

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.

zohaib.awan@rub.de, abdellatif.zaidi@univ-mlv.fr, aydin.sezgin@rub.de

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 $\lambda_{S_1 S_2}$ be the fraction of time the state $S_1 S_2$ occurs, and focus on the symmetric case such that $\lambda_{S_1 S_2} = \lambda_{S_2 S_1}$. 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, a higher SDoF region is achievable by joint encoding across these states.

I. INTRODUCTION

Simultaneous transmission of information over a shared wireless medium emanates an important issue of interference in networks. A key resource to mitigate interference is the availability of CSIT. In literature, different multi-user networks are studied under ideal assumption of perfect channel state information (CSI) at the transmitter in [1] (and references therein), where quality of CSIT plays a major role in aligning interference in networks. Recently, a growing body of research has attracted attention to study a wide variety of two-user CSIT models, for instance, with delayed CSI in [2], [3], no CSIT in [4], [5] and with mixed CSIT (perfect delayed CSI along with imperfect instantaneous CSI) in [6], all from degrees of freedom (DoF) perspective. In all these models it is assumed that symmetric CSI is available at the transmitter, i.e., either perfect, delayed or no CSI is conveyed by *both* receivers. In [7], Tandon *et al.* studied a two-user broadcast channel with asymmetric CSI conveyed to the transmitter. In this model, the channel to one receiver is instantaneously available at the transmitter, while the channel to the other receiver is conveyed with certain delay. The authors call this model as partially perfect CSIT and characterize the DoF region. Due to the random fluctuations in the wireless medium, it becomes difficult for the receivers to convey the same quality of CSI over time. In another related work [8], Tandon *et al.* studied the two-user broadcast channel by taking the time varying nature of CSIT into account. The authors assumed that the CSI conveyed by *both* receivers can vary over time, and characterize the DoF region.

In this paper, we consider a two-user Gaussian MISO broadcast channel in which the transmitter is equipped with two antennas, and each of the 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,

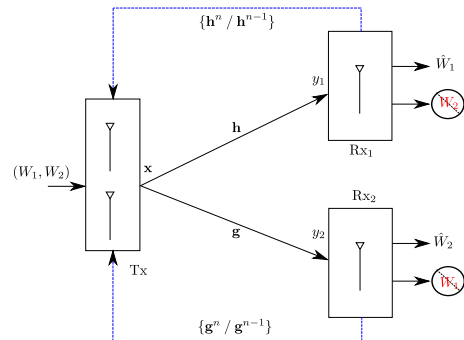


Fig. 1. Two-user MISO broadcast channel with alternating CSIT, and security constraints.

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 [8] 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 [9] 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 [8] 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 [8]; and generalizes it to account for secrecy constraints. 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 scaling SDoF of fixed CSIT schemes. Alternating CSIT not only provides significant gains in DoF region as previously noted in [8] in the context of two-user MISO broadcast channel, it also increases the *secure* DoF region of this channel model.

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 $W_1 \in \mathcal{W}_1 = \{1, \dots, 2^{nR_1(P)}\}$ to receiver 1, and message $W_2 \in \mathcal{W}_2 = \{1, \dots, 2^{nR_2(P)}\}$ 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

$$\begin{aligned} y_t &= \mathbf{h}_t \mathbf{x}_t + n_{1t} \\ z_t &= \mathbf{g}_t \mathbf{x}_t + n_{2t}, \quad t = 1, \dots, n \end{aligned} \quad (1)$$

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 $\mathbf{S}^{t-1} = \{\mathbf{S}_1, \dots, \mathbf{S}_{t-1}\}$ 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 denotes the CSIT state of user 1 and S_2 denotes 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,

$$(S_1, S_2) \in \{P, D\}^2. \quad (2)$$

We denote $\lambda_{S_1 S_2}$ be the fraction of time state $S_1 S_2$ occurs, such that

$$\sum_{(S_1, S_2) \in \{P, D\}^2} \lambda_{S_1 S_2} = 1. \quad (3)$$

Also, due to the symmetry of problem as reasoned in [8], 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 $(\lambda_{S_1 S_2})$ consists of se-

quence of stochastic encoders at the transmitter,

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

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,

$$\begin{aligned} \psi_1 : \mathcal{Y}^n \times \mathcal{S}^{n-1} \times \mathcal{H}_n &\longrightarrow \hat{\mathcal{W}}_1 \\ \psi_2 : \mathcal{Z}^n \times \mathcal{S}^{n-1} \times \mathcal{G}_n &\longrightarrow \hat{\mathcal{W}}_2. \end{aligned} \quad (5)$$

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,

$$\limsup_{n \rightarrow \infty} \Pr\{\hat{W}_i \neq W_i | W_i\} = 0, \quad \forall i \in \{1, 2\}. \quad (6)$$

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:

$$\limsup_{n \rightarrow \infty} \Pr\{\hat{W}_i \neq W_i | W_i\} = 0, \quad \forall i \in \{1, 2\}, \quad (7)$$

- 2) Perfect secrecy condition:

$$\begin{aligned} \limsup_{n \rightarrow \infty} \frac{I(W_2; \mathbf{y}^n, \mathbf{S}^n)}{n} &= 0, \\ \limsup_{n \rightarrow \infty} \frac{I(W_1; \mathbf{z}^n, \mathbf{S}^n)}{n} &= 0, \end{aligned} \quad (8)$$

- 3) and Communication rate condition:

$$\lim_{P \rightarrow \infty} \liminf_{n \rightarrow \infty} \frac{\log |\mathcal{W}_i(n, P)|}{n \log P} \geq d_i, \quad \forall i \in \{1, 2\} \quad (9)$$

at both receivers.

Definition 4: We define the secure degrees of freedom (SDoF) region, $\mathcal{C}_{\text{SDoF}}(\lambda_{S_1 S_2})$, 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 [10].

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 $(\lambda_{S_1 S_2})$ is given by

$$d_s(\lambda_{S_1 S_2}) = 1 - \frac{\lambda_{DD}}{3}. \quad (10)$$

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

Remark 1: The outer bound generalizes the converse proof of [9] 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 [8] 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 [9, 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, PD , DP or PP states, $\frac{2}{3}$ -rd fraction of time.

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 [11] 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 [12], Liu *et al.* generalize the model in [11] 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.* [9] 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 [13], the authors generalized the model in [9] 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

$$d_1 + d_2 \leq 1. \quad (11)$$

The achievability in (11) 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 $(\lambda_{S_1}, \lambda_{S_2})$ and state our main result. For convenience, we first define the following quantity

$$d_s^{\text{low}} = d_s - \frac{6\lambda_{PD}}{11}. \quad (12)$$

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 $\mathcal{C}_{\text{SDoF}}(\lambda_{S_1}, \lambda_{S_2})$ 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

$$d_1 \leq d_s \quad (13a)$$

$$d_2 \leq d_s \quad (13b)$$

$$\frac{d_1}{d_s^{\text{low}}} + \frac{d_2}{2} \leq 1 + \frac{\lambda_{PP} + \lambda_{PD}}{2} \quad (13c)$$

$$\frac{d_1}{2} + \frac{d_2}{d_s^{\text{low}}} \leq 1 + \frac{\lambda_{PP} + \lambda_{PD}}{2}. \quad (13d)$$

Proof: The achievability proof is provided in [10]. \square

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 [8, Theorem 1] by setting $d_s = d_s^{\text{low}} := 1$ in (13).

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. 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 higher SDoF region is achievable.

Remark 3 (Synergistic Gains in Asymmetric Configurations): In Theorem 2, the inner bound provides synergistic benefits of alternating CSIT under the symmetric assumption of $\lambda_{PD} = \lambda_{DP}$.

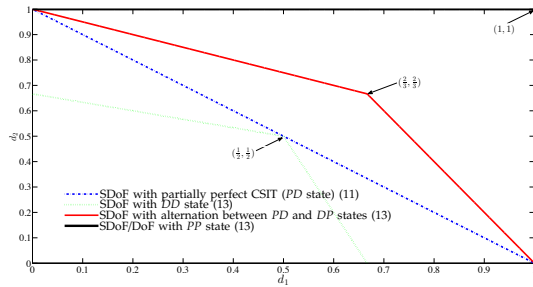


Fig. 2. Achievable SDoF region of (2, 1, 1)-MISO broadcast channel with alternating CSIT.

We note that this gain in SDoF region is not restricted to symmetric setting and can also be appreciated under the asymmetric setting, i.e., $\lambda_{PD} \neq \lambda_{DP}$. We consider a simple example in which states PD and DP occurs $\lambda_{PD} = \frac{1}{6}$ and $\lambda_{DP} = \frac{2}{6}$ fractions of time, respectively. From (11), it is easy to note that the achievable SDoF of each of these states is 1. However, as previously noted in [8] for a similar model without secrecy constraints, by synergistically using these states one can obtain higher DoF gains with secrecy constraints as well; for instance, by completely using scheme $S_1^{4/3}$ (which is based on synergistically using state PD and DP) $\frac{1}{3}$ -rd fraction of time and using DP state in the remaining fraction of time, we get

$$\text{SDoF} = \underbrace{\frac{1}{3} \times \left(\frac{4}{3}\right)}_{S_1^{4/3}} + \underbrace{\frac{2}{3} \times (1)}_{DP} = \frac{10}{9} \geq 1 \quad (14)$$

which shows the benefits of alternating CSIT under asymmetric configurations.

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 [8], 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 [9] 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, $(d_1, d_2) = (\frac{4}{3}, \frac{2}{3})$ 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, $(d_1, d_2) = (\frac{4}{3}, \frac{2}{3})$ 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

$$y_1 = \mathbf{h}_1 \mathbf{u}, \quad (15a)$$

$$z_1 = \mathbf{g}_1 \mathbf{u}. \quad (15b)$$

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

$$\mathbf{x}_2 = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} + \begin{bmatrix} y_1 \\ \phi \end{bmatrix}. \quad (16)$$

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

$$y_2 = \mathbf{h}_2 \tilde{\mathbf{v}} + h_{21} y_1, \quad (17a)$$

$$z_2 = \underbrace{\mathbf{g}_2 \tilde{\mathbf{v}} + g_{21} y_1}_{\text{interference}}. \quad (17b)$$

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

$$\mathbf{x}_3 = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ \phi \end{bmatrix} + \mathbf{b}_1 v_3, \quad (18)$$

where $\mathbf{b}_1 \in \mathbb{C}^{2 \times 1}$ denotes 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

$$y_3 = \underbrace{\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1}_{\text{interference}} + \mathbf{h}_3 \mathbf{b}_1 v_3, \quad (19a)$$

$$z_3 = \mathbf{g}_3 \tilde{\mathbf{w}} + g_{31} z_1. \quad (19b)$$

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 decodes 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

$$\mathbf{x}_4 = \begin{bmatrix} \mathbf{g}_2 \tilde{\mathbf{v}} + g_{21} y_1 \\ \phi \end{bmatrix} + \mathbf{b}_2 w_3, \quad (20)$$

where $\mathbf{b}_2 \in \mathbb{C}^{2 \times 1}$ denotes 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

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

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

At the end of phase 4, receiver 1 subtracts out the contribution of y_1 from the channel outputs (y_2, y_4) and decodes (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 decodes 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

$$\mathbf{x}_5 = \begin{bmatrix} \mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1 \\ \phi \end{bmatrix} + \mathbf{b}_3 v_4, \quad (22)$$

where $\mathbf{b}_3 \in \mathbb{C}^{2 \times 1}$ denotes 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

$$y_5 = h_{51} (\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1) + \mathbf{h}_5 \mathbf{b}_3 v_4, \quad (23a)$$

$$z_5 = g_{51} (\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1). \quad (23b)$$

At the end of phase 5, receiver 2 subtracts out the contribution of z_1 from the channel outputs (z_3, z_5) and decodes (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 decodes 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

$$\mathbf{x}_6 = \begin{bmatrix} \mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1 \\ \phi \end{bmatrix} + \mathbf{b}_4 w_4, \quad (24)$$

where $\mathbf{b}_4 \in \mathbb{C}^{2 \times 1}$ denotes 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

$$y_6 = h_{61} (\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1), \quad (25a)$$

$$z_6 = g_{61} (\mathbf{h}_3 \tilde{\mathbf{w}} + h_{31} z_1) + \mathbf{g}_6 \mathbf{b}_4 w_4. \quad (25b)$$

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 decodes 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 decodes w_4 through channel inversion.

The complete security analysis of this scheme is provided in [10]. Then, through straightforward algebra, it can be easily seen that 4 symbols are securely transmitted to each receiver over 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 lines as in $S_1^{4/3}$ and is provided in [10].

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

$$\mathbf{x} = \begin{bmatrix} v \\ \phi \end{bmatrix} + \mathbf{b}u, \quad (26)$$

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

$$y = h_{11}v \quad (27a)$$

$$z = g_{11}v + \mathbf{g}_1 \mathbf{b}u \quad (27b)$$

Receiver 1 knows the CSI (\mathbf{h}) and can easily decodes 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 [10], 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 [9, 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 $\lambda_{PP} \cdot (1) + \lambda_{PD} \cdot (1) + \lambda_{DP} \cdot (1) + \lambda_{DD} \cdot (\frac{2}{3}) = 1 - \frac{\lambda_{DD}}{3}$.

Converse Proof. The converse borrows elements from the proof established in the context of MIMO wiretap channel with delayed CSIT [9] and the one established in the context of MISO broadcast channel with alternating CSIT [8]. For convenience, we denote the channel output at each receiver as $y^n := (y_{PP}^n, y_{PD}^n, y_{DP}^n, y_{DD}^n)$, and $z^n := (z_{PP}^n, z_{PD}^n, z_{DP}^n, z_{DD}^n)$, where $y_{S_1 S_2}^n (z_{S_1 S_2}^n)$ denotes the part of channel output at receiver 1 (receiver 2), when $(S_1, S_2) \in \{P, D\}^2$ channel state occurs. We begin the proof as follows.

$$\begin{aligned} nR_e &= H(W|z^n) \\ &\stackrel{(a)}{=} H(W|z^n, \mathbf{S}^n) \\ &= H(W|\mathbf{S}^n) - I(W; z^n|\mathbf{S}^n) \\ &= I(W; y^n|\mathbf{S}^n) + H(W|y^n, \mathbf{S}^n) - I(W; z^n|\mathbf{S}^n) \\ &\stackrel{(b)}{\leq} I(W; y^n|\mathbf{S}^n) - I(W; z^n|\mathbf{S}^n) + n\epsilon_n \end{aligned}$$

$$\begin{aligned} &= h(y_{PP}^n, y_{PD}^n, y_{DP}^n, y_{DD}^n|\mathbf{S}^n) - h(y_{PP}^n, y_{PD}^n, y_{DP}^n, y_{DD}^n|W, \mathbf{S}^n) \\ &\quad - I(W; z_{DD}^n|\mathbf{S}^n) - I(W; z_{PP}^n, z_{PD}^n, z_{DP}^n|z_{DD}^n, \mathbf{S}^n) + n\epsilon_n \\ &\leq h(y_{PP}^n|\mathbf{S}^n) + h(y_{PD}^n|\mathbf{S}^n) + h(y_{DP}^n|\mathbf{S}^n) + h(y_{DD}^n|\mathbf{S}^n) - h(y_{DD}^n|W, \mathbf{S}^n) \\ &\quad - h(y_{PP}^n, y_{PD}^n, y_{DP}^n|y_{DD}^n, W, \mathbf{S}^n) - I(W; z_{DD}^n|\mathbf{S}^n) \\ &\quad - I(W; z_{PP}^n, z_{PD}^n, z_{DP}^n|z_{DD}^n, \mathbf{S}^n) + n\epsilon_n \\ &\stackrel{(c)}{\leq} \underbrace{h(y_{PP}^n|\mathbf{S}^n) + h(y_{PD}^n|\mathbf{S}^n) + h(y_{DP}^n|\mathbf{S}^n) + h(y_{DD}^n|\mathbf{S}^n) - h(y_{DD}^n|W, \mathbf{S}^n)}_{\geq n \log(P)} \\ &\quad - h(y_{PP}^n, y_{PD}^n, y_{DP}^n|y_{DD}^n, W, \mathbf{x}^n, \mathbf{S}^n) - I(W; z_{DD}^n|\mathbf{S}^n) + n\epsilon_n \\ &\stackrel{(d)}{\leq} h(y_{PP}^n|\mathbf{S}^n) + h(y_{PD}^n|\mathbf{S}^n) + h(y_{DP}^n|\mathbf{S}^n) + I(W; y_{DD}^n|\mathbf{S}^n) \\ &\quad - I(W; z_{DD}^n|\mathbf{S}^n) + n\epsilon_n \\ &\leq n \log(P) (\lambda_{PP} + \lambda_{PD} + \lambda_{DP}) + I(W; y_{DD}^n|\mathbf{S}^n) - I(W; z_{DD}^n|\mathbf{S}^n) + n\epsilon_n \\ &\stackrel{(e)}{\leq} n \log(P) (\lambda_{PP} + \lambda_{PD} + \lambda_{DP}) + \frac{2\lambda_{DD}}{3} n \log(P) + n\epsilon_n \\ &\stackrel{(f)}{=} n \log(P) (1 - \frac{\lambda_{DD}}{3}) + n\epsilon_n \quad (28) \end{aligned}$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$; (a) follows due to the independence of W and \mathbf{S}^n , (b) follows from Fano's inequality, (c) follows from the non-negativity of $I(W; z_{PP}^n, z_{PD}^n, z_{DP}^n|z_{DD}^n, \mathbf{S}^n)$ and the fact that conditioning reduces entropy, (d) follows because $(y_{PP}^n, y_{PD}^n, y_{DP}^n)$ can be obtained within noise distortion form (x^n, \mathbf{S}^n) , (e) follows by exploiting the properties of channel output symmetry as in [9, Lemma 1] for the MIMO wiretap channel with delayed CSI; and (f) follows by definition (3).

REFERENCES

- [1] S. A. Jafar, "Interference alignment — A new look at signal dimensions in a communication network," *Foundations and Trends in Communications and Information Theory*, vol. 7, no. 1, pp. 1–134, 2010.
- [2] M. A. Maddah-Ali and D. Tse, "Completely stale transmitter channel state information is still very useful," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4418–4431, Jul. 2012.
- [3] C. S. Vaze and M. K. Varanasi, "The degrees of freedom region of the two-user and certain three-user MIMO broadcast channel with delayed CSI," 2011. [Online]. Available: <http://arxiv.org/abs/1101.0306>
- [4] C. Huang, S. Jafar, S. Shamai, and S. Vishwanath, "On degrees of freedom region of MIMO networks without channel state information at transmitters," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 849–857, Feb. 2012.
- [5] 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*, vol. 58, no. 8, pp. 5354–5374, Aug. 2012.
- [6] T. Gou and S. Jafar, "Optimal use of current and outdated channel state information: Degrees of freedom of the MISO BC with mixed CSIT," *IEEE Commun. Lett.*, vol. 16, no. 7, pp. 1084–1087, Jul. 2012.
- [7] R. Tandon, M. A. Maddah-Ali, A. M. Tulino, H. V. Poor, and S. Shamai (Shitz), "On fading broadcast channels with partial channel state information at the transmitter," in *Int. Symp. on Wireless Commun. Sys.*, Paris, France, Aug. 2012, pp. 1004–1008.
- [8] 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.
- [9] 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.
- [10] Z. H. Awan, A. Zaidi, and A. Sezgin, "On secure degrees of freedom of MISO broadcast channel with alternating CSIT," 2014. [Online]. Available: <http://www6.rz.rub.de:8331/mam/pdf/proofs-isit.pdf>
- [11] 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.
- [12] 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.
- [13] 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.