Secrecy Games on the One-Sided Interference Channel

Jianwei Xie Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
xiejw@umd.edu *ulukus@umd.edu*

***Abstract*—In this paper, we study the two-user one-sided interference channel with confidential messages. In this interference channel, in addition to the usual selfishness of the users, the relationship between the two pairs of users is further adversarial in the sense of both receivers' desires to eavesdrop on the communication of the other pair. We develop a game-theoretic model to study the information-theoretic secure communications in this setting. We first start with a game-theoretic model where each pair's payoff is their own secrecy rate. The analysis of the binary deterministic interference channel with this payoff function shows that self-jamming of a transmitter, which injures the eavesdropping ability of its own receiver, is not excluded by the Nash equilibria. We propose a refinement for the payoff function by explicitly accounting for the desire of the receiver to eavesdrop on the other party's communication. This payoff function captures the adversarial relationship between the two pairs of users better. We determine the Nash equilibria for the binary deterministic channel for both payoff functions.**

I. Introduction

In the interference channel, multiple users share the transmission medium, and simultaneously wish to have reliable communication with their respective receivers. The information-theoretic capacity region of the interference channel is mostly unknown; it is known only in certain special cases, e.g., a class of deterministic interference channels [1], a class of strong interference channels [2]–[4], and a class of degraded interference channels [5]. In order to achieve a particular rate point on the capacity region of the interference channel, the transmitter-receiver pairs need to jointly choose encoding and decoding schemes, and cooperate to agree on the particular operating rate point, and coordinate their actions, e.g., time-sharing.

In actual interference networks, such kinds of cooperations may not be practical or agreeable by the users. It is reasonable to assume that all transmitter-receiver pairs in the network are selfish and rational. Moreover, each pair is only interested in transmitting their messages at the maximum reliable rate. Consequently, the information-theoretic capacity region may not be fully achievable. Reference [6] made this intuition precise by considering the interference channel from a game-theoretic point of view, and found the Nash equilibrium operating points on the capacity region, especially focusing on the binary deterministic interference channel and the Gaussian interference channel. Taking the reliable communication rate for each transmitter as its payoff function, [6] showed that, in a non-cooperative game, two transmitters agree only on a subset of the capacity region of the interference channel, which forms the set of Nash equilibria.

This work was supported by NSF Grants CCF 07-29127, CNS 09-64632, CCF 09-64645 and CCF 10-18185.

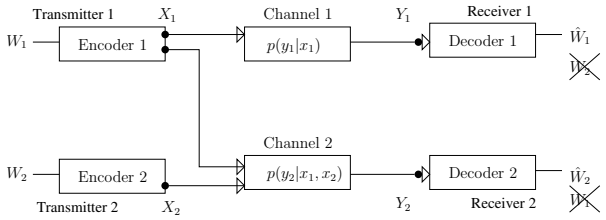

Fig. 1. One-sided interference channel with confidential messages.

In this paper, we consider an interference channel with confidential messages, where two transmitters communicate with two receivers, while each receiver eavesdrops on the other pair's communication. Information-theoretic security was first introduced by using the wiretap channel by Wyner [7], in which the transmitter wishes to send a message to the receiver secret from the eavesdropper. If the quality of the transmitter-receiver channel is *better* than that of the transmitter-eavesdropper channel, Wyner showed that the messages can be transmitted securely at a positive rate. Later, this result was generalized by Csiszar and Korner [8] to broadcast channels with confidential messages and extended by Leung-Yan-Cheong and Hellman [9] to Gaussian wiretap channels. In recent years, many research works studied secure communications in multi-user channels, including the interference channel [10]–[12].

In this paper, we focus on the two-user one-sided interference channel with confidential messages, in which one transmitter-receiver pair is interference-free as shown in Fig. 1. The best known achievable secrecy rate region for the interference channel with confidential messages was developed in [10]. As in the case of interference channels without secrecy constraints, in [10], the two transmitter-receiver pairs need to jointly choose encoding and decoding schemes and further cooperate and coordinate their actions to achieve a secrecy rate pair in this region. In addition, the achievable scheme in [10] requires that the parties trust each other in that they will not unilaterally change their encoding-decoding schemes. Hence, even if it was known, secrecy capacity region might not be sufficient to understand the adversarial relationship in this

network. Reference [11], addressed the issue of trust. In [11], the transmitters can deviate from their transmit strategies. In their definition of robust-secrecy [11], a transmitter can deviate from its strategy, however, arbitrary deviations are not allowed; a transmitter can only deviate to a strategy if the new strategy does not injure the performance of the other transmitter-receiver pair in terms of reliability. When the transmitters are selfish, such kind of behavior may not be guaranteed. Selfish transmitters would care only about their own reliability and secrecy of their own messages. Such selfish transmitters may choose any strategy to maximize the secrecy rate of their own private message, which may hurt the other user's performance.

To develop a model to characterize the adversarial relationship between the two pairs, we only assume that the two transmitter-receiver pairs are selfish and rational; other than these two, they are free to choose any transmission strategy to maximize their own payoff. Under these assumptions, we give a formal definition of the game on interference channels with confidential messages and define the Nash equilibrium in the secrecy rate region. We first consider the case where the payoff function is the reliable secrecy rate of each user. We analyze the binary deterministic interference channel for this payoff function. This analysis reveals that some of the Nash equilibrium secrecy rate pairs are achieved only by self-jamming of a transmitter of its own receiver. This hurts the eavesdropping ability of its own receiver, which in fact is one of the interests of the receivers. Among all the strategies achieving the same secrecy rate, a transmitter-receiver pair is more likely to choose the one that allows the receiver to more strongly eavesdrop on the other pair. To overcome this difficulty, we propose a refinement to the equilibrium. Specifically, we modify the payoff function by incorporating an information leakage measure to it in addition to the secure reliable rate. We find the Nash equilibria with both payoff functions.

II. Problem Formulation

We consider a two-user one-sided interference channel, where each transmitter is free to choose a transmission strategy, which is defined as follows.

Definition 1 (Strategy s_i) *is the encoding method at transmitter i, such that:*

- *the number of information bits of equiprobable messages W_i is $\log(M_i)$, and the block length of codewords is n;*
- *the stochastic encoding function $f_i : \{1, 2, \cdots, M_i\} \to C_i$ maps the message w_i to an n-length codeword x_i^n which belongs to the codebook C_i;*
- *the corresponding rate of this encoder is $R_i = \frac{\log(M_i)}{n}$.*

We assume that the receiver i performs maximum-likelihood decoding on the received signal to get an estimate of the message $\hat{w}_i$. We denote the resulting probability of error as $P_{e,i} = P[W_i \neq \hat{W}_i]$. The decoding error probability $P_{e,i}$ is jointly determined by both strategies s_1 and s_2 due to interference. To characterize information-theoretic secrecy, we define the measure of information leakage of transmitter i as

$$L_i = \frac{1}{n} I(W_i; Y_j^n) \tag{1}$$

where $j = \bar{i}$, i.e., $i = 1, j = 2$ or $i = 2, j = 1$, and Y_j^n is the n-length symbol observed at receiver j.

Then, for any fixed threshold $\epsilon > 0$, which is small enough, given s_1 and s_2, we define the payoff of each transmitter as

$$\pi_i(s_1, s_2) = \begin{cases} R_i, & P_{e,i} \leq \epsilon \text{ and } L_i \leq \epsilon \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

for $i = 1, 2$. It is important to emphasize that, as defined above, s_1 and s_2 jointly determine the payoff π_i of transmitter i. In order to improve π_i, transmitter i can deviate from s_i to any other strategy s_i', and the only criteria for this improvement are $P_{e,i}$ and L_i, not $P_{e,j}$ or L_j. This implies that such a deviation may affect the performance of the other transmitter j. To model the behavior of transmitters, who have the freedom to choose their strategies, it is reasonable to assume that each transmitter is selfish. Furthermore, each transmitter i is rational and intelligent, i.e., its objective is to find the best strategy s_i to maximize corresponding payoff π_i (given the other transmitter's strategy s_j), and each transmitter understands the situation, including the fact that another transmitter is also an intelligent rational decision maker.

Based on the above consideration and assumptions, the definition of the Nash equilibrium secrecy rate region $C_{s,NE}$ is given as follows:

Definition 2 (Nash equilibrium secrecy rate region) *Nash equilibrium secrecy rate region $C_{s,NE}$ is the closure of all rate pairs (R_{s1}, R_{s2}) such that, there exists a $\bar{\epsilon} > 0$ such that for all $\epsilon \in (0, \bar{\epsilon})$, there exists a strategy pair (s_1^*, s_2^*) which achieves the payoffs $\pi_i(s_1^*, s_2^*) = R_{si}$ for $i = 1, 2$ and s_i^* is the best response to s_j^* in the sense that*

$$\pi_i(s_i^*, s_j^*) \geq \pi_i(s_i', s_j^*), \quad \forall s_i' \tag{3}$$

By this definition, if any transmitter i unilaterally attempts to deviate from the equilibrium strategy while the other transmitter j's strategy remains the same, the corresponding payoff π_i of transmitter-receiver pair i will not be improved, i.e., there is no incentive for each transmitter to deviate from the equilibrium strategy. Such a secrecy rate pair achieved by the best response strategy pair is an equilibrium in the secrecy rate region.

III. Binary Deterministic Channels with Confidential Messages

In this section, we consider the binary deterministic one-sided interference channel with confidential messages to analyze the Nash equilibrium secrecy rate region with the payoff function defined above. The channel model shown in Fig. 2 is:

$$Y_{1a} = X_{1a}, \qquad Y_{1b} = X_{1b} \tag{4}$$

$$Y_{2a} = X_{1b} \oplus X_{2a}, \quad Y_{2b} = X_{2b} \tag{5}$$

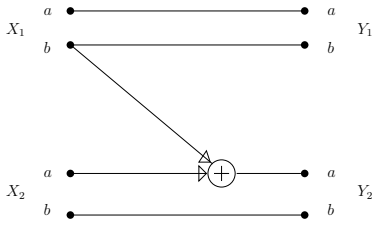

Fig. 2. Binary deterministic one-sided interference channel with confidential messages.

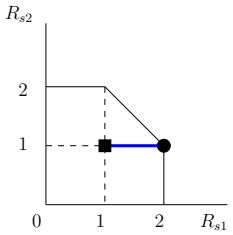

Fig. 3. The (secrecy) capacity region. Unique Nash equilibrium point (filled circle) and Nash equilibrium secrecy rate region (blue wide line including the two end points) with the first payoff function, and the unique Nash equilibrium secrecy rate point (filled square) for the second payoff function.

where $\oplus$ is modulo-2 addition. This is a simple example to analyze the equilibrium. However, it is not difficult to see that it could be easily extended to the general one-sided binary deterministic channel which was used in [12].

Based on the capacity results of deterministic interference channels [1], the capacity region of this channel is the following region

$$C = \{(R_1, R_2) | R_1 \leq 2, R_2 \leq 2, R_1 + R_2 \leq 3\} \tag{6}$$

In fact, it is also easy to check to see that each corner point of this pentagon is an achievable *secrecy* rate pair also, and therefore, the unconstrained capacity region is equal to the secrecy capacity region. In addition, if we do not consider the secrecy constraint L_i in the payoff function, then [6] already found the unique Nash equilibrium rate pair (R_1^*, R_2^*) to be $R_1^* = 2$ and $R_2^* = 1$. The explanation for this is the following: Since there is no secrecy constraint, transmitter 1 can always transmit unencoded messages on both sub-channels with maximum rate 2 bits, and due to the interference, transmitter 2 can only achieve 1 bit as the maximum rate. It can be shown that neither user will have any incentive to deviate from this point, and there exists no other such point. The capacity region is shown in Fig. 3. The unique Nash equilibrium with no secrecy constraints is shown with a filled circle.

With secrecy constraints, we will show that the Nash equilibrium secrecy rate region is not a unique point. We give the precise form of the Nash equilibrium secrecy rate region of this channel with the following theorem.

Theorem 1 (Nash equilibrium secrecy rate region $C_{s,NE}$)

$$C_{s,NE} = \{(R_{s1}, R_{s2}) | R_{s1} \in [1, 2], R_{s2} = 1\} \tag{7}$$

Proof: First, note that $R_{s1} \geq 1$ and $R_{s2} \geq 1$. This is because, given any strategy s_2, transmitter 1 can at least employ independent encoding on two sub-channels and transmit unencoded information on sub-channel a with zero decoding error probability and without any information leakage. The same argument can be applied to sub-channel b of transmitter 2. Next, note that $R_{s1} \leq 2$ is trivial. To prove $R_{s2} = 1$, it suffices to prove that $R_{s2} \leq 1$.

Assume that (s_1, s_2) is an equilibrium strategy, which is the best response to each other and public to both transmitter-receiver pairs. The reliable transmission rate for transmitter 2 is upper bounded by

$$\begin{aligned} nR_{s2} &= nR_2 && (8)\\ &\leq \max_{P(X_2^n)} I(X_2^n; Y_2^n) && (9)\\ &\leq \max_{P(X_2^n)} [I(X_{2a}^n; Y_{2a}^n) + H(X_{2b}^n)] && (10) \end{aligned}$$

where the inequality in (10) is proved in Appendix with $X_{2b} = Y_{2b}$. This could always (but not limited to) be achieved by independently encoding on both sub-channels. The necessary condition for the equality in (10) is

$$I(Y_{2a}^n; X_{2b}^n) = 0 \tag{11}$$

Considering s_1, the channel $X_1 \to Y_1, Y_2$ is a degraded wiretap channel with the following upper bound for the secrecy rate:

$$nR_{s1} \leq \max_{P(X_1^n)} I(X_1^n; Y_1^n) - I(X_1^n; Y_2^n) \tag{12}$$

The difference can be maximized by

$$\begin{aligned} &I(X_1^n; Y_1^n) - I(X_1^n; Y_2^n)\\ &\leq H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_1^n; Y_2^n) && (13)\\ &= H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_{1a}^n, X_{1b}^n; Y_2^n) && (14)\\ &= H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n)\\ &\quad - I(X_{1b}^n; Y_2^n) - I(X_{1a}^n; Y_2^n | X_{1b}^n) && (15)\\ &= H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_{1b}^n; Y_2^n) && (16)\\ &= H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n)\\ &\quad - I(X_{1b}^n; Y_{2a}^n) - I(X_{1b}^n; Y_{2b}^n | Y_{2a}^n) && (17) \end{aligned}$$

where (13) is proven in Appendix with $X_{1a} = Y_{1a}$, (16) is due to the Markov chain $X_{1a}^n \to X_{1b}^n \to Y_2^n$. The fourth item in (17) is equal to

$$\begin{aligned} I(X_{1b}^n; Y_{2b}^n | Y_{2a}^n) &= H(Y_{2b}^n | Y_{2a}^n) - H(Y_{2b}^n | X_{1b}^n, Y_{2a}^n) && (18)\\ &= H(X_{2b}^n | Y_{2a}^n) - H(X_{2b}^n | X_{1b}^n, Y_{2a}^n) && (19)\\ &= H(X_{2b}^n) - H(X_{2b}^n | X_{1b}^n, Y_{2a}^n) && (20)\\ &= H(X_{2b}^n) - H(X_{2b}^n | X_{2a}^n, Y_{2a}^n) && (21)\\ &= H(X_{2b}^n) - H(X_{2b}^n | X_{2a}^n) && (22)\\ &= I(X_{2a}^n; X_{2b}^n) && (23) \end{aligned}$$

where (20) is due to (11) and (22) is due to the Markov chain

$X_{2b}^n \to X_{2a}^n \to Y_{2a}^n$. Substituting (23) in (17), we get

$$\begin{aligned}
&I(X_1^n;Y_1^n) - I(X_1^n;Y_2^n) \\
&\quad \le H(X_{1a}^n) + I(X_{1b}^n;Y_{1b}^n) \\
&\qquad - I(X_{1b}^n;Y_{2a}^n) - I(X_{2a}^n;X_{2b}^n) && (24)\\
&\quad = H(X_{1a}^n) + H(X_{1b}^n) - H(Y_{2a}^n) \\
&\qquad + H(Y_{2a}^n|X_{1b}^n) - I(X_{2a}^n;X_{2b}^n) && (25)\\
&\quad = H(X_{1a}^n) + H(X_{1b}^n) - H(Y_{2a}^n) \\
&\qquad + H(X_{2a}^n) - I(X_{2a}^n;X_{2b}^n) && (26)\\
&\quad = H(X_{1a}^n) + H(X_{1b}^n|X_{2a}^n) - H(Y_{2a}^n) + H(X_{2a}^n|X_{2b}^n) && (27)\\
&\quad = H(X_{1a}^n) + H(Y_{2a}^n|X_{2a}^n) - H(Y_{2a}^n) + H(X_{2a}^n|X_{2b}^n) && (28)\\
&\quad = H(X_{1a}^n) - I(X_{2a}^n;Y_{2a}^n) + H(X_{2a}^n|X_{2b}^n) && (29)\\
&\quad \le H(X_{1a}^n) + H(X_{2a}^n|X_{2b}^n) && (30)\\
&\quad \le n + H(X_{2a}^n|X_{2b}^n) && (31)
\end{aligned}$$

where (26) is due to $H(Y_{2a}^n|X_{1b}^n) = H(X_{2a}^n|X_{1b}^n) = H(X_{2a}^n)$ and (30) is due to $I(X_{2a}^n;Y_{2a}^n) \ge 0$. When s_2 is given, $H(X_{2a}^n|X_{2b}^n)$ is a fixed item for transmitter 1. (31) could always (but not limited to) be achieved by a wiretap code with independent and uniform distributions for X_{1a}^n and X_{1b}^n. The necessary condition is

$$I(X_{2a}^n;Y_{2a}^n) = 0 \tag{32}$$

which means that, under the condition that transmitter 1 achieves the maximum secrecy rate, the upper bound for the reliable transmission rate (10) for transmitter 2 is only

$$\begin{aligned}
nR_{s2} &\le \max_{P(X_2^n)} [I(X_{2a}^n;Y_{2a}^n) + H(X_{2b}^n)] && (33)\\
&\le \max_{P(X_2^n)} H(X_{2b}^n) && (34)\\
&\le n && (35)
\end{aligned}$$

which is achievable. Therefore, the reliable secrecy rate R_{s2} is upper bounded by 1.

Finally, we prove the achievability here. Assume that s_2 is the following: transmit unencoded information on sub-channel b, but pure noise with input distribution $P(X_{2a}=0) = 1 - P(X_{2a}=1) = p$, for some $0 \le p \le 1/2$ on sub-channel a. Then, $R_{s2} = 1$.

Given s_2, the channel $X_1 \to Y_1 \to Y_2$ is a degraded wiretap channel with the optimal encoder s_1^* which independently encodes the signals on two sub-channels. On sub-channel a, unencoded message is transmitted, and on sub-channel b, encoder transmits the secure message via a wiretap code with the optimal distribution $P^*(X_{1b}=0) = 1/2$. It is straightforward to see that s_1^* and s_2 jointly determine the achievable secrecy rate for transmitter 1 as $R_{s1a} + R_{s1b} = 1 + I(X_{1b};Y_{1b}) - I(X_{1b};Y_{2a}) = 1 + \{1 - [1 - h_2(p)]\} = 1 + h_2(p)$, where h_2 is the binary entropy function.

It is easy to check that, to maximize the payoff π_2, s_2 is also the best response s_2^* to s_1^*, i.e., (s_1^*, s_2^*) are best responses to each other, and therefore form an equilibrium, by definition. Then, the corresponding payoffs are

$$R_{s1} = 1 + h_2(p), \quad R_{s2} = 1 \tag{36}$$

where $0 \le p \le 1/2$, which means $R_{s1} \in [1,2]$ and $R_{s2} = 1$. The Nash equilibrium line is shown as the blue line going from $[1,1]$ to $[2,1]$ in Fig. 3. ■

IV. Refinement of the Equilibrium

Achieving the Nash equilibrium pairs in the previous section required transmitter 2 to transmit artificial noise on sub-channel a to self-jam its own receiver. Since all of the equilibrium points yield the same payoff for pair 2, a rational transmitter 2 would rather help its receiver eavesdrop on the other pair than self-jam its own receiver. However, the self-jamming scheme is not excluded by the Nash equilibrium in Section III.

We now modify the payoff function of the game in order for the resulting Nash equilibrium to reflect the adversarial relationship between the two pairs of user better in this interference channel with confidential messages. Here we explicitly account for the desire of the receiver to eavesdrop on the other party's communication by including the leakage of the other user's message in the payoff function of a user together with its own secret rate.

Definition 3 (Refinement of the game and equilibria) *The equilibrium secrecy rate region $\tilde{C}_{s,NE}$ is the closure of all rate pairs (R_{s1}, R_{s2}) such that there exists a $\bar{\epsilon} > 0$ such that for all $\epsilon \in (0, \bar{\epsilon})$, there exists a strategy pair (s_1^*, s_2^*) which achieves the payoffs $\pi_i(s_1^*, s_2^*) = R_{si}$ for $i = 1, 2$, and s_i^* is the best response to s_j^* in the sense that*

$$\pi_i(s_i^*, s_j^*) \ge \pi_i(s_i', s_j^*), \quad \forall s_i' \tag{37}$$

In addition, (s_1^*, s_2^*) is also the best responses with respect to the following payoff

$$\tilde{\pi}_i(s_i, s_j) = \begin{cases} R_i + \beta \cdot L_j, & P_{e,i} \le \epsilon \text{ and } L_i \le \epsilon \\ 0, & \text{otherwise} \end{cases} \tag{38}$$

for any $\beta > 0$ and for all $i = 1, 2$ with $j = \bar{i}$.

We emphasize a few points here. First, any rate pair in $\tilde{C}_{s,NE}$ must also belong to $C_{s,NE}$. Secondly, we include the information leakage L_j defined in (1) into the definition of $\tilde{\pi}_i$ in addition to the R_i to further limit the rational behavior of the selfish transmitters and receivers, i.e., eavesdropping is at least not bad for the receiver. Lastly, for any rate pair $(R_{s1}, R_{s2}) \in \tilde{C}_{s,NE}$, by the definition of payoff π, there must exist a strategy pair which does not violate the secrecy constraint even though it is also an equilibrium with respect to the payoff $\tilde{\pi}$, which includes the information leakage in the definition.

We again examine the channel in Section III to illustrate the idea of the refined payoff function and the resulting equilibrium. With the new definition, the equilibrium rate pairs in the secrecy rate region are modified as stated in the following theorem.

Theorem 2 (Nash equilibrium secrecy rate region $\tilde{C}_{s,NE}$)

$$\tilde{C}_{s,NE} = \{(1,1)\} \tag{39}$$

Proof: $(1,1) \in \tilde{C}_{s,NE}$. This is because each transmitter transmits unencoded information on the private sub-channel, e.g., sub-channel a of transmitter 1 and sub-channel b of transmitter 2. Transmitter 1 sends pure noise with uniform distribution on sub-channel b. Transmitter 2 keeps silent. Here by silence, we mean that transmitter 2 sends a constant symbol which is known to everyone in this network, i.e., the corresponding rate is zero. Since no information is transmitted on the interfered sub-channel, there is no information leakage which implies that $(1,1) \in \tilde{C}_{s,NE}$.

$(2,1) \notin \tilde{C}_{s,NE}$. The only scheme to achieve this rate pair is that transmitter 1 transmits unencoded information on both sub-channels as s_1. And, for s_2 transmitter 2 transmits unencoded information on sub-channel b but sends pure noise (uniform distribution) on sub-channel a. Obviously, if transmitter 2 deviates from s_2 to one special strategy s_2' which keeps silent on sub-channel a, then the payoff $\tilde{\pi}_2$ will increase due to the information leakage L_1.

$(R_{s1},1) \notin \tilde{C}_{s,NE}$ for any $R_{s1} > 1$. We prove this by contradiction. Assume that this rate pair is in the set $\tilde{C}_{s,NE}$ and is achieved by some strategy pair (s_1, s_2). $R_{s1} > 1$ means that $H(W_1) \geq n(1+\triangle)$ for a positive constant value $\triangle > 0$. It is not difficult to see that transmitter 2 could always deviate to s_2', i.e., keeping silent on sub-channel a, then the secrecy rate R_{s2} remains the same but the information leakage increases:

$$\begin{aligned}
nL_1 &= I(W_1; Y_2^n) = I(W_1; Y_{2a}^n) && (40)\\
&= I(W_1; X_{1b}^n) && (41)\\
&= I(W_1; Y_{1b}^n) && (42)\\
&= I(W_1; Y_{1a}^n, Y_{1b}^n) - I(W_1; Y_{1a}^n | Y_{1b}^n) && (43)\\
&= H(W_1) - H(W_1 | Y_{1a}^n, Y_{1b}^n) - I(W_1; Y_{1a}^n | Y_{1b}^n) && (44)\\
&\geq H(W_1) - I(W_1; Y_{1a}^n | Y_{1b}^n) - n\epsilon' && (45)\\
&\geq n(1+\triangle) - H(Y_{1a}^n) - n\epsilon' && (46)\\
&\geq n(\triangle - \epsilon') && (47)
\end{aligned}$$

where by Fano's inequality, $H(W_1|Y_{1a}^n, Y_{1b}^n) \leq n\epsilon'$ for some negligible ϵ'. Hence, the payoff $\tilde{\pi}_2(s_1, s_2') = R_{s2} + \beta L_1 > R_{s2} = \tilde{\pi}_2(s_1, s_2)$ which means that s_2 is not the best response to s_1 with respect to $\tilde{\pi}$, which implies that $(R_{s1}, 1) \notin \tilde{C}_{s,NE}$.

Therefore, we conclude that the Nash equilibrium contains only a single rate pair: $\tilde{C}_{s,NE} = \{(1,1)\}$, which is shown with the filled square in Fig. 3. ■

This theorem shows that all the secrecy rate pairs in the set $C_{s,NE}$ but not in the set $\tilde{C}_{s,NE}$ are only achieved by the strategies employing self-jamming. The modified definition for the payoff and the resulting equilibrium are essential to rule out such rate pairs.

V. Conclusions

In this paper, we studied the one-sided interference channel with confidential messages. To model the adversarial relationship between two transmitter-receiver pairs, we considered a scenario where each transmitter has the freedom to choose any strategy, and the only objective is to maximize a certain given payoff. To this end, we formally developed a game theory model and studied its equilibria. When we defined the payoff function to be only the secrecy rate of each user, the resulting Nash equilibria did not reject the behavior of self-jamming, in which a transmitter jams its own receiver. To improve the modeling of the adversarial relationship between the two pairs better, we defined a refined payoff function to explicitly incorporate the receiver's desire to eavesdrop on the other user. The equilibrium achieved with this payoff function excluded the possibility of self-jamming, for the deterministic binary channel considered here.

Appendix

For independent parallel channel $P(Y_\alpha, Y_\beta | X_\alpha, X_\beta) = P(Y_\alpha|X_\alpha)P(Y_\beta|X_\beta)$ with $Y_\beta = X_\beta$, the upper bound of the mutually information $I(X;Y)$ is the following:

$$\begin{aligned}
I(X;Y) &= I(X_\alpha, X_\beta; Y_\alpha, Y_\beta) && (48)\\
&= I(X_\beta; Y_\alpha, Y_\beta) + I(X_\alpha; Y_\alpha, Y_\beta | X_\beta) && (49)\\
&= H(X_\beta) + I(X_\alpha; Y_\alpha | X_\beta) && (50)\\
&= H(X_\beta) + H(Y_\alpha|X_\beta) - H(Y_\alpha|X_\alpha, X_\beta) && (51)\\
&\leq H(X_\beta) + H(Y_\alpha) - H(Y_\alpha|X_\alpha, X_\beta) && (52)\\
&= H(X_\beta) + H(Y_\alpha) - H(Y_\alpha|X_\alpha) && (53)\\
&= H(X_\beta) + I(X_\alpha; Y_\alpha) && (54)
\end{aligned}$$

where the (53) is due to the Markov chain $X_\beta \to X_\alpha \to Y_\alpha$. The equality holds iff $I(Y_a; X_\beta) = 0$.

References

[1] A. El Gamal and M. Costa, "The capacity region of a class of deterministic interference channels," *IEEE Trans. Inf. Theory*, vol. 28, no. 2, pp. 343–346, 1982.

[2] A. B. Carleial, "A case where interference does not reduce capacity," *IEEE Trans. Inf. Theory*, vol. 21, no. 5, pp. 569–570, 1975.

[3] H. Sato, "On the capacity region of a discrete two-user channel for strong interference," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 377–379, 1978.

[4] ——, "The capacity of the gaussian interference channel under strong interference," *IEEE Trans. Inf. Theory*, vol. 27, no. 6, pp. 786–788, 1981.

[5] N. Liu and S. Ulukus, "The capacity region of a class of discrete degraded interference channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4372–4378, 2008.

[6] R. A. Berry and D. Tse, "Shannon meets nash on the interference channel," submitted to *IEEE Transactions on Information Theory* 2010. Also available at [arXiv:1007.1756].

[7] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[8] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[9] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July, 1978.

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

[11] R. D. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," *IEEE ISIT*, 2008.

[12] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," *IEEE ISIT*, 2008.