An Eavesdropping Game with SINR as an Objective Function

Andrey Garnaev[1] and Wade Trappe[2]

[1] St. Petersburg State University, Russia
agarnaev@rambler.ru
[2] WINLAB, Rutgers University, USA
trappe@winlab.rutgers.edu

Abstract. We examine eavesdropping over wireless channels, where secret communication in the presence of an eavesdropper is formulated as a zero-sum game. In our problem, the legitimate receiver does not have complete knowledge about the environment, i.e. does not know the exact values of the channels gains, but instead knows just their distribution. To communicate secretly, the user must decide how to transmit its information across subchannels under a worst-case condition and thus, the legal user faces a max-min optimization problem. To formulate the optimization problem, we pose the environment as a secondary player in a zero-sum game whose objective is to hamper communication by the user. Thus, nature faces a min-max optimization problem. In our formulation, we consider signal-to-interference ratio (SINR) as a payoff function. We then study two specific scenarios: (i) the user does not know the channels gains; and (ii) the user does not know how the noise is distributed among the main channels. We show that in model (i) in his optimal behavior the user transmits signal energy uniformly across a subset of selected channels. In model (ii), if the user does not know the eavesdropper's channel gains he/she also employs a strategy involving uniformly distributing energy across a subset of channels. However, if the user acquires extra knowledge about environment, e.g. the eavesdropper's channel gains, the user may better tune his/her power allocation among the channels. We provide criteria for selecting which channels the user should transmit on by deriving closed-form expressions for optimal strategies for both players.

1 Introduction

Security is one of the most prominent problems surrounding wireless communications, largely due to the broadcast nature of the wireless medium, which facilitates eavesdropping. Although much of the work in confidentiality for wireless systems has focused on cryptographic solutions, which necessitate key management, there has been a recent movement towards exploring new security mechanisms for wireless systems. There has been an effort by the wireless research community to develop new forms of confidential communication that

Y. Chen et al. (Eds.): SecureComm 2009, LNICST 19, pp. 142–162, 2009.

exploit the fading characteristics of the wireless channel to achieve secret communications through appropriate coding constructions[1,2,3,4,6,7]. Such work has largely built upon prior information-theoretic work of [8,9,10,11], where the notion of secrecy capacity was introduced to describe the rate at which a sender could communicate in an information-theoretically confidential manner in the presence of an eavesdropper. Recent results have sought to incorporate modern communication system design, and take advantage of the many degrees of freedom available in a dynamic wireless fading environment. For example, it is possible to use multiple subcarriers in order to provide a large number of parallel subchannels, as is utilized in OFDM transceivers (which is becoming a de facto physical layer strategy for many existing and emerging wireless systems, including 802.11g and WiMax), and the underlying frequency selectivity induced by multipaths can provide a diversity advantage. Recent results related to secret communication over independent, parallel channels has been reported in [4,5].

In the basic formulation of confidential communication, we have three entities: Alice, Bob and Eve. Alice seeks to communicate secretly with Bob while in the presence of an eavesdropper Eve. In this formulation, there are two sets of channels of interest, first is the channel from Alice to Bob, and second is the channel from Alice to Eve. Using G as a generic representation for the Alice to Bob channel, and H as a generic representation for the Alice to Eve channel, a natural question that arises is how secret communication rates can be characterized under different assumptions regarding which entities know the states of various channel states. The results of [4], for example, were formulated for the case of complete channel state information where Alice, Bob and Eve all have perfect knowledge of the CSI for channels G and H. For complete CSI it has been shown that the secrecy capacity for a collection of independent parallel channels can be solved through appropriate water-filling of the channel differences between G and H.

Unfortunately, the case of complete CSI is not representative of what one would expect to face in an adversarial setting, where the eavesdropper is not likely to reveal its presence. Instead, incomplete CSI cases are more appropriate but, for the most part, have not been considered in the literature. Generally, it is reasonable to assume that the receiver has knowledge of the state of the channel from the transmitter. Hence, we are interested in cases where Alice does not have complete knowledge of G or H. In this paper, we examine the problem of secret communication over fading channels for several specific cases of incomplete CSI.

To address the problem of how the sender can best communicate secretly to a legitimate receiver while having varying levels of knowledge about the corresponding channel states, we formulate the problem of secret communication as a zero-sum game. Here, the user must decide how to transmit information across which subchannels under a worst-case condition, while we pose the environment as a secondary player in a zero-sum game whose objective is to hamper successful communication by the user. We consider signal-to-interference ratio (SINR) as a payoff function since, in the regime of low SINR, this objective is an approximation to the secrecy rate.

We begin the paper in Section 2 by presenting our three entities (Alice, Bob and Eve), and providing a description of the basic communication model that we will use throughout this paper. In the sections that follow, we examine several distinct cases where different assumptions are placed on how well Alice or Eve know the channel gains. Throughout the paper we present conclusions that can be drawn from theoretically formulating the eavesdropping problem in a game-theoretic scenario. We provide proofs in the Appendix.

2 Problem Overview

Alice seeks to communicate secretly with Bob, while in the presence of a potential (passive) eavesdropper, Eve. We consider a communication system involving n independent subchannels, as might arise in an OFDM system. Letting Alice's transmitted signal on channel i be X_i, then Bob's received signal is

$$Y_i = \sqrt{g_i} X_i + W_i^{AB}, \tag{1}$$

while Eve receives the signal

$$Z_i = \sqrt{h_i} X_i + W_i^{AE}. \tag{2}$$

We may collect Alice's channel input as $X^n = [X_1, \cdots, X_n]$, and similarly define Bob's received signals as Y^n, and Eve's as Z^n. In the communication literature, the channel gains g_i and h_i may follow many different distributions and one of the most common is the Rayleigh fading model, where g_i and h_i follow an exponential distribution with an average channel gain $E[g_i]$ or $E[h_i]$ capturing distance-dependent attenuation and shadowing. In general the Alice-to-Bob channel and Alice-to-Eve channel will have different average characteristics, i.e. in general $E[g_i] \neq E[h_i]$. Further, we note that the W_i^{AB} and W_i^{AE} are additive noise terms that (unless noted otherwise) have been normalized appropriately (relative to the main Alice-to-Bob channel gains g_i) to have unit variance.

In [4], it was shown under the complete CSI assumption, that the secrecy capacity of the system of n independent channels for Alice-Bob-Eve can be expressed as $\mathcal{C}_n(\mathbf{g}, \mathbf{h}, \mathbf{P}^*) = \sum_{i=1}^n \mathcal{C}_{AWGN}(g_i, h_i, P_i)$, where $\mathcal{C}_{AWGN}(g_i, h_i, P_i)$ is the secrecy capacity for an additive white Gaussian noise channel model, and was given by Leung-Yan-Cheong and Hellman in [13]. Further, $\mathbf{P}^*$ is the optimal power allocation across the n subchannels and corresponds to waterfilling appropriately by considering the relative differences between $\mathbf{g}$ and $\mathbf{h}$.

3 Optimization with SINR as the Objective Function

In this section, we formulate the secret communication problem as an optimization problem. As noted earlier, Alice would like to transmit information through n channels, and to do this she must allocate power $P = (P_1, \dots, P_n)$ across these channels, where

$$P_i \geq 0 \text{ for } i \in [1, n] \tag{3}$$

and

$$\sum_{i=1}^{n} P_i = \bar{P}. \tag{4}$$

Here $\bar{P} > 0$ denotes the signal total power budget she may transmit. Up to a normalization factor, Alice's payoff is given as follows

$$v(P) = \sum_{i=1}^{n} \Big[\ln(1 + g_i P_i) - \ln(1 + h_i P_i)\Big]_+ \tag{5}$$

where g_i and h_i are the corresponding fading channel gains of the main (Alice to Bob) and eavesdropper (Alice to Eve) channels. The individual secrecy rate terms $\ln(1 + g_i P_i) - \ln(1 + h_i P_i)$ are generally unwieldy, and as a useful approximation, we may instead define a more convenient payoff function, which we shall refer to as the SINR payoff. The SINR payoff for Alice is given as follows

$$v(P) = \sum_{i=1}^{n} g_i P_i - \sum_{i=1}^{n} h_i P_i. \tag{6}$$

SINR has been considered in non-eavesdropping communication scenarios. Specifically, it has been used as an objective function in the power control game in [16], [17] and [15]. In [16], the Braess paradox in the context of the power control game has been studied and in [17] all users have a single common channel and choose between several base stations, while in [15] jamming and cooperative scenarios are considered. Lastly, we note that in the regime of low SINR the present objective serves as an approximation to the secrecy rate.

Since the payoff is linear in P the optimal power strategy assigns transmission power across the channels by placing a preference to channels with greater difference between the channel gains of the main and eavesdropper channels, $g_i - h_i$. Namely, the following result holds.

Theorem 1. *The optimal power allocation strategy, P, for Alice for the secret communication optimization problem with SINR as the payoff, under condition (3) and (4), is given as follows*

$$P_i \begin{cases} = 0 & \text{for } i \in [1, n] \backslash I_*, \\ \geq 0 \text{ such that } \sum_{i \in I_*} P_i = \bar{P} & \text{for } i \in I_*, \end{cases}$$

where $I_* = \{i \in [1, n] : g_i - h_i = \max\{g_j - h_j : j \in [1, n]\}\}$ is the maximal difference between fading channel gains of the main (Alice to Bob) and eavesdropper (Alice to Eve) channels. The payoff corresponding to this strategy is $v = \bar{P} \max\{g_j - h_j : j \in [1, n]\}$.

Now look at the problem assuming that Alice has fixed the power allocation, i.e. the vector $P = (P_1, \ldots, P_n)$ satisfying (3) and (4), yet the environmental parameters are not completely known, i.e. Alice does not know the exact values of the channels gains. To capture this assumption, we shall further assume that Alice knows the best case scenario for the main and eavesdropper channel gains, but does not know the precise values of any instantaneous realization. Hence, we assume that the gains g_i for the main subchannel i is given by

$$g_i = g_i^0 - G_i, \tag{7}$$

where g_i^0 is the best possible channel gain, and G_i reflects additional degradation of the channel that might arise from fading or other factors. For analysis, we assume that Alice knows that the degradation G_i is such that

$$G_i \geq 0 \text{ for } i \in [1, n] \tag{8}$$

and that she knows an (ensemble) characterization of this degradation across all n subchannels

$$\sum_{i=1}^{n} G_i = \bar{G}, \tag{9}$$

where $\bar{G} > 0$ thus corresponds to the total main channel perturbation.

Similarly, we assume that Alice has imprecise knowledge of the gains of the eavesdropper subchannel i, given by

$$h_i = h_i^0 + H_i, \tag{10}$$

where h_i^0 is (best, and hence smallest) possible channel gain and is known to the user. However, as before, about the perturbation of this channel gain, H_i, she knows only that it is such that

$$H_i \geq 0 \text{ for } i \in [1, n] \tag{11}$$

and

$$\sum_{i=1}^{n} H_i = \bar{H}, \tag{12}$$

where $\bar{H} > 0$ is the total eavesdropper's channels perturbation known to Alice.

The payoff is then given as follows

$$\begin{aligned} v((G, H)) &= \sum_{i=1}^{n} (g_i^0 - G_i) P_i - \sum_{i=1}^{n} (h_i^0 + H_i) P_i \\ &= \sum_{i=1}^{n} \xi_i^0 P_i - \sum_{i=1}^{n} (G_i + H_i) P_i, \end{aligned} \tag{13}$$

where ξ_i is the difference between fading channel gains of the main (Alice to Bob) and eavesdropper (Alice to Eve) channels i, namely,

$$\xi_i^0 = g_i^0 - h_i^0, \quad i \in [1, n]. \tag{14}$$

We will assume that $g_i^0 > h_i^0$ for $i \in [1, n]$, so $\xi_i^0 > 0$ for $i \in [1, n]$. The following result allows Alice to quantify the worst payoff she could have, as she would like to minimize (13) for any admissible (G, H).

Theorem 2. *Let $I_{max} = \{i \in [1,n] : P_i = P_{max}\}$ where $P_{max} = \max_{j \in [1,n]} P_j$. Then the optimal strategy (G, H) is given as follows*

$$G_i \begin{cases} = 0, & i \in [1,n] \backslash I_{max}, \\ \geq 0 \text{ such that } \sum_{j \in I_{max}} G_j = \bar{G}, & i \in I_{max}, \end{cases} \tag{15}$$

$$H_i \begin{cases} = 0, & i \in [1,n] \backslash I_{max}, \\ \geq 0 \text{ such that } \sum_{j \in I_{max}} H_j = \bar{H}, & i \in I_{max}. \end{cases} \tag{16}$$

The payoff corresponding to this strategy is $v = \sum_{i=1}^{n} \xi_i^0 P_i - P_{max}(\bar{G} + \bar{H})$.

4 An Eavesdropping Game with Unknown Gains

We continue our analysis of the situation where Alice does not know the exact values of the channels gains, as described previously. Alice faces the problem of allocating power so that information can be transmitted under the worst-case conditions or, in other words, Alice faces a maxmin problem. To address this question we draw upon game theory since we may consider Alice as a player in a game, while we may model the environment (nature) as a second player with a goal opposite to Alice's, namely, to hamper information transmission by Alice (by selecting channel states so as to benefit the eavesdropper Eve)[1]. Thus, nature faces a minmax problem and the optimal strategies of the players for the maxmin and minmax problems will coincide with each other.

We assume that the gains of the main channel i is given by (7) and the gains of the eavesdropper channel i is given by (10). The strategy for the environment is governed by appropriately selecting (G, H), which consists of two components: $G = (G_1, \dots, G_n)$ – the main channel's degradations about g; and $H = (H_1, \dots, H_n)$ – the eavesdropper's channel degradations about h, as per the conditions (8), (9) and (11), (12). Alice's P is given by satisfying (3) and (4). The SINR payoff for Alice is given as follows

$$v(P, (G, H)) = \sum_{i=1}^{n} (g_i^0 - G_i) P_i - \sum_{i=1}^{n} (h_i^0 + H_i) P_i. \tag{17}$$

Both players know the values of g_i^0, h_i^0, $i \in [1,n]$ as well as $\bar{P}$, $\bar{G}$ and $\bar{H}$. We consider the situation as a zero-sum game Alice versus nature with Alice's payoff as (36), while the payoff to nature is $-v(P, (G, H))$.

We will look for the value of the game v and the optimal strategies P^* of Alice and (G^*, H^*) for nature. Recall that optimal strategies and the value of the game satisfy the conditions:

$$v(P, (G^*, H^*)) \leq v := v(P^*, (G^*, H^*)) \leq v(P^*, (G, H))$$

for any strategies P and (G, H) for the players (Alice and nature).

[1] We note, contrary to intuition, Eve is not the second player in our formulation, but is a passive beneficiary of the strategy employed by the environment.

Note that the payoff (17) of the game by (14) can be rewritten in the following equivalent form

$$v(P,(G,H)) = \sum_{i=1}^{n} \xi_i^0 P_i - \sum_{i=1}^{n}(G_i + H_i)P_i. \tag{18}$$

Without loss of generality we can assume that the channels are arranged in such a way that

$$\xi_1^0 \geq \xi_2^0 \geq \ldots \geq \xi_n^0 > 0. \tag{19}$$

We introduce the following auxiliary notation,

$$\varphi_k := \sum_{i=1}^{k}(\xi_i^0 - \xi_k^0) \text{ for } k \in [1,n]. \tag{20}$$

It is clear that the sequence φ_k, $k \in [1,n]$ is increasing since the following relations hold:

$$\varphi_{k+1} - \varphi_k = \sum_{i=1}^{k+1}(\xi_i^0 - \xi_{k+1}^0) - \sum_{i=1}^{k}(\xi_i^0 - \xi_k^0) = (\xi_k^0 - \xi_{k+1}^0)k \geq 0,$$

and $\varphi_1 = 0$. For this game we can prove the following result describing the optimal strategies as well as the value of the game.

Theorem 3. *(a) Let*

$$\bar{G} + \bar{H} \geq \varphi_n, \tag{21}$$

then the value of the game is given by

$$v = \frac{\bar{P}}{n}\left(\sum_{i=1}^{n}\xi_i^0 - \bar{G} - \bar{H}\right). \tag{22}$$

Alice's optimal strategy P^* assigns power uniformly across all the n channels, i.e.

$$P_i^* = \bar{P}/n \text{ for } i \in [1,n]. \tag{23}$$

Nature's optimal strategy (G^*, H^*), meanwhile, involves assigning the eavesdropper and main channel components H^* and G^* to equalize the difference in quality between the fading channel gains of the main (Alice to Bob) and eavesdropper (Alice to Eve) channels, namely, H^* satisfies (11) and (12), G^* satisfies (8) and (9) and

$$G_i^* + H_i^* = \frac{1}{n}\left(\bar{H} + \bar{G} - \sum_{j=1}^{n}(\xi_j^0 - \xi_i^0)\right), \tag{24}$$

say,

$$G_i^* = \frac{\bar{G}}{n(\bar{G}+\bar{H})}\left(\bar{H} + \bar{G} - \sum_{j=1}^{n}(\xi_j^0 - \xi_i^0)\right), \tag{25}$$

$$H_i^* = \frac{\bar{H}}{n(\bar{G}+\bar{H})}\left(\bar{H}+\bar{G}-\sum_{j=1}^{n}(\xi_j^0-\xi_i^0)\right) \tag{26}$$

for $i \in [1, n]$.

(b) Let

$$\bar{G}+\bar{H} < \varphi_n.$$

Then, there is a $k_* \in [1, n-1]$ *such that*

$$\varphi_{k_*} \le \bar{G}+\bar{H} < \varphi_{k_*+1}. \tag{27}$$

The value of the game is given as follows

$$v = \frac{\bar{P}}{k_*}\left(\sum_{i=1}^{k_*}\xi_i^0 - \bar{G} - \bar{H}\right).$$

Alice's optimal strategy P^* *assigns power equally among the first* k_* *channels, i.e.*

$$P_i^* = \begin{cases} \bar{P}/k_* & \text{for } i \in [1, k_*], \\ 0 & \text{for } i \in [k_*+1, n]. \end{cases} \tag{28}$$

Nature's optimal strategy (G^*, H^*) *assigns* G^* *only to the main channel components unused by Alice, while* H^* *and* G^* *are assigned across the eavesdropper's subchannels so as to equalize the* k_* *best differences in quality between fading channel gains of the main (Alice to Bob) and eavesdropper (Alice to Eve) channels. Namely,* H^* *satisfies (11) and (12),* G^* *satisfies (8) and (9),*

$$G_i^* = H_i^* = 0 \text{ for } i \in [k_*+1, n] \tag{29}$$

and

$$G_i^* + H_i^* = \frac{1}{k_*}\left(\bar{H}+\bar{G}-\sum_{j=1}^{k_*}(\xi_j^0-\xi_i^0)\right), \tag{30}$$

say,

$$G_i^* = \frac{\bar{G}}{k_*(\bar{G}+\bar{H})}\left(\bar{H}+\bar{G}-\sum_{j=1}^{k_*}(\xi_j^0-\xi_i^0)\right), \tag{31}$$

$$H_i^* = \frac{\bar{H}}{k_*(\bar{G}+\bar{H})}\left(\bar{H}+\bar{G}-\sum_{j=1}^{k_*}(\xi_j^0-\xi_i^0)\right) \tag{32}$$

for $i \in [1, k_*]$.

5 Either the Eavesdropper's Channels Gains or the Main Channels Gains Are Unknown

In this section, we first consider the case where Alice does not know the exact values of gains of the eavesdropper's channels, but she does have full knowledge about the main (Alice to Bob) channel gains. The payoff for Alice is

$$v(P,H) = \sum_{i=1}^{n} g_i^0 P_i - \sum_{i=1}^{n}(h_i^0 + H_i)P_i. \tag{33}$$

Nature's strategy thus consists only of appropriately selecting the eavesdropper's channels component H while satisfying (11) and (12). For this case we can prove the following result, which basically states that in order to harm Alice (and thus help Eve), nature has to spoil equalizing k channels with the largest gains differences, while Alice has to assign power uniformly across these k channels.

Theorem 4. *The value of the game is given as follows*

$$v = \frac{\bar{P}}{k}\left(\sum_{i=1}^{k}\xi_i^0 - \bar{H}\right).$$

where

$$k = \begin{cases} n & \text{for } \varphi_n \le H, \\ k_* : \varphi_{k_*} \le \bar{H} < \varphi_{k_*+1} & \text{for } \varphi_n > H. \end{cases}$$

Alice's optimal strategy P^* has her using an equalizing strategy among the k best channels. Namely,

$$P^* = \begin{cases} \bar{P}/k, & i \in [1,k], \\ 0, & \text{otherwise.} \end{cases} \tag{34}$$

Nature's optimal strategy H^* involves equalizing the k best channels. Namely,

$$H_i^* = \begin{cases} \frac{1}{k}\left(\bar{H} - \sum_{j=1}^{k}(\xi_j^0 - \xi_i^0)\right), & i \in [1,k] \\ 0, & \text{otherwise.} \end{cases}$$

If Alice does not know the exact values of the gains of the main subchannels, while she has full knowledge about eavesdropper's channel gains, then the payoff to Alice is given as follows

$$v(P,G) = \sum_{i=1}^{n}(g_i^0 - G_i)P_i - \sum_{i=1}^{n} h_i^0 P_i. \tag{35}$$

Theorem 5. *The value of the game is given as follows*

$$v = \frac{\bar{P}}{k}\left(\sum_{i=1}^{k}\xi_i^0 - \bar{G}\right).$$

where

$$k = \begin{cases} n & \textit{for } \varphi_n \le G, \\ k_* : \varphi_{k_*} \le \bar{G} < \varphi_{k_*+1} & \textit{for } \varphi_n > G. \end{cases}$$

Alice's optimal strategy P^* has her using an equalizing strategy among the k best channels. Namely,

$$P^* = \begin{cases} \bar{P}/k, & i \in [1,k], \\ 0, & \textit{otherwise.} \end{cases}$$

Nature's optimal strategy G^* involves equalizing the k best channels. Namely,

$$G_i^* = \begin{cases} \frac{1}{k}\left(\bar{G} - \sum_{j=1}^{k}(\xi_j^0 - \xi_i^0)\right), & i \in [1,k] \\ 0, & \textit{otherwise.} \end{cases}$$

Let us demonstrate some numerical results showing how information about the channels impacts the value of the eavesdropping game we have formulated. Suppose there are five subchannels, $n = 5$, and ξ_i is given by an exponential law, namely, let $\xi_i = 4\kappa^{i-1}$ for $i \in [1,n]$ and $\kappa = 0.7$. We examine the value of the game and the number of channels employed to communicate for the two cases: (1) with unknown gains as in Section 4, (2) with unknown eavesdropper channels gains. For both plots we will assume that $\bar{P} = 3$ and $\bar{G} \in [1,7]$ and $\bar{H} = 1$. However, for the second case we assume that $\bar{H}$ is uniformly distributed across the subchannels H_i. In Table 1 we present the value of the game for different values of k. Of course, when the players use all the five channels then the value of the two cases of the eavesdropping game coincide, which occurs for large $\bar{G}$ (in this example, $\bar{G} = 7$). If $\bar{G}$ is small (equals 1) then having extra information about the channels (the second case) allows her to improve her SINR (and hence secrecy) payoff by a factor of roughly 1.5.

Table 1. The value of the game and k for two plots

$\bar{G}$	Case 1	k	Case 2	k
1	1.587	3	2.400	1
2	1.283	4	1.800	2
3	1.033	4	1.320	3
4	0.818	5	0.987	3
5	0.618	5	0.683	4
6	0.418	5	0.433	4
7	0.218	5	0.218	5

6 The Worst Case for the Main Gains Are Known

To show that the optimal strategies essentially depend on the information the players have, in this section we slightly change the formulation of the game to assume that the worst possible values for the main channels gains are known (instead of the best possible values), and then demonstrate the impact that such a change has on the optimal strategies. We assume that the SINR payoff for Alice is given as follows

$$v(P,(G,H)) = \sum_{i=1}^{n}(g_i^0 + G_i)P_i - \sum_{i=1}^{n}(h_i^0 + H_i)P_i, \tag{36}$$

where now g_i^0 is the worst possible value for the main subchannel i's gain.

For this game we can prove the following result describing the optimal strategies as well as the value of the resulting eavesdropping game:

Theorem 6. *(a) Let (21) hold. Then the value of the game is given by*

$$v = \frac{\bar{P}}{n}\left(\sum_{i=1}^{n}\xi_i^0 - \bar{H} + \bar{G}\right). \tag{37}$$

Alice's optimal strategy P^* *assigns power uniformly across all* n *subchannels, i.e. by (23). Nature's optimal strategy* (G^*, H^*)*, meanwhile, involves assigning the eavesdropper channel component* H^* *to equalize the eavesdropper channels, while assigning the main channel component* G^* *uniformly across subchannels,*

$$G_i^* = \bar{G}/n, \tag{38}$$

$$H_i^* = \frac{1}{n}\left(\bar{H} - \sum_{j=1}^{n}(\xi_j^0 - \xi_i^0)\right) \tag{39}$$

for $i \in [1, n]$.

(b) Let $\bar{H} < \varphi_n$. *Then, there is a* $k_* \in [1, n-1]$ *such that (27) holds.Also, let*

$$A < 0, \tag{40}$$

where

$$\begin{aligned} A &:= \bar{G} - \frac{1}{k_*}\sum_{i=k_*+1}^{n}\left(\sum_{j=1}^{k_*}(\xi_j^0 - \xi_i^0) - \bar{H}\right) \\ &= \bar{G} - \frac{1}{k_*}\Big((n-k_*)\sum_{j=1}^{k_*}\xi_j^0 \\ &\quad - k_*\sum_{j=k_*+1}^{n}\xi_j^0 - \bar{H}(n-k_*)\Big). \end{aligned} \tag{41}$$

Then the value of the game is $v = \bar{P}\left(\sum_{i=1}^{k_*}\xi_i^0 - \bar{H}\right)/k_*$. *Alice's optimal strategy* P^* *assigns power equally among the first* k_* *channels, i.e. it is given by (28).*

Nature's optimal strategy (G^*, H^*) assigns G^* only to the main channel components not used by Alice, while H^* is assigned across the eavesdropper's subchannels so as to equalize the quality of the k_* best channels for Alice. Namely,

$$G_i^* \begin{cases} = 0, & i \in [1, k_*], \\ \le \frac{1}{k_*}\left(\sum_{j=1}^{k_*}(\xi_j^0 - \xi_i^0) - \bar{H}\right) \\ \textit{such that } \sum_{j=k_*+1}^{n} G_i^* = \bar{G}, & i \in [k_*+1, n], \end{cases} \tag{42}$$

$$H_i^* = \begin{cases} \frac{1}{k_*}\left(\bar{H} - \sum_{j=1}^{k_*}(\xi_j^0 - \xi_i^0)\right), & i \in [1, k_*], \\ 0, & i \in [k_*+1, n]. \end{cases} \tag{43}$$

(c) Let $\bar{H} < \varphi_n$ and $A \ge 0$. The value of the game is given by (37). Alice's optimal strategy P^* is given by (23). Nature's optimal strategy (G^*, H^*) assigns H^* according to (43), and equalizes the quality of the k_* best channels, while component for the main channel G^* is assigned to supplement all the channels until they have an equal level, as follows

$$G_i^* = \begin{cases} \frac{A}{n}, & i \le k_*, \\ \frac{A}{n} + \frac{1}{k_*}\left(\sum_{j=1}^{k_*}(\xi_j^0 - \xi_i^0) - \bar{H}\right), & i > k_*. \end{cases} \tag{44}$$

Since the inequality

$$\frac{\bar{P}}{n}\left(\sum_{i=1}^{n}\xi_i^0 - \bar{H} + \bar{G}\right) < \frac{\bar{P}}{k_*}\left(\sum_{i=1}^{k_*}\xi_i^0 - \bar{H}\right)$$

is equivalent to

$$k_*\bar{G} < (n - k_*)\sum_{j=1}^{k_*}\xi_j^0 - k_*\sum_{j=k_*+1}^{n}\xi_j^0 - \bar{H}(n - k_*)$$

or, by (41), to $A < 0$, we can summarize the result of Theorem 6 about the value of the game in the following statement.

Theorem 7. *The value of the game is given as follows: if $\varphi_n > \bar{H}$, then*

$$v = \max\left\{\frac{\bar{P}}{n}\left(\sum_{i=1}^{n}\xi_i^0 - \bar{H} + \bar{G}\right), \frac{\bar{P}}{k_*}\left(\sum_{i=1}^{k_*}\xi_i^0 - \bar{H}\right)\right\}.$$

We now present some numerical results to illustrate the implications of Theorem 6 and 7. As before, suppose there are five subchannels, $n = 5$ and ξ_i is given by the exponential law, namely, let $\xi_i = 4\kappa^{i-1}$ for $i \in [1, n]$ and $\kappa = 0.7$. We compare how the optimal strategies change around the switching point A. In Table 2 we put together the optimal strategies for nature when $\bar{G} = 1$, $\bar{P} = \{3, 4\}$ corresponding to the values of the game 5.76 and 4.855. In spite of the fact that $k_* = 3$ for both cases, there is a switching point between $\bar{P} = 3$ and $\bar{P} = 4$ since for the first case

Table 2. The optimal strategies for the *nature* player in the example eavesdropping game

$H^*\&G^*(\bar{P})$	1	2	3	4	5
$H^*(3)$	2.08	0.88	0.04	0	0
$G^*(3)$	0	0	0	$\le$0.446	$\le$0.858
$H^*(4)$	2.413	1.213	0.373	0	0
$G^*(4)$	0.032	0.032	0.032	0.246	0.658

$A = -0.507$ and for the second case $A = 0.159$. In the case $\bar{P} = 3$ a variety of G components is possible that do not use the first three channels. For example, it could be any $G^* = (0, 0, 0, G_4^*, G_5^*)$ such that $G_4^* \le 0.446$, $G_5^* = 0.858$, $G_4^* + G_5^* = 1$. Meanwhile, in the case $\bar{P} = 4$ the G^* component uses all the channels.

7 The Optimization Problem with Unknown Noise and Eavesdropper's Channel Gains

In this section, we relax the assumptions about the noise term (W_i^{AB} from Section 2), and consider the situation where Alice does not know how the noise is distributed among the main (Alice to Bob) subchannels. For example, the noise power may not be uniform across subchannels. To reflect this case, we assume that the main channels gains are given by

$$g_i = 1/(N_i^0 + N_i) \text{ for } i \in [1, n],$$

where N_i^0 is a constant part of the noise level in the main channel i and N_i is a variable component for which Alice knows only the total perturbation $\bar{N}$, which satisfies

$$\sum_{i=1}^{n} N_i = \bar{N} \tag{45}$$

and

$$N_i \ge 0 \text{ for } i \in [1, n]. \tag{46}$$

We note that this is representation allows us to reflect the variable noise terms directly in the channel gains g_i. For example, low levels of noise (i.e. small N_i^0 and N_i) leads to a correspondingly large subchannel gain g_i, which implies that the ith subchannel is good.

Assume that Alice has fixed the power allocation strategy for signal transmission, i.e. the vector $P = (P_1, \dots, P_n)$ satisfying (3) and (4), but the parameters for the environment are not completely known, i.e. Alice does not know how the noise is distribution for Eve, or the values the eavesdropper's channels gains. The payoff is given as follows

$$v((N, H)) = \sum_{i=1}^{n} \frac{P_i}{N_i^0 + N_i} - \sum_{i=1}^{n} (h_i^0 + H_i) P_i. \tag{47}$$

Alice would like to know what the worst payoff she could have, so, she would like to minimize (47) by (N, H).

Since the payoff is linear in H and concave in N, the strategy (N^*, H^*) is the optimal one if and only if there is ν, such that

$$\frac{P_i}{(N_i^0 + N_i^*)^2} \begin{cases} = \nu & \text{for } N_i^* > 0, \\ \leq \nu & \text{for } N_i^* = 0, \end{cases} \tag{48}$$

$$H_i^* \begin{cases} \geq 0 & \text{for } P_i = P_{max}, \\ = 0 & \text{otherwise.} \end{cases} \tag{49}$$

Then the optimal H^* is given by (16) and the optimal N^* is of the form

$$N_i^* = N_i(\nu) = \left[\sqrt{P_i/\nu} - N_i^0\right]_+ \text{ for } i \in [1, n],$$

where $\nu = \nu_*$ is the unique positive root of the equation

$$\sum_{i=1}^{n} \left[\sqrt{P_i/\nu} - N_i^0\right]_+ = \bar{N}.$$

The payoff corresponding to (N^*, H^*) is given as follows

$$v = \sqrt{\nu_*} \sum_{N_i(\nu_*)>0} \sqrt{P_i} - \sum_{i=1}^{n} h_i^0 P_i - \bar{H} P_{max}.$$

8 The Game with Unknown Noise in the Main Subchannels

In this section we consider the situation where there is unknown noise in the main subchannels, and examine this case from game-theoretical position. There are two players: Alice and nature. Alice has to transmit the total power $\bar{P}$ using strategy P satisfying (3) and (4). Recall that nature's objective is to harm Alice-to-Bob communication, and thus in this case nature's strategy consists only of a jamming component N satisfying (45) and (46), i.e. nature introduces noise to the main subchannels. The payoff to Alice is given as follows

$$v(P, N) = \sum_{i=1}^{n} \frac{P_i}{N_i^0 + N_i} - \sum_{i=1}^{n} h_i^0 P_i \tag{50}$$

The payoff to nature is $-v(P, N)$.

In the following theorem we find the value of the game and the optimal strategies for the players. In particular, we show that nature should hamper precisely the same channels that Alice employs. The optimal strategy for nature is a water filling strategy, but from an adversarial point of view.

Theorem 8. *The value of the game is* $\omega_* \bar{P}$ *where* ω_* *is the unique root in* $[-\min_i h_i^0, \infty)$ *of the water filling equation*

$$H_N(\omega) := \sum_{i=1}^{n} \left[\frac{1}{h_i^0 + \omega} - N_i^0 \right]_+ = \bar{N}. \tag{51}$$

The optimal nature's strategy is given by

$$N_i^* = N_i(\omega) = \left[\frac{1}{h_i^0 + \omega} - N_i^0 \right]_+, \ i \in [1, n]. \tag{52}$$

The optimal Alice's strategy is given as follows

$$P_i^* = \begin{cases} \bar{P} \dfrac{1/(h_i^0 + \omega_*)^2}{\displaystyle\sum_{j:N_j(\omega_*)>0} (1/(h_j^0 + \omega_*)^2)} & \text{if } N_i(\omega_*) > 0. \\ 0 & \text{otherwise.} \end{cases}$$

Remark 1. *It is interesting that the optimal strategy for nature does not take into account the power of signal Alice has to transmit but only the parameters of the environment, which is quite reasonable because nature is Alice's rival.*

As a numerical example we consider five channels $n = 5$ *case. Let* N_i^0 *and* h_i^0 *are given by the same exponential law, namely,* $N_i^0 = h_i^0 = \kappa^{i-1}$ *for* $i \in [1, n]$ *where* $\kappa = 0.5$*. Also, let* $\bar{P} = 1$ *and* $\bar{N} = 0.5$ *In Table 3 the value of the game and the players' optimal strategies are given as a function of* κ*. For* $\kappa = 0.1$ *these strategies use four out of the five subchannels, for* $\kappa = 0.8$ *they use two subchannels, and for intermediate values these strategies use three subchannels.*

Table 3. The value of the game and the optimal strategies of the players

κ	v		1	2	3	4	5
0.1	6.315	N	0.000	0.047	0.142	0.154	0.157
		P	0.000	0.230	0.248	0.258	0.263
0.2	5.314	N	0.000	0.000	0.140	0.176	0.184
		P	0.000	0.000	*0.321*	0.336	0.344
0.3	4.655	N	0.000	0.000	0.114	0.182	0.204
		P	0.000	0.000	0.319	0.336	0.345
0.4	3.858	N	0.000	0.000	0.083	0.187	0.229
		P	0.000	0.000	0.316	0.336	0.347
0.5	3.056	N	0.000	0.000	0.052	0.189	0.258
		P	0.000	0.000	0.312	0.337	0.351
0.6	2.345	N	0.000	0.000	0.025	0.189	0.286
		P	0.000	0.000	0.306	0.338	0.356
0.7	1.764	N	0.000	0.000	0.006	0.186	0.307
		P	0.000	0.000	**0.298**	0.339	0.363
0.8	1.314	N	0.000	0.000	0.000	0.183	0.317
		P	0.000	0.000	0.000	0.478	0.522

It is interesting to note that for $\kappa \in [0.2, 0.7]$ the maximal difference is 11% (it is accentuated in bold font) from the uniform strategy, and arises right before switching to using smaller number of channels and smallest in 1% (accentuated in italic font right after the switching point).

9 Conclusion

Recently, there has been increasing interest in using the properties of the physical layer in a wireless system to support security (specifically, confidentiality) objectives. The basic principle behind this new form of confidentiality is to take advantage of conditions where the main Alice-to-Bob channel is better than the adversarial channel Alice-to-Eve. One fundamental challenge facing the formulation of such physical layer secrecy is understanding the implications of varying assumptions for what knowledge the participants (Alice, Bob and Eve) have in the secret communication. In this paper we have examined the problem of eavesdropping over fading channels, where the problem of secret communication in the presence of an eavesdropper is formulated as a zero-sum game. In our problem, the legitimate receiver does not have complete knowledge about the environment, i.e. does not know the exact values of the channels gains. Rather, we consider that the receiver has some partial knowledge characterizing the channel, such as its distribution. The transmitter's task then involves deciding how to transmit its information across which subchannels. We have posed this problem as an optimization problem, where the environment acts as a secondary player in a zero-sum game whose objective is to hamper successful communication by the user. In our formulation, we have chosen to use signal-to-interference ratio (SINR) as the payoff function, due to the tractability it provides, but note that at low SINR our objective function approximates the secrecy capacity. We have studied a variety of scenarios where different assumptions are placed on the amount of knowledge that the transmitter, Alice, has in the eavesdropping game. In the case where Alice does not know the gains for the various subchannels, then the best strategy is to distribute energy equally across a subset of selected channels. On the other hand, if Alice does not know the eavesdropper's channel gains, then Alice should also employ a strategy involving uniformly distributing energy across a subset of channels. However, if the user acquires extra knowledge about environment, e.g. the eavesdropper's channel gains, then we show how Alice may better tune her power allocation among the channels.

References

1. Li, X., Chen, M., Ratazzi, E.P.: Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy. In: Proc. IEEE SPAWC 2005, June 2005, pp. 811–815 (2005)
2. Koorapaty, H., Hassan, A.A., Chennakeshu, S.: Secure Information Transmission for Mobile Radio. IEEE Trans. Wireless Commun., 52–55 (July 2003)
3. Hero, A.E.: Secure Space-Time Communication. IEEE Trans. Info. Theory, 3235–3249 (December 2003)

4. Li, Z., Yates, R., Trappe, W.: Secrecy Capacity of Independent Parallel Channels. In: Allerton Conference on Communication, Control, and Computing (2006)
5. Li, Z., Xu, W., Miller, R., Trappe, W.: Securing wireless systems via lower layer enforcements. In: WiSe 2006: Proceedings of the 5th ACM workshop on Wireless security, pp. 33–42 (2006)
6. Liang, Y., Poor, H.V., Shamai, S.: Secure Communication over Fading Channels. IEEE Transactions on Information Theory, Special issue on Information Theoretic Security 54(6), 2470–2492 (2008)
7. Gopala, P., Lai, L., El Gamal, H.: On the secrecy capacity of fading channels. IEEE Trans. Inform. Theory (accepted for publication)
8. Wyner, A.: The wire-tap channel. Bell. Syst. Tech. J. 54(8), 1355–1387 (1975)
9. Csiszár, I., Körner, J.: Broadcast channels with confidental messages. IEEE Trans. on Inf. Theory 24(3), 339–348 (1978)
10. Maurer, U.M., Wolf, S.: Information-theoretic key agreement: From weak to strong secrecy for free. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 351–368. Springer, Heidelberg (2000)
11. Bennett, C., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. on Information Theory 41, 1915–1923 (1995)
12. Van Dijk, M.: On a special class of broadcast channels with confidential messages. IEEE Trans. on Information Theory 43(2), 712–714 (1997)
13. Leung-Yan-Cheong, S.K., Hellman, M.: The gaussian wire-tap channel. IEEE Transactions on Information Theory 24(4), 451–456 (1978)
14. Altman, E., Avrachenkov, K., Garnaev, A.: A jamming game in wireless networks with transmission cost. In: Chahed, T., Tuffin, B. (eds.) NET-COOP 2007. LNCS, vol. 4465, pp. 1–12. Springer, Heidelberg (2007)
15. Altman, E., Avrachenkov, K., Garnaev, A.: Transmission power control game with SINR as objective function. In: Altman, E., Chaintreau, A. (eds.) NET-COOP 2008. LNCS, vol. 5425, pp. 112–120. Springer, Heidelberg (2009)
16. Altman, E., Kamble, V., Kameda, H.: A Braess Type Paradox in Power Control over Interference Channels. In: Physicomnet workshop, Berlin, April 4 (2008)
17. Ji, H., Huang, C.-Y.: Non-cooperative uplink power control in cellular radio systems. Wireless Networks 4, 233–240 (1998)

A Appendix

Proof of Theorem 3. Since the payoff is linear in P, G and H, the strategies P^*, (G^*,H^*) for Alice and nature are in equilibrium (so, these strategies are the best response to one another) if and only if there are ω, ν_G and ν_H such that

$$P_i^* \begin{cases} \geq 0 & \text{for } \xi_i^0 - G_i^* - H_i^* = \omega, \\ = 0 & \text{for } \xi_i^0 - G_i^* - H_i^* < \omega, \end{cases} \tag{53}$$

$$G_i^* \begin{cases} \geq 0 & \text{for } P_i^* = \nu_G, \\ = 0 & \text{for } P_i^* < \nu_G, \end{cases} \tag{54}$$

$$H_i^* \begin{cases} \geq 0 & \text{for } P_i^* = \nu_H, \\ = 0 & \text{for } P_i^* < \nu_H. \end{cases} \tag{55}$$

(a) Let P^* be given by (23). Then, by (54) and (55), $\nu_G = \nu_H = \bar{P}/n$ and any strategy (G, H) is the best response one for (23), in particular, the strategy given by (29). Let H^* and G^* be given by (29). Then, by (21) they present a strategy and $\xi_i^0 - G_i^* - H_i^* = \omega$ for $i \in [1, n]$ where $\omega = \left(\sum_{j=1}^n \xi_j^0 - \bar{H} - \bar{G}\right)/n$. Then, by (53), any strategy for Alice is the best response strategy to nature's strategy given by (29). This proves (a).

(b) Let P^* be given by (28). Then, by (54) and (55), $\nu_G = \nu_H = \bar{P}/k_*$ and any strategy for nature (G, H) satisfying the following conditions is the best response for (28).

$$H_i = 0 \text{ and } G_i = 0 \text{ for } i \in [k_* + 1, n]. \tag{56}$$

By (27), (G^*, H^*) given by (29) and (30) is a strategy which satisfies to (56). So, (G^*, H^*) is the best response one for (28). Let (G^*, H^*) be given by (29) and (30). Then

$$\xi_i^0 - G_i^* - H_i^* \begin{cases} = \omega, & i \in [1, k_*], \\ \le \omega, & i \in [k_* + 1, n], \end{cases}$$

where $\omega = \left(\sum_{j=1}^{k_*} \xi_j^0 - \bar{H} - \bar{G}\right)/k_*$. So, (28) is the best response to (29) and (30) by (53).

Proof of Theorem 6. Since the payoff is linear in P, G and H, the strategies P^*, (G^*,H^*) for Alice and nature is in equilibrium (so, these strategies are the best response each other) if and only if there are ω, ν_G and ν_H such that

$$P_i^* \begin{cases} \ge 0 & \text{for } \xi_i^0 + G_i^* - H_i^* = \omega, \\ = 0 & \text{for } \xi_i^0 + G_i^* - H_i^* < \omega, \end{cases} \tag{57}$$

$$G_i^* \begin{cases} \ge 0 & \text{for } P_i^* = \nu_G, \\ = 0 & \text{for } P_i^* > \nu_G, \end{cases} \tag{58}$$

$$H_i^* \begin{cases} \ge 0 & \text{for } P_i^* = \nu_H, \\ = 0 & \text{for } P_i^* < \nu_H. \end{cases} \tag{59}$$

(a) Let P^* be given by (23). Then, by (58) and (59), $\nu_G = \nu_H = \bar{P}/n$ and any strategy (G, H) is the best response one for (23), in particular, the strategy given by (38) and (39). Let H^* be given by(39). It is clear that for this H^* (11) holds and, by (39), (19) and (21),

$$H_j^* = \frac{1}{n}\left(\bar{H} - \sum_{j=1}^n (\xi_j^0 - \xi_i^0)\right) \ge \frac{1}{n}\left(\bar{H} - \varphi_n\right) \ge 0 \text{ for } j \in [1, n].$$

So, (11) also holds and H^* is the eavesdropper's channel component arising in nature's strategy to harm the secrecy of communication between Alice and

Bob. It is clear that G^* given by (38) satisfies (8) and (9) and for G^* and H^* holds the following relation: $\xi_i^0 + G_i^* - H_i^* = \omega$ for $i \in [1,n]$ where $\omega = \left(\sum_{j=1}^n \xi_j^0 - \bar{H} + \bar{G}\right)/n$. Then, by (57), any strategy for Alice is the best response strategy to nature's strategy given by (38) and (39). This proves (a).

(b) Let P^* be given by (28). Then, by (58) and (59), $\nu_G = 0$ and $\nu_H = \bar{P}/k_*$ and any nature's strategy (G,H) satisfying the following conditions is the best response for (28).

$$\begin{aligned} &H_i = 0 \text{ for } i \in [k_*+1, n], \\ &G_i = 0 \text{ for } i \in [1, k_*]. \end{aligned} \tag{60}$$

Let H^* be given by (43). It is clear that for this H^* (11) holds. Also, by (22), (19) and (21)

$$H_j^* = \frac{1}{k_*}\left(\bar{H} - \sum_{j=1}^{k_*}(\xi_j^0 - \xi_i^0)\right) \geq \frac{1}{k_*}\left(\bar{H} - \varphi_{k_*}\right) \geq 0 \text{ for } j \in [1, k_*]. \tag{61}$$

So, for H^*, (12) also holds and it is the eavesdropper's channel components for a strategy employed by nature. By (19) and (27),

$$\begin{aligned} \sum_{j=1}^{k_*}(\xi_j^0 - \xi_i^0) - \bar{H} &\geq \sum_{j=1}^{k_*}(\xi_j^0 - \xi_{k_*+1}^0) - \bar{H} \\ &= \varphi_{k_*+1} - \bar{H} \geq 0 \text{ for } j \in [k_*+1, n]. \end{aligned} \tag{62}$$

Thus, for G^* given by (42), (9) holds. Then, by (40), it is the main channels component of a strategy by nature. It is clear that H^* and G^* satisfy (60). Therefore, they present the best response to (28).

Let G^* and H^* be given by (43) and (42). Then

$$\xi_i^0 + G_i^* - H_i^* \begin{cases} = \omega, & i \in [1, k_*], \\ \leq \omega, & i \in [k_*+1, n], \end{cases}$$

where $\omega = \left(\sum_{j=1}^{k_*} \xi_j^0 - \bar{H}\right)/k_*$. So, (28) is the best response to (43) and (42).

(c) Let P^* be given by (23), then any strategy (G,H) is the best response for (23), in particular to the strategy given by (43) and (44).

Let G^* and H^* be given by (43) and (44). Then, by (22), (19), (21) and (61), H^* are the eavesdropper channel components of a strategy by nature. Also, as $A > 0$, then, by (62), G^* corresponds to the main channel components for a strategy employed by nature. Then $\xi_i^0 + G_i^* - H_i^* = \omega$ for $i \in [1,n]$ where

$$\omega = \frac{A}{n} + \frac{1}{k_*}\left(\sum_{i=1}^{k_*} \xi_i^0 - \bar{H}\right).$$

Thus, any Alice strategy is the best response for (H^*, G^*), such as the strategy given by (23), and $\omega\bar{P}$ is the value of the game. Then, since

$$\begin{aligned}
&\frac{A}{n} + \frac{1}{k_*}\left(\sum_{i=1}^{k_*} \xi_i^0 - \bar{H}\right)\\
&= \frac{1}{n}\left(\bar{G} - \frac{(n-k_*)\sum_{j=1}^{k_*}\xi_j^0 - k_*\sum_{j=k_*+1}^{n}\xi_j^0 - \bar{H}(n-k_*)}{k_*}\right)\\
&+ \frac{1}{k_*}\left(\sum_{i=1}^{k_*}\xi_i^0 - \bar{H}\right) = \frac{1}{n}\left(\sum_{i=1}^{n}\xi_i^0 + \bar{G} - \bar{H}\right).
\end{aligned}$$

the value of the game is given by (37). This completes the proof of Theorem 6.

Proof of Theorem 8. Since the payoff is linear in P and concave on N, the strategies P^*, N^* of Alice and nature is in equilibrium (so, these strategies are the best response to each other) if and only if there are ω, ν such that

$$P_i^* \begin{cases} \geq 0 & \text{for } \dfrac{1}{N_i^0 + N_i^*} - h_i^0 = \omega, \\ = 0 & \text{for } \dfrac{1}{N_i^0 + N_i^*} - h_i^0 < \omega, \end{cases} \tag{63}$$

$$\frac{P_i^*}{(N_i^0 + N_i^*)^2} \begin{cases} = \nu & \text{for } N_i^* > 0, \\ \leq \nu & \text{for } N_i^* = 0. \end{cases} \tag{64}$$

Thus, by (64), if $P_i^* = 0$ then $N_i^* = 0$. It is reasonable to look for the optimal nature strategy in a subclass of strategies which hamper only the channels employed by Alice to transmit the signal, so for the strategies that have $P_i^* > 0$ then $N_i^* > 0$. Then, by (63), the optimal strategy N^* is of the form

$$N_i^* = N_i(\omega) = \left[\frac{1}{h_i^0 + \omega} - N_i^0\right]_+, \tag{65}$$

where $\omega = \omega_*$ is the unique root in $[-\min_i h_i^0, \infty)$ of the following water filling equation

$$H_N(\omega) := \sum_{i=1}^{n}\left[\frac{1}{h_i^0 + \omega} - N_i^0\right]_+ = \bar{N}. \tag{66}$$

By (64) and (65) we have that the Alice's optimal strategy is of the form

$$P_i^* = P_i(\nu) = \begin{cases} \dfrac{\nu}{(h_i^0 + \omega_*)^2} & \text{if } N_i(\omega_*) > 0, \\ 0 & \text{otherwise} \end{cases} \tag{67}$$

and $\nu = \nu_*$ can be found as the unique root of $H_P(\nu) := \sum_{i=1}^{n} P_i(\nu) = \bar{P}$. Thus,

$$\nu_* = \frac{\bar{P}}{\sum_{j:N_j(\omega_*)>0}(1/(h_j^0 + \omega_*)^2)}.$$

It is clear that the strategies defined by (65) and (67) satisfies the conditions (63) and (64). That is why they are the optimal ones. This completes the proof of Theorem 8.