An Achievable Secrecy Throughput of Hybrid-ARQ Protocols for Block Fading Channels

Xiaojun Tang
WINLAB, Rutgers University
xtang@winlab.rutgers.edu

Ruoheng Liu
EE, Princeton University
rliu@princeton.edu

Predrag Spasojević
WINLAB, Rutgers University
spasojev@winlab.rutgers.edu

***Abstract*—In applications of wireless packet-oriented data networks, a special coding scheme, the hybrid automatic retransmission request (HARQ) exhibits high throughput efficiency by adapting its error correcting code redundancy to channel conditions. Motivated by the increasing importance of secure communication over wireless networks, we investigate secure packet communication based on HARQ over block-fading (BF) channels. More specifically, we consider two legitimate users communicating over a BF channel in the presence of a passive eavesdropper who intercepts the transmission through another independent BF channel. We assume that the transmitter can obtain a 1-bit ACK/NACK feedback from the receiver via a reliable *public* channel. Under this setting, we consider incremental redundancy (IR) and repetition time diversity (RTD) HARQ schemes based on rate-compatible Wyner secrecy codes from an information theoretic point of view. We study a *good* Wyner code sequence, with which the legitimate receiver can decode the message and the eavesdropper can be perfectly confused. For a given pair of *reliability / secrecy outage probabilities*, we derive an achievable secrecy throughput of HARQ protocols for block-fading channels. Finally, we illustrate numerically that HARQ can benefit both throughput and secrecy.**

I. Introduction

In a seminal paper [1], Wyner proposed the discrete memoryless wire-tap channel model, where the communication between two legitimate users is eavesdropped upon via a degraded channel. Wyner showed that secure communication is possible without sharing a secret key between legitimate users. The level of ignorance of the eavesdropper 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 result and determined the secrecy capacity region of the broadcast channel with confidential messages in [2]. The result was extended to the Gaussian wire-tap channel in [3].

Secure communication over wireless networks has become increasingly important. The effect of fading on wireless secure communications has been studied recently in [4]–[7]. Block-fading (BF) has been a primary consideration, where the channel gain is constant within each coherence interval while varying from interval to interval. As shown in [8], [9], the block-fading channel model is good for many practical applications. Furthermore, it has been assumed in [4]–[7] that the number of channel uses within each coherence interval is large enough to allow for invoking random coding arguments. More specifically, assuming that all communication parties have perfect channel state information of both the main channel and the eavesdropper channel prior to the message transmission, [4] has studied the delay limited secrecy capacity of wireless channels, based on secrecy capacity outage probability; [5]–[7] have studied the secrecy capacity of the ergodic fading channel with advance perfect CSI. [7] has also considered the ergodic scenario where the transmitter does not have any CSI describing the eavesdropper channel.

We assume in this paper that the transmitter does not have the CSI of the main channel or the eavesdropper channel, but receives a 1-bit ACK/NACK feedback from the legitimate receiver via a reliable *public* channel. It is well known that HARQ protocols exhibit high throughput efficiency in wireless communication systems with ACK/NACK feedback. An information theoretic study of HARQ protocols without secrecy consideration has been presented by Caire and Tuninetti in [10]. In this paper, we investigate secure packet communication based on HARQ schemes over block-fading channels. More specifically, we consider two legitimate users communicating over a block-fading channel in the presence of a passive eavesdropper who intercepts the transmission through another independent block-fading channel. Under this setting, we consider incremental redundancy (IR) and repetition time diversity (RTD) HARQ schemes based on rate-compatible Wyner secrecy codes from an information theoretic point of view. We study a *good* Wyner code sequence, which ensures that the legitimate receiver can decode the message and the eavesdropper can be perfectly confused. We prove that there exists a rate-compatible Wyner code family good for a certain set of channel states. For a given reliability / secrecy outage probability pair, we derive an achievable secrecy throughput of HARQ protocols for block-fading channels. Finally, we illustrate numerically that HARQ can benefit both throughput and secrecy.

II. System Model and Preliminaries

A. System Model

As shown in Fig. 1, the transmitter sends confidential messages to the destination via the main channel in the presence of a passive eavesdropper, who listens to the transmission through its own channel. Both the main channel and the eavesdropper channel experience independent block fading,

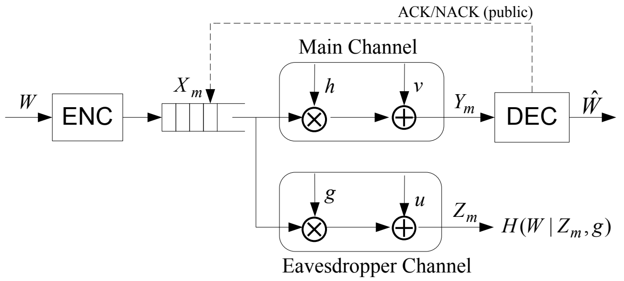

Fig. 1. System model

where the channel gain is constant within a block while varying independently form block to block.

Confidential message $w \in \mathcal{W}$ is encoded into a codeword $x^n = [x(1), x(2), \ldots, x(n)]$ and divided into M blocks $\{x_1^{n_1}, x_2^{n_1}, \ldots, x_M^{n_1}\}$ each of length $n_1 = n/M$. The first block $x_1^{n_1}$ is sent and decoding errors are detected at the receiver. If no error is detected, the receiver sends back an acknowledgement (ACK) to stop the transmission; otherwise a negative acknowledgement (NACK) is sent to request retransmission. If a retransmission is requested, the transmitter sends the second block, which experiences independent channel gains. Decoding is again attempted at the receiver, where the new block is combined with the previous received blocks. This is repeated until an ACK is generated or all blocks are sent out. The error detection relies on the built-in error detection capability of the suboptimal decoder as in [10].

The codeword x^n spans at most M transmissions during a HARQ scheme. Equivalently, we can study the communication over M parallel channels. The outputs from the main and the eavesdropper channels are as follows:

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

where $\{v(t)\}$ and $\{u(t)\}$ ($t = 1, \ldots, n$) are i.i.d. with normal distribution $\mathcal{N}(0, 1)$, 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. Additionally, we assume that any codeword x^n is with constant average energy per symbol

$$E[|x(t)|^2] \leq \bar{P}. \tag{2}$$

$\mathbf{h} = [h_1, \ldots, h_M]$ and $\mathbf{g} = [g_1, \ldots, g_M]$ are vectors of the main channel and the eavesdropper channel gains, respectively. Let $(\mathbf{h}, \mathbf{g})$ be the *channel pair*. We assume that the destination knows $\mathbf{h}$, while the eavesdropper knows $\mathbf{g}$. When $M = 1$, the transmitted codeword only spans a single fading block, we can easily compare the main channel and the eavesdropper channel. For example, if the main channel is better, i.e. $h_1 \geq g_1$, then we say that z^n is a *degraded* version of y^n. However, when $M > 1$, x^n spans multiple fading blocks, there is virtually no degraded ordering between y^n and z^n.

B. Wyner Code Ensembles

The mother code is chosen as a Wyner secrecy code [1]. Let $\mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ denote an ensemble of Wyner codes of size 2^{nR_0} to convey a message set $\mathcal{W} = \{1, 2, \ldots, 2^{nR_s}\}$. The basic idea of the Wyner code is to use a stochastic encoding, since randomization can increase secrecy. We describe the random code generation in Appendix A.

The Wyner code consists of a stochastic encoder $f(\cdot) : \mathcal{W} \rightarrow \mathcal{X}^n$ and a decoding function $\phi(\cdot)$. A stochastic encoder [2] is described 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 the channel input x^n.

For a HARQ scheme, decoding is attempted at the destination after each transmission. For convenience, let $\mathbf{x}_m = [x_1^{n_1}, \ldots, x_m^{n_1}]$, $\mathbf{y}_m = [y_1^{n_1}, \ldots, y_m^{n_1}]$, and $\mathbf{z}_m = [z_1^{n_1}, \ldots, z_m^{n_1}]$ be the input, the output at the destination, and the output at the eavesdropper after m transmissions, respectively. The average error probability after the m-th transmission is defined as

$$P_e(m) = \sum_{w \in \mathcal{W}} \Pr\big(\phi\big(\mathbf{y}_m(w)\big) \neq w | w \text{ is sent}\big) \Pr(w). \tag{3}$$

where $\phi\big(\mathbf{y}_m(w)\big)$ is the output of the decoder at the destination and $\Pr(w)$ is the probability that message $w \in \mathcal{W}$ is sent.

The secrecy, i.e., the degree to which the eavesdropper is confused, is measured by the equivocation rate at the eavesdropper after the HARQ scheme stops. Suppose that the HARQ scheme stops after m transmissions. We say that *perfect secrecy* is achieved if for any $\epsilon > 0$ the equivocation rate satisfies

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

For conciseness, we consider the following definition of good Wyner codes.

Definition 1: A Wyner code sequence $C \triangleq \{C(n)\}$ is *good* for the first m transmissions and a channel pair $(\mathbf{h}, \mathbf{g})$, if $P_e(m) \rightarrow 0$ and perfect secrecy requirement (4) is satisfied, for any $n \rightarrow \infty$.

III. Coding and Transmission

We consider two schemes: repetition time diversity ARQ (RTD-ARQ) and incremental redundancy ARQ (IR-ARQ).

A. Repetition Time Diversity ARQ

The RTD code $C(n)$ is a concatenated code, consisting of a Wyner code $C_1(n_1) \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n_1)$ as the outer code and a repetition code of length M as the inner code, where $n_1 = n/M$, i.e.,

$$C(n) = [\underbrace{C_1(n_1), C_1(n_1), \ldots, C_1(n_1)}_{M}]. \tag{5}$$

The optimal receivers perform maximal ratio combining (MRC), which essentially transforms the vector channel pair $(\mathbf{h}, \mathbf{g})$ into a scalar (Gaussian) channel pair $(\widetilde{h}(m), \widetilde{g}(m))$. The equivalent channel model (after combining) is

$$y(t) = \sqrt{\widetilde{h}(m)}x(t) + v(t); \quad z(t) = \sqrt{\widetilde{g}(m)}x(t) + u(t) \tag{6}$$

for $t = 1, \ldots, n_1$, where $\widetilde{h}(m) = \sum_{i=1}^{m} h_i$ and $\widetilde{g}(m) = \sum_{i=1}^{m} g_i$.

Theorem 1: There exists a RTD code $C(n)$ good for all $m \in \{1, \ldots, M\}$ and all channel pairs $(\mathbf{h}, \mathbf{g})$ for which

$$
\begin{aligned}
I_{XY}^{[\mathrm{RTD}]}(m) &\triangleq I(X;Y|\widetilde{h}(m)) \geq MR_0, \\
I_{XZ}^{[\mathrm{RTD}]}(m) &\triangleq I(X;Z|\widetilde{g}(m)) \leq M(R_0 - R_s),
\end{aligned} \tag{7}
$$

where $I(X;Y|\widetilde{h}(m))$ and $I(X;Z|\widetilde{g}(m))$ are single letter mutual information characterizations of channel (6).

Proof: We show that a code C_1 constructed for a channel pair (h^*, g^*) with $I(X;Y|h^*) = MR_0$ and $I(X;Z|g^*) = M(R_0 - R_s)$ is good for all channel pairs $(\widetilde{h}(m), \widetilde{g}(m))$ satisfying (7). The proof is given in Appendix B. ■

B. Incremental Redundancy ARQ

The transmitter encodes its information message by using a code $C \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$. Codewords are divided into M sub-blocks of length $n_1 = n/M$. Each sub-block is transmitted over a slot (coherence interval), until either an ACK feedback is received from the legitimate receiver or all sub-blocks are sent.

Let

$$C_m = [\underbrace{x_1^{n_1}, \ldots, x_m^{n_1}}_{m}]$$

be the first m transmitted blocks. We note that

$$C_m \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, mn_1),$$

that is, C_m is essentially a Wyner code of length mn_1 and rate pair $(MR_0/m, MR_s/m)$. Hence, we refer to

$$\{C_1, C_2, \ldots, C_M\}$$

as a family of rate-compatible Wyner secrecy codes with the rate set

$$\{MR_s, MR_s/2, \ldots, R_s\}.$$

Theorem 2: There exists a family of rate compatible Wyner secrecy codes $\{C_1, C_2, \ldots, C_M\}$, where C_m is good for all channel pairs $(\mathbf{h}, \mathbf{g})$ for which

$$
\begin{aligned}
I_{XY}^{[\mathrm{IR}]}(m) &\triangleq \sum_{i=1}^{m} I(X;Y|h_i) \geq MR_0, \\
I_{XZ}^{[\mathrm{IR}]}(m) &\triangleq \sum_{i=1}^{m} I(X;Z|g_i) \leq M(R_0 - R_s),
\end{aligned} \tag{8}
$$

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

Proof: The proof is outlined in Appendix C, where we show that:

i) There is a code $C^\star$ good for all channel pairs satisfying

$$
\begin{aligned}
&\sum_{i=1}^{M} I(X;Y|h_i) \geq MR_0, \\
&\sum_{i=1}^{M} I(X;Z|g_i) \leq M(R_0 - R_s).
\end{aligned} \tag{9}
$$

ii) Let the mother code $C_M = C^\star$, the punctured code C_m is good for all channel pairs satisfying (8).

■

IV. Achievable Secrecy Throughput

We define two outage events: reliability outage for the main channel and secrecy outage for the eavesdropper channel. Reliability outage occurs when the legitimate receiver cannot decode the mother code C_M. Assuming that the HARQ scheme completes after m transmissions, secrecy outage occurs when the eavesdropper cannot be perfectly confused when the HARQ scheme completes.

Definition 2: A channel pair $(\mathbf{h}, \mathbf{g})$ is in the *reliability outage* if

$$I_{XY}(M) < MR_0. \tag{10}$$

The *secrecy outage* occurs after m transmissions if

$$I_{XZ}(m) > M(R_0 - R_s). \tag{11}$$

1) Repetition Time Diversity ARQ: The optimal input distribution is Gaussian [3] and the mutual information pair can be written as

$$
\begin{aligned}
I_{XY}^{[\mathrm{RTD}]}(m) &= \log_2\left(1 + \sum_{i=1}^{m} \lambda_i\right), \\
I_{XZ}^{[\mathrm{RTD}]}(m) &= \log_2\left(1 + \sum_{i=1}^{m} \nu_i\right),
\end{aligned} \tag{12}
$$

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

2) Incremental Redundancy ARQ: The optimal input distribution $p(X)$ is not known in general when both CSIs are not available to the transmitter and the codeword spans multiple fading blocks. For the sake of mathematical tractability, we consider Gaussian input. Hence, the channel mutual information pair is given by

$$
\begin{aligned}
I_{XY}^{[\mathrm{IR}]}(m) &= \sum_{i=1}^{m} \log_2(1 + \lambda_i), \\
I_{XZ}^{[\mathrm{IR}]}(m) &= \sum_{i=1}^{m} \log_2(1 + \nu_i).
\end{aligned} \tag{13}
$$

The probability that an HARQ transmission completes after the transmission of m sub-blocks is

$$
\begin{aligned}
p[m] &= \Pr\left(I_{XY}(m-1) < MR_0 \text{ and } I_{XY}(m) \geq MR_0\right) \\
&= \Pr\left(I_{XY}(m-1) < MR_0\right) - \Pr\left(I_{XY}(m) < MR_0\right).
\end{aligned}
$$

Let P_e be the probability of reliability outage and P_s be the probability of secrecy outage. P_e and P_s can be evaluated as

$$P_e = \Pr\left(I_{XY}(M) < MR_0\right); \tag{14}$$

$$P_s = \sum_{m=1}^{M} p[m] \Pr\left(I_{XZ}(m) > M(R_0 - R_s)\right). \tag{15}$$

Given a target outage probability pair (ζ_e, ζ_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 problem

$$\max_{\{R_0, R_s\}} \quad \eta \qquad (16)$$
$$\text{s.t.} \quad P_e \leq \zeta_e \text{ and } P_s \leq \zeta_s.$$

By applying the renewal-reward theorem [10], [11], we obtain the secrecy throughput as

$$\eta = \frac{M}{E[m]} R_s \qquad (17)$$

where $E[m]$ is the expected number of sub-blocks being transmitted in order to complete a codeword transmission.

To evaluate $p[m]$, P_e and P_s, we need the CDFs of $I_{XY}(m)$ and $I_{XZ}(m)$. For RTD-ARQ, we can use the fact that $\sum_{i=1}^{m} \lambda_i$ and $\sum_{i=1}^{m} \nu_i$ are Gamma distributed with means $m\overline{\lambda}$ and $m\overline{\nu}$ respectively, express the CDFs of $I_{XY}^{[\text{RTD}]}(m)$ and $I_{XZ}^{[\text{RTD}]}(m)$ in terms of incomplete Gamma functions. For IR-ARQ, distributions of $I_{XY}^{[\text{IR}]}(m)$ and $I_{XZ}^{[\text{IR}]}(m)$ cannot be written in a closed form. Hence, we resort to Monte-Carlo simulation to obtain empirical CDFs. For both RTD-ARQ and IR-ARQ, we can solve (16) by a search method.

V. Numerical Results

In this section, we study the secrecy throughput of Rayleigh block fading channels based on numerical evaluations. Due to the page limit, we only show the relationship between the secrecy throughput η and the number of fading blocks M. We choose average main channel SNR $\overline{\lambda} = 20dB$, average eavesdropper channel SNR $\overline{\nu} = 10dB$, target probability of reliability outage $\zeta_e = 0.05$, target probability of secrecy outage $\zeta_s = 0.05$. Through simulations, we observe that similar results are obtained by using other parameter settings.

The result is shown in Fig. 2. It is clear that RTD and M-FBC are outperformed by their ARQ versions (RTD-ARQ and IR-ARQ respectively) significantly. This confirms the intuition that to send more symbols than what is just enough for message decoding during the codeword transmission causes not only the loss of data rate but also the risk of message interception by the eavesdropper.

In practice, different delay limits require different number of transmission blocks M. When the delay limit is strict ($M \leq 3$ is small), it is shown that RTD-ARQ may outperform IR-ARQ. If the delay limit is relaxed, IR-ARQ quickly outperforms RTD-ARQ as M increases. We observe that the secrecy throughput of RTD-ARQ actually decrease when M gets large. In fact, there exists an optimal M for RTD-ARQ scheme, e.g., in Figure 2, the optimal number of fading blocks is $M = 4$ for RTD-ARQ (and $M = 5$ for RTD). In contrast, the secrecy throughput of IR-ARQ increase monotonically with M.

Appendix

A. Wyner Code Generation

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 $p_X(\cdot)$.

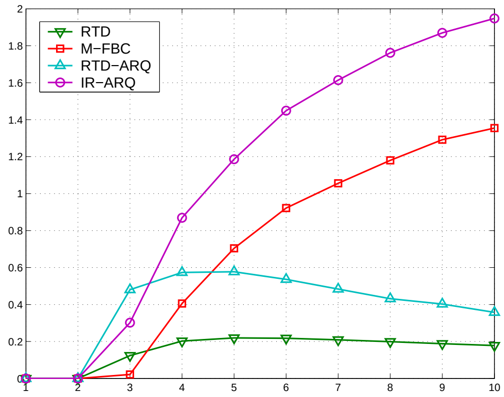

Fig. 2. Secrecy throughput η versus the number of fading blocks M

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. Proof of Theorem 1

To avoid confusion, denote $Y_1^{n_1}$ and $Z_1^{n_1}$ to be the output at the legitimate receiver and the eavesdropper respectively, through a 'virtual' Gaussian wire-tap channel (h^*, g^*) with single letter mutual information $I(X; Y_1 | h^*) = MR_0$ and $I(X; Z_1 | g^*) = M(R_0 - R_s)$.

Since $R_s = (1/M)[I(X; Y_1 | h^*) - I(X; Z_1 | g^*)]$, there exists a code $C_1 \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n_1)$ good for the channel pair (h^*, g^*) [3], such that $Y_1^{n_1}$ can be decoded with arbitrarily small error probability and the equivocation at the eavesdropper with $Z_1^{n_1}$ is

$$H(W | Z_1^{n_1}, g^*) \geq H(W) - n_1 \epsilon \qquad (18)$$

It can be shown that this code C_1 is good for all channel pairs $(\widetilde{h}(m), \widetilde{g}(m))$ such that $I(X; Y | \widetilde{h}(m)) > MR_0$ and $I(X; Z | \widetilde{g}(m)) < M(R_0 - R_s)$. Since $I(X; Y | \widetilde{h}(m)) > MR_0 = I(X; Y_1 | h^*)$, $\widetilde{h}(m) > h^*$ and $Y_1^{n_1}$ is a degraded version of Y^{n_1}, if $Y_1^{n_1}$ can be decoded at the legitimate receiver with arbitrarily small error probability, so can Y^{n_1}. We also have

$$\begin{aligned} & H(W | Z^{n_1}, \widetilde{g}(m)) - H(W | Z_1^{n_1}, g^*) \\ = \; & I(W; Z_1^{n_1} | g^*) - I(W; Z^{n_1} | \widetilde{g}(m)) \geq 0 \end{aligned}$$

where we use the fact that Z^{n_1} is a degraded version of $Z_1^{n_1}$.

$$H(W | Z^{n_1}, \widetilde{g}(m)) \geq H(W | Z_1^{n_1}, g^*) \geq H(W) - n_1 \epsilon. \quad (19)$$

for any $\epsilon > 0$ as $n_1 \to \infty$.

C. Outline of the proof of Theorem 2

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

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Y|h_i) = R_0 + \delta, \tag{20}$$

$$\frac{1}{M}\sum_{i=1}^{M} I(X;Z|g_i) = R_0 - R_s + \delta. \tag{21}$$

It is clear that $\mathcal{P}_* \subset \mathcal{P}$ when $\delta \to 0$. To prove that there exists a code good for $\mathcal{P}$, we start with proving that there is a code good for $\mathcal{P}_*$.

Given a channel pair $\mathbf{P}$ and a code ensemble $\mathcal{C}$, we consider $\Pr(\mathcal{E}_1|\mathbf{P},\mathcal{C})$, the error probability that the legitimate receiver cannot decode message W. We also consider $\Pr(\mathcal{E}_2\ |\mathbf{P},\mathcal{C})$, the probability that the eavesdropper cannot decode X^n given that it knows W and observes Z^n. When channel pair $\mathbf{P} \in \mathcal{P}_*$ is given, on every fading block $i = 1,\dots,M$, the channel is time-invariant and memoryless. By following the same steps in [12, Theorem 8.7.1], we can show that the error probabilities, averaged over the Wyner code ensemble $\mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ are

$$E_{\mathcal{C}}[\Pr(\mathcal{E}_1|\mathbf{P},\mathcal{C})] \le \epsilon_1; E_{\mathcal{C}}[\Pr(\mathcal{E}_2|\mathbf{P},\mathcal{C})] \le \epsilon_2 \tag{22}$$

for any channel pair $\mathbf{P} \in \mathcal{P}_*$ and codeword length $n \to \infty$. We define a new event $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2$. By using the union bound and taking the expectation over all $\mathbf{P} \in \mathcal{P}_*$,

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

where $\epsilon_3 = \epsilon_1 + \epsilon_2$. After exchanging the order of two expectations, we found that there exists a sequence of codes $C^\star$ such that

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

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

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

Let $\sqrt{\epsilon_3} = \epsilon_4$ and change the direction of the inequality. Also note that $\Pr(\mathcal{E}_1|\mathbf{P},C^\star)$ and $\Pr(\mathcal{E}_2|\mathbf{P},C^\star)$ are upper bounded by $\Pr(\mathcal{E}|\mathbf{P},C^\star)$, we have

$$\Pr\left(\Pr(\mathcal{E}_1|\mathbf{P},C^\star) < \epsilon_4\right) \ge 1 - \epsilon_4 \tag{23}$$

$$\Pr\left(\Pr(\mathcal{E}_2|\mathbf{P},C^\star) < \epsilon_4\right) \ge 1 - \epsilon_4 \tag{24}$$

(23) and (24) reveal that we can find a sequence of code $C^\star \in \mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$, for all $\mathbf{P} \in \mathcal{P}_*$ with probability 1, such that the legitimate receiver can decode the message W 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,

$$H(X^n|W,Z^n,\mathbf{h}^*,\mathbf{g}^*) \le 1 + n(R_0 - R_s)\Pr(\mathcal{E}_2|\mathbf{P},C^\star) \triangleq n\delta_n$$

for all $(\mathbf{h}^*,\mathbf{g}^*)$ satisfying (20) and (21). With code $C^\star$ being used, the equivocation at the eavesdropper can be bounded as

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

We can also show that $I(X^n;Z^n|\mathbf{h}^*,\mathbf{g}^*) \le n(R_0 - R_s + \delta - \epsilon)$ for any $\delta, \epsilon > 0$ and $H(X^n|h^*,\mathbf{g}^*) = nR_0$. Hence,

$$H(W|Z^n,\mathbf{h}^*,\mathbf{g}^*) \ge n(R_s - \delta_1)$$

The perfect secrecy can be achieved for any $\mathbf{P} \in \mathcal{P}_*$ with probability 1, when code C^* is used. Therefore, code C^* is good for all channel pair $\mathbf{P} \in \mathcal{P}_*$ with probability 1.

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

Now we prove that the punctured code C_m is good for any channel pair satisfying (8), for all $m = 1,\dots,M$. The punctured code C_m is obtained by taking the first m sub-blocks of C, which are then transmitted over m memoryless channel pairs $(\mathbf{h}^m,\mathbf{g}^m)$, where $\mathbf{h}^m = [h_1,\dots,h_m]$ and $\mathbf{g}^{\mathbf{m}} = [g_1,\dots,g_m]$. We can form a new sequence of channel pairs by adding other $M - m$ dummy memoryless channels whose outputs are independent of the input. For example, we can let $\mathbf{P} = (\mathbf{h},\mathbf{g})$ with $\mathbf{h} = [h_1,\dots,h_m,\dots,h_M]$ and $\mathbf{g} = [g_1,\dots,g_m,\dots,g_M]$, where $h_i = 0$ and $g_i = 0$ for all $i = m+1,\dots,M$. The dummy channel pairs have zero mutual information between the input and output. Hence, if $(\mathbf{h}^m,\mathbf{g}^m)$ satisfies (8), $\mathbf{P} = (\mathbf{h},\mathbf{g})$ satisfies (9). By using $C^\star$ as the mother code, which is good for $\mathbf{P}$, one can see that the punctured code C_m is good for $(\mathbf{h}^m,\mathbf{g}^m)$ satisfying (8).

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

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

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

[6] 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.

[7] P. Gopala, L. Lai, and H. E. gamal, "On the secrecy capacity of fading channels," *IEEE Trans. on Inf. Theory*, 2006, submitted.

[8] S. Shamai, L. Ozarow, and A. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. on Vehic. Technol.*, vol. 43, no. 2, pp. 359–378, May 1994.

[9] E. Biglieri, J. Proakis, and S. Shamai, "Fading channels: information-theoretic and communications aspects," *IEEE Trans. on Inf. Theory*, vol. 44, pp. 1895–1911, Oct. 1998.

[10] G. Caire and D. Tuninetti, "The throughput of hybrid-ARQ protocols for the gaussian collision channel," *IEEE Trans. on Inf. Theory*, vol. 47, no. 5, pp. 1971–1988, July 2001.

[11] M. Zorzi and R. R. Rao, "On the use of renewal theory in the analysis of arq protocols," *IEEE Trans. on Commun.*, vol. 44, pp. 1077–1081, Sept. 1996.

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