On the Multi-Antenna Wiretap Channel with Delayed CSI at the Transmitter

Mari Kobayashi,
Dept. Telecommunications,
SUPELEC
91192 Gif-sur-Yvette, France
mari.kobayashi@supelec.fr

Pablo Piantanida
Dept. Telecommunications,
SUPELEC
91192 Gif-sur-Yvette, France
pablo.piantanida@supelec.fr

Sheng Yang
Dept. Telecommunications,
SUPELEC
91192 Gif-sur-Yvette, France
sheng.yang@supelec.fr

Shlomo Shamai (Shitz)
Technion-Israel Institute of
Technology
Haifa, Israel
sshlomo@ee.technion.ac.il

ABSTRACT

The multi-input single-output (MISO) Gaussian wiretap channel with delayed channel state information (CSI) available at the transmitter and at the eavesdropper is investigated. This scenario may occur when the legitimate receiver sends its channel state to the transmitter via a delayed feedback link which can be also overheard by an eavesdropper. We show that delayed CSI, even completely outdated, offers the opportunity to ensure the secrecy. Namely, by aligning the artificial noise at the legitimate receiver, a secrecy degrees of freedom (SDoF) of $1/2$ can be achieved. It turns out that the result is irrelevant to whether the transmitter knows the legitimate channel or the eavesdropper channel with a delay and both cases yield the equivalent opportunity. The artificial noise scheme can be further extended to the case of broadcast channel with two confidential messages.

Categories and Subject Descriptors

H.1.1 [**Models and Principles**]: Systems and Information Theory; E.4 [**Coding and Information Theory**]

General Terms

Theory, Security

Keywords

Physical layer security, Wiretap channel

1. INTRODUCTION

Although transmitter perfect channel state information at transmitter (CSIT) may not be available in most practical scenarios due to time-varying nature of wireless channels, many wireless applications must still guarantee secure and reliable communication. In fast fading scenarios, the channel estimation/feedback process is often slower than the coherence time and CSIT may be further outdated. In [1], the authors considered such scenario in the context of multi-input single-output (MISO) broadcast channels. By assuming delayed CSIT from each receiver and perfect CSI at the receivers, they established the optimal sum degrees of freedom (DoF). These results show that, by a careful design of linear precoding schemes, completely outdated CSIT which is independent of the current channel state can significantly increase the DoF. Recently, [2] extended the work for the two-user multi-input multi-output (MIMO) broadcast channels. The same feedback model has been also studied in [3] where the authors proposed the so-called retrospective interference alignment for networks with distributed encoders.

The secrecy capacity of MISO Gaussian wiretap channels is not yet fully understood for the case of partial or imperfect CSIT (see [4] and references therein). Due to the difficulty of the complete characterization, a number of contributions have first focused on secrecy degrees of freedom (SDoF) capturing the behavior in high signal-to-noise (SNR) regime (see e.g. [5–8]). References [5–7] have studied compound models where the channel uncertainty is given as a set of finite states and the channel remains in one of these states during the whole communication. In this paper, inspired by the previous works on delayed CSIT, we study the impact of delayed CSIT on the MISO Gaussian wiretap channel where the transmitter wishes to convey a confidential message to the legitimate receiver in the presence of an eavesdropper. Namely, we assume that the legitimate receiver sends its CSI over a delayed feedback link which is overheard by the eavesdropper as well. It is shown that, analogy with the conclusions in [1, 3], delayed CSIT, even though completely outdated, can increase the SDoF. More precisely, a SDoF of $1/2$ can be achieved by a simple artificial noise scheme which aligns the artificial noise at the legitimate receiver. Interestingly, the result is irrelevant to whether the transmitter knows the legitimate channel or the eavesdropper channel with a delay, but both cases yield the equivalent opportunity. Finally, we consider the broadcast channel where the transmitter wishes to send two confidential messages respectively to two receivers while keeping each of them secret to the unintended receiver. We show that by generalizing the artificial noise scheme a SDoF of $1/3$ can be achieved for each receiver.

This paper is organized as follows. Section II introduces the system

SECURENETS 2011, May 16, Paris, France

DOI 10.4108/icst.valuetools.2011.245781

model and main definitions while in Section III noise alignment schemes are derived. Finally, Section IV concludes the paper.

In this paper, we adopt the following notations. Let $[x]_+ = \max\{0, x\}$ and define the indicator function $\mathbf{1}\{\cdot\}$. We use $||\mathbf{a}||, |\mathbf{A}|, \mathbf{A}^\dagger, \mathbf{A}^H, \text{tr}(\mathbf{A})$ to denote the norm of a vector $\mathbf{a}$, the determinant, the transpose, the hermitian transpose, and the trace of a matrix $\mathbf{A}$, respectively. Denote the n-length vector $\mathbf{x}^n = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ and let $\text{diag}(\mathbf{a}_1, \ldots, \mathbf{a}_T)$ be a block-diagonal matrix where the t-th row contains $\mathbf{a}_t$ for $t = \{1, \ldots, T\}$. We let $\mathbf{I}_n, \mathbf{0}_{n\times m}$ denote a $n \times n$ identity matrix, and a $n \times m$ matrix with zero entries.

2. SYSTEM MODEL

Consider the Gaussian MISO wiretap channel where the transmitter with M antennas sends a confidential message to the legitimate receiver in the presence of an eavesdropper. The corresponding channel models are given by

$$y_\tau = \mathbf{h}_\tau^\dagger \mathbf{x}_\tau + n_\tau, \tag{1}$$

$$z_\tau = \mathbf{g}_\tau^\dagger \mathbf{x}_\tau + \nu_\tau, \tag{2}$$

for $\tau = \{1, \ldots, n\}$, where (y_τ, z_τ) denotes the observations at the legitimate and the eavesdropper receivers at channel use τ, associated to M-input single-output channel vector $\mathbf{h}_\tau, \mathbf{g}_\tau \in \mathbb{C}^{M\times 1}$, respectively, and (n_τ, ν_τ) are assumed to be independent and identically distributed (i.i.d.) additive white Gaussian noises $\sim \mathcal{N}_{\mathbb{C}}(0, 1)$, the input vector $\mathbf{x}_\tau \in \mathbb{C}^{M\times 1}$ is subjected to the power constraint $\sum_{\tau=1}^{n} \text{tr}(\mathbf{x}_\tau \mathbf{x}_\tau^H) \leq nP$. We assume that any arbitrary stationary fading process where $\{\mathbf{h}_\tau\}$ and $\{\mathbf{g}_\tau\}$ are mutually independent and change from a channel use to another in an independent manner.

DEFINITION 1 (CODE AND ACHIEVABILITY). *A $(2^{nR_s(P)}, n, \epsilon)$-code for the Gaussian MISO wiretap channel consists of a sequence of stochastic encoders $\left\{F_S^n : \mathcal{W}_n \times \mathscr{H}^{n-1} \longmapsto \mathscr{X}^n\right\}$ for a random variable $S \in \mathcal{S}$ unknown at the decoder, a message set $\mathcal{W} = \{1, \ldots, 2^{nR_s(P)}\}$ with $w \in \mathcal{W}_n$ uniformly distributed over $\mathcal{W}_n$ and a legitimate decoder $\left\{\phi : \mathscr{Y}^n \times \mathscr{H}^n \longmapsto \mathcal{W}_n\right\}$ where $\mathscr{H}^n$ is the set of possible channel state vectors. A rate R_s is* achievable *if for any $\epsilon > 0$, there exists a $(2^{nR_s}, n, \epsilon)$-code that simultaneously satisfies the average error probability of the legitimate receiver*

$$P_e^{(n)} \leq \epsilon$$

and the equivocation rate

$$nR_s(P) - H(W|Z^n, G^n, H^{n-1}) \leq n\epsilon. \tag{3}$$

Notice that (3) *requires perfect secrecy of the confidential message at the eavesdropper with delayed state knowledge. The achievable SDoF is defined by*

$$d_s = \lim_{P\to\infty} \frac{R_s(P)}{\log P}. \tag{4}$$

ASSUMPTION 2.1. *It is assumed that both the transmitter and the eavesdropper have delayed CSI of the legitimate channel, i.e. at time τ they know $\mathbf{h}_1, \ldots, \mathbf{h}_{\tau-1}$. In addition, at each time τ the legitimate and the eavesdropper receiver know $\mathbf{h}_1, \ldots, \mathbf{h}_\tau$ and $\mathbf{g}_1, \ldots, \mathbf{g}_\tau$, respectively.*

An achievable rate is given by the following expression:

$$R_s(P) \geq \liminf_{n\to\infty} \sup_{(X^n, V^n|H^{n-1})} \frac{1}{n}\big[I(V^n; Y^n, H_n|H^{n-1}) - I(V^n; Z^n, G^n|H^{n-1})\big], \tag{5}$$

where the supremum is taken over all sequences of random variables (V^n, X^n) satisfying $V_\tau \longleftrightarrow (X_\tau, H_\tau, G_\tau) \longleftrightarrow (Y_\tau, Z_\tau)$ for all $\tau = \{1, \ldots, n\}$ and the power constraint, where (V_τ, X_τ) do not depend on $(G^n, H_\tau, \ldots, H_n)$.

3. ARTIFICIAL NOISE ALIGNMENT WITH DELAYED CSIT

3.1 Staggered fading channel

Hereafter, we focus on the two-antenna case $M = 2$ without loss of generality [1].

Let us first recall the optimal linear strategy for the staggered fading channel where the eavesdropper channel varies twice faster than the legitimate channel, i.e. $T_\tau = 2$ and $T_e = 1$, given by the following block diagonal matrix [8]

$$\mathbf{H} = \text{diag}(\mathbf{h}_1^\dagger, \mathbf{h}_1^\dagger), \quad \mathbf{G} = \text{diag}(\mathbf{g}_1^\dagger, \mathbf{g}_2^\dagger), \tag{6}$$

where $\mathbf{g}_1$ and $\mathbf{g}_2$ are linearly independent. The transmitter knows the structure of the channel but does not know the specific realizations $(\mathbf{h}_1, \mathbf{g}_1, \mathbf{g}_2)$. In this case, we adapt the artificial noise (AN) scheme [9] to the specific channel structure and form the transmit vector of dimension over two symbols $\mathbf{x} = [\mathbf{x}_1^\dagger, \mathbf{x}_2^\dagger]^\dagger$ as

$$\mathbf{x} = \begin{bmatrix} 1 \\ \mathbf{0}_3 \end{bmatrix} v + \begin{bmatrix} \mathbf{I}_2 \\ \mathbf{I}_2 \end{bmatrix} \mathbf{u}, \tag{7}$$

where $v \sim \mathcal{N}_{\mathbb{C}}(0, \tilde{P})$ denotes the symbol corresponding to the confidential message and $\mathbf{u} \sim \mathcal{N}_{\mathbb{C}}(\mathbf{0}, \tilde{P}\mathbf{I}_2)$ denotes the AN, independent of v, and we let $\tilde{P} = P/3$. By ignoring the Gaussian noise, the observations over two symbols at the legitimate receiver and the eavesdropper are respectively given by

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} h_1[1] \\ 0 \end{bmatrix} v + \underbrace{\begin{bmatrix} \mathbf{h}_1^\dagger \\ \mathbf{h}_1^\dagger \end{bmatrix}}_{\text{rank 1}} \mathbf{u} \tag{8}$$

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} g_1[1] \\ 0 \end{bmatrix} v + \underbrace{\begin{bmatrix} \mathbf{g}_1^\dagger \\ \mathbf{g}_2^\dagger \end{bmatrix}}_{\text{rank 2}} \mathbf{u}.$$

It follows immediately that the artificial noise aligns in one dimension at the legitimate receiver while it occupies two full dimensions at the eavesdropper. As a result, the confidential message spans in one dimension which yields the SDoF=$1/2$. It has been proved in [8] that this is indeed the optimal SDoF.

3.2 Delayed CSIT over i.i.d. varying channel

Assume now an i.i.d. fading with the delayed CSIT assumption 2.1. The artificial noise alignment of (7) can be suitably modified here to provide a positive SDoF as summarized in the next theorem.

THEOREM 1. *The MISO Gaussian wiretap channel with $M \geq 2$ transmit antennas under the assumption 2.1 achieves the SDoF=1/2.*

[1] The extension to $M > 2$ is rather trivial and the results remain unchanged.

PROOF. Let us consider two consecutive symbols and form the transmitted vector $\mathbf{x}_t$ such that

$$\mathbf{x}_1 = \begin{bmatrix} v \\ 0 \end{bmatrix} + \mathbf{u}, \quad \mathbf{x}_2 = c \begin{bmatrix} \mathbf{h}_1^\dagger \mathbf{u} \\ 0 \end{bmatrix} \tag{9}$$

where $v \sim \mathcal{N}_{\mathbb{C}}(0, \tilde{P})$ is the confidential symbol and $\mathbf{u} \sim \mathcal{N}_{\mathbb{C}}(\mathbf{0}, \tilde{P}\mathbf{I}_2)$ is the AN of dimension 2, and c is any constant chosen to satisfy the power constraint where $\tilde{P} = \frac{P}{3}$. Notice that at time 2, only one of the antennas, say antenna 1, is used to send the AN observed by the legitimate receiver in symbol 1. By ignoring the Gaussian noise, the observations over two symbols at the legitimate receiver and the eavesdropper are respectively given by

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} h_1[1] \\ 0 \end{bmatrix} v + \underbrace{\begin{bmatrix} \mathbf{h}_1^\dagger \\ ch_2[1]\mathbf{h}_1^\dagger \end{bmatrix}}_{\text{rank 1}} \mathbf{u} \tag{10}$$

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} g_1[1] \\ 0 \end{bmatrix} v + \underbrace{\begin{bmatrix} \mathbf{g}_1^\dagger \\ cg_2[1]\mathbf{h}_1^\dagger \end{bmatrix}}_{\mathbf{G}} \mathbf{u}.$$

By following the same lines as the previous staggered model in (8), here the AN term $\mathbf{u}$ is aligned at the legitimate receiver while it spans in two-dimensional space at the eavesdropper ($\mathbf{h}_1$ and $\mathbf{g}_1$ are linearly independent almost surely due to independence assumption over users). Again, one confidential symbol can be secretly conveyed over two channel uses. More precisely, we have the following mutual informations

$$I(v; y_1^2 | \mathbf{h}_1, \mathbf{h}_2) = I(v; y_1 - ch_2[1]y_2) \tag{11}$$

$$= \log\left(1 + \tilde{P}|h_1[1]|^2\right) \tag{12}$$

$$I(v; z_1^2 | \mathbf{h}_1, \mathbf{g}_1, \mathbf{g}_2) = \log\left(1 + \frac{\tilde{P}|g_1[1]|^2}{1 + \tilde{P}\text{tr}(\mathbf{G})}\right). \tag{13}$$

By repeating the same strategy every two channel uses and plugging the above expressions into (5), it follows that a SDoF=$1/2$ is achievable. □

Remark 3.1. *It is interesting to remark that the same SDoF can be achieved when the transmitter has the delayed channel state of the eavesdropper channel instead. In this case, we consider two consecutive slots and form the input vectors as follows.*

$$\mathbf{x}_1 = \begin{bmatrix} v \\ u \end{bmatrix}, \quad \mathbf{x}_2 = c \begin{bmatrix} \mathbf{g}_1^\dagger \mathbf{x}_1 \\ 0 \end{bmatrix} \tag{14}$$

where v, u denotes the confidential symbol, the artificial noise and c is a constant to satisfy the power constraint. It is not difficult to see that at the legitimate receiver both the useful signal and the artificial noise span one dimension, whereas the eavesdropper is unable to detect v from the observation spanning in a single dimension.

Remark 3.2. *Comparing (7) and (9), the artificial noise is* repeated *over two time slots such that it is aligned at the legitimate receiver but spans in the full dimension at the eavesdropper. The way how it is repeated depends on the side information available to the transmitter. On one hand, in the staggered fading channel there is no CSIT but the encoder exploits the structure of the fading process, namely $\mathbf{h}_2 = \mathbf{h}_1$, in the upcoming two symbols. On the other hand, in the delayed CSIT model the encoder learns $\mathbf{h}_1$ at the time 2. In both cases, the side information enables the encoder to identify in which subspace the vectors $[\mathbf{h}_1, \mathbf{h}_2]$ lie in. Namely, the subspace of the staggered model is given by*

$$[\mathbf{I}_2\ \mathbf{I}_2]\mathbf{h}$$

while the subspace of the delayed CSIT model is given by

$$[\mathbf{0}_{2\times 2}\ \mathbf{I}_2]\mathbf{h} + [\mathbf{h}_1\ \mathbf{0}_{2\times 1}]$$

for $\mathbf{h} \in \mathbb{C}^{M\times 1}$. Clearly both subspaces have two dimensions. Such partial knowledge is sufficient to align the AN at the desired receiver.

Remark 3.3. *The SDoF of Theorem 1 might be pessimistic over the temporally correlated fading channel if the transmitter can (almost) perfectly predict the channel via the delayed CSIT. The Doppler process [10] corresponds to such a case. A well-known example of the Doppler process is the* Jakes correlation model. *Let us assume that the covariance[2] is given by $\mathbb{E}[\mathbf{h}_{\tau+i}\mathbf{h}_\tau^\dagger] = \mathbf{R}_i$ for any τ and i. With the knowledge on $\{\mathbf{R}_i\}$, the transmitter can predict the channel for $t \geq 2$ and can send the AN in the null space at each symbol rather than applying the AN over symbols. By repeating this for T channel uses the SDoF=$\frac{T-1}{T} \longrightarrow 1$ for T arbitrarily large.*

Although we are not able to prove the optimality of the SDoF stated by Theorem 1, it is possible to show the optimality by limiting ourselves to the class of linear Gaussian schemes with artificial noise, as already proposed for other multi-user networks with delayed CSIT [1, 3]. In general, by stacking T blocks such that $\mathbf{x} = [\mathbf{x}_1^\dagger, \ldots, \mathbf{x}_T^\dagger]^\dagger$, the input vector of dimension MT can be expressed as[3]

$$\mathbf{x}^{(T)} = \mathbf{v}^{(T)} + \mathbf{u}^{(T)},$$

where $\mathbf{v}^{(T)}$ corresponds to the useful symbols of the legitimate receiver, and $\mathbf{u}^{(T)}$ independent of $\mathbf{v}^{(T)}$ is destined to the other receiver (in our case this is the AN to perturb the eavesdropper). Accordingly, we consider the MT-input T-output MIMO system with block diagonal matrices $\mathbf{H} = \text{diag}(\mathbf{h}_1, \ldots, \mathbf{h}_T)$ and $\mathbf{G} = \text{diag}(\mathbf{g}_1, \ldots, \mathbf{g}_T)$. With this precoding scheme, we have

$$I(\mathbf{v}^{(T)}; \mathbf{y}^{(T)}) - I(\mathbf{v}^{(T)}; \mathbf{z}^{(T)} | \mathbf{h}^{(T-1)}) = H(\mathbf{z}^{(T)} | \mathbf{v}^{(T)}, \mathbf{h}^{(T-1)}) - H(\mathbf{y}^{(T)} | \mathbf{v}^{(T)}) + H(\mathbf{y}^{(T)}) - H(\mathbf{z}^{(T)} | \mathbf{h}^{(T-1)}). \tag{15}$$

By letting $\mathbf{R}_v, \mathbf{R}_u$ denote the covariance of $\mathbf{v}^{(T)}, \mathbf{u}^{(T)}$, respectively, we perform the Choleskey decomposition such that $\mathbf{R}_u = \mathbf{U}\mathbf{U}^H$ and $\mathbf{R}_v = \mathbf{V}\mathbf{V}^H$. Then, it is not difficult to see that an achievable SDoF over a block length T is given by

$$\begin{aligned} Td_s^{(T)} &= \text{rank}(\mathbf{GU}) - \text{rank}(\mathbf{HU}) \\ &\quad + \text{rank}(\mathbf{H}(\mathbf{U}+\mathbf{V})) - \text{rank}(\mathbf{G}(\mathbf{U}+\mathbf{V})) \\ &\leq \text{rank}(\mathbf{GU}) - \text{rank}(\mathbf{HU}) \end{aligned} \tag{16}$$

where the last inequality comes from the fact that $\mathbf{G}$ does not depend on $\mathbf{U}$ and $\mathbf{V}$. Finally, we have the following result.

[2] If there is no spatial correlation, $\mathbf{R}_i = J_0(2\pi F i)\mathbf{I}$ where F denotes the maximum Doppler frequency shift.

[3] Here we assume that the input vector is repeated as an arbitrary large number of m channel uses with $n = mT$.

PROPOSITION 3.1. *Under the assumption 2.1, we have*

$$Td_s^{(T)} \leq \min\{rank(\mathbf{HU}), T - rank(\mathbf{HU})\} \quad (17)$$

which implies

$$d_s^{(T)} \leq \frac{1}{2}. \quad (18)$$

PROOF. Let us rewrite $\mathbf{HU}$ as $[\mathbf{U}_1\mathbf{h}_1 \ \cdots \ \mathbf{U}_T\mathbf{h}_T]^\dagger$ where $\mathbf{U}_t^\dagger \in \mathbb{C}^{MT\times M}$ is the t th subblock matrix of $\mathbf{U}$ such that $\mathbf{U} = [\mathbf{U}_1^\dagger \ \cdots \ \mathbf{U}_T^\dagger]$. Defining $k \triangleq \text{rank}(\mathbf{HU})$ and assume, without loss of generality that, the first k rows of $\mathbf{HU}$ are linear independent, i.e.,

$$\text{rank}\left(\mathbf{U}_1^\dagger\mathbf{H}_1, \ldots, \mathbf{U}_k^\dagger\mathbf{H}_k\right) = k.$$

Let $\mathcal{S}$ denote the associated row subspace with $\dim(\mathcal{S}) = k$. It is readily shown that the rows in $\mathbf{U}_t$ should lie in $\mathcal{S}$ for $t \geq k+1$. Otherwise, there would exist a linear combination defined by $\mathbf{H}_t$ such that $\text{rank}(\mathbf{HU}) > k$, which contradicts the assumption. Thus, we have

$$\text{rank}\left(\mathbf{U}_{k+1}^\dagger, \ldots, \mathbf{U}_T^\dagger\right) \leq k. \quad (19)$$

It implies that the rank of the last $T-k$ rows of $\mathbf{GU}$, rewritten as

$$\text{diag}\left\{\mathbf{G}_{k+1}^\dagger, \ldots, \mathbf{G}_T^\dagger\right\}[\mathbf{U}_{k+1}^\dagger \ \cdots \ \mathbf{U}_T^\dagger]^\dagger$$

cannot exceed $\min\{k, T-k\}$ since for matrices $\mathbf{A}$ and $\mathbf{B}$,

$$\text{rank}\left(\mathbf{AB}\right) \leq \min\left\{\text{rank}\left(\mathbf{A}\right), \text{rank}\left(\mathbf{B}\right)\right\}. \quad (20)$$

Finally, we have

$$\text{rank}\left(\mathbf{GU}\right) - \text{rank}\left(\mathbf{HU}\right) \leq \min\{k, T-k\}. \quad (21)$$

□

4. BROADCAST CHANNEL WITH CONFIDENTIAL MESSAGES (BCC)

Consider now the two-user MISO broadcast channel with confidential messages (BCC) in which the transmitter sends two confidential messages (W_1, W_2) to the receivers 1 and 2, respectively. Each of these messages must be kept secret from the other. We assume delayed CSIT from both channel states which means that at the time τ the states $(\mathbf{h}^{\tau-1}, \mathbf{g}^{\tau-1})$ are available to the encoder and the receivers as stated below.

ASSUMPTION 4.1. *It is assumed that $\mathbf{h}^{\tau-1}$ is known to the transmitter and receiver 2 while $\mathbf{g}^{\tau-1}$ is known to the transmitter and receiver 1 at time τ. However, both receivers know perfectly their own channels.*

An achievable rate region is given by the convex hull of the set of rates

$$R_1(P) \geq \liminf_{n\to\infty} \frac{1}{n}\big[I(V^n; Y^n, H^n|H^{n-1}, G^{n-1}) - I(V^n; U^n, Z^n, G^n|H^{n-1}, G^{n-1})\big], \quad (22)$$

$$R_2(P) \geq \liminf_{n\to\infty} \frac{1}{n}\big[I(U^n; Z^n, G^n|H^{n-1}, G^{n-1}) - I(U^n; V^n, Y^n, H^n|H^{n-1}, G^{n-1})\big], \quad (23)$$

where the union is taken over all sequence of random variables (V^n, U^n, X^n) satisfying $(U_\tau, V_\tau) \longleftrightarrow (X_\tau, H_\tau, G_\tau) \longleftrightarrow (Y_\tau, Z_\tau)$ for all $\tau = \{1, \ldots, n\}$ and the power constraint, where (U_τ, V_τ, X_τ) do not depend on $(G_\tau, \ldots, G_n, H_\tau, \ldots, H_n)$. Then, an achievable SDoF region is given by the set of positive numbers

$$d_k = \lim_{P\to\infty} \frac{R_k(P)}{\log P}, \ \ k = 1, 2. \quad (24)$$

In the next theorem we show that the AN scheme previously derived can be suitably modified to convey two confidential messages. Interestingly, the scheme coincides with the linear precoding strategy [1] proposed for the MISO broadcast channel to the MISO-BCC.

THEOREM 2. *The two-user MISO Gaussian BCC achieves a pair of SDoF $(d_1, d_2) = (\frac{1}{3}, \frac{1}{3})$ under the assumption 4.1.*

PROOF. We extend the AN scheme of (9) to the case of two messages by considering an additional (third) symbol. Namely, we form the transmit vector $\mathbf{x}_t$ such that

$$\mathbf{x}_1 = \mathbf{v} + \mathbf{u}, \ \ \mathbf{x}_2 = c_1\begin{bmatrix}\mathbf{h}_1^\dagger\mathbf{u}\\ 0\end{bmatrix}, \ \ \mathbf{x}_3 = c_2\begin{bmatrix}\mathbf{g}_1^\dagger\mathbf{v}\\ 0\end{bmatrix} \quad (25)$$

where $\mathbf{v}, \mathbf{u} \sim \mathcal{N}_{\mathbb{C}}(\mathbf{0}, \tilde{P}\mathbf{I}_2)$, mutually independent, corresponds to the vector of the confidential message to receivers 1 and 2, c_1, c_2 are constant so that the power constraint is satisfied and we have $\tilde{P} = \frac{P}{4}$. By interpreting the confidential message destined to the other user as artificial noise, the above coding scheme is a straightforward extension of (9), where the artificial noise overheard by receiver 2 is repeated in the third symbol. It essentially coincides with the interference alignment first proposed in [1]. The output observations over three symbols are given by

$$\begin{bmatrix}y_1\\ y_2\\ y_3\end{bmatrix} = \underbrace{\begin{bmatrix}\mathbf{h}_1^\dagger\\ \mathbf{0}_{1\times 2}\\ h_3[1]c_2\mathbf{g}_1^\dagger\end{bmatrix}}_{\mathcal{H}}\mathbf{v} + \begin{bmatrix}\mathbf{h}_1^\dagger\\ ch_2[1]\mathbf{h}_1^\dagger\\ \mathbf{0}_{1\times 2}\end{bmatrix}\mathbf{u},$$

$$\begin{bmatrix}z_1\\ z_2\\ z_3\end{bmatrix} = \underbrace{\begin{bmatrix}\mathbf{g}_1^\dagger\\ c_1g_2[1]\mathbf{h}_1^\dagger\\ \mathbf{0}_{1\times 2}\end{bmatrix}}_{\mathcal{G}}\mathbf{u} + \begin{bmatrix}\mathbf{g}_1^\dagger\\ \mathbf{0}_{1\times 2}\\ c_2g_3[1]\mathbf{g}_1^\dagger\end{bmatrix}\mathbf{v}. \quad (26)$$

It readily follows that the unintended symbol vector is aligned in one dimension at both receivers while the useful symbol vector spans in two dimensions. More precisely we have the following mutual informations

$$I(\mathbf{v}; y^3, \mathbf{h}^3) = I(v; y_1 - c_1h_2[1]y_2, y_3) = \log\left|\mathbf{I}_3 + \tilde{P}\mathcal{H}\mathcal{H}^H\right|, \quad (27)$$

$$I(\mathbf{v}; \mathbf{z}^3, \mathbf{g}^3|\mathbf{u}, \mathbf{h}^2) = \log\{1 + \tilde{P}(1 + |c_2g_3[1]|^2|\mathbf{g}_1|^2)\}. \quad (28)$$

By plugging these into (22) and repeating the same strategy every three symbols, it follows that $d_1 = \frac{1}{3}$. By symmetry, we also have $d_2 = \frac{1}{3}$. □

5. CONCLUSIONS

Inspired by recent results [1–3], we studied in terms of secrecy degrees of freedom (SDoF) the impact of delayed CSIT on the MISO

Gaussian wiretap channel. It is shown that even with completely outdated CSIT, either on the legitimate or the eavesdropper channel, a simple artificial noise alignment scheme enables the encoder to achieve a SDoF=$1/2$. Furthermore, this scheme can be suitably extended to the broadcast channel with two confidential messages and yields a sum SDoF=$2/3$. Although we focus on simple scenarios and achievability results, more complex scenarios and upper bounds on the corresponding SDoF have to be further investigated.

Acknowledgment

This work is partially supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications NEWCOM++.

6. REFERENCES

[1] M. Maddah-Ali and D. Tse, "On the degrees of freedom of miso broadcast channels with delayed feedback," *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2010-122, Sep*, pp. 2010–122, 2010.

[2] C. Vaze and M. Varanasi, "The Degrees of Freedom Region of the Two-User MIMO Broadcast Channel with Delayed CSI," *Arxiv preprint arXiv:1101.0306*, 2010.

[3] H. Maleki, S. Jafar, and S. Shamai, "Retrospective Interference Alignment," *Arxiv preprint arXiv:1009.3593*, 2010.

[4] R. Bustin, R. Liu, H. V. Poor, and S. S. (Shitz), "An MMSE Approach to the Secrecy Capacity of the MIMO Gaussian Wiretap Channel," *EURASIP, special issue on Wireless Physical Security*, 2009.

[5] Y. Liang and G. Kramer and H. V. Poor and S. Shamai (Shitz), "Compound Wiretap Channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[6] A. Khisti, "Interference Alignment for the Multi-Antenna Compound Wiretap Channel," *Arxiv preprint arXiv:1002.4548*, 2010.

[7] M. Kobayashi, Y. Liang, S. Shamai, and M. Debbah, "On the Compound MIMO Broadcast Channels with Confidential Messages," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT'09), Seoul, Korea.*, 2009, pp. 1283–1287.

[8] M. Kobayashi, P. Piantanida, S. Yang, and S. Shamai, "On the secrecy degrees of freedom of the multi-antenna block fading wiretap channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT'10), Austin, TX.*, 2010, pp. 2563–2567.

[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[10] E. Biglieri, J. Proakis, and S. Shamai, "Fading Channels: Information-Theoretic and Communications Aspects," *IEEE Trans. on Inform. Theory*, vol. 44, no. 6, p. 2619, 1998.