Private Broadcasting over Independent Parallel Channels

Ashish Khisti Member, IEEE, and Tie Liu Member, IEEE

Abstract—We study private broadcasting of two messages to two groups of receivers over independent parallel channels. Group 1 consists of $K$ receivers, all interested in a common message, whereas group 2 has only one receiver. Each message must be kept confidential from the receiver(s) in the other group. Each of the sub-channels is degraded, but the degradation order across the sub-channels can be different. We establish the optimality of a superposition construction where the codewords of the group 2 receiver form cloud-centres whereas the codewords of group 1 form satellite codewords. For the case of parallel Gaussian channels, we establish the optimality of Gaussian codebooks. We also discuss an application to secure broadcasting over block-fading channels and show that significant performance gains can be achieved using the proposed scheme over a baseline time-sharing scheme.

I. INTRODUCTION

There has been a considerable interest in applying ideas from information theory for securing wireless systems at the physical layer in recent years. Temporal channel fluctuations arising due to fading in wireless channels provide a new opportunity to transmit confidential information to desired receiver [11]–[15], while keeping it secure from the undesired receivers. When multicasting a common message, the transmitter needs to simultaneously adapt to multiple legitimate receivers, which appears to be more challenging. However even as the number of legitimate receivers goes to infinity, the secrecy capacity does not vanish to zero and is lower bounded by a constant that does not depend on the number of receivers [4]. More generally, the setup involving multiple legitimate receivers and/or eavesdroppers can be studied using the framework of a compound wiretap channel [4], [6]–[10].

We study a setup where a single transmitter needs to serve two groups of receivers over a wireless fading channel. There are $K$ receivers in group 1, all interested in a common message, whereas there is a single receiver in group 2. The message of group 1 must be kept confidential from the group 2 receiver, whereas the message of group 2 must be kept confidential from group 1. We will refer to this setup as private broadcasting. References [8], [11]–[13] study some related problems. In this paper we first consider the related problem of $M$ independent, parallel and degraded sub-channels and thereafter treat the extension to fading channels.

Our setup involving two groups, with a single receiver in one of the groups, reduces to previously known results at the corner points of the capacity region. When we only need to transmit the message for group 1, the capacity can be achieved using a secure multicast codebook [4]. Instead, when we only need to transmit the message for group 2 the capacity can be achieved using a secure product codebook [1], [7]. Both constructions extend the single user wiretap codebook [14] in different directions. A secure multicast codebook repeats the common message by using an independent wiretap codebook on each of the $M$ sub-channels. Provided that each codebook individually secures the message on its sub-channel, and independent randomization is used in each codebook, the message remains secure against the eavesdropper. The secure product codebook construction is based on a different idea. It guarantees that the output codeword on any given sub-channel is (almost) independent of the output codewords on other sub-channels. This limits the amount of information that gets leaked to an eavesdropper on any given sub-channel and in general results in a higher rate than what is achieved using a vector wiretap codebook.

It is naturally of interest to build upon the above techniques when both the messages need to be transmitted. We show that a superposition construction achieves the entire capacity region. There exists a natural order to layer the secure multicast and secure product codebooks — the codewords in the product codebook must constitute the cloud-centres, whereas the codewords in the multicast codebook must constitute satellite codewords. It should be noted that such a layering approach may not be optimal in the absence of secrecy constraints. To the best of our knowledge the capacity region remains open, even though the corner points are well known [15].

For the case of Gaussian sub-channels, we establish that the capacity is achieved using a Gaussian codebook. The proof involves obtaining a Lagrangian dual for any point on the boundary of the capacity region and then using an extremal inequality [16], [17] to show that the expression is maximized using Gaussian inputs. The result for the Gaussian channels naturally extends to a block fading channel model. We numerically evaluate the rate-region for a sub-optimal power allocation and observe significant gains over a naive time-sharing approach.

II. PROBLEM STATEMENT AND MAIN RESULTS

A. Independent Parallel Channels

Our setup involves $M$ independent parallel sub-channels and two groups of receivers. There are $K$ receivers in group
1 and one receiver in group 2. The output symbols at receiver
$k$ in group 1 across the $M$ sub-channels is denoted by
\[ y_k = (y_{k,1}, y_{k,2}, \ldots, y_{k,M}), \tag{1} \]
whereas the output symbols of the group 2 receiver across the
$M$ sub-channels are denoted by
\[ z = (z_1, z_2, \ldots, z_M), \tag{2} \]
and the channel input symbols are denoted by $x = (x_1, \ldots, x_M)$.
Each sub-channel is a degraded broadcast channel. The
degradation on sub-channel $i$ channel output over sub-channel
$1$ group $k,i$ without loss of generality we may assume that for each sub-
marginals and that Gaussian variables are infinitely divisible,
for some permutation \( \{\pi_i(1), \ldots, \pi_i(K)\} \) of the set
\( \{1, \ldots, K\} \).
We intend to transmit message $m_i$ to receivers $1, \ldots, K$
in group 1, while the message $m_2$ must be transmitted to the re-
ceiver in group 2. A length-$n$ private broadcast code encodes a
message pair \( (m_1, m_2) \in [1, 2^n r_1] \times [1, 2^n r_2] \) into a sequence $x^n$
such that $Pr(m_1 \neq m_1, k) \leq \varepsilon_n$, and $Pr(m_2 \neq m_2) \leq \varepsilon_n$,
and furthermore the secrecy constraints
\[ \frac{1}{n} I(m_1; z^n) \leq \varepsilon_n, \quad \frac{1}{n} I(m_2; y^n_k) \leq \varepsilon_n, \quad k = 1, 2, \ldots, K, \tag{4} \]
are also satisfied. Here \( \{\varepsilon_n\} \) approaches zero as $n \to \infty$.

**Theorem 1:** Let auxiliary variables \( \{u_i\}_{1 \leq i \leq M} \) satisfy the
Markov condition
\[ u_i \to x_i \to y_{\pi_i(1),i} \cdots y_{\pi_i(j),i} \to z_i \to y_{\pi_i(j+1),i} \cdots y_{\pi_i(K),i}, \tag{5} \]
The capacity region is given by the union of all rate pairs
\( (R_1, R_2) \) that satisfy the following constraints:
\[ R_1 \leq \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^{M} I(x_i; y_{k,i}|u_i, z_i) \right\} \tag{6} \]
\[ R_2 \leq \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^{M} I(u_i; z_i|y_{k,i}) \right\} \tag{7} \]
for some choice of \( \{u_i\}_{1 \leq i \leq M} \) that satisfy (5). The alphabet
of $u_i$ satisfies the cardinality constraint \( |U_i| \leq |X_i| + K \). \( \square \)

**B. Gaussian Channels**

Consider the discrete-time real Gaussian model where the
channel output over sub-channel $i$ at time index $t$ is given by
\[ y_{k,i}(t) = x_i(t) + n_{k,i}(t) \tag{8} \]
\[ z_i(t) = x_i(t) + w_i(t), \quad t = 1, \ldots, T. \tag{9} \]
The additive noise vectors $n_{k,i} = (n_{k,i}(1), \ldots, n_{k,i}(T))$ and $w_i = (w_i(1), \ldots, w_i(T))$ have entries that are sampled
i.i.d. $N(0, \sigma_{n,k,i}^2)$ and $N(0, \sigma_w^2)$, respectively. Since the capacity
region of the channel depends on the joint distribution of the additive noise
\( (n_{1,i}(t), \ldots, n_{K,i}(t), w_i(t)) \) only through the marginals and that Gaussian variables are infinitely divisible,
without loss of generality we may assume that for each sub-
channel $i$ the receivers are degraded as expressed in (3).

We shall consider both the per sub-channel average power constraint
\[ \frac{1}{T} E \left[ \|x_i(t)\|^2 \right] \leq P_i, \quad \forall i = 1, \ldots, M \tag{10} \]
and the total average power constraint
\[ \frac{1}{T} \sum_{i=1}^{M} E \left[ \|x_i(t)\|^2 \right] \leq P \tag{11} \]
where $x_i = (x_{i}(1), \ldots, x_{i}(T))$ is the input vector for sub-
channel $i$.

**Theorem 2:** The capacity region under the per sub-channel
average power constraint (10) is given by the union of all rate pairs
\( (R_1, R_2) \) that satisfy the following constraints:
\[ R_1 \leq \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^{M} A_{k,i}^{(1)}(Q) \right\} \tag{12} \]
\[ R_2 \leq \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^{M} A_{k,i}^{(2)}(Q) \right\} \tag{13} \]
for some power vector $Q = (Q_1, \ldots, Q_M)$, where $0 \leq Q_i \leq P_i$ for all $i = 1, \ldots, M$.
\[ A_{k,i}^{(1)}(Q) := \left\lfloor \frac{1}{2} \log \left( \frac{Q_i + \sigma_{n,k,i}^2}{\sigma_w^2} \right) - \frac{1}{2} \log \left( \frac{Q_i + \sigma_w^2}{\sigma_{n,k,i}^2} \right) \right\rfloor^+ \tag{14} \]
\[ A_{k,i}^{(2)}(Q) := \left\lfloor \frac{1}{2} \log \left( \frac{P_i + \sigma_{n,k,i}^2}{Q_i + \sigma_{n,k,i}^2} \right) - \frac{1}{2} \log \left( \frac{P_i + \sigma_{n,k,i}^2}{Q_i + \sigma_w^2} \right) \right\rfloor^+ \tag{15} \]
and $x^+ := \max\{x, 0\}$.

**Corollary 1:** The capacity region under the total average
power constraint (11) is given by the union of all rate pairs
\( (R_1, R_2) \) that satisfy the constraints (12) and (13) for some
power vectors $P = (P_1, \ldots, P_M)$ and $Q = (Q_1, \ldots, Q_M)$,
where $0 \leq Q_i \leq P_i$ for all $i = 1, \ldots, M$ and $\sum_{i=1}^{M} P_i \leq P$.
\( \square \)

The above corollary follows directly from Theorem 2 and
the well-known connection between the per sub-channel and
the total average power constraints.

**C. Fading Channels**

We consider a block-fading channel model with a coherence
period of $T$ complex symbols. The channel output in
coherence block $i$ is given by
\[ y_k(i) = h_k(i)x(i) + n_k(i) \tag{16} \]
\[ z(i) = g(i)x(i) + w(i), \quad i = 1, 2, \ldots, M \tag{17} \]
where the channel gains $h_k(i)$ of the $K$ receivers in group 1
and the channel gain $g(i)$ of the special receiver in group 2
are sampled independently in each coherence block $i$ and stay
constant throughout the block. The channel input $x(i) \in \mathbb{C}^T$
satisfies a long-term average power constraint
\[ E \left\lfloor \frac{1}{MT} \sum_{i=1}^{M} \|x(i)\|^2 \right\rfloor \leq P \tag{18} \]
Fig. 1: Our proposed superposition construction for the case of two channels. The product codebook for the group 2 user is obtained by taking a cartesian \( C_{21} \times C_{22} \) of two independently generated codebooks and binning the resulting codeword pairs. The multicast codebook is generated, conditioned on the codewords of \( C_{21} \) and \( C_{22} \), whereas the additive noise vectors \( \mathbf{n}(i) \) and \( \mathbf{w}(i) \) have entries that are sampled i.i.d. \( \mathcal{CN}(0,1) \). We are interested in the ergodic communication scenario where the number of blocks \( M \) used for communication can be arbitrarily large. Furthermore we assume that the channel gains in each coherence block are revealed to all terminals including the transmitter at the beginning of each coherence block.

**Theorem 3:** The private broadcasting capacity region for the fading channel model consists of all rate pairs \( (R_1,R_2) \) that satisfy the following constraints:

\[
R_1 \leq \min_{1 \leq k \leq K} E \left[ \log \left( \frac{1 + P(h,g)|h_k|^2}{1 + Q(h,g)|g|^2} \right) \right],
\]

\[
R_2 \leq \min_{1 \leq k \leq K} E \left[ \log \left( \frac{1 + P(h,g)|h_k|^2}{1 + Q(h,g)|g|^2} \right) - \log \left( \frac{1 + P(h,g)|h_k|^2}{1 + Q(h,g)|h_k|^2} \right) \right],
\]

for some power allocation functions \( P(h,g) \) and \( Q(h,g) \) that satisfy \( 0 \leq Q(h,g) \leq P(h,g) \) and \( E[P(h,g)] \leq P \), where \( h := (h_1, \ldots, h_K) \) denotes the channel gains of the receivers in group 1.

**III. CODING THEOREM**

The basic idea behind our coding scheme is illustrated in Fig. 1. The message \( m_2 \) is encoded using a product codebook [1], [7], whose codewords are obtained by taking cartesian product of the \( M \) codebooks, one for each of the parallel channels. The message \( m_1 \) is encoded using a multicast codebook [4], also consisting of \( M \) codebooks. As shown in Fig. 1, the codewords of the product-codebook constitute cloud centres of the superposition codebook, whereas the codewords of the multicast codebook constitute the satellite codewords.

We describe the details of our construction in the following sub-sections.

**A. Product-Codebook Construction**

The message \( m_2 \) is encoded using a product codebook [1], [7]. Let \( \mathcal{M}_{2,i} \) be the set of all binary sequences of length \( N_{2,i} = n(I(u_i;z_i) - 2\varepsilon) \) i.e.,

\[
\mathcal{M}_{2,i} := \{0,1\}^{N_{2,i}}.
\]

(21)

On channel \( i \), we generate a codebook \( \mathcal{C}_{2,i} : \mathcal{M}_{2,i} \rightarrow \mathcal{U}_i^n \) consisting of \( |\mathcal{M}_{2,i}| \) codewords, i.e.,

\[
\mathcal{C}_{2,i} := \left\{ u_i^n(m_{2,i}) : m_{2,i} \in [1,2^{N_{2,i}}] \right\},
\]

where each sequence \( u_i^n \) is sampled i.i.d. from the distribution \( p_{u_i}() \). Let

\[
\mathcal{M}_2 := \mathcal{M}_{2,1} \times \mathcal{M}_{2,2} \times \ldots \times \mathcal{M}_{2,M}
\]

\[
= \left\{ (\bar{m}_{2,1},\ldots,\bar{m}_{2,M}) : \bar{m}_{2,i} \in \{0,1\}^{N_i}, i = 1,\ldots,M \right\}.
\]

(23)

(24)

As shown in Fig. 1, we partition the set \( \mathcal{M}_2 \) into \( 2^{nN_2} \) bins such that there are \( L_2 = 2^n(\Sigma_{i=1}^M, I(u_i;z_i)=R_2-M\varepsilon) \) sequences in each bin. Each bin corresponds to one message \( m_2 \in \{1,2^{nN_2}\} \). Thus given a message \( m_2 \) the encoder selects one sequence \( (\bar{m}_{2,1},\ldots,\bar{m}_{2,M}) \in \mathcal{M}_2 \) uniformly at random from the corresponding bin. On channel \( i \) we select the codeword \( u_i^n \in \mathcal{C}_{2,i} \) associated with \( \bar{m}_{2,i} \). We note that from our construction, each sequence in \( \mathcal{M}_2 \) is equally likely i.e.,

\[
\Pr(\bar{m}_{2,1} = \bar{m}_{2,1},\ldots,\bar{m}_{2,M} = \bar{m}_{2,M})
\]

\[
= \prod_{j=1}^M \Pr(\bar{m}_{2,j} = \bar{m}_{2,j}) = \frac{1}{|\mathcal{M}_{2,1}| \times |\mathcal{M}_{2,2}| \ldots |\mathcal{M}_{2,M}|}.
\]

(25)

**B. Multicast Code Construction**

The codebook associated with \( m_1 \) is a secure multicast codebook [4]. For each \( u_i^n \in \mathcal{C}_{2,i} \), and each \( m_1 \in \{1,2^{nM_1}\} \) we construct a codebook \( \mathcal{C}_{1,i}(u_i^n, m_1) \) consisting of a total of \( L_{1,i} = 2^n(I(x_i;z_i|u_i) + \varepsilon) \) codeword sequences of length \( n \), each sampled i.i.d. from the distribution \( \prod_{j=1}^M p_{x_i|u_i}(x_{ij}|u_{ij}) \), and define:

\[
\hat{C}_{1,i}(u_i^n) := \bigcup_{m_1=1}^{2^{nM_1}} \mathcal{C}_{1,i} (u_i^n, m_1).
\]

Let \( l_{1,i} \) be uniformly distributed over \( [1,L_{1,i}] \). Given a message \( m_1 \in \{1,2^{nM_1}\} \) and codewords \( (u_1^n,\ldots,u_M^n) \), selected in the base layer, we select the sequence \( x^n_i \) from the codebook \( \mathcal{C}_{1,i}(u_i^n, m_1) \) corresponding to the randomly generated index \( l_{1,i} \).
C. Decoding

Receiver $k$ in group 1 selects those sub-channels $\mathcal{J}_k$ where $I(x_i; y_{i,z_i}, u_i) > 0$. It searches for a message $m_1 \in [1, 2^{nH_1}]$ such that for each $i \in \mathcal{J}_k$, there exists a pair $(x_i^n, u_i^n)$ with $x_i^n \in C_1(u_i^n, m_1)$, jointly typical with $y_{i,z_i}$. An error event happens if there is another message $m'_1$ such that for each $i \in \mathcal{J}_k$ the receiver finds some $u_i^n \in C_{2,i}$ and $x_i^n \in C_{1,i}(u_i^n, m')$ that $(u_i^n, x_i^n, y_{i,z_i})$ are jointly typical. Using the joint-typicality lemma [18, Chapter 2, p. 29] and the standard union-bound argument, it can be shown that the error probability at each receiver $k$ approaches zero if $R_1$ satisfies (6).

The receiver in group 2 decodes message $\hat{m}_{2,i}$ on sub-channel $i$ by searching for a sequence $u_i^n \in C_{2,i}$ that is jointly typical with $z_i^n$. Since the number of codewords in $C_{2,i}$ is not greater than $2^{n(I(u_i;z_i)-2\varepsilon)}$ this event succeeds with high probability. Hence the receiver correctly decodes $(\hat{m}_{2,1}, \ldots, \hat{m}_{2,M})$ and in turn message $m_2$ with high probability.

D. Secrecy Analysis

In order to establish the secrecy of message $m_1$ we need to show that

$$\frac{1}{n} I(m_1; z^n_i | C) \leq \varepsilon_n$$  \hspace{1cm} (26)

Since the message sequence $(\hat{m}_{2,1}, \ldots, \hat{m}_{2,M})$ is uniformly distributed (c.f. (25)), it follows that the sequences $(z^n_1, \ldots, z^n_M)$ are conditionally independent given $m_1$, and hence

$$\frac{1}{n} I(m_1; z^n_i | C) \leq \sum_{i=1}^{M} I(m_1; z^n_i | C)$$  \hspace{1cm} (27)

holds. Since in our conditional codebook construction, there are $2^{n(I(x_i;z_i|u_i)+\varepsilon)}$ sequences in each codebook $C_{1,i}(u_i^n, m_1)$, it follows from standard arguments that

$$\frac{1}{n} I(m_1; z^n_i | C) \leq \varepsilon_n.$$  \hspace{1cm} (28)

The condition (26) follows immediately.

To establish secrecy of message $m_2$ with respect to user 1 in group 1, we show that

$$\frac{1}{n} H(m_2 | y^n_{1,i}, m_1) \geq R_2 - \varepsilon_n.$$  \hspace{1cm} (29)

Without loss of generality, we assume that sub-channels $i = 1, 2, \ldots, L$ satisfy $x_i \rightarrow y_{1,i} \rightarrow z_i$ while sub-channels $i = L + 1, \ldots, M$ satisfy $x_i \rightarrow z_i \rightarrow y_{1,i}$. Thus we have

$$\frac{1}{n} H(m_2 | y^n_{1,i}, m_1) \geq \frac{1}{n} H(m_2 | y^n_{1,i}, m_1, \hat{m}_{2,i}^L, C)$$

\hspace{1cm} (30)

where $\hat{m}_{2,i}^L := (\hat{m}_{2,1}, \ldots, \hat{m}_{2,M})$ is the randomly selected sequence in the bin index of $m_2$ in the product codebook.

To complete the analysis, we show that the two terms in (30) satisfy the following:

$$\frac{1}{n} H(\hat{m}_{2,i}^L | \hat{m}_{2,i}^L, y^n_{1,i}, m_1, C) \geq \sum_{i=L+1}^{M} I(u_i; z_i) - I(u_i; y_{1,i}) - \varepsilon,$$  \hspace{1cm} (31)

and

$$\frac{1}{n} H(\hat{m}_{2,i}^L | \hat{m}_{2,i}^L, m_2, m_1, y^n_{1,i}, C) \leq \sum_{i=L+1}^{M} I(u_i; z_i) - I(u_i; y_{1,i}) - R_2 + \varepsilon.$$  \hspace{1cm} (32)

From the mutual independence of $(\hat{m}_{2,1}, \ldots, \hat{m}_{2,M})$ in (25) it follows that

$$\frac{1}{n} H(\hat{m}_{2,i}^L | \hat{m}_{2,i}^L, y^n_{1,i}, m_1) = \sum_{i=L+1}^{M} \frac{1}{n} H(\hat{m}_{2,i}^L | m_1, y^n_{1,i}, C)$$  \hspace{1cm} (33)

Thus we treat each term on the right-hand side of (33) separately. Consider

$$\frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1)$$

$$= \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1) = \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1) = \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1)$$  \hspace{1cm} (34)

$$= \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1) = \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1)$$

$$= \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1) = \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1)$$  \hspace{1cm} (35)

From the construction we have

$$\frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1) = \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1) = \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1)$$

$$= \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1) = \frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1)$$  \hspace{1cm} (36)

$$\geq I(u_1; z_1) + I(x_1; z_1 | u_1) - \varepsilon$$  \hspace{1cm} (37)

$$\geq I(x_1; z_1) - \varepsilon,$$  \hspace{1cm} (38)

where (36) follows from the fact that $m_2$ is selected independently of $m_1$, and $i_1$ is selected independently of $(m_2,i_1)$. Using the Markov chain $(m_1, C, m_2, i_1, i_1) \rightarrow x^n_1 \rightarrow y^n_{1,i_1}$ and the fact that the sequences $(x_1^n, y^n_{1,i_1}) \sim \prod_{j=1}^{L} p(x_j, y_{1,i_1})$ we have

$$\frac{1}{n} I(m_2, i_1, i_1, i_1, i_1, i_1 | m_1, C) \leq I(x_1; y_{1,i_1}).$$  \hspace{1cm} (39)

The third term in (35) can be bounded from above using [9, Lemma 1]. Since the codebook $C_1(u^n_1, m_1)$ consists of a total of $L_1 = 2^{n(I(x; z_i|u_i)+\varepsilon)}$ codeword sequences and $I(x_1; z_1 | u_1) > I(x_1; y_{1,i_1} | u_1)$ we have that

$$\frac{1}{n} H(m_2, i_1, i_1, i_1, i_1, i_1) \geq I(x_1; z_1 | u_1) - I(x_1; y_{1,i_1} | u_1) - \varepsilon.$$  \hspace{1cm} (40)

Substituting (38)-(40) into (35) and (33) we obtain (31).

To establish (32) we observe that from the symmetry of the code construction we have

$$\frac{1}{n} H(\hat{m}_{2,i}^L | \hat{m}_{2,i}^L, m_2, m_1, y^n_{1,i}, C)$$

$$= \frac{1}{n} H(\hat{m}_{2,i}^L | \hat{m}_{2,i}^L, m_2, m_1, y^n_{1,i}, C)$$  \hspace{1cm} (41)
Associated with \((m_2, m_{L,1}^M) = (1, 1^L)\), there are a total of 
\(2^nS\) possible sequences \((m_2, L+1, \ldots, m_2, M)\), where 
\(S = \sum_{i=L+1}^{M} I(u_i; z_i) - R_2 - \varepsilon\). For any \(R_2\) satisfying (7) by 
applying \([18, \text{Lemma 22.1, Remark 22.2, pp. 554-555}]\), we have
\[
\frac{1}{n} H(m_{2,L+1}^M | m_{2,L}^1) = 1^L, m_2 = 1, m_1 = 1, y_1^n, C \leq S - I(u_1, \ldots, u_M; y_1, \ldots, y_M) - \varepsilon \tag{42}
\]
\[
= S - \sum_{i=L+1}^{M} I(u_i; y_1, \ldots, y_i) - \varepsilon \tag{43}
\]
\[
= \sum_{i=L+1}^{M} I(u_i; z_i) - I(u_i; y_1, \ldots, y_i) - R_2 - 2\varepsilon \tag{44}
\]
where we use the fact that the pair \((u_i, y_1, \ldots, y_i)\) is independent of all 
variables in \((43)\). This completes the secrecy analysis for 
message \(m_2\) with respect to user 1 in group 1. The analysis for 
the remaining users in group 1 is completely analogous and 
will be omitted.

IV. CONVERSE

We first show that there exists a choice of auxiliary variables 
\(u_i(j)\) that satisfy the Markov chain condition
\[
u_i(j) \rightarrow x_i(j) \rightarrow y_{\pi(1),i}(j) \cdots y_{\pi(i),i}(j) \rightarrow \]
\(z_i(j) \rightarrow y_{\pi(i+1),i}(j) \cdots y_{\pi(K),i}(j). \tag{45}\)
such that the rates \(R_1\) and \(R_2\) are upper bounded by
\[
nR_1 \leq \sum_{i=1}^{M} n \sum_{j=1}^{n} I(x_i(j); y_{k,i}(j)|u_i(j), z_i(j)) + n\varepsilon_n \tag{46}
\]
\[
nR_2 \leq \sum_{i=1}^{M} n \sum_{j=1}^{n} I(u_i(j); z_i(j)|y_{k,i}(j)) + n\varepsilon_n \tag{47}
\]
for each \(k \in \{1, \ldots, K\} \).

In particular we show that the choice of \(u_i(j)\) is given by the 
following
\[
u_i(j) = \left\{ m_2, z_{n,i}^n, z_{i+1}^n, \bar{z}_{i}^{n-1} \right\} \tag{48}
\]
where we have introduced (c.f. \((45)\))
\[
\bar{z}_{i}^{n} = (\bar{z}_{i}^{n}, y_{n,(i+1),i}^{n}, \ldots, y_{n,(K),i}^{n}), \tag{49}
\]
\[
\bar{z}_{i}^{n} = (\bar{z}_{i}^{n}, z_{i+1}^{n}, \ldots, z_{n}^{n}), \tag{50}
\]
\[
\bar{z}_{i}^{n-1} = (\bar{z}_{i}^{n-1}, y_{n,(i+1),i}^{n-1}, \ldots, y_{n,(K),i}^{n-1}), \tag{51}
\]
\[
\bar{z}_{i+1}^{n} = (\bar{z}_{i+1}^{n}, y_{n,(i+1),i+1}, \ldots, y_{n,(K),i+1}), \tag{52}
\]
and observe our choice of \(u_i(j)\) in \((48)\) indeed satisfies \((45)\). 
Note that \(\bar{z}_{i}^{n}\) is the collection of the eavesdropper’s channel 
output as well as the output of all the receivers that are 
degraded with respect to the eavesdropper on sub-channel \(i\).

We begin with the secrecy constraint associated with 
message \(m_2\) with respect to user \(k\) in group 1. Let us define the 
following:
\[
\bar{y}_{k,i}^n := \begin{cases} 
  y_{k,i}^n, & \text{if } y_{k,i} = z_k \\
  z_k^n, & \text{if } y_{k,i} = z_k 
\end{cases} \tag{53}
\]
and let
\[
y_k^n := (\bar{y}_{k,1,i}^n, \ldots, \bar{y}_{k,M,i}^n). \tag{54}
\]
\[
z^n := (z_1^n, \ldots, z_M^n). \tag{55}
\]
Thus \(y_k^n\) corresponds to a weaker receiver, whose output on 
channel \(i\) is degraded to \(z_i^n\), if user \(k\) is stronger than the group 
2 user on this sub-channel. Clearly we also have \(\frac{1}{n} I(m_2; \bar{y}_k^n) \leq \varepsilon_n\).

Thus
\[
nR_2 \leq I(m_2; z^n) - I(m_2; \bar{y}_k^n) \tag{56}
\]
\[
\leq I(m_2; z^n \bar{y}_k^n) \tag{57}
\]
\[
= \sum_{i=1}^{M} \sum_{j=1}^{n} I(m_2; z_{i,j})|z_{i,j}^{n-1}, z_{i,j-1}^{n}, \bar{y}_k^n) \tag{58}
\]
\[
\leq \sum_{i=1}^{M} \sum_{j=1}^{n} I(m_2; z_{i,j}^{n-1}, z_{i,j+1}^{n}, z_{i,j-1}^{n}, \bar{y}_k^n) \tag{59}
\]
\[
\leq \sum_{i=1}^{M} \sum_{j=1}^{n} I(m_2; z_{i,j}^{n-1}, z_{i,j+1}^{n}, z_{i,j-1}^{n}, \bar{y}_k^n) \tag{60}
\]
\[
= \sum_{i=1}^{M} \sum_{j=1}^{n} I(u_i(j); z_i(j)|y_{k,i}(j)) \tag{61}
\]
\[
= \sum_{i=1}^{M} \sum_{j=1}^{n} I(u_i(j); z_i(j)|y_{k,i}(j)) \tag{62}
\]
where \((60)\) follows from the fact that
\[
(z_{i-1}^{n}, \bar{y}_{k,i}^{n}) \subseteq \bar{z}_i^{n} \tag{63}
\]
\[
(z_{i}^{n-1}, \bar{y}_{k,i}^{n-1}) \subseteq \bar{z}_i^{n-1} \tag{64}
\]
\[
(z_{i-1}^{n}, \bar{y}_{k,i+1}^{n}) \subseteq \bar{z}_i^{n+1} \tag{65}
\]
and the last step follows from the fact whenever \(y_{k,i}(j) \neq \bar{y}_{k,i}(j)\) 
then \(z_i(j)\) is a degraded version of \(y_{k,i}(j)\) and 
from \((53)\), we have that
\[
I(u_i(j); z_i(j)|y_{k,i}(j)) = I(u_i(j); z_i(j)|\bar{y}_{k,i}(j)) = 0. \tag{66}
\]
This establishes \((47)\). Next, we upper bound \(R_1\) as follows:
\[
nR_1 \leq I(m_1; \bar{y}_i^n) - I(m_1; z^n, m_2) + 2n\varepsilon_n \tag{67}
\]
\[
\leq I(m_1; \bar{y}_i^n | z^n, m_2) + 2n\varepsilon_n \tag{68}
\]
\[
\leq \sum_{i=1}^{M} \sum_{j=1}^{n} I(m_1; y_{i,k}(j)|z_{i,j}^{n-1}, y_{k,i-1}^n, z^n, m_2) + 2n\varepsilon_n \tag{69}
\]
\[
\leq \sum_{i=1}^{M} \sum_{j=1}^{n} H(y_{i,k}(j)|z_{i,j}^{n-1}, y_{k,i-1}^n, z^n, m_2) \tag{70}
\]
\[
- H(y_{i,k}(j)|z_{i,j}^{n-1}, y_{k,i-1}^n, z^n, m_1, m_2, x_i(j)) \tag{71}
\]
\[
= \sum_{i=1}^{M} \sum_{j=1}^{n} H(y_{i,k}(j)|z_{i,j}^{n-1}, y_{k,i-1}^n, z^n, m_2) \tag{72}
\]
\[
- H(y_{i,k}(j)|x_i(j), z_i(j)) \tag{73}
\]
\[
\leq \sum_{i=1}^{M} \sum_{j=1}^{n} H(y_{i,k}(j)|z^n, m_2) - H(y_{i,k}(j)|x_i(j), z_i(j)) \tag{74}
\]
where (71) follows from the fact that for our channel model
\( y_k,i(j) \) are independent of all other random variables
given \( x_i(j) \) whereas (73) follows from the fact that even
though \( Z^n \subseteq \{ Z^n_k, Z^n_{i,j+1}, Z^{i,j}(j) \} \) holds, the additional elements
in the latter are only a degraded version of \( Z^n \). This
establishes (46).

To complete the converse, let \( q_i \) to be a random variable
uniformly distributed over the set \( \{ 1, 2, \ldots, n \} \) and furthermore we let
\( u_i = (u_i(q_i), q_i) \), \( x_i = x_i(q_i) \) etc. Then (46) and (47) can be reduced to

\[
R_1 \leq \sum_{i=1}^{M} I(x_i; y_{k,i}|u_i, z_i, q_i) = \sum_{i=1}^{M} I(x_i; y_{k,i}|u_i, z_i) \tag{76}
\]

\[
R_2 \leq \sum_{i=1}^{M} I(u_i; z_i|y_{k,i}, q_i) \leq \sum_{i=1}^{M} I(u_i; z_i|y_{k,i}) \tag{77}
\]

The upper bound on the cardinality of \( U_i \) follows by a
straightforward application of Caratheodory’s theorem and the
proof will be omitted.

A. Special case of \( K = 2 \) receivers

For the case when there are \( K = 2 \) receivers, the upper bound
can be obtained by combining single-letter bounds generated from
a pair-wise comparison. In particular, suppose that we only need to transmit message \( m_1 \) to receiver \( 1 \) in
group 1. Suppose that the message \( m_2 \) only needs to be secure
from user 2 in group 1. Under these relaxed constraints, it can
be show that the rate-pairs must satisfy:

\[
R_1 \leq \sum_{i=1}^{M} I(x_i; y_{1,i}|z_i, u_i), \quad R_2 \leq \sum_{i=1}^{M} I(u_i; z_i|y_{2,i}). \tag{78}
\]

for some auxiliary variables \( \{ u_i \} \) that satisfy the
Markov chain in (45). Similarly if we instead consider
transmitting message \( m_1 \) only to user 2 in group 1 and require
secrecy of \( m_2 \) only with respect to user 1 in group 1, one can show that the rate-pairs must satisfy:

\[
R_1 \leq \sum_{i=1}^{M} I(x_i; y_{2,i}|z_i, v_i), \quad R_2 \leq \sum_{i=1}^{M} I(v_i; z_i|y_{1,i}). \tag{79}
\]

for some auxiliary variables \( \{ v_i \} \) that satisfy the
Markov chain in (45). Similarly if we instead consider
transmitting message \( m_1 \) only to user 2 in group 1 and require
secrecy of \( m_2 \) only with respect to user 1 in group 1, one can show that the rate-pairs must satisfy:

\[
\text{Group 2 receiver satisfies } x_i \rightarrow z_i \rightarrow (y_{1,i}, y_{2,i}); \text{ It }
\text{suffices to take } u_i = v_i = x_i \text{ in (78) and (79) as the contribution of this sub-channel in the expressions for } R_1 \text{ is always zero.}
\]

\[
\text{Group 2 receiver satisfies } x_i \rightarrow (y_{1,i}, y_{2,i}) \rightarrow z_i; \text{ It }
\text{suffices to take } u_i = v_i = 0 \text{ since the contribution of this sub-channel in the expressions for } R_2 \text{ is zero.}
\]

\[
\text{Group 2 receiver satisfies } x_i \rightarrow y_{1,i} \rightarrow z_i \rightarrow y_{2,i}; \text{ Since the contribution of sub-channel } i \text{ in the expressions for both } R_1 \text{ and } R_2 \text{ in (79) is zero, we can set } v_i = u_i.
\]

\[
\text{Group 2 receiver satisfies } x_i \rightarrow y_{2,i} \rightarrow z_i \rightarrow y_{1,i}; \text{ Since the contribution of sub-channel } i \text{ in the expressions for both } R_1 \text{ and } R_2 \text{ in (78) is zero, we can set } u_i = v_i.
\]

Thus we have no more than one non-trivial auxiliary variable
on each sub-channel. Setting \( v_i = u_i \) in (79) we have

\[
R_1 \leq \sum_{i=1}^{M} I(x_i; y_{2,i}|z_i, u_i), \quad R_2 \leq \sum_{i=1}^{M} I(u_i; z_i|y_{1,i}). \tag{80}
\]

The converse follows by combining (78) and (80).

Unfortunately when there are more than two receivers in
one group, we have not been able to obtain the converse directly
from such single-letter expressions. The method of directly
identifying \( u_i \) as in (48) appears necessary.

V. GAUSSIAN CHANNELS

In this section we provide a proof for Theorem 2. Note that
the achievability of the rate pairs \( (R_1^*, R_2^*) \) constrained
by (12) and (13) follows that of those constrained by (6) and
(7) by setting \( x_i = u_i + v_i \), where \( u_i \) and \( v_i \) are independent
\( N(0, P_i - Q_i) \) and \( N(0, Q_i) \) respectively for some \( 0 \leq Q_i \leq P_i \) and \( i = 1, \ldots, M \). For the rest of the section, we shall
focus on proving the converse result.

Considering proof by contradiction, let us assume that
\( (R_1^*, R_2^*) \) is an achievable rate pair that lies outside the rate
region constrained by (12) and (13). Note that the maximum
rate for message \( m_1 \) is given by the right-hand side of (12) by
setting \( Q_i = P_i \) for all \( i = 1, \ldots, M \) [4], and the maximum
rate for message \( m_2 \) is given by the right-hand side of (13) by
setting \( Q_i = 0 \) for all \( i = 1, \ldots, M \) [1], [7]. Thus, without
loss of generality we may assume that \( R_2^* = R_2^* + \delta \) for some
\( \delta > 0 \) where \( R_2^* \) is given by

\[
\max_{(Q,R)} R_2 \tag{81}
\]

subject to

\[
R_1^* \leq \sum_{i=1}^{M} A_{k,i}((Q), \forall k = 1, \ldots, K \tag{82}
\]

\[
R_2 \leq \sum_{i=1}^{M} A_{k,i}((Q), \forall k = 1, \ldots, K \tag{83}
\]

\[
Q_i \geq 0, \quad \forall i = 1, \ldots, M \tag{83}
\]

\[
Q_i \leq P_i, \quad \forall i = 1, \ldots, M. \tag{84}
\]

For each \( k = 1, \ldots, K \) and \( i = 1, \ldots, M \) let \( \alpha_k, \beta_k, M_{k,i}, M_{k,i}, \) and \( M_{k,i} \) be the Lagrangians that correspond to the constrains
(81)–(84) respectively, and let
\[ L := R_2^0 + \sum_{k=1}^{K} \alpha_k \left[ \sum_{i=1}^{M} A_{k,i}^{(1)}(Q) - R_i^0 \right] + \sum_{k=1}^{K} \beta_k \left[ \sum_{i=1}^{M} A_{k,i}^{(2)}(Q) - R_2^0 \right] + \sum_{i=1}^{M} M_{1,i}Q_i + \sum_{i=1}^{M} M_{2,i}(P_i - Q_i). \] (85)

It is straightforward to verify that the above optimization program that determines \( R_2^0 \) is a convex program. Therefore, taking partial derivatives of \( L \) over \( Q_i, i = 1, \ldots, M \) and \( R_2 \) respectively gives the following set of Karush-Kuhn-Tucker (KKT) conditions, which must be satisfied by any optimal solution \((Q^*, R_2^0)\):

\[
\sum_{k \in Y_i} \alpha_k (Q_i^* + \sigma_{k,i}^2)^{-1} + \sum_{k \in Z_i} \beta_k (Q_i^* + \sigma_{k,i}^2)^{-1} = \left( \sum_{k \in Y_i} \alpha_k + \sum_{k \in Z_i} \beta_k \right) (Q_i^* + \delta_i^2)^{-1} + M_{1,i}
\] (86)

\[
\sum_{k=1}^{K} \beta_k = 1
\] (87)

\[
\alpha_k \left[ \sum_{i=1}^{M} A_{k,i}^{(1)}(Q^*) - R_i^0 \right] = 0, \forall k = 1, \ldots, K
\] (88)

\[
\beta_k \left[ \sum_{i=1}^{M} A_{k,i}^{(2)}(Q^*) - R_2^0 \right] = 0, \forall k = 1, \ldots, K
\] (89)

\[
M_{1,i}Q_i^* = 0, \forall i = 1, \ldots, M
\] (90)

\[
M_{2,i}(P_i - Q_i^*) = 0, \forall i = 1, \ldots, M
\] (91)

\[
\alpha_k, \beta_k \geq 0, \forall k = 1, \ldots, K
\] (92)

\[
M_{1,i}, M_{2,i} \geq 0, \forall i = 1, \ldots, M
\] (93)

where

\[
Y_i := \{ k : \sigma_{k,i}^2 < \delta_i^2 \} \tag{94}
\]

\[
Z_i := \{ k : \sigma_{k,i}^2 > \delta_i^2 \} \tag{95}
\]

Note that \( \delta > 0 \), so we have

\[
\left( \sum_{k=1}^{K} \alpha_k \right) R_1^0 + R_2^0 > \left( \sum_{k=1}^{K} \alpha_k \right) R_1^0 + R_2^0
\] (96)

\[
= \sum_{k=1}^{K} \left( \alpha_k R_1^0 + \beta_k R_2^0 \right)
\] (97)

\[
= \sum_{k=1}^{K} \left[ \alpha_k \sum_{i=1}^{M} A_{k,i}^{(1)}(Q^*) + \beta_k \sum_{i=1}^{M} A_{k,i}^{(2)}(Q^*) \right]
\] (98)

\[
= \sum_{i=1}^{M} \sum_{k=1}^{K} \left[ \alpha_k A_{k,i}^{(1)}(Q^*) + \beta_k A_{k,i}^{(2)}(Q^*) \right], \quad \text{(99)}
\]

where (97) follows from the KKT condition (87), and (98) follows from the KKT conditions (88) and (89).

Next, we shall show that by assumption \((R_1^0, R_2^0)\) is achievable, so we have

\[
\left( \sum_{k=1}^{K} \alpha_k \right) R_1^0 + R_2^0 \leq \sum_{i=1}^{M} \sum_{k=1}^{K} \left[ \alpha_k A_{k,i}^{(1)}(Q^*) + \beta_k A_{k,i}^{(2)}(Q^*) \right] \tag{100}
\]

which is an apparent contradiction to (99) and hence will help to complete the proof of the theorem.

To prove (100), let us use the converse part of Theorem 1 on \((R_1^0, R_2^0)\) and write

\[
\left( \sum_{k=1}^{K} \alpha_k \right) R_1^0 + R_2^0 \leq \left( \sum_{k=1}^{K} \alpha_k \right) \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^{M} I(x_i; y_{k,i}|u_i, z_i) \right\} + \sum_{i=1}^{M} \sum_{k=1}^{K} \alpha_k I(x_i; y_{k,i}|u_i, z_i) + \sum_{k=1}^{K} \beta_k I(u_i; z_i|y_{k,i}) \tag{101}
\]

\[
\leq \sum_{k=1}^{K} \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^{M} I(x_i; y_{k,i}|u_i, z_i) \right\} + \sum_{k=1}^{K} \sum_{i=1}^{M} \beta_k I(u_i; z_i|y_{k,i}) \tag{102}
\]

\[
= \sum_{i=1}^{M} \sum_{k=1}^{K} \alpha_k I(x_i; y_{k,i}|u_i, z_i) + \sum_{k=1}^{K} \beta_k I(u_i; z_i|y_{k,i}) \tag{103}
\]

where (102) follows from the well-known fact that minimum is no more than any weighted mean. By the degradedness assumption (3), we have

\[
I(x_i; y_{k,i}|u_i, z_i) = I(x_i; y_{k,i}|u_i) - I(x_i; z_i|u_i) \tag{104}
\]

\[
= h(y_{k,i}|u_i) - h(z_i|u_i) - h(n_{k,i}) + h(w_i) \tag{105}
\]

\[
= h(y_{k,i}|u_i) - h(z_i|u_i) - \frac{1}{2} \log \left( \frac{\sigma_{k,i}^2}{\delta_i^2} \right) \tag{106}
\]

for any \( k \in Y_i \) and \( I(x_i; y_{k,i}|u_i, z_i) = 0 \) for any \( k \notin Y_i \).

Similarly,

\[
I(u_i; z_i|y_{k,i}) = h(z_i|u_i) - h(n_{k,i}) + h(w_i) \tag{107}
\]

\[
\leq \frac{1}{2} \log \left( \frac{P_i + \delta_i^2}{P_i + \sigma_{k,i}^2} \right) - h(z_i|u_i) + h(y_{k,i}|u_i) \tag{109}
\]

for any \( k \in Z_i \), where (109) follows from the worst additive noise Lemma [19], and \( I(u_i; z_i|y_{k,i}) = 0 \) for any \( k \notin Z_i \).

Thus, for each \( i = 1, \ldots, M \) we have

\[
\sum_{k=1}^{K} \left[ \alpha_k I(x_i; y_{k,i}|u_i, z_i) + \beta_k I(u_i; z_i|y_{k,i}) \right]
\]

\[
\leq \sum_{k \in Y_i} \alpha_k \left[ h(y_{k,i}|u_i) - h(z_i|u_i) - \frac{1}{2} \log \left( \frac{\sigma_{k,i}^2}{\delta_i^2} \right) \right] + \sum_{k \in Z_i} \beta_k \left[ \frac{1}{2} \log \left( \frac{P_i + \sigma_{k,i}^2}{P_i + \sigma_{k,i}^2} \right) - h(z_i|u_i) + h(y_{k,i}|u_i) \right] \tag{110}
\]
We have the following lemma, which is the scalar version of the extremal inequality established in [17, Theorem 2].

**Lemma 1:** For any real scalars $\alpha_k, \beta_k, Q_i^*, M_{1,i}$ and $M_{2,i}$ that satisfy KKT conditions (86) and (90)–(93), we have

\[
\sum_{k \in Y_i} \alpha_k h(y_k,i; u_i) + \sum_{k \in Z_i} \beta_k h(y_k,i; u_i) - \left( \sum_{k \in Y_i} \alpha_k + \sum_{k \in Z_i} \beta_k \right) h(z_i|u_i) - \sum_{k \in Y_i} \frac{\alpha_k}{2} \log \left( \frac{Q_i^* + \sigma^2_{k,i}}{\delta^2_{i}} \right) - \sum_{k \in Z_i} \frac{\beta_k}{2} \log \left( \frac{P_i + \delta^2_{i}}{P_i + \sigma^2_{k,i}} \right) .
\]

(111)

for any $(u_i, x_i)$ that is independent of the additive Gaussian noise $(n_{1,i}, \ldots, n_{K,i}, w_i)$ and such that $E[x_i^2] \leq P_i$.

We note here that the extremal inequality in [17, Theorem 2] was established using a vector generalization of Costa's entropy-power inequality. The scalar version that we used here, however, can be directly established using the original Costa's entropy-power inequality [16]. Substituting (112) into (111) gives

\[
\sum_{k=1}^{K} [\alpha_k I(x_i; y_k,i|u_i, z_i) + \beta_k I(u_i; z_i|y_k,i)]
\leq \sum_{k \in Y_i} \frac{\alpha_k}{2} \log (Q_i^* + \sigma^2_{k,i}) + \sum_{k \in Z_i} \frac{\beta_k}{2} \log (Q_i^* + \sigma^2_{k,i}) - \sum_{k \in Y_i} \frac{\alpha_k}{2} \log \left( \frac{\sigma^2_{k,i}}{\delta^2_{i}} \right) + \sum_{k \in Z_i} \frac{\beta_k}{2} \log \left( \frac{P_i + \sigma^2_{k,i}}{P_i + \delta^2_{i}} \right) .
\]

(113)

Further substituting (115) into (103) completes the proof of (100). We have thus completed the proof of Theorem 2.

### VI. Fading Channels

To establish the connection to fading channels, first observe that Theorem 2 and Corollary 1 can be extended in the following way.

**Corollary 2:** For the Gaussian parallel-channel in Theorem 2, suppose that at each time, each of the sub-channels is selected with a probability of $p_i$. The capacity region consists of all rate pairs $(R_1, R_2)$ that satisfy

\[
R_1 \leq \min_{1 \leq k \leq K} \sum_{i=1}^{M} p_i \left[ \frac{1}{2} \log \left( \frac{Q_i + \sigma^2_{k,i}}{\sigma^2_{k,i}} \right) - \frac{1}{2} \log \left( \frac{Q_i + \delta^2_{i}}{\delta^2_{i}} \right) \right] +
\]

(116)

\[
R_2 \leq \min_{1 \leq k \leq K} \sum_{i=1}^{M} p_i \left[ \frac{1}{2} \log \left( \frac{P_i + \sigma^2_{k,i}}{Q_i + \sigma^2_{k,i}} \right) - \frac{1}{2} \log \left( \frac{P_i + \delta^2_{i}}{Q_i + \delta^2_{i}} \right) \right] +
\]

(117)

for some $0 \leq Q_i \leq P_i$ and $i = 1, \ldots, M$.

Clearly if the fading coefficients in (17) are all discrete-valued, then the result in Theorem 3 follows immediately from Corollary 2. When the fading coefficients are continuous valued, we can generalize Theorem 2 by suitably quantizing the channel gains.

First without loss of generality, we assume that each fading coefficient is real-valued, since each receiver can cancel out the phase of the fading gain through a suitable multiplication at the receiver. Consider a discrete set:

\[
A := \{ A_1, A_2, \ldots, A_N, A_{N+1} \}
\]

where $A_i \leq A_{i+1}$, $A_1 := 0$, $A_N := \infty$, and $A_{N+1} := \infty$. Given a set of channel gains $(h_1(i), \ldots, h_K(i), g(i))$ in coherence block $i$, we discretize them to one of $(N + 1)^K$ states as described below:

- **Encoding message $m_1$:** Suppose that the channel gain of receiver $k$ satisfies $A_0 \leq h_k(i) \leq A_{N+1}$, then we assume that the channel gain equals $\tilde{s}_{k,i} = A_0$. If the channel gain of the group $2$ user satisfies $A_0 \leq g(i) \leq A_{N+1}$ then we assume that its channel gain equals $\tilde{s}_{k,i+1} = A_0$.

- **Encoding message $m_2$:** Suppose that the channel gain of the group $2$ user satisfies $A_0 \leq g(i) \leq A_{N+1}$, then we assume that the channel gain equals $\tilde{s}_{k,i+1} = A_0$. If the channel gain of a group $1$ receiver satisfies $A_0 \leq h_k(i) \leq A_{N+1}$ then we assume it equals $\tilde{s}_{k,i} = A_0$.

Thus the channel gains in coherence block are mapped to one of $L = (N + 1)^{K-1}$ states $\{ s_j \}_{j=1}^{L}$. We denote the channel gains of the associated receivers in state $s_j$ as $(\tilde{s}_{j,1}, \ldots, \tilde{s}_{j,K}, \tilde{s}_{j,K+1})$ and the channel gains of the associated eavesdroppers as $\{ \tilde{s}_{j,1}, \ldots, \tilde{s}_{j,K+1} \}$. Note that in our notation, the $K$ receivers in group $1$ are labeled $\{ 1, \ldots, K \}$ while the group $2$ receiver is labeled $(K + 1)$.

Our coding scheme can be extended to show that any rate-pair that satisfies the following is achievable:

\[
R_1 \leq \min_{1 \leq k \leq K} \sum_{j=1}^{L} \Pr(s_j) A_{1,i,k}(s_j)
\]

(118)

\[
R_2 \leq \min_{1 \leq k \leq K} \sum_{j=1}^{L} \Pr(s_j) A_{2,i,k}(s_j)
\]

(119)
Fig. 2: Achievable rates (nats/symbol) for the two groups at different SNR values. The x-axis shows the rate $R_1$ for group 1 whereas the y-axis shows the rate $R_2$ for group 2.

where

$$A_{j,k}^{(1)}(s_j) := \left\{ \log \frac{1 + Q(s_j)|s_{j,k}|^2}{1 + Q(s_j)|s_{j,K+1}|^2} \right\}^+$$  \hspace{1cm} (120)$$

$$A_{j,k}^{(2)}(s_j) := \left\{ \log \frac{1 + P(s_j)|s_{j,K+1}|^2}{1 + Q(s_j)|s_{j,K}|^2} - \log \frac{1 + P(s_j)|s_{j,K}|^2}{1 + Q(s_j)|s_{j,k}|^2} \right\}^+.$$  \hspace{1cm} (121)$$

For any $J$, taking the limit $N \to \infty$ we have that

$$\sum_{j=1}^{L} \Pr(s_j)A_{j,k}^{(1)}(h,g) \to \int_0^J \int_0^J A_{k}^{(1)}(h,g)dF(g)dF(h)$$

$$= \int_0^J \int_0^\infty A_{k}^{(1)}(h,g)dF(g)dF(h)$$  \hspace{1cm} (122)$$

and (123) follows from the fact that $A_{k}^{(1)}(\cdot) = 0$ for $s_{K+1} > J$. Finally, by taking $J$ arbitrarily large, the right hand side in (118) approaches

$$R_1 \leq \min_{1 \leq k \leq K} \int_0^\infty \int_0^\infty A_{k}^{(1)}(h,g)dF(g)dF(h)$$  \hspace{1cm} (123)$$

as required. In a similar fashion the achievability of $R_2$ can be established.

The converse follows by noticing that the converse argument in Theorem 1 and Theorem 2 can also be extended to continuous valued fading coefficients.

A. Numerical Results

In order to evaluate the achievable rate region, we assume that the fading gains are all sampled from $CN(0,1)$. Furthermore instead of finding the optimal power allocation we assume a potentially sub-optimal power allocation:

$$Q(h, g) = \begin{cases} P, & |g|^2 \geq \theta \\ 0, & |g|^2 < \theta. \end{cases}$$  \hspace{1cm} (125)$$

where $\theta$ is a certain fixed parameter and assume that $P(h, g) = P$ for all values of $(h, g)$. Notice that our power allocation does not depend on the channel gains of the receivers in group 1. This is a reasonable simplification when $K$ is large and the channel gains $(h_1, \ldots, h_K)$ are identically distributed. The achievable rate expressions (19) and (20) reduce to:

$$R_1 \leq \Pr(|g|^2 \leq \theta)E \left[ \log \frac{1 + P|h|^2}{1 + P|g|^2} \right] |g|^2 \leq \theta$$  \hspace{1cm} (126)$$

$$R_2 \leq \Pr(|g|^2 \geq \theta)E \left[ \log \frac{1 + P|g|^2}{1 + P|h|^2} \right] |g|^2 \geq \theta.$$  \hspace{1cm} (127)$$

In Fig. 2, we plot the achievable rates for $P \in \{2, 10, 100\}$. We make the following observations:

- The corner points for $R_1$ and $R_2$ are obtained by setting $\theta = \infty$ and $\theta = 0$ respectively. By symmetry of the rate-expressions in (126) and (127), it is clear that both the corner points evaluate to the same numerical constant.

- As we approach the corner point $(0, R_2)$ the boundary of the capacity region is nearly flat. Any coherence block, where $|g(i)| \leq \max_{1 \leq k \leq K} |h_k(i)|$ is clearly not useful to the group 2 receiver. By transmitting $m_2$ in these slots one can increase the rate $R_1$ without decreasing $R_2$.

- As we approach the corner point $(R_1, 0)$, the boundary of the capacity region is nearly vertical. The argument is very similar to the previous case. In any period where $|g(i)| \geq \max_{1 \leq k \leq K} |h_k(i)|$ one cannot transmit to group 1. By transmitting $m_2$ in these slots we increase $R_2$ without decreasing $R_1$.

- We observe that a natural alternative to the proposed scheme is time-sharing. The rate achieved by such a scheme corresponds to a straight line connecting the corner points. The rate-loss associated with such a scheme is significant compared to the proposed scheme.

VII. Conclusion

We establish the optimality of a superposition construction for private broadcasting of two messages to two groups of receivers over independent parallel channels, when there are an arbitrary number of receivers in group 1 but there is only one receiver in group 2. We observe that in the optimal construction the codewords of group 2 constitute the “cloud-centers” whereas the codewords of group 1 constitute “satellite codebooks”. The optimality of such a layering solution is somewhat unexpected, because in absence of secrecy constraints the problem remains open, to the best of our knowledge. For the case of Gaussian sub-channels the optimality of Gaussian codebooks is established. This is accomplished by obtaining a Lagrangian dual for each point on the boundary of the capacity region and then using an extremal inequality to show that the resulting expression is maximized using a Gaussian input distribution. An extension to block-fading channels is also discussed. Numerical results for Rayleigh-fading channels
indicate that the proposed scheme can provide significant performance gains over naive time-sharing techniques.

REFERENCES


