On the Compound MIMO Broadcast Channels with Confidential Messages

Mari Kobayashi
SUPELEC
Gif-sur-Yvette, France

Yingbin Liang
University of Hawaii
Honolulu, HI, USA

Shlomo Shamai (Shitz)
Technion-Israel Institute of Technology
Haifa, Israel

Mérouane Debbah
SUPELEC
Gif-sur-Yvette, France

***Abstract*— We study the compound multi-input multi-output (MIMO) broadcast channel with confidential messages (BCC), where one transmitter sends a common message to two receivers and two confidential messages respectively to each receiver. The channel state may take one of a finite set of states, and the transmitter knows the state set but does not know the realization of the state. We study achievable rates with perfect secrecy in the high SNR regime by characterizing an achievable secrecy degree of freedom (s.d.o.f.) region for two models, the Gaussian MIMO-BCC and the ergodic fading multi-input single-output (MISO)-BCC without a common message. We show that by exploiting an additional temporal dimension due to state variation in the ergodic fading model, the achievable s.d.o.f. region can be significantly improved compared to the Gaussian model with a constant state, although at the price of a larger delay.**

I. Introduction

In most practical scenarios, perfect channel state information at transmitter (CSIT) may not be available due to time-varying nature of wireless channels (in particular for fast fading channels) and limited resources for channel estimation. However, many wireless applications must guarantee secure and reliable communication in the presence of the channel uncertainty. In this paper, we consider such a scenario in the context of the multi-input multi-output (MIMO) broadcast channel, in which a transmitter equipped with multi-antennas wishes to send one common message to two receivers and two confidential messages respectively to the two receivers. The channel uncertainty at the transmitter is modeled as a compound channel, i.e., the channel to two receivers may take one state from a finite set of states. The transmitter knows the state set, but does not know the realization of the channel state. The transmitter needs to send all messages reliably while keeping each confidential message perfectly secret from the non-intended receiver, no matter which channel state occurs.

We note that the compound MIMO broadcast channel with confidential messages (BCC) is not yet fully understood. This can be expected from two special cases studied in [1] and [2]. One the one hand, it is well known that without secrecy constraints the capacity region of the MIMO-BC under general CSIT is unknown. Moreover, even the d.o.f. region of the compound MIMO-BC is not fully known despite the recent progress [1]. On the other hand, although the secrecy capacity region of the two-user MISO-BCC has recently been characterized [2], the secrecy capacity of a general MIMO-BCC remains open.

In this paper, we study achievable secrecy degree of freedom (s.d.o.f.) regions of the MIMO-BCC, which characterize the behavior of an achievable secrecy rate region in the high signal-to-noise (SNR) regime. We consider two compound MIMO-BCC models. The first model is the Gaussian compound MIMO-BCC, in which the channel remains in the same state during the entire transmission. We assume that each terminal is equipped with multiple antennas and the transmitter sends one common message as well as two confidential messages to two receivers. We propose a beamforming scheme to obtain an achievable s.d.o.f., and characterize the impact of the number of antennas and the number of channel states on this region. We show that with M transmit antennas, N_k receive antennas and J_k states for $k = 1, 2$, a positive s.d.o.f. is ensured to both receivers only if the number of transmit antennas is sufficiently large, i.e. $M > \max(J_1N_1, J_2N_2)$.

The second model we study is the ergodic fading compound multi-input single-output (MISO)-BCC, where the channel remains in one state for a block duration and then changes independently from one block to another. We model the channel state at each block as a set of random variables uniformly distributed over a finite set. Applying the variable-rate transmission strategy proposed for the ergodic fading wiretap channel with partial CSIT [3], we characterize an achievable s.d.o.f. region. It is shown that time variation of the channel (which introduces an additional temporal dimension) enables to improve the s.d.o.f. region compared to the Gaussian model with constant channel state, although the second model applies only to delay-tolerant applications.

We note that the compound MIMO-BCC yields a number of previously studied models as special cases. For the special case of perfect CSIT, the secrecy capacity region of the two-user MISO-BCC has been recently characterized in [2]. A more general two-user MIMO-BCC is considered in [4], where the secrecy capacity region of the MIMO-BCC with one common message and one confidential message is characterized. For the frequency-selective BCC modeled as a special Toeplitz structure of the MIMO-BCC, the s.d.o.f. region is analyzed in [5]. All above studies do not address the compound nature of the channel. For the special case of only one confidential message, the capacity of the degraded MIMO compound wiretap channel is characterized and an achievable s.d.o.f. of the MIMO compound wiretap channel is derived in [6]. The s.d.o.f. of the compound wiretap parallel channels is considered in [7], [8].

The paper is organized as follows. In Sections II and III, we study the Gaussian MIMO-BCC and the ergodic fading MISO-BCC, respectively. Section IV concludes the paper.

In this paper, we adopt the following notations. We let $[x]_+ = \max\{0, x\}$ and $C(x) = \log(1+x)$. We use $\mathbf{x}^n$ to denote the sequence $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$, and use $u, v, w, \mathbf{x}, \mathbf{y}$ to denote the realization of the random variables U, V, W, X, Y. We use $|\mathbf{A}|, \mathbf{A}^H, \mathrm{tr}(\mathbf{A})$ to denote the determinant, the hermitian transpose, and the trace of a matrix $\mathbf{A}$, respectively.

II. Gaussian compound MIMO-BCC

A. Model and Definitions

We consider the MIMO-BCC, where the transmitter sends the confidential messages W_1, W_2 to receivers 1 and 2 as well as a common message W_0 to both receivers. The transmitter, and receivers 1 and 2 are equipped with M, N_1, N_2 antennas, respectively. The transmitter knows a discrete set of possible channel states, and each receiver has perfect CSI. The channel output of receiver k in state j at each channel use is given by

$$\mathbf{y}_{k,j} \quad = \quad \mathbf{H}_k^j \mathbf{x} + \boldsymbol{\nu}_k^j, \;\; j = 1, \ldots, J_k, \; k = 1, 2 \qquad (1)$$

where J_k denotes the number of possible channel states of receiver k, $\mathbf{H}_k^j \in \mathbb{C}^{N_k \times M}$ is the channel matrix of user k in state j, $\boldsymbol{\nu}_k^j \sim \mathcal{N}_{\mathbb{C}}(\mathbf{0}, \mathbf{I})$ is an additive white Gaussian noise (AWGN) and is independent and identically distributed (i.i.d.) over k and j, and the covariance $\mathbf{S}_x$ of the input vector $\mathbf{x}$ satisfies the power constraint $\mathrm{tr}(\mathbf{S}_x) \le P$. For the channel matrices, we have the following assumption.

Assumption 2.1: Any M rows taken from the matrices $\mathbf{H}_1^1, \ldots, \mathbf{H}_1^{J_1}, \mathbf{H}_2^1, \ldots, \mathbf{H}_2^{J_2}$ has rank M.

Definition 1: A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ block code for the Gaussian compound MIMO-BCC consists of following:

- Three message sets : $\mathcal{W}_i = \{1, \ldots, 2^{nR_i}\}$ and W_i is uniformly distributed over $\mathcal{W}_i$ for $i = 0, 1, 2$.
- A stochastic encoder that maps a message set $(w_0, w_1, w_2) \in (\mathcal{W}_0, \mathcal{W}_1, \mathcal{W}_2)$ into a codeword $\mathbf{x}^n$.
- Two decoders : decoder k maps a received sequence $\mathbf{y}_{k,j}^n$ into $(\hat{w}_0^{(k,j)}, \hat{w}_k{}^{(j)}) \in (\mathcal{W}_0, \mathcal{W}_k)$ for $j = 1, \ldots, J_k$ and $k = 1, 2$.

A rate tuple (R_0, R_1, R_2) is *achievable* if for any $\epsilon > 0$, there exists a $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ block code such that the average error probability of receivers 1 and 2 at state (j, l) satisfy

$$P_{e,1,j}^{(n)} \le \epsilon, \;\; P_{e,2,l}^{(n)} \le \epsilon,$$

and

$$nR_1 - H(W_1 | Y_{2,l}^n) \le n\epsilon, \;\; nR_2 - H(W_2 | Y_{1,j}^n) \le n\epsilon \qquad (2)$$

for any $j = 1, \ldots, J_1, l = 1, \ldots, J_2$. Note that (2) requires perfect secrecy for the confidential messages at the non-intended receiver.

We further define the degree of freedom (d.o.f.) of the common message and the secrecy degree of freedom of the confidential messages as

$$r_0 = \lim_{P \to \infty} \frac{R_0(P)}{\log(P)}, \quad r_k = \lim_{P \to \infty} \frac{R_k(P)}{\log(P)}, \; k = 1, 2.$$

B. Secrecy Degree of Freedom Region

An achievable secrecy rate region for the discrete memoryless broadcast channel with one common and two confidential messages was given in [9]. We can extend this result to the corresponding compound channel studied in this paper and obtain an achievable secrecy rate region given by

$$\begin{aligned} 0 &\le R_0 \le \min_{k,j} I(U; Y_{k,j}) \qquad (3)\\ 0 &\le R_1 \le \min_{j,l} [I(V_1; Y_{1,j}|U) - I(V_1; Y_{2,l}, V_2|U)]\\ 0 &\le R_2 \le \min_{j,l} [I(V_2; Y_{2,l}|U) - I(V_2; Y_{1,j}, V_1|U)] \end{aligned}$$

over all possible joint distributions of (U, V_1, V_2, X) satisfying

$$U \to (V_1, V_2) \to X \to (Y_{1,j}, Y_{2,l}), \forall j, l. \qquad (4)$$

Based on the preceding region, we obtain the following theorem on an achievable s.d.o.f. region..

Theorem 1: Consider the Gaussian compound MIMO-BCC with M transmit antennas, N_k receive antennas and J_k channel states at receiver k for $k = 1, 2$. If $J_1 N_1 < M$ and $J_2 N_2 < M$, an achievable s.d.o.f. region is a union of (r_0, r_1, r_2) that satisfies

$$\begin{aligned} r_1 &\le \min(N_1, M - J_2 N_2)\\ r_2 &\le \min(N_2, M - J_1 N_1)\\ r_0 + r_1 &\le N_1\\ r_0 + r_2 &\le N_2 \qquad (5) \end{aligned}$$

Proof: (Outline) We apply a simple linear beamforming strategy to provide an achievable s.d.o.f. region. We first prove a useful lemma.

Lemma 1: For $0 \le r_1 \le \min(N_1, M - J_2 N_2)$ and $0 \le r_2 \le \min(N_2, M - J_1 N_1)$, there exist $\mathbf{v}_k^1, \ldots, \mathbf{v}_k^{r_k}$ for $k = 1, 2$, each with dimension M that form a matrix $\mathbf{V}_k = [\mathbf{v}_k^1 \cdots \mathbf{v}_k^{r_k}]$, such that

$$\mathbf{H}_k^j \mathbf{V}_{k'} = 0 \quad \text{for } k' \neq k, \quad j = 1, \ldots, J_k \qquad (6)$$

and $\mathrm{rank}(\mathbf{H}_k^j \mathbf{V}_k) = r_k$ for $j = 1, \ldots, J_k$.

The proof of Lemma 1 is omitted due to space limitations. Based on $\mathbf{V}_1$ and $\mathbf{V}_2$ given in Lemma 1, for the given $0 \le r_1 \le \min(N_1, M - J_2 N_2)$ and $0 \le r_2 \le \min(N_2, M - J_1 N_1)$, we let $\mathbf{v}_0^1, \ldots, \mathbf{v}_0^K$ be orthnormal vectors in the null space of $[\mathbf{V}_1, \mathbf{V}_2]$, where $K = M - \mathrm{rank}[\mathbf{V}_1 \mathbf{V}_2]$. Hence, if we let $\mathbf{V}_0 = [\mathbf{v}_0^1, \ldots, \mathbf{v}_0^K]$, then $\mathbf{V}_0^H [\mathbf{V}_1, \mathbf{V}_2] = \mathbf{0}$.

We form the transmit vector at each channel use by Gaussian superposition coding

$$\mathbf{x} = \mathbf{V}_0 \mathbf{u}_0 + \mathbf{V}_1 \mathbf{u}_1 + \mathbf{V}_2 \mathbf{u}_2 \qquad (7)$$

where $\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2$ are mutually independent with i.i.d. entries $u_{k,i} \sim \mathcal{N}_{\mathbb{C}}(0, p_{k,i})$ for any k, i with $u_{k,i}$ denoting the i-th element of $\mathbf{u}_k$.

From (6), the received signals are given by

$$\mathbf{y}_1^j = \mathbf{H}_1^j(\mathbf{V}_0\mathbf{u}_0 + \mathbf{V}_1\mathbf{u}_1) + \mathbf{n}_1^j, \ \ j = 1, \ldots, J_1 \quad (8)$$
$$\mathbf{y}_2^l = \mathbf{H}_2^l(\mathbf{V}_0\mathbf{u}_0 + \mathbf{V}_2\mathbf{u}_2) + \mathbf{n}_2^l, \ \ l = 1, \ldots, J_2 \quad (9)$$

By letting $U = \mathbf{V}_0\mathbf{u}_0$, $V_k = U + \mathbf{V}_k\mathbf{u}_k$, $X = V_1 + V_2$, we obtain

$$I(U; Y_{k,j}) = \log \frac{|\mathbf{I} + \mathbf{H}_k^j(\mathbf{V}_0\text{diag}(\mathbf{p}_0)\mathbf{V}_0^H + \mathbf{V}_k\text{diag}(\mathbf{p}_k)\mathbf{V}_k^H)\mathbf{H}_k^{j\,H}|}{|\mathbf{I} + \mathbf{H}_k^j\mathbf{V}_k\text{diag}(\mathbf{p}_k)\mathbf{V}_k^H\mathbf{H}_k^{j\,H}|} \quad (10)$$

$$I(V_k; Y_{k,j}|U) = \log |\mathbf{I} + \mathbf{H}_k^j\mathbf{V}_k\text{diag}(\mathbf{p}_k)\mathbf{V}_k^H\mathbf{H}_k^{j\,H}| \quad (11)$$

In order to find the s.d.o.f., we consider equal power allocation over all beamforming directions. we first notice that the pre-log factor of $\log |\mathbf{I} + P\mathbf{A}|$ is determined by rank$(\mathbf{A})$ as $P \to \infty$.

From Lemma 1, we obtain

$$\text{rank}(\mathbf{H}_1^j\mathbf{V}_1\mathbf{V}_1^H\mathbf{H}_1^{j\,H}) = \text{rank}(\mathbf{H}_1^j\mathbf{V}_1) = r_1$$
$$\text{rank}(\mathbf{H}_2^j\mathbf{V}_2\mathbf{V}_2^H\mathbf{H}_2^{j\,H}) = r_2.$$

We then obtain

$$r_0 = \text{rank}\left(\mathbf{H}_1^j(\mathbf{V}_0\mathbf{V}_0^H + \mathbf{V}_1\mathbf{V}_1^H)\mathbf{H}_1^{j\,H}\right) - \text{rank}(\mathbf{H}_1^j\mathbf{V}_1\mathbf{V}_1^H\mathbf{H}_1^{j\,H})$$
$$= N_1 - r_1$$

and similarly, $r_0 = N_2 - r_2$, which concludes the proof. ■

By using the beamforming scheme similar to that for Theorem 1, we obtain the following corollaries.

Corollary 2.1: For the Gaussian compound MIMO-BCC with $J_1N_1 < M$ and $J_2N_2 \geq M$, an achievable s.d.o.f. region includes (r_0, r_1, r_2) that satisfies $r_1 = 0$, $r_2 \leq \min(N_2, M - J_1N_1)$, and $r_0 \leq \min(N_1, N_2 - r_2)$.

Corollary 2.2: For the Gaussian compound MIMO-BCC with $J_1N_1 \geq M$ and $J_2N_2 \geq M$, an achievable s.d.o.f. region includes $(r_0, 0, 0)$ with r_0 satisfying $r_0 \leq \min(M, N_1, N_2)$.

To gain insight into these results, we consider some special cases. For the case of perfect CSIT ($J_1 = J_2 = 1$), the optimal strategy in the high SNR regime is to transmit the confidential message k in the null space of the channel matrix of the other k'. This yields the s.d.o.f. $r_1 \leq \min(N_1, M - N_2), r_2 \leq \min(N_2, M - N_1)$ for $M > \max(N_1, N_2)$. Clearly, the s.d.o.f. of user k corresponds to the s.d.o.f. of the MIMO wiretap channel [10] where the transmitter sends one confidential message to receiver k in the presence of an eavesdropper (user $k' \neq k$). In addition, Theorem 1 states that if $J_1 = J_2 = 1$ and the total number of receive antennas is large, i.e., $N_1 + N_2 > M$, we can achieve the sum d.o.f. M. This is certainly optimal since the MIMO-BC achieves the sum d.o.f. of $\min(M, N_1 + N_2) = M$.

For the case with a single receive antenna at each receiver, i.e., $N_1 = N_2 = 1$, and without common message, i.e., $r_0 = 0$, we have $r_1 \leq \min(1, M - J_2)$ and $r_2 \leq \min(1, M - J_1)$. This result can be compared to the d.o.f. of the compound MIMO-BC [1]. A positive s.d.o.f. tuple $(1, 1)$ is achievable if $J_1 < M$ and $J_2 < M$. If the channel uncertainty of one user increases, for example, $J_2 = M$, the s.d.o.f. of user 1 collapses. Moreover, the s.d.o.f. of both users becomes zero if $J_1 \geq M, J_2 \geq M$. We remark that secrecy constraints significantly reduce d.o.f. and sometimes may yield pessimistic results with respect to [1].

III. Ergodic Fading Compound MISO-BCC

A. Model and Definitions

We consider the MISO-BCC, where the transmitter with M antennas sends the confidential messages W_1, W_2 respectively to two receivers, each equipped with single antenna. We consider the ergodic block fading model, in which the channel remains in one state for a block of T channel uses and changes to another channel state independently from one block to another. We assume that the fading process is stationary and ergodic over time. Hence, the channel state at block t is given by the set of random variables $(A_1[t], A_2[t], H[t]) \in \mathcal{A}$, where $\mathcal{A} = \{1, \ldots, J_1\} \times \{1, \ldots, J_2\} \times \{1, \ldots, N\}$ denotes the space of fading states and each random variable is uniformly distributed over its set. Under non-perfect CSIT, the transmitter is assumed to know $H[t]$ and J_1J_2 possible states at block t but not the realization of $A_1[t]$ and $A_2[t]$, and receiver k is assumed to know both $H[t]$ and $A_k[t]$. At each block t, the channel of user k is expressed by two random vectors $\mathbf{h}_k^{A_k[t]}[H[t]]$, for which we denote $\mathbf{h}_k^{A_k[t]}[t]$ for the notational simplicity. Finally, we assume that for each t, any M vectors taken from $\{\mathbf{h}_1^1[t], \ldots, \mathbf{h}_1^{J_1}[t], \mathbf{h}_2^1[t], \ldots, \mathbf{h}_2^{J_2}[t]\}$ has rank M.

For each channel use at block t, the ergodic fading compound MISO-BCC is expressed by

$$y_k[t] = \mathbf{h}_k^j[t]^H\mathbf{x}[t] + \nu_k[t], \ \text{w.p.}\ P(A_k[t] = j|H[t]) = \tfrac{1}{J_K}, \forall j$$

for $k = 1, 2$ and $t = 1, \ldots, m$, where w.p. denotes with probability, $\nu_k[t] \sim \mathcal{N}_{\mathbb{C}}(0, 1)$ is an AWGN and i.i.d. over k, t, and the input covariance $\mathbf{S}_x[t]$ of $\mathbf{x}[t]$ satisfies the long-term power constraint $\frac{1}{m}\sum_{t=1}^m \text{tr}(\mathbf{S}_x[t]) \leq P$. We let $n = mT$ denote the total number of symbols over m blocks. The definition for the s.d.o.f. is the same as that in Section II-A.

B. Variable-Rate Transmission

We first note that as $m \to \infty, T \to \infty$, the *ergodic* achievable secrecy rate region is given by the union of all (R_1, R_2) such that [2],

$$0 \leq R_1 \leq \mathbb{E}[I(V_1; Y_1)] - \mathbb{E}[I(V_1; Y_2, V_2)]$$
$$0 \leq R_2 \leq \mathbb{E}[I(V_2; Y_2)] - \mathbb{E}[I(V_2; Y_1, V_1)] \quad (12)$$

where the expectation is with regard to the fading space $\mathcal{A}$ and the union is over all possible distributions V_1, V_2, X satisfying

$$(V_1, V_2) \to X \to (Y_1, Y_2). \quad (13)$$

It can be seen that the ergodic secrecy rate of user k can be expressed by

$$R_k \leq \mathbb{E}[I(V_k; Y_k)] - \mathbb{E}[I(V_k; V_{k'})] - \mathbb{E}[I(V_k; Y_{k'}|V_{k'})] \quad (14)$$

where the first two terms can be interpreted as the ergodic Marton broadcast rate without secrecy constraint, and the last term $\mathbb{E}[I(V_k; Y_{k'}|V_{k'})]$ represents the information accumulated at the non-intended receiver k'.

We next adapt the variable-rate transmission proposed in [3, Theorem 2] to the compound MISO-BCC. We focus on the zero-forcing beamforming to provide an achievable s.d.o.f. region. At each channel use of block t, the transmitter forms the codeword

$$\mathbf{x}[t] = \mathbf{x}_1[t] + \mathbf{x}_2[t] = \mathbf{v}_1[t]u_1[t] + \mathbf{v}_2[t]u_2[t] \qquad (15)$$

where $\mathbf{v}_k[t]$ denotes a unit-norm beamforming vector of user k (to be specified below) and $u_k[t] \sim \mathcal{N}_{\mathbb{C}}(0, p_k[t])$ is symbol of user k, and $u_1[t], u_2[t]$ are mutually independent. Clearly, the Markov chain (13) is satisfied by letting $V_k = \mathbf{v}_k[t]u_k[t]$ and $X = V_1 + V_2$ at each t. Following [3], we assume that the transmitter sends the codeword $\mathbf{x}_k[t]$ to user k at rate given by

$$\begin{aligned} R_{k,\mathrm{tx}}[t] &= I(u_k[t]; y_k[t]) - I(u_k[t]; u_{k'}[t]) \qquad (16)\\ &\overset{(a)}{=} I(u_k[t]; y_k[t]) \\ &= \sum_{j=1}^{J_k} P(A_k[t] = j | H[t]) I(u_k[t]; y_k[t] | A_k[t] = j) \end{aligned}$$

where (a) follows from the independency between $u_1[t]$ and $u_2[t]$. This variable-rate strategy enables to limit the leaked information at the non-intended receiver k' at each block t such that

$$\begin{aligned} & I(u_k[t]; y_{k'}[t] | u_{k'}[t]) \\ &= \sum_{j=1}^{J_{k'}} P(A_{k'}[t] = j | H[t]) I(u_k[t]; y_{k'}[t] | u_{k'}[t], A_{k'}[t] = j) \\ &\leq R_{k,\mathrm{tx}}[t] \qquad (17) \end{aligned}$$

for $k' \neq k$ and $k = 1, 2$. By combining (16) and (17), the averaged secrecy rate of user k over m blocks is given by

$$\begin{aligned} R_k^m &= \frac{1}{m}\sum_{t=1}^{m} R_{k,\mathrm{tx}}[t] - \frac{1}{m}\sum_{t=1}^{m} I(u_k[t]; y_{k'}[t] | u_{k'}[t]) \\ &= \frac{1}{m}\sum_{t=1}^{m} R_k[t] \qquad (18) \end{aligned}$$

where the secrecy rate of user k at block t is given by

$$R_k[t] = [R_{k,\mathrm{tx}}[t] - I(u_k[t]; y_{k'}[t] | u_{k'}[t])]_+ \qquad (19)$$

We remark that similar to [3], the variable rate strategy avoids the non-intended receiver k' to accumulate the information on symbol k over m blocks, whenever the channel condition is better than the transmission rate of user k.

C. Secrecy Degree of Freedom Region

In the following, we provide the s.d.o.f. analysis for different cases of (J_1, J_2).

Theorem 2: The two-user ergodic fading compound MISO-BCC with $J_1 < M, J_2 < M$ achieves the s.d.o.f. region

$$\{(r_1, r_2) : r_1 \leq 1, r_2 \leq 1\}.$$

Proof: At each block t, the transmitter forms $\mathbf{x}[t]$ given in (15) by choosing $\mathbf{v}_1[t]$ orthogonal to $\mathbf{h}_2^1[t], \dots, \mathbf{h}_2^{J_2}[t]$ and $\mathbf{v}_2[t]$ orthogonal to $\mathbf{h}_1^1[t], \dots, \mathbf{h}_1^{J_1}[t]$. This yields the received signals for $k = 1, 2$ given by

$$y_k[t] = \phi_{k,k}^j[t]u_k[t] + \nu_k[t], \text{ w.p. } P(A_k[t] = j | H[t]) = \tfrac{1}{J_k}, \forall j$$

where $\phi_{k,i}^j[t] = \mathbf{h}_k^j[t]^H \mathbf{v}_i[t]$. It can be shown that $\mathbf{v}_1[t]$ and $\mathbf{v}_2[t]$ can be chosen such that $\phi_{k,k}^j[t] \neq 0$. Since the ZF creates two parallel channels for any pair $(A_1[t], A_2[t])$, the averaged secrecy rate of user k over m blocks is readily given by

$$R_k^m \leq \frac{1}{mJ_k}\sum_{t=1}^{m}\sum_{j=1}^{J_k} C(p_k[t]|\phi_{k,k}^j[t]|^2)$$

As $m \to \infty$, the corner point $(1, 0), (0, 1)$ is achieved by allocating $p_1[t] = P, \forall t$, $p_2[t] = P, \forall t$, respectively, and the rate point $(1, 1)$ is achieved by equal power allocation $p_1[t] = p_2[t] = P/2$ at each t. Time-sharing between three points yields the region. ■

Theorem 3: The two-user ergodic fading compound MISO-BCC with $J_1 < M, J_2 \geq M$ achieves the s.d.o.f. region (see Fig.1) that includes (r_1, r_2) satisfying

$$r_1 \leq \frac{M-1}{J_2}, \qquad \left(\frac{J_2}{M-1} - 1\right) r_1 + r_2 \leq 1 \qquad (20)$$

Proof: At each block t, the transmitter chooses $\mathbf{v}_1[t]$ orthogonal to the first $M-1$ states[1] $\mathbf{h}_2^1[t], \dots, \mathbf{h}_2^{M-1}[t]$ and $\mathbf{v}_2[t]$ orthogonal to $\mathbf{h}_1^1[t], \dots, \mathbf{h}_1^{J_1}[t]$ to form the codeword (15) at each t. This yields the receive signals

$$y_1[t] = \phi_{1,1}^j[t]u_1[t] + \nu_1[t], \quad \text{w.p. } P(A_1[t] = j | H[t]) = \tfrac{1}{J_1}, \forall j$$

$$y_2[t] = \begin{cases} \phi_{2,2}^j[t]u_2[t] + \nu_2[t], \\ \qquad \text{w.p. } P(A_2[t] = j | H[t]) = \frac{1}{J_2} \text{ for } j \leq M-1 \\ \phi_{2,1}^j[t]u_1[t] + \phi_{2,2}^j[t]u_2[t] + \nu_2[t] \\ \qquad \text{w.p. } P(A_2[t] = j | H[t]) = \frac{1}{J_2} \text{ for } M \leq j \leq J_2 \end{cases}$$

We remark that the increased channel uncertainty at user 2 $(J_2 \geq M)$ incurs two effects. First, it decreases the transmission rate of user 2 due to interference from user 1. Second, it decreases the secrecy rate of user 1 since user 2 observes $u_1[t]$ with probability $\frac{J_2-M+1}{J_2}$, if $A_k[t]$ is between M and J_2. We obtain the secrecy rates at block t given by

$$R_1[t] \leq \left[\frac{1}{J_1}\sum_{j=1}^{J_1} C(p_1[t]|\phi_{1,1}^j[t]|^2) - \frac{1}{J_2}\sum_{j=M}^{J_2} C(p_1[t]|\phi_{2,1}^j[t]|^2)\right]_+$$

$$R_2[t] \leq \frac{1}{J_2}\sum_{j=1}^{M-1} C(p_2[t]|\phi_{2,2}^j[t]|^2) + \frac{1}{J_2}\sum_{j=M}^{J_2} C\left(\frac{p_2[t]|\phi_{2,2}^j[t]|^2}{1 + p_1[t]|\phi_{2,1}^j[t]|^2}\right)$$

Plugging these expressions into (18) and letting $m \to \infty$, the corner point $(0, 1), (\frac{M-1}{J_2}, 0)$ is achieved by letting $p_2[t] = P$ and $p_1[t] = P$ for all t. Under equal power allocation $p_1[t] = p_2[t] = \frac{P}{2}$ for all t, $\left(\frac{M-1}{J_2}, \frac{M-1}{J_2}\right)$ is achieved. Time-sharing of these three points yields the region. ■

Theorem 4: Consider the two-user ergodic compound MISO-BCC with $J_1 \geq M, J_2 \geq M$. We define the function $f(J_1, J_2) = \frac{M-1}{J_1} + \frac{M-1}{J_2} - 1 - \frac{M-1}{J_1+J_2}$. If $f(J_1, J_2) \leq 0$, an achievable region is given by the time-sharing between $(\frac{M-1}{J_2}, 0)$ and $(0, \frac{M-1}{J_1})$. If $f(J_1, J_2) > 0$, an achievable

[1]The same result holds for any $M-1$ set taken from $\{\mathbf{h}_2^1[t], \dots, \mathbf{h}_2^{J_2}[t]\}$.

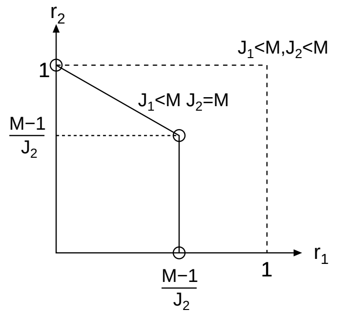

Fig. 1. s.d.o.f. region for $J_1, J_2 < M$ and $J_1 < M, J_2 \geq M$

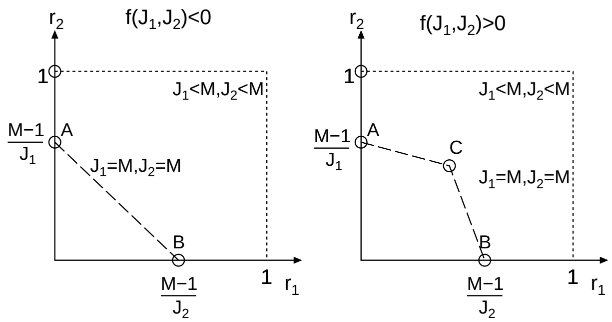

Fig. 2. s.d.o.f. region for $J_1 \geq M, J_2 \geq M$

region (see Fig.2) is time-sharing between these two points and (r_s, r_s) with $r_s = \frac{M-1}{J_1} + \frac{M-1}{J_2} - 1$.

Proof: Without loss of generality, the transmitter chooses $\mathbf{v}_1[t]$ orthogonal to $\mathbf{h}_2^1[t], \dots, \mathbf{h}_2^{M-1}[t]$ and $\mathbf{v}_2[t]$ orthogonal to $\mathbf{h}_1^1[t], \dots, \mathbf{h}_1^{M-1}[t]$ to form the codeword given in (15) at block t. This yields the receive signals

$$y_k[t] = \begin{cases} \phi_{k,k}^j[t] u_k[t] + \nu_k[t], \\ \qquad \text{w.p. } P(A_k[t] = j | H[t]) = \frac{1}{J_k} \text{ for } j \leq M-1 \\ \phi_{k,k}^j[t] u_k[t] + \phi_{k,k'}^j[t] u_{k'}[t] + \nu_k[t], \\ \qquad \text{w.p. } P(A_k[t] = j | H[t]) = \frac{1}{J_k} \text{ for } M \leq j \leq J_k \end{cases}$$

for $k = 1, 2$. By taking into account the two effects caused by the increased channel uncertainty mentioned above, we obtain the secrecy rate of user k at block t is given by

$$R_k[t] = \Bigg[\frac{1}{J_k} \sum_{j=1}^{M-1} C(p_k[t] |\phi_{k,k}^j[t]|^2) - \frac{1}{J_{k'}} \sum_{j=M}^{J_{k'}} C(p_k[t] |\phi_{k',k}^j[t]|^2) + \frac{1}{J_k} \sum_{j=M}^{J_k} C\left(\frac{p_k[t] |\phi_{k,k}^j[t]|^2}{1 + p_{k'}[t] |\phi_{k,k'}^j[t]|^2} \right) \Bigg]_+$$

for $k = 1, 2$. Plugging the above expression into (18) and letting $m \to \infty$, the corner point $A = \left(\frac{M-1}{J_2}, 0 \right), B = \left(0, \frac{M-1}{J_1} \right)$ is achieved by letting $p_1[t] = P, p_2[t] = P, \forall t$, respectively. Under equal power allocation $p_1[t] = p_2[t] = P/2, \forall t$, we have two different behaviors according to the value of $f(J_1, J_2)$. Interestingly, if $f(J_1, J_2) > 0$, the s.d.o.f. point $C = (r_s, r_s)$ which dominates the line segment A B is achieved, as shown in Fig.2. On the contrary, if $f(J_1, J_2) \leq 0$, the point (r_s, r_s) is below the line segment A B. This can be easily verified by comparing r_s and the intersection between the line segment A B and $r_2 = r_1$. ∎

We remark that an achievable s.d.o.f. with the ergodic model gradually decreases as the uncertainty increases. Moreover, the time variation of the channel state creates an additional temporal dimension, and significantly improves the s.d.o.f. with respect to the Gaussian model with constant channel state. We provide a simple example to illustrate the difference between two models. Consider the compound MISO-BCC with $M = 7, J_1 = J_2 = 8$. The ergodic model achieves $(1/2, 1/2)$ which dominates the time-sharing between the corner points $(3/4, 0)$ and $(0, 3/4)$. The Gaussian model yields zero s.d.o.f. for both users. This radical difference is because the number of channel states over which perfect secrecy must be kept for the Gaussian model equals the number of wiretappers, which is not the case for the ergodic model.

IV. Conclusions

We have studied the two-user compound MIMO-BCC, for which we have found that time variation of the channel state provides an additional temporal dimension for the ergodic model, which improves an achievable s.d.o.f. region compared to the Gaussian model with a constant fading state, although at the price of a larger delay. We note also that in contrast to the compound MIMO-BC [1], the gain by multiletter approaches (i.e. combining several time instances) is not expected here. Finally, we conjecture that an achievable s.d.o.f. region provided in the paper is indeed the s.d.o.f. region and the proof remains as a future investigation.

Acknowledgment

This work is partially supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications NEWCOM++.

References

[1] H. Weingarten, S. Shamai, and G. Kramer, “On the compound MIMO broadcast channel,” in *Proceedings of Annual Information Theory and Applications Workshop (ITA)*, San Diego, CA, 2007.

[2] R. Liu and H. V. Poor, “Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages,” *IEEE Trans. on Inform. Theory*, vol. 55, no. 3, pp. 1235–1249, March 2008.

[3] P. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. on Inform. Theory*, vol. 54, no. 10, October 2008.

[4] H. D. Ly, T. Liu, and Y. Liang, “MIMO Broadcasting with Common, Private, and Confidential Messages,” in *Proc. Inter. Symp. Inform. Theory and its App. (ISITA)*, New Zealand, December 2008.

[5] M. Kobayashi, M. Debbah, and S. Shamai (Shitz), “Secured communications over frequency-selective fading channels: A practical Vandermonde precoding,” *submitted to Eurasip, Special Issue on Wireless Physical Security, November 2008.*

[6] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), “Compound wire-tap channels,” in *Proc. 45th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, USA, 2007.

[7] ——, “Recent results on compound wire-tap channels,” in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Cannes, France, 2008.

[8] T. Liu, V. Prabhakaran, and S. Vishwanath, “The secrecy capacity of a class of parallel Gaussian compound wiretap channels,” in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, 2008, pp. 116–120.

[9] J. Xu, Y. Cao, and B. Chen, “Capacity Bounds for Broadcast Channels with Confidential Messages,” *submitted to ”IEEE Trans. on Inform. Theory”, May 2008, also available Arxiv preprint arXiv:0805.4374*, 2008.

[10] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, “On the Gaussian MIMO wiretap channel,” in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Nice, France, 2007.