On the Achievable Secrecy Throughput of Block Fading Channels with No Channel State Information at Transmitter

Xiaojun Tang, Ruoheng Liu and Predrag Spasojević
WINLAB, ECE department, Rutgers University
{xtang,liurh,spasojev}@winlab.rutgers.edu

***Abstract*— We study the block fading wire-tap channel, where a transmitter sends confidential messages to a legitimate receiver over a block fading channel in the presence of an eavesdropper, which listens to the transmission through another independent block fading channel. We assume that the transmitter has no channel state information (CSI) available from either the main channel or the eavesdropper channel. The transmitter uses an in advance given *Wyner secrecy code* (instead of adapting the code based on CSI). In this case, both reliability and perfect secrecy can be achieved only for a subset of channel states. We identify this channel state set and provide an achievable average secrecy throughput of the block fading wire-tap channel for given reliability and secrecy outage probabilities.**

I. Introduction

Shannon introduced the notion of *perfect secrecy* from the information theoretic point of view in [1], where a secret key is considered to protect the confidential messages. Later Wyner proposed the so-called discrete memoryless wire-tap channel model in the seminal paper [2], where the signal transmitted over the main channel is eavesdropped by a wire-tapper. Assuming that the eavesdropper channel is a degraded version of the main channel, Wyner showed that secure communication is possible without sharing a secret key between legitimate users. The level of ignorance of the wire-tapper with respect to the confidential message is measured by the equivocation rate. Perfect secrecy requires that the equivocation rate is asymptotically equal to the message entropy rate. Csiszár and Körner generalized the results and determined the secrecy capacity region of broadcast channel with confidential messages in [3]. The result was extended to the Gaussian wire-tap channel in [4]. Some recent research efforts aim to determine the capacity regions of the multiple access channel [5]–[7] and the broadcast/interference channels [8] with confidential messages.

Due to its broadcast nature, wireless communication is particularly susceptible to eavesdropping. The effect of fading on the secure wireless communications was studied in [9]–[12]. More specifically, [10]–[12] studied the secrecy capacity of ergodic fading channels with the full CSI assumption, i.e., when all parties have perfect CSI of both the main channel and the eavesdropper channel prior to the message transmission. [12] also studied the ergodic scenario where the transmitter does not have the CSI of the eavesdropper channel.

In this paper, we consider communicating confidential information over block fading channels when the transmitter has no channel state information, but only channel statistics. This setting is of strong interests in many practical communication systems, in particular, where the feedback of the instantaneous CSI is either too costly or physically infeasible. Due to the absence of CSI, we consider the case when a fixed Wyner secrecy code is used at the transmitter for all channel states. However, both reliability and perfect secrecy can be achieved only for a subset of channel states in this case. Hence, we identify this *reliable and secure* channel state set for a given Wyner code. Furthermore, we prove that there exists a single Wyner code ensuring reliability and perfect secrecy for all channel states within the set. Outage events correspond to the channel state pairs that are not in the set. More specifically, we define two outage events: *reliability outage* and *secrecy outage* for the main channel and the eavesdropper channel respectively. The secrecy throughout is evaluated for given outage probabilities. We study the Rayleigh block fading channel under different coding schemes, in which a codeword can span a single or multiple coherence intervals corresponding to different delay constraints. Our results show that the diversity obtained through multiple fading block coding can increase the secrecy throughput significantly.

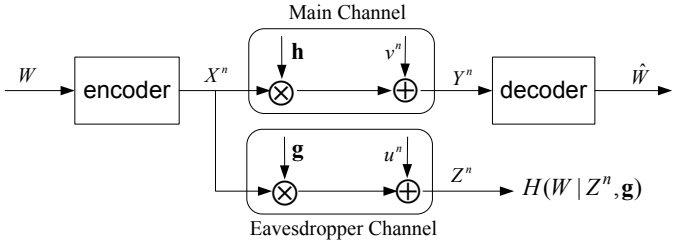

Fig. 1. System model

II. System Model and Preliminaries

A. Channel Model

As shown in Figure 1, the transmitter sends a confidential message to the destination via the main channel in the presence of an wire-tapper, who listens to the message through the eavesdropper channel. Both the main channel and the eavesdropper channel experience independent M-block fading, that is, the channel gain is constant within a block while varying for different blocks.

Confidential message $w \in \mathcal{W}$ is encoded into a codeword $x^n = [x(1), x(2), \ldots, x(n)]$, which spans M fading blocks. The outputs from the main channel and the eavesdropper

channel are shown as follows:

$$\begin{aligned} y(t) &= \sqrt{h_i}x(t) + v(t) \\ z(t) &= \sqrt{g_i}x(t) + u(t) \quad \text{for } t = 1, \ldots, n,\ i = \left\lceil \frac{Mt}{n} \right\rceil, \end{aligned} \tag{1}$$

where $\{v(t)\}$ and $\{u(t)\}$ $(t = 1, \ldots, n)$ are i.i.d. with normal distributed $\mathcal{N}(0, 1)$, and h_i and g_i, for $i = 1, \ldots, M$, denote the normalized (real) channel gains of the main channel and the eavesdropper channel respectively.

Let $\mathbf{h} = [h_1, \ldots, h_M]$ and $\mathbf{g} = [g_1, \ldots, g_M]$ represent the vectors of channel gain for the main channel and the eavesdropper channel, respectively, and $(\mathbf{h}, \mathbf{g})$ be the *channel pair*. We assume that the destination knows $\mathbf{h}$, while the eavesdropper knows $\mathbf{g}$.

When the transmitted codeword x^n spans a single fading block, i.e., $M = 1$, we can easily compare the main channel and the eavesdropper channel. For example, if the main channel has better condition, i.e. $h_1 \geq g_1$, then we say that z^n is a *degraded* version of y^n. However, when x^n spans multiple fading blocks ($M > 1$), there is virtually no degraded ordering between y^n and z^n.

B. Wyner Code Ensembles

In this subsection, we review Wyner codes, which achieve the secrecy capacity of the wire-tap channel [2].

Let $\mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ denote an ensemble of Wyner codes with size 2^{nR_0} in order to convey a message set $\mathcal{W} = \{1, 2, \ldots, 2^{nR_s}\}$ (We describe the random code generation in Appendix A). Here, the basic idea is to use a stochastic encoding since randomization can increase secrecy. The Wyner code consists of a stochastic encoder $f_n(\cdot) : \mathcal{W} \to \mathcal{X}^n$ and a decoding function $\phi(\cdot) : \mathcal{Y}^n \to \mathcal{W}$.

A stochastic encoder [3] is specified by a matrix of conditional probabilities $f(x^n|w)$, here $x^n \in \mathcal{X}^n$, $w \in \mathcal{W}$, $\sum_{x^n} f(x^n|w) = 1$ and $f(x^n|w)$ is the probability that message w is encoded as channel input x^n. We further assume that any code $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ is constrained by the power budget $\bar{P}$ as

$$\frac{1}{n}\sum_{t=1}^{n} |x(t)|^2 \leq \bar{P}. \tag{2}$$

Let $\phi\big(y^n(w)\big)$ be the output of the decoder at the destination when message w is sent, the average error probability of a $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ code is defined as

$$P_e = \sum_{w \in \mathcal{W}} \Pr\left(\phi\big(y^n(w)\big) \neq w | w \text{ is sent}\right) \Pr(w). \tag{3}$$

where $\Pr(w)$ is the probability that message $w \in \mathcal{W}$ is sent.

The secrecy level, i.e. the degree to which the eavesdropper is confused, is measured by the equivocation rate $(1/n)H(W|Z^n, \mathbf{g})$. *Perfect secrecy* is defined that for any $\epsilon > 0$, the equivocation

$$\frac{1}{n}H(W|Z^n, \mathbf{g}) \geq \frac{1}{n}H(W) - \epsilon \tag{4}$$

When perfect secrecy is achieved, we also say that the eavesdropper can be perfectly confused. For conciseness we consider the following definition of good Wyner codes.

Definition 1: A Wyner code sequence $C \triangleq \{C(n)\}$ is ***good*** for a channel pair $(\mathbf{h}, \mathbf{g})$ if, by using code $C(n)$, the legitimate receiver can decode the message with arbitrarily small error probability while the eavesdropper can be perfectly confused, as $n \to \infty$.

C. Related Works

A closely related result is the secrecy rate for the memoryless Gaussian wire-tap channel, in which the main channel and the eavesdropper channel are Gaussian but of no fading. For the Gaussian wiretap channel, it is shown in [4] that there exists a code $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ such that the secrecy rate

$$R_s = I(X;Y) - I(X;Z) \tag{5}$$

can be achieved, where $I(X;Y)$ and $I(X;Z)$ are single-letter characterized mutual information of the main channel and the eavesdropper channel. It is also shown that the secrecy capacity, i.e. the maximum secrecy rate is achieved when the input distribution is Gaussian.

For block fading channels, when the transmitter has channel state information of the main channel and the eavesdropper channel, it can adapt either code rate or power level as in [12] to achieve the maximum secrecy rate.

III. Reliable and Secure Channel State Set

We are interested in the achievable secrecy rate for fading channels when the transmitter has no channel state information. Due to the absence of CSI, a fixed Wyner code is used. Arbitrarily small error probability and perfect secrecy can be achieved only for a subset of channel states. In this section, we identify this set of channel states and provide sufficient conditions on the secure communication over both single-block fading and multiple-block fading channels.

A. Coding over a Single Fading Block ($M = 1$)

In a single fading block case, we denote the channel pair by (h, g) for convenience, where h and g are channel gains for the main and the eavesdropper channel, respectively.

Lemma 1: There exists a single Wyner code $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ good for all channel pairs (h, g) such that

$$\begin{aligned} I(X;Y|h) &\geq R_0 \\ I(X;Z|g) &\leq R_0 - R_s \end{aligned} \tag{6}$$

where $I(X;Y|h)$ and $I(X;Z|g)$ are single letter mutual information characterizations of channel (1).

Proof: To avoid confusion, we denote Y_1^n and Z_1^n to be the output at the legitimate receiver and the eavesdropper respectively, when a channel pair (h^*, g^*) gives single letter characterized mutual information $I(X;Y_1|h^*) = R_0$ and $I(X;Z_1|g^*) = R_0 - R_s$.

Since $R_s = I(X;Y_1|h^*) - I(X;Z_1|g^*)$, there exists a code $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ for the Gaussian wire-tap channel (h^*, g^*) according to (5), such that Y_1^n can be decoded with

arbitrarily small error probability and the equivocation at the eavesdropper with Z_1^n is

$$H(W|Z_1^n, g^*) \geq H(W) - n\epsilon \tag{7}$$

It can be shown that this code C is also good for all channel pairs (h, g) such that $I(X;Y|h) > R_0$ and $I(X;Z|g) < R_0 - R_s$.

Since $I(X;Y|h) > R_0 = I(X;Y_1|h^*)$, $h > h^*$ and Y_1^n is a degraded version of Y^n from the discussion in section II, if Y_1^n can be decoded at the legitimate receiver with arbitrarily small error probability, so can Y^n. We also have

$$\begin{aligned} & H(W|Z^n, g) - H(W|Z_1^n, g^*) \\ = \;& I(W; Z_1^n|g^*) - I(W; Z^n|g) \geq 0 \end{aligned}$$

where we use the fact that Z^n is a degraded version of Z_1^n.

$$H(W|Z^n, g) \geq H(W|Z_1^n, g^*) \geq H(W) - n\epsilon \tag{8}$$

for any $\epsilon \to 0$ as $n \to \infty$. ∎

For a given Wyner code $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$, (6) describes a sufficient condition on the secure communication over a single-block fading channel. In other words, it identifies the set of *good* channel states. This will be used in Section IV to define outage events and evaluate outage probabilities.

B. Coding Over Multiple Fading Blocks

In this section, we consider the secure communication over M-block fading channel. Under the assumption of using Wyner codes here, we attempt to answer the question whether there exists a single code sequence (for increasing block length n) good for all fading states such that

$$\begin{aligned} \frac{1}{M}\sum_{i=1}^{M} I(X;Y|h_i) &\geq R_0 \\ \frac{1}{M}\sum_{i=1}^{M} I(X;Z|g_i) &\leq R_0 - R_s \end{aligned} \tag{9}$$

where $I(X;Y|h_i)$ and $I(X;Z|g_i)$ are single letter characterized mutual information of channel (1) during the i-th fading block. Notice that this is not a trivial question, since if the choice of the code sequence depends on the particular fading state, it would require side information at the transmitter. The existence of *asymptotically good* Wyner codes is given by the following lemma.

Lemma 2: There exists a single code $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ good for all channel pairs $(\mathbf{h}, \mathbf{g})$ satisfying (9).

Proof: In Lemma 1, we have used degradation arguments to show that there exists a single code C good for a set of channel pairs when coding is confined over a single fading block. However, when the code can span multiple fading blocks, there is virtually no degraded ordering between channel vector pairs as shown in section II. It demands a new approach to prove Lemma 2. Due to the page limit, we only outline the proof in Appendix B. ∎

IV. Achievable Secrecy Throughput of Rayleigh Block Fading Channels

We first define two outage events (similar as the outage defined for ordinary communication without considering the secrecy constraint): reliability outage for the main channel and secrecy outage for the eavesdropper channel.

Definition 2: A channel pair $(\mathbf{h}, \mathbf{g})$ is in the *outage*, if it cannot meet the conditions given in (9). More specifically, the *reliability outage* occurs if

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Y|h_i) < R_0; \tag{10}$$

The *secrecy outage* occurs if

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Z|g_i) > R_0 - R_s. \tag{11}$$

Let P_e be the probability of reliability outage and P_s be the probability of secrecy outage. Given a target outage probability pair (ϵ_e, ϵ_s), we can properly choose R_0 and R_s to maximize the secrecy throughput while satisfying reliability and secrecy requirements. Let η denote the secrecy throughput, we consider the following problem

$$\begin{aligned} \max_{\{R_0, R_s\}} \quad & \eta \\ \text{s.t.} \quad & P_e \leq \epsilon_e \text{ and } P_s \leq \epsilon_s. \end{aligned} \tag{12}$$

When the transmitted codeword spans only a single fading block, the optimal input distribution is Gaussian [4]. However, the optimal input distribution $p(X)$ is not known in general when the codeword spans multiple fading blocks and both CSIs are not available to the transmitter. For the sake of mathematical tractability, we consider Gaussian input. Hence, the channel mutual information pair is given by

$$\begin{aligned} I_{XY}^{[\mathrm{M}]} &\triangleq \sum_{i=1}^{M} I(X;Y|h_i) = \sum_{i=1}^{M} \log_2(1+\lambda_i), \\ I_{XZ}^{[\mathrm{M}]} &\triangleq \sum_{i=1}^{M} I(X;Z|g_i) = \sum_{i=1}^{M} \log_2(1+\nu_i), \end{aligned} \tag{13}$$

where $\lambda_i = h_i \cdot \bar{P}$ and $\nu_i = g_i \cdot \bar{P}$ are the signal-to-noise ratio (SNR) at the receiver and the eavesdropper respectively during the i-th slot.

Here, we also consider a repetition coding (also called *repetition time diversity* or RTD) scheme as a comparison. The RTD code $C(n)$ is a concatenated code, including a Wyner code $C_1(n_1) \in \mathcal{C}(2^{n_1 R_0}, 2^{n_1 R_s}, n_1)$ as the outer code and a simple repetition code of length M as the inner code, i.e.,

$$C(n) = [\underbrace{C_1(n_1), C_1(n_1), \ldots, C_1(n_1)}_{M}]. \tag{14}$$

By using RTD codes, the maximal ratio combining (MRC) is performed at both receivers, which essentially transform the parallel channel pairs into a scalar (Gaussian) channel pair. In this case, the optimal input distribution is Gaussian and the

mutual information pair can be written as

$$I_{XY}^{[\mathrm{RTD}]} \triangleq \log_2\left(1+\sum_{i=1}^{M}\lambda_i\right)$$
$$I_{XZ}^{[\mathrm{RTD}]} \triangleq \log_2\left(1+\sum_{i=1}^{M}\nu_i\right). \quad (15)$$

Following the approach for proving Lemma 1, we can show that there exists a single RTD code sequence good for all channel pairs satisfying

$$I_{XY}^{[\mathrm{RTD}]} \geq MR_0 \quad \text{and} \quad I_{XZ}^{[\mathrm{RTD}]} \leq M(R_0-R_s).$$

A. Secrecy Throughput of Single-Block Fading Channels

We consider the secrecy throughput of Rayleigh block fading channels ($M=1$). In this case, the SNRs λ and ν are exponentially distributed with the mean $\overline{\lambda}$ and $\overline{\nu}$, respectively. The probability of reliability outage P_e and the probability of secrecy outage P_s can be evaluated now by

$$P_e = \Pr(I_{XY}^{[1]} < R_0) = 1-\exp\left[-\frac{2^{R_0}-1}{\overline{\lambda}}\right],$$
$$P_s = \Pr(I_{XZ}^{[1]} > R_0-R_s) = \exp\left[-\frac{2^{(R_0-R_s)}-1}{\overline{\nu}}\right],$$

and the secrecy throughput η is given by

$$\eta^{[1]} = \log_2\left(1+\overline{\lambda}\delta_e\right) - \log_2\left(1+\overline{\nu}\delta_s\right), \quad (16)$$

where $\delta_e = -\log(1-\epsilon_e)$ and $\delta_s = -\log(\epsilon_s)$. When there is no secrecy constraint, $\epsilon_s = 1$ and then $\delta_s = 0$, (16) is the delay limited capacity of Rayleigh block fading channel.

B. Secrecy Throughput of M-Block Fading Channels

Now, we compute the secrecy throughput of Rayleigh M-block fading channels based on RTD and (M-Block) Wyner codes.

1) RTD Scheme: In this case, the channel mutual information pair is given by (15). Note that $\sum_{i=1}^{M}\lambda_i$ and $\sum_{i=1}^{M}\nu_i$ are Gamma distributed with the mean $M\overline{\lambda}$ and $M\overline{\nu}$, respectively. P_e and P_s can be evaluated by

$$P_e = \Pr(I_{XY}^{[\mathrm{RTD}]} < MR_0) = \Gamma\left(M, \frac{2^{MR_0}-1}{\overline{\lambda}}\right), \quad (17)$$

$$P_s = \Pr\left(I_{XZ}^{[\mathrm{RTD}]} > M(R_0-R_s)\right)$$
$$= 1-\Gamma\left(M, \frac{2^{M(R_0-R_s)}-1}{\overline{\nu}}\right), \quad (18)$$

where $\Gamma(a,b) = \frac{1}{\Gamma(a)}\int_0^b t^{a-1}e^{-t}dt$ is the lower incomplete Gamma function and $\Gamma(a)$ is the complete Gamma function.

It can be shown that the secrecy throughput is

$$\eta^{[\mathrm{RTD}]} = \frac{1}{M}\left[\log_2\left(1+\overline{\lambda}\delta_e\right) - \log_2\left(1+\overline{\nu}\delta_s\right)\right], \quad (19)$$

where $\delta_e = \Gamma^{-1}(M,\epsilon_e)$, $\delta_s = \Gamma^{-1}(M,1-\epsilon_s)$, and $\Gamma^{-1}(a,p)$ denotes the inverse Gamma function (the inverse function of $p=\Gamma(a,b)$). We note that the inverse gamma function turns into a logarithm function when $M=1$. Hence, it is not surprise that the throughput in (19) is equal to the result in (16) for the single-block case.

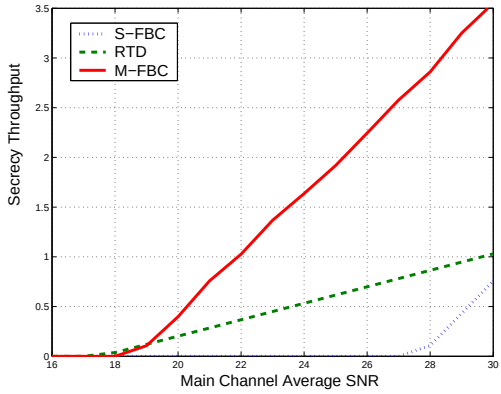

Fig. 2. Secrecy throughput η versus main channel average SNR $\overline{\lambda}$.

2) M-Fading-Block Coding: By using (M-block) Wyner codes $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$, we can calculate P_e and P_s as follows

$$P_e = \Pr\left(I_{XY}^{[\mathrm{M}]} < MR_0\right), \quad (20)$$
$$P_s = \Pr\left(I_{XZ}^{[\mathrm{M}]} > M(R_0-R_s)\right). \quad (21)$$

In general, distributions of $I_{XY}^{[\mathrm{M}]}$ and $I_{XZ}^{[\mathrm{M}]}$ cannot be written in a closed form. Hence, we resort to the Monte-Carlo simulation to obtain the inverse empirical CDF of $I_{XY}^{[\mathrm{M}]}$ and $I_{XZ}^{[\mathrm{M}]}$, denoted by $F^{-1}(M,\overline{\lambda},p)$ and $F^{-1}(M,\overline{\nu},p)$, respectively. The secrecy throughput is written as

$$\eta^{[\mathrm{M}]} = \frac{1}{M}\left[F^{-1}(M,\overline{\lambda},\epsilon_e) - F^{-1}(M,\overline{\nu},1-\epsilon_s)\right]. \quad (22)$$

V. Numerical Results

In this section, we study the secrecy throughput of Rayleigh block fading channels based on some numerical computations. We consider secrecy throughput η versus main channel average SNR $\overline{\lambda}$ and eavesdropper channel average SNR $\overline{\nu}$ respectively. We also investigate the relationship between the secrecy throughput η and the number of fading blocks M.

Simulation settings are as follows: main channel average SNR $\overline{\lambda} = 20dB$, eavesdropper channel average SNR $\overline{\nu} = 10dB$, target probability of reliability outage $\epsilon_e = 0.05$, target probability of secrecy outage $\epsilon_s = 0.05$, the number of fading blocks $M=4$. Through simulations, we observe that similar results are obtained by using other parameter settings.

Figure 2 illustrates the secrecy throughput η v.s. the main channel average SNR $\overline{\lambda}$ for different schemes, where S-FBC and M-FBC stand for the single and multiple fading-block coding schemes. When $\overline{\lambda} < 16dB$, the secrecy throughput closes to zero for all three coding schemes. RTD and M-FBC yield positive secrecy throughput from $17dB$ and $18dB$ respectively. The S-FBC cannot give positive secrecy throughput unless

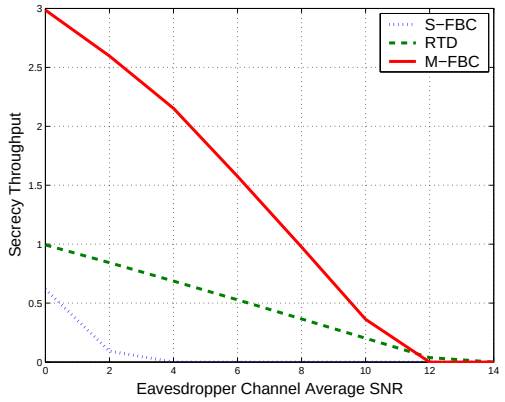

Fig. 3. Secrecy throughput η versus eavesdropper channel average SNR $\overline{\nu}$

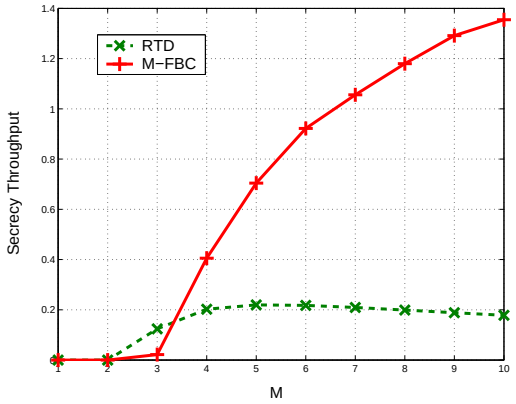

Fig. 4. Secrecy throughput η versus M, the number of fading blocks.

$\overline{\lambda} > 27dB$. RTD outperforms M-FBC in lower SNR region.[1] We also observe that, in high SNR region, M-FBC outperforms RTD significantly and RTD suffers large loss, even comparing with S-FBC, which outperforms RTD when $\overline{\lambda} > 32dB$ in the simulation.

Figure 3 shows the secrecy throughput η vs. the eavesdropper channel average SNR $\overline{\nu}$ for different schemes. When $\overline{\nu} > 14dB$ (the eavesdropper channel is good), the secrecy throughput approaches to zero for all coding schemes. RTD outperforms M-FBC in the SNR region near to the critical SNR point ($\overline{\nu} \in [11dB - 14dB]$). When $\overline{\nu}$ is lower, for example, $\overline{\nu} < 8dB$, M-FBC are much more favorable.

Figure 4 illustrates the relationship between the secrecy throughput and the number of fading blocks M. In practice, different delay limits require different numbers of transmission blocks. When the delay limit is strict ($M \leq 3$ is small), it is shown that RTD may outperform M-FBC. If the delay limit is relaxed, M-FBC quickly outperforms RTD as M increases. We observe that the secrecy throughput of RTD actually decreases when M gets large. In fact, there exists an optimal M for the RTD scheme, e.g., in figure 4, the optimal number of fading blocks is $M = 5$ for RTD. In contrast, the secrecy throughput of M-FBC increases monotonically with the increase of M.

VI. Conclusions

In this paper, we consider the reliable and secure communication over block fading wire-tap channels when the transmitter has no channel state information. We assume that the transmitter uses a fixed Wyner code for all channel states and identify a set of channel pairs, on which reliability and perfect secrecy can be ensured by using a deterministic code sequence. We define the corresponding reliability and secrecy outage probabilities. The secrecy throughput of block fading channels follows these definitions. We consider different scenarios, where a codeword can span a single or multiple fading blocks due to different delay constraints. Our results show that the diversity obtained through multiple fading block coding can increase the secrecy throughput significantly, but the repetition time diversity coding scheme may not. In general, multiple fading block coding outperforms repetition time diversity except for the region in which secrecy throughput is close to zero.

[1]Here and hereafter, by lower SNR region, we mean the SNR region near to the critical point below which the secrecy throughput is zero.

Appendix

A. Wyner Code

The random coding ensemble $\mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ is constructed based on random binning [2], [3].

Code Construction: Generate 2^{nR_0} codewords $x^n(w, v)$, $w = 1, 2, \ldots, 2^{R_s}$, $v = 1, 2, \ldots, 2^{n(R_0 - R_s)}$ by choosing the $n2^{R_0}$ symbols $x_i(w, v)$ independently at random according to the input distribution $P_X(\cdot)$.

Encoder: Given w, randomly and uniformly select v from $(1, 2, \ldots, 2^{n(R_0 - R_s)})$ and transmit $x^n = x^n(w, v)$.

Decoder: Given y^n, try to find a pair $(\tilde{w}, \tilde{v})$ such that $(x^n(\tilde{w}, \tilde{v}), y^n) \in T_\epsilon^n(P_{XY})$. If there is no such pair, then put out $\tilde{w} = 1$.

B. Outline Proof of Lemma 2

For convenience, denote $\mathbf{P} \triangleq (\mathbf{h}, \mathbf{g})$ and denote $\mathcal{P}$ as the set of channel pairs satisfying (9) . We also denote $\mathcal{P}_\star = \{(\mathbf{h}, \mathbf{g})\}$ as the set of channel pairs satisfying

$$\frac{1}{M}\sum_{i=1}^{M} I(X; Y|h_i) = R_0 + \delta, \tag{23}$$

$$\frac{1}{M}\sum_{i=1}^{M} I(X; Z|g_i) = R_0 - R_s + \delta. \tag{24}$$

It is clear $\mathcal{P}_\star \subset \mathcal{P}$ when $\delta \to 0$. Given any channel pair $\mathbf{P} \in \mathcal{P}_\star$, on every fading block $i = 1, \ldots, M$, the channel is time-invariant memoryless. By following the same steps in [13, Theorem 8.7.1], we can show that the average probability of error, averaged over the code ensemble $\mathcal{C}$ is

$$E_{\mathcal{C}}[\Pr(\mathcal{E}_1|\mathbf{P}, \mathcal{C})] \leq \epsilon_1 \tag{25}$$

for any given channel pair $\mathbf{P} \in \mathcal{P}_\star$ as the codeword length $n \to \infty$. we also consider $\Pr(\mathcal{E}_2)$, the error probability that

the eavesdropper cannot decode X^n given that it observes Z^n and also knows W. Denote $B(w)$ to be the set of codewords corresponding to message $w \in \mathcal{W}$. Given w, the eavesdropper declares that $\tilde{x}_n$ was transmitted, if $\tilde{x}_n$ is the only codeword in $B(w)$ that is jointly typical with z^n. The eavesdropper declares an error if either there is no codeword in $B(w)$ jointly typical with z^n, or there is more than one. It can be shown that

$$E_{\mathcal{C}}[\Pr(\mathcal{E}_2|\mathbf{P},\mathcal{C})] \leq \epsilon_2 \tag{26}$$

for any given channel pair $\mathbf{P} \in \mathcal{P}_\star$ as the codeword length $n \to \infty$. We define an event $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2$. According to (25) and (26), by using the union bound, we have for any $\mathbf{P} \in \mathcal{P}_\star$,

$$E_{\mathcal{C}}[\Pr(\mathcal{E}|\mathbf{P},\mathcal{C})] \leq \epsilon_1 + \epsilon_2 = \epsilon_3$$

The average error probability, averaged over channel pair set $\mathcal{P}_\star$ is

$$E_{\mathbf{P}}\left[E_{\mathcal{C}}[\Pr(\mathcal{E}|\mathbf{P},\mathcal{C})]\right] \leq \epsilon_3$$

Exchanging expectations with respect to $\mathcal{C}$ and with respect to $\mathbf{P}$ (since the integrand is nonnegative and bounded by 1) yields

$$E_{\mathcal{C}}\left[E_{\mathbf{P}}[\Pr(\mathcal{E}|\mathbf{P},\mathcal{C})]\right] \leq \epsilon_3$$

There exists a sequence of codes C^* such that

$$E_{\mathbf{P}}[\Pr(\mathcal{E}|\mathbf{P},C^*)] \leq \epsilon_3.$$

where $\Pr(\mathcal{E}|\mathbf{P},C^*)$ is a random variable which is a function of $\mathbf{P} \in \mathcal{P}_\star$. According to the Markov inequality, we have

$$\Pr\left(\Pr(\mathcal{E}|\mathbf{P},C^*) \geq \sqrt{\epsilon_3}\right) \leq \frac{E_{\mathbf{P}}[\Pr(\mathcal{E}|\mathbf{P},C^*)]}{\sqrt{\epsilon_3}} \leq \frac{\epsilon_3}{\sqrt{\epsilon_3}} = \sqrt{\epsilon_3}$$

By letting $\sqrt{\epsilon_3} = \epsilon_4$ and changing the direction of the inequality, we have

$$\Pr\left(\Pr(\mathcal{E}|\mathbf{P},C^*) < \epsilon_4\right) \geq 1 - \epsilon_4$$

Because $\Pr(\mathcal{E}_1|\mathbf{P},C^*) \leq \Pr(\mathcal{E}|\mathbf{P},C^*)$ and $\Pr(\mathcal{E}_2|\mathbf{P},C^*) \leq \Pr(\mathcal{E}|\mathbf{P},C^*)$, we have

$$\Pr\left(\Pr(\mathcal{E}_1|\mathbf{P},C^*) < \epsilon_4\right) \geq 1 - \epsilon_4 \tag{27}$$

$$\Pr\left(\Pr(\mathcal{E}_2|\mathbf{P},C^*) < \epsilon_4\right) \geq 1 - \epsilon_4 \tag{28}$$

(27) and (28) reveal that we can find a sequence of code $C^* \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$, for all $\mathbf{P} \in \mathcal{P}_\star$ with probability 1, such that the legitimate receiver can decode the message with arbitrarily small error probability (A.S.E.P.), while the eavesdropper can decode X^n with A.S.E.P., given that W is known and Z^n is observed. Using Fano's inequality, we have

$$H(X^n|W,Z^n,\mathbf{h},\mathbf{g}) \leq n\delta_n$$

With code C^* being used, the equivocation at the eavesdropper can be bounded as follows.

$$\begin{aligned} H(W|Z^n,\mathbf{h},\mathbf{g}) &\geq H(X^n|\mathbf{h},\mathbf{g}) - I(X^n;Z^n|\mathbf{h},\mathbf{g}) \\ &\quad - H(X^n|W,Z^n,\mathbf{h},\mathbf{g}) \end{aligned}$$

For the first two terms, we have

$$H(X^n|\mathbf{h},\mathbf{g}) = nR_0$$

$$\begin{aligned} I(X^n;Z^n|\mathbf{h},\mathbf{g}) &\leq n\left(\frac{1}{M}\sum_{i=1}^{M} I(X;Z|g_i) - \epsilon\right) \\ &= n(R_0 - R_s + \delta - \epsilon) \end{aligned}$$

Therefore, we have

$$\begin{aligned} H(W|Z^n,\mathbf{h},\mathbf{g}) &\geq nR_0 - n(R_0 - R_s + \delta - \epsilon) - n\delta_n \\ &= n(R_s - \delta_1) \end{aligned}$$

The perfect secrecy can be achieved for any $\mathbf{P} \in \mathcal{P}_\star$ when the sequence of code C^* is used (with probability 1). According to definition 1, code C^* is good for all channel pair $\mathbf{P} \in \mathcal{P}_\star$ with probability 1.

To show that code C^* is good for any channel pair $\mathbf{P} \in \mathcal{P}$, we can now use the degradation arguments as in the proof of Lemma 1. For any channel pair $\mathbf{P} = (\mathbf{h},\mathbf{g}) \in \mathcal{P}$, we can always find a channel pair $\mathbf{P}^* = (\mathbf{h}^*,\mathbf{g}^*) \in \mathcal{P}_\star$, such that $\mathbf{h}^* \preceq \mathbf{h}$ and $\mathbf{g}^* \succeq \mathbf{g}$. Since code C^* is good for $\mathbf{P}^*$, we can show that C^* is also good for $\mathbf{P}$ by following the same steps as in the proof of Lemma 1.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

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

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

[4] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Info. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[5] R. Liu, I. Maric, R. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *IEEE Int. Symp. Information Theory, ISIT*, July 2006.

[6] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in *IEEE Int. Symp. Information Theory, ISIT*, July 2006.

[7] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *IEEE Int. Symp. Information Theory, ISIT*, Seattle, USA, July 2006.

[8] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proc. Allerton Conference on Commun. Contr. Computing*, Urbana, IL, USA, Sept 2006.

[9] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Int. Symp. Information Theory, ISIT*, Seattle, USA, July 2006.

[10] Y. Liang and H. V. Poor, "Secure communication over fading channels," in *Proc. Allerton Conference on Commun. Contr. Computing*, Urbana, IL, USA, Sept 2006.

[11] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of indepedent parallel channels," in *Proc. Allerton Conference on Commun. Contr. Computing*, Urbana, IL, USA, Sept 2006.

[12] P. Gopala, L. Lai, and H. El gamal, "On the secrecy capacity of fading channels," *submitted to the IEEE Transactions on Information Theory*, 2006.

[13] T. Cover and J. Thomas, *Elements of Information Theory*, John Wiley Sons, Inc., 1991.