On SDoF of Multi-Receiver Wiretap 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.
[‡]Mathematical and Algorithmic Sciences Lab., Huawei Technologies, 92100 Paris, France.

***Abstract*—We study the problem of secure transmission over a Gaussian multi-input single-output (MISO) two receiver channel with an external eavesdropper, under the assumption that the state of the channel which is available to each receiver is conveyed either perfectly (*P*) or with delay (*D*) to the transmitter. Denoting by S_1, S_2, and S_3 the channel state information at the transmitter (CSIT) of user 1, user 2, and eavesdropper, respectively, the overall CSIT can then alternate between eight possible states, i.e., $(S_1, S_2, S_3) \in \{P, D\}^3$. We denote by $\lambda_{S_1S_2S_3}$ the fraction of time during which the state $S_1S_2S_3$ occurs. Under these assumptions, we consider the multi-receiver setup and characterize the SDoF region of fixed hybrid states *PPD*, *PDP*, and *DDP*. We then focus our attention on the symmetric case in which $\lambda_{PDD} = \lambda_{DPD}$. For this case, we establish bounds on the SDoF region. The analysis reveals that alternating CSIT allows synergistic gains in terms of SDoF; and shows that, by opposition to encoding separately over different states, joint encoding across the states enables strictly better secure rates.**

I. Introduction

In this work, we consider a $(3, 1, 1, 1)$–two-user Gaussian MISO channel with an external eavesdropper in which the transmitter is equipped with three antennas, and each of the three receivers is equipped with a single antenna as shown in Figure 1. The transmitter wants to reliably transmit messages 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 instantaneously (*P*) or with a unit delay (*D*) to the transmitter. In both cases, it is assumed that the CSI is perfect. We assume that the eavesdropper is the part of the communication system, and in its desire to learn the information, is willing to convey its own CSI to the transmitter. Thus, the CSIT vector that is obtained at the transmitter from the two receivers and the eavesdropper can alternate among eight possible states, *PPP*, *PPD*, *PDP*, *PDD*, *DPP*, *DPD*, *DDP*, and *DDD*. Furthermore, the transmitter wants to conceal the message W_1 that is intended to receiver 1, and the message W_2 that is intended to receiver 2 from the external eavesdropper. We study this model from SDoF perspective, that measures the way how secrecy capacity scales asymptotically with logarithm of signal-to-noise ratio (SNR).

In the literature, various multi-user networks are studied under different quality of symmetric CSIT, namely perfect [1], with strictly causal (delayed) CSI in [2], [3], and with mixed CSIT (perfect delayed CSI along with imperfect instantaneous CSI) in [4], all from degrees of freedom (DoF) perspective. For the two-user MISO broadcast model with asymmetric or hybrid CSIT in [5] and later on for alternating CSIT in [6], the authors characterized the complete DoF region. By taking secrecy constraints into account in [7], the authors study the two-user MISO broadcast channel where either *P* or *D* CSI is available from both receivers to the transmitter and establish bounds on SDoF region. Recently, in [8] the authors generalized the model in [7] to a setup in which either *P*, *D* or no CSI is available from the receivers and characterized the corresponding SDoF region. However, for the general *K*-user setting only a limited work is available in existing literature. Towards this direction, in [9], the authors study the $(3, 1, 1, 1)$–Gaussian MISO channel wiretap with symmetric outdated CSIT (*DDD*) and establish bounds on SDoF region. The model that we study in this work can be seen as a step further in studying these class of channels with hybrid and alternating CSIT.

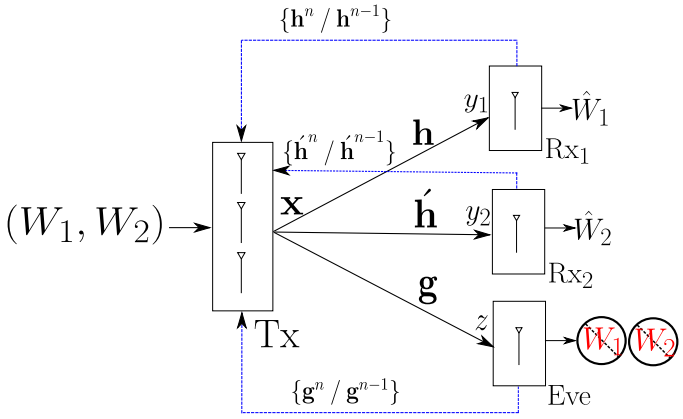

Fig. 1. (3,1,1,1)–Multi-receiver wiretap channel with alternating CSIT, and security constraints.

The main contributions of this work are summarized as follows. We consider the multi-receiver wiretap channel as shown in Figure 1 and establish bounds on SDoF region. In particular, we first consider the hybrid states, *PPD*, *PDP* (*DPP*), and *DDP* and characterize the complete SDoF region. Afterwards, we consider the case in which the transmitter is allowed to alternate between two states, i.e., *PDD* and *DPD* equal fractions of the communication time. For this case, we establish both inner and outer bounds on SDoF region. The coding scheme that we use to establish the inner bound, sheds light on how to multicast common information securely to both receivers. Although non-optimal in general, the results of this work show that for the multi-receiver wiretap channel, alternating CSIT not only enables interesting synergistic gains in terms of degrees of freedom in the case without secrecy constraints for two-user broadcast channel as was shown in [6], but also if secrecy constraints are imposed on the communication.

II. System Model and Definitions

We consider a multi-user wiretap channel which consists of two legitimate receivers and an external eavesdropper as shown in Figure 1. In this setup, the transmitter is equipped with three transmit antennas and the two receivers and the eavesdropper are equipped with a single antenna each. The transmitter wants to reliably transmit message $W_1 \in \mathcal{W}_1 = \{1, \ldots, 2^{nR_1(P)}\}$ to the receiver 1, and message $W_2 \in \mathcal{W}_2 = \{1, \ldots, 2^{nR_2(P)}\}$ to the receiver 2. In doing so, the transmitter also wishes to conceal both messages (W_1, W_2) from the eavesdropper. We assume that the eavesdropper is passive, i.e., it is not allowed to modify the communication.

We consider a fast fading channel model, 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

$$y_{1,t} = \mathbf{h}_t \mathbf{x}_t + n_{1t} \tag{1a}$$
$$y_{2,t} = \acute{\mathbf{h}}_t \mathbf{x}_t + n_{2t} \tag{1b}$$
$$z_t = \mathbf{g}_t \mathbf{x}_t + n_{3t}, \;\; t = 1, \ldots, n \tag{1c}$$

where $\mathbf{x} \in \mathbb{C}^{3\times 1}$ is the channel input vector, $\mathbf{h} \in \mathcal{H} \subseteq \mathbb{C}^{1\times 3}$ is the channel vector connecting receiver 1 to the transmitter, $\acute{\mathbf{h}} \in \acute{\mathcal{H}} \subseteq \mathbb{C}^{1\times 3}$ is the channel vector connecting receiver 2 to the transmitter, and $\mathbf{g} \in \mathcal{G} \subseteq \mathbb{C}^{1\times 3}$ is the channel vector connecting the eavesdropper 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 $i = 1,2,3$. The channel input is subjected to block power constraints, as $\sum_{t=1}^{n} \mathbb{E}[\|\mathbf{x}_t\|^2] \leq nP$. For ease of exposition, we denote $\mathbf{S}_t = \begin{bmatrix} \mathbf{h}_t \\ \acute{\mathbf{h}}_t \\ \mathbf{g}_t \end{bmatrix}$ 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 states $\mathbf{h}_t$, $\acute{\mathbf{h}}_t$, and $\mathbf{g}_t$ is known only to the receiver 1, receiver 2, and eavesdropper, respectively. Although, there are numerous forms of CSIT, in this work we focus on two of them as follows.

1) **Perfect CSIT**: corresponds to those instances in which the 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, the transmitter has perfect knowledge of *only* the past $(t-1)$ channel states. We denote these states by 'D'.

Let S_1 denotes the CSIT state of user 1, S_2 denotes the CSIT state of user 2 and S_3 denotes the CSIT state of the eavesdropper. Then, based on the availability of the CSIT, the model that we study (1) belongs to any of the following eight states

$$(S_1, S_2, S_3) \in \{PPP, PPD, PDP, PDD, DPP, DPD, DDP, DDD\}. \tag{2}$$

We denote $\lambda_{S_1S_2S_3}$ be the fraction of time state $S_1S_2S_3$ occurs, such that

$$\sum_{(S_1,S_2,S_3)\in\{P,D\}^3} \lambda_{S_1S_2S_3} = 1. \tag{3}$$

For simplicity of analysis in this work, we assume that $\lambda_{PDD} = \lambda_{DPD}$, i.e., the fractions of time spent in states *PDD* and *DPD* are equal.

Definition 1: A code for the Gaussian $(3,1,1,1)$–multi-receiver wiretap channel with alternating CSIT $(\lambda_{S_1S_2S_3})$ consists of sequence of stochastic encoders at the transmitter,

$$\begin{aligned}
\{\phi_{1t} &: \mathcal{W}_1\times\mathcal{W}_2\times\mathcal{S}^t \longrightarrow \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{X}_3\}_{t=1}^{\lceil n\lambda_{PPP}\rceil} \\
\{\phi_{2t} &: \mathcal{W}_1\times\mathcal{W}_2\times\mathcal{S}^{t-1}\times\mathcal{H}_t\times\acute{\mathcal{H}}_t \longrightarrow \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{X}_3\}_{t=1}^{\lceil n\lambda_{PPD}\rceil} \\
\{\phi_{3t} &: \mathcal{W}_1\times\mathcal{W}_2\times\mathcal{S}^{t-1}\times\mathcal{H}_t\times\mathcal{G}_t \longrightarrow \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{X}_3\}_{t=1}^{\lceil n\lambda_{PDP}\rceil} \\
\{\phi_{4t} &: \mathcal{W}_1\times\mathcal{W}_2\times\mathcal{S}^{t-1}\times\mathcal{H}_t \longrightarrow \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{X}_3\}_{t=1}^{\lceil n\lambda_{PDD}\rceil} \\
\{\phi_{5t} &: \mathcal{W}_1\times\mathcal{W}_2\times\mathcal{S}^{t-1}\times\acute{\mathcal{H}}_t\times\mathcal{G}_t \longrightarrow \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{X}_3\}_{t=1}^{\lceil n\lambda_{DPP}\rceil} \\
\{\phi_{6t} &: \mathcal{W}_1\times\mathcal{W}_2\times\mathcal{S}^{t-1}\times\acute{\mathcal{H}}_t \longrightarrow \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{X}_3\}_{t=1}^{\lceil n\lambda_{DPD}\rceil} \\
\{\phi_{7t} &: \mathcal{W}_1\times\mathcal{W}_2\times\mathcal{S}^{t-1}\times\mathcal{G}_t \longrightarrow \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{X}_3\}_{t=1}^{\lceil n\lambda_{DDP}\rceil} \\
\{\phi_{8t} &: \mathcal{W}_1\times\mathcal{W}_2\times\mathcal{S}^{t-1} \longrightarrow \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{X}_3\}_{t=1}^{\lceil n\lambda_{DDD}\rceil}
\end{aligned} \tag{4}$$

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,

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

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,

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

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 (6),
2) Perfect secrecy condition:[1]

$$\limsup_{n\to\infty} I(W_1, W_2; z^n, \mathbf{S}^n)/n = 0,$$

3) and communication rate condition:

$$\lim_{P\to\infty}\lim_{n\to\infty} \frac{\log|\mathcal{W}_i(n,P)|}{n\log P} \geq d_i, \quad \forall \; i \in \{1,2\} \tag{7}$$

at receiver 1 and 2, respectively.

Definition 4: We define the SDoF region, $\mathcal{C}_{\text{SDoF}}(\lambda_{S_1S_2S_3})$, of the multi-receiver wiretap channel as the set of all achievable non-negative pairs (d_1, d_2).

Due to the space limitations, some proofs in this work are only outlined or omitted. Detailed proofs are provided in [10].

III. SDoF of Multi-receiver Wiretap channel with fixed CSIT

In this section, we consider the multi-receiver wiretap channel shown in Figure 1 with fixed hybrid CSIT states and establish bounds on SDoF region.

A. 2-SDoF using PPD state

The following theorem provides the SDoF region of the multi-receiver wiretap channel with the *PPD* state.

Theorem 1: The SDoF region of the multi-receiver wiretap channel with the *PPD* state is given by the set of all non-negative pairs (d_1, d_2) satisfying

$$d_1 \leq 1 \tag{8a}$$
$$d_2 \leq 1 \tag{8b}$$
$$d_1 + d_2 \leq 2. \tag{8c}$$

Proof: The converse proof of Theorem 1 appears in [10, Appendix II]. In what follows, we provide the direct part of the proof that is used to establish Theorem 1. We now show that the SDoF of $(d_1, d_2) = (1,1)$ is achievable. The transmitter wants to send confidential symbols v to the receiver 1 and w to the receiver 2 and wishes to conceal them from the external eavesdropper. In this scheme, the transmitter sends symbols v and w along with the artificial noise u where perfect CSIT from both receivers are utilized in two ways 1) it zero-forces the interference being caused by symbol w intended for the receiver 2 and artificial noise u, at the receiver 1 and the interference being caused by symbol v intended for the receiver 1 and artificial noise u, at the receiver 2, and in doing so 2) it also secures these two symbols from the external eavesdropper. The transmitter sends

$$\mathbf{x}_1 = \acute{\mathbf{b}}_1 \begin{bmatrix} v & \phi & \phi \end{bmatrix}^T + \mathbf{b}_1 \begin{bmatrix} w & \phi & \phi \end{bmatrix}^T + \mathbf{b}_{12} \begin{bmatrix} u & \phi & \phi \end{bmatrix}^T, \tag{9}$$

where $\acute{\mathbf{b}}_1 \in \mathbb{C}^{3\times 1}$, $\mathbf{b}_1 \in \mathbb{C}^{3\times 1}$, and $\mathbf{b}_{12} \in \mathbb{C}^{3\times 1}$ are the precoding vectors chosen such that $\acute{\mathbf{h}}_1\acute{\mathbf{b}}_1 = 0$, $\mathbf{h}_1\mathbf{b}_1 = 0$, and $\acute{\mathbf{h}}_1\mathbf{b}_{12} = \mathbf{h}_1\mathbf{b}_{12} = 0$. These precoding vectors are known at all nodes. The channel input-output relationship is given by

$$y_1 = \mathbf{h}_1\acute{\mathbf{b}}_1 v, \tag{10a}$$
$$y_2 = \acute{\mathbf{h}}_1\mathbf{b}_1 w, \tag{10b}$$
$$z = \mathbf{g}_1\acute{\mathbf{b}}_1 v + \mathbf{g}_1\mathbf{b}_1 w + \mathbf{g}_1\mathbf{b}_{12} u. \tag{10c}$$

[1]For convenience, with a slight abuse in notations, we replace $\mathbf{S}^n := (\mathbf{S}^{n-1}, \mathbf{g}_n)$ in (7).

At the end of time slot 1, since the receiver 1 knows the CSI ($\mathbf{h}_1$) and $\acute{\mathbf{b}}_1$, it decodes the desired symbol v from y_1 through channel inversion. The receiver 2 can also perform similar operations to decode the desired symbol w. The eavesdropper gets the confidential symbols embedded in with artificial noise and is unable to decode them. The information leaked to the eavesdropper $I(v, w; z|\mathbf{S})$ can be bounded by

$$\begin{aligned} I(v, w; z|\mathbf{S}) &= h(z|\mathbf{S}) - h(z|v, w, \mathbf{S}) \\ &\leq \log(P) - h(u|\mathbf{S}) + o(\log(P)) \\ &\leq \log(P) - \log(P) + o(\log(P)) \\ &= o(\log(P)). \end{aligned} \tag{11}$$

From the above analysis, it can be easily seen that 1 symbol is securely send to each receiver over a total of 1 time slot, which yields a SDoF of 1 at each receiver, respectively. □

B. 3/2-SDoF using PDP state

The following theorem provides the SDoF region of the multi-receiver wiretap channel with the *PDP* state.

Theorem 2: The SDoF region of the multi-receiver wiretap channel with the *PDP* state is given by the set of all non-negative pairs (d_1, d_2) satisfying

$$d_1 \leq 1 \tag{12a}$$

$$d_1 + 2d_2 \leq 2. \tag{12b}$$

Proof: The converse proof of Theorem 2 appears in [10, Appendix III]. We now provide the coding scheme that shows that the SDoF of $(d_1, d_2) = (1, \frac{1}{2})$ is achievable. In this scheme, the transmitter wants to send two confidential symbols $\mathbf{v} := (v_1, v_2)$ to receiver 1 and a confidential symbol w to receiver 2 and wishes to conceal them from the external eavesdropper. The coding scheme comprises of two time slots. In the first time slot the transmitter sends

$$\mathbf{x}_1 = \mathbf{b}_3 \begin{bmatrix} v_1 & v_2 & \phi \end{bmatrix}^T + \mathbf{b}_{13} \begin{bmatrix} w & \phi & \phi \end{bmatrix}^T, \tag{13}$$

where $\mathbf{b}_3 \in \mathbb{C}^{3\times 1}$ and $\mathbf{b}_{13} \in \mathbb{C}^{3\times 1}$ are the precoding vectors chosen such that $\mathbf{g}_1\mathbf{b}_3 = 0$ and $\mathbf{g}_1\mathbf{b}_{13} = \mathbf{h}_1\mathbf{b}_{13} = 0$. These precoding vectors are known at all nodes. The channel input-output relationship is given by

$$y_{1,1} = \mathbf{h}_1\mathbf{b}_3\mathbf{v}, \tag{14a}$$

$$y_{2,1} = \underbrace{\acute{\mathbf{h}}_1\mathbf{b}_3\mathbf{v}}_{\text{interference}} + \acute{\mathbf{h}}_1\mathbf{b}_{13}w, \tag{14b}$$

$$z_1 = 0. \tag{14c}$$

At the end of time slot 1, the receiver 1 gets one equation with two unknowns and requires an extra equation to decode the desired symbols. This equation is being available as interference (side information) at the receiver 2. Receiver 2 gets the desired symbol w embedded in with some interference ($\acute{\mathbf{h}}_1\mathbf{b}_3\mathbf{v}$). Conveying this interference *securely* to both legitimate receivers will be useful in two ways, 1) it provides the extra equation to the receiver 1 to decode the desired symbols $\mathbf{v}$, and 2) also helps the receiver 2 to remove the interference from $y_{2,1}$ to decode w. Due to the availability of delayed CSI from the receiver 2 ($\acute{\mathbf{h}}$) and since the transmitter knows $\mathbf{v}$, it can readily construct $\acute{\mathbf{h}}_1\mathbf{b}_3\mathbf{v}$ and sends

$$\mathbf{x}_2 = \mathbf{b} \begin{bmatrix} \acute{\mathbf{h}}_1\mathbf{b}_3\mathbf{v} & \phi & \phi \end{bmatrix}^T, \tag{15}$$

where $\mathbf{b} \in \mathbb{C}^{3\times 1}$ is the precoding vector chosen such that $\mathbf{g}_2\mathbf{b} = 0$. This precoding vector is known at all nodes. The channel input-output relationship is given by

$$y_{1,2} = \mathbf{h}_2\mathbf{b}\acute{\mathbf{h}}_1\mathbf{b}_3\mathbf{v}, \tag{16a}$$

$$y_{2,2} = \acute{\mathbf{h}}_2\mathbf{b}\acute{\mathbf{h}}_1\mathbf{b}_3\mathbf{v}, \tag{16b}$$

$$z_2 = 0. \tag{16c}$$

At the end of time slot 2, since the receiver 1 knows the CSI, it decodes (v_1, v_2) from $(y_{1,1}, y_{1,2})$ through channel inversion. Similarly, since the receiver 2 knows the CSI and $y_{2,2}$, it subtracts out the contribution of $\acute{\mathbf{h}}_1\mathbf{b}_3\mathbf{v}$ from $y_{2,1}$ to decode w. The eavesdropper is unable to get any information from the two time slots and thus the information leaked to the eavesdropper $I(\mathbf{v}, w; z_1, z_2|\mathbf{S}^n) = 0$.

From the above analysis, it can be easily seen that 2 symbols are securely send to the receiver 1 over a total of 2 time slots, which yields a SDoF of 1 at the receiver 1. Similarly, 1 symbol is send to the receiver 2 over a total of 2 time slots, which yields a SDoF of $\frac{1}{2}$ at the receiver 2. □

C. 4/3-SDoF using DDP state

In this state, perfect CSIT is available from the eavesdropper and only past or outdated CSIT is available from both legitimate receivers. The following theorem provides the SDoF region of the multi-receiver wiretap channel with the *DDP* state.

Theorem 3: The SDoF region of the multi-receiver wiretap channel with the *DDP* state is given by the set of all non-negative pairs (d_1, d_2) satisfying

$$d_1 + 2d_2 \leq 2 \tag{17a}$$

$$2d_1 + d_2 \leq 2. \tag{17b}$$

Proof: The converse proof of Theorem 3 follows along very similar lines as in (12b) and is omitted for brevity. We now provide the sketch of the proof that is used to establish Theorem 3. This scheme consists of three time slots where the transmitter wants to send two confidential symbols $\mathbf{v} := (v_1, v_2)$ to receiver 1 and two confidential symbols $\mathbf{w} := (w_1, w_2)$ to receiver 2 and wishes to conceal them from the eavesdropper. Due to the availability of perfect CSIT from the eavesdropper, the transmitter is able to zero force all the information leaked towards it. The rest of the coding scheme can be seen as an extension of the $(2, 1, 1)$–Maddah-Ali-Tse scheme [2], where the transmitter uses two antennas to send information to both receivers securely. The complete proof appears in [10]. □

D. 1-SDoF using PDD state

In this state perfect CSIT is available from the receiver 1 and delayed or past CSIT is available from the receiver 2 and the eavesdropper. For this state, we now show that the sum SDoF of 1 is achievable. The transmitter sends a confidential symbol v intended for the receiver 1 along with artificial noise u as

$$\mathbf{x}_1 = \begin{bmatrix} v & \phi & \phi \end{bmatrix}^T + \mathbf{b}_1 \begin{bmatrix} u & \phi & \phi \end{bmatrix}^T, \tag{18}$$

where the precoding vector $\mathbf{b}_1 \in \mathbb{C}^{3\times 1}$ is chosen such that $\mathbf{h}_1\mathbf{b}_1 = 0$. Thus, receiver 1 can easily decode the desired symbol. The eavesdropper gets the confidential symbol embedded in with artificial noise and thus is unable to decode it. Thus, 1 symbol is securely send to the receiver 1 over a total of 1 time slot, yielding the SDoF pair $(d_1, d_2) = (1, 0)$.

IV. SDoF of Multi-User Wiretap channel with alternating CSIT

We now turn our attention to the multi-receiver wiretap channel, in which the transmitter is allowed to alternate between two states, i.e., *PDD* and *DPD*, equal fractions of the communication time.

A. Outer Bound

The following theorem provides an outer bound on the SDoF region of the multi-receiver wiretap channel with alternating CSIT.

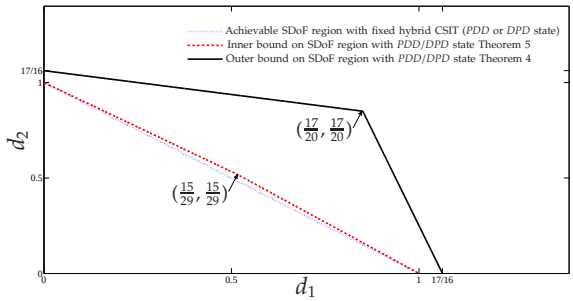

Fig. 2. SDoF region of multi-user wiretap channel with alternating CSIT.

Theorem 4: An outer bound on the SDoF region $\mathcal{C}_{\text{SDoF}}(\lambda_{S_1S_2S_3})$ of the multi-receiver wiretap channel with alternating CSIT is given by the set of all non-negative pairs (d_1, d_2) satisfying

$$16d_1 + 4d_2 \leq 17 \tag{19a}$$
$$4d_1 + 16d_2 \leq 17. \tag{19b}$$

Proof: The proof of Theorem 4 appears in [10, Appendix IV]. □

B. Inner Bound

Next, we establish an inner bound on the multi-receiver wiretap channel with alternating CSIT.

Theorem 5: An inner bound on the SDoF region $\mathcal{C}_{\text{SDoF}}(\lambda_{S_1S_2S_3})$ of the multi-receiver MISO wiretap channel with alternating CSIT is given by the set of all non-negative pairs (d_1, d_2) satisfying

$$15d_1 + 14d_2 \leq 15 \tag{20a}$$
$$14d_1 + 15d_2 \leq 15. \tag{20b}$$

Proof: The region in (20) is characterized by the corner points $(1,0)$, $(0,1)$ and the point $(15/29, 15/29)$ obtained by the intersection of line equations in (20). The achievability of the two corner points $(1,0)$ and $(0,1)$ follow by the coding scheme developed in [10, Theorem 1], where the transmitter is interested to send confidential message to the receiver 1 being eavesdropped by the eavesdropper. The achievability of the point $(15/29, 15/29)$ is provided in subsection IV-C. □

Figure 2 shows the outer and inner bounds on SDoF with alternating CSIT in (19) and (20), respectively. For comparison reasons, we also plot the SDoF region obtained by fixed state *PDD*. Although the optimality of inner bounds is still to be shown, it can be easily seen from Figure 2 that, by synergistically using *PDD* and *DPD* states the inner bound in (20) provides a sum rate

$$\text{SDoF}_{\text{sum}} = \underbrace{\frac{30}{29}}_{\text{PDD/DPD}} \geq \underbrace{1}_{\text{PDD}} \tag{21}$$

which is clearly larger than the sum rate with fixed CSIT.

C. $S_1^{30/29}$ — Coding scheme using PDD and DPD states

We now establish some coding schemes that provide the main ingredients to establish the inner bound in Theorem 5. The following schemes achieve 30/29 SDoF.

1) $S_1^{30/29}$ – using *PDD*, *DPD* states for $(\frac{22}{29}, \frac{7}{29})$ fractions of time, $(d_1, d_2) = (\frac{15}{29}, \frac{15}{29})$ SDoF is achievable.
2) $S_2^{30/29}$ – using *PDD*, *DPD* states for $(\frac{7}{29}, \frac{22}{29})$ fractions of time, $(d_1, d_2) = (\frac{15}{29}, \frac{15}{29})$ SDoF is achievable.

The achievability of the corner point $(15/29, 15/29)$ in Theorem 5 follows by using $S_1^{30/29}$ and $S_2^{30/29}$ schemes equal fractions of communication time.

1) $S_1^{30/29}$ — Coding scheme using PDD and DPD states $(\frac{22}{29}, \frac{7}{29})$ fractions of time: We now show that by using *PDD* and *DPD* states for $(\frac{22}{29}, \frac{7}{29})$ fractions of time, $(d_1, d_2) = (\frac{15}{29}, \frac{15}{29})$ SDoF is achievable. In this scheme, the transmitter wants to transmit three symbols (v_1, v_2, v_3) to the receiver 1 and three symbols (w_1, w_2, w_3) to the receiver 2 and wishes to conceal them from the eavesdropper. The communication takes place in two phases, i.e., data dissemination phase and transmission of common information.

A) Data dissemination phase: In this phase the transmitter sends fresh information to both receivers. In the first time slot, the transmitter chooses *PDD* state and injects artificial noise $\mathbf{u} := [u_1, u_2, u_3]^T$, from all antennas. At the end of time slot 1, the channel input-output relationship is given by

$$y_{1,1} = \mathbf{h}_1\mathbf{u}, \tag{22a}$$
$$y_{2,1} = \acute{\mathbf{h}}_1\mathbf{u}, \tag{22b}$$
$$z_1 = \mathbf{g}_1\mathbf{u}. \tag{22c}$$

At the end of time slot 1, the receiver 2 and eavesdropper feed back the delayed CSI to the transmitter.

In the second time slot, the transmitter remains in *PDD* state and sends fresh information $\mathbf{v} := [v_1, v_2, v_3]^T$ to the receiver 1 along with a linear combination of channel output $y_{1,1}$ at the receiver 1. The transmitter can easily learn $y_{1,1}$, since it already knows the perfect CSI $(\mathbf{h}_1)$ and $\mathbf{u}$. During this phase, the transmitter sends

$$\mathbf{x}_2 = [v_1 \ v_2 \ v_3]^T + \left[y_{1,1} \ \phi \ \phi\right]^T. \tag{23}$$

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

$$y_{1,2} = \mathbf{h}_2\mathbf{v} + h_{21}y_{1,1}, \tag{24a}$$
$$y_{2,2} = \underbrace{\acute{\mathbf{h}}_2\mathbf{v} + \acute{h}_{21}y_{1,1}}_{\text{side information}}, \tag{24b}$$
$$z_2 = \underbrace{\mathbf{g}_2\mathbf{v} + g_{21}y_{1,1}}_{\text{side information}}. \tag{24c}$$

At the end of time slot 2, the receiver 2 and eavesdropper feed back the delayed CSI to the transmitter. At the end of time slot 2, the receiver 1 can subtracts out the contribution of $y_{1,1}$ to get one equation with 3 confidential symbols and requires two extra equations to successfully decode the intended variables. This side information is available at the receiver 2 and eavesdropper, and will be conveyed in phase 2.

In the third time slot, the transmitter remains in *PDD* state and sends fresh information $\mathbf{w} := [w_1, w_2, w_3]^T$ to the receiver 2 along with a linear combination of channel output $y_{2,1}$ at the receiver 2 at the end of first time slot. The transmitter can easily re-construct $y_{2,1}$, since it knows the past CSI $(\acute{\mathbf{h}}_1)$ and $\mathbf{u}$. During this phase, the transmitter sends

$$\mathbf{x}_3 = [w_1 \ w_2 \ w_3]^T + \left[y_{2,1} \ \phi \ \phi\right]^T. \tag{25}$$

The channel input-output relationship is given by

$$y_{1,3} = \underbrace{\mathbf{h}_3\mathbf{w} + h_{31}y_{2,1}}_{\text{side information}}, \tag{26a}$$
$$y_{2,3} = \acute{\mathbf{h}}_3\mathbf{w} + \acute{h}_{31}y_{2,1}, \tag{26b}$$
$$z_3 = \underbrace{\mathbf{g}_3\mathbf{w} + g_{31}y_{2,1}}_{\text{side information}}. \tag{26c}$$

At the end of time slot 3, the receiver 2 and eavesdropper feed back the delayed CSI to the transmitter. At the end of time slot 3, the receiver 2 subtracts out the contribution of $y_{2,1}$ to get one equation with 3 confidential symbols and requires two extra equations to successfully decode the intended variables. This side information is available at the receiver 1 and eavesdropper, respectively.

Recall that, at the end of three time slots, the receiver 1 requires side information available at the receiver 2 ($y_{2,2}$) and eavesdropper (z_2) and the receiver 2 requires side information available at the receiver 1 ($y_{1,3}$) and eavesdropper (z_3). Due to the availability of non-causal and strictly causal CSIT, the transmitter can learn these side informations and the next step is how to convey them securely. The information leaked to eavesdropper after 3 time slots $I(\mathbf{v},\mathbf{w};z_1,z_2,z_3|\mathbf{S}^n)$ is bounded by

$$I(\mathbf{v},\mathbf{w};z_1,z_2,z_3|\mathbf{S}^n) = o(\log(P)). \tag{27}$$

The side information available at the eavesdropper can be conveyed in the spirit of alternating CSIT scheme developed in [6, Theorem 1] where alternation between *PD* and *DP* states equal fractions of communication time yields an optimal $\text{DoF}_{\text{PD/DP}} = 5/3$. Thus, the side information required by the receiver 1 (z_2) and the receiver 2 (z_3) can be conveyed to both receivers over a total of $\frac{2}{\text{DoF}_{\text{PD/DP}}} = 6/5$ time slots. After conveying these side informations to respective receivers, the receiver 1 requires $y_{2,2}$ which is available at the receiver 2 at the end of time slot 2 and the receiver 2 requires $y_{1,3}$ which is available at the receiver 1 at the end of time slot 3 to successfully decode the desired symbols. Note that, one can not merely multicast these side information similar to $\text{DoF}_{\text{PD/DP}}$ [6, Theorem 1], since it will leak extra information to the eavesdropper. Next, we define a common message $W_{12} := y_{2,2} + y_{1,3}$. Conveying W_{12} to both receivers securely will suffice to decode their respective symbols. The resulting SDoF at each receiver can be concisely written as

$$d_i = \frac{3}{3 + \frac{2}{\text{DoF}_{\text{PD/DP}}} + \frac{1}{\text{SDoF}_{\text{common}}}}, \quad i = 1,2 \tag{28}$$

where $\text{SDoF}_{\text{common}}$ denotes the SDoF of the common message W_{12}.

B) Multicasting common information with alternating CSIT: We now provide the description of the coding scheme which is used to send two common symbols v_{12} and w_{12} over a total of $\frac{16}{5}$ time slots to both receivers with alternating CSIT, securely. In the first time slot, the transmitter chooses *PDD* state and transmits the confidential symbol v_{12} embedded in with artificial noise q_1 as

$$\mathbf{x}_1 = \begin{bmatrix} v_{12} & \phi & \phi \end{bmatrix}^T + \mathbf{b}_1 \begin{bmatrix} q_1 & \phi & \phi \end{bmatrix}^T, \tag{29}$$

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

$$y_{1,1} = h_{11}v_{12}, \tag{30a}$$
$$y_{2,1} = \acute{h}_{11}v_{12} + \acute{\mathbf{h}}_1\mathbf{b}_1 q_1, \tag{30b}$$
$$z_1 = \underbrace{g_{11}v_{12} + \mathbf{g}_1\mathbf{b}_1 q_1}_{\text{side information}}. \tag{30c}$$

At the end of time slot 1, the receiver 1 can readily decode symbol v_{12} through channel inversion. Receiver 2 gets the confidential symbol embedded in with artificial noise q_1 and requires one extra equation to decode v_{12}. This side information is available at the eavesdropper.

In the second time slot, the transmitter switches to *DPD* state and transmits the confidential symbol w_{12} embedded in with artificial noise q_2 as

$$\mathbf{x}_2 = \begin{bmatrix} w_{12} & \phi & \phi \end{bmatrix}^T + \mathbf{b}_2 \begin{bmatrix} q_2 & \phi & \phi \end{bmatrix}^T, \tag{31}$$

where $\mathbf{b}_2 \in \mathbb{C}^{3\times 1}$ is the precoding vector chosen such that $\acute{\mathbf{h}}_2\mathbf{b}_2 = 0$. At the end of timeslot 2, the channel input-output relationship is given by

$$y_{1,2} = h_{21}w_{12} + \mathbf{h}_2\mathbf{b}_2 q_2, \tag{32a}$$
$$y_{2,2} = \acute{h}_{21}w_{12}, \tag{32b}$$
$$z_2 = \underbrace{g_{21}w_{12} + \mathbf{g}_2\mathbf{b}_2 q_2}_{\text{side information}}. \tag{32c}$$

At the end of time slot 2, the receiver 2 can readily decode symbol w_{12} through channel inversion. Receiver 1 gets the confidential symbol embedded in with artificial noise q_2 and requires one extra equation to decode w_{12}.

At the end of two time slots, both receivers require one extra equation to decode their respective messages being available at the eavesdropper. By using $\text{DoF}_{\text{PD/DP}}$ scheme z_1 is send to the receiver 2 and z_2 is send to the receiver 1 over a total of $\frac{2}{\text{DoF}_{\text{PD/DP}}} = 6/5$ time slots. Thus, 2 symbols are securely send to both receivers over a total of $2 + 6/5$ time slots which yields a SDoF of

$$\text{SDoF}_{\text{common}} = \frac{2}{2 + \frac{6}{5}} = \frac{5}{8}. \tag{33}$$

Finally replacing (33) in (28) yields the SDoF of

$$d_i = \frac{3}{3 + \frac{2}{5/3} + \frac{1}{5/8}} = \frac{15}{29} \tag{34}$$

at each receiver securely.

2) $S_2^{30/29}$ — Coding scheme using PDD and DPD states ($\frac{7}{29}, \frac{22}{29}$) fractions of time: The coding scheme in this case follows along similar lines as the scheme illustrated above by reversing the roles of receiver 1 and receiver 2, respectively.

V. Acknowledgment

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

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] S. Yang, M. Kobayashi, D. Gesbert, and X. Yi, "Degrees of freedom of time correlated MISO broadcast channel with delayed CSIT," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 315–328, Jan. 2013.

[5] 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 Wirl. Com. Sys.*, France, Aug. 2012, pp. 1004–1008.

[6] 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, Jul. 2013.

[7] Z. H. Awan, A. Zaidi, and A. Sezgin, "Achievable secure degrees of freedom of MISO broadcast channel with alternating CSIT," in *IEEE Int. Sym. on Information Theory*, Honolulu, USA, June 2014, pp. 31–35.

[8] P. Mukherjee, R. Tandon, and S. Ulukus, "Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT," 2015. [Online]. Available: http://arxiv.org/abs/1502.02647

[9] R. Tandon, P. Piantanida, and S. Shamai, "On multi-user MISO wiretap channels with delayed CSIT," in *IEEE Int. Sym. on Information Theory*, Honolulu, USA, June 2014, pp. 211–215.

[10] Z. H. Awan, A. Zaidi, and A. Sezgin, "On SDoF of multi-receiver wiretap channel with alternating CSIT," 2015. [Online]. Available: http://arxiv.org/pdf/1503.06333v2.pdf