On MISO Wiretap Channel With Delayed CSIT and Alternating Topology

Zohaib Hassan Awan and Aydin Sezgin
Chair of Communication Systems
Ruhr-Universität Bochum, 44780 Bochum, Germany.
{zohaib.awan, aydin.sezgin}@rub.de

***Abstract*—We study the problem of secure transmission over a Gaussian $(2,1,1)$–multi-input single-output (MISO) wiretap channel under the assumption that links connecting the legitimate receiver and the eavesdropper, may have unequal strengths *statistically* and delayed channel state information is available at the transmitter (CSIT) from both receivers, respectively. We focus on a two state topological setting of strong v.s. weak links. For this model, we establish bounds on generalized secure degrees of freedom (SDoF). For some special cases, the upper and lower bounds coincide and SDoF is characterized. The encoding scheme sheds light on the usage of both resources, i.e., topology and delayed CSIT, in a non-trivial manner.**

I. Introduction

In a communication network, due to the scarcity of available resources and increase in the demand of higher data rates imposed by the consumers, multiple nodes communicate with each other over a shared medium. This in turn leads to a fundamental problem of interference in networks. A key tool to eradicate this issue is by utilizing interference alignment schemes previously introduced in literature [1]. The schemes established in [1], generally assume that perfect channel state information (CSI) about all nodes is conveyed to the transmitter, which is used to align the interference at the receivers. However, due to random fluctuations in the wireless medium, it becomes difficult to convey the perfect CSI to the transmitter. In [2], Maddah-Ali *et al.* study a MISO broadcast channel and show a rather surprising result that delayed or past CSIT is still useful in the sense that it enlarges the degrees of freedom (DoF) compared to a similar model with no CSIT. The result developed in [2] is generalized to study a variety of models namely, two- and three-user multi-input multi-output (MIMO) broadcast channel in [3], [4], two-user interference channel in [5], [6], and X-channel in [7], [8], all from DoF perspective. In all these works, it is assumed that all non-zero channels are equally strong in the sense that each link is capable of carrying 1 DoF, irrespective of the magnitude of channel coefficient. In cellular networks due to the mobility, links connecting users are affected by different topological factors for instance, inter-cell interference, and wave propagation path loss. These external factors influence links in an asymmetric manner, which leads to some links being stronger than others *statistically*. In [9], Chen *et al.* study a two-user MISO broadcast channel by taking these topological factors into account. The authors consider the two state topological setting and assume that CSI conveyed by both receivers can vary over time and establish bounds on generalize DoF region.

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

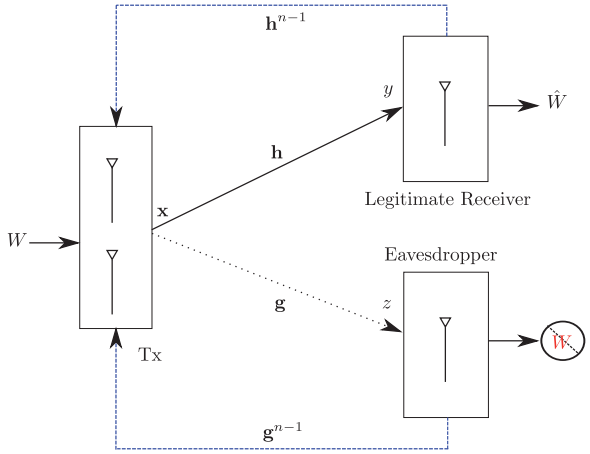

Fig. 1. $(2,1,1)$–MISO wiretap channel, where the link to eavesdropper is weaker than to the legitimate receiver.

Due to the broadcast nature of wireless medium, information transmission is over heard by unintended nodes in the network for free. Wyner in his seminal paper [10], introduced a basic wiretap channel to study secrecy by taking physical layer attributes of the channel into account. Wyner's wiretap channel is extended to study a variety of multi-user networks [11] (and references therein). The complete secrecy capacity characterization of multi-user channels is difficult so recently, a growing body of research has attracted attention to study the asymptotic behaviour of these models in high signal-to-noise ratio (SNR) regimes, where SDoF captures the relevant performance metrics. Khisti *et al.* in [12], study the Gaussian MIMO wiretap channel in which perfect CSI is available at the Transmitter and establish the secrecy capacity as well as the SDoF. In [13], the authors study the two-user MIMO broadcast channel with past or delayed CSI and characterize the SDoF region.

In this paper, we consider a Gaussian $(2,1,1)$–MISO wiretap channel which consists of three nodes — a transmitter, a legitimate receiver and a eavesdropper as shown in Figure 1.

ISBN 978-3-8007-3659-1

The transmitter is equipped with two antennas and each of the receiver and eavesdropper is equipped with a single antenna. The transmitter wants to reliably transmit message W to the receiver and wishes to conceal it from the eavesdropper. In investigating this model we make three assumptions, namely, 1) each receiver knows the perfect instantaneous CSI and also the CSI of the other receiver with a unit delay, 2) each receiver is allowed to convey the past or delayed CSI to the transmitter and 3) links connecting receivers may have different strengths, statistically; thus the topology of this network can alternate between four possible states. We assume that the eavesdropper is passive and is not allowed to modify the communication.

Compared to the wiretap channel studied in [13], in this work the links connecting both receivers may have unequal strengths. The $(2,1,1)$–MISO wiretap channel that we study can be seen as a special case of the one in [9] but with imposed security constraints. We focus on the asymptotic behaviour of this network model, where system performance is measured by SDoF.

The main contributions of this work are summarized as follows. We first establish an upper bound on the generalized SDoF of $(2,1,1)$–MISO wiretap channel. The upper bound follows by extending the proof developed earlier in the context of MIMO wiretap channel with delayed CSIT in [13] by taking topology of the network into account. For the case in which legitimate receiver is stronger than the eavesdropper, the lower bound that we establish in this work coincides with the upper bound; and, thus SDoF is established. The encoding scheme is based on the noise injection scheme in [13] and also borrows some elements from the one developed in [9] by taking imposed secrecy constraints into account. The encoding scheme carefully utilize the topology of the network and CSI available from the receivers in a non-trivial manner.

We structure this paper as follows. Section II provides a formal description of the channel model along with some useful definitions. Section III states the main result of this work, where we have established an upper bound and the encoding schemes for the $(2,1,1)$–MISO wiretap channel. Finally, in section IV we conclude this paper by summarizing its contributions.

Notations: A few words about notations. Boldface upper case letter $\mathbf{X}$ denote matrices; boldface lower case letter $\mathbf{x}$ denote vectors; and calligraphic letter $\mathcal{X}$ designate alphabets. At each time instant t, $\mathbf{x}_t$ denote $[x_{t1},\ldots,x_{tn}]$, and $\mathbb{E}[.]$ denote the expectation operator. We use $\doteq$ to denote an exponential equality, such that given $f(\rho) \doteq \rho^{\beta}$ implies $\lim_{\rho\to\infty} \log f(\rho)/\log(\rho) = \beta$. We use $\mathcal{O}(f(\rho))$ to denote the asymptotic behaviour of the function $f(\rho)$. The term $o(n)$ is some function $g(n)$ such that $\lim_{n\to\infty} \frac{g(n)}{n} = 0$. The Gaussian distribution with mean μ and variance σ^2 is denoted by $\mathcal{CN}(\mu,\sigma^2)$. Finally, throughout the paper, logarithms are taken to base 2.

II. System Model and Definitions

We consider the $(2,1,1)$–Gaussian MISO wiretap channel, as shown in Figure 1. In this channel model, 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 $W \in \mathcal{W} = \{1,\ldots,2^{nR(A_1,\rho)}\}$ to legitimate receiver and wishes to conceal it from the eavesdropper. For this setting, we consider a fast fading environment and assume that each receiver is fully aware of its own perfect instantaneous CSI and also the CSI of the other receiver with a unit delay. In addition to this, each receiver is allowed to convey only the past or outdated CSI to the transmitter, i.e., at time instant t, transmitter has perfect knowledge of *only* the past $(t-1)$ channel states from both receivers.

Due to the inherent randomness of the wireless channel and topological changes that may arise, for instance — due to the mobility of the users or interference (jamming) from unintended nodes, some elements of the network can experience more interference compared to the others. These factors in turn originate two fundamental classes of links, where few links are stronger than others statistically. Let $A_1 \in \{1,\alpha\}$ denote the link power exponent from the transmitter to legitimate receiver and $A_2 \in \{1,\alpha\}$ denote the link power exponent from transmitter to eavesdropper, respectively, for $0 \le \alpha \le 1$; where we denote the stronger link by $A_i := 1$ and the weaker link by $A_i := \alpha$, $i = 1,2$, respectively. As alluded before, the notion of stronger v.s. weaker links implies a statistical comparison, for instance, $A_1 > A_2$ refers to the case in which intended receiver is stronger than eavesdropper statistically. Then, based on the topology of the network, the model that we study belongs to any of the four states, $(A_1,A_2) \in \{1,\alpha\}^2$. We denote $\lambda_{A_1A_2}$ be the fraction of time topology state A_1A_2 occurs, such that

$$\sum_{(A_1,A_2)\in\{1,\alpha\}^2} \lambda_{A_1A_2} = 1. \tag{1}$$

The channel input-output relationship at time instant t is

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

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 intended receiver to the transmitter and $\mathbf{g} \in \mathcal{G} \subseteq \mathbb{C}^{1\times 2}$ is the channel vector connecting eavesdropper to the transmitter, respectively, the parameter ρ is subject to input power constraint; 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 $i = 1,2$. For convenience, we normalize the channel input vector, $||\mathbf{x}_t||^2 \le 1$, then the average received SNR for each link at time instant t is given by

$$\begin{aligned} \mathbb{E}_{\mathbf{h}_t,\mathbf{x}_t}[||\sqrt{\rho^{A_{1,t}}}\mathbf{h}_t\mathbf{x}_t||^2] &= \rho^{A_{1,t}} \\ \mathbb{E}_{\mathbf{g}_t,\mathbf{x}_t}[||\sqrt{\rho^{A_{2,t}}}\mathbf{g}_t\mathbf{x}_t||^2] &= \rho^{A_{2,t}}. \end{aligned}$$

For ease of exposition, we denote $\mathbf{S}_t = \left[\begin{smallmatrix}\mathbf{h}_t\\ \mathbf{g}_t\end{smallmatrix}\right]$ as the channel state matrix and $\mathbf{S}^{t-1} = \{\mathbf{S}_1,\ldots,\mathbf{S}_{t-1}\}$ captures the collection of channel state matrices over the past $(t-1)$ symbols, respectively, where $\mathbf{S}^0 = \emptyset$. 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 nodes. However, the instantaneous states $\mathbf{h}_t$ and $\mathbf{g}_t$ are known only to the legitimate receiver, and eavesdropper, respectively.

ISBN 978-3-8007-3659-1

Definition 1: A code for the Gaussian $(2,1,1)$–MISO wiretap channel with delayed CSIT and alternating topology consists of sequence of stochastic encoders at the transmitter,

$$\{\phi_t \ : \ \mathcal{W}\times\mathcal{S}^{t-1} \longrightarrow \mathcal{X}_1 \times \mathcal{X}_2\}_{t=1}^{n} \tag{3}$$

where the message W is drawn uniformly over $\mathcal{W}$; and a decoding function at intended receiver

$$\psi \ : \ \mathcal{Y}^n\times\mathcal{S}^{n-1}\times\mathcal{H}_n \longrightarrow \hat{\mathcal{W}}. \tag{4}$$

Definition 2: A rate $R(A_1,\rho)$ is said to be achievable if there exists a sequence of codes such that

$$\limsup_{n\to\infty} \Pr\{\hat{W} \neq W|W\} = 0. \tag{5}$$

Definition 3: A generalized SDoF $d(A_1)$ is said to be achievable if there exists a sequence of codes satisfying following

1) Reliability condition:

$$\limsup_{n\to\infty} \Pr\{\hat{W} \neq W|W\} = 0, \tag{6}$$

2) Perfect secrecy condition:

$$\limsup_{n\to\infty} \frac{I(W; z^n, \mathbf{S}^n)}{n} = 0, \tag{7}$$

3) and communication rate condition:

$$\lim_{\rho\to\infty} \liminf_{n\to\infty} \frac{\log|\mathcal{W}(n,\rho,A_1)|}{n\log\rho} \geq d(A_1). \tag{8}$$

III. Generalized SDoF of MISO wiretap channel with delayed CSIT

In this section, we state our main results on the generalized SDoF of the MISO wiretap channel with delayed CSIT. Before proceeding to state the result, we first digress to provide a useful lemma which we will repetitively use in this work.

Lemma 1: The following quantities hold under channel output symmetry

$$h(y^n, z^n|\mathbf{S}^n) \leq 2h(z^n|\mathbf{S}^n) + n\lambda_{1\alpha}(1-\alpha)\log(\rho), \tag{9a}$$
$$h(y^n, z^n|\mathbf{S}^n) \leq 2h(y^n|\mathbf{S}^n) + n\lambda_{\alpha 1}(1-\alpha)\log(\rho), \tag{9b}$$
$$h(y^n|\mathbf{S}^n) \leq 2h(z^n|\mathbf{S}^n) + n\lambda_{1\alpha}(1-\alpha)\log(\rho), \tag{9c}$$
$$h(z^n|\mathbf{S}^n) \leq 2h(y^n|\mathbf{S}^n) + n\lambda_{\alpha 1}(1-\alpha)\log(\rho). \tag{9d}$$

Proof: The proof of Lemma 1 appears in Appendix A.The inequalities in Lemma 1 also holds with additional conditioning over message W. □

A. Upper Bound

We now establish an upper bound on the generalized SDoF of the MISO wiretap channel with delayed CSIT and alternating topology.

Theorem 1: For the (2,1,1)–MISO wiretap channel with delayed CSIT and alternating topology $(\lambda_{A_1A_2})$, an upper bound on generalized SDoF is given by

$$d(\lambda_{A_1A_2}) \leq \frac{(3-\alpha)\lambda_{1\alpha} + 2(\lambda_{11} + \alpha\lambda_{\alpha\alpha}) + (1+\alpha)\lambda_{\alpha 1}}{3}. \tag{10}$$

Proof: The proof of the upper bound is provided in Appendix B. □

Remark 1: The upper bound generalizes the proof established earlier in the context of SDoF of wiretap channel with delayed CSIT [13] by taking topological fluctuations into account. By removing the topology consideration, i.e., setting $\lambda_{11} := 1$, the upper bound reduces to the SDoF of MISO wiretap channel with delayed CSI [13, Theorem 1].

B. Generalized SDoF with fixed topology

In this subsection, we provide some optimal encoding schemes for fixed topological states. For simplicity of analysis and in accordance with DoF framework, we ignore the additive Gaussian noise and only mention the asymptotic behaviour of the inputs by ignoring the exact power allocations.

1) Fixed Topology ($\lambda_{11} = 1$): By removing the topology consideration, i.e., by setting $(A_{1t}, A_{2t}) := (1,1) \ \forall \ t$, the model reduces to the MISO wiretap channel with delayed CSIT studied in [13], for which the optimal SDoF is given by $2/3$ SDoF. The coding scheme in this case is established in [13] and is omitted for brevity.

2) Fixed Topology ($\lambda_{1\alpha} = 1$): We now focus on the case in which the legitimate receiver is stronger than the eavesdropper and state the optimal SDoF.

Proposition 1: For the case in which the legitimate receiver is stronger than the eavesdropper ($\lambda_{1\alpha} = 1$), the SDoF is

$$d = \frac{3-\alpha}{3}. \tag{11}$$

Proof: The converse follows immediately from the upper bound established in Theorem 1 by setting $\lambda_{1\alpha} := 1$ in (10). We now provide the description of the encoding scheme that we use to prove the direct part of Proposition 1. In this scheme, the transmitter intends to send three symbols (v_1, v_2, v_3) to the legitimate receiver and wishes to conceal them from the eavesdropper. The communication takes place in three phases, each comprising of only one time slot. In the first time slot, the transmitter injects artificial noise, $\mathbf{u} := [u_1, u_2]^T$, along with the confidential symbol (v_1) intended for the legitimate receiver. In this phase, the leverage provided by the topology of the network is utilized as follows. Similar to the coding scheme in [13], the transmitter injects artificial noise from both antennas, where due to the topology of the network the output at eavesdropper is obtained at a lower power level $(\mathcal{O}(\rho^\alpha))$ compared to the legitimate receiver $(\mathcal{O}(\rho))$. Thus, by reducing the transmission power of the artificial noise to the order of eavesdropper $(\mathcal{O}(\rho^\alpha))$, the transmitter can then use the remaining power $(\mathcal{O}(\rho^{1-\alpha}))$ to send confidential symbol to legitimate

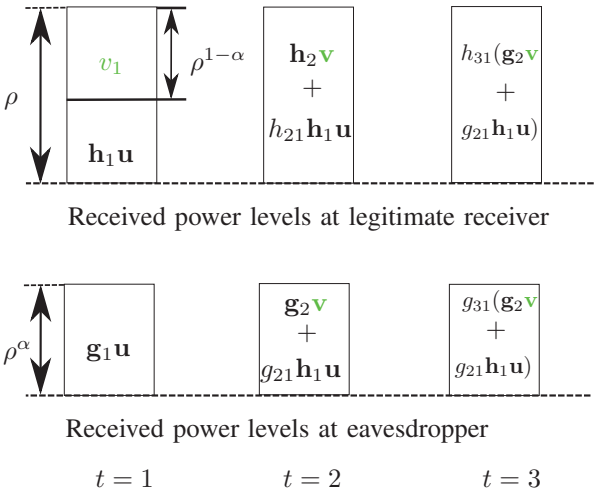

Fig. 2. Received power levels at the legitimate receiver and eavesdropper.

receiver. The eavesdropper will receive the confidential symbol embedded in with artificial noise but at reduced power level; and hence can not decode it. In this phase, the transmitter sends

$$\mathbf{x}_1 = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \begin{bmatrix} v_1\rho^{-\alpha/2} \\ \phi \end{bmatrix} \tag{12}$$

where $\mathbb{E}[\mathbf{u}^T\mathbf{u}] \doteq 1$ and $\mathbb{E}[||v_1||^2] \doteq 1$. The channel input-output relationship is given by

$$y_1 = \underbrace{\sqrt{\rho}\mathbf{h}_1\mathbf{u}}_{\mathcal{O}(\rho)} + \underbrace{\sqrt{\rho^{(1-\alpha)}}h_{11}v_1}_{\mathcal{O}(\rho^{1-\alpha})}, \tag{13a}$$

$$z_1 = \underbrace{\sqrt{\rho^{\alpha}}\mathbf{g}_1\mathbf{u}}_{\mathcal{O}(\rho^{\alpha})} + \underbrace{\sqrt{\rho^{0}}g_{11}v_1}_{\mathcal{O}(\rho^{0})}. \tag{13b}$$

At the end of phase 1, each receiver conveys the past CSI to the transmitter. Figure 2 illustrates the received power levels at the legitimate receiver and eavesdropper, respectively. At the end of phase 1, eavesdropper gets a linear combination of artificial noise along with the confidential symbol (v_1) at noise level; and, thus, it can not decode it. The legitimate receiver gets the confidential symbol embedded in with a linear combination of artificial noise ($\mathbf{h}_1\mathbf{u}$). It first re-constructs $\mathbf{h}_1\mathbf{u}$, from the channel output (y_1) by treating v_1 as noise, within bounded noise distortion. Afterwards, it subtracts out the contribution of $\mathbf{h}_1\mathbf{u}$ from y_1 and decodes v_1 through channel inversion. The information transmitted to legitimate receiver via v_1 symbol is given by

$$\begin{aligned} R_{v_1} &= I(v_1; y_1|\mathbf{h}_1\mathbf{u}) \\ &= h(\sqrt{\rho}\mathbf{h}_1\mathbf{u} + \sqrt{\rho^{(1-\alpha)}}h_{11}v_1|\mathbf{h}_1\mathbf{u}) \\ &\quad -h(\sqrt{\rho}\mathbf{h}_1\mathbf{u} + \sqrt{\rho^{(1-\alpha)}}h_{11}v_1|\mathbf{h}_1\mathbf{u}, v_1) \\ &= (1-\alpha)\log(\rho). \end{aligned} \tag{14}$$

Note that, via symbol v_1 only $(1-\alpha)\log(\rho)$ bits are securely transmitted.

In the second phase, the transmitter transmits fresh information ($\mathbf{v} := [v_2, v_3]^T$) to the legitimate receiver along with a linear combination of channel output ($\mathbf{h}_1\mathbf{u}$) at the legitimate receiver during the first phase. Since the transmitter already knows $\mathbf{u}$ and due to the availability of past CSI of legitimate receiver ($\mathbf{h}_1$) in phase 1, it can easily construct ($\mathbf{h}_1\mathbf{u}$) and sends

$$\mathbf{x}_2 = \begin{bmatrix} v_2 \\ v_3 \end{bmatrix} + \begin{bmatrix} \mathbf{h}_1\mathbf{u} \\ \phi \end{bmatrix} \tag{15}$$

The channel input-output relationship is given by

$$y_2 = \sqrt{\rho}\mathbf{h}_2\mathbf{v} + \sqrt{\rho}h_{21}\mathbf{h}_1\mathbf{u}, \tag{16a}$$

$$z_2 = \sqrt{\rho^{\alpha}}\mathbf{g}_2\mathbf{v} + \sqrt{\rho^{\alpha}}g_{21}\mathbf{h}_1\mathbf{u}. \tag{16b}$$

At the end of phase 2, each receiver conveys the past CSI to the transmitter. Since the legitimate receiver knows the CSI ($\mathbf{h}_2$) and also the channel output y_1 from phase 1, it subtracts out the contribution of $\mathbf{h}_1\mathbf{u}$ from the channel output y_2, to obtain one equation with two unknowns ($\mathbf{v} := [v_2, v_3]^T$). Thus, the legitimate receiver requires one extra equation to successfully decode the intended variables, being available as interference (side information) at eavesdropper but with *reduced* power level.

In the third phase, due to the availability of delayed CSIT, transmitter can construct the side information (z_2) at the eavesdropper and sends

$$\mathbf{x}_3 = \begin{bmatrix} \mathbf{g}_2\mathbf{v} + g_{21}\mathbf{h}_1\mathbf{u} \\ \phi \end{bmatrix}. \tag{17}$$

The channel input-output relationship is given by

$$y_3 = \sqrt{\rho}h_{31}\mathbf{g}_2\mathbf{v} + \sqrt{\rho}h_{31}g_{21}\mathbf{h}_1\mathbf{u}, \tag{18a}$$

$$z_3 = \sqrt{\rho^{\alpha}}g_{31}\mathbf{g}_2\mathbf{v} + \sqrt{\rho^{\alpha}}g_{31}g_{21}\mathbf{h}_1\mathbf{u}. \tag{18b}$$

At the end of phase 3, by using y_1, the legitimate receiver subtracts out the contribution of $\mathbf{h}_1\mathbf{u}$ from (y_2, y_3) and decodes $\mathbf{v}$ through channel inversion.

Equivocation Analysis. We can write the channel input-output relationship in compact form as

$$\mathbf{y} := \begin{bmatrix} \sqrt{\rho^{\alpha}} & \mathbf{0} \\ \sqrt{\rho}h_{21} & \sqrt{\rho}\mathbf{h}_2 \\ \sqrt{\rho}h_{31}g_{21} & \sqrt{\rho}h_{31}\mathbf{g}_2 \end{bmatrix} \begin{bmatrix} \mathbf{h}_1\mathbf{u} \\ \mathbf{v} \end{bmatrix}, \tag{19}$$

$$\mathbf{z} := \begin{bmatrix} \sqrt{\rho^{\alpha}}\mathbf{g}_1 & 0 \\ \sqrt{\rho^{\alpha}}g_{21}\mathbf{h}_1 & \sqrt{\rho^{\alpha}} \\ \sqrt{\rho^{\alpha}}g_{31}g_{21}\mathbf{h}_1 & \sqrt{\rho^{\alpha}}g_{31} \end{bmatrix} \begin{bmatrix} \mathbf{u} \\ \mathbf{g}_2\mathbf{v} \end{bmatrix}, \tag{20}$$

where the channel output in time slot 1 at legitimate receiver is normalized for convenience.

The information rate to legitimate receiver is bounded by

$$\begin{aligned} I(\mathbf{v}; \mathbf{y}|\mathbf{S}^n) &= I(\mathbf{v}; y_1|\mathbf{S}^n) + I(\mathbf{v}; y_2, y_3|y_1, \mathbf{S}^n) \\ &\overset{(a)}{=} I(\mathbf{v}; y_2, y_3|y_1, \mathbf{S}^n) \\ &= 2\log(\rho) \end{aligned} \tag{21}$$

where (a) follows due to the independence of $\mathbf{v}$ and y_1.

We can bound the information leakage to eavesdropper as

$$\begin{aligned} I(\mathbf{v};\mathbf{z}|\mathbf{S}^n) &\leq I(\mathbf{g}_2\mathbf{v},\mathbf{u};\mathbf{z}|\mathbf{S}^n) - I(\mathbf{u};\mathbf{z}|\mathbf{g}_2\mathbf{v},\mathbf{S}^n) \\ &= 2\alpha\log(\rho) - 2\alpha\log(\rho) \\ &= 0. \end{aligned} \tag{22}$$

From the above analysis, it can be easily seen that 3 symbols are securely transmitted to the legitimate receiver over a total of 3 time slots, yielding $\frac{3-\alpha}{3}$ SDoF. □

IV. Conclusion

In this paper, we study the generalize SDoF of a MISO wiretap channel. We assume perfect CSI is available at the receivers and each receiver only conveys the past CSI to the transmitter. In addition to this, links connecting both receivers may have unequal strengths. For this set-up we establish bounds on SDoF. For the case in which the legitimate receiver is stronger than the eavesdropper, the lower and upper bounds agree.

Appendix A
Proof of Lemma 1

Before proceeding to the proof of Lemma 1, for completeness we first introduce a property which is used to establish the results in this work.

Recall that, the channel output at eavesdropper is given by

$$z_i = \sqrt{\rho^{A_{2,i}}}\mathbf{g}_i\mathbf{x}_i + n_{2i}.$$

Now, lets consider an artificial channel $\tilde{z}_i$ at eavesdropper, such that channel input-output relationship at i-th time instant is

$$\tilde{z}_i = \sqrt{\rho^{A_{2,i}}}\tilde{\mathbf{g}}_i\mathbf{x}_i + \tilde{n}_{2i}$$

where $\tilde{\mathbf{g}}_i$ is the vector connecting artificial receiver to the transmitter and $\tilde{n}_{2i}$ is the channel noise. Let $\lambda_{\mathbf{g}_i}$ denotes the probability distribution from which, $\mathbf{g}_i$ and $\tilde{\mathbf{g}}_i$ are independent and identically drawn. Let $\mathbf{S}^n := \{\mathbf{g}_i, \tilde{\mathbf{g}}_i\}_{i=1}^n$.

Property 1: The channel local output symmetry states that

$$h(z_i|z^{i-1},\mathbf{S}^n) = h(\tilde{z}_i|z^{i-1},\mathbf{S}^n). \tag{23}$$

Proof: We begin the proof as follows.

$$\begin{aligned} h(z_i|z^{i-1},\mathbf{S}^n) &= h(z_i|z^{i-1},\mathbf{g}_i,\tilde{\mathbf{g}}_i,\mathbf{S}^n\setminus\mathbf{S}_i) \\ &= \mathbb{E}_{\lambda_{\mathbf{g}_i}}[h(\sqrt{\rho^{A_{2,i}}}\mathbf{g}\mathbf{x}_i + n_{2i} \\ &\quad |z^{i-1},\mathbf{g}_i=\mathbf{g},\tilde{\mathbf{g}}_i,\mathbf{S}^n\setminus\mathbf{S}_i)] \\ &\overset{(a)}{=} \mathbb{E}_{\lambda_{\mathbf{g}_i}}[h(\sqrt{\rho^{A_{2,i}}}\mathbf{g}\mathbf{x}_i + \tilde{n}_{2i}|z^{i-1},\mathbf{S}^n\setminus\mathbf{S}_i)] \\ &\overset{(b)}{=} \mathbb{E}_{\lambda_{\mathbf{g}_i}}[h(\sqrt{\rho^{A_{2,i}}}\mathbf{g}\mathbf{x}_i + \tilde{n}_{2i} \\ &\quad |z^{i-1},\tilde{\mathbf{g}}_i=\mathbf{g},\mathbf{g}_i,\mathbf{S}^n\setminus\mathbf{S}_i)] \\ &\overset{(c)}{=} \mathbb{E}_{\lambda_{\mathbf{g}_i}}[h(\tilde{z}_i|z^{i-1},\mathbf{g}_i,\tilde{\mathbf{g}}_i=\mathbf{g},\mathbf{S}^n\setminus\mathbf{S}_i)] \\ &= h(\tilde{z}_i|z^{i-1},\mathbf{S}^n) \end{aligned} \tag{24}$$

where (a) follows because n_{2i} and $\tilde{n}_{2i}$ are independent from $(\mathbf{x}_i,\mathbf{g}_i,\tilde{\mathbf{g}}_i)$ and have same statistics, (b) follows since $\mathbf{g}_i$ and $\tilde{\mathbf{g}}_i$ belongs to $\lambda_{\mathbf{g}_i}$ and have the same alphabet set; and (c) follows due to the independence of $\mathbf{x}_i$ and $(\mathbf{g}_i,\tilde{\mathbf{g}}_i)$. □

We now provide the proof of (9a) and (9c); due to the symmetry rest of the inequalities follow straightforwardly. We proceed as follows.

$$h(z^n|\mathbf{S}^n) = \sum_{i=1}^n h(z_i|z^{i-1},\mathbf{S}^n) \tag{25}$$

$$h(z^n|\mathbf{S}^n) = \sum_{i=1}^n h(\tilde{z}_i|z^{i-1},\mathbf{S}^n) \tag{26}$$

where (26) follows due to the property of channel local output symmetry. Then, by combining (25) and (26), we get

$$\begin{aligned} 2h(z^n|\mathbf{S}^n) &= \sum_{i=1}^n h(z_i|z^{i-1},\mathbf{S}^n) + h(\tilde{z}_i|z^{i-1},\mathbf{S}^n) \\ &\overset{(d)}{\geq} \sum_{i=1}^n h(z_i,\tilde{z}_i|z^{i-1},\mathbf{S}^n) \\ &= \sum_{i=1}^n h(z_i,\tilde{z}_i,y_i|z^{i-1},\mathbf{S}^n) - h(y_i|z^n,\tilde{z}_i,\mathbf{S}^n) \\ &= \sum_{i=1}^n h(z_i,y_i|z^{i-1},\mathbf{S}^n) + h(\tilde{z}_i|z_i,y_i,z^{i-1},\mathbf{S}^n) \\ &\quad - h(y_i|z^n,\tilde{z}_i,\mathbf{S}^n) \\ &\overset{(e)}{\geq} \sum_{i=1}^n h(z_i,y_i|z^{i-1},\mathbf{S}^n) \\ &\overset{(f)}{\geq} \sum_{i=1}^n h(z_i,y_i|z^{i-1},y^{i-1},\mathbf{S}^n) \\ &= h(z^n,y^n|\mathbf{S}^n) \\ &\geq h(z^n,y^n|\mathbf{S}^n) - n\lambda_{1\alpha}(1-\alpha)\log(\rho) \end{aligned} \tag{27}$$

where (d) and (f) follow form the fact that conditioning reduces entropy and (e) follows because with $(z_i,\tilde{z}_i,\mathbf{S}^n)$, one can first construct $\mathbf{x}_i$; and then y_i within bounded noise distortion, $h(y_i|z^n,\tilde{z}_i,\mathbf{S}^n) \leq no(\log(\rho))$.

We can also bound (27) as follows

$$\begin{aligned} 2h(z^n|\mathbf{S}^n) + n\lambda_{1\alpha}(1-\alpha)\log(\rho) &\geq h(z^n,y^n|\mathbf{S}^n) \\ &\geq h(y^n|\mathbf{S}^n) \end{aligned} \tag{28}$$

This concludes the proof.

Appendix B
Proof of Theorem 1

The converse uses elements from the proof established earlier in the context of wiretap channel with delayed CSIT [13] and also, uses properties of channel local output symmetry in Lemma 1. For convenience, we first denote the channel output at each receiver as

$$\begin{aligned} y^n &:= (y_{11}^n, y_{1\alpha}^n, y_{\alpha 1}^n, y_{\alpha\alpha}^n), \\ z^n &:= (z_{11}^n, z_{1\alpha}^n, z_{\alpha 1}^n, z_{\alpha\alpha}^n), \end{aligned}$$

ISBN 978-3-8007-3659-1

where $y^n_{A_1A_2}(z^n_{A_1A_2})$ denotes the part of channel output at receiver (eavesdropper), when $(A_1A_2) \in \{1,\alpha\}^2$ channel state occurs. We begin the proof as follows.

$$\begin{aligned}
nR_e &= H(W|z^n,\mathbf{S}^n)\\
&= H(W|\mathbf{S}^n) - I(W;z^n|\mathbf{S}^n)\\
&= I(W;y^n|\mathbf{S}^n) + H(W|y^n,\mathbf{S}^n) - I(W;z^n|\mathbf{S}^n)\\
&\overset{(a)}{\leq} I(W;y^n|\mathbf{S}^n) - I(W;z^n|\mathbf{S}^n) + n\epsilon_n \qquad (29)\\
&\leq I(W;y^n,z^n|\mathbf{S}^n) - I(W;z^n|\mathbf{S}^n) + n\epsilon_n\\
&= h(y^n,z^n|\mathbf{S}^n) - h(y^n|W,z^n,\mathbf{S}^n) - h(z^n|\mathbf{S}^n) + n\epsilon_n\\
&\leq h(y^n,z^n|\mathbf{S}^n) - h(z^n|\mathbf{S}^n) - \underbrace{h(y^n|W,\mathbf{x}^n,z^n,\mathbf{S}^n)}_{\geq no(\log(\rho))} + n\epsilon_n\\
&\overset{(b)}{\leq} h(z^n|\mathbf{S}^n) + n\lambda_{1\alpha}(1-\alpha)\log(\rho) + n\epsilon_n \qquad (30)
\end{aligned}$$

where $\epsilon_n \to 0$ as $n \to \infty$; (a) follows from Fano's inequality, (b) follows because (y^n) can be obtained within noise distortion form $(\mathbf{x}^n, \mathbf{S}^n)$, and using (9a).

We can also bound R_e as follows. From (29), we get

$$\begin{aligned}
nR_e &\leq I(W;y^n|\mathbf{S}^n) - I(W;z^n|\mathbf{S}^n) + n\epsilon_n\\
&\overset{(c)}{\leq} h(y^n|\mathbf{S}^n) - \frac{1}{2}h(z^n|W,\mathbf{S}^n) + \frac{n\lambda_{\alpha1}(1-\alpha)}{2}\log(\rho)\\
&\quad - h(z^n|\mathbf{S}^n) + h(z^n|W,\mathbf{S}^n) + n\epsilon_n\\
&\overset{(d)}{\leq} h(y^n|\mathbf{S}^n) - \frac{1}{2}h(z^n|\mathbf{S}^n) + \frac{n\lambda_{\alpha1}(1-\alpha)}{2}\log(\rho) + n\epsilon_n \qquad (31)
\end{aligned}$$

where (c) follows from (9d) and (d) follows from the fact that conditioning reduces entropy.

Then, combining these two upper bounds in (30) and (31), we get

$$\begin{aligned}
nR_e &\leq \min\Bigg\{h(z^n|\mathbf{S}^n) + n\lambda_{1\alpha}(1-\alpha)\log(\rho), h(y^n|\mathbf{S}^n)\\
&\quad - \frac{1}{2}h(z^n|\mathbf{S}^n) + \frac{n\lambda_{\alpha1}(1-\alpha)}{2}\log(\rho)\Bigg\} + n\epsilon_n \qquad (32)\\
&\overset{(e)}{\leq} \max_{h(y^n)} \frac{2}{3}h(y^n|\mathbf{S}^n) + \frac{n(1-\alpha)(\lambda_{1\alpha}+\lambda_{\alpha1})}{3}\log(\rho) + n\epsilon_n\\
&\overset{(f)}{\leq} \max_{h(y^n)} \frac{2}{3}\Bigg(h(y^n_{11}|\mathbf{S}^n) + h(y^n_{1\alpha}|\mathbf{S}^n) + h(y^n_{\alpha1}|\mathbf{S}^n)\\
&\quad + h(y^n_{\alpha\alpha}|\mathbf{S}^n)\Bigg) + \frac{n(1-\alpha)(\lambda_{1\alpha}+\lambda_{\alpha1})}{3}\log(\rho) + n\epsilon_n\\
&\leq \frac{(3-\alpha)\lambda_{1\alpha} + 2(\lambda_{11}+\alpha\lambda_{\alpha\alpha}) + (1+\alpha)\lambda_{\alpha1}}{3}n\log(\rho)\\
&\quad + n\epsilon_n \qquad (33)
\end{aligned}$$

where (e) follows by maximizing (32) with respect to $h(z^n|\mathbf{S}^n)$, and (f) follows from the fact that conditioning reduces entropy.

This concludes the proof.

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] M. J. Abdoli, A. Ghasemi, and A. K. Khandani, "On the degrees of freedom of three-user MIMO broadcast channel with delayed CSIT," in *IEEE International Symposium on Information Theory*, St. Petersburg, Russia, Aug. 2011, pp. 209–213.

[5] C. S. Vaze and M. K. Varanasi, "The degrees of freedom region and interference alignment for the MIMO interference channel with delayed CSIT," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4396–4417, Jul. 2012.

[6] A. Ghasemi, A. S. Motahari, and A. K. Khandani, "Interference alignment for the MIMO interference channel with delayed local CSIT," 2011. [Online]. Available: http://arxiv.org/abs/1102.5673

[7] R. Tandon, S. Mohajer, H. V. Poor, and S. Shamai (Shitz), "On X-channels with feedback and delayed CSI," in *IEEE International Symposium on Information Theory*, Boston, USA, Jul. 2012, pp. 1887–1891.

[8] A. Ghasemi, M. J. Abdoli, and A. K. Khandani, "On the degrees of freedom of MIMO X channel with delayed CSIT," in *IEEE International Symposium on Information Theory*, Boston, USA, Jul. 2012, pp. 1902–1906.

[9] J. Chen, P. Elia, and S. A. Jafar, "On the vector broadcast channel with alternating CSIT: A topological perspective," 2014. [Online]. Available: http://arxiv.org/abs/1402.5912

[10] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[11] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[12] 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.

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