Achievable Secure Degrees of Freedom of MISO Broadcast Channel With Alternating CSIT

Zohaib Hassan Awan†, Abdellatif Zaidi‡ and Aydin Sezgin†
†Chair of Communication Systems, Ruhr-Universität Bochum, 44780 Bochum, Germany.
‡Université Paris-Est Marne-la-Vallée, 77454 Marne-la-Vallée Cedex 2, France.

***Abstract*—We study the problem of secure transmission over a two-user Gaussian multi-input single-output (MISO) broadcast channel under the assumption that the channel to each receiver is conveyed either perfectly (P) or with delay (D) to the transmitter. Denoting S_1 and S_2 to be the channel state information at the transmitter (CSIT) of user 1 and user 2, respectively; the overall CSIT can then alternate between four states, i.e., $(S_1, S_2) \in \{P, D\}^2$. We denote $\lambda_{S_1S_2}$ be the fraction of time the state S_1S_2 occurs, and focus on the symmetric case such that $\lambda_{S_1S_2} = \lambda_{S_2S_1}$. Under these assumptions, we first consider the Gaussian MISO wiretap channel and characterize the secure degrees of freedom (SDoF). Next, we generalize this model to the two-user Gaussian MISO broadcast channel and establish an inner bound on the SDoF region. This result shows the synergistic SDoF gains of alternating CSIT and illustrates that, as opposed to encoding separately over different states, an improved SDoF region is achievable by joint encoding across these states.**

I. Introduction

We consider a two-user Gaussian MISO broadcast channel in which the transmitter is equipped with two antennas, and each receiver is equipped with a single antenna as shown in Figure 1. The transmitter wants to transmit message W_1 and W_2 to receiver 1 and receiver 2, respectively. In investigating this model we make three assumptions, namely, 1) the communication is subjected to a fast fading environment, 2) each receiver knows the perfect instantaneous CSI and also the CSI of the other receiver with a unit delay, and 3) the channel to each receiver is conveyed either perfect instantaneously (P) or with a unit delay (D) to the transmitter; thus, the CSIT configuration can alternate between four states. Furthermore, the transmitter wants to conceal the message W_1 intended to receiver 1 from receiver 2; and the message W_2, that is intended to receiver 2, from receiver 1. Thus, receiver 2 plays two roles; 1) it is an eavesdropper of message W_1 intended to receiver 1, and also 2) a legitimate receiver to the message W_2. Similarly, receiver 1 not only is an eavesdropper of message W_2 intended to receiver 2, it is also a legitimate receiver to the message W_1. We assume that both eavesdroppers are passive, i.e., they are not allowed to modify the communication. The model that we study can be seen as a special case of the one in [1] but with imposed security constraints. We consider the case of perfect secrecy and focus on the asymptotic behaviour of this network model, where SDoF captures the pertinent performance metrics.

The main contributions of this work are summarized as follows. First, we characterize the SDoF of the $(2, 1, 1)$–MISO wiretap channel with alternating CSIT. The coding scheme in this case is based on an appropriate combination of schemes developed for fixed CSIT configurations, namely, *PP*, *PD*, *DP* and *DD* states. The converse proof follows by extending the proof of [2] developed in the context of SDoF of MIMO wiretap channel with delayed CSIT to the case with alternating CSIT; and, also, borrows some elements from the converse proof of [1] established for the broadcast model with alternating CSIT by taking imposed security constraints into account. Next, we study the MISO broadcast channel with alternating CSIT as shown in Figure 1 and establish an inner bound on the SDoF region. The inner bound follows by carefully choosing the elemental coding schemes developed in [1]; and generalizes it to account for secrecy constraints. Although the optimality of the inner bound is still to be shown, this result shows the synergistic gains of alternating CSIT and illustrates that the SDoF of alternating CSIT is strictly greater than the one obtained by the combination of appropriately scaled SDoF of fixed CSIT schemes. Alternating CSIT not only provides significant gains in DoF region as previously noted in [1] in the context of two-user MISO broadcast channel, it also enlarges the *secure* DoF region of this channel model.

This work is supported by the German Research Foundation, Deutsche Forschungsgemeinschaft (DFG), Germany, under grant SE 1697/11.

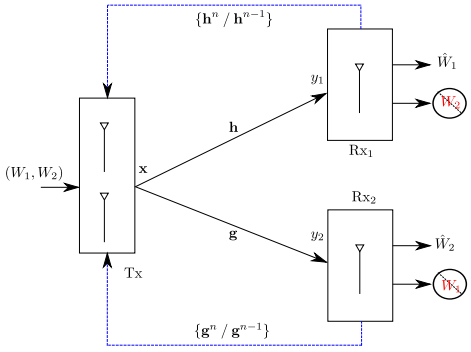

Fig. 1. Two-user MISO broadcast channel with alternating CSIT, and security constraints.

II. System Model and Definitions

We consider a two-user Gaussian MISO broadcast channel, as shown in Figure 1. In this setting, the transmitter is equipped with two transmit antennas and each of the receiver is equipped with a single antenna. The transmitter wants to reliably transmit message $W_1 \in \mathcal{W}_1 = \{1, \ldots, 2^{nR_1(P)}\}$ to receiver 1, and message $W_2 \in \mathcal{W}_2 = \{1, \ldots, 2^{nR_2(P)}\}$ to receiver 2, respectively. In doing so, the transmitter also wishes to conceal the message W_1, that is intended to receiver 1, from receiver 2; and the message W_2, that is intended to receiver 2, from receiver 1. Thus, in the considered system configuration, receiver 2 acts as

an eavesdropper on the MISO channel to receiver 1; and receiver 1 acts an eavesdropper on the MISO channel to receiver 2.

We consider a fast fading environment, and assume that each receiver knows the perfect instantaneous CSI and also the past CSI of the other receiver. The channel input-output relationship at time instant t is given by

$$\begin{aligned} y_t &= \mathbf{h}_t \mathbf{x}_t + n_{1t} \\ z_t &= \mathbf{g}_t \mathbf{x}_t + n_{2t}, \;\; t = 1, \ldots, n \end{aligned} \tag{1}$$

where $\mathbf{x} \in \mathbb{C}^{2\times 1}$ is the channel input vector, $\mathbf{h} \in \mathcal{H} \subseteq \mathbb{C}^{1\times 2}$ is the channel vector connecting receiver 1 to the transmitter and $\mathbf{g} \in \mathcal{G} \subseteq \mathbb{C}^{1\times 2}$ is the channel vector connecting receiver 2 to the transmitter, respectively; and n_i is assumed to be independent and identically distributed (i.i.d.) white Gaussian noise, with $n_i \sim \mathcal{CN}(0,1)$ for $i = 1, 2$. The channel input is subjected to block power constraints, $\sum_{t=1}^{n} \mathbb{E}[\|\mathbf{x}_t\|^2] \leq nP$. For ease of exposition, we denote $\mathbf{S}_t = \begin{bmatrix} \mathbf{h}_t \\ \mathbf{g}_t \end{bmatrix}$ as the channel state matrix and $\mathbf{S}^{t-1} = \{\mathbf{S}_1, \ldots, \mathbf{S}_{t-1}\}$ denotes the collection of channel state matrices over the past $(t-1)$ symbols, respectively. For convenience, we set $\mathbf{S}^0 = \emptyset$. We assume that, at each time instant t, the channel state matrix $\mathbf{S}_t$ is full rank almost surely. At each time instant t, the past states of the channel matrix $\mathbf{S}^{t-1}$ are known to all terminals. However the instantaneous state $\mathbf{h}_t$ is known only to receiver 1, and the instantaneous state $\mathbf{g}_t$ is known only to receiver 2.

Communication over the wireless channel is particularly sensitive to the quality of CSIT. Although, there are numerous forms of CSIT, in this setting we focus our attention to two of the following fundamental aspects.

1) **Perfect CSIT**, corresponds to those instances in which transmitter has perfect knowledge of the instantaneous channel state information. We denote these states by 'P'.
2) **Delayed CSIT**, corresponds to those instances in which at time t, transmitter has perfect knowledge of *only* the past $(t-1)$ channel states. Also, we assume that at time instant t the current channel state is independent of the past $(t-1)$ channel states. We denote these states by 'D'.

Let S_1 denote the CSIT state of user 1 and S_2 denote the CSIT state of user 2, respectively. Then, based on the availability of the CSIT, the model that we study (1) belongs to any of the four states, $(S_1, S_2) \in \{P, D\}^2$. We denote $\lambda_{S_1S_2}$ be the fraction of time state S_1S_2 occurs, such that

$$\sum_{(S_1,S_2)\in\{P,D\}^2} \lambda_{S_1S_2} = 1. \tag{2}$$

Also, due to the symmetry of problem as reasoned in [1], in this work we assume that $\lambda_{PD} = \lambda_{DP}$, i.e., the fraction of time spent in state PD and DP are equal.

Definition 1: A code for the Gaussian two-user $(2,1,1)$–MISO broadcast channel with alternating CSIT $(\lambda_{S_1S_2})$ consists of sequence of stochastic encoders at the transmitter,

$$\begin{aligned} \{\phi_{1t} &: \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}^t \longrightarrow \mathcal{X}_1 \times \mathcal{X}_2\}_{t=1}^{\lceil n\lambda_{PP}\rceil} \\ \{\phi_{2t} &: \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}^{t-1} \longrightarrow \mathcal{X}_1 \times \mathcal{X}_2\}_{t=1}^{\lceil n\lambda_{DD}\rceil} \\ \{\phi_{3t} &: \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}^{t-1} \times \mathcal{H}_t \longrightarrow \mathcal{X}_1 \times \mathcal{X}_2\}_{t=1}^{\lceil n\lambda_{PD}\rceil} \\ \{\phi_{4t} &: \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}^{t-1} \times \mathcal{G}_t \longrightarrow \mathcal{X}_1 \times \mathcal{X}_2\}_{t=1}^{\lceil n\lambda_{DP}\rceil} \end{aligned} \tag{3}$$

where the messages W_1 and W_2 are drawn uniformly over the sets $\mathcal{W}_1$ and $\mathcal{W}_2$, respectively; and two decoding functions at the receivers,

$$\begin{aligned} \psi_1 &: \mathcal{Y}^n \times \mathcal{S}^{n-1} \times \mathcal{H}_n \longrightarrow \hat{\mathcal{W}}_1 \\ \psi_2 &: \mathcal{Z}^n \times \mathcal{S}^{n-1} \times \mathcal{G}_n \longrightarrow \hat{\mathcal{W}}_2. \end{aligned} \tag{4}$$

Definition 2: A rate pair $(R_1(P), R_2(P))$ is said to be achievable if there exists a sequence of codes such that,

$$\limsup_{n\to\infty} \Pr\{\hat{W}_i \neq W_i | W_i\} = 0, \quad \forall \; i \in \{1, 2\}. \tag{5}$$

Definition 3: A SDoF pair (d_1, d_2) is said to be achievable if there exists a sequence of codes satisfying following,

1) Reliability condition:

$$\limsup_{n\to\infty} \Pr\{\hat{W}_i \neq W_i | W_i\} = 0, \qquad \forall \; i \in \{1, 2\}, \tag{6}$$

2) Perfect secrecy condition:

$$\begin{aligned} \limsup_{n\to\infty} \frac{I(W_2; y^n, \mathbf{S}^n)}{n} = 0, \\ \limsup_{n\to\infty} \frac{I(W_1; z^n, \mathbf{S}^n)}{n} = 0, \end{aligned} \tag{7}$$

3) and Communication rate condition:

$$\lim_{P\to\infty} \liminf_{n\to\infty} \frac{\log|\mathcal{W}_i(n,P)|}{n \log P} \geq d_i, \quad \forall \; i \in \{1, 2\} \tag{8}$$

at both receivers.

Definition 4: We define the secure degrees of freedom (SDoF) region, $\mathcal{C}_{\text{SDoF}}(\lambda_{S_1S_2})$, of the MISO broadcast channel as the set of all achievable non-negative pairs (d_1, d_2).

Due to the space limitations, the proofs in this work are only outlined or omitted. Detailed proofs and equivocation analysis are provided in [3].

III. SDoF of MISO wiretap channel with alternating CSIT

The following theorem characterizes the SDoF of the MISO wiretap channel with alternating CSIT.

Theorem 1: The SDoF of the (2,1,1)–MISO wiretap channel with alternating CSIT $(\lambda_{S_1S_2})$ is given by

$$d_s(\lambda_{S_1S_2}) = 1 - \frac{\lambda_{DD}}{3}. \tag{9}$$

Proof: We provide the achievability and the converse proof in Appendix A. □

Remark 1: The outer bound generalizes the converse proof of [2] established in the context of SDoF of MIMO wiretap channel with delayed CSIT to the case with alternating CSIT; and, also, uses elements from the converse proof of [1] established for the two-user broadcast channel with alternating CSIT by taking imposed security constraints into account. Note that, if delayed CSI of both receivers is conveyed to the transmitter, i.e., $\lambda_{DD} := 1$, the outer bound recovers the SDoF of MISO wiretap channel with delayed CSI [2, Theorem 1].

The achievability in Theorem 1 follows by appropriately combining several encoding schemes. It is interesting to note that, any given fixed CSIT scheme can be completely alternated by another encoding scheme; for example, encoding scheme using DD state can be completely alternated by using either of PD, DP or PP states, $\frac{2}{3}$-rd fraction of time. We note that, for the MISO wiretap model the results established in Theorem 1 also holds for the *asymmetric* CSIT configuration where, $\lambda_{PD} \neq \lambda_{DP}$.

IV. SDoF of MISO broadcast channel with alternating CSIT

In this section, before proceeding to state our result on the general model (1) with alternating CSIT, we recall some of the known results in related settings. Khisti *et al.* in [4] study the Gaussian MIMO wiretap channel in which perfect CSI of legitimate receiver and eavesdropper is available at the transmitter and establish the secrecy capacity as well as the SDoF. In [5], Liu *et al.* generalize the model in [4] to the broadcast setting and characterize the secrecy capacity region. For the two-user (2,1,1)–MISO broadcast channel the optimal SDoF is $(d_1, d_2) = (1, 1)$. Yang *et al.* [2] study the MIMO broadcast channel in which only past or delayed CSI of both receivers is conveyed to the transmitter, and characterize the SDoF region. In [6], the authors generalized the model in [2] to the MIMO-X setting with asymmetric feedback and delayed CSIT and characterize the SDoF region. However, for the two-user MISO broadcast channel with partially perfect CSIT (*PD* state) configuration, i.e., perfect CSI of one receiver and delayed CSI of the other receiver is conveyed to the transmitter, SDoF region is unknown. We first consider the $(2, 1, 1)$–MISO broadcast channel with partially perfect CSIT and establish a lower bound on the SDoF region. A trivial lower bound on the SDoF region of the two user (2,1,1)–MISO broadcast channel with partially perfect CSIT (*PD* state) is given by the set of all non-negative pairs (d_1, d_2) satisfying

$$d_1 + d_2 \leq 1. \tag{10}$$

The achievability in (10) follows from the coding scheme that we use for the proof of Theorem 1 by choosing *PD* state.

We now turn our attention to consider the MISO broadcast channel with alternating CSIT ($\lambda_{S_1S_2}$) and state our main result. For convenience, we first define the following quantity, $d_s^{\text{low}} := d_s - \frac{6\lambda_{PD}}{11}$.

The following theorem provides an inner bound on the SDoF region of the MISO broadcast channel with alternating CSIT.

Theorem 2: An inner bound on the SDoF region $\mathcal{C}_{\text{SDoF}}(\lambda_{S_1S_2})$ of the two-user (2,1,1)–MISO broadcast channel with alternating CSIT is given by the set of all non-negative pairs (d_1, d_2) satisfying

$$d_1 \leq d_s \tag{11a}$$

$$d_2 \leq d_s \tag{11b}$$

$$\frac{d_1}{d_s^{\text{low}}} + \frac{d_2}{2} \leq 1 + \frac{\lambda_{PP} + \lambda_{PD}}{2} \tag{11c}$$

$$\frac{d_1}{2} + \frac{d_2}{d_s^{\text{low}}} \leq 1 + \frac{\lambda_{PP} + \lambda_{PD}}{2}. \tag{11d}$$

Proof: The achievability proof is provided in [3]. □

Remark 2: The region established in Theorem 2 reduces to the DoF region of the MISO broadcast channel with alternating CSIT and no security constraints in [1, Theorem 1] by setting $d_s = d_s^{\text{low}} := 1$ in (11).

Figure 2 sheds light on the benefits of alternation between the states and shows the SDoF regions of *DD*, partially perfect CSIT (*PD* state), *PP* states and the region obtained by alternation between *PD* and *DP* states. Although the optimality of the inner bound is still to be shown, from Fig. 2 it can be easily seen that, alternation between *PD* and *DP* states enlarges the SDoF region in comparison to using only *PD* state. This gain highlights the fact that, as opposed to encoding separately over different states, by encoding jointly across these states an improved SDoF region is achievable.

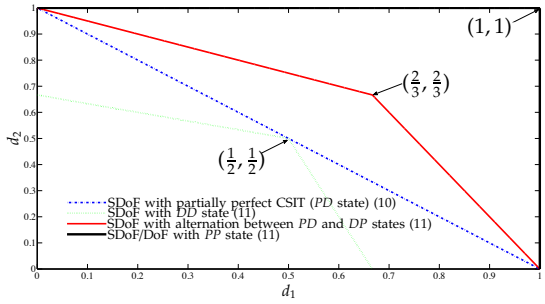

Fig. 2. Achievable SDoF region of $(2, 1, 1)$–MISO broadcast channel with alternating CSIT.

V. Coding Scheme

We now provide an outline of the elemental encoding schemes that provide the main ingredients to establish the inner bound of Theorem 2. The coding schemes, that we construct in this section, can be seen as an extension of the one established by Tandon *et al.* in the context of MISO broadcast channel with alternating CSIT [1], by taking security constraints into account.

A. Coding scheme achieving 2-SDoF

The following scheme achieves 2-SDoF.

- S^2 – using *PP* state, $(d_1, d_2) = (1, 1)$ is achievable.

Due to the availability of perfect CSI of both receivers, transmitter can zero-force the information leaked to unintended receiver. Thus, it can be readily shown that one symbol is securely transmitted to each receiver in a single timeslot, yielding 1-SDoF at each receiver.

B. Coding scheme achieving 1-SDoF

The following scheme achieves 1-SDoF.

- S^1 – using *DD* state, $(d_1, d_2) = (\frac{1}{2}, \frac{1}{2})$ is achievable.

For the case in which delayed CSI of both receivers is conveyed to the transmitter, $(d_1, d_2) = (\frac{1}{2}, \frac{1}{2})$ SDoF is achievable. The coding scheme in this case is established in [2] and is omitted for brevity.

C. Coding schemes achieving 4/3-SDoF

The following schemes achieve 4/3 SDoF.

1) $S_1^{4/3}$ – using *DP*, *PD* state for $(\frac{1}{2}, \frac{1}{2})$ fraction of time, $(d_1, d_2) = (\frac{2}{3}, \frac{2}{3})$ SDoF is achievable.
2) $S_2^{4/3}$ – using *DD*, *DP*, *PD* state for $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ fraction of time, $(d_1, d_2) = (\frac{2}{3}, \frac{2}{3})$ SDoF is achievable.

1) $S_1^{4/3}$ — Coding scheme using DP and PD states: In the coding scheme that follows, we highlight the benefits of alternation between the states. We now show that by using *PD* and *DP* state, $(d_1, d_2) = (\frac{2}{3}, \frac{2}{3})$ SDoF is achievable. Transmitter wants to transmit four symbols (v_1, v_2, v_3, v_4) to receiver 1 and wishes to conceal it from receiver 2; and four symbols (w_1, w_2, w_3, w_4) to receiver 2 and wishes to conceal it from receiver 1, respectively. The

communication takes place in six phases, each comprising of only one time slot. In this scheme, transmitter alternate between different states and choose *DP* at $t = 1, 3, 5$, and *PD* at $t = 2, 4, 6$, respectively. In the first phase transmitter chooses *DP* state and injects artificial noise, $\mathbf{u} = [u_1, u_2]^T$. The channel input-output relationship is given by

$$y_1 = \mathbf{h}_1 \mathbf{u}, \tag{12a}$$

$$z_1 = \mathbf{g}_1 \mathbf{u}. \tag{12b}$$

At the end of Phase 1, the past CSI of receiver 1 is conveyed to the transmitter. In the second phase, utilizing the leverage provided by the alternating CSIT model, transmitter switches from *DP* to *PD* state and sends $\tilde{\mathbf{v}} := [v_1, v_2]^T$ along with a linear combination of channel output y_1 of receiver 1 during the first phase. Due to the availability of past CSI of receiver 1 ($\mathbf{h}_1$) in phase 1 and since the transmitter already knows $\mathbf{u}$, it can easily re-construct the channel output y_1. During this phase, transmitter sends

$$\mathbf{x}_2 = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} + \begin{bmatrix} y_1 \\ \phi \end{bmatrix}. \tag{13}$$

At the end of phase 2, the channel input-output relationship is given by

$$y_2 = \mathbf{h}_2 \tilde{\mathbf{v}} + h_{21} y_1, \tag{14a}$$

$$z_2 = \underbrace{\mathbf{g}_2 \tilde{\mathbf{v}} + g_{21} y_1}_{\text{interference}}. \tag{14b}$$

At the end of phase 2, receiver 2 feeds back the delayed CSI to the transmitter. Since receiver 1 knows the CSI ($\mathbf{h}_2$) and also the channel output y_1 from Phase 1, it subtracts out the contribution of y_1 from the channel output y_2, to obtain one equation with two unknowns ($\tilde{\mathbf{v}} := [v_1, v_2]^T$). Thus, receiver 1 requires one extra equation to successfully decode the intended variables, being available as interference (side information) at receiver 2.

In the third phase, the transmitter alternate from *PD* to *DP* state and sends $\tilde{\mathbf{w}} := [w_1, w_2]^T$ and v_3 along with a linear combination of channel output z_1 of receiver 2 during the first phase. In phase 3, perfect CSI of receiver 2 ($\mathbf{g}_3$) at transmitter is utilized in two ways, 1) it zero-forces the interference at receiver 2 being caused by symbol v_3, and in doing so 2) it also secures symbol v_3 which is intended to receiver 1, being eavesdropped by receiver 2. During this phase, transmitter sends

$$\mathbf{x}_3 = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ \phi \end{bmatrix} + \mathbf{b}_1 v_3, \tag{15}$$

where $\mathbf{b}_1 \in \mathbb{C}^{2\times 1}$ denote the precoding vector chosen such that $\mathbf{g}_3 \mathbf{b}_1 = 0$. At the end of phase 3, the channel input-output relationship is given by

$$y_3 = \underbrace{\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1}_{\text{interference}} + \mathbf{h}_3 \mathbf{b}_1 v_3, \tag{16a}$$

$$z_3 = \mathbf{g}_3 \tilde{\mathbf{w}} + g_{31} z_1. \tag{16b}$$

At the end of phase 3, receiver 1 feeds back the delayed CSI to the transmitter. Since receiver 2 knows the CSI ($\mathbf{g}_3$) and also the channel output z_1 from Phase 1, it subtracts out the contribution of z_1 from the channel output z_3, to obtain one equation with two unknowns ($\tilde{\mathbf{w}} := [w_1, w_2]^T$). Thus, it requires one extra equation to successfully decode the intended variables being available as interference or side information at receiver 1. Receiver 1 gets the intended symbol v_3 embedded in with some interference ($\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1$) from the transmitter. If this interference can be conveyed to the receiver 1, it can then subtracts out the interference's contribution from y_3 and decode v_3 through channel inversion.

At the end of phase 3, due to availability of delayed CSI ($\mathbf{g}_2, \mathbf{h}_3$), transmitter can learn the interference at receiver 2 in phase 2 and at receiver 1 in phase 3, respectively. In the fourth phase, transmitter switches from *DP* to *PD* state and sends the interference ($\mathbf{g}_2 \tilde{\mathbf{v}} + g_{21} y_1$) at receiver 2 during the second phase and fresh information w_3. During this phase, transmitter sends

$$\mathbf{x}_4 = \begin{bmatrix} \mathbf{g}_2 \tilde{\mathbf{v}} + g_{21} y_1 \\ \phi \end{bmatrix} + \mathbf{b}_2 w_3, \tag{17}$$

where $\mathbf{b}_2 \in \mathbb{C}^{2\times 1}$ denote the precoding vector chosen such that $\mathbf{h}_4 \mathbf{b}_2 = 0$. At the end of phase 4, the channel input-output relationship is given by

$$y_4 = h_{41}(\mathbf{g}_2 \tilde{\mathbf{v}} + g_{21} y_1), \tag{18a}$$

$$z_4 = g_{41}(\mathbf{g}_2 \tilde{\mathbf{v}} + g_{21} y_1) + \mathbf{g}_4 \mathbf{b}_2 w_3. \tag{18b}$$

At the end of phase 4, receiver 1 subtracts out the contribution of y_1 from the channel outputs (y_2, y_4) and decode (v_1, v_2) through channel inversion. Similarly, since receiver 2 knows the CSI and z_2 from phase 2, it first subtracts out the contribution of z_2 from the channel output z_4 and decode w_3.

In the fifth phase, transmitter switches from *PD* to *DP* state and sends the interference ($\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1$) at receiver 1 during phase 3 and fresh information v_4 to receiver 1. During this phase, transmitter sends

$$\mathbf{x}_5 = \begin{bmatrix} \mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1 \\ \phi \end{bmatrix} + \mathbf{b}_3 v_4, \tag{19}$$

where $\mathbf{b}_3 \in \mathbb{C}^{2\times 1}$ denote the precoding vector chosen such that $\mathbf{g}_5 \mathbf{b}_3 = 0$. At the end of phase 5, the channel input-output relationship is given by

$$y_5 = h_{51}(\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1) + \mathbf{h}_5 \mathbf{b}_3 v_4, \tag{20a}$$

$$z_5 = g_{51}(\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1). \tag{20b}$$

At the end of phase 5, receiver 2 subtracts out the contribution of z_1 from the channel outputs (z_3, z_5) and decode (w_1, w_2) through channel inversion. Receiver 1 gets the intended symbol v_4 embedded within the same interference as in phase 3. If this interference can be conveyed to the receiver 1, it can then subtracts out the interference's contribution from y_5 and decode v_4 through channel inversion.

In the sixth phase, transmitter switches from *DP* to *PD* state and sends interference ($\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1$) at receiver 1 during phase 3 with fresh information w_4 for receiver 2. During this phase transmitter sends

$$\mathbf{x}_6 = \begin{bmatrix} \mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1 \\ \phi \end{bmatrix} + \mathbf{b}_4 w_4, \tag{21}$$

where $\mathbf{b}_4 \in \mathbb{C}^{2\times 1}$ denote the precoding vector chosen such that $\mathbf{h}_6 \mathbf{b}_4 = 0$. At the end of phase 6, the channel input-output relationship is given by

$$y_6 = h_{61}(\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1), \tag{22a}$$

$$z_6 = g_{61}(\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1) + \mathbf{g}_6 \mathbf{b}_4 w_4. \tag{22b}$$

At the end of phase 6, since receiver 1 knows the CSI and by using y_6, subtracts out the contribution of $(\mathbf{h}_3\tilde{\mathbf{w}} + h_{31}z_1)$ from the channel outputs (y_3, y_5) and decode v_3 and v_4 through channel inversion. Similarly, since receiver 2 knows the CSI and also z_5, it can then subtracts out the contribution of $(\mathbf{h}_3\tilde{\mathbf{w}} + h_{31}z_1)$ from channel output z_6 and decode w_4 through channel inversion.

The complete security analysis of this scheme is provided in [3]. Then, through straightforward algebra, it can be easily seen that 4 symbols are securely transmitted to each receiver over a total of 6 time slots, thus yielding $(d_1, d_2) = (2/3, 2/3)$ SDoF.

The coding scheme $S_2^{4/3}$ follows along the same line as in $S_1^{4/3}$ and is provided in [3].

Appendix A
Proof of Theorem 1

Achievability. We first digress to construct some elemental coding schemes which form the basic building blocks to establish the achievability in Theorem 1. These schemes have some connections to the one in section V and so we outline it briefly.

S^1—***Coding schemes achieving*** 1-***SDoF:*** For PP, and DP state 1-SDoF is achievable. Due to the availability of perfect CSI of the unintended receiver (wire-taper), the transmitter can zero-force the information leaked to it. Thus, it can be readily shown that one symbol is securely transmitted to the legitimate receiver in a single timeslot, yielding 1-SDoF.

For the case in which PD state occurs, the transmitter transmits one confidential message (v) along with the artificial noise (u). In this state, perfect CSI of the legitimate receiver is utilize to zero force the injected artificial noise. The communication takes place in only one time slot and transmitter sends

$$\mathbf{x} = \begin{bmatrix} v \\ \phi \end{bmatrix} + \mathbf{b}u, \tag{23}$$

where $\mathbf{b} \in \mathbb{C}^{2\times 1}$ denote the precoding vector chosen such that $\mathbf{h}_1\mathbf{b} = 0$. The channel input-output relationship is given by

$$y = h_{11}v, \tag{24a}$$
$$z = g_{11}v + \mathbf{g}_1\mathbf{b}u. \tag{24b}$$

Receiver 1 knows the CSI ($\mathbf{h}$) and can easily decode v via channel inversion. Receiver 2 gets the confidential message v embedded in artificial noise and is unable to decode it. Then, following security analysis similar to in [3], it can be easily shown that 1 symbol is securely transmitted to the legitimate receiver over 1 timeslot yielding 1-SDoF.

$S^{2/3}$—***Coding scheme achieving*** 2/3-***SDoF:*** For the case in which DD state occurs, 2/3 SDoF is achievable. The coding scheme in this case is similar to the one in [2, Section IV-B-2] for the MIMO wiretap channel with delayed CSIT from both receivers.

Then, the achievable SDoF follows by choosing PP, PD, DP and DD states, λ_{PP}, λ_{PD}, λ_{DP} and λ_{DD} fractions of time, respectively, yields $\lambda_{PP}.(1) + \lambda_{PD}.(1) + \lambda_{DP}.(1) + \lambda_{DD}.(\frac{2}{3}) = 1 - \frac{\lambda_{DD}}{3}$.

Converse Proof. The converse borrows elements from the proof established in the context of MIMO wiretap channel with delayed CSIT [2] and the one established in the context of MISO broadcast channel with alternating CSIT [1]. For convenience, we denote the channel output at each receiver as $y^n := (y^n_{PP}, y^n_{PD}, y^n_{DP}, y^n_{DD})$, and $z^n := (z^n_{PP}, z^n_{PD}, z^n_{DP}, z^n_{DD})$, where $y^n_{S_1S_2}(z^n_{S_1S_2})$ denotes the part of channel output at receiver 1 (receiver 2), when $(S_1S_2) \in \{P, D\}^2$ channel state occurs. We begin the proof as follows.

$$\begin{aligned}
nR_e &= H(W|z^n, \mathbf{S}^n) \\
&= H(W|\mathbf{S}^n) - I(W; z^n|\mathbf{S}^n) \\
&= I(W; y^n|\mathbf{S}^n) + H(W|y^n, \mathbf{S}^n) - I(W; z^n|\mathbf{S}^n) \\
&\overset{(a)}{\leq} I(W; y^n|\mathbf{S}^n) - I(W; z^n|\mathbf{S}^n) + n\epsilon_n \\
&= h(y^n_{PP}, y^n_{PD}, y^n_{DP}, y^n_{DD}|\mathbf{S}^n) - h(y^n_{PP}, y^n_{PD}, y^n_{DP}, y^n_{DD}|W, \mathbf{S}^n) \\
&\quad - I(W; z^n_{DD}|\mathbf{S}^n) - I(W; z^n_{PP}, z^n_{PD}, z^n_{DP}|z^n_{DD}, \mathbf{S}^n) + n\epsilon_n \\
&\leq h(y^n_{PP}|\mathbf{S}^n) + h(y^n_{PD}|\mathbf{S}^n) + h(y^n_{DP}|\mathbf{S}^n) + h(y^n_{DD}|\mathbf{S}^n) - h(y^n_{DD}|W, \mathbf{S}^n) \\
&\quad - h(y^n_{PP}, y^n_{PD}, y^n_{DP}|y^n_{DD}, W, \mathbf{S}^n) - I(W; z^n_{DD}|\mathbf{S}^n) \\
&\quad - I(W; z^n_{PP}, z^n_{PD}, z^n_{DP}|z^n_{DD}, \mathbf{S}^n) + n\epsilon_n \\
&\overset{(b)}{\leq} h(y^n_{PP}|\mathbf{S}^n) + h(y^n_{PD}|\mathbf{S}^n) + h(y^n_{DP}|\mathbf{S}^n) + h(y^n_{DD}|\mathbf{S}^n) - h(y^n_{DD}|W, \mathbf{S}^n) \\
&\quad \underbrace{- h(y^n_{PP}, y^n_{PD}, y^n_{DP}|y^n_{DD}, W, \mathbf{x}^n, \mathbf{S}^n)}_{\geq no(\log(P))} - I(W; z^n_{DD}|\mathbf{S}^n) + n\epsilon_n \\
&\overset{(c)}{\leq} h(y^n_{PP}|\mathbf{S}^n) + h(y^n_{PD}|\mathbf{S}^n) + h(y^n_{DP}|\mathbf{S}^n) + I(W; y^n_{DD}|\mathbf{S}^n) \\
&\quad - I(W; z^n_{DD}|\mathbf{S}^n) + n\epsilon_n \\
&\leq n\log(P)(\lambda_{PP} + \lambda_{PD} + \lambda_{DP}) + I(W; y^n_{DD}|\mathbf{S}^n) - I(W; z^n_{DD}|\mathbf{S}^n) + n\epsilon_n \\
&\overset{(d)}{\leq} n\log(P)(\lambda_{PP} + \lambda_{PD} + \lambda_{DP}) + \frac{2\lambda_{DD}}{3}n\log(P) + n\epsilon_n \\
&\overset{(e)}{=} n\log(P)(1 - \frac{\lambda_{DD}}{3}) + n\epsilon_n
\end{aligned} \tag{25}$$

where $\epsilon_n \to 0$ as $n \to \infty$; (a) follows from Fano's inequality, (b) follows from the non-negativity of $I(W; z^n_{PP}, z^n_{PD}, z^n_{DP}|z^n_{DD}, \mathbf{S}^n)$ and the fact that conditioning reduces entropy, (c) follows because $(y^n_{PP}, y^n_{PD}, y^n_{DP})$ can be obtained within noise distortion form $(\mathbf{x}^n, \mathbf{S}^n)$, (d) follows by exploiting the properties of entropy symmetry of channel output in [2, Property 2] for the MIMO wiretap channel with delayed CSI; and (e) follows by definition (2).

References

[1] R. Tandon, S. A. Jafar, S. Shamai (Shitz), and H. V. Poor, "On the synergistic benefits of alternating CSIT for the MISO broadcast channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4106–4128, 2013.

[2] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai, "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5244–5256, 2013.

[3] Z. H. Awan, A. Zaidi, and A. Sezgin, "On secure degrees of freedom of MISO broadcast channel with alternating CSIT," *in preparation for submission*, 2014.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[5] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, 2010.

[6] A. Zaidi, Z. Awan, S. Shamai (Shitz), and L. Vandendorpe, "Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSIT," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1760–1774, 2013.