Secret-Key Sharing Based on Layered Broadcast Coding over Fading Channels

Xiaojun Tang
WINLAB, Rutgers University

Ruoheng Liu
Princeton University

Predrag Spasojević
WINLAB, Rutgers University

H. Vincent Poor
Princeton University

***Abstract*—A secret-key sharing strategy based on layered broadcast coding is introduced for slow fading channels. In the model considered, Alice wants to share a key with Bob while keeping the key secret from a passive eavesdropper, Eve. Both Alice-Bob and Alice-Eve channels are assumed to undergo slow fading, and perfect channel state information (CSI) is assumed to be known only at the receivers during the transmission. Layered coding facilitates adapting the reliably decoded rate at Bob to the actual channel state without CSI available at Alice. The index of a reliably decoded layer is sent back to Alice via a public and error-free channel, which is exploited by Alice and Bob to generate the secret key. In this paper, the secrecy key rate is derived. In addition, the optimal power distribution over coded layers is characterized. It is shown that layered coding can increase the secrecy key rate significantly compared with single-level coding.**

I. Introduction

Wireless secrecy has attracted considerable research interest due to the concern that wireless communication is highly vulnerable to security attacks, particularly eavesdropping attacks. Much recent research was motivated by Wyner's wire-tap channel model [1] where the transmission between two legitimate users (Alice and Bob) is eavesdropped upon by Eve via a degraded channel. The secrecy level in this model is measured by the equivocation rate at Eve. Wyner showed that secret communication is possible without sharing a secret-key between legitimate users. Later, Csiszár and Körner generalized Wyner's model to consider general broadcast channels in [2].

Interestingly, the wireless medium provides its own endowments that facilitate defending against eavesdropping. One such endowment is fading [3], whose effects on secret transmission has been studied in [4]–[6]. In these works, assuming that all communicating parties have perfect channel state information (CSI) prior to transmission, the ergodic secrecy capacity has been derived. The ergodic scenario in which Alice has no CSI about Eve's channel (but knows the channel statistics) has also been studied in [4]. When Alice does not know any prior CSI (except channel statistics), but can receive 1-bit of automatic repeat request (ARQ) feedback per channel coherence interval from Bob reliably, the throughput of several secure hybrid-ARQ protocols has been derived in [7].

The work was supported by the National Science Foundation under Grants CNS-06-25637, CCF-07-28208 and CCF-0729142.

Arguably, the most useful application of (keyless) secret message transmission is secret-key sharing as discussed in [8], [9] and other related works, although there exist some fundamental differences between these two problems. Roughly speaking, in secret message transmission, the message is known to Alice before starting the transmission; while in secret-key sharing, the key (a secret message to be shared by Alice and Bob) can be established (and become known to Alice) after the transmission is completed.

In this paper, we consider a key-sharing problem in which Alice wants to share a key with Bob while keeping it secret from Eve. Alice-Bob and Alice-Eve channels are assumed to undergo slow fading, and CSI is assumed known only at the receivers during the transmission. The key-sharing scheme consists of a communication phase and a key-generation phase. The communication phase is based on Gaussian layered broadcast coding. The index of a reliably decoded layer at Bob is sent back to Alice through a public and error-free channel. The key-generation phase is based on the layer index and follows Wyner's secrecy binning scheme [1]. We derive the secrecy key rate and also characterize the optimal power distribution over coded layers. Interestingly, layered broadcast coding creates interference, where the undecodable layers (for Bob) play the role of self-interference. We show that the best Eve can do is to treat the interference as noise (as Bob does), and therefore cannot benefit from the structure of the interference either.

There are several closely related works. Layered coding over slowly fading single-input single-output (SISO) channels was originally introduced by Shamai in [10] and discussed in more detail in [11]. The results in this paper are consistent with [10] and [11] if the additional secrecy constraint is disregarded. An ARQ-based secret-key sharing scheme was studied in [12], where single-level coding is used. The scheme can be viewed as a special case of the proposed layered-coding scheme. Finally, the problem of secret communication over a medium with interference was discussed in [13] for a more general (but non-fading) setting.

II. System Model

As depicted in Fig. 1, we consider a three-terminal model, in which Alice and Bob want to share a secret key in the presence of Eve (a passive eavesdropper).

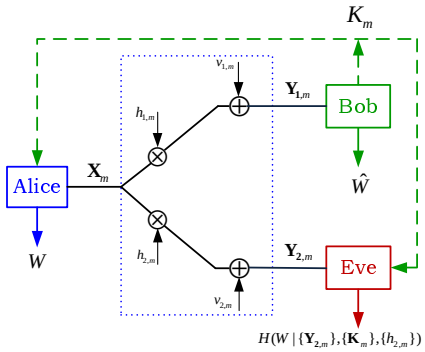

Fig. 1. Alice and Bob want to agree on a key ($W = \hat{W}$), while keeping the key secret from Eve ($H(W|\mathbf{Y}_2, \mathbf{H}_2, \mathbf{K})/n \to 0$).

A. Channel Model

The Alice-Bob and Alice-Eve channels undergo block fading, in which the channel gains are constant within a block while varying independently from block to block [3]. We assume that each block is associated with a time slot of duration T and bandwidth W; that is, $n_1 = \lfloor 2WT \rfloor$ real symbols can be sent in each slot. We also assume that the number of channel uses within each slot (i.e., n_1) is large enough to allow for the invocation of random coding arguments.

In a certain time slot indexed by m, Alice sends $\mathbf{x}_m$, which is a vector of n_1 real symbols. Bob receives $\mathbf{y}_{1,m}$ through the channel gain $h_{1,m}$ and Eve receives $\mathbf{y}_{2,m}$ through the channel gain $h_{2,m}$. A discrete time baseband-equivalent block-fading channel model can be expressed as

$$\mathbf{y}_{t,m} = \sqrt{h_{t,m}}\mathbf{x}_m + \mathbf{z}_{t,m} \tag{1}$$

for $t = 1, 2$, where $\{\mathbf{z}_{t,m}\}$ are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian $\mathcal{N}(0, 1)$ random sequences. Without any confusion, we drop the index m and denote h_t as a random channel realization. We assume that it is a real random variables with a probability density function (PDF) f_t and a cumulative distribution function (CDF) F_t, for each $t = 1, 2$.

Furthermore, we assume a short term power constraint (excluding power variation across time slots) such that the average power of the signal $\mathbf{x}_m$ per slot has the constraint that $E[\|\mathbf{x}_m\|^2] \le n_1 P$ for every m.

There exists an error-free feedback channel from Bob to Alice, through which Bob sends back k_m for time slot m. The feedback channel is assumed to be public, and therefore k_m is obtained by both Alice and Eve without any error.

B. Secret Key Sharing Protocol

The secret-key sharing protocol consists of two phases: a communication phase and a key-generation phase.

1) Communication Phase: We assume that the transmission during the communication phase takes place over M time slots. That is, Alice sends a sequence of signals $\mathbf{x} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M]$ to the channel. Accordingly, Bob receives from his channel a sequence of signals denoted by $\mathbf{y}_1 = [\mathbf{y}_{1,1}, \mathbf{y}_{1,2}, \ldots, \mathbf{y}_{1,M}]$ and Eve receives $\mathbf{y}_2 = [\mathbf{y}_{2,1}, \mathbf{y}_{2,2}, \ldots, \mathbf{y}_{2,M}]$ from her channel. We let $n = Mn_1$ denote the number of symbols sent by Alice in the communication phase.

Let $\mathbf{h}_1 = [h_{1,1}, \ldots, h_{1,M}]$ and $\mathbf{h}_2 = [h_{2,1}, \ldots, h_{2,M}]$ denote vectors whose elements are the power gains of the Alice-Bob and Alice-Eve channels, respectively. We assume that Bob and Eve know their own channel gains perfectly; Alice does not know the CSI before its transmission, except for the channel statistics. After the communication, Bob uses the feedback channel to send $\mathbf{k} = [k_1, \ldots, k_M]$, which is obtained by both Alice and Eve.

2) Key-Generation Phase: The communication phase is followed by a key-generation phase, in which both Alice and Bob generate the key based on the signals sent and received. Let $\mathcal{W} = \{1, 2, \ldots, 2^{nR_s}\}$, where R_s represents the secrecy key rate. Alice generates a secret key $w \in \mathcal{W}$ by using a decoding function f_a, i.e., $w = f_a(\mathbf{x}, \mathbf{k})$. Bob generates the secret key $\hat{w} \in \mathcal{W}$ by using a decoding function f_b, i.e.,

$$\hat{w} = f_b(\mathbf{y}_1, \mathbf{h}_1, \mathbf{k}) = f_b(\mathbf{y}_1, \mathbf{h}_1), \tag{2}$$

where the second equality holds since we assume that $\mathbf{k}$ is a deterministic function of $\mathbf{y}_1$ and $\mathbf{h}_1$.

The secrecy level at Eve is measured by the equivocation rate R_e defined as the entropy rate of the key W conditioned upon the observations at Eve, i.e.,

$$R_e \triangleq \frac{1}{n} H(W|\mathbf{Y}_2, \mathbf{H}_2, \mathbf{K}).^1 \tag{3}$$

A secrecy key rate R_s is achievable if the conditions

$$\Pr\left(W = \hat{W}\right) \ge 1 - \epsilon, \tag{4}$$

$$\text{and} \qquad R_e \ge R_s - \epsilon, \tag{5}$$

are satisfied for any $\epsilon > 0$ as the number of channel uses $n \to \infty$.

III. Key Sharing Based on Layered Coding

In this section, we introduce a secret-key sharing scheme, in which Gaussian layered broadcast coding is used for the communication phase, and random secrecy binning is used for the key generation phase. Before presenting the scheme, we first introduce Gaussian layered broadcast coding.

A. Gaussian Layered Broadcast Coding

As an example, we consider the Alice-Bob channel given by (1). First, let us assume there are L layers in a layered coding scheme. That is, the transmitted codeword is a superposition of L codewords, i.e.,

$$\mathbf{x} = \sum_{l=1}^{L} \mathbf{x}^{[l]} \tag{6}$$

where $\mathbf{x}^{[l]}$ is a codeword from codebook $\mathcal{C}^{[l]}$ with a rate $r^{[l]}$ and a constant power $p^{[l]}$ for $l = 1, \ldots, L$, and the

[1] Capital letters W, $\hat{W}$, $\mathbf{X}$, $\mathbf{Y}_1$, $\mathbf{Y}_2$, H_1, H_2, $\mathbf{H}_1$, $\mathbf{H}_2$, and $\mathbf{K}$ represent the random variables (or vectors), while corresponding realizations are represented by lower-case letters.

total power is constrained by $\sum_{l=1}^{L} p^{[l]} = P$. In general, L depends on the cardinality of the random channel variable (H_1). For a Gaussian fading channel, a continuum of code layers ($L \to \infty$) is required. For a certain fading realization $h^{[l]}$, the receiver can decode up to the l-th layer, i.e., the codewords $\{\mathbf{x}^{[1]}, \ldots, \mathbf{x}^{[l]}\}$ can be decoded reliably, while the codewords $\{\mathbf{x}^{[l+1]}, \ldots, \mathbf{x}^{[L]}\}$ are undecodable. The decoding is based on successive interference cancelation. More specifically, in the decoding process, the receiver first decodes $\mathbf{x}^{[1]}$ by treating the remaining codewords ($\{\mathbf{x}^{[i]}, i > 1\}$) as interference. After decoding $\mathbf{x}^{[1]}$, the receiver will subtract $\mathbf{x}^{[1]}$ and then decode $\mathbf{x}^{[2]}$ by treating the remaining codewords ($\{\mathbf{x}^{[i]}, i > 2\}$) as interference. This process repeats until the l-th layer $\mathbf{x}^{[l]}$ is decoded reliably by treating the remaining codewords ($\{\mathbf{x}^{[i]}, i > l\}$) as interference. Note that this predetermined ordering can be achieved because of the degraded nature of Gaussian SISO channels.

When a continuum of layers is used, the transmitter sends an infinite number of layers of coded information. Each layer conveys a fractional rate, denoted by dR, whose value depends on the index of the layer. We refer to s, the realization of the fading power, as a continuous index. The incremental differential rate is given by[2]

$$dR(s) = \log\left(1 + \frac{s\rho(s)ds}{1 + sI(s)}\right) = \frac{s\rho(s)ds}{1 + sI(s)}, \qquad (7)$$

where $\rho(s)ds$ is the transmit power of a layer parameterized by s, and also represents the transmit power distribution over coded layers. The layers indexed by $u > s$ are undecodable and function as additional interference, whose power is denoted by $I(s)$ and is given by

$$I(s) = \int_s^{\infty} \rho(u)du. \qquad (8)$$

The total power over all layers is constrained by

$$I(0) = \int_0^{\infty} \rho(u)du = P. \qquad (9)$$

B. Secret Key Sharing Based on Layered Coding

In this section, we discuss the key sharing scheme based on Gaussian layered coding.

1) Codebook Construction: We need two types of codebooks, each of which is used for the communication or key-generation phase, respectively.

The codebook used for the communication phase consists of a continuum of coded layers represented by $\{\mathcal{C}(2^{n_1 dR(s)}, n_1)\}$, where n_1 is the codeword length and $dR(s)$ is the (incremental differential) rate at layer s. The (sub-)codebook for each layer is generated randomly and independently. That is, for any codebook $\mathcal{C}(2^{n_1 dR(s)}, n_1)$, we generate $2^{n_1 dR(s)}$ codewords $x^{[s]}(w)$, where $w = 1, 2, \ldots, 2^{n_1 dR(s)}$, by choosing the $n_1 2^{n_1 dR(s)}$ Gaussian symbols (with power $\rho(s)ds$) independently at random.

[2]All logarithms are to the natural base, and thus rates are in terms of nats per second per Hertz.

The codebook used for the key generation phase is based on Wyner's secrecy coding [1], [4]. By letting

$$R = \int_0^{\infty} \int_0^{H_1} \frac{s\rho(s)ds}{1 + sI(s)} dF_1(H_1), \qquad (10)$$

we first generate all binary sequences $\{\mathcal{B}\}$ of length $n(R - \epsilon)$, where $n = Mn_1$. The sequences $\{\mathcal{B}\}$ are then randomly and uniformly grouped into nR_s groups each with $n(R - R_s - \epsilon)$ sequences. Each secret key $w \in \{1, \ldots, 2^{nR_s}\}$ is then randomly assigned to a group, denoted by $\mathcal{B}(w)$.

2) Communication Phase: The communication takes places over M time slots. At time slot $m \in [1, M]$, Alice first randomly selects a message $w_m^{[s]} \in \{1, \ldots, 2^{n_1 dR(s)}\}$ for coded layer s, independent of the message chosen for other layers. For convenience, we use w_m to represent the total message sent in time slot m (through all layers). Then, Alice sends a superposition of all layers to the channel.

Bob receives $\mathbf{y}_{1,m}$ and tries to decode all his decodable layers, which depends on his channel state $h_{1,m}$. For convenience, we use $w_m^{[D_1]}$ to denote the set of layers reliably decoded by Bob, and $w_m^{[\bar{D}_1]}$ to denote the set of layers undecodable to Bob in time slot m. After decoding, Bob sends back the index of the highest decodable layer (represented by k_m) to Alice. This completes the transmission in time slot m. The communication phase ends when all M (independent) transmissions are completed.

3) Key-Generation Phase: Once the communication phase is completed, both Alice and Bob can generate the secret key. Based on the feedback sequence $\mathbf{k} = \{k_m\}$, Alice generates a binary sequence $\mathbf{v}$ from all the messages reliably decoded by Bob (across all layers and time slots) based on a deterministic one-to-one mapping Φ as

$$\mathbf{v} = \Phi(\{w_m^{[D_1]}, m = 1, \ldots, M\}). \qquad (11)$$

Alice then looks up in the key-generation codebook for a w such that $\mathbf{v} \in \mathcal{B}(w)$, and outputs w as the secret key generated. Note that all those messages are decoded by Bob, and therefore Bob can generate the same sequence $\mathbf{v}$ and the same key w as Alice does.

IV. Secrecy Key Rate

In this section, we present the secrecy key rate achieved, and the optimal distribution of power over coded layers. Due to space limitations, we defer all proofs to an upcoming long version of this paper.

A. Layered-Coding Based Key Sharing

The following result characterizes the secrecy rate when the power distribution is given.

Theorem 1: For a given power distribution $\rho(s)$ over layers indexed by s, the secrecy key rate of the layered-coding based key sharing scheme is

$$R_s = \int_0^{\infty} \int_0^{H_1} \Delta(H_1, H_2) dF_2(H_2) dF_1(H_1), \qquad (12)$$

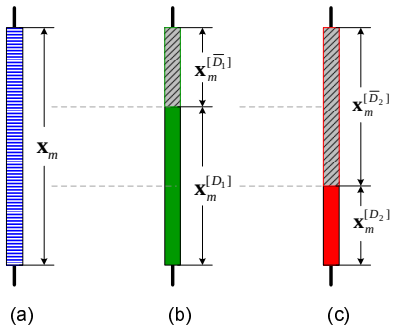

Fig. 2. (a) Coded layers sent by Alice, (b) decodable and undecodable layers for Bob, and (c) decodable and undecodable layers for Eve, in time slot m with the channel gains $h_1 > h_2$.

where $\Delta(H_1, H_2)$ is given by

$$\Delta(H_1, H_2) = \int_{H_2}^{H_1} \left[\frac{s\rho(s)}{1 + sI(s)} - \frac{H_2\rho(s)}{1 + H_2 I(s)} \right] ds \quad (13)$$

and

$$I(s) = \int_s^{\infty} \rho(u)du \quad \text{with } I(0) = P. \quad (14)$$

We discuss some insights from Theorem 1. First, except for the rare case in which H_1 is always smaller than H_2, R_s is positive. Note that this is impossible without feedback (one-way communication). Furthermore, R_s can be written as

$$R_s = \mathbb{E}_{H_1,H_2} \left[\tilde{\Delta}(H_1, H_2) \right], \quad (15)$$

where

$$\tilde{\Delta}(H_1, H_2) = \begin{cases} \Delta(H_1, H_2) & \text{if } H_1 > H_2 \\ 0 & \text{otherwise.} \end{cases} \quad (16)$$

The key rate R_s is the average of rewards (designated by $\tilde{\Delta}(H_1, H_2)$) collected from all possible channel realizations. Positive rewards are obtained from the time slots in which Bob's channel is better than Eve's channel ($H_1 > H_2$). On the other hand, when $H_1 \leq H_2$, the reward is zero.

We focus on a particular time slot m in which $(H_1, H_2) = (h_1, h_2)$ with $h_1 > h_2$, and use $\mathbf{x}_m$ to denote all layers sent in the slot. As depicted in Fig. 2, $\mathbf{x}_m$ can be divided as

$$\mathbf{x}_m = \mathbf{x}_m^{[D_2]} \cup \left(\mathbf{x}_m^{[D_1]} \cap \mathbf{x}_m^{[\bar{D}_2]} \right) \cup \mathbf{x}_m^{[\bar{D}_1]}, \quad (17)$$

where $\mathbf{x}_m^{[D_1]}$ and $\mathbf{x}_m^{[\bar{D}_1]}$ denote the set of decodable and undecodable layers at Bob, respectively, and $\mathbf{x}_m^{[D_2]}$ and $\mathbf{x}_m^{[\bar{D}_2]}$ denote the set of decodable and undecodable layers at Eve, respectively. Note that $\mathbf{x}_m^{[D_1]} \supset \mathbf{x}_m^{[D_2]}$ since $h_1 > h_2$.

Both Alice and Bob can decode $\mathbf{x}_m^{[D_2]}$, and neither of them can decode $\mathbf{x}_m^{[\bar{D}_1]}$. Therefore, a nonzero reward $\Delta(h_1, h_2)$ comes from the set of layers $\mathbf{x}_m^{[D_1]} \cap \mathbf{x}_m^{[\bar{D}_2]}$. To show this, we rewrite (13) as

$$\Delta(h_1, h_2) = \int_{h_2}^{h_1} \frac{s\rho(s)ds}{1 + sI(s)} - \int_{h_2}^{h_1} \frac{h_2\rho(s)ds}{1 + h_2 I(s)}. \quad (18)$$

The first term at the right hand side of (18) is the sum-rate decoded by Bob from $\mathbf{x}_m^{[D_1]} \cap \mathbf{x}_m^{[\bar{D}_2]}$ (by decoding and canceling $\mathbf{x}_m^{[D_2]}$ first, and treating the interference term $\mathbf{x}_m^{[\bar{D}_1]}$ as noise). Furthermore, the second term can be written as

$$\int_{h_2}^{h_1} \frac{h_2\rho(s)ds}{1 + h_2 I(s)} = \log \left(1 + \frac{h_2 \left[I(h_2) - I(h_1) \right]}{1 + h_2 I(h_1)} \right). \quad (19)$$

By noticing that $I(h_2) - I(h_1)$ is the total power used for the layers $\mathbf{x}_m^{[D_1]} \cap \mathbf{x}_m^{[\bar{D}_2]}$, and $I(h_1)$ is the total power used for the layers $\mathbf{x}_m^{[\bar{D}_1]}$, (19) gives the rate of information that Eve can possibly deduce from $\mathbf{x}_m^{[D_1]} \cap \mathbf{x}_m^{[\bar{D}_2]}$ through her channel with power gain h_2. An interesting finding here is that what the best Eve can do is to treat the interference term $\mathbf{x}_m^{[\bar{D}_1]}$ as noise (as Bob does), and therefore cannot benefit from the structure of interference either.

Due to the absence of CSI at the transmitter before the transmission, the layered broadcast coding strategy creates a medium with interference, where the undecodable layers play the role of *self-interference*. We remark here that this is a special case of secret communication over a medium with interference as discussed in [13].

B. Single-Level-Coding Based Key Sharing

When single-level coding is used, self-interference does not occur. In this case, the following secrecy key rate can be achieved.

Lemma 1: [12, Theorem 1] The secrecy key rate of a single-level-coding based scheme is given by

$$R_s = \Pr \left[R_1 \leq \log(1 + H_1 P) \right] \mathbb{E}_{H_2} \left[R_1 - \log \left(1 + H_2 P \right) \right]^+, \quad (20)$$

where R_1 is the rate of single-level coding.

Comparing with the layered-coding based scheme, the single-level-coding based approach has lower decoding complexity, and requires less feedback (only 1-bit per time slot). However, it is sub-optimal in general. Also, a single-level coding scheme can be considered as a special case of a layered-coding scheme, in which all power is allocated to one layer. This again motivates us to find the power distribution for optimizing the layered-coding scheme.

C. Secrecy Key Rate Under Optimal Power Distribution

The secrecy rate given by (12) is hard to evaluate and optimize. After some tedious steps of derivation (mainly integration by parts), we have an alternative form.

Lemma 2: The secrecy key rate given by (12) is equivalent to

$$R_s = \max_{I(x)} \int_0^{\infty} \left[1 - F_1(x) \right] \rho(x) \left[\int_0^x \frac{F_2(y)dy}{\left[1 + yI(x) \right]^2} \right] dx, \quad (21)$$

with the constraint $I(0) = P$, and $\rho(x) = -dI(x)/dx$.

In certain cases, optimization of R_s with respect to the power distribution $\rho(x)$, or, equivalently, the interference distribution $I(x)$, under the power constraint P can be found by using the calculus of variations. First, we define the functional of (21) as

$$L\left(x, I(x), I'(x)\right) = -\left[1 - F_1(x) \right] I'(x) \left[\int_0^x \frac{F_2(y)dy}{\left[1 + yI(x) \right]^2} \right].$$

A necessary condition for a maximum of the integral of $L(x, I(x), I'(x))$ over x is a zero variation of the functional. By solving the associated Eüler-Lagrangian equation [14] given as

$$\frac{\partial L}{\partial I} - \frac{d}{dx}\left(\frac{\partial L}{\partial I'}\right) = 0, \tag{22}$$

we have the following characterization for the optimal $I(x)$.

Lemma 3: A necessary condition for optimizing $I(x)$ in order to maximize the secrecy rate given by (21) is to choose $I(x)$ to satisfy

$$\int_0^x \frac{F_2(y)dy}{[1+yI(x)]^2} = \frac{[1-F_1(x)]\,F_2(x)}{f_1(x)\,[1+xI(x)]^2}, \tag{23}$$

where $I(x) = 0$ when $x < x_0$ or $x \geq x_1$. Here, x_0 and x_1 can be found by letting $I(x_0) = P$ and $I(x_1) = 0$ in (23).

Finally, we have the following secrecy key rate under the optimal power distribution.

Theorem 2: When the optimal power distribution is used, the following secrecy key rate is achieved,

$$R_s = \int_{x_0}^{x_1} \frac{-[1-F_1(x)]^2\,F_2(x)dI(x)}{f_1(x)[1+xI(x)]^2}, \tag{24}$$

where $I(x)$ and (x_0, x_1) are found from the condition given by (23).

V. A Rayleigh Fading Channel

In this section, we assume Rayleigh fading for Alice-Bob and Alice-Eve channels. We consider a symmetric scenario in which both fading power gains (H_1 and H_2) are exponentially distributed with unit means.

The secrecy rate with layered coding is computed by numerically evaluating

$$R_s = \int_{x_0}^{x_1} \frac{e^{-x}[e^{-x}-1]}{[1+xI(x)]^2} dI(x),$$

where $I(x)$ can be found according to Lemma 3 by solving

$$E_i\left(\frac{1}{I(x)}\right) - E_i\left(x + \frac{1}{I(x)}\right) = \frac{I(x)[1+I(x)]}{[1+xI(x)]^2} \times \left\{\exp\left(-\frac{1}{I(x)}\right) - \exp\left(-\left[x + \frac{1}{I(x)}\right]\right)\right\}, \tag{25}$$

where $E_i(x) = \int_x^\infty [\exp(-t)/t]dt$ is the exponential integral function. By letting $I(x_0) = P$ in (25), we can solve for x_0. By letting $I(x_1) = 0$ in (23), we can solve for x_1. Every equation has a unique solution after excluding a trivial solution 0.

Fig. 3 shows the optimal power distribution for coded layers. A clear trend is that more power is allocated to lower layers as the total power P becomes larger. In general, the optimal power distribution does not concentrate much on a certain layer (or a short interval), especially when P is large. Fig. 4 compares the secrecy key rates of layered coding and single-level coding based schemes (both optimized). The secrecy key rate of the layered-coding based scheme is significantly higher.

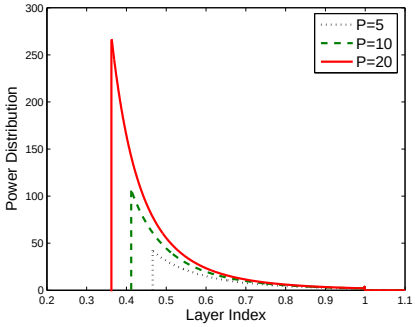

Fig. 3. Optimal power distribution over coded layers

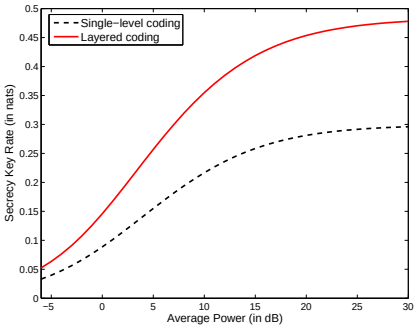

Fig. 4. Secrecy key rate in nats/second/Hertz

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–138, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] E. Biglieri, J. Proakis, and S. Shamai (Shitz), "Fading channels: Information-theoretic and communications aspects," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 1895–1911, Oct. 1998.

[4] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[5] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[6] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of indepedent parallel channels," in *Proc. 44th Annual Allerton Conference on Commun., Cont., and Comp.*, Monticello, IL, Sep. 2006.

[7] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[8] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[9] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[10] S. Shamai (Shitz), "A broadcast strategy for the Gaussian slowly fading channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Ulm, Germany, Jun. 29 - Jul. 4 1997.

[11] S. Shamai (Shitz) and A. Steiner, "A broadcast approach for a single-user slowly fading MIMO channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2617–2635, Oct. 2003.

[12] M. A. Ghany, A. Sultan, and H. El Gamal, "ARQ based secret key sharing," *http://arxiv.org/abs/0810.1319*, Oct. 2008.

[13] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference-assisted secret communication," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Porto, Portugal, May 2008.

[14] I. M. Gelfand and S. V. Fomin, *Calculus of Variations*. Englewood Cliffs, NJ: Prentice-Hall, 1963.