Secrecy for MISO Broadcast Channels via 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]Discovery Analytics Center and Department of Computer Science, Virginia Tech, Blacksburg, VA 24061

***Abstract*—The two-user multiple-input single-output (MISO) broadcast channel with confidential messages (BCCM) is studied in which the nature of channel state information at the transmitter (CSIT) from each user can be of the form I_i, $i = 1, 2$ where $I_1, I_2 \in \{P, D, N\}$, and the forms P, D and N correspond to perfect and instantaneous, completely delayed, and no CSIT, respectively. Thus, the overall CSIT can alternate over time between 9 possible states corresponding to all possible values of $I_1 I_2$, with each state occurring for $\lambda_{I_1 I_2}$ fraction of the total duration. The main contribution of this paper is to establish the secure degrees of freedom (s.d.o.f.) region of the MISO BCCM with alternating CSIT with the symmetry assumption $\lambda_{I_1 I_2} = \lambda_{I_2 I_1}$. The results highlight the synergistic benefits of coding across CSIT states for secrecy and the interplay between various aspects of channel knowledge and its impact on s.d.o.f.**

I. Introduction

Wireless systems are particularly vulnerable to security attacks because of the inherent openness of the transmission medium. With the adoption of multiple-input multiple-output (MIMO) systems, there has been a significant recent interest in information theoretic physical layer security, which seeks to exploit the difference in the wireless channels between different users to ensure security. Information theoretic security has been investigated for a variety of channel models including fading channels [1]–[3], MIMO wiretap channels [4]–[7], and broadcast channels with confidential messages [8]–[10].

The focus of this paper is on the secure degrees of freedom (s.d.o.f.) region of 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 (see Fig. 1). The secrecy capacity region of the MISO broadcast channel for the case of perfect and instantaneous channel state information (CSI) at all terminals (transmitter and the receivers) has been characterized in [9], [10]. Using these results, it follows that for the two-user MISO BCCM, the sum s.d.o.f. is 2 with perfect and instantaneous channel state information at the transmitter (CSIT). In practice, the assumption of perfect and instantaneous CSIT may be too optimistic as CSIT may be delayed, imprecise or may not be available at all.

The impact of relaxing such assumptions on the rate (secure or otherwise) has been widely studied in the literature. With perfect CSIT and no secrecy constraints, the sum degrees of freedom (d.o.f.) for the two-user MISO broadcast channel is 2. With no CSIT however, reference [11] showed that the d.o.f. collapses to 1. With delayed (in which the delay in acquiring CSIT is larger than the channel coherence time as in [12]) CSIT, it is shown in [12] that the sum d.o.f. for the two-user MISO BC increases to $\frac{4}{3}$.

When security constraints are introduced, the s.d.o.f. is known for several scenarios of delayed or no CSIT. For the two-user MISO BCCM 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, it has been shown in [13] that the sum s.d.o.f. increases to 1.

In practice, the nature of CSIT can vary across users. This observation naturally leads to the setting of heterogeneous (or hybrid) CSIT which models the variability in the quality/delay of channel knowledge supplied by different users. To the best of our knowledge, the complete characterization of the d.o.f. of all fixed heterogeneous CSIT configurations is only known for the two-user MISO broadcast channel: see [14], [15] for state PD for which the optimal sum d.o.f. is shown to be $3/2$; and [16] which recently settled the states PN and DN through a novel converse proof and showed that the optimal sum d.o.f. is given by 1. Partial results are available for the three-user MISO BC with hybrid CSIT in [17], [18] but by and large the problem of heterogeneous CSIT even without secrecy constraints remains open.

Besides exhibiting heterogeneity across users, the nature of channel knowledge may also vary over time/frequency. Such variability can arise either naturally due to the time variation in tolerable feedback overhead from a user or it can be artificially induced by deliberately altering the channel feedback mechanism over time/frequency. This leads naturally to the setting of alternating CSIT in which multiple CSIT states arise over time. The alternating CSIT framework was introduced in [19] where the d.o.f. region was characterized for the two-user MISO BC.

In this paper, we consider the two-user MISO BCCM with alternating CSIT with all 9 possible CSIT states: PP, PD, PN, DP, DD, DN, NP, ND, and NN. We assume that these states occur for arbitrary fractions of time, except for a mild condition of symmetry, which is that states $I_1 I_2$ and $I_2 I_1$ occur for equal fractions of the time if $I_1 \neq I_2$. In our preliminary

This work was supported by NSF Grants CNS 13-14733, CCF 14-22111, CCF 14-22129 and CCF 14-22090.

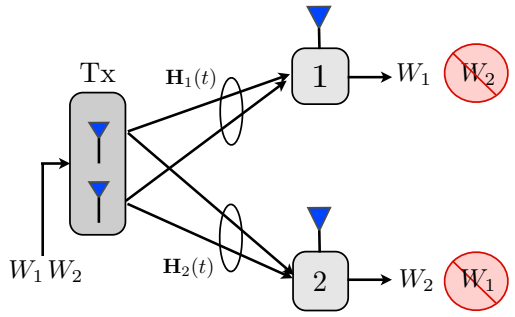

Fig. 1: MISO broadcast channel with confidential messages.

work [20], we considered the problem with only two states, PD and DP and established the optimal s.d.o.f. region for this specific problem. The main contribution of the present paper is the characterization of the optimal s.d.o.f. region for the general model with all 9 states. We highlight the synergistic benefits of coding across states for secrecy and the impact of channel knowledge on security.

II. System model

We consider a two-user MISO BCCM, shown in Fig. 1, where the transmitter Tx, equipped with 2 antennas, wishes to send independent confidential messages to two single antenna receivers 1 and 2. The input-output relations at time t are given by,

$$Y(t) = \mathbf{H}_1(t)\mathbf{X}(t) + N_1(t) \tag{1}$$
$$Z(t) = \mathbf{H}_2(t)\mathbf{X}(t) + N_2(t), \tag{2}$$

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 $\mathbf{H}^n = \{\mathbf{H}(1), \ldots, \mathbf{H}(n)\}$ as the sequence of channel vectors up until and including time n.

In practice, the receivers estimate the channel coefficients and feed them back to the transmitter. At any time t, the receiver may send any function of all the channel measurements upto and including time t to the transmitter. As an idealization, we assume that the CSIT, if available, has infinite precision.

In order to model the delay in CSIT, we assume that at each time t, there are three possible CSIT states for each user:

- *Perfect CSIT* (P): This denotes the availability of precise and instantaneous CSI of a user at the transmitter. Essentially, the transmitter has precise channel knowledge before the start of the communication.
- *Delayed CSIT* (D): In this state, the transmitter does not have the CSI at the beginning of the communication. In slot t, the receiver may send any function of all the channel coefficients upto and including time t as CSI to the transmitter. However, the CSIT becomes available only after a delay such that the CSI is completely outdated, that is, independent of the current channel realization.
- *No CSIT* (N): In this state, there is no CSI of the user available at the transmitter.

Denote the CSIT of user 1 by I_1 and the CSIT of user 2 by I_2. Then,

$$I_1, I_2 \in \{\mathsf{P}, \mathsf{D}, \mathsf{N}\}. \tag{3}$$

Thus, for the two-user MISO broadcast channel, we have 9 CSIT states, namely PP, PD, PN, DP, DD, DN, NP, ND, and NN. Let $\lambda_{I_1 I_2}$ be the fraction of the time the state $I_1 I_2$ occurs. Then,

$$\sum_{I_1, I_2} \lambda_{I_1 I_2} = 1. \tag{4}$$

We also assume symmetry: $\lambda_{I_1 I_2} = \lambda_{I_2 I_1}$ for every I_1, I_2. Specifically,

$$\lambda_{PD} = \lambda_{DP} \tag{5}$$
$$\lambda_{DN} = \lambda_{ND} \tag{6}$$
$$\lambda_{PN} = \lambda_{NP}. \tag{7}$$

Further we assume that perfect and global CSI is available at both receivers.

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,

$$\frac{1}{n} I(W_1; Z^n, \mathbf{H}^n) \leq \epsilon_n, \qquad \frac{1}{n} I(W_2; Y^n, \mathbf{H}^n) \leq \epsilon_n, \tag{8}$$

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

$$d_1 = \lim_{P \to \infty} \frac{R_1}{\log P}, \qquad d_2 = \lim_{P \to \infty} \frac{R_2}{\log P}. \tag{9}$$

Given the probability mass function (pmf), $\lambda_{I_1 I_2}$, our goal is to characterize the s.d.o.f. region $\mathcal{D}(\lambda_{I_1 I_2})$.

Before stating our main results, we define the following:

$$\lambda_P \triangleq \lambda_{PP} + \lambda_{PD} + \lambda_{PN} \tag{10}$$
$$\lambda_D \triangleq \lambda_{PD} + \lambda_{DD} + \lambda_{DN} \tag{11}$$
$$\lambda_N \triangleq \lambda_{PN} + \lambda_{DN} + \lambda_{NN}. \tag{12}$$

Using these definitions, it is easy to verify that

$$\lambda_P + \lambda_D + \lambda_N = 1. \tag{13}$$

Here, we can interpret these three quantities as following:

- λ_P: represents the total fraction of time the CSIT of a user is in the P state.
- λ_D: represents the total fraction of time the CSIT of a user is delayed, that is, the state D.
- λ_N: represents the total fraction of time a user supplies no CSIT.

III. Main Result and Discussion

Theorem 1: The s.d.o.f. region for the two-user MISO BCCM with alternating CSIT, $\mathcal{D}(\lambda_{I_1 I_2})$, is the set of all non-negative pairs (d_1, d_2) satisfying,

$$d_1 \leq \min\left(\frac{2+2\lambda_P-\lambda_{PP}}{3}, 1-\lambda_{NN}\right) \tag{14}$$

$$d_2 \leq \min\left(\frac{2+2\lambda_P-\lambda_{PP}}{3}, 1-\lambda_{NN}\right) \tag{15}$$

$$3d_1+d_2 \leq 2+2\lambda_P \tag{16}$$

$$d_1+3d_2 \leq 2+2\lambda_P \tag{17}$$

$$d_1+d_2 \leq 2(\lambda_P+\lambda_D). \tag{18}$$

Due to space constraints, the proof of Theorem 1 is omitted here and is presented in [21]. We briefly present the key ideas and challenges behind the achievability of the s.d.o.f. region in Section IV along with a representative example which illustrates the benefits of alternating CSIT for secrecy.

In the remainder of this section, we present a series of remarks based on Theorem 1 to highlight several interesting aspects and consequences of alternating channel knowledge for secrecy.

Remark 1. *[Sum s.d.o.f.:* $\max(d_1+d_2)$*]:* From the region stated in (14)-(18), it is clear that the sum s.d.o.f is given by,

$$\text{sum s.d.o.f.} = \min\left(2\left(\frac{2+2\lambda_P-\lambda_{PP}}{3}\right), 2(1-\lambda_{NN}), 2(\lambda_P+\lambda_D), 1+\lambda_P\right) \tag{19}$$

We simplify the above expression by noting that the first two terms in the minimum are inactive due to the inequalities $1+\lambda_P \leq 2\left(\frac{2+2\lambda_P-\lambda_{PP}}{3}\right)$, and $2(\lambda_P+\lambda_D) = 2(1-\lambda_N) \leq 2(1-\lambda_{NN})$. These inequalities follow directly from (10)-(13). Using these inequalities, the sum s.d.o.f. expression above is equivalent to

$$\text{sum s.d.o.f.} = \min\left(2(\lambda_P+\lambda_D), 1+\lambda_P\right) \tag{20}$$

$$= \min\left(2(\lambda_P+\lambda_D), 2\lambda_P+\lambda_D+\lambda_N\right) \tag{21}$$

$$= 2\lambda_P+\lambda_D+\min(\lambda_D,\lambda_N). \tag{22}$$

Fig. 2 shows the sum s.d.o.f. as a function of λ_P and λ_D.

Remark 2. *[Same-marginals property]:* From (22), we notice that the marginal probabilities λ_P, λ_D and λ_N are sufficient to determine the sum s.d.o.f. Thus, for any given pmf $\lambda_{I_1 I_2}$, satisfying the symmetry conditions (5)-(7), there exists an *equivalent alternating CSIT problem* having only three states: PP, DD and NN occurring for λ_P, λ_D and λ_N fractions of the time respectively, that has the same sum s.d.o.f. This observation is similar to the case when there is no secrecy constraint [19]. However unlike in [19], the s.d.o.f. region does not have the same property as we can see the explicit dependence of the s.d.o.f. region on λ_{PP} and λ_{NN}.

Remark 3. *[Benefit of delayed CSIT]:* From a sum s.d.o.f. perspective, we see that when $\lambda_D \geq \lambda_N$, the sum s.d.o.f. depends only on λ_P. Hence, as long as $\lambda_D \geq \lambda_N$ holds, the N states behave as D states in the sense that, if the N states were enhanced to D states, the sum s.d.o.f. would not increase. Essentially, the N states can be combined with various D states and we obtain the same sum s.d.o.f. as if every N state were replaced by a D state. On the other hand, if $\lambda_D \leq \lambda_N$, the delayed CSIT is as good as perfect CSIT, that is, enhancing every D state to a P state does not increase the sum s.d.o.f.

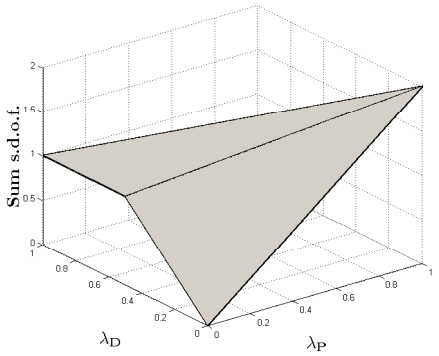

Fig. 2: The sum s.d.o.f. as a function of λ_P and λ_D.

Remark 4. *[Minimum CSIT required for a sum s.d.o.f. value]:* Fig. 3 shows the trade-off between λ_P and λ_D for a given value of sum s.d.o.f. The highlighted corner point in each curve shows the most *efficient* point in terms of CSIT requirement. Any other feasible point either involves redundant CSIT or unnecessary instantaneous CSIT where delayed CSIT would have sufficed. For example, following are the minimum CSIT requirements for various sum s.d.o.f. values:

$$\text{sum s.d.o.f.} = 2 : (\lambda_P,\lambda_D)_{\min} = (1,0) \tag{23}$$

$$\text{sum s.d.o.f.} = \frac{3}{2} : (\lambda_P,\lambda_D)_{\min} = \left(\frac{1}{2},\frac{1}{4}\right) \tag{24}$$

$$\text{sum s.d.o.f.} = \frac{4}{3} : (\lambda_P,\lambda_D)_{\min} = \left(\frac{1}{3},\frac{1}{3}\right) \tag{25}$$

$$\text{sum s.d.o.f.} = 1 : (\lambda_P,\lambda_D)_{\min} = \left(0,\frac{1}{2}\right) \tag{26}$$

In general, for a given value of sum s.d.o.f. $= s$, the minimum CSIT requirements are given by:

$$(\lambda_P,\lambda_D)_{\min} = \begin{cases} \left(s-1, 1-\frac{s}{2}\right), & \text{if } 1 \leq s \leq 2 \\ \left(0,\frac{s}{2}\right), & \text{if } 0 \leq s \leq 1 \end{cases} \tag{27}$$

Remark 5. *[Cost of security]:* We recall that in the case with no security [19], the sum d.o.f. is given by,

$$\text{sum d.o.f.} = 2-\frac{2\lambda_N}{3}-\frac{\max(\lambda_N,2\lambda_D)}{3} \tag{28}$$

Defining loss $\triangleq$ (sum d.o.f.) $-$ (sum s.d.o.f.), and using (22), we see that the loss in d.o.f. that must be incurred to incorporate secrecy constraints is given by,

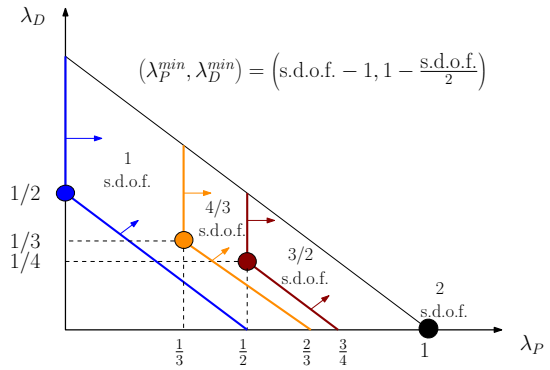

Fig. 3: Trade-off between delayed and perfect CSIT.

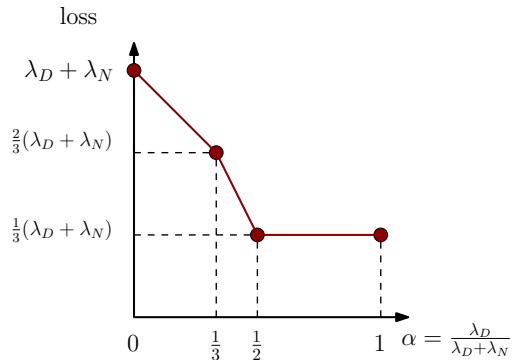

Fig. 4: Cost of security.

$$\text{loss} = \begin{cases} \lambda_N, & \text{if } \lambda_N \geq 2\lambda_D \\ \frac{2}{3}(2\lambda_N - \lambda_D), & \text{if } 2\lambda_D \geq \lambda_N \geq \lambda_D \\ \frac{1}{3}(\lambda_N + \lambda_D), & \text{if } \lambda_D \geq \lambda_N \end{cases} \tag{29}$$

If we define $\alpha = \lambda_D/(\lambda_D + \lambda_N)$, we can rewrite (29) as follows,

$$\text{loss} = (\lambda_D + \lambda_N) \times \begin{cases} (1-\alpha), & \text{if } \alpha \leq \frac{1}{3} \\ \left(\frac{4}{3} - 2\alpha\right), & \text{if } \frac{1}{2} \geq \alpha \geq \frac{1}{3} \\ \frac{1}{3}, & \text{if } \alpha \geq \frac{1}{2} \end{cases} \tag{30}$$

We show this loss as a function of α in Fig. 4. Note that $\lambda_D + \lambda_N$ is the fraction of the time a user feeds back imperfect (delayed or none) CSIT. If this fraction is fixed, and $\lambda_N \geq \lambda_D$, increasing the fraction of delayed CSIT leads to a decrease in the penalty due to the security constraints. However, when $\lambda_D \geq \lambda_N$, increasing the fraction of delayed CSIT further does not reduce the penalty any more.

Remark 6. *[Synergistic benefits for secrecy]:* It was shown in [19] that by coding across different states one can achieve higher sum d.o.f. than by optimal encoding for each state separately and time sharing. A similar result holds true in our case as well. We illustrate this with the help of a few examples.

Example 1. Consider a special case where only states PD and DP occur, each for half of the time. In our previous work, [20], we showed that optimal sum s.d.o.f. is $\frac{3}{2}$ in this case. The optimal s.d.o.f. for the PD (or DP) state alone is established to be 1 in [21]. This can be achieved either by treating the PD state as a PN state and zero forcing, or by treating PD as a DD state. Thus, by encoding for each state separately and time sharing between the PD and DP states, we can achieve only 1 sum s.d.o.f., whereas joint encoding across the states achieves sum s.d.o.f. of $\frac{3}{2}$. Thus, we have synergistic benefit of 50% in this case.

Example 2. Consider another special case with three states: PD, DP and NN each occurring for one-third of the time. The optimal sum s.d.o.f. is $\frac{4}{3}$. If we encode for each state separately and time share between them, we can achieve a sum s.d.o.f. of $\frac{1}{3} \times 1 + \frac{1}{3} \times 1 + \frac{1}{3} \times 0 = \frac{2}{3}$, since the NN state does not provide any secrecy. If we encode across the PD and DP states optimally and then time share with the NN state, we can achieve $\frac{2}{3} \times \frac{3}{2} + \frac{1}{3} \times 0 = 1$ sum s.d.o.f. Thus, in this case too, we get synergistic benefit by coding across all the states together.

Example 3. Now, assume we have the following three states: PN, NP and DD each occurring for one-third of the time. The optimal sum s.d.o.f. for this case is $\frac{4}{3}$. By separately encoding for each state and time sharing, we can achieve $\frac{1}{3} \times 1 + \frac{1}{3} \times 1 + \frac{1}{3} \times 1 = 1$ sum s.d.o.f. Note that the optimal s.d.o.f. for PN and NP states, each occurring for half of the time, is 1. Thus, by optimal encoding for PN and NP together and time sharing with the DD state also yields sum s.d.o.f. of 1. Therefore, there is synergistic benefit to be gained by coding across all the states together in this case too.

Remark 7. *[Lack of synergistic benefits]:* There are some situations where joint encoding across alternating states yields no benefit in terms of the s.d.o.f. region. For example, consider a case with only two states, PN and NP, each occurring for half of the time. The optimal sum s.d.o.f. for the PN state alone is 1, which is achieved by zero forcing. The optimal sum s.d.o.f. of both PN and NP states together is also 1; thus encoding for each state separately is optimal in this case. This result is perhaps surprising, since in the case with no security, we do get synergistic benefits of joint encoding across the PN and NP states, [19]. The optimal sum d.o.f. with joint encoding is $\frac{3}{2}$, while that for each state alone is 1.

IV. Achievability

The proof of the achievability of the s.d.o.f. region has two steps: (1) We first identify and develop several key constituent schemes. A summary of these constituent schemes is shown in Table I. (2) These schemes are then combined carefully by time sharing depending on the fractions of the different states.

Notation for Table I: A particular sum s.d.o.f. value can be achieved in various ways through alternation between different possible sets of CSIT states. To this end, we use the following notation: if there are r schemes achieving a particular sum s.d.o.f. value, we denote these schemes as: $S_1^{\text{sum s.d.o.f.}}, S_2^{\text{sum s.d.o.f.}}, \ldots, S_r^{\text{sum s.d.o.f.}}$. For example, in Table I, for achieving the sum s.d.o.f. value of 1, we present $r = 3$ distinct schemes and these are denoted as S_1^1, S_2^1 and S_3^1.

Due to space constraints, we are unable to present all the schemes here; the complete proofs are provided in [21]. As a representative example, here we elaborate on one of the schemes, $S_1^{4/3}$ for the three states $(\text{PD}, \text{DP}, \text{NN})$.

Summary of Constituent Schemes (CS)				
Sum s.d.o.f.	CS Notation	CSIT States	Fractions	(d_1, d_2)
2	S^2	PP	1	$(1,1)$
3/2	$S_1^{3/2}$	PD, DP	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$\left(\frac{3}{4}, \frac{3}{4}\right)$
	$S_2^{3/2}$	PD, DP, PN, NP	$\left(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right)$	$\left(\frac{3}{4}, \frac{3}{4}\right)$
4/3	$S_1^{4/3}$	PD, DP, NN	$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$	$\left(\frac{2}{3}, \frac{2}{3}\right)$
	$S_2^{4/3}$	PN, NP, DD	$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$	$\left(\frac{2}{3}, \frac{2}{3}\right)$
1	S_1^{1}	DD	1	$\left(\frac{1}{2}, \frac{1}{2}\right)$
	S_2^{1}	DD, NN	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$\left(\frac{1}{2}, \frac{1}{2}\right)$
	S_3^{1}	DN, ND	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$\left(\frac{1}{2}, \frac{1}{2}\right)$
2/3	$S_1^{2/3}$	DD	1	$\left(\frac{2}{3}, 0\right)$
	$S_2^{2/3}$	DD, NN	$\left(\frac{2}{3}, \frac{1}{3}\right)$	$\left(\frac{2}{3}, 0\right)$
	$S_3^{2/3}$	DN, ND, NN	$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$	$\left(\frac{2}{3}, 0\right)$

TABLE I: Constituent schemes.

Remark 8. From [20], it follows that the optimal sum s.d.o.f. for two states PD and DP is $3/2$. On the other hand, for the NN state itself, the optimal sum s.d.o.f. is 0. Hence, time sharing between (PD, DP) and NN achieves a sum s.d.o.f. of $\frac{2}{3} \times \frac{3}{2} + \frac{1}{3} \times 0 = 1$. The scheme $S_1^{4/3}$ achieves sum s.d.o.f. of $4/3$ and shows that the states PD, DP, NN are inseparable and joint coding across all of the states is necessary to achieve the optimal s.d.o.f.

A. Scheme $S_1^{4/3}$

The scheme $S_1^{4/3}$ uses the states (PD, DP, NN) for fractions $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ to achieve s.d.o.f. pair $(d_1, d_2) = (\frac{2}{3}, \frac{2}{3})$. As shown in Fig. 5, we send 2 symbols to each user in 3 time slots. Let (u_1, u_2) and (v_1, v_2) be the symbols intended for the first and second user, respectively. It is as follows:

1) Time $t = 1$, $S(1) =$ PD: The Tx knows $\mathbf{H}_1(1)$, it sends:

$$\mathbf{X}(1) = [u_1 \quad 0]^T + q\mathbf{H}_1(1)^{\perp}, \tag{31}$$

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 a 2×1 beamforming vector that ensures that the artificial noise q does not create interference at receiver 1. The receivers' outputs are:

$$Y(1) = h_{11}(1)u_1 \tag{32}$$

$$Z(1) = h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp} \triangleq K. \tag{33}$$

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) Time $t = 2$, $S(2) =$ DP: The Tx knows $\mathbf{H}_2(2), K$. It sends

$$\mathbf{X}(2) = [v_1 + K \quad v_2 + K]^T + u_2\mathbf{H}_2(2)^{\perp}. \tag{34}$$

The received signals are:

$$\begin{aligned} Y(2) =& h_{11}(2)v_1 + h_{12}(2)v_2 + (h_{11}(2) + h_{12}(2))K \\ &+ u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^{\perp} \end{aligned} \tag{35}$$

$$= L_1(v_1, v_2, K) + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^{\perp} \tag{36}$$

$$Z(2) = h_{21}(2)v_1 + h_{22}(2)v_2 + (h_{21}(2) + h_{22}(2))K \tag{37}$$

$$\triangleq L_2(v_1, v_2, K), \tag{38}$$

where we have defined $L_1(v_1, v_2, K)$ and $L_2(v_1, v_2, K)$ as independent linear combinations of v_1, v_2 and K at receivers 1 and 2, respectively.

3) Time $t = 3$, $S(3) =$ NN: The Tx sends

$$\mathbf{X}(3) = [L_1(v_1, v_2, K) \quad 0]^T \tag{39}$$

The receivers get:

$$Y(3) = h_{11}(3)L_1(v_1, v_2, K) \tag{40}$$

$$Z(3) = h_{21}(3)L_1(v_1, v_2, K) \tag{41}$$

At the end of three slots, therefore, the received outputs can be summarized as:

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

Using $\mathbf{Y}$, receiver 1 can decode (u_1, u_2), while receiver 2 can decode (v_1, v_2) using $\mathbf{Z}$.

Now, we view the three slots described above as a block and treat the equivalent channel from $\underline{\mathbf{u}} = (u_1, u_2)$ to $(\mathbf{Y}, \mathbf{H})$ and $(\mathbf{Z}, \mathbf{H})$ as a memoryless wiretap channel by ignoring the CSI of the previous block. We do the same for the channel from $\underline{\mathbf{v}} = (v_1, v_2)$ to $(\mathbf{Y}, \mathbf{H})$ and $(\mathbf{Z}, \mathbf{H})$. Note also that no information about $\mathbf{H}$ is used to create the codebooks for $\underline{\mathbf{u}}$ and $\underline{\mathbf{v}}$. Using the proposed scheme, (u_1, u_2) (resp., (v_1, v_2)) can be reconstructed from $(\mathbf{Y}, \mathbf{H})$ (resp., $(\mathbf{Z}, \mathbf{H})$) to within a noise distortion. More formally, following secrecy rate is achievable for receiver 1 [22], [23]:

$$R_1 = I(\underline{\mathbf{u}}; \mathbf{Y}, \mathbf{H}) - I(\underline{\mathbf{v}}; \mathbf{Z}, \mathbf{H}) \tag{42}$$

$$= I(\underline{\mathbf{u}}; \mathbf{Y}|\mathbf{H}) - I(\underline{\mathbf{v}}; \mathbf{Z}|\mathbf{H}) \tag{43}$$

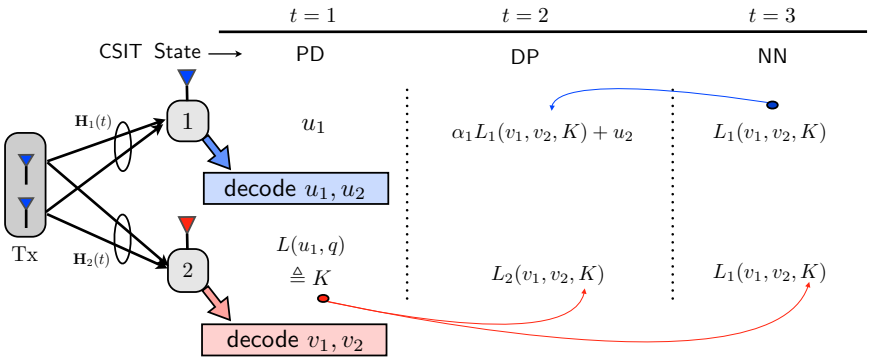

Fig. 5: Achieving sum s.d.o.f. of $4/3$ using the scheme $S_1^{4/3}$ for states $(\mathsf{PD},\mathsf{DP},\mathsf{NN})$.

where we noted that $\underline{\mathbf{u}}$, $\underline{\mathbf{v}}$ and q and independent of $\mathbf{H}$. Now,

$$I(\underline{\mathbf{u}};\mathbf{Y}|\mathbf{H}) = h(u_1)+h(u_2)-h(u_1,u_2|\mathbf{Y},\mathbf{H}) \quad (44)$$
$$= 2\log P + o(\log P), \quad (45)$$

where (44) follows since u_is are independent of each other and $\mathbf{H}$, and (45) follows since (u_1,u_2) can be reconstructed from $\mathbf{Y}$ and $\mathbf{H}$ within noise distortion. Also, we have,

$$I(\underline{\mathbf{v}};\mathbf{Y}|\mathbf{H}) \leq I(\underline{\mathbf{v}};L_1(\underline{\mathbf{v}},K)|\mathbf{H}) \quad (46)$$
$$= h(L_1(\underline{\mathbf{v}},K)|\mathbf{H}) - h(L_1(\underline{\mathbf{v}},K)|\underline{\mathbf{v}},\mathbf{H}) \quad (47)$$
$$\leq \log P - h(K|\underline{\mathbf{v}},\mathbf{H}) + o(\log P) \quad (48)$$
$$= \log P - h(K) + o(\log P) \quad (49)$$
$$= \log P - \log P + o(\log P) = o(\log P) \quad (50)$$

where (46) follows from the Markov chain $(v_1,v_2) \to L_1(v_1,v_2,K) \to \mathbf{Y}$. Thus, for the first user, a secrecy rate of $2\log P - o(\log P)$ is achievable per block (which itself contains 3 channel uses). This means that a s.d.o.f. of $\frac{2}{3}$ is achievable for receiver 1. Similarly, a s.d.o.f. of $\frac{2}{3}$ is achievable for the second user, thus showing the achievability of a sum s.d.o.f. of $\frac{4}{3}$ for the system.

V. Conclusions

We studied the two-user MISO BCCM and characterized its s.d.o.f. region with alternating CSIT. The achievability of the s.d.o.f. region is established by first identifying several constituent schemes and then time-sharing between them. We highlight the synergistic benefits of joint encoding across multiple CSIT states over time-sharing between their individually optimal schemes. The optimal s.d.o.f. region also quantifies the information theoretic minimal CSIT required from each user to attain a certain s.d.o.f. value. In addition, we also quantify the loss in d.o.f., as a function of the overall CSIT quality, which must be incurred for incorporating confidentiality constraints.

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] P. Mukherjee and S. Ulukus. Fading wiretap channel with no CSI anywhere. In *IEEE ISIT*, Jul. 2013.

[4] 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, Sept. 2009.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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, Sept. 2010.

[11] C. S. Vaze and M. K. Varanasi. The degrees of freedom regions of MIMO broadcast, interference, and cognitive radio channels with no CSIT. *IEEE Trans. Inf. Theory*, 58(8):5354–5374, Aug. 2012.

[12] M. A. Maddah-Ali and D. Tse. Completely stale transmitter channel state information is still useful. *IEEE Trans. Inf. Theory*, 58(7):4418–4431, Jul. 2012.

[13] 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, Sept. 2013.

[14] H. Maleki, S. A. Jafar, and S. Shamai(Shitz). Retrospective interference alignment over interference networks. *IEEE Journal of Selected Topics in Signal Processing*, 6(3):228–240, Jun. 2012.

[15] R. Tandon, M.-A. Maddah-Ali, A. Tulino, H.V. Poor, and S. Shamai. On fading broadcast channels with partial channel state information at the transmitter. In *IEEE ISWCS*, Aug. 2012.

[16] A. G. Davoodi and S. A. Jafar. Aligned image sets under channel uncertainty: Settling a conjecture by Lapidoth, Shamai and Wigger on the collapse of degrees of freedom under finite precision CSIT. Available at [arXiv:1403.1541].

[17] S. Amuru, R. Tandon, and S. Shamai. On the degrees-of-freedom of the 3-user MISO broadcast channel with hybrid CSIT. In *IEEE ISIT*, Jun. 2014.

[18] K. Mohanty and M. K. Varanasi. On the DoF region of the K-user MISO broadcast channel with hybrid CSIT. Available at [arXiv:1312.1309].

[19] 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.

[20] P. Mukherjee, R. Tandon, and S. Ulukus. MISO broadcast channels with confidential messages and alternating CSIT. In *IEEE ISIT*, June 2014.

[21] P. Mukherjee, R. Tandon, and S. Ulukus. Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT. Available at [arXiv:1502.02647].

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

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