MISO Broadcast Channels with Confidential Messages and Alternating CSIT

Pritam Mukherjee[1], Ravi Tandon[2], and Sennur Ulukus[1]

[1]Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742
[2]Hume Center and Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061

***Abstract*—We study the two-user multiple-input single-output (MISO) broadcast channel with confidential messages under the assumption of alternating channel state information at the transmitter (CSIT). We consider two alternating states: PD and DP which occur for an equal fraction of time. In state PD, the CSIT of the channel to the first receiver is available perfectly without delay (P) while that of the second receiver is available with a delay of one channel use (D); in state DP, the roles of the receivers are reversed. We characterize the exact secure degrees of freedom (s.d.o.f.) region of this system, and show as a corollary that the sum s.d.o.f. is $\frac{3}{2}$. We observe that this sum s.d.o.f. is the same as what can be achieved by the states PP and DD occurring for equal fraction of time. Though the s.d.o.f. of the system in the states PD and DP is not known individually, we are able to establish the s.d.o.f. region when the two states alternate and occur for an equal fraction of the time.**

I. Introduction

Wireless systems are particularly vulnerable to security attacks because of the inherent openness of the transmission medium. With the widespread adoption of multiple-input multiple-output (MIMO) systems, there has been a significant recent interest in information theoretic physical layer security, the main premise of which is to exploit the difference in the wireless channels of different users. Information theoretic security has been investigated for a variety of channel models ranging from fading channels [1], [2], MIMO wiretap channels [3]–[6], multiple access channels [7]–[9], multi-receiver wiretap channels [10], broadcast channels with confidential messages [11]–[13], wiretap channels with helpers [14], etc.

The focus of this paper is on the fading two-user multiple-input single-output (MISO) broadcast channel with confidential messages (BCCM), in which the transmitter (with two antennas) has two confidential messages, one for each of the single antenna users; Fig. 1. The secrecy capacity region of the MISO BCCM for the case of perfect CSI at all terminals has been characterized in [12], [13]. In practice, the CSIT may be delayed, imperfect or may not even be available at all. While the exact secrecy capacity is unknown for most of such cases, the secure degrees of freedom (s.d.o.f.) is known for several scenarios. For the two-user MISO BCCM, the sum s.d.o.f. is 2 with perfect and instantaneous CSIT [12]. With no CSIT, the sum s.d.o.f. is zero as the two users are statistically equivalent and hence no secrecy is possible. On the other hand, with completely outdated CSIT from both users, [15] has recently shown a surprising result that sum s.d.o.f. increases to 1.

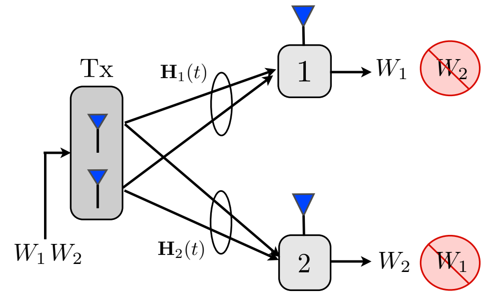

Fig. 1. MISO broadcast channel with confidential messages.

In practice, the nature of CSIT can vary across users. For instance, consider the heterogeneous setting in which user 1 supplies perfect and instantaneous (P) CSIT while user 2 supplies delayed (D) CSIT; in short, we denote this CSIT state as PD. In this setting, it is clear that a sum s.d.o.f. of 1 is achievable. This can be done by transmitting to only one user by using instantaneous channel knowledge from user 1. Alternatively, the sum s.d.o.f. of 1 can also be achieved by treating this PD state as DD [15], i.e., by ignoring the instantaneous CSI and using it only in a delayed manner. The optimal s.d.o.f. for the state PD (as well as the state DP by symmetry) remains an open problem.

We next argue that the nature of the channel knowledge may also vary over time (in addition to varying over users). This leads naturally to the setting of alternating CSIT in which multiple CSIT states, for instance, PD and DP, arise over time. The alternating CSIT framework was introduced in [16] where it was shown that synergistic gains are possible by jointly coding across these states. This motivates us to investigate whether such synergies can be harnessed for secrecy as well.

To this end, we consider the two-user MISO BCCM with alternating CSIT, in which the nature of CSIT alternates between two states: PD and DP, and each of these states occur for half of the total duration. The main contributions of this paper are summarized as follows: (a) We characterize the exact optimal s.d.o.f. region with alternating CSIT and show as a corollary that the exact sum s.d.o.f. is $\frac{3}{2}$. (b) We present a novel coding scheme which achieves this s.d.o.f. region by coding across multiple CSIT states and jointly utilizing disparate channel knowledge over time. Finally, it is worth

This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811, and L-3 Communications.

noting that while the optimal s.d.o.f. for the individual CSIT states PD and DP remain open, we are able to determine the exact s.d.o.f. for the alternating CSIT case. Further, if the best achievable sum s.d.o.f. of the PD (or, by symmetry, DP) state is indeed 1, then our results show that coding across the PD and DP states jointly provides synergistic benefits for secrecy.

II. Problem Statement

In the two-user MISO BCCM shown in Fig. 1, the received signals at time t are given as follows:

$$Y(t) = \mathbf{H}_1(t)\mathbf{X}(t) + N_1(t) \tag{1}$$

$$Z(t) = \mathbf{H}_2(t)\mathbf{X}(t) + N_2(t), \tag{2}$$

where $Y(t)$ and $Z(t)$ are the channel outputs of receivers 1 and 2, respectively. The 2×1 channel input $\mathbf{X}(t)$ is power constrained as $\mathbb{E}[||\mathbf{X}(t)||^2] \leq P$, and $N_1(t)$ and $N_2(t)$ are circularly symmetric complex white Gaussian noises with zero-mean and unit-variance. The 1×2 channel vectors $\mathbf{H}_1(t)$ and $\mathbf{H}_2(t)$ of receivers 1 and 2, respectively, are independent and identically distributed (i.i.d.) with continuous distributions, and are also i.i.d. over time. We denote $\mathbf{H}(t) = \{\mathbf{H}_1(t), \mathbf{H}_2(t)\}$ as the collective channel vectors at time t and $\mathbf{H}^n$ as the sequence of channel vectors up until and including time n.

The nature of CSIT *alternates* between the following two states which occur in equal fractions of time: 1) state $S(t) = \mathsf{PD}$, where the transmitter knows $\mathbf{H}_1(t)$ at time t but gets to know $\mathbf{H}_2(t)$ at time $t+1$; and 2) state $S(t) = \mathsf{DP}$, where the transmitter knows $\mathbf{H}_2(t)$ at time t but gets to know $\mathbf{H}_1(t)$ at time $t+1$. Thus, at any given instance of time, the transmitter knows the channel vector of one receiver perfectly and instantaneously, whereas it gets to know the channel vector of the other receiver with a unit delay.

A secure rate pair (R_1, R_2) is achievable if there exists a sequence of codes which satisfy the reliability constraints at the receivers, namely, $\Pr\left[W_i \neq \hat{W}_i\right] \leq \epsilon_n$, for $i = 1, 2$, and the secrecy constraints, namely,

$$\frac{1}{n} I(W_1; Z^n, \mathbf{H}^n) \leq \epsilon_n, \qquad \frac{1}{n} I(W_2; Y^n, \mathbf{H}^n) \leq \epsilon_n, \tag{3}$$

where $\epsilon_n \to 0$ as $n \to \infty$. A s.d.o.f. pair (d_1, d_2) is achievable, if there exists an achievable rate pair (R_1, R_2) such that

$$d_1 = \lim_{P\to\infty} \frac{R_1}{\log P}, \qquad d_2 = \lim_{P\to\infty} \frac{R_2}{\log P}. \tag{4}$$

III. Main Result and Discussion

Theorem 1 *The s.d.o.f. region of the two-user MISO BCCM with alternating CSIT of* PD *and* DP *is:*

$$3d_1 + d_2 \leq 3 \tag{5}$$

$$d_1 + 3d_2 \leq 3. \tag{6}$$

Fig. 2 shows the s.d.o.f. region stated in Theorem 1 together with the s.d.o.f. regions with perfect CSIT from both receivers [12] and delayed CSIT from both receivers [15].

The converse proof is presented in Section III-B. The novel aspect of the achievable scheme, which is presented in Section III-A, is that it uses a *single* artificial noise signal and optimally mixes it with the information bearing signals to guarantee the confidentiality for *both* users by leveraging alternating CSIT. To the best of our knowledge, this use of *single* noise for *dual* secrecy was unexplored previously.

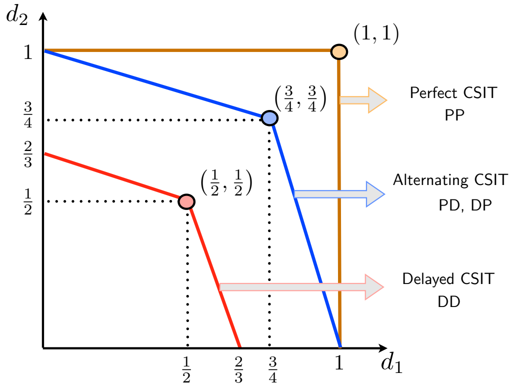

Fig. 2. Comparison of the s.d.o.f. regions.

A. Achieving the s.d.o.f. pair $(\frac{3}{4}, \frac{3}{4})$ via Alternating CSIT

To show the achievability of the region described in Theorem 1, it suffices to show the achievability of the point $(\frac{3}{4}, \frac{3}{4})$. To do so, we propose a scheme to send 3 confidential symbols from the transmitter to each of the receivers in 4 channel uses at high P (that is negligible noise). Let us denote by (u_1, u_2, u_3) and (v_1, v_2, v_3) the confidential symbols intended for receivers 1 and 2, respectively. Also, in 2 of the 4 channel uses, the channel is in state PD; in the remaining 2 uses, the channel is in state DP. The scheme is as follows:

1) At time $t = 1$, $S(1) = \mathsf{PD}$: As the transmitter knows $\mathbf{H}_1(1)$, it sends:

$$\mathbf{X}(1) = [u_1 \quad 0]^T + q\mathbf{H}_1(1)^\perp, \tag{7}$$

where $\mathbf{H}_1(1)\mathbf{H}_1(1)^\perp = 0$, and q denotes an artificial noise distributed as $\mathcal{CN}(0, P)$. Here $\mathbf{H}_1(1)^\perp$ is the beamforming vector that ensures that the artificial noise q does not create interference at receiver 1. For s.d.o.f. calculations, we disregard the additive noise and the receivers' outputs are:

$$Y(1) = h_{11}(1)u_1 \tag{8}$$

$$Z(1) = h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^\perp \triangleq K. \tag{9}$$

Thus, receiver 1 has observed u_1 while receiver 2 gets a linear combination of u_1 and q, which we denote as K. Due to delayed CSIT from receiver 2, the transmitter can reconstruct K in the next channel use and use it for transmission.

2) At time $t = 2$, $S(2) = \mathsf{DP}$: the transmitter knows $\mathbf{H}_2(2)$ and K. It sends

$$\mathbf{X}(2) = [v_1 + K \quad v_2 + K]^T + u_2\mathbf{H}_2(2)^\perp. \tag{10}$$

The received signals are:

$$\begin{aligned} Y(2) =& h_{11}(2)v_1 + h_{12}(2)v_2 + (h_{11}(2) + h_{12}(2))K \\ &+ u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^\perp \qquad (11) \\ =& L_1(v_1, v_2, K) + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^\perp \qquad (12) \end{aligned}$$

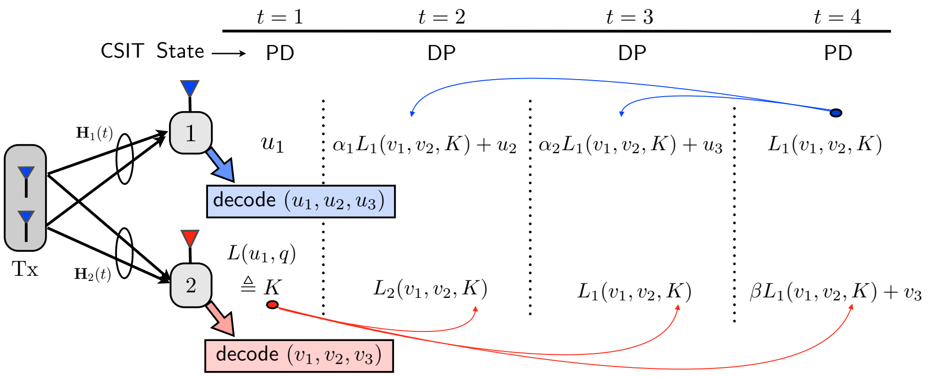

Fig. 3. Achieving $\frac{3}{2}$ s.d.o.f. via alternating CSIT.

$$\begin{aligned} Z(2) &= h_{21}(2)v_1 + h_{22}(2)v_2 + (h_{21}(2)+h_{22}(2))K \\ &\triangleq L_2(v_1,v_2,K), \end{aligned} \tag{13}$$

where we have defined $L_1(v_1,v_2,K)$ and $L_2(v_1,v_2,K)$.

3) At time $t=3$, $S(3) =$ DP: the transmitter knows $\mathbf{H}_2(3)$ and $L_1(v_1,v_2,K)$ (via delayed CSIT from $t=2$). Using these, it transmits:

$$\mathbf{X}(3) = \begin{bmatrix} L_1(v_1,v_2,K) & 0 \end{bmatrix}^T + u_3\mathbf{H}_2(3)^{\perp}, \tag{14}$$

and the channel outputs are:

$$Y(3) = h_{11}(3)L_1(v_1,v_2,K) + u_3\mathbf{H}_1(3)\mathbf{H}_2(3)^{\perp} \tag{15}$$

$$Z(3) = h_{21}(3)L_1(v_1,v_2,K). \tag{16}$$

At the end of this step, note that, receiver 2 can decode v_1 and v_2 by first eliminating K using $Z(1)$ and $Z(3)$ to get a linear combination of v_1 and v_2, which it can then use with $Z(2)$ to solve for v_1 and v_2.

4) At time $t=4$, $S(4) =$ PD: the transmitter knows $\mathbf{H}_1(4)$ and it sends

$$\mathbf{X}(4) = \begin{bmatrix} L_1(v_1,v_2,K) & 0 \end{bmatrix}^T + v_3\mathbf{H}_1(4)^{\perp}, \tag{17}$$

and the channel outputs are:

$$Y(4) = h_{11}(4)L_1(v_1,v_2,K) \tag{18}$$

$$Z(4) = h_{21}(4)L_1(v_1,v_2,K) + v_3\mathbf{H}_2(4)\mathbf{H}_1(4)^{\perp}. \tag{19}$$

Thus, at the end of these four steps the outputs at the two receivers can be summarized (see Fig. 3) as:

$$\mathbf{Y} = \begin{bmatrix} u_1 \\ \alpha_1 L_1(v_1,v_2,K)+u_2 \\ \alpha_2 L_1(v_1,v_2,K)+u_3 \\ L_1(v_1,v_2,K) \end{bmatrix}, \mathbf{Z} = \begin{bmatrix} K \\ L_2(v_1,v_2,K) \\ L_1(v_1,v_2,K) \\ \beta L_1(v_1,v_2,K)+v_3 \end{bmatrix}$$

Using $\mathbf{Y}$, receiver 1 can decode all three symbols (u_1,u_2,u_3) and using $\mathbf{Z}$, receiver 2 can decode (v_1,v_2,v_3).

Now we view the four slots described above as a block and treat the equivalent channel from $\mathbf{U} = (U_1,U_2,U_3)$ to $(\mathbf{Y},\mathbf{H})$ and $(\mathbf{Z},\mathbf{H})$ as a memoryless channel by ignoring the CSI of the previous block. We do the same for the channel from $\mathbf{V} = (V_1,V_2,V_3)$ to $(\mathbf{Y},\mathbf{H})$ and $(\mathbf{Z},\mathbf{H})$. Note that using the proposed scheme, (U_1,U_2,U_3) (resp., (V_1,V_2,V_3)) can be reconstructed from $(\mathbf{Y},\mathbf{H})$ (resp., $(\mathbf{Z},\mathbf{H})$) to within a noise distortion. More formally, the following secrecy rate is achievable for receiver 1 from [11], [17], [18]:

$$\begin{aligned} R_1 =& I(\mathbf{U};\mathbf{Y},\mathbf{H}) - I(\mathbf{U};\mathbf{Z},\mathbf{H}) && (20) \\ =& I(\mathbf{U};\mathbf{Y}|\mathbf{H}) - I(\mathbf{U};\mathbf{Z}|\mathbf{H}) && (21) \end{aligned}$$

where we noted that $\mathbf{U}$, $\mathbf{V}$ and Q and independent of $\mathbf{H}$. Choosing $\mathbf{U}$, $\mathbf{V}$ i.i.d. from a Gaussian distribution, we have:

$$\begin{aligned} I(\mathbf{U};\mathbf{Y}|\mathbf{H}) =& I(U_1,U_2,U_3;\mathbf{Y}|\mathbf{H}) \\ &\overset{(a)}{=} h(U_1)+h(U_2)+h(U_3) - h(U_1,U_2,U_3|\mathbf{Y},\mathbf{H}) \\ &\overset{(b)}{=} 3\log P + o(\log P), \end{aligned}$$

where, (a) follows since U_is are independent of each other and $\mathbf{H}$, and (b) follows since (U_1,U_2,U_3) can be reconstructed from $\mathbf{Y}$ within noise distortion. We also have:

$$\begin{aligned} I(\mathbf{U};\mathbf{Z}|\mathbf{H}) = I(U_1,U_2,U_3;\mathbf{Z}|\mathbf{H}) &\overset{(c)}{=} I(U_1;\mathbf{Z}|\mathbf{H}) \\ &\overset{(d)}{\leq} I(U_1;K|\mathbf{H}) \\ &= o(\log P), \end{aligned}$$

where (c) follows because $\mathbf{Z}$ does not have any term involving (U_2,U_3), and (d) follows from the Markov chain $U_1 \rightarrow K \rightarrow \mathbf{Z}$. Thus, for the first user, a secrecy rate of $3\log P - o(\log P)$ is achievable per block (which itself contains 4 channel uses). This means that a s.d.o.f. of $\frac{3}{4}$ is achievable for receiver 1. Similarly, s.d.o.f. of $\frac{3}{4}$ is achievable for the second user, thus showing the achievability of a sum s.d.o.f. of $\frac{3}{2}$ for the system.

B. Converse Proof

Due to symmetry, it suffices to prove the bound in (5). To this end, we denote the channel outputs as $Y^n = (Y^n_{pd}, Y^n_{dp})$ and $Z^n = (Z^n_{dp}, Z^n_{pd})$, where the subscript Y^n_{ab} (resp., Z^n_{ab}) denotes the portion of the channel output at receiver 1 (resp., receiver 2) corresponding to state AB.

Before we begin the converse proof, we introduce a property of the channel which we call *local statistical equivalence*. Let us focus on the channel output of receiver 2 corresponding to the state PD at time t:

$$Z_{pd}(t) = \mathbf{H}_{2,pd}(t)\mathbf{X}_{pd}(t) + N_{2,pd}(t). \tag{22}$$

Now consider $\widetilde{\mathbf{H}}_{2,pd}(t)$, $\widetilde{N}_{2,pd}(t)$, which are independent of and identically distributed as $\mathbf{H}_{2,pd}(t)$ and $N_{2,pd}(t)$, respectively. Using these random variables, we define an artificial channel output as:

$$\widetilde{Z}_{pd}(t) = \widetilde{\mathbf{H}}_{2,pd}(t)\mathbf{X}_{pd}(t) + \widetilde{N}_{2,pd}(t). \tag{23}$$

Let $\Omega = (\mathbf{H}^n, \widetilde{\mathbf{H}}^n)$. Now the *local statistical equivalence* property is the following:

$$h(Z_{pd}(t)|Z_{pd}^{t-1}, \Omega) = h(\widetilde{Z}_{pd}(t)|Z_{pd}^{t-1}, \Omega). \tag{24}$$

The proof of this property is given in Appendix A. We next present the following lemma which is proved in Appendix B.

Lemma 1 *For the channel model given in* (1)-(2)*, with alternating CSIT, we have:*

$$\begin{align} h(Z^n|\Omega) &\overset{\cdot}{\geq} h(Y_{pd}^n|Z^n, \Omega) \tag{25}\\ 2h(Z^n|\Omega) &\overset{\cdot}{\geq} h(Y_{pd}^n|\Omega) \tag{26}\\ h(Y^n|\Omega) &\overset{\cdot}{\geq} h(Z_{dp}^n|Y^n, \Omega) \tag{27}\\ 2h(Y^n|\Omega) &\overset{\cdot}{\geq} h(Z_{dp}^n|\Omega) \tag{28}\end{align}$$

where $a \overset{\cdot}{\geq} b$ *denotes* $\lim\limits_{P\to\infty} \frac{a}{\log P} \geq \lim\limits_{P\to\infty} \frac{b}{\log P}$.

We proceed with the proof of the converse as follows:

$$\begin{align} nR_1 \leq& I(W_1; Y^n|\Omega) + no(n) \tag{29}\\ \leq& I(W_1; Y^n|\Omega) - I(W_1; Z^n|\Omega) + no(\log P) + no(n) \tag{30}\\ =& h(Y^n|\Omega) - h(Y^n|W_1, \Omega) - h(Z^n|\Omega) \nonumber\\ &+ h(Z^n|W_1, \Omega) + no(\log P) + no(n) \tag{31}\\ \leq& h(Y^n|\Omega) - \frac{1}{2}h(Z_{dp}^n|W_1, \Omega) - h(Z_{dp}^n, Z_{pd}^n|\Omega) \nonumber\\ &+ h(Z_{dp}^n, Z_{pd}^n|W_1, \Omega) + no(\log P) + no(n) \tag{32}\\ =& h(Y^n|\Omega) - \frac{1}{2}h(Z_{dp}^n|W_1, \Omega) - h(Z_{dp}^n|\Omega) \nonumber\\ &- h(Z_{pd}^n|Z_{dp}^n, \Omega) + h(Z_{dp}^n|W_1, \Omega) \nonumber\\ &+ h(Z_{pd}^n|Z_{dp}^n, W_1, \Omega) + no(\log P) + no(n) \tag{33}\\ \leq& h(Y^n|\Omega) - \frac{1}{2}h(Z_{dp}^n|W_1, \Omega) - h(Z_{dp}^n|\Omega) \nonumber\\ &+ h(Z_{dp}^n|W_1, \Omega) + no(\log P) + no(n) \tag{34}\\ =& h(Y^n|\Omega) + \frac{1}{2}h(Z_{dp}^n|W_1, \Omega) \nonumber\\ &- h(Z_{dp}^n|\Omega) + no(\log P) + no(n) \tag{35}\\ \leq& h(Y^n|\Omega) + \frac{1}{2}h(Z_{dp}^n|\Omega) - h(Z_{dp}^n|\Omega) \nonumber\\ &+ no(\log P) + no(n) \tag{36}\\ =& h(Y^n|\Omega) - \frac{1}{2}h(Z_{dp}^n|\Omega) + no(\log P) + no(n) \tag{37}\\ \leq& n\log P - \frac{1}{2}h(Z_{dp}^n|\Omega) + no(\log P) + no(n), \tag{38}\end{align}$$

where (32) follows from the conditional version of (28) (conditioned on W_1) when applied to the second term in (31), and (34) is due to the fact that $h(Z_{pd}^n|Z_{dp}^n, W_1, \Omega) \leq h(Z_{pd}^n|Z_{dp}^n, \Omega)$. We also have the following bounds for user 1:

$$\begin{align} nR_1 \leq& I(W_1; Y^n|W_2, \Omega) + no(n) \tag{39}\\ \leq& I(W_1; Y^n, Z^n|W_2, \Omega) + no(n) \tag{40}\\ =& I(W_1; Y^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{41}\\ \leq& h(Y^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{42}\\ =& h(Y_{pd}^n, Y_{dp}^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{43}\\ \leq& h(Y_{dp}^n|Z^n, W_2, \Omega) + h(Y_{pd}^n|Z^n, W_2, \Omega) \nonumber\\ &+ no(\log P) + no(n) \tag{44}\\ \leq& \frac{n}{2}\log P + h(Y_{pd}^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{45}\\ \leq& \frac{n}{2}\log P + h(Z^n|W_2, \Omega) + no(\log P) + no(n), \tag{46}\end{align}$$

where (46) follows from the conditional version of (25) (conditioned on W_2). For receiver 2, we have

$$\begin{align} nR_2 \leq& I(W_2; Z^n|\Omega) + no(n) \tag{47}\\ =& h(Z^n|\Omega) - h(Z^n|W_2, \Omega) + no(n) \tag{48}\\ =& h(Z_{pd}^n, Z_{dp}^n|\Omega) - h(Z^n|W_2, \Omega) + no(n) \tag{49}\\ \leq& h(Z_{pd}^n|\Omega) + h(Z_{dp}^n|\Omega) - h(Z^n|W_2, \Omega) + no(n) \tag{50}\\ \leq& \frac{n}{2}\log P + h(Z_{dp}^n|\Omega) - h(Z^n|W_2, \Omega) + no(n). \tag{51}\end{align}$$

In summary, from (38), (46) and (51), we have,

$$\begin{align} nR_1 \leq& n\log P - \frac{1}{2}h(Z_{dp}^n|\Omega) + no(\log P) + no(n), \tag{52}\\ nR_1 \leq& \frac{n}{2}\log P + h(Z^n|W_2, \Omega) + no(\log P) + no(n), \tag{53}\\ nR_2 \leq& \frac{n}{2}\log P + h(Z_{dp}^n|\Omega) - h(Z^n|W_2, \Omega) + no(n). \tag{54}\end{align}$$

Eliminating $h(Z_{dp}^n|\Omega)$ and $h(Z^n|W_2, \Omega)$ from these inequalities and taking the limit $n \to \infty$, we arrive at

$$3R_1 + R_2 \leq 3\log P + o(\log P) \tag{55}$$

Dividing by $\log P$ and taking the limit $P \to \infty$, we get the required result $3d_1 + d_2 \leq 3$.

IV. Conclusions

We characterized the exact s.d.o.f. region of the two-user MISO BCCM and alternating CSIT, in which the nature of the CSIT alternates between two states, PD and DP, each occurring for an equal fraction of time. As a corollary, we showed that the sum s.d.o.f. is $\frac{3}{2}$. The proposed scheme shows how to optimally utilize such variations in channel knowledge for secrecy. The novel aspect of the scheme is that a single artificial noise signal suffices to guarantee confidentiality of both of the receivers. A more complete characterization involving all possible nine combinations of the three states, perfect (P), delayed (D) and no CSIT (N), will be pursued in the future.

Appendix A
Proof of local statistical equivalence

Let us denote the common distribution of $\mathbf{H}_{2,pd}(t)$, $\widetilde{\mathbf{H}}_{2,pd}(t)$ by F. Also, let $\Omega_t = \Omega \backslash \left\{\mathbf{H}_{2,pd}(t), \widetilde{\mathbf{H}}_{2,pd}(t)\right\}$. We have,

$$\begin{aligned}
&h(Z_{pd}(t)|Z_{pd}^{t-1},\Omega)\\
=&\mathbb{E}_F\left[h(Z_{pd}(t)|Z_{pd}^{t-1},\Omega_t,\widetilde{\mathbf{H}}_{2,pd}(t),\mathbf{H}_{2,pd}(t)=\mathbf{h}(t))\right] && (56)\\
=&\mathbb{E}_F\left[h(\mathbf{h}(t)\mathbf{X}_{pd}(t)+N_{2,pd}(t)|Z_{pd}^{t-1},\Omega_t)\right] && (57)\\
=&\mathbb{E}_F\left[h(\mathbf{h}(t)\mathbf{X}_{pd}(t)+\widetilde{N}_{2,pd}(t)|Z_{pd}^{t-1},\Omega_t)\right] && (58)\\
=&\mathbb{E}_F\left[h(\mathbf{h}(t)\mathbf{X}_{pd}(t)+\widetilde{N}_{2,pd}(t)|Z_{pd}^{t-1},\Omega_t,\widetilde{\mathbf{H}}_{2,pd}(t)=\mathbf{h}(t))\right] && (59)\\
=&\mathbb{E}_F\left[h(\widetilde{Z}_{pd}(t)|Z_{pd}^{t-1},\Omega_t,\mathbf{H}_{2,pd}(t),\widetilde{\mathbf{H}}_{2,pd}(t)=\mathbf{h}(t))\right] && (60)\\
=&h(\widetilde{Z}_{pd}(t)|Z_{pd}^{t-1},\Omega), && (61)
\end{aligned}$$

where (57) follows because $\mathbf{X}_{pd}(t)$ does not depend on $(\mathbf{H}_{2,pd}(t),\widetilde{\mathbf{H}}_{2,pd}(t))$, (58) follows since the additive noises $N_{2,pd}(t)$ and $\widetilde{N}_{2,pd}(t)$ are i.i.d. and independent of all other random variables, (59)-(60) follow since $\mathbf{H}_{2,pd}(t)$ and $\widetilde{\mathbf{H}}_{2,pd}(t)$ have the same distribution F and the fact that $\mathbf{X}_{pd}(t)$ does not depend on $(\mathbf{H}_{2,pd}(t),\widetilde{\mathbf{H}}_{2,pd}(t))$.

Appendix B
Proof of Lemma 1

Due to symmetry, it suffices to prove (25) and (26):

$$\begin{aligned}
h(Z^n|\Omega)=&h(Z_{pd}^n|\Omega)+h(Z_{dp}^n|Z_{pd}^n,\Omega) && (62)\\
=&\sum_{t=1}^{n}h(Z_{pd}(t)|Z_{pd}^{t-1},\Omega)+h(Z_{dp}^n|Z_{pd}^n,\Omega) && (63)
\end{aligned}$$

Using the *local statistical equivalence* property, we get,

$$h(Z^n|\Omega)=\sum_{t=1}^{n}h(\widetilde{Z}_{pd}(t)|Z_{pd}^{t-1},\Omega)+h(Z_{dp}^n|Z_{pd}^n,\Omega) \quad (64)$$

Adding (63) and (64), and lower bounding, we get,

$$\begin{aligned}
2h(Z^n|\Omega)\geq&\sum_{t=1}^{n}h(Z_{pd}(t),\widetilde{Z}_{pd}(t)|Z_{pd}^{t-1},\Omega)+2h(Z_{dp}^n|Z_{pd}^n,\Omega)\\
\geq&\sum_{t=1}^{n}h(Z_{pd}(t),\widetilde{Z}_{pd}(t)|Z_{pd}^{t-1},\Omega)\\
&+h(Z_{dp}^n|Z_{pd}^n,\Omega)+no(\log P) && (65)\\
=&\sum_{t=1}^{n}h(Z_{pd}(t),\widetilde{Z}_{pd}(t),Y_{pd}(t)|Z_{pd}^{t-1},\Omega)\\
&-\sum_{t=1}^{n}h(Y_{pd}(t)|Z_{pd}(t),\widetilde{Z}_{pd}(t),Z_{pd}^{t-1},\Omega)\\
&+h(Z_{dp}^n|Z_{pd}^n,\Omega)+no(\log P) && (66)\\
\geq&\sum_{t=1}^{n}h(Z_{pd}(t),Y_{pd}(t)|Z_{pd}^{t-1},\Omega)\\
&+h(Z_{dp}^n|Z_{pd}^n,\Omega)+no(\log P) && (67)\\
\geq&\sum_{t=1}^{n}h(Z_{pd}(t),Y_{pd}(t)|Z_{pd}^{t-1},Y_{pd}^{t-1},\Omega)\\
&+h(Z_{dp}^n|Z_{pd}^n,Y_{pd}^n,\Omega)+no(\log P) && (68)\\
=&h(Z_{pd}^n,Y_{pd}^n|\Omega)+h(Z_{dp}^n|Z_{pd}^n,Y_{pd}^n,\Omega)+no(\log P) && (69)\\
=&h(Z^n,Y_{pd}^n|\Omega)+no(\log P), && (70)
\end{aligned}$$

where (65) follows by noting that

$$h(Z_{dp}^n|Z_{pd}^n,\Omega)\geq h(Z_{dp}^n|Z_{pd}^n,X^n,\Omega)=no(\log P) \quad (71)$$

and (66) follows since given $(Z_{pd}(t),\widetilde{Z}_{pd}(t))$, one can reconstruct $X_{pd}(t)$ and hence $Y_{pd}(t)$ within noise distortion, implying that $h(Y_{pd}(t)|Z_{pd}(t),\widetilde{Z}_{pd}(t),Z_{pd}^{t-1},\Omega)\leq no(\log P)$.

Now we use (70) in two ways:

$$\begin{aligned}
2h(Z^n|\Omega)\geq&h(Z^n,Y_{pd}^n|\Omega)+no(\log P) && (72)\\
=&h(Z^n|\Omega)+h(Y_{pd}^n|Z^n,\Omega)+no(\log P) && (73)
\end{aligned}$$

which implies $h(Z^n|\Omega)\overset{\cdot}{\geq}h(Y_{pd}^n|Z^n,\Omega)$. Alternatively from (70), we also have

$$\begin{aligned}
2h(Z^n|\Omega)\geq&h(Y_{pd}^n|\Omega)+h(Z^n|Y_{pd}^n,\Omega)+no(\log P) && (74)\\
\geq&h(Y_{pd}^n|\Omega)+no(\log P) && (75)
\end{aligned}$$

which implies $2h(Z^n|\Omega)\overset{\cdot}{\geq}h(Y_{pd}^n|\Omega)$ thus proving Lemma 1.

References

[1] Y. Liang, H. V. Poor, and S. Shamai. Secure communication over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2470–2492, Jun. 2008.

[2] P. K. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory*, 54(10):4687–4698, Oct. 2008.

[3] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory*, 55(9):4033–4039, Sep. 2009.

[4] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas - Part II: The MIMOME wiretap channel. *IEEE Trans. Inf. Theory*, 56(11):5515–5532, Nov. 2010.

[5] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory*, 57(8):4961–4972, Aug. 2011.

[6] T. Liu and S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Trans. Inf. Theory*, 55(6):2547–2553, Jun. 2009.

[7] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, Dec. 2008.

[8] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *Allerton Conference*, Sep. 2008.

[9] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian multiple access wiretap channel. In *IEEE ISIT*, Jul. 2013.

[10] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. *IEEE Trans. Inf. Theory*, 57(4):2083–2114, Apr. 2011.

[11] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, Jun. 2008.

[12] R. Liu and H. V. Poor. Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inf. Theory*, 55(3):1235–1249, Mar. 2009.

[13] R. Liu, T. Liu, H. V. Poor, and S. Shamai. Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 56(9):4215–4227, Sep. 2010.

[14] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers. In *Allerton Conference*, Oct. 2012.

[15] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai. Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT. *IEEE Trans. Inf. Theory*, 59(9):5244–5256, Sep. 2013.

[16] R. Tandon, S. A. Jafar, S. Shamai, and H. V. Poor. On the synergistic benefits of alternating CSIT for the MISO broadcast channel. *IEEE Trans. Inf. Theory*, 59(7):4106–4128, Jul. 2013.

[17] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct. 1975.

[18] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.