Secure communication in K-user multi-antenna broadcast channel with state feedback

Sheng Yang, Mari Kobayashi

Secure Communication in K-user Multi-Antenna Broadcast Channel with State Feedback

Sheng Yang and Mari Kobayashi
LSS, CentraleSupélec
Gif-sur-Yvette, France
{sheng.yang,mari.kobayashi}@centralesupelec.fr

***Abstract*—In this paper, we consider the secure communication in a K-user multi-antenna broadcast channel (BC) with state feedback. We characterize the optimal secure degrees of freedom (SDoF) region of multiple-input single-output (MISO) channel. The SDoF region is achievable by a secret key based linear scheme, which generates analog secret keys by sending artificial noise and then performs space-time alignment scheme secured by these secret keys. The optimality is proved by deriving a new outer bound on the capacity region in a systematic way. Interestingly, the proposed outer bounding technique also applies to the erasure broadcast channel and provides a simpler proof as compared to the existing one. Finally, an explicit connection between the multi-antenna BC and the erasure BC is revealed. We show that, with a large number of users, secrecy cannot be guaranteed in the erasure BC, while it comes almost "for free" in the multi-antenna BC when the number of transmit antennas grows accordingly.**

I. Introduction

In wireless communication systems, channel state information at transmitter is usually obtained via feedback from receivers. Hence, it may not be accurate due to the time-varying nature of the underlying channel as well as limited resource for the channel estimation/feedback. In fast fading scenarios, the state information may be even outdated when it becomes available at the transmitter. Recent works have shown the usefulness of such feedback, even if it is completely outdated. In [4], [5], the authors have studied the state feedback in the context of K-user broadcast erasure channel and characterized the capacity region under some symmetry conditions. In [1], Maddah-Ali and Tse have considered K-user multi-input single-output (MISO) broadcast channel with K antennas and characterized its degrees of freedom (DoF) region, i.e., the prelog factor of capacity at high signal-to-noise ratio (SNR), for most cases of interest. The main finding of these works is that by exploiting the multicasting opportunity created by the overheard signals (side information) at receivers, an unbounded capacity gain can be achieved. Such idea of the opportunistic multicasting has been widely applied in various multiuser networks (see e.g. [2], [6], [8] and references therein).

In this work, we consider the state feedback in the K-user secured MISO broadcast channel so that the transmitter must convey each message to its intended receiver reliably while keeping it secret to all other receivers. As for the non-secured communication setups, a number of recent contributions have shown that a non-negligible gain can be achieved in the secured networks with state feedback [2], [3], [7], [8]. While in [8] the optimal secrecy DoF (SDoF) of the multi-antenna broadcast channel has been characterized for the case of two users, the work [2] has characterized the secrecy capacity of the $K > 2$-user the secured erasure broadcast channel with state feedback under some symmetry conditions. The latter result has been also extended to other secured networks [3].

The main contribution of our work is the characterization of the SDoF region in the K-user MISO broadcast channel with state feedback. The achievability builds on a secret key based linear scheme consisting of three phases, as a secured counterpart of the scheme in [1]. In phase 0, each user acquires an analog secret key when the transmitter sends some artificial noise. Such keys, available at the transmitter thanks to the state feedback, can be used to secure the data to be sent in the subsequent phases 1 and 2. The transmission of the secured data is performed with space-time interference alignment [1]. To prove the optimality, we propose a systematic way to derive an outer bound, which can be applied to a large class of channels. For instance, it can be used straightforwardly to the erasure broadcast channel studied in [2]. The proof in [2], which relies on the properties of discrete entropies, is unfortunately not suitable for our channel model. Finally, we observe that, with a large number K of users, the secrecy sum capacity of the erasure BC vanishes with K as $O(1/\log K)$, whereas the secrecy sum DoF of the MISO BC scales as $\Theta(K/\log K)$ when the number of transmit antennas grows accordingly with $M \geq K$. In other words, in a large network, it is too costly to provide secrecy in the erasure BC, while the secrecy comes almost "for free" in a multi-antenna BC.

Throughout the paper, we use the following notational conventions. Boldface lower-case letters $\boldsymbol{v}$ and upper-case letters $\boldsymbol{M}$ are used to denote vectors and matrices, respectively. We use the superscript notation X^n to denote a sequence $(X_1, \ldots, X_n)$ of variables. $X_{\mathcal{J}}$ is used to denote the set of variables $\{X_i\}_{i\in\mathcal{J}}$. Matrix transpose and Hermitian transpose are denoted by $\boldsymbol{A}^{\mathsf{T}}$ and $\boldsymbol{A}^{\mathsf{H}}$, respectively. Logarithm is in base 2. The entropy and differential entropy of X are denoted by $H(X)$ and $h(X)$, respectively. $o(\cdot)$, $O(\cdot)$, $\Theta(\cdot)$ are standard Landau notations. ϵ_n is a shorthand for $o(1)$ when $n \to \infty$.

Due to the space limitation, proofs for the lemmas are omitted and will be deferred to the full version of the paper.

II. Channel Model and Main Result

We consider the discrete-time K-user MISO broadcast channel with M transmit antennas. Then, the corresponding channel outputs at time instant t is given by

$$y_{k,t} = \boldsymbol{h}_{k,t}^{\mathsf{H}} \boldsymbol{x}_t + z_{k,t}, \quad k = 1, \ldots, K$$

where $\boldsymbol{h}_{k,t}^{\mathsf{H}} \in \mathbb{C}^{1\times M}$ is the channel coefficient vector for the k th user; $z_{1,t}, \ldots, z_{K,t}$ are the additive white Gaussian noises (AWGN) $\sim \mathcal{N}_{\mathbb{C}}(0,1)$ and are assumed to be independent to each other; the input vector $\boldsymbol{x}_t \in \mathbb{C}^{M\times 1}$ is subject to the average power constraint $\frac{1}{n}\sum_{t=1}^{n} \mathrm{tr}(\boldsymbol{x}_t \boldsymbol{x}_t^{\mathsf{H}}) \leq \mathsf{snr}$. Note that since we normalize the noise variances, snr is identified with the SNR at the transmitter side. We assume fast fading channel such that $\{\boldsymbol{h}_{k,t}\}_t$ are independent and identically distributed (i.i.d.) across time. The matrix $\boldsymbol{S}_t = [\boldsymbol{h}_{1,t} \ \cdots \ \boldsymbol{h}_{K,t}]^{\mathsf{H}} \in \mathcal{S}$ is called the state matrix at instant t. At the end of instant t, each receiver k feeds back the channel vector $\boldsymbol{h}_{k,t}^{\mathsf{H}}$ to the transmitter through a noiseless channel. Thus, $\boldsymbol{S}_1, \ldots, \boldsymbol{S}_{t-1}$ are available to the transmitter at instant t whereas the state matrices are known to all users at the end of the transmission. We make a further assumption on the state matrix.

Assumption 1 (channel symmetry): At any instant t, the rows of the state matrix $\boldsymbol{S}_t$ are independent and identically distributed. Furthermore, we limit ourselves to the class of fading processes in which the state matrix $\boldsymbol{S}_t$ has full rank and bounded entries almost surely at any time instant t.

Under these assumptions, we define the code and the optimal SDoF region summarized below.

Definition 1 (code and SDoF region): The encoder and the set of decoders are formally defined as follows:

- A sequence of stochastic encoders given by $\left\{F_t : \mathcal{W}_1 \times \cdots \times \mathcal{W}_K \times \mathcal{S}^{t-1} \longmapsto \mathbb{C}^{M\times 1}\right\}_{t=1}^{n}$ where the messages $W_1, \ldots, W_K$ are uniformly distributed over $\mathcal{W}_1, \ldots, \mathcal{W}_K$, respectively.
- The decoder of user k, $k = 1, \ldots, K$, is given by the mapping $\hat{W}_k : \mathbb{C}^{1\times n} \times \mathcal{S}^n \longmapsto \mathcal{W}_k$.

A SDoF tuple $(d_1, \ldots, d_K)$ is said to be *achievable* if there exists a code that satisfies simultaneously the following

- reliability condition: $\limsup_{n\to\infty} \Pr\left\{W_k \neq \hat{W}_k\right\} = 0, \forall\, k$;
- secrecy condition:

$$\limsup_{n\to\infty} \frac{1}{n} I(W_k; \{Y_l^n\}_{l\neq k}, S^n) = 0, \quad \forall\, k; \qquad (1)$$

- rate condition: $\lim_{\mathsf{snr}\to\infty} \liminf_{n\to\infty} \frac{\log|\mathcal{W}_k(n,\mathsf{snr})|}{n\log \mathsf{snr}} \geq d_k, \quad \forall\, k.$

The union of all achievable tuples $(d_1, \ldots, d_K)$ is called the optimal SDoF region.

Note that the perfect secrecy condition above imposes each message be secret to *all* $K-1$ other users even if they collude. The main result of this work is stated in the following theorem.

Theorem 1 (SDoF of K-user BC): The optimal SDoF region of the K-user MISO BC with M transmit antennas ($M \geq K$) is the set of tuples $(d_1, \ldots, d_K)$ satisfying

$$\frac{K-1}{K} d_{\pi_1} + \sum_{k=1}^{K} \frac{1}{k} d_{\pi_k} \leq 1, \qquad (2)$$

for any permutation π of $\{1, \ldots, K\}$. In particular, the sum SDoF is

$$\sum_{k=1}^{K} d_k \leq \frac{K}{\frac{K-1}{K} + \sum_{k=1}^{K} \frac{1}{k}}. \qquad (3)$$

The proof of this result is deferred to the upcoming sections. Some comments are in place on the above result. First, we remark that the above result covers some existing results as special cases including the SDoF region of the two-user MISO broadcast channel [8] as well as the DoF region of the K-user MISO broadcast channel [1]. In fact, compared to the non-secured broadcast setup, the secured scheme requires an additional phase of artificial noise transmission, in order to generate analog "secret keys". The resource overhead for the secret key generation is represented by the first term $\frac{(K-1)}{K} d_{\pi_1}$ in (2), where $\frac{K-1}{K}$ corresponds to the normalized length of the secret key generation phase (phase 0) with respect to the broadcast phase (phase 1). Without this term, the region boils down into that of the K-user non-secured broadcast channel. Finally, there is an explicit connection between our result and the secrecy capacity of the erasure BC, which will be discussed in section V.

III. Achievability

Lemma 1: The SDoF region (2) is a polyhedron, all the vertices of which are in the following form

$$d_k = \begin{cases} \frac{1}{\frac{K-1}{K} + \sum_{j=1}^{|\mathcal{K}|} \frac{1}{j}}, & k \in \mathcal{K} \\ 0, & k \notin \mathcal{K} \end{cases}$$

for some $\mathcal{K} \subseteq \{1, \ldots, K\}$.

It is thus enough to show that each corner point is achievable. After briefly reviewing the space-time interference alignment scheme, we present our secret key based linear scheme and show that all corner points are achievable. Since we are only interested in DoF of the channel, we remove the AWGN for simplicity of presentation unless otherwise indicated.

A. Space-time interference alignment revisited

Essentially, the scheme proposed in [1] consists of two phases: 1) broadcast of new information symbols, and 2) multicast of side information (overheard symbols). In the first phase, fresh information symbols are sent to all the users successively. At the end of the first phase, each user feeds back the channel state to the transmitter. The transmitter then reconstructs the overheard signals of each user (up to the background noise level) and generates side information as a function of such signals. In the second phase, the side information is multicast to the users. Mathematically, we recall the following high level description of the scheme.

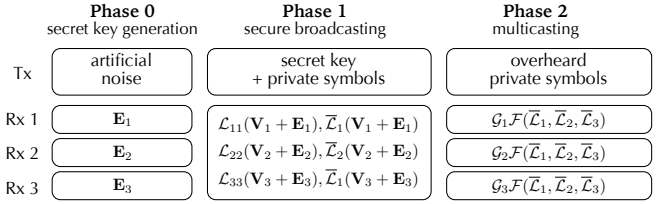

Fig. 1. The three-phase secure broadcasting scheme for three receivers

- In the first phase of $T_1 = t_1 K$ channel uses, the transmitter generates K sets of information symbols represented by K independent matrices $\boldsymbol{V}_1, \ldots, \boldsymbol{V}_K$, with $\boldsymbol{V}_k \in \mathbb{C}^{M \times t_1}$ containing information for user k. The matrices are transmitted successively. Due to the broadcast nature of the wireless medium, each user receives some linear functions of these matrices. Without loss of generality, we let $\mathcal{L}_{jk}(\boldsymbol{V}_k)$ denote the vector of all symbols received by user j when $\boldsymbol{V}_k$ is transmitted. Further we let $\bar{\mathcal{L}}_k(\boldsymbol{V}_k) \triangleq \{\mathcal{L}_{jk}(\boldsymbol{V}_k)\}_{j \neq k}$ denote the vector of *overheard* symbols on $\boldsymbol{V}_k$ by other $K-1$ users.
- In the second phase of T_2 channel uses, the transmitter, thanks to the state feedback, reconstructs the overheard symbols $\bar{\mathcal{L}}_1(\boldsymbol{V}_1), \ldots, \bar{\mathcal{L}}_K(\boldsymbol{V}_K)$. Then, the side information symbols are generated as a linear function of the overheard symbols, i.e., $\mathcal{F}(\bar{\mathcal{L}}_1(\boldsymbol{V}_1), \ldots, \bar{\mathcal{L}}_K(\boldsymbol{V}_K))$. The latter is sent through the MISO channel and each user k receives a linear function of the side information symbols, denoted by $\mathcal{G}_k\mathcal{F}(\bar{\mathcal{L}}_1(\boldsymbol{V}_1), \ldots, \bar{\mathcal{L}}_K(\boldsymbol{V}_K))$.

The achievability result in [1] implies the following lemma.

Lemma 2: There exist T_1 and T_2 with $(T_1+T_2)/T_1 = \sum_{k=1}^{K} \frac{1}{k}$ and a linear function $\mathcal{F}$, such that T_1 independent linear functions of $\boldsymbol{V}_k$ can be obtained from $\{\mathcal{L}_{kj}(\boldsymbol{V}_j)\}_{j=1}^{K}$ and $\mathcal{G}_k\mathcal{F}(\bar{\mathcal{L}}_1(\boldsymbol{V}_1), \ldots, \bar{\mathcal{L}}_K(\boldsymbol{V}_K))$, almost surely.

It is easy to verify that each user achieves $\frac{T_1}{T_1+T_2} = \frac{1}{\sum_{k=1}^{K} \frac{1}{k}}$ DoF per channel use.

B. Proposed secret key based linear scheme

In order to secure the K-user MISO broadcast channel, we propose a secret key based linear scheme as a secure counterpart of the above space-time interference alignment. Namely, the proposed scheme consists of secret key generation (phase 0) followed by secure broadcasting (phase 1), and side information multicasting (phase 2). The construction of our proposed scheme is illustrated in Fig. 1 for the case of three users.

1) Achieving the symmetric SDoF: In the secret key generation phase of $T_0 = t_1(K-1)$ channel uses, the transmitter sends T_0 i.i.d. vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{T_0} \sim \mathcal{CN}(0, \frac{\mathsf{snr}}{M}\mathbf{I}_M)$. Each user k receives $\boldsymbol{h}_{k,1}^{\mathsf{H}}\boldsymbol{u}_1, \ldots, \boldsymbol{h}_{k,T_0}^{\mathsf{H}}\boldsymbol{u}_{T_0}$ and put them into a matrix $\boldsymbol{E}_k \in \mathbb{C}^{(K-1)\times t_1}$. The state information $\{\boldsymbol{h}_{k,t}\}_t$ is known at the transmitter at the end of phase 0, thanks to state feedback, so that the matrix $\boldsymbol{E}_k$ can be reconstructed by the transmitter (up to the background noise level). Then, $\boldsymbol{E}_k$ is used as analog secret keys to "hide" the useful information $\boldsymbol{V}_k$. Specifically, in phase 1, the transmitter sends the useful symbol vector superimposed by the analog secret keys, i.e., $\tilde{\boldsymbol{V}}_k = \boldsymbol{V}_k + \boldsymbol{A}\boldsymbol{E}_k$ where $\boldsymbol{A} \in \mathbb{C}^{M \times (K-1)}$ is a constant full rank matrix (e.g., $\boldsymbol{A} = [\mathbf{I}_{K-1}\ 0_{(K-1)\times(M-K+1)}]^{\mathsf{T}}$) that scales the dimension of $\boldsymbol{E}_k$ up to the dimension of $\boldsymbol{V}_k$. The matrices $\{\tilde{\boldsymbol{V}}_k\}$ are sent exactly in the same way as $\{\boldsymbol{V}_k\}$ in the previous subsection. Phase 2 remains unchanged.

According to Lemma 2, T_1 independent equations of $\tilde{\boldsymbol{V}}_k$ can be recovered almost surely from the received signal of user k. Since $\boldsymbol{A}$ and $\boldsymbol{E}_k$ are known to user k, T_1 independent equations of $\boldsymbol{V}_k$ can be found reliably by user k. The corresponding DoF is $\frac{T_1}{T_0+T_1+T_2} = \frac{1}{\frac{K-1}{K}+\sum_{k=1}^{K}\frac{1}{k}}$. It remains to show that the per-user DoF is secured. Due to the symmetry, by focusing on user 1 without loss of generality, we aim to show that $\boldsymbol{V}_1$ cannot be inferred from the received signals of *all* other $K-1$ users. To this end, we analyze the mutual information between the useful signal $\boldsymbol{V}_1$ and the received signals of other users.

$$
\begin{aligned}
& I(\boldsymbol{V}_1; Y_2^n, \ldots, Y_K^n, S^n) \\
&= I(\boldsymbol{V}_1; Y_2^n, \ldots, Y_K^n \,|\, S^n) \\
&\le I(\boldsymbol{V}_1; \boldsymbol{E}_2, \ldots, \boldsymbol{E}_K, \{\mathcal{L}_{kk}(\tilde{\boldsymbol{V}}_k)\}_{k=2}^{K}, \{\bar{\mathcal{L}}_k(\tilde{\boldsymbol{V}}_k)\}_{k=1}^{K}, \\
&\qquad \{\mathcal{G}_k\mathcal{F}(\bar{\mathcal{L}}_1(\tilde{\boldsymbol{V}}_1), \ldots, \bar{\mathcal{L}}_K(\tilde{\boldsymbol{V}}_K))\}_{k=1}^{K} \,|\, S^n) \qquad (4) \\
&= I(\boldsymbol{V}_1; \boldsymbol{E}_2, \ldots, \boldsymbol{E}_K, \{\mathcal{L}_{kk}(\tilde{\boldsymbol{V}}_k)\}_{k=2}^{K}, \{\bar{\mathcal{L}}_k(\tilde{\boldsymbol{V}}_k)\}_{k=1}^{K}, \,|\, S^n) \\
&= I(\boldsymbol{V}_1; \boldsymbol{E}_2, \ldots, \boldsymbol{E}_K, \bar{\mathcal{L}}_1(\tilde{\boldsymbol{V}}_1) \,|\, S^n) \qquad (5) \\
&= I(\boldsymbol{V}_1; \bar{\mathcal{L}}_1(\boldsymbol{V}_1) + \bar{\mathcal{L}}_1(\boldsymbol{A}\boldsymbol{E}_1) \,|\, \boldsymbol{E}_2, \ldots, \boldsymbol{E}_K, S^n) \qquad (6) \\
&= T_1 o(\log \mathsf{snr})
\end{aligned}
$$

where the first equality is from the independence between $\boldsymbol{V}_1$ and the channel state; (4) follows because providing additional observations of user 1 on $\boldsymbol{V}_2, \ldots, \boldsymbol{V}_K$ does not reduce the mutual information; (5) is from the Markov chain $\boldsymbol{V}_1 \leftrightarrow (\boldsymbol{E}_2, \ldots, \boldsymbol{E}_K, \bar{\mathcal{L}}_1(\tilde{\boldsymbol{V}}_1)) \leftrightarrow \{\mathcal{L}_{kk}(\tilde{\boldsymbol{V}}_k), \bar{\mathcal{L}}_k(\tilde{\boldsymbol{V}}_k)\}_{k\neq 1}$; (6) is from the linearity of $\bar{\mathcal{L}}_1$; finally, the last equality is from the fact that $h(\bar{\mathcal{L}}_1(\boldsymbol{A}\boldsymbol{E}_1) \,|\, \boldsymbol{E}_2, \ldots, \boldsymbol{E}_K, S^n) = \mathrm{rank}(\bar{\mathcal{L}}_1)\Theta(\log \mathsf{snr})$ by construction[1].

2) Achieving other corner points in the SDoF region: Now let us assume that the transmitter sends messages to only K' out of K users, say, user 1 to user K'. However, each message should be kept secret to all $K-1$ other users. We need a slightly more general version of Lemma 2 in this case.

Lemma 3: There exist T_1 and T_2 with $(T_1+T_2)/T_1 = \frac{K}{K'}\sum_{k=1}^{K'}\frac{1}{k}$ as well as a linear function $\mathcal{F}$, such that $t_1 K$ independent linear functions of $\boldsymbol{V}_k$ can be obtained from $\{\mathcal{L}_{kj}(\boldsymbol{V}_j)\}_{j=1}^{K}$ and $\mathcal{G}_k\mathcal{F}(\bar{\mathcal{L}}_1(\boldsymbol{V}_1), \ldots, \bar{\mathcal{L}}_{K'}(\boldsymbol{V}_{K'}))$, almost surely, for $k = 1, \ldots, K'$.

Specifically, three phases are as follows:

- key generation phase (phase 0) is the same with $T_0 = t_1(K-1)$ channel uses;
- secured broadcasting phase (phase 1) lasts $T_1 = t_1 K'$ channel uses;
- multicasting phase (phase 2) lasts $T_2 = T_1\frac{K}{K'}\sum_{k=1}^{K'}\frac{1}{k} - T_1$ channel uses, so that, according to Lemma 3, $\frac{K}{K'}T_1$

[1]Proof is omitted and will be added in the full version.

independent linear equations of $\boldsymbol{V}_k$ can be recovered by user k, $k = 1, \ldots, K'$.

This scheme achieves the symmetric DoF among the K' active users $\frac{K}{K'}\frac{T_1}{T_0+T_1+T_2} = \frac{1}{\frac{K-1}{K}+\sum_{k=1}^{K'}\frac{1}{k}}$. For brevity, we omit the verification of secrecy constraints, which follows closely to the proof of the symmetric DoF.

We conclude this section by providing an example of $M = K = 3$. In this case, the region is characterized by three types of corner points. The symmetric DoF $\left(\frac{2}{5}, \frac{2}{5}, \frac{2}{5}\right)$ is achieved by sending 6 symbols to each user over the whole duration of $T_0 + T_1 + T_2 = 4 + 6 + 5 = 15$ channel uses. This yields the sum SDoF of $\frac{6}{5}$, smaller than the DoF $\frac{6}{11}$ without secrecy constraints. The corner point $\left(\frac{6}{13}, \frac{6}{13}, 0\right)$ is achieved by sending 6 information symbols to users 1 and 2 over the duration of $T_0+T_1+T_2 = 4+4+5 = 13$ channel uses. Finally, the $\left(\frac{3}{5}, 0, 0\right)$ is achieved by sending 6 symbol to user 1 over $T_0 + T_1 + T_2 = 4 + 2 + 4 = 10$ channel uses. The last corner point coincides with the achievable DoF of the MIMO wiretap channel with three-antenna transmitter, a single-antenna legitimate receiver, and a two-antenna eavesdropper [8].

IV. Converse

From the following proposition, the converse part of Theorem 1 is straightforward.

Proposition 1 (K-user capacity outer bound): Any achievable secrecy rate $(R_1, \ldots, R_K)$ for the K-user MISO broadcast channel must satisfy

$$\frac{K-1}{K}\max_k R_k + \sum_{k=1}^{K}\frac{1}{k}R_{\pi_k} \le C_{\text{SU-MISO}},$$

for any permutation π of $\{1, \ldots, K\}$; $C_{\text{SU-MISO}} \triangleq \max_{p_X} I(X; Y_k \,|\, S)$ is the single-user MISO channel capacity.[2]

The rest of the section is dedicated to the proof of the proposition. Due to the symmetry, we only need to prove the case without permutation. The proof relies on the channel output symmetry through the following lemma.

Lemma 4: Let U be such that $h(Y_{\mathcal{I},i} \,|\, Y_{\mathcal{J}}^{i-1}, S^i, U) = h(Y_{\mathcal{J}',i} \,|\, Y_{\mathcal{J}}^{i-1}, S^i, U), \forall\, i, \forall\, \mathcal{I}, \mathcal{J}' \subseteq \{1, \ldots, K\}$ with $|\mathcal{I}| = |\mathcal{J}'|$. Then,

$$\frac{1}{|\mathcal{I}|}h(Y_{\mathcal{I}}^n \,|\, U, S^n) \le \frac{1}{|\mathcal{J}|}h(Y_{\mathcal{J}}^n \,|\, U, S^n), \tag{7}$$

for any sets $\mathcal{I}, \mathcal{J}$ such that $\mathcal{J} \subseteq \mathcal{I} \subseteq \{1, \ldots, K\}$.

Three main steps are needed. First, we apply the genie-aided bounds, independent of the secrecy constraints. Then, we apply the secrecy constraints. Finally, we combine both bounds.

A. Genie-aided bounds

Let us define $\mathcal{I}_k \triangleq \{1, \ldots, k\}$, $k = 1, \ldots, K$. First, without the secrecy constraint, we have, by providing $(W^k, Y_{\mathcal{I}_k}^n)$ to user $k+1$, $k = 1, \ldots, K-1$, and using Fano's inequality,

$$\begin{aligned} n(R_1 - \epsilon_n) &\le I(W_1; Y_1^n \,|\, S^n) \\ &= h(Y_1^n) - h(Y_1^n \,|\, W_1 S^n) \\ &\vdots \\ n(R_K - \epsilon_n) &\le I(W_K; Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) \\ &= h(Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) - h(Y_{\mathcal{I}_K}^n \,|\, W^K S^n) \end{aligned}$$

Summing up the above inequalities with different weights, and applying Lemma 4 for $K-1$ times, namely,

$$\frac{1}{k+1}h(Y_{\mathcal{I}_{k+1}}^n \,|\, W^k S^n) \le \frac{1}{k}h(Y_{\mathcal{I}_k}^n \,|\, W^k S^n),$$

$k = 1, \ldots, K-1$, we obtain

$$\sum_{k=1}^{K}\frac{n}{k}(R_k - \epsilon_n) \le h(Y_1^n \,|\, S^n) - \frac{1}{K}h(Y_{\mathcal{I}_K}^n \,|\, W^K S^n). \tag{8}$$

B. Applying the secrecy constraint

Then, providing $(W^{K-1}, Y_{\mathcal{I}_{K-1}}^n)$ to user K, and applying the secrecy constraint (1), we have

$$\begin{aligned} &n(R_K - \epsilon_n) \\ &\le I(W_K; Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) - I(W_K; Y_{\mathcal{I}_{K-1}}^n \,|\, W^{K-1} S^n) \\ &= h(Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) - h(Y_{\mathcal{I}_{K-1}}^n \,|\, W^{K-1} S^n) \\ &\quad + h(Y_{\mathcal{I}_{K-1}}^n \,|\, W^K S^n) - h(Y_{\mathcal{I}_K}^n \,|\, W^K S^n) \\ &= h(Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) - h(Y_{\mathcal{I}_{K-1}}^n \,|\, W^{K-1} S^n) \\ &\quad - h(Y_K^n \,|\, Y_{\mathcal{I}_{K-1}}^n W^K S^n) \\ &\le h(Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) - h(Y_{\mathcal{I}_{K-1}}^n \,|\, W^{K-1} S^n) \\ &\quad - h(Z_K^n \,|\, S^n) \qquad (9) \\ &\le h(Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) - \frac{K-1}{K}h(Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) \\ &\quad - h(Z^n) \qquad (10) \\ &= \frac{1}{K}h(Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) - h(Z^n) \\ &= \frac{1}{K}h(Y_{\mathcal{I}_K}^n \,|\, W^K S^n) + \frac{1}{K}I(W_K; Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n) \\ &\quad - h(Z^n) \\ &\le \frac{1}{K}h(Y_{\mathcal{I}_K}^n \,|\, W^K S^n) + \frac{n}{K}R_K - h(Z^n) \qquad (11) \end{aligned}$$

where (9) is the application of $h(Y_K^n \,|\, Y_{\mathcal{I}_{K-1}}^n W^K S^n) \ge h(Y_K^n \,|\, X^n, Y_{\mathcal{I}_{K-1}}^n W^K S^n) = h(Z_K^n)$; (10) is from Lemma 4; the last inequality is from $nR_K = H(W_K) \ge I(W_K; Y_{\mathcal{I}_K}^n \,|\, W^{K-1} S^n)$. From (11) ,

$$n(R_K - \epsilon_n) \le \frac{1}{K-1}h(Y_{\mathcal{I}_K}^n \,|\, W^K S^n) - \frac{K}{K-1}h(Z^n).$$

Due to the symmetry, we have, for any k,

$$n(R_k - \epsilon_n) \le \frac{1}{K-1}h(Y_{\mathcal{I}_K}^n \,|\, W^K S^n) - \frac{K}{K-1}h(Z^n),$$

which implies

$$n\big(\max_k R_k - \epsilon_n\big) \le \frac{1}{K-1}h(Y_{\mathcal{I}_K}^n \,|\, W^K S^n) - \frac{K}{K-1}h(Z^n). \tag{12}$$

[2]It is independent of k due to the channel output symmetry assumption.

C. Combining both bounds

Summing up the above bounds (8) and (12) with weights,

$$\begin{aligned}\sum_{k=1}^{K}\frac{1}{k}R_k+\frac{K-1}{K}\max_k R_k&\le\frac{1}{n}\left(h(Y_1^n\,|\,S^n)-h(Z^n)\right)+\epsilon_n\\&\le\frac{1}{n}\sum_{i=1}^{n}(h(Y_{1i}\,|\,S_i)-h(Z_i))+\epsilon_n\\&\le\max_{p_{X_i}}I(X_i;Y_{1i}\,|\,S_i)+\epsilon_n\\&=C_{\text{SU-MISO}}+\epsilon_n\end{aligned}$$

which completes the proof by letting $n\to\infty$.

V. Connection to the erasure broadcast channel

The multi-antenna BC is closely related to the erasure BC. The former is a state-dependent Gaussian noise channel whereas the latter is a state-dependent deterministic channel. While optimal DoF regions are characterized for the multi-antenna BC (e.g., [1], [8] and the current work), exact capacity regions can be obtained, with [2] or without (e.g., [4], [5]) secrecy constraints. To highlight the connection, let us consider the erasure BC with the i.i.d. erasure (with probability δ) across users. The capacity region obtained in [2] can be rewritten as

$$\frac{\alpha_{K-1}}{\alpha_K(\alpha_K-\alpha_{K-1})}R_{\pi_1}+\sum_{k=1}^{K}\frac{1}{\alpha_k}R_{\pi_k}\le 1,\qquad(13)$$
$$\alpha_k\triangleq 1-\delta^k$$

which is in exactly the same form as the SDoF region in (2), if we let $\alpha_k=k$ instead of $1-\delta^k$ and replace the DoF by rate. The achievability schemes for both cases are based on similar ideas of key generation except that analog keys from artificial noise are used in our setting (as well as [8]).

The achievability schemes for both cases have a similar structure consisting of three phases. In the erasure channel, the *digital* secret keys, generated by sending random packets, are used to encrypt messages, whereas our analog secret keys is created by the artificial noise. Quite remarkably, it turns out that the converse of the capacity region (13) can be proved, in an alternative way, using the same techniques we propose in this paper, namely, the three steps described in the previous section. As a matter of fact, we can obtain the following equivalent of Lemma 4 for the erasure channel, before applying the three-step procedure.

Lemma 5: For the erasure broadcast channel with independent erasure events (with probability $\{\delta_k\}$) for different users, if U is such that $X_i\leftrightarrow UY_{\mathcal{J}}^{i-1}S^{i-1}\leftrightarrow(S_{i+1},\ldots,S_n)$, $\forall\,\mathcal{J}$,

$$\frac{1}{\beta_{\mathcal{J}}}H(Y_{\mathcal{J}}^n\,|\,U,S^n)\le\frac{1}{\beta_{\mathcal{J}}}H(Y_{\mathcal{J}}^n\,|\,U,S^n),$$
$$\text{with }\beta_{\mathcal{J}}\triangleq 1-\prod_{i\in\mathcal{J}}\delta_i,\qquad(14)$$

for any sets $\mathcal{I},\mathcal{J}$ such that $\mathcal{J}\subseteq\mathcal{I}\subseteq\{1,\ldots,K\}$.

With a large number K of users, the sum SDoF of the MISO BC is $O(K/\log K)$ provided that $M\ge K$. Therefore, the scaling is the same with or without secrecy. From (3), it is clear that, to send K symbols securely, one only needs $\frac{K-1}{K}$ channel uses to generate secret keys in addition to the $\sum_{k=1}^{K}\frac{1}{k}$ channel uses for data transmission. The extra cost is negligible (goes to 1) when K is large. This is due to the high diversity order of the channel that scales with K when $M\ge K$. As a matter of fact, in average K secret key symbols are generated per channel use. On the other hand, from (13), the sum secrecy capacity of the symmetric erasure BC is

$$R_{\text{sum}}^{\text{E-BC}}=\frac{K}{\frac{1-\delta^{K-1}}{(1-\delta^K)(1-\delta)\delta^{K-1}}+\sum_{k=1}^{K}\frac{1}{1-\delta^k}}.\qquad(15)$$

In this case, secrecy costs in average $\tau_K\triangleq\frac{1-\delta^{K-1}}{(1-\delta^K)(1-\delta)\delta^{K-1}}$ channel uses for every K symbols sent. Obviously, if δ is bounded away from 1, then $\tau_K=\Theta(\delta^{-(K-1)})$, i.e., grows exponentially with K. And the sum capacity vanishes exponentially with K as $R_{\text{sum}}^{\text{E-BC}}=\Theta(K\delta^{K-1})$. In fact, even when δ can be optimized for each K, the sum secrecy capacity of symmetric erasure BC is vanishing with K.

Proposition 2: For any erasure probability δ, the sum secrecy capacity of the symmetric erasure BC satisfies $R_{\text{sum}}^{\text{E-BC}}\le\Theta(1/\log K)$ when $K\to\infty$, with equality when $\delta=1-\Theta(K^{-1})$.

Therefore, in a sharp contrast with the MISO BC, it is too costly to provide secrecy in the erasure BC when the number of users is large. Intuitively, the low "diversity" of the erasure BC is the cause to blame, i.e., secret key generation is highly inefficient is this regime.

References

[1] M. A. Maddah-Ali and D. N. C. Tse, "Completely Stale Transmitter Channel State Information is Still Very Useful," *IEEE Trans. Inf. Theory* vol. 58, no. 7, pp. 4418–4431, July 2012.

[2] L. Czap, V. Prabhakaran, C. Fragouli, and S. Diggavi, "Secret Communication over Broadcast Erasure Channels with State-feedback", arXiv preprint arXiv:1408.1800, 2014

[3] L. Czap, V. Prabhakaran, C. Fragouli, and S. Diggavi, "Triangle Network Secrecy", in *Proceedings of the IEEE International Symposium on Information Theory (ISIT'14)*, Hawaii, USA, 2014

[4] C. C. Wang, "On the Capacity of 1-to-Broadcast Packet Erasure Channels with Channel Output feedback", *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 931–956, February 2012.

[5] M. Gatzianas, L. Georgiadis, and L. Tassiulas, "Multiuser Broadcast Erasure Channel With Feedback-Capacity and Algorithms", *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5779–5804, September 2013.

[6] H. Maleki, S. A. Jafar, and S. Shamai (Shitz), "Retrospective Interference Alignment over Interference Networks" , *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 3, pp. 228–240, June 2012.

[7] A. Zaidi, Z. H. Awan, S. Shamai (Shitz) and L. Vandendorpe, "Secure Degrees of Freedom of MIMO X-Channels with Output Feedback and Delayed CSIT", *IEEE Trans. on Information Forensics and Security*, vol. 8, no. 11, pp. 1760–1774, August 2013

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

APPENDIX

ELEMENTS OF PROOFS

Proof of Lemma 1: The SDoF region in (2) is the polyhedron characterized by $K!$ inequalities. We let $f(d_{\pi_1},\dots,d_{\pi_K})$ denote the left hand side of (2). Since this function is linear in $(d_{\pi_1},\dots,d_{\pi_K})$ with decreasing weights $1+\frac{K-1}{K} > \frac{1}{2} > \cdots > \frac{1}{K}$, the permutation maximizing $f(d_{\pi_1},\dots,d_{\pi_K})$ is such that $d_{\pi_i} > d_{\pi_j}$ whenever $i<j$. Since this is exactly the same structure as the MISO broadcast channel without secrecy constraints, we follow the similar footsteps as [1, section V] to prove that any point in the polyhedron such that $d_i>0$ for all i and $d_i \neq d_j$ for some $i\neq j$ cannot be a corner point. ∎

Proof of Lemma 2 and Lemma 3: Since Lemma 3 includes Lemma 2 as a special case, it is enough to prove the former. To prove the existence of such (T_1,T_2), we rely on the construction based on the scheme proposed in [1]. In the first phase, we sent $K'\leq K$ matrices $\boldsymbol{V}_1,\dots,\boldsymbol{V}_{K'}\in\mathbb{C}^{M\times t_1}$ suceesively. These matrices are intended to user $1,\dots,K'$, respectively. We let the T_1 be the duration of this phase, i.e., $T_1=t_1K'$ channel uses. The second phase of length T_2 can be divided into two sub-phases:

- first, $\frac{T_1(K-1)}{2}$ "order-2" symbols are formed based on $\{\mathcal{L}_{jk}(\boldsymbol{V}_k)\}_{j\neq k=1\dots K'}$, specifically as
$$\{\mathcal{L}_{jk}(\boldsymbol{V}_k)+\mathcal{L}_{kj}(\boldsymbol{V}_j)\}_{j\neq k=1\dots K'}.$$
These "order-2" symbols are coded linearly with the state feedback received during the transmission in phase 2A, using the "order-2" scheme in [1]. The length of this phase is
$$T_{2A}=\frac{\frac{T_1(K-1)}{2}}{\mathsf{DoF}_2(M,K')}$$
where $\mathsf{DoF}_2(M,K') \triangleq \frac{K-1}{2}\frac{1}{\sum_{k=2}^{K'}\frac{1}{k}}$. At the end of phase 2A, both users $k,j\in\{1\dots K'\}$ can recover $\mathcal{L}_{jk}(\boldsymbol{V}_k)+\mathcal{L}_{kj}(\boldsymbol{V}_j)$, and then both $\mathcal{L}_{jk}(\boldsymbol{V}_k)$ and $\mathcal{L}_{kj}(\boldsymbol{V}_j)$.
- second, $T_1(K-K')$ "order-1" symbols are directly generated as $\{\mathcal{L}_{jk}(\boldsymbol{V}_k)\}_{j=K'+1\dots K,k=1\dots K'}$. These "order-1" symbols are coded linearly with the state feedback received during the transmission in phase 2B, using the "order-1" scheme in [1]. The length of this phase is
$$T_{2B}=\frac{T_1(K-K')}{\mathsf{DoF}_1(M,K')}.$$
where $\mathsf{DoF}_1(M,K') \triangleq \frac{K'}{\sum_{k=1}^{K'}\frac{1}{k}}$. At the end of phase 2B, each users $k\in\{1\dots K'\}$ can recover $\{\mathcal{L}_{jk}(\boldsymbol{V}_k)\}_{j=K'+1\dots K}$.

At the end, each user k obtains $\mathcal{L}_{kk}(\boldsymbol{V}_k)$ from phase 1, $\{\mathcal{L}_{jk}(\boldsymbol{V}_k)\}_{j\neq k=1\dots K'}$ from phase 2A, and $\{\mathcal{L}_{jk}(\boldsymbol{V}_k)\}_{j=K'+1\dots K}$ from phase 2B, i.e., in total t_1K equations $\{\mathcal{L}_{jk}(\boldsymbol{V}_k)\}_{j,k=1\dots K}$ of $\boldsymbol{V}_k$. The length of phase 2 is $T_2=T_{2A}+T_{2B}=T_1\frac{K}{K'}\sum_{k=1}^{K'}\frac{1}{k}-T_1$. ∎

Proof of Lemma 4: This lemma has been proved in [8]. For completeness, we provide the following sketch. For $\mathcal{J}\subseteq\mathcal{I}$,

$$\begin{aligned}
&h(Y_{\mathcal{J}}^n\,|\,U,S^n)\\
&=\sum_{i=1}^n h(Y_{\mathcal{I},i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^n)\\
&=\sum_{i=1}^n h(Y_{\mathcal{I},i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1},S_i)\\
&=\sum_{i=1}^n \binom{K}{|\mathcal{I}|}^{-1}\sum_{\mathcal{I}':|\mathcal{I}'|=|\mathcal{I}|} h(Y_{\mathcal{I}',i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1},S_i)\\
&\leq\sum_{i=1}^n \frac{|\mathcal{I}|}{|\mathcal{J}|}\binom{K}{|\mathcal{J}|}^{-1}\sum_{\mathcal{J}':|\mathcal{J}'|=|\mathcal{J}|} h(Y_{\mathcal{J}',i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1},S_i)\\
&=\sum_{i=1}^n \frac{|\mathcal{I}|}{|\mathcal{J}|}h(Y_{\mathcal{J},i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1},S_i)\\
&\leq\sum_{i=1}^n \frac{|\mathcal{I}|}{|\mathcal{J}|}h(Y_{\mathcal{J},i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1},S_i) \qquad (16)
\end{aligned}$$

where the first equality is from the chain rule; the second one is due to the current input does not depend on future states conditional on the past outputs/states and U; the third one is from the assumption of entropy symmetry; the fourth step is from the monotonicity of average entropy; the fifth step again from the assumption of entropy symmetry; the final step is from removing the terms $Y_{\mathcal{I}\setminus\mathcal{J}}^{i-1}$ in the condition, which increases the entropy. Following the first three steps as above, we also have

$$h(Y_{\mathcal{J}}^n\,|\,U,S^n)=\sum_{i=1}^n\frac{|\mathcal{I}|}{|\mathcal{J}|}h(Y_{\mathcal{J},i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1},S_i)$$

from which and (16), we obtain (7). ∎

Proof of Lemma 5: Let us define S_i as the set of indices of the receivers *not* in erasure at time instant i, i.e., $S_i\triangleq\{k: Y_{k,i}=X_{k,i}\}$. Then, we have, for $\mathcal{J}\subseteq\mathcal{I}$,

$$\begin{aligned}
&H(Y_{\mathcal{J}}^n\,|\,U,S^n)\\
&=\sum_{i=1}^n H(Y_{\mathcal{I},i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^n)\\
&=\sum_{i=1}^n H(Y_{\mathcal{I},i}\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1},S_i)\\
&=\sum_{i=1}^n \Pr\{S_i\cap\mathcal{I}\neq\emptyset\}\,H(X_i\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1},S_i\cap\mathcal{I}\neq\emptyset)\\
&=\sum_{i=1}^n \big(1-\prod_{i\in\mathcal{J}}\delta_i\big)H(X_i\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1})\\
&\leq\big(1-\prod_{i\in\mathcal{J}}\delta_i\big)\sum_{i=1}^n H(X_i\,|\,Y_{\mathcal{J}}^{i-1},U,S^{i-1}) \qquad (17)
\end{aligned}$$

where the first equality is from the chain rule; the second equality is due to the current input does not depend on future states conditional on the past outputs/states and U; the third one holds since $Y_{\mathcal{I},i}$ is deterministic and has entropy 0 when

all outputs in $\mathcal{I}$ are erased ($S_i \cap \mathcal{I} = \emptyset$); the fourth equality is from the independence between X_i and S_i; and we get the last inequality by removing the terms $Y_{\mathcal{I}\setminus\mathcal{J}}^{i-1}$ in the condition of the entropy. Following the same steps, we have

$$H(Y_{\mathcal{J}}^n \,|\, U, S^n) = \big(1 - \prod_{i\in\mathcal{J}} \delta_i\big) \sum_{i=1}^{n} H(X_i \,|\, Y_{\mathcal{J}}^{i-1}, U, S^{i-1})$$

from which and (17), we obtain (14). ∎

Proof of Proposition 2: Since the sum secrecy capacity (15) vanishes exponentially with K for any erasure probability δ bounded from 1, we assume in the following that $\delta = 1-\varepsilon_K$ with $\varepsilon_K = \Theta(K^{-l})$ for some $l > 0$. That is, δ goes to 1 when K is large. Then, it follows that

$$\delta^K = \Theta(e^{-K^{-l+1}}) = \begin{cases} \Theta(K^{-\infty}), & l < 1 \\ \Theta(1), & l = 1 \\ 1 - \Theta(K^{-l+1}), & l > 1 \end{cases}$$

and similar for δ^{K-1}. Thus, we have

$$\begin{aligned} \tau_K &\triangleq \frac{1-\delta^{K-1}}{(1-\delta^K)(1-\delta)\delta^{K-1}} \\ &= \Theta\left(\frac{1}{(1-\delta)\delta^{K-1}}\right). \end{aligned}$$

We can exclude the case $l < 1$ since it would also lead to exponential decreasing of the sum secrecy capacity. Therefore, we have $l \geq 1$ instead and $\tau_K = \Theta(K^l)$.

Next, we consider duration of data transmission assuming $l \geq 1$. Then,

$$\begin{aligned} \mu_K &\triangleq \sum_{k=1}^{K} \frac{1}{1-\delta^k} \\ &= \int_1^{K+1} \frac{\mathrm{d}\,x}{1-\delta^x} + O\left(\frac{\delta - \delta^{K+1}}{(1-\delta)(1-\delta^{K+1})}\right) \\ &= \int_1^{K+1} \frac{\mathrm{d}\,x}{1-\delta^x} + O\left(K^l\right) \\ &= K + \frac{\log\frac{1-\delta}{1-\delta^{K+1}}}{\log\delta} + O\left(K^l\right) \\ &= K + \frac{\log\Theta\left(\frac{K^{-l}}{K^{-l+1}}\right)}{\log(1-\Theta(K^{-l}))} + O\left(K^l\right) \\ &= \Theta(K^l \log K) + O\left(K^l\right) = \Theta(K^l \log K). \end{aligned}$$

Obviously, $\tau_K + \mu_K = \Theta(K^l \log K)$ and the sum secrecy capacity is $\Theta(K^{-l+1}/\log(K))$ with $l \geq 1$ and is $\Theta(K^{-\infty})$ otherwise, which completes the proof.

∎