Secrecy Capacity Region of Gaussian Broadcast Channel

Ghadamali Bagherikaram, Abolfazl S. Motahari, Amir K. Khandani
Coding and Signal Transmission Laboratory,
Department of Electrical and Computer Engineering,
University of Waterloo, Waterloo, Ontario, N2L 3G1
Emails: {gbagheri,abolfazl,khandani}@cst.uwaterloo.ca

[1] ***Abstract*—In this paper, we first consider a scenario where a source node wishes to broadcast two confidential messages for two respective receivers, while a wire-taper also receives the transmitted signal. We assume that the signals are transmitted over additive white Gaussian noise channels. We characterize the secrecy capacity region of this channel. Our achievable coding scheme is based on superposition coding and the random binning. We refer to this scheme as Secret Superposition Coding. The converse proof combines the converse proof for the conventional Gaussian broadcast channel and the perfect secrecy constraint. This capacity region matches the capacity region of the broadcast channel without security constraint. It also matches the secrecy capacity of the wire-tap channel. Based on the rate characterization of the secure Gaussian broadcast channel, we then use a multilevel coding approach for the slowly fading wire-tap. We assume that the transmitter only knows the eavesdropper's channel. In this approach, source node sends secure layered coding and the receiver viewed as a continuum ordered users. We derive optimum power allocation for the layers which maximizes the total average rate.**

I. Introduction

The notion of information theoretic secrecy in communication systems was first introduced by Shannon in [1]. The information theoretic secrecy requires that the received signal of the eavesdropper not provide even a single bit information about the transmitted messages. Wyner in [2] considered a scenario in which a wire-tapper receives the transmitted signal over a degraded channel with respect to the legitimate receiver's channel. He further assumed that the wire-tapper has no computational limitations and knows the codebook used by the transmitter. He measured the level of ignorance at the eavesdropper by its equivocation and characterized the capacity-equivocation region. Interestingly, a non-negative perfect secrecy capacity is always achievable for this scenario.

Csiszar and Korner in [3], extended the Wyner's work to the general (non-degraded) broadcast channel with confidential messages. They considered transmitting confidential information to the legitimate receiver while transmitting common information to both the legitimate receiver and the wire-tapper. They established a capacity-equivocation region of this channel.

We recently studied a secure broadcast channel in [4], where the source node transmits two independent messages for two respective receivers in the presence of an additional illegitimate receiver. In this work, we characterized the secrecy capacity region of the degraded broadcast channel and showed that secret superposition coding is optimal. In this scheme, finding the optimal distribution when the channels are Gaussian involves solving a functional, nonconvex optimization problem. Usually nontrivial techniques and strong inequalities are used to solve optimization problems of this sort. Indeed, for the single user case, Leung-Yan-Cheong in [5] successfully evaluated the capacity expression of the wire-tap channel by using the entropy power inequality. Alternatively, it can also be evaluated using a classical result from the Estimation Theory and the relationship between mutual information and minimum mean-squared error estimation.

The secrecy capacity of the conventional wire-tap channel is studied in [6], [7], when the channels are slowly fading. In these works, it is assumed that the fading is quasi-static and the transmitter is not aware of the fading gains. The outage probability is defined in these works. In an outage strategy, the transmission rate is fixed and the information is secure and reliably detected when the instantaneous main channel is stronger than the instantaneous eavesdropper's channel. The term outage capacity refers to the maximum achievable average rate. In [8] a broadcast strategy for the slowly fading Gaussian point-to-point channel is introduced. In this strategy, the transmitter uses a layered coding scheme and the receiver is viewed as a continuum of ordered users.

In this paper, we first consider a natural extension of the Gaussian wire-tap channel to the multi-user case. In this scenario, a source node wishes to broadcast two confidential messages for two respective receivers, while a wire-taper also receives the transmitted signal. All broadcast channels are assumed to be AWGN. We establish the secrecy capacity region of this channel. Our achievable coding scheme is based on superposition of Gaussian codebooks and the random binning. We refer to this scheme as Secret Superposition Coding. This capacity region matches the capacity region of the Gaussian broadcast channel without any security constraint. It also matches the secrecy capacity of the Gaussian wire-

[1] Financial support provided by Nortel and the corresponding matching funds by the Natural Sciences and Engineering Research Council of Canada (NSERC), and Ontario Centers of Excellence (OCE) are gratefully acknowledged.

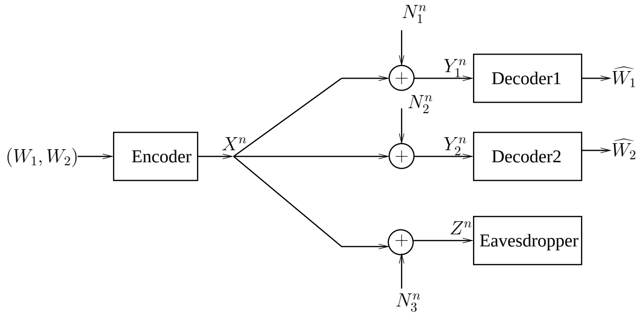

Fig. 1. Gaussian Broadcast Channel with Confidential Messages

tap channel. Based on the rate characterization of the secure broadcast channel, we then use broadcast strategy for the slow fading wire-tap channel when the transmitter only knows the eavesdropper's channel. In broadcast strategy, source node sends secure layered coding and the receiver viewed as a continuum ordered users. We derive optimum power allocation for the layers which maximizes the total average rate.

The rest of the paper is organized as follows. In section II we introduce some preliminaries. In section III, we establish the secrecy capacity region of the Gaussian broadcast channel. In section IV, we introduce the secret multilevel coding approach for the slowly fading wire-tap channel. We derive the optimum power allocation for this scheme which maximize the total average rate over all fading realizations. In Section V, we conclude the paper.

II. Preliminaries

In this paper, random variables are denoted by capital letters (e.g. X) and their realizations are denoted by corresponding lower case letters (e.g. x). The finite alphabet of a random variable is denoted by a script letter (e.g. $\mathcal{X}$) and its probability distribution is denoted by $P(x)$. The vectors will be written as $x^n = (x_1, x_2, ..., x_n)$, where subscripted letters denote the components and superscripted letters denote the vector. Bold capital letters represent matrices (e.g. $\mathbf{A}$). The notation x^{i-1} denotes the vector $(x_1, x_2, ..., x_{i-1})$ and the notation $\widetilde{x}^i$ denotes the vector $(x_i, x_{i+1}, ..., x_n)$. A similar notation will be used for random variables and random vectors.

Consider a Gaussian Broadcast Channel with Confidential Messages (G-BCCM) as depicted in Fig.1. The transmitter wishes to send two independent messages (W_1, W_2) to the respective receivers in n uses of the channel while insuring perfect secrecy. At the time i, the signals received by the destinations and the eavesdropper are given by

$$\begin{aligned} Y_{1i} &= X_i + N_{1i} \qquad (1) \\ Y_{2i} &= X_i + N_{2i} \\ Z_i &= X_i + N_{3i} \end{aligned}$$

where N_{1i}, N_{2i} and N_{3i} represent the i.i.d additive Gaussian noises with zero mean variances of σ_1^2, σ_2^2 and σ_3^2 at the destinations and the eavesdropper respectively. We assume that $\sigma_1^2 \leq \sigma_2^2 \leq \sigma_3^2$. A $((2^{nR_1}, 2^{nR_2}), n)$ code for a broadcast channel with confidential messages consists of a stochastic encoder

$$f : (\{1, 2, ..., 2^{nR_1}\} \times \{1, 2, ..., 2^{nR_2}\}) \rightarrow \mathcal{X}^n, \qquad (2)$$

and two decoders,

$$g_1 : \mathcal{Y}_1^n \rightarrow \{1, 2, ..., 2^{nR_1}\} \qquad (3)$$

and

$$g_2 : \mathcal{Y}_2^n \rightarrow \{1, 2, ..., 2^{nR_2}\}. \qquad (4)$$

The average probability of error is defined as the probability that the decoded messages are not equal to the transmitted messages; that is,

$$P_e^{(n)} = P(g_1(Y_1^n) \neq W_1 \cup g_2(Y_2^n) \neq W_2). \qquad (5)$$

The secrecy levels of confidential messages W_1 and W_2 are measured at the eavesdropper in terms of equivocation rates which are defined as follows.

Definition 1 *The equivocation rates R_{e1}, R_{e2} and R_{e12} for the broadcast channel with confidential messages are:*

$$\begin{aligned} R_{e1} &= \frac{1}{n} H(W_1 | Z^n), \qquad (6) \\ R_{e2} &= \frac{1}{n} H(W_2 | Z^n), \\ R_{e12} &= \frac{1}{n} H(W_1, W_2 | Z^n). \end{aligned}$$

The perfect secrecy rates R_1 and R_2 are the amount of information that can be sent to the legitimate receivers not only reliably but also confidentially.

Definition 2 *A secrecy rate pair (R_1, R_2) is said to be achievable if for any $\epsilon > 0, \epsilon_1 > 0, \epsilon_2 > 0, \epsilon_3 > 0$, there exists a sequence of $((2^{nR_1}, 2^{nR_2}), n)$ codes, such that for sufficiently large n, we have:*

$$\begin{aligned} P_e^{(n)} &\leq \epsilon, \qquad (7) \\ R_{e1} &\geq R_1 - \epsilon_1, \qquad (8) \\ R_{e2} &\geq R_2 - \epsilon_2, \qquad (9) \\ R_{e12} &\geq R_1 + R_2 - \epsilon_3. \qquad (10) \end{aligned}$$

In the above definition, the first condition concerns the reliability, while the other conditions guarantee perfect secrecy for each individual message and both messages as well. The capacity region is defined as follows.

Definition 3 *The capacity region of the broadcast channel with confidential messages is the closure of the set of all achievable rate pairs (R_1, R_2).*

III. Gaussian Broadcast Channel with Confidential Messages

In this section we consider the Gaussian broadcast channel with confidential messages. In [4] we proved the following theorem for the degraded BCCM

Theorem 1 *The capacity region for transmitting independent secret information over the degraded broadcast channel is the convex hull of the closure of all (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq I(X;Y_1|U) - I(X;Z|U), && (11)\\ R_2 &\leq I(U;Y_2) - I(U;Z). && (12) \end{aligned}$$

for some joint distribution $P(u)P(x|u)P(y_1, y_2, z|x)$.

Note that evaluating (11) and (12) for the fading channels involves solving a functional, nonconvex optimization problem. Usually nontrivial techniques and strong inequalities is used to solve the optimization problems of this type. Indeed, for the single user case, Leung-Yan-Cheong in [3] successfully evaluated the capacity expression of wire-tap channel by using the entropy power inequality. Alternatively, it can also be evaluated using a classical result from estimation theory and the relationship between mutual information and minimum mean-squared error estimation. On the other hand, the entropy power inequality is sufficient to establish the converse proof of a gaussian broadcast channel without secrecy constraint. Unfortunately, the traditional entropy power inequality does not extend to the secret multi user case. Here, by using the generalized version of the entropy power inequality, we show that secret superposition coding with Gaussian codebook is optimal.

At time i the received signals are modeled as (1). Assume that transmitted power is limited to $E[X^2] \leq P$. Since the channels are degraded, at time i, $Y_{1i} = X_i + N_{1i}$, $Y_{2i} = Y_{1i} + N^{'}_{2i}$ and $Z_i = Y_{2i} + N^{'}_{3i}$, where N_{1i} are i.i.d $\mathcal{N}(0, \sigma_1^2)$, $N^{'}_{2i}$ are i.i.d $\mathcal{N}(0, \sigma_2^2 - \sigma_1^2)$, and $N^{'}_{3i}$'s are i.i.d $\mathcal{N}(0, \sigma_3^2 - \sigma_2^2)$. The following theorem illustrates the secrecy capacity region of our channel.

Theorem 2 *The secrecy capacity region of the Gaussian broadcast channel with confidential messages is given by the set of rates pairs (R_1, R_2) such that*

$$\begin{aligned} R_1 &\leq C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_3^2}\right), && (13)\\ R_2 &\leq C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_3^2}\right). \end{aligned}$$

for some $\alpha \in [0,1]$ and $C(x) = \frac{1}{2}\log(1+x)$.

Proof:

Achievability: Let $U \sim \mathcal{N}(0, (1-\alpha)P)$ and $X^{'} \sim \mathcal{N}(0, \alpha P)$ be independent and $X = U + X^{'} \sim \mathcal{N}(0, P)$. Therefore, the amount of $I(X;Y_1|U)$, $I(X;Z|U)$, $I(U;Z)$ and $I(U;Y_2)$ can be easily evaluated. Now consider the following secure superposition coding scheme:

1) *Codebook Generation*: Generate $2^{nI(U;Y_2)}$ i.i.d Gaussian codewords u^n with average power $(1-\alpha)P$ and randomly distribute these codewords into 2^{nR_2} bins. Then index each bin by $w_2 \in \{1, 2, ..., 2^{nR_2}\}$. Generate an independent set of $2^{nI(X^{'};Y_1)}$ i.i.d Gaussian codewords $x^{'n}$ with average power αP. Then, Randomly distribute them into 2^{nR_1} bins. Index each bin by $w_1 \in \{1, 2, ..., 2^{nR_1}\}$.

2) *Encoding*: To send messages w_1 and w_2, the transmitter randomly chooses one of the codewords in bin w_2, (say u^n) and one of the codewords in bin w_1 (say $x^{'n}$). Then, simply transmits $x^n = u^n + x^{'n}$.

3) *Decoding*: The received signal at the legitimate receivers are y_1^n and y_2^n respectively. Receiver D_2 determines the unique u^n such that (u^n, y_2^n) are jointly typical and declares the index of the bin containing u^n as the message received. If there is none of such or more than of one such, an error is declared. Receiver D_1 uses successive cancelation method; first decodes u^n and subtracts off y_1^n and then looks for the unique $x^{'n}$ such that $(x^{'n}, y_1^n)$ are jointly typical and declares the indexes of the bin containing $x^{'n}$ as the message received.

The error probability analysis and equivocation calculation is given in [1] and may therefor be omitted here.

Converse: R_2 is bounded as follows (See [1] for details):

$$nR_2 \leq I(Y_2^n; U^n|Z) = h(Y_2^n|Z^n) - h(Y_2^n|U^n, Z^n) \qquad (14)$$

where h is differential entropy. The classical entropy power inequality states that:

$$2^{\frac{2}{n}h(Y_2^n + N_3^{'n})} \geq 2^{\frac{2}{n}h(Y_2^n)} + 2^{\frac{2}{n}h(N_3^{n'})}$$

Therefore, $h(Y_2|Z)$ can be written as follows:

$$\begin{aligned} h(Y_2^n|Z^n) &= h(Z^n|Y_2^n) + h(Y_2^n) - h(Z^n)\\ &= \frac{n}{2}\log 2\pi e(\sigma_3^2 - \sigma_2^2) + h(Y_2^n)\\ &\quad - h(Y_2^n + N_3^{n'})\\ &\leq \frac{n}{2}\log 2\pi e(\sigma_3^2 - \sigma_2^2) + h(Y_2^n)\\ &\quad - \frac{n}{2}\log(2^{\frac{2}{n}h(Y_2^n)} + 2\pi e(\sigma_3^2 - \sigma_2^2)) \end{aligned}$$

On the other hand, for any fixed $a \in \mathcal{R}$, the function

$$f(t, a) = t - \frac{n}{2}\log(2^{\frac{2}{n}t} + a)$$

is concave in t and has a global maximum at $t = t_{max}$. Thus, $h(Y_2^n|Z^n)$ is maximized when Y_2^n (or equivalently X^n) has Gaussian distribution. Hence,

$$\begin{aligned} h(Y_2^n|Z^n) &\leq \frac{n}{2}\log 2\pi e(\sigma_3^2 - \sigma_2^2) + \frac{n}{2}\log 2\pi e(P + \sigma_2^2)\\ &\quad - \frac{n}{2}\log 2\pi e(P + \sigma_3^2)\\ &= \frac{n}{2}\log\left(\frac{2\pi e(\sigma_3^2 - \sigma_2^2)(P + \sigma_2^2)}{P + \sigma_3^2}\right) \qquad (15) \end{aligned}$$

Now consider the term $h(Y_2^n|U^n, Z^n)$. This term is lower bounded with $h(Y_2^n|U^n, X^n, Z^n) = \frac{n}{2}\log 2\pi e(\sigma_2^2)$ which is greater than $\frac{n}{2}\log 2\pi e(\frac{\sigma_2^2(\sigma_3^2-\sigma_2^2)}{\sigma_3^2})$. Hence,

$$\frac{n}{2}\log 2\pi e(\frac{\sigma_2^2(\sigma_3^2-\sigma_2^2)}{\sigma_3^2}) \leq h(Y_2^n|U^n,Z^n) \leq h(Y_2^n|Z^n) \quad (16)$$

Inequalities (15) and (16) imply that there exists an $\alpha \in [0,1]$ such that

$$h(Y_2^n|U^n,Z^n) = \frac{n}{2}\log\left(\frac{2\pi e(\sigma_3^2-\sigma_2^2)(\alpha P+\sigma_2^2)}{\alpha P+\sigma_3^2}\right) \quad (17)$$

Substituting (17) and (15) into (14) yields the desired bound

$$\begin{aligned} nR_2 &\leq h(Y_2^n|Z^n) - h(Y_2^n|U^n,Z^n) \\ &\leq \frac{n}{2}\log\left(\frac{(P+\sigma_2^2)(\alpha P+\sigma_3^2)}{(P+\sigma_3^2)(\alpha P+\sigma_2^2)}\right) \\ &= nC\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - nC\left(\frac{(1-\alpha)P}{\alpha P+\sigma_3^2}\right) \quad (18) \end{aligned}$$

Note that the left side of (17), can be written as $h(Y_2^n,Z^n|U^n) - h(Z^n|U^n)$ which implies that

$$h(Y_2^n|U^n) - h(Z^n|U^n) = \frac{n}{2}\log\left(\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_3^2}\right) \quad (19)$$

Since $\sigma_1^2 \leq \sigma_2^2 \leq \sigma_3^2$, there exists a $0 \leq \beta \leq 1$ such that $\sigma_2^2 = \beta\sigma_1^2 + (1-\beta)\sigma_3^2$ or equivalently $Y_2^n = \mathbf{A}Y_1^n + \overline{\mathbf{A}}Z^n$ where, $\mathbf{A} = \sqrt{\beta}\mathbf{I}_n$ and $\overline{\mathbf{A}} = \sqrt{1-\beta}\mathbf{I}_n$. According to the entropy power inequality and the fact that $h(\mathbf{A}X^n) = h(X^n) + \log(\det(\mathbf{A}))$, we have

$$\begin{aligned} &\frac{n}{2}\log\left(\beta 2^{\frac{2}{n}h(Y_1^n|U^n)} + (1-\beta)2^{\frac{2}{n}h(Z^n|Uv)}\right) - h(Z^n|U^n) \\ &\leq \frac{n}{2}\log\left(\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_3^2}\right) \quad (20) \end{aligned}$$

After some manipulation on (20), we have

$$\begin{aligned} &h(Y_1^n|U^n) - h(Z^n|U^n) \\ &\leq \frac{n}{2}\log\left(\frac{\alpha P+\sigma_2^2+(\beta-1)(\alpha P+\sigma_3^2)}{\beta(\alpha P+\sigma_3^2)}\right) \\ &= \frac{n}{2}\log\left(\frac{\alpha P+\sigma_1^2}{\alpha P+\sigma_3^2}\right) \quad (21) \end{aligned}$$

The rate R_1 is bounded as follows

$$\begin{aligned} nR_1 &\leq I(X^n;Y_1^n|U^n) - I(X^n;Z^n) + I(U^n;Z^n) \quad (22) \\ &= h(Y_1^n|U^n) - h(Y_1^n|X^n,U^n) + h(Z^n|X^n) \\ &- h(Z^n|U^n) \\ &= h(Y_1^n|U^n) - h(Z^n|U^n) + \frac{n}{2}\log(\frac{\sigma_3^2}{\sigma_1^2}) \\ &\overset{(a)}{\leq} \frac{n}{2}\log\left(\frac{\alpha P+\sigma_1^2}{\alpha P+\sigma_3^2}\frac{\sigma_3^2}{\sigma_1^2}\right) \\ &= nC\left(\frac{\alpha P}{\sigma_1^2}\right) - nC\left(\frac{\alpha P}{\sigma_3^2}\right) \end{aligned}$$

where (a) follows from (21). ■

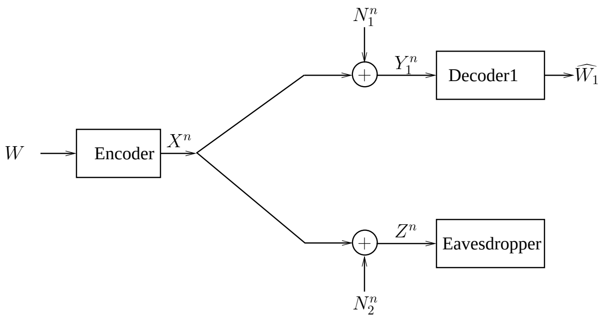

Fig. 2. Gaussian Wire-tap Channel

IV. A Multilevel Coding Approach to the Slowly Fading Wire-Tap channel

As an application of the previous section, we describe a strategy for a slowly fading wire-tap channel in this section. We use the secure degraded broadcast channel from the previous section to develop this broadcast strategy. This strategy assumes an infinite number of ordered receivers which are related to different channel realizations. First, some preliminaries and definitions are given, and then the multilevel coding approach is described. Here, we follow the steps of the broadcast strategy for the slowly fading point-to-point channel of [8].

A. Channel Model

Consider a wire-tap channel as depicted in Fig.2. The transmitter wishes to communicate with the destination in the presence of an eavesdropper. At time i, the signal received by the destination and the eavesdropper are given as follows

$$\begin{aligned} Y_i &= h_M X_i + N_{1i} \quad (23) \\ Z_i &= h_E X_i + N_{2i} \end{aligned}$$

where X_i is the transmitted symbol and h_M, h_E are the fading coefficients from the source to legitimate receiver and to the eavesdropper respectively. The fading power gains of the main and eavesdropper's channels are denoted by $s = |h_M|^2$ and $s^{'} = |h_E|^2$ respectively. N_{1i}, N_{2i} are the additive noise samples, which are Gaussian i.i.d with zero mean and unit variance. We assume that the main channel is slowly fading and the eavesdropper's channel is fixed. We also assume that the transmitter knows only channel state information of the eavesdropper channel. For each realization of h_M there is an achievable rate. Since the transmitter has no information about the main channel and the channel is slowly fading then the system is non-ergodic. Here, we are interested in the average rate for various independent transmission blocks. The average shall be calculated over the distribution of h_M.

B. The Secret Multilevel Coding Approach

An equivalent broadcast channel for our channel is depicted in Fig.3. In this Figure, the transmitter sends an infinite number of secure layers of coded information. The receiver is

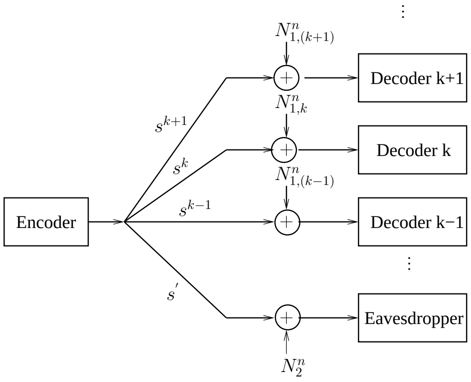

Fig. 3. Equivalent Broadcast Channel Model.

equivalent to a continuum of ordered users. For each channel realization h^k_M with the fading power gain s^k,the information rate is $R(s^k)$. We drop the superscript k, and denote the realization of the random variable S of fading power by s. Therefore, the transmitter views the main channel as secure degraded Gaussian broadcast channel with infinite number of receivers. The result of the previous section for two receiver can easily extended to arbitrary number of users. According to theorem 2, the incremental differential secure rate is then given by

$$dR(s)= \frac{1}{2}\left[\log\left(1+\frac{s\rho(s)ds}{1+sI(s)}\right)-\log\left(1+\frac{s^{'}\rho(s)ds}{1+s^{'}I(s)}\right)\right]^+$$

where $\rho(s)ds$ is the transmit power of a layer parameterized by s, intended for receiver s. As an approximation, the $\log$ function may be discardedx. The function $I(s)$ represents the interference noise of the receivers indexed by $u > s$ which cannot be canceled at receiver s. The interference at receiver s is, therefore, given by

$$I(s) = \int_s^\infty \rho(u)d(u) \qquad (24)$$

The total transmitted power is the summation of the power assigned to the layers

$$P = I(0) = \int_0^\infty \rho(u)d(u) \qquad (25)$$

The total achievable rate for a fading realization s is an integration of the incremental rates over all receivers which successfully can decode the respective layer

$$R(s) = \frac{1}{2}\int_0^s \left[\frac{u\rho(u)du}{1+uI(u)} - \frac{s^{'}\rho(u)du}{1+s^{'}I(u)}\right]^+ \qquad (26)$$

Our goal is to maximize the total average rate over all fading realizations with respect to the power distribution $\rho(s)$ (or equivalently, with respect to $I(u)$, $u \geq 0$) under the power constraint of 25. The optimization problem can be written as

$$R_{\max}= \max_{I(u)} \int_0^\infty R(u)f(u)du \qquad (27)$$
$$s.t$$
$$P= I(0) = \int_0^\infty \rho(u)d(u)$$

where $f(u)$ is the probability distribution function (pdf) of the fading power S. Nothing that the cumulative distribution function (cdf) is $F(u) = \int_0^u f(a)da$, the optimization problem can be written as

$$R_{\max}= \frac{1}{2}\max_{I(u)} \int_0^\infty (1-F(u))G(u)du \qquad (28)$$
$$s.t$$
$$P= I(0) = \int_0^\infty \rho(u)d(u)$$

where $G(u) = \left[\frac{u}{1+uI(u)} - \frac{s^{'}}{1+s^{'}I(u)}\right]^+ \rho(u)$. Note that $\rho(u) = -I^{'}(u)$. The functional of (28), therefore, can be written as

$$J(x, I(x), I^{'}(x)) = \qquad (29)$$
$$-(1-F(x))\left[\frac{x}{1+xI(x)} - \frac{s^{'}}{1+s^{'}I(x)}\right]^+ I^{'}(x)$$

The necessary condition for maximization of a integral of J over x is

$$J_I - \frac{d}{dx}J_{I^{'}} = 0 \qquad (30)$$

where J_I means derivation of function J with respect to I and similarly $J_{I'}$ is the derivation of J with respect to $I^{'}$. After some mathematic, The optimum $I(x)$ is given by

$$I(x) = \begin{cases} \frac{1-F(x)-(x-s^{'})f(x)}{s^{'}(1-F(x))+x(x-s^{'})f(x)}, & \max\{s^{'}, x_0\} \leq x \leq x_1; \\ 0, & \text{else.} \end{cases}$$

where x_0 is determined by $I(x_0) = P$, and x_1 by $I(x_1) = 0$.

As a special case, consider the Rayleigh flat fading channel. The random variable S is exponentially distributed with

$$f(s) = e^{-s}, \qquad F(s) = 1 - e^{-s}, \qquad s \geq 0 \qquad (31)$$

Substituting of $f(s)$ and $F(s)$ into the optimum $I(s)$ and taking the derivative with respect to the fading power s yields to the following optimum transmitter power policy

$$\rho(s)= -\frac{d}{ds}I(s) = \begin{cases} \frac{-s^2+2(s^{'}+1)s-s^{'2}}{(s^2-s^{'}s+s^{'})^2}, & \max\{s^{'}, s_0\} \leq s \leq s_1; \\ 0, & \text{else.} \end{cases}$$

where s_0 is the solution of the equation $I(s_0) = P$, which is

$$s_0 = \frac{-1 + Ps^{'} + \sqrt{P^2 s^{'2} + 2P(1-2P)s^{'} + 4P + 1}}{2P}$$

and s_1 is determined by $I(s_1) = 0$, which is

$$s_1 = 1 + s^{'}$$

V. Conclusion

A generalization of the Gaussian wire-tap channel to the case of two receivers and one eavesdropper is considered. We established the perfect secrecy capacity region for this channel. The achievability coding scheme is a secret superposition scheme where randomization in the first layer helps the secrecy of the second layer. The converse proof combines the converse proof for the Gaussian broadcast channel without security constraint and the perfect secrecy constraint. We proved that the secret superposition scheme with Gaussian codebook is optimal in G-BCCs. The converse proof is based on the the entropy power inequality. Based on the rate characterization of the secure Gaussian broadcast channel, a multilevel coding approach for the slowly fading wire-tap is used. We assumed that the transmitter only knows the eavesdropper's channel. In this approach, source node sends secure layered coding and the receiver viewed as a continuum ordered users. We derived optimum power allocation for the layers which maximizes the total average

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, vol. 28, pp. 656-715, October. 1949.

[2] A. Wyner, "The Wire-tap Channel",*Bell System Technical Journal*, vol. 54, pp. 13551387, 1975

[3] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages", *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339348, May 1978.

[4] G. Bagherikaram, A. S. Motahari and A. K. Khandani, "The Secrecy Rate Region of the Broadcast Channel", *Allerton Conference on Communications, Control and Computing,*, September 2008.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian Wiretap Channel", *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451456, July 1978.

[6] P. Parada and R. Blahut, "Secrecy Capacity of SIMO and Slow Fading Channels", *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sep. 2005, pp. 21522155.

[7] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels", *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, July 2006, pp. 356360.

[8] S. Shamai and A. Steiner, "A Broadcast Approach for a Single-User Slowly Fading MIMO Channel", *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 26172635, October 2003.