 0, B < 0, P_{2C} \notin p_2 \end{cases} \quad (32)$$

d) If $J > 0, K > 0$ and $L > 0$

$$P_2^* = \begin{cases} \delta & A > 0, B > 0 \\ \delta & A < 0, B > 0 \\ \kappa & A < 0, B < 0 \end{cases} \quad (33)$$

e) If $J < 0, K < 0$ and $L < 0$

$$P_2^* = \begin{cases} \mu & A > 0, B > 0 \\ \lambda_2 & A < 0, B > 0 \\ \lambda_2 & A < 0, B < 0 \end{cases} \quad (34)$$

where C_s is the objective function in (20) and $P_{2C} = \frac{-2\sigma_n^2\gamma L - \sqrt{\Delta}}{2J}$, and $\Delta = 4egiHI(\sigma_n^2)^4\gamma(f + h\gamma)(f + j\gamma)$.

Proof: The proof can be obtained in the similar way to that of Theorem 2. ■

For problem (11), the optimal solution of P_1 is as (17) when $\chi = P_{\max_1}$. The closed-form solution for the P_2 is given in the following theorem.

Theorem 4: Assume $a = |h_{U_1,D_1}|^2$, $b = |h_{U_2,D_2}|^2$, $c = |h_{U_1,D_2}|^2$, $d = |h_{U_2,D_1}|^2$, $e = |h_{U_1,E}|^2$, $A = b(a - e)\sigma + d(-e\gamma\sigma + c\gamma\sigma)$, $B = 2bde(a\gamma\sigma - c\gamma\sigma)$, $C = -bce\gamma\sigma^2 + a(bc\gamma\sigma^2 + d\gamma\sigma(-e\gamma\sigma + c\gamma\sigma))$, $\psi = \frac{\sigma_n^2(|h_{U_1,D_1}|^2 - |h_{U_1,E}|^2)}{|h_{U_1,E}|^2|h_{U_2,D_1}|^2}$, $\lambda_1 = \frac{\gamma(P_{\max_1}|h_{U_1,D_2}|^2 + \sigma_n^2)}{|h_{U_2,D_2}|^2}$, $\lambda_2 = \frac{\gamma\sigma_n^2}{|h_{U_2,D_2}|^2}$, and $\varsigma = \min(P_{\max_2}, \inf \psi, \inf \lambda_1)$. Then, optimal P_2 is given as follows:

1) If $A < 0$

$$P_2^* = \lambda_2 \quad (35)$$

2) If $A > 0$

a) If $C > 0$ or $B > 0$ and $C < 0$

$$P_2^* = \begin{cases} P_{2C} & P_{2C} \in p_2 \\ \arg \max_{P_2 \in \{\lambda_2, \psi\}} C_s & P_{2C} \notin p_2 \end{cases} \quad (36)$$

b) If $B < 0$ and $C < 0$

$$P_2^* = \arg \max_{P_2 \in \{\lambda_2, \psi\}} C_s \quad (37)$$

where C_s is the secrecy rate, $P_{2C} = \frac{-B - \sqrt{\Delta}}{2D}$, $\Delta = 4Aabcde\gamma(d\gamma\sigma + b\sigma)$, $D = -bde(ab + cd\gamma)$, and p_2 is the feasibility domain of the problem.

Proof: The proof is similar to that of Theorem 2, thus was omitted. ■

IV. PROBLEM FORMULATION: EGOISTIC SCENARIO

In this section, we develop closed-form solutions for the case when U_2 is selfish from the view point of U_1 's secrecy rate, and adjusts its transmission power just to meet its QoS, i.e., SINR= γ . Later, we compare this case with respect to the altruistic scenario. If one of the Cases 7a, 7b, or 7c holds and U_2 is selfish, (14) can be written as

$$\begin{aligned}
&\max_{P_1, P_2} \frac{1 + \frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2 + \sigma_n^2}}{1 + \frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2 + \sigma_n^2}} \\
&\text{s. t. } P_1 \leq P_{\max_1}, P_1 \stackrel{(7a)}{\geq} \omega, P_2 \leq P_{\max_2}, \frac{P_2|h_{U_2,D_2}|^2}{P_1|h_{U_1,D_2}|^2 + \sigma_n^2} = \gamma. \quad (38)
\end{aligned}$$

In Case 7b, any P_1 ensures that the eavesdropper cannot employ SIC, so no additional constraint over P_1 is necessary. For Case 7d, the problem is solved as follows

$$\begin{aligned} & \max_{P_1, P_2} \frac{1 + \frac{P_1 |h_{U_1, D_1}|^2}{P_2 |h_{U_2, D_1}|^2 + \sigma_n^2}}{1 + \frac{P_1 |h_{U_1, E}|^2}{\sigma_n^2}} \\ & \text{s. t. } P_1 \leq P_{\max_1}, P_2 \leq P_{\max_2}, \frac{P_2 |h_{U_2, D_2}|^2}{P_1 |h_{U_1, D_2}|^2 + \sigma_n^2} = \gamma. \end{aligned} \quad (39)$$

We first solve (38) and then (39). Using the last constraint in (38), we can directly derive the solution for P_2 as $P_2 = \gamma \frac{(P_1 |h_{U_1, D_2}|^2 + \sigma_n^2)}{|h_{U_2, D_2}|^2}$ and replace it with the corresponding value. Consequently, we can rewrite (38) as

$$\begin{aligned} & \max_{P_1} \frac{1 + \frac{P_1 |h_{U_1, D_1}|^2}{\gamma \frac{(P_1 |h_{U_1, D_2}|^2 + \sigma_n^2)}{|h_{U_2, D_2}|^2} |h_{U_2, D_1}|^2 + \sigma_n^2}}{1 + \frac{P_1 |h_{U_1, E}|^2}{\gamma \frac{(P_1 |h_{U_1, D_2}|^2 + \sigma_n^2)}{|h_{U_2, D_2}|^2} |h_{U_2, E}|^2 + \sigma_n^2}} \\ & \text{s. t. } P_1 \leq P_{\max_1}, P_1 \stackrel{(7a)}{\geq} \omega, P_1 \leq \frac{P_{\max_2} |h_{U_2, D_2}|^2 - \gamma \sigma_n^2}{\gamma |h_{U_1, D_2}|^2}. \end{aligned} \quad (40)$$

Since the minimum value for the secrecy rate is zero, the objective function in (40) should be greater or equal to one. Proposition 4.1 gives the required condition on P_1 in order to have a positive secrecy rate. According to the channel conditions, these constraints should be added to (40).

Proposition 4.1: In order for the objective function in (40) to result in a non-negative secrecy rate, P_1 should have the following bounds:

$$P_1 > \frac{A'}{B'} \quad \text{if} \quad A' > 0, B' > 0, \quad (41a)$$

$$P_1 > 0 \quad \text{if} \quad A' < 0, B' > 0, \quad (41b)$$

$$P_1 < \frac{A'}{B'} \quad \text{if} \quad A' < 0, B' < 0, \quad (41c)$$

where $A' = ((1+c)d - b(1+e))\sigma_n^2$, $B' = a(be - cd)$. Also, for the case $A' > 0$ and $B' < 0$, irrespective of the value for P_2 , no positive secrecy rate is possible for U_1 . The values for b, c, d and e are defined in Theorem 5.

Proof: The proof is similar to that of Theorem 1, thus was omitted. ■

According to Proposition 4.1, we can rewrite (40) as

$$\begin{aligned} & \max_{P_1} \frac{1 + \frac{P_1 |h_{U_1, D_1}|^2}{\gamma \frac{(P_1 |h_{U_1, D_2}|^2 + \sigma_n^2)}{|h_{U_2, D_2}|^2} |h_{U_2, D_1}|^2 + \sigma_n^2}}{1 + \frac{P_1 |h_{U_1, E}|^2}{\gamma \frac{(P_1 |h_{U_1, D_2}|^2 + \sigma_n^2)}{|h_{U_2, D_2}|^2} |h_{U_2, E}|^2 + \sigma_n^2}} \\ & \text{s. t. } P_1 \leq P_{\max_1}, P_1 \stackrel{(7a)}{\geq} \omega, P_1 \stackrel{(41a)}{\stackrel{(41c)}{\geq}} \frac{A'}{B'} = \varphi_3, \\ & P_1 \leq \frac{P_{\max_2} |h_{U_2, D_2}|^2 - \gamma \sigma_n^2}{\gamma |h_{U_1, D_2}|^2} = \lambda_3. \end{aligned} \quad (42)$$

Assuming that (42) is feasible, we give a closed-form solution for (42) in Theorem 5.

Theorem 5: Assuming $a = |h_{U_1, D_2}|^2$, $b = |h_{U_1, D_1}|^2$, $c = \gamma \frac{|h_{U_2, D_1}|^2}{|h_{U_2, D_2}|^2}$, $d = |h_{U_1, E}|^2$, $e = \gamma \frac{|h_{U_2, E}|^2}{|h_{U_2, D_2}|^2}$, $Q = c - e$, $R = -(1+c)d + a(c-e) + b(1+e)$, $S = -ac^2d(1+e) + b(e(d+ae) + c(-d+ae^2))$, $T = \frac{-A'}{\sigma_n^2} = -(1+c)d + b(1+e)$, $U = \frac{B'}{a} = be - cd$, $\eta = \min\{P_{\max_1}, \lambda_3\}$, $\eta' = \min\{\eta, \omega\}$, $\theta = \min\{P_{\max_1}, \lambda_3, \varphi_3\}$, and $\theta' = \min\{\theta, \omega\}$ (40) can be solved as follows

1) If $QR < 0$

a) If $S > 0, A'' > 0, B'' > 0$, (or $A'' < 0, B'' > 0$)

$$P_1^* = \begin{cases} \eta & Q > 0, R < 0 \\ \theta & B' < 0, Q < 0, R > 0 \\ \eta & B' > 0, Q < 0, R > 0 \end{cases} \quad (43)$$

b) If $S > 0, A'' < 0, B'' < 0$

$$P_1^* = \begin{cases} \eta' & Q > 0, R < 0 \\ \theta' & B' < 0, Q < 0, R > 0 \\ \eta' & B' > 0, Q < 0, R > 0 \end{cases} \quad (44)$$

c) If $S < 0, A'' > 0, B'' > 0$

$$P_1^* = \begin{cases} \max\{\varphi_3, \omega\} & B' > 0, Q > 0, R < 0 \\ \omega & Q < 0, R > 0 \end{cases} \quad (45)$$

d) If $S < 0, A'' < 0, B'' < 0$ (or $A'' < 0, B'' > 0$)

$$P_1^* = \begin{cases} \varphi_3 & B' > 0, Q > 0, R < 0 \\ 0 & Q < 0, R > 0 \end{cases} \quad (46)$$

2) If $QR > 0$

a) If $S > 0, T < 0$ and $B' > 0$

$$P_1^* = \begin{cases} \arg \max_{P_1 \in \{\max\{\varphi_3, \omega\}, \eta\}} C_s & A'' > 0, B'' > 0 \\ \arg \max_{P_1 \in \{\varphi_3, \eta'\}} C_s & A'' < 0, B'' < 0 \\ \arg \max_{P_1 \in \{\varphi_3, \eta\}} C_s & A'' < 0, B'' > 0 \end{cases} \quad (47)$$

b) If $S < 0, T > 0, A'' > 0, B'' > 0$

$$P_1^* = \begin{cases} P_{1C} & P_{1C} \in p_1 \\ \arg \max_{P_1 \in \{\omega, \eta\}} C_s & P_{1C} \notin p_1, B' > 0 \\ \arg \max_{P_1 \in \{\omega, \theta\}} C_s & P_{1C} \notin p_1, B' < 0 \end{cases} \quad (48)$$

c) If $S < 0$ and $T > 0, A'' < 0, B'' < 0$

$$P_1^* = \begin{cases} P_{1C} & P_{1C} \in p_1 \\ \arg \max_{P_1 \in \{0, \eta'\}} C_s & P_{1C} \notin p_1, B' > 0 \\ \arg \max_{P_1 \in \{0, \theta'\}} C_s & P_{1C} \notin p_1, B' < 0 \end{cases} \quad (49)$$

d) If $S < 0$ and $T > 0, A'' < 0, B'' > 0$

$$P_1^* = \begin{cases} P_{1C} & P_{1C} \in p_1 \\ \arg \max_{P_1 \in \{0, \eta\}} C_s & P_{1C} \notin p_1, B' > 0 \\ \arg \max_{P_1 \in \{0, \theta\}} C_s & P_{1C} \notin p_1, B' < 0 \end{cases} \quad (50)$$

e) If $S > 0, T > 0, U < 0$ and $A'' > 0, B'' > 0$

$$P_1^* = \begin{cases} \arg \max_{P_1 \in \{P_{1C}, \omega, \theta\}} C_s & P_{1C} \in p_1 \\ \arg \max_{P_1 \in \{\omega, \theta\}} C_s & P_{1C} \notin p_1 \end{cases} \quad (51)$$

f) If $S > 0, T > 0, U < 0$ and $A'' < 0, B'' < 0$

$$P_1^* = \begin{cases} \arg \max_{P_1 \in \{P_{1C}, 0, \theta'\}} C_s & P_{1C} \in p_1 \\ \arg \max_{P_1 \in \{0, \theta'\}} C_s & P_{1C} \notin p_1 \end{cases} \quad (52)$$

g) If $S > 0, T > 0, U < 0$ and $A'' < 0, B'' > 0$

$$P_1^* = \begin{cases} \arg \max_{P_1 \in \{P_{1C}, 0, \theta\}} C_s & P_{1C} \in p_1 \\ \arg \max_{P_1 \in \{0, \theta\}} C_s & P_{1C} \notin p_1 \end{cases} \quad (53)$$

h) If $S < 0, T < 0, U > 0, A'' > 0, B'' > 0$ (or $A'' < 0, B'' > 0$)

$$P_1^* = \begin{cases} \arg \max_{P_1 \in \{P_{1C}, \max\{\varphi_3, \omega\}, \eta\}} C_s & P_{1C} \in p_1 \\ \arg \max_{P_1 \in \{\max\{\varphi_3, \omega\}, \eta\}} C_s & P_{1C} \notin p_1 \end{cases} \quad (54)$$

i) If $S < 0, T < 0, U > 0$ and $A'' < 0, B'' < 0$

$$P_1^* = \begin{cases} \arg \max_{P_1 \in \{P_{1C}, \varphi_3, \eta'\}} C_s & P_{1C} \in p_1 \\ \arg \max_{P_1 \in \{\varphi_3, \eta'\}} C_s & P_{1C} \notin p_1 \end{cases} \quad (55)$$

j) If $S > 0, T > 0$ and $U > 0$

$$P_1^* = \begin{cases} \eta & A'' > 0, B'' > 0 \\ \eta & A'' < 0, B'' > 0 \\ \eta' & A'' < 0, B'' < 0 \end{cases} \quad (56)$$

where $P_{1C} = \frac{-2a(1+c)(1+e)U\sigma_n^2 - \sqrt{\Delta}}{2aS}$ and $\Delta = 4abdQR(\sigma_n^2)^4(1+c)(1+e)$.

Proof: The proof can be obtained in the similar way to that of Theorem 2. ■

For problem (39), the closed-form solution for P_1 is given in the following theorem.

Theorem 6: Assume $f = |h_{U_1, D_1}|^2, g = |h_{U_1, D_2}|^2, h = |h_{U_2, D_1}|^2, i = |h_{U_2, D_2}|^2, j = |h_{U_1, E}|^2, E = ad + bc\gamma - e(d + c\gamma), F = ad - e(d + c\gamma)$, and $\tau = \min(P_{\max_2}, \inf \rho)$. Then, optimal P_1 is as follows:

1) If $E < 0$

$$P_2^* = 0 \quad (57)$$

2) If $E > 0$

a) If $F > 0$

$$P_2^* = \begin{cases} P_{2C} & P_{2C} \in p_2 \\ \arg \max_{P_2 \in \{0, \tau\}} C_s & P_{2C} \notin p_2 \end{cases} \quad (58)$$

b) If $F < 0$

$$P_2^* = \arg \max_{P_2 \in \{0, \tau\}} C_s \quad (59)$$

where $P_{2C} = \frac{-G - \sqrt{\Delta}}{2H}, \Delta = 4Eabcde\gamma(d + c\gamma)\sigma^2, G = -2bce\gamma(d + c\gamma)\sigma, H = -bce\gamma(ad + bc\gamma), \rho = \frac{\sigma_n^2(|h_{U_1, D_1}|^2 - |h_{U_1, E}|^2)|h_{U_2, D_2}|^2}{\gamma|h_{U_1, E}|^2|h_{U_2, D_1}|^2|h_{U_1, D_2}|^2} - \frac{\sigma_n^2}{|h_{U_1, D_2}|^2}$, and p_2 is the feasibility domain of the problem.

Proof: The proof can be obtained in the similar way to that of Theorem 2. ■

V. SECRECY ENERGY EFFICIENCY

Before going to Section VI, we define a metric in order to investigate the energy efficiency of the considered scenario. We define the secrecy energy efficiency, η_{SEE} , as the maximum secrecy rate obtained from the objective of (9), namely Ψ , to the optimal consumed power of U_1, P_1^* , ratio as $\eta_{SEE} = \frac{\Psi}{P_1^*}$. Similarly, in the case we have only one transceiver pair and an eavesdropper with no interfering user, the secrecy energy efficiency metric, η_{SEE} , can be defined as $\eta_{SEE_{su}} = \frac{\log((\sigma_n^2 + P^*|h_{U, D}|^2)/(\sigma_n^2 + P^*|h_{U, E}|^2))}{P^*}$, where P is the transmission power, and P^* is the optimal transmission power obtained from the optimization problem in the nominator. When the condition $|h_{U, D}|^2 > |h_{U, E}|^2$ holds, the optimum consumed power in the single-user case is P_{max} . In contrast, as we shall see in Section VI, the optimal power consumed by U_1 in the interference channel is considerably lower than P_{max} . Hence, as shall be shown in Section VI, in a wide range of powers, the interference network outperforms the single-user network in terms of secrecy energy efficiency.

VI. NUMERICAL RESULTS

In this section, we present different scenarios as numerical examples to further clarify the derived results. As a benchmark, we consider a single-user scenario where only one user is present in the environment and there is no second user to produce interference [39]. Then, we compare this benchmark with our system model. Here, we refer to the altruistic and egoistic scenarios as interference channel modes. In all simulation scenarios, we assume that the noise power is equal to one, i.e., $\sigma_n^2 = 1$. All the channel coefficients are modeled as i.i.d. complex normal random variables with real and imaginary parts being $\mathcal{N}(0, 1)$. The channel coefficients are normalized to have a unit variance as $\mathcal{CN}(0, 1)$.

For the first scenario, we consider the effect of the users' power limits, P_{\max_1} and P_{\max_2} , on the average secrecy rate as shown in Fig. 3 for SINR = 1 at U_2 's destination. By observing the results in Fig. 3, we can draw the following conclusions for both altruistic and egoistic scenarios:

- 1) Average secrecy rate of U_1 increases as P_{\max_1} or P_{\max_2} increases.
- 2) Increasing P_{\max_1} is more effective on improving the average secrecy rate rather than increasing P_{\max_2} . The reason is that increasing U_2 's power creates more interference to both U_1 and E .
- 3) The average secrecy rate of U_1 is lower in the egoistic scenario since U_2 does not change its transmitted power in favor of U_1 , and only adjusts it according to the required QoS at D_2 . Also, by comparing Fig. 4 and Fig. 5, it can be seen that U_2 consumes less power in the egoistic scenario. When the Cases (15a) and (15b) of Theorem 1 are true, U_2 can improve the secrecy rate by providing more power in the altruistic scenario.

The average optimal powers consumed by U_1 and U_2 are shown in Fig. 4 for the altruistic scenario. Following points are implied by Fig. 4 as:

- 1) In contrast to the single-user case where the maximum power consumption is optimum when the data link is stronger than the wiretap link, average optimal powers expended by users in the interference channel modes are considerably less than the available quantity. So, the optimum power control in the interference channel leads to enormous power saving.
- 2) As P_{\max_1} increases, U_2 consumes more power. A higher power transmission from U_1 produces more interference on D_2 . This makes U_2 to choose higher transmission power in order to maintain the QoS at D_2 .
- 3) As P_{\max_2} increases, U_1 utilizes more power. A higher available power for U_2 enables it to compensate a higher interference from U_1 , so U_1 transmits with a higher power to increase the secrecy rate.
- 4) Depending on the maximum available power to the users, the optimal consumed power by one user can be higher or lower than the power consumed by the other user.

Consumed powers by U_1 and U_2 for the egoistic scenario are illustrated in Fig. 5. As we can see, the power consumption pattern is similar to the altruistic scenario as in Fig. 4. By comparing Fig. 5 with Fig. 4, it is noticed that the power

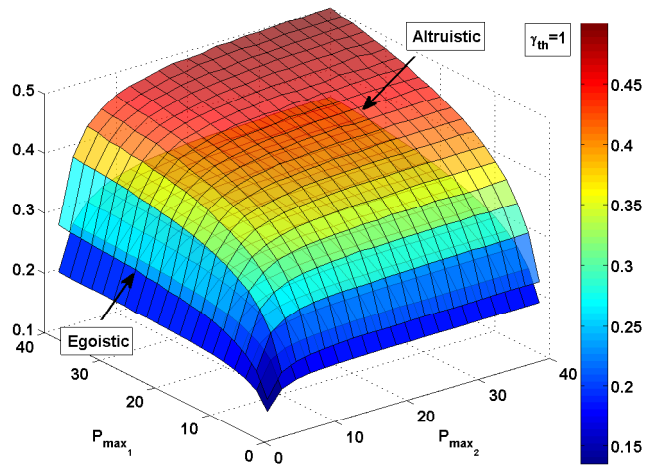


Fig. 3: Average secrecy rate versus the users' maximum available powers in altruistic and egoistic scenarios.

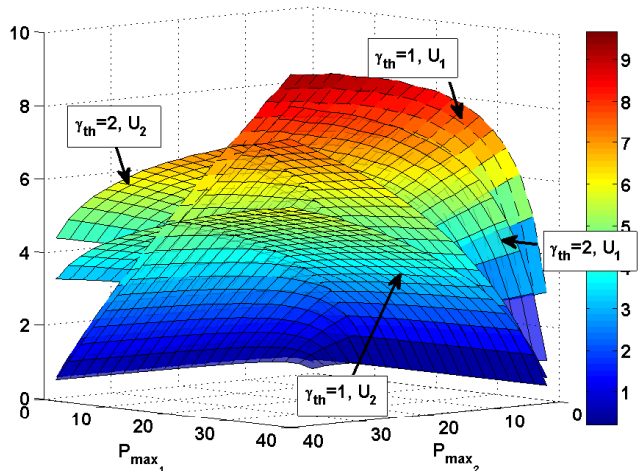


Fig. 4: Average optimal power consumed by the users versus their maximum available powers in altruistic scenario.

consumed by the users in the altruistic scenario is higher than the egoistic scenario.

Average excess SINR provided by U_2 at D_2 in the altruistic scenario is shown in Fig. 6 for different values of the required QoS, γ_{th} . Following messages are conveyed by Fig. 6 as:

- 1) By increasing P_{\max_1} for a fixed P_{\max_2} , the excess SINR provided at D_2 drops due to increased interference from U_1 's transmission.
- 2) Increasing P_{\max_2} for a fixed P_{\max_1} leads to a higher excess SINR at D_2 .

The average secrecy rate comparison among the single-user benchmark and the interference channel modes is presented in Fig. 7 with respect to the maximum available power of U_1 . Following conclusions can be made according to Fig. 7:

- 1) Increasing P_{\max_2} also enhances the average secrecy rate but much less compared to increasing the P_{\max_1} , because U_2 induces interference on both D_1 and E .
- 2) The secrecy rate in the egoistic scenario is always lower than the one in the altruistic scenario. In the egoistic

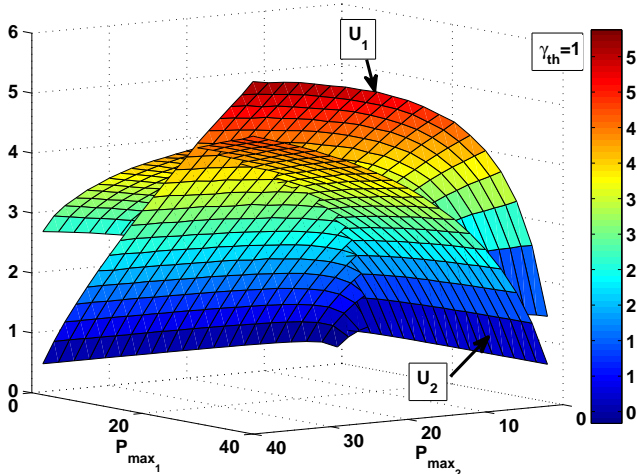


Fig. 5: Average optimal power consumed by the users versus their maximum available powers in the egoistic scenario.

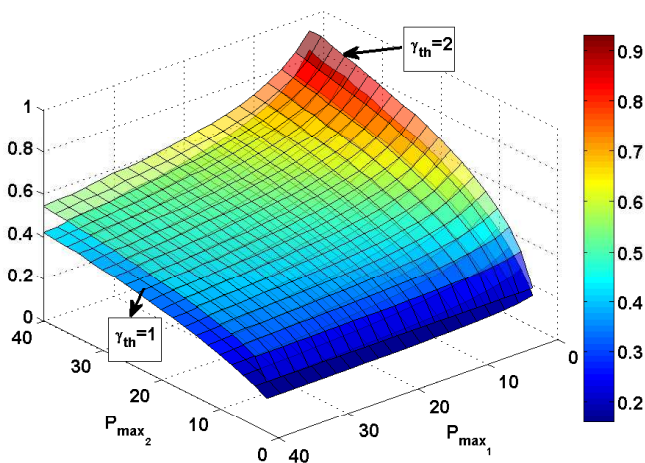


Fig. 6: Average excess QoS provided at D_2 versus users' maximum available powers in the altruistic scenario.

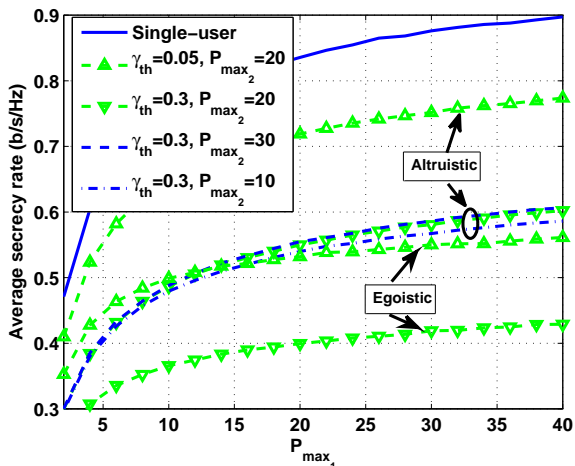


Fig. 7: Average secrecy rate versus U_1 's maximum available power.

scenario, U_2 consumes power to only fulfil the QoS at

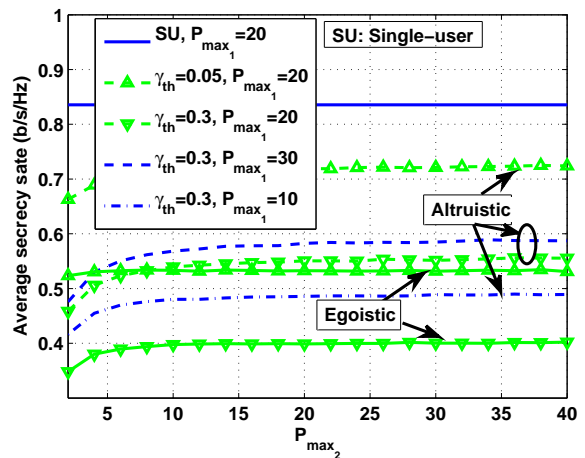


Fig. 8: Average secrecy rate versus U_2 's maximum available power.

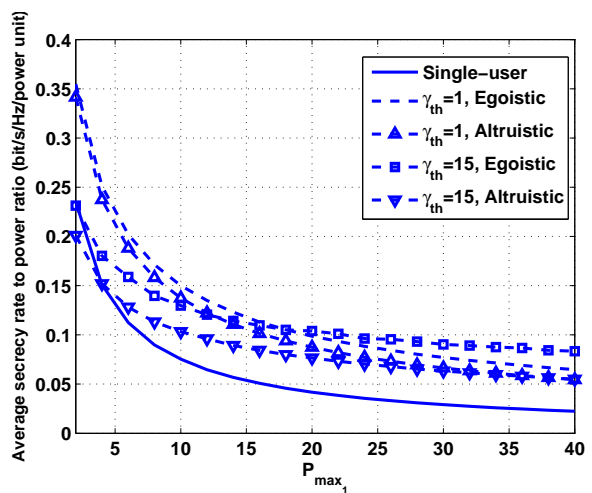


Fig. 9: Average secrecy energy efficiency versus U_1 's maximum available power.

D_2 . As a result, U_2 does not increase its transmission power to produce interference on E when the Cases (15a) and (15b) of Theorem 1 hold. However, in the altruistic scenario, U_2 can change its transmission power in favor of U_1 when it becomes necessary.

A similar comparison as in Fig. 7 is displayed in Fig. 8 with respect to the maximum available power of U_2 . The Statements 1 and 2 of Fig. 7 also hold for Fig. 8. As we see in Fig. 8, increasing P_{\max_2} also increases the average secrecy rate. By increasing P_{\max_2} , U_2 gets a higher ability to suppress the interference coming from U_1 as well as causing more interference on E when the Cases (15a) and (15b) of Theorem 1 hold. As a result, U_1 can transmit with a higher power and enhance the secrecy rate.

As we can see from Fig. 7 and Fig. 8, the average secrecy rate in the interference channel modes is lower than its value in the single-user case. However, we should note that the power consumed in the interference channel modes is considerably lower than the single-user case. To make a fair comparison, we

use the “secrecy energy efficiency” metric defined in Section V to compare the secrecy rates of the interference channel modes and the single-user benchmark. This metric is derived for different values of γ_{th} in Fig. 9. According to graphs in Fig. 9, we can make the following conclusions:

- 1) The secrecy energy efficiency is higher for the interference channel modes in a considerable range of γ_{th} and P_{\max_1} . If we consider a specific available power for U_1 , the acquired secrecy rate in the interference channel modes becomes higher than the one achieved in the single-user case.
- 2) As the maximum available power to U_1 increases, the secrecy energy efficiency falls faster for the cases with lower γ_{th} .

VII. CONCLUSION

We studied the effect of interference on improving the secrecy rate in a two-user wireless interference network with input signals following Gaussian distribution. We developed channel dependent expressions for both altruistic and egoistic scenarios to define the proper range of transmission power for the interfering user, namely user 2, in order to sustain a positive secrecy rate for the other user, namely user 1. Closed-form solutions were obtained in order to perform joint optimal power control for both users in the altruistic and egoistic scenarios. It was shown that by decreasing the required QoS at user 2’s destination, the secrecy rate in the interference channel improves and gets closer to the single-user case.

Moreover, to fairly compare our scheme with the benchmark, the ratio of the secrecy rate over the optimal consumed power by user 1 was introduced as a new metric called “secrecy energy efficiency”, in order to take into account both the secrecy rate and the consumed power. It was shown that in comparison with the single-user case, the secrecy energy efficiency is considerably higher in the interference channel for a wide range of QoS at user 2’s destination.

APPENDIX A PROOF OF THEOREM 1

For the objective function in (12) to be positive, the following condition must hold

$$\begin{aligned}
& \log_2 \left(1 + \frac{P_1 |h_{U_1, D_1}|^2}{P_2 |h_{U_2, D_1}|^2 + \sigma_n^2} \right) \\
& - \log_2 \left(1 + \frac{P_1 |h_{U_1, E}|^2}{P_2 |h_{U_2, E}|^2 + \sigma_n^2} \right) > 0 \\
& \Rightarrow \frac{P_1 |h_{U_1, D_1}|^2}{P_2 |h_{U_2, D_1}|^2 + \sigma_n^2} > \frac{P_1 |h_{U_1, E}|^2}{P_2 |h_{U_2, E}|^2 + \sigma_n^2} \\
& \Rightarrow \begin{cases} P_2 > \frac{\sigma_n^2 (|h_{U_1, E}|^2 - |h_{U_1, D_1}|^2)}{B} & B > 0 \\ P_2 < \frac{\sigma_n^2 (|h_{U_1, E}|^2 - |h_{U_1, D_1}|^2)}{B} & B < 0 \end{cases} \quad (60)
\end{aligned}$$

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

APPENDIX B PROOF OF THEOREM 2

In order to find the optimal P_2 for (19), we analyze the derivative of the objective function in (19). The derivative is defined at the top of next page in (61) where $a = P_{\max_1} |h_{U_1, D_1}|^2$, $b = |h_{U_2, D_1}|^2$, $c = P_{\max_1} |h_{U_1, E}|^2$, and $d = |h_{U_2, E}|^2$. According to the sign of the derivative, the optimal P_2 can be found. The denominator in (61) is already positive, so the sign of (61) directly depends on the sign of the numerator. The numerator is a quadratic equation. According to the sign of the discriminant of the quadratic equation [40, Section 5.1], denoted by $\Delta = 4abcd\sigma_n^2(b-d)[-d(a+\sigma_n^2)+b(c+\sigma_n^2)]$, the status of the roots can be defined. The sign of the discriminant can be defined as

- 1) If $(b-d)[-d(a+\sigma_n^2)+b(c+\sigma_n^2)] < 0$, $\Delta < 0$.
- 2) If $(b-d)[-d(a+\sigma_n^2)+b(c+\sigma_n^2)] > 0$, $\Delta > 0$.

Using the sign of Δ as well as the sign of the P_2 ’s coefficients in the quadratic equation which we denote them from highest order to constant as a' , b' and c' in (61), the sign of the derivative can be defined and consequently the optimal value for P_2 , P_2^* , can be found as follows:

- 1) If $\Delta < 0$, no root exists for the numerator in (61) leading to the following cases:
 - a) $a' > 0$, then the derivative is strictly positive, as shown in Fig. 10a, and is monotonically increasing, so the highest value in the feasible set is the P_2^* .
 - b) $a' < 0$, then the derivative is strictly negative, as shown in Fig. 10b, and is monotonically decreasing, so the lowest possible value in the feasible set is the P_2^* .
- 2) If $\Delta > 0$, there exist two roots (two critical points for the objective function in (19)) for the derivative leading to the following cases:
 - a) Only one of the roots is positive. This happens when the product of the roots [40, Section 5.1], $\frac{c'}{a'}$, is negative in the following cases:
 - i) $a' > 0$ and $c' < 0$, as shown in Fig. 10c. In this case, the critical point is a minimum, so one of the vertices of the feasible domain is the P_2^* .
 - ii) $a' < 0$ and $c' > 0$, as shown in Fig. 10d. For this case, the critical point is a maximum and if falls into the feasibility domain of P_2 , it is the P_2^* . Otherwise, one of the vertices of the feasible domain is the P_2^* .
 - b) Both of the roots are positive. This happens when both the product, $\frac{c'}{a'}$, and the sum [40, Section 5.1], $-\frac{b'}{a'}$, of the roots are positive in two following conditions:
 - i) $a' > 0$, $c' > 0$ and $b' < 0$, as shown in Fig. 10e. For the first case, the derivative is first positive, then negative and then positive, respectively, meaning that the first root results in a maximum and the second root results in a minimum. If the smaller root falls in the feasibility domain of P_2 , then by comparing it with the vertices of the feasibility domain, P_2^* is found. If the

$$\frac{\partial OF}{\partial P_2} = \frac{bd(bc - ad)P_2^2 + 2b(-a + c)d\sigma_n^2 P_2 + \sigma_n^2(cd\sigma_n^2 - a(-cd + b(c + \sigma_n^2)))}{(\sigma_n^2 + bP_2)^2(c + \sigma_n^2 + dP_2)^2} \quad (61)$$

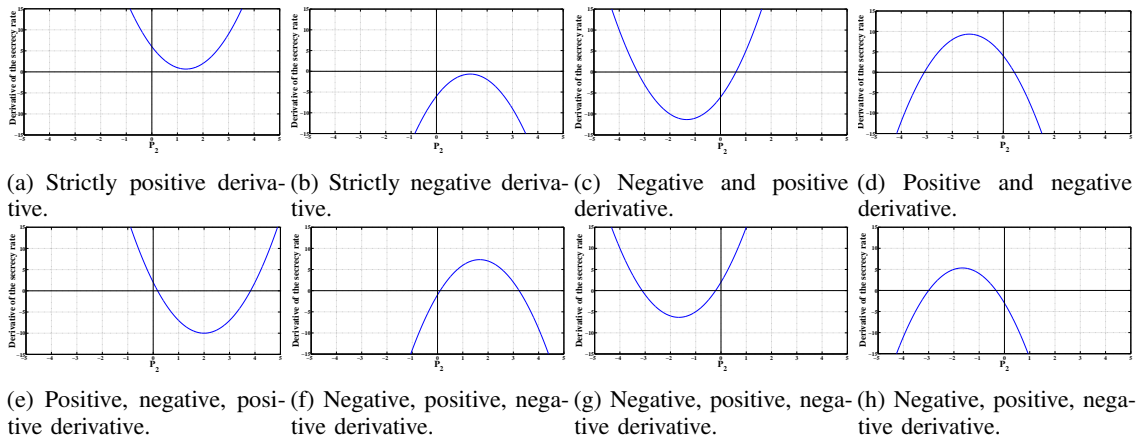


Fig. 10: Different cases for the sign of the derivative in (61).

smaller root is not in the feasibility domain of P_2 , the optimal value of P_2 is at one of the vertices of the feasibility domain.

- ii) $a' < 0$, $c' < 0$ and $b' > 0$, as shown in Fig. 10f. In this case, we find out that the larger root is a maximum. If the larger root falls in the feasibility domain of P_2 , then by comparing it to the vertices of the feasibility domain of P_2 , we can find the P_2^* . If the larger root is not in the feasibility domain of P_2 , we should find the optimal value of P_2 in the vertices of the feasibility domain.
- c) Both of the roots are negative. This happens when the product of the roots, $\frac{c'}{a'}$, is positive and the sum of the roots, $-\frac{b'}{a'}$, is negative in two following conditions:
 - i) $a' > 0$, $c' > 0$ and $b' > 0$, as shown in Fig. 10g. Since the transmission power is always positive, the critical points cannot be the answer to P_2^* . For the first case, the derivative is first positive, then negative and then positive, respectively. As a result, the secrecy rate will be increasing after $P_2 > 0$. So, P_2^* is the maximum possible value of P_2 inside the feasibility set.
 - ii) $a' < 0$, $c' < 0$ and $b' < 0$, as shown in Fig. 10h. As in Case 2(c)i, the critical points cannot be the answer to P_2^* . For the first case, the derivative is first negative, then positive and then negative, respectively. So, the secrecy rate is decreasing after $P_2 > 0$. Hence, P_2^* is the minimum possible value of P_2 inside the feasibility set.

In deriving the above closed-form optimal solutions, we have considered all the possible cases of discriminant sign, Δ , and the coefficients of the quadratic equation, a' , b' , and c' . In each case, we have calculated all the critical points and if

applicable, these critical points are compared with the vertices of the domain to make sure that the derived power value is globally optimum. Hence, the optimal solutions presented in Appendix B are global optimum.

REFERENCES

- [1] M. A. Olson, M. M. Bykowsky, and W. W. Sharkey, "Modeling the efficiency of spectrum designated to licensed service and unlicensed operations," *FCC OSP Working Paper Series*, Feb. 2008.
- [2] 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, Sep. 2003.
- [3] N. Sklavos and X. Zhang, *Wireless Security and Cryptography: Specifications and Implementations*. Taylor & Francis, 2007.
- [4] Physical layer wireless security. Seventh framework programme (FP7). [Online]. Available: <http://www.phylaws-ict.org>
- [5] O. Koyluoglu, H. El-Gamal, L. Lai, and H. Poor, "On the secure degrees of freedom in the K-user gaussian interference channel," in *IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, Jul. 2008, pp. 384–388.
- [6] 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.
- [7] O. Koyluoglu and H. El-Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.
- [8] 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.
- [9] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Feasibility of positive secrecy rate in wiretap interference channels," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Atlanta, GA, Dec. 2014, pp. 1190–1194.
- [10] Z. Shu, Y. Yang, Y. Qian, and R. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Houston, TX, Dec. 2011.
- [11] 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.
- [12] S. Jeong, K. Lee, J. Kang, Y. Baek, and B. Koo, "Transmit beamforming with imperfect CSIT in spectrum leasing for physical-layer security," in *IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, Jan. 2012, pp. 874–878.
- [13] K. Lee, C.-B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4672–4678, Nov. 2013.

- [14] T. Kwon, V. Wong, and R. Schober, "Secure MISO cognitive radio system with perfect and imperfect CSI," in *IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, Dec. 2012, pp. 1236–1241.
- [15] 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.
- [16] 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.
- [17] 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.
- [18] 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, MD, Mar. 2009, pp. 318–323.
- [19] S. Fakoorian and A. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640–649, Sept. 2011.
- [20] P. Mohapatra and C. Murthy, "Secrecy in the 2-user symmetric deterministic interference channel with transmitter cooperation," in *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Darmstadt, Germany, Jun. 2013, pp. 270–274.
- [21] 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.
- [22] 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.
- [23] S. Ma, M. Hong, E. Song, X. Wang, and D. Sun, "Outage constrained robust secure transmission for MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5558–5570, Oct. 2014.
- [24] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2730–2745, May 2011.
- [25] A. Rabbachin, A. Conti, and M. Win, "The role of aggregate interference on intrinsic network secrecy," in *IEEE International Conference on Communications (ICC)*, Ottawa, Canada, Jun. 2012, pp. 3548–3553.
- [26] Z. Fei, J. Ni, N. Wang, C. Xing, and J. Kuang, "A robust and distributed design for coordinated downlink beamforming for secure MISO interference channels," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 10, pp. 1020–1027, Apr. 2014.
- [27] 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.
- [28] 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.
- [29] P. Xu, Z. Ding, X. Dai, and K. Leung, "A general framework of wiretap channel with helping interference and state information," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 182–195, Feb. 2014.
- [30] M. El-Halabi and C. Georghiadis, "On secure communication with known interference," in *International Symposium on Information Theory and its Applications (ISITA)*, Honolulu, HI, Oct. 2012.
- [31] A. Rabbachin, A. Conti, and M. Win, "Intentional network interference for denial of wireless eavesdropping," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Houston, TX, Dec. 2011.
- [32] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.
- [33] Y. Liang, A. Somekh-Baruch, H. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.
- [34] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.
- [35] 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.
- [36] T. Chiueh and P. Tsai, *OFDM Baseband Receiver Design for Wireless Communications*. Wiley, 2008.
- [37] D. Tse and S. Hanly, "Multiaccess fading channels. I. polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2796–2815, Nov. 1998.
- [38] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY: Cambridge University Press, 2005.
- [39] A. D. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
- [40] M. Spiegel, S. Lipschutz, and J. Liu, *Schaum's Outline of Mathematical Handbook of Formulas and Tables*, 3rd ed., ser. McGraw Hill professional. McGraw-hill, 2008.



Ashkan Kalantari Ashkan Kalantari (AK) was born in Yazd, Iran, 1987. He received his BSc and MSc degrees from K. N. Toosi University of Technology, Tehran, Iran in 2009 and 2012, respectively. He is currently working toward the Ph.D. degree with the research group SIGCOM in the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg. His research interest is physical layer security in wireless and satellite communications.



Sina Maleki received his BSc degree from Iran University of Science and Technology, Tehran, Iran in 2006, and MSc and PhD degrees from Delft University of Technology, Delft, The Netherlands, in 2009 and 2013, respectively. From July 2008 to April 2009, he was an intern student at the Philips Research Center, Eindhoven, The Netherlands, working on spectrum sensing for cognitive radio networks. Since August 2013, he has been working at the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, where he is

working on cognitive radio for satellite communications within the EU FP7 CoRaSat project, and EU H2020 SANSAs, as well as Luxembourgish national projects SATSENT, and SeMIGod.



Gan Zheng (S'05-M'09-SM'12) is currently a Lecturer in School of Computer Science and Electronic Engineering, University of Essex, UK. He received the B. E. and the M. E. from Tianjin University, Tianjin, China, in 2002 and 2004, respectively, both in Electronic and Information Engineering, and the PhD degree in Electrical and Electronic Engineering from The University of Hong Kong, Hong Kong, in 2008. Before he joined University of Essex, he worked as a Research Associate at University College London, UK, and University of Luxembourg, Luxembourg.

His research interests include cooperative communications, cognitive radio, physical-layer security, full-duplex radio and energy harvesting. He is the first recipient for the 2013 IEEE Signal Processing Letters Best Paper Award.



Symeon Chatzinotas (MEng, MSc, PhD, SMIEEE) received the M.Eng. in Telecommunications from Aristotle University of Thessaloniki, Greece and the M.Sc. and Ph.D. in Electronic Engineering from University of Surrey, UK in 2003, 2006 and 2009 respectively. He is currently a Research Scientist with the research group SIGCOM in the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, managing H2020, ESA and FNR projects. In the past, he has worked in numerous R&D projects for the Institute of Informatics & Telecom-

munications, National Center for Scientific Research Demokritos, the Institute of Telematics and Informatics, Center of Research and Technology Hellas and Mobile Communications Research Group, Center of Communication Systems Research, University of Surrey. He has authored more than 120 technical papers in refereed international journals, conferences and scientific books. His research interests are on multiuser information theory, cooperative/cognitive communications and wireless networks optimization. Dr Chatzinotas is the co-recipient of the 2014 Distinguished Contributions to Satellite Communications Award, Satellite and Space Communications Technical Committee, IEEE Communications Society. He is currently co-editing a book on "Cooperative and Cognitive Satellite Systems" to appear in 2015 by Elsevier and he is co-organizing the First International Workshop on Cognitive Radios and Networks for Spectrum Coexistence of Satellite and Terrestrial Systems (CogRaN-Sat) in conjunction with the IEEE ICC 2015, 8-12 June 2015, London, UK.



Björn Ottersten was born in Stockholm, Sweden, 1961. He received the M.S. degree in electrical engineering and applied physics from Linköping University, Linköping, Sweden, in 1986. In 1989 he received the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA. Dr. Ottersten has held research positions at the Department of Electrical Engineering, Linköping University, the Information Systems Laboratory, Stanford University, the Katholieke Universiteit Leuven, Leuven, and the University of Luxembourg. During 96/97 Dr.

Ottersten was Director of Research at ArrayComm Inc, a start-up in San Jose, California based on Otterstens patented technology. He has co-authored journal papers that received the IEEE Signal Processing Society Best Paper Award in 1993, 2001, 2006, and 2013 and 3 IEEE conference papers receiving Best Paper Awards. In 1991 he was appointed Professor of Signal Processing at the Royal Institute of Technology (KTH), Stockholm. From 1992 to 2004 he was head of the department for Signals, Sensors, and Systems at KTH and from 2004 to 2008 he was dean of the School of Electrical Engineering at KTH. Currently, Dr. Ottersten is Director for the Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg. Dr. Ottersten is a board member of the Swedish Research Council and as Digital Champion of Luxembourg, he acts as an adviser to the European Commission. Dr. Ottersten has served as Associate Editor for the IEEE Transactions on Signal Processing and on the editorial board of IEEE Signal Processing Magazine. He is currently editor in chief of EURASIP Signal Processing Journal and a member of the editorial boards of EURASIP Journal of Applied Signal Processing and Foundations and Trends in Signal Processing. Dr. Ottersten is a Fellow of the IEEE and EURASIP and a member of the IEEE Signal Processing Society Board of Governors. In 2011 he received the IEEE Signal Processing Society Technical Achievement Award. He is a first recipient of the European Research Council advanced research grant. His research interests include security and trust, reliable wireless communications, and statistical signal processing.