Blind Wiretap Channel with Delayed CSIT

Sina Lashgari and Amir Salman Avestimehr

Abstract—We consider the Gaussian wiretap channel where a transmitter wishes to communicate a secure message to a legitimate receiver in the presence of eavesdroppers, without the eavesdroppers being able to decode the secure message. We focus on a setting that the transmitter is blind with respect to the state of channels to eavesdroppers, and only has access to delayed channel state information (CSI) of the legitimate receiver, which is referred to as “blind wiretap channel with delayed CSIT”. We then consider two scenarios: (i) the case where the secure communication is aided via a distributed jammer, (ii) the case where all nodes in the network are equipped with multiple antennas, referred to as blind MIMO wiretap channel with delayed CSIT. We completely characterize the secure Degrees of Freedom (SDoF) in both scenarios, when assuming linear coding strategies at the transmitter(s).

I. INTRODUCTION

Wiretap channel is one of the canonical settings in the information-theoretic study of secrecy in wireless networks. It consists of a transmitter that wishes to communicate a secret message to a legitimate receiver in the presence of an eavesdropper that should not decode the secure message. There has been a large amount of work on this problem, and its secrecy capacity has been determined in several configurations (e.g., [2]–[5]). In particular, the secrecy capacity of the Gaussian wiretap channel is characterized in [5], and it is known that if the channel to the legitimate receiver is “less noisy” than the channel to the eavesdropper, then a positive rate of secret communication is achievable.

However, the secrecy capacity of the Gaussian wiretap channel does not scale with the available transmit power, i.e., the secure degrees of freedom (SDoF) of Gaussian wiretap channel is zero. This has motivated the utilization of helping jammers and multi-antenna transmitters in the network to increase the achievable SDoF (e.g., [6]–[15]). In particular, it has been shown in [9] that the SDoF of wiretap channel with a helping jammer (i.e. cooperative jamming) in a wireless setting in which the channels remain constant is \( \frac{1}{2} \). This work has also been extended in [16] to the case that transmitters have no knowledge of channels to the eavesdropper (i.e., blind cooperative jamming), and it has been shown that even if transmitters have no eavesdropper CSIT, the same SDoF can be achieved. However, these results rely on the assumption that channels are constant, and do not change over time.

The case of time-varying channels (i.e. ergodic channels) has also been considered in some prior works in the literature. In particular, in [16] Yang et. al. have considered the Gaussian MIMO wiretap channel with delayed CSIT; and they have characterized the SDoF of such network for arbitrary number of antennas. However, they assume that the transmitter has access to perfect delayed CSIT of the eavesdropper, which in many scenarios is not a realistic assumption. For the case where no eavesdropper CSIT is available, [16] only provides some inner bounds on the SDoF.

In this work, we focus on the ergodic wiretap channel in which channels are changing over time; and we consider arbitrary number of eavesdroppers in the network. We assume that the transmitter is blind with respect to the state of channels to the eavesdroppers, and only has access to delayed channel state information (CSI) of the legitimate receiver. In short, we refer to this scenario as “blind wiretap channel with delayed CSIT”. We focus on two different scenarios. First, we consider the scenario where the communication is aided via a distributed single-antenna cooperative jammer, which is referred to as “blind cooperative wiretap channel with delayed CSIT”. Second, we consider the case where all nodes in the network are equipped with multiple antennas, which is referred to as “blind MIMO wiretap channel with delayed CSIT”.

For the case of blind cooperative wiretap channel with delayed CSIT, we show that a strictly positive SDoF of \( \frac{1}{3} \) is achievable, no matter how many eavesdroppers exist in the network. Further, we show that \( \frac{1}{3} \) is indeed the secure DoF when linear coding strategies are employed. In our achievable scheme transmitters cooperatively transmit artificial noise to perform two tasks: first, the artificial noise signals are aligned at the legitimate receiver in order to provide some room for the secret message to be decoded. Second, the artificial noise signals span the entire received signal space at the eavesdroppers to completely drown the secure message at the eavesdroppers. The transmitters only have access to the delayed knowledge of channels to the legitimate receiver to perform the two tasks, and they are completely blind with respect to the eavesdroppers.

The converse proof for blind cooperative wiretap channel is based on two key lemmas. The first lemma, namely Rank Ratio Inequality, is a new bounding technique developed in [17], which states that if two distributed transmitters employ linear strategies, the ratio of the dimensions of received linear subspaces at any two receivers cannot exceed \( \frac{3}{2} \), due to delayed CSIT. The Rank Ratio Inequality in [17] led to the converse proof for X-channel with delayed CSIT, as well as a new outer bound for 3-user interference channel with delayed CSIT, under the realm of linear schemes. Rank Ratio Inequality (Lemma [1]) is also an essential component of the converse proof for the blind cooperative wiretap channel with delayed CSIT. The second lemma, called Least Alignment Lemma, is also a crucial ingredient of the converse. It states that once

S. Lashgari is with the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY (email: sll2232@cornell.edu); and A. S. Avestimehr is with the EE department of University of Southern California, Los Angeles, CA 90089 (email: avestimehr@ee.usc.edu). The research of A. S. Avestimehr and S. Lashgari is supported by NSF Grants CAREER 0953117, CCF-1161720, NETS-1161904, and ONR award N000141510084. This work will be presented in part at the IEEE International Symposium on Information Theory 2014 [1].

arXiv:1405.0521v1 [cs.IT] 2 May 2014
the transmitters in a network have no CSIT with respect to a certain receiver, the least amount of alignment will occur at that receiver, meaning that transmit signals will occupy the maximal signal dimensions at that receiver. This would in turn imply that the total received signal dimension at each eavesdropper is no less than that of the legitimate receiver.

Second, we use the insights obtained from studying the received signal and noise dimensions in different receivers to provide new achievable schemes for blind MIMO wiretap channel with delayed CSIT; and as a result, we improve the state-of-the-art achievable schemes presented in [19]. Further, we extend the developed converse techniques, and in particular the Least Alignment Lemma, to the blind MIMO wiretap channel with delayed CSIT, and completely characterize the secure DoF when restricted to linear schemes. As a special case, the converse result implies that the achievable scheme presented in [18] for blind MISO wiretap channel with delayed CSIT, which achieves \( \frac{1}{2} \), is indeed optimal when restricted to linear coding schemes.

**Other Related Works:** Artificial Noise Alignment was introduced in [8] to drown the secure message in the artificial noise at the undesired receivers. Khisti in [15] has studied interference alignment for the multi-antenna compound wiretap channel. On the other hand, Shamai et. al. have studied secrecy degrees of freedom of the multiantenna block fading wiretap channel [19]. In [9] Xie and Ulukus have studied the SDoF of four fundamental one-hop wireless networks: Gaussian wiretap channel, Gaussian broadcast channel with confidential messages, Gaussian interference channel with confidential messages, and Gaussian multiple access wiretap channel. They assume constant channel gains, and prove their achievability results based on Real Interference Alignment.

**II. SYSTEM MODEL & MAIN RESULTS**

We consider the Gaussian wiretap channel depicted in Fig. 1, which consists of a transmitter (Tx1), a jammer (Tx2), and \( k + 1 \) receivers, where Tx1 has a secret message for Rx1 (legitimate receiver), and Rx2, . . . , Rx_{k+1} are the eavesdroppers. The role of Tx2, although it does not have access to the secret message is to help Tx1 communicate its message securely to Rx1, while Rx2, . . . , Rx_{k+1} cannot decode any part of that message. Each node in the network is equipped with a single antenna.

The received signal at Rxj \(( j \in \{1, \ldots , k + 1\} )\) at time \( t \) is given by

\[
y_j(t) = g_{j1}(t)x_1(t) + g_{j2}(t)x_2(t) + z_j(t),
\]

where \( x_1(t) \) is the transmit signal of Tx1; \( g_{j1}(t) \in \mathbb{C} \) indicates the channel from Tx1 to Rxj; and \( z_j(t) \sim \mathcal{CN}(0, 1) \). The channel coefficients \( g_{j1}(t) \) are i.i.d across time and users, and they are drawn from a continuous distribution. We denote by \( \mathcal{G}(t) \) the set of all channel coefficients at time \( t \). In addition, we denote by \( \mathcal{G}^n \) the set of all channel coefficients from time 1 to \( n \), i.e.,

\[
\mathcal{G}^n \triangleq \{ g_{ji}(t) : j \in \{1, \ldots , k+1\}, i \in \{1, 2\}, t \in \{1, \ldots , n\} \}.
\]

\(^1\)This assumption is not necessary; and even if the jammer has access to the secret message, the analysis remains the same.

Denoting the vector of transmit signals for Tx1 in a block of length \( n \) by \( \bar{x}_1^n \), each transmitter Tx1 obeys an average power constraint, \( \frac{1}{T}E[|\bar{x}_1^n|^2] \leq P \). We assume delayed channel state information at the transmitters (CSIT) with respect to channels to the legitimate receiver; however, transmitters have no knowledge of eavesdroppers. In other words, at time \( t \), only the states of the past \( G_{0}^{t-1} \triangleq \{ g_{ti}(h) : i = 1, 2, h = 1, \ldots , t-1 \} \) are known to the transmitters.

We restrict ourselves to linear coding strategies as defined in [17], [20], [21]. In particular, consider a communication scheme with block length \( n \), in which Tx1 wishes to communicate a vector \( \bar{x} \in \mathbb{C}^{m_1(n)} \) of \( m_1(n) \in \mathbb{N} \) information symbols to Rx1. Each of the information symbols is a Gaussian random variable with variance \( P \). The information symbols are then modulated with precoding vectors \( \bar{v}_1(t) \in \mathbb{C}^{m_1(n)} \) at times \( t = 1, 2, \ldots , n \). Note that the precoding vector \( \bar{v}_1(t) \) depends only upon the outcome of \( G_{0}^{t-1} \) due to the delayed channel knowledge constraint:

\[
\bar{v}_1(t) = f_{\text{signal}, 1, t}(G_{0}^{t-1}).
\]

In addition, Tx1 is allowed to use a vector \( \bar{w}_1 \in \mathbb{C}^{m_2(n)} \) of \( m_2(n) \in \mathbb{N} \) noise symbols, which are not necessarily to the interest of any receiver, but can help drown \( \bar{x} \) in the received signal of Rx2, . . . , Rx_{k+1} such that they cannot decode the message. Each of the noise symbols is a Gaussian random variable with variance \( P \). The noise symbols are also modulated with precoding vectors \( \bar{u}_1(t) \in \mathbb{C}^{m_2(n)} \) at times \( t = 1, 2, \ldots , n \). Note that the precoding vector \( \bar{u}_1(t) \) depends only upon the outcome of \( G_{0}^{t-1} \) due to the delayed channel knowledge constraint:

\[
\bar{u}_1(t) = f_{\text{noise}, 1, t}(G_{0}^{t-1}).
\]

Similarly, the jammer (i.e. Tx2) is allowed to use a vector \( \bar{w}_2 \in \mathbb{C}^{m_3(n)} \) of \( m_3(n) \in \mathbb{N} \) noise symbols, independent of \( \bar{w}_1 \), which are modulated at time \( t \) with precoding vector \( \bar{u}_2(t) \in \mathbb{C}^{m_3(n)} \), where

\[
\bar{u}_2(t) = f_{\text{noise}, 2, t}(G_{0}^{t-1}).
\]

Based on this linear precoding, Tx1 will then send \( x_1(t) = \bar{v}_1(t)^\top \bar{x} + \bar{u}_1(t)^\top \bar{w}_1 \), and Tx2 will send \( x_2(t) = \bar{u}_2(t)^\top \bar{w}_2 \).
at time \( t \). We denote the precoding functions used by Tx
\( 1 \) by \( f_1^{(n)} = \{ f_{\text{signal},1}, f_{\text{noise},1} \} \), and the ones used by Tx
\( 2 \) by \( f_2^{(n)} = \{ f_{\text{signal},2}, f_{\text{noise},2} \} \). In addition, we denote by \( V_1^n \in \mathbb{C}^{m \times n \times n} \), \( U_1^n \in \mathbb{C}^{m \times m \times n} \), and \( U_2^n \in \mathbb{C}^{m \times m \times n} \) the overall precoding matrices such that the \( t \)-th row of \( V_1^n \) is \( \tilde{v}_1(t)^\top \), the \( t \)-th row of \( U_1^n \) is \( \tilde{u}_1(t)^\top \), and the \( t \)-th row of \( U_2^n \) is \( \tilde{u}_2(t)^\top \).

Based on the above setting, the received signal at Rx \( j \) (\( j \in \{1, \ldots, k+1\} \)) after the \( n \) time steps of the communication will be

\[
\begin{align*}
S_j^n &= G_j^n V_1^n \tilde{x}_1 + G_j^n U_1^n \tilde{w}_1 + G_j^n U_2^n \tilde{w}_2 + Z_j^n,
\end{align*}
\]

where \( G_j^n \) is the \( n \times n \) diagonal matrix whose \( t \)-th element on the diagonal is \( g_{ji}(t) \). Now, consider decoding \( \tilde{x} \) at Rx \( j \) for \( j = 1, \ldots, k+1 \). The interference subspace at Rx \( j \) will be

\[
\mathcal{I}_j = \text{colspan}\left( \begin{bmatrix} G_{ji}^n U_1^n & G_{ji}^n U_2^n \end{bmatrix} \right),
\]

where colspan(.) of a matrix is the subspace spanned by its columns, and \([A \ B]\) denotes the horizontal concatenation of two matrices \( A, B \). Let \( \mathcal{I}_j \subseteq \mathbb{C}^n \) denote the orthogonal subspace of \( \mathcal{I}_j \). Then, in the regime of asymptotically high transmit powers (i.e., ignoring the noise), the decodability of information symbols from Tx \( j \) at Rx \( j \) corresponds to the constraints that the image of colspan\( (G_{ji}^n V_1^n) \) on \( \mathcal{I}_j \) has dimension \( m_1(n) \):

\[
\dim \left( \text{Proj}_{\mathcal{I}_j} \text{colspan} \left( G_{ji1}^n V_1^n \right) \right) = \dim (\text{colspan} \left( V_1^n \right)) = m_1(n),
\]

where \( \text{Proj}_{\mathcal{I}_j} \text{colspan} \left( G_{ji1}^n V_1^n \right) \) is the orthogonal projection of column span of \( G_{ji1}^n V_1^n \) on \( \mathcal{I}_j \).

Based on this setting, we now define the linear secure degrees of freedom (LSDoF) of the blind cooperative wiretap channel with delayed CSIT.

**Definition 1.** A secure degree of freedom is linearly achievable if there exists a sequence \( \left\{ f_1^{(n)}, f_2^{(n)} \right\}_{n=1}^\infty \) such that for each \( n \), \( V_1^n \) satisfies the decodability condition of (7) with probability \( 1 \), and

\[
d = \lim_{n \to \infty} \frac{m_1(n)}{n},
\]

and (Equivocation Condition):

\[
\lim_{n \to \infty} \frac{\dim \left( \text{Proj}_{\mathcal{I}_j} \text{colspan} \left( G_{ji1}^n V_1^n \right) \right)}{n} \overset{a.s.}{\to} 0, \quad 2 \leq j \leq k+1.
\]

We define \( \mathcal{D} \) to be the set of all achievable \( d \)'s. We also define linear secure degrees of freedom (LSDoF) to be the supremum of all \( d \in \mathcal{D} \).

**Remark 1.** Equivocation condition in (9) implies that

\[
\lim_{n \to \infty} \frac{I(W; Y^n)}{n \log PP} = 0, \quad 2 \leq j \leq k+1,
\]

for linear schemes, where \( W \) is the secret message and \( Y^n \) is the received signal at Rx \( j \); this means that the prelog factor of the Equivocation rate to eavesdroppers would asymptotically vanish as \( n \to \infty \).\(^2\)

\(^2\)This condition is weaker than the condition \( \lim_{n \to \infty} \frac{I(W; Y^n)}{n \log PP} = 0, \quad 2 \leq j \leq k+1 \), considered in some prior works. However, one can combine our achievable scheme for blind wiretap channel with delayed CSIT with random binning to satisfy the latter condition as well.

The following theorem, proved in Section III, states that \( \frac{1}{3} \) is the maximum secure DoF that can be achieved using linear encoding schemes.

**Theorem 1.** For the blind cooperative wiretap channel with a distributed jammer and delayed CSIT,

\[
\text{LSDoF} = \frac{1}{3}.
\]

In the case that transmitters have no CSIT with respect to the legitimate receiver (Rx\( 1 \)), the received signal at all the receivers are statistically the same, and therefore, LSDoF is equal to 0. In addition, in the case that transmitters have instantaneous CSIT with respect to the legitimate receiver, one can show that LSDoF is \( \frac{1}{3} \). Therefore, Theorem 1 captures the impact of delayed CSIT as well.

**Remark 2.** Theorem 1 implies that no matter how many eavesdroppers exist in the network (as long as there is at least one), the linear secure DoF will be the same.

On the other hand, similar to the prior work on blind MIMO wiretap channel [16], one can consider the case where all the nodes in the network (i.e., the transmitter and all the receivers) are equipped with multiple antennas (details are presented in Section IV). For such network, Yang et. al. have presented achievable schemes in [16] which show that strictly positive SDof can be achieved in some configurations. However, there is no known converse for the problem. The following result improves the achievable schemes presented in [16], and it further shows that the proposed achievable schemes are optimal when using linear coding strategies.

**Theorem 2.** For the blind MIMO wiretap channel with delayed CSIT and with \( M \) antennas at the transmitter and \( N_j \) antennas at Rx\( j \), let \( N_{max} \) denote the maximum of \( N_1, \ldots, N_{k+1} \). Then, LSDoF is characterized as following:

- If \( M \leq \max(N_1, N_{max}) \),

\[
\text{LSDoF} = \left[ M - N_{max} \right]^+.
\]

- If \( N_{max} \leq N_1 < M \),

\[
\text{LSDoF} = \frac{N_1 \left( \min(M, N_1 + N_{max}) - N_{max} \right)}{\min(M, N_1 + N_{max})}\]

- If \( N_1 \leq N_{max} < M < N_1 + N_{max} \),

\[
\text{LSDoF} = \frac{N_1 (M - N_{max})}{M + N_1 - N_{max}}\]

- If \( N_1 \leq N_{max}, M \geq N_1 + N_{max} \),

\[
\text{LSDoF} = \frac{N_1}{2},
\]

where \( \lfloor x \rfloor^+ = \max(0, x) \).

Theorem 2 improves the achievable schemes presented in [16], while providing tight outer bounds. Furthermore, as a special case, Theorem 2 implies that the achievable scheme presented in [18] for blind MISO wiretap channel with delayed CSIT, which achieves \( \frac{1}{2} \), is indeed optimal when restricted to linear coding schemes.

In the following sections (Section III and Section IV) we provide the proofs for Theorem 1 and Theorem 2 and explain the key ideas behind the proofs.
III. PROOF OF THEOREM 1

In this section we prove Theorem 1 which characterizes the LSDoF of blind cooperative wiretap channel with delayed CSIT. We first present the achievability, and then prove the converse, which is the main contribution of this Section.

A. Achievability

Our achievable scheme uses artificial noise alignment to achieve \( \frac{1}{4} \). In particular, the scheme keeps the dimension of received signals the same in all receivers, but makes sure the dimension of noise at the legitimate receiver is \( \frac{2}{3} \) of that at the eavesdroppers. This way, the legitimate receiver can use \( \frac{1}{4} \) of its total received signal dimension to decode its desired message, while the message is completely drowned in noise at the eavesdroppers. Therefore, noise at the eavesdroppers will occupy the whole received signal dimension.

We set \( n = 3 \). Let the symbols of the transmitters be denoted by

\[
\vec{x} = \begin{bmatrix} x \\ a_1 \\ a_2 \end{bmatrix}, \quad \vec{w}_1 = \begin{bmatrix} \vec{a}_1 \\ b_1 \\ b_2 \end{bmatrix}, \quad \vec{w}_2 = \begin{bmatrix} \vec{a}_2 \\ b_1 \\ b_2 \end{bmatrix}.
\] (11)

Transmit symbols are Gaussian random variables with variance \( \sigma \). In \( t = 1 \), \( \text{Tx}_1 \) sends the noise symbol \( \vec{a}_1 \), and \( \text{Tx}_2 \) sends the noise symbol \( \vec{b}_1 \), which results in receiving the following linear combinations at the receivers:

\[
\text{Rx}_j : \quad L_j(\vec{a}_1, \vec{b}_1), \quad j = 2, \ldots, k + 1.
\]

In \( t = 2 \), \( \text{Tx}_1 \) retransmits noise symbol \( \vec{a}_1 \), and \( \text{Tx}_2 \) sends noise symbol \( \vec{b}_2 \), resulting in the following received signals:

\[
\text{Rx}_j : \quad L_j(\vec{a}_1, \vec{b}_2), \quad j = 2, \ldots, k + 1.
\] (12)

By the end of timeslot 2, \( \text{Rx}_1 \) has received two equations regarding \( \vec{a}_1, \vec{b}_1, \vec{b}_2 \); therefore, it can linearly combine the two equations to remove \( \vec{a}_1 \) and get a new equation \( L(\vec{b}_1, \vec{b}_2) \).

In \( t = 3 \), \( \text{Tx}_1 \) sends information symbol \( \vec{x} \), and \( \text{Tx}_2 \) sends noise equation \( L(\vec{b}_1, \vec{b}_2) \), which is already known by \( \text{Rx}_1 \), but not known by the eavesdroppers almost surely. Therefore, \( \text{Rx}_1 \) can decode \( \vec{x} \), while \( \text{Rx}_j \), for \( j = 2, \ldots, k + 1 \), almost surely cannot decode \( \vec{x} \). Therefore, \( \frac{1}{3} \) linear secure DoF is achieved.

Remark 3. Note that the above achievable scheme does not depend on how many eavesdroppers exist in the network, hence it implies that LSDoF \( \geq \frac{1}{4} \) (\( \forall k \geq 1 \)).

B. Converse

Note that LSDoF is non-increasing in the number of eavesdroppers \( k \). Therefore, it is sufficient to show that for the special case of \( k = 1 \), LSDoF \( \leq \frac{1}{3} \).

There are two key ingredients in proving the converse. The first one is the Rank Ratio Inequality, which is developed in [17], and captures how much the minimum ratio of \( \text{rank} [G_{11}^n U_1^n G_{12}^n U_2^n] \) to \( \text{rank} [G_{21}^n U_1^n G_{22}^n U_2^n] \) is, or more formally the following lemma.

**Lemma 1. (Rank Ratio Inequality [17])** For any linear coding strategy \( \{f_1(n), f_2(n)\} \), with corresponding \( U_1^n, U_2^n \) as defined in (3)-(4),

\[
\text{rank} [G_{21}^n U_1^n G_{22}^n U_2^n] \leq \frac{3}{2} \text{rank} [G_{11}^n U_1^n G_{12}^n U_2^n].
\] (13)

The second ingredient of the converse is the following lemma, which captures the impact of asymmetric CSIT in the network, and we prove later in Section III-C.

**Lemma 2. (Least Alignment Lemma)** For any linear coding strategy \( \{f_1(n), f_2(n)\} \), with corresponding \( V_1^n, U_1^n, U_2^n \) as defined in (2)-(4),

\[
\text{rank} [G_{11}^n V_1^n G_{12}^n U_1^n G_{12}^n U_2^n] \leq \text{rank} [G_{21}^n V_1^n G_{22}^n U_1^n G_{22}^n U_2^n].
\]

Remark 4. Lemma 2 implies that when using linear schemes, once the transmitters in a network have no CSIT with respect to a certain receiver, the least amount of alignment will occur at that receiver, meaning that transmit signals will occupy the maximal signal dimensions at that receiver.

We will now prove the converse using the above two lemmas. First, we state the following claim which can be proved using simple linear algebra, and hence the proof is omitted for brevity.

**Claim 1.** For two matrices \( A, B \) of the same row size,

- \( \text{rank}[A B] - \text{rank}[B] = \text{dim}(\text{Proj}_{\text{rowspan}(B)}[\text{colsran}(A)]); \)
- \( \text{rank}[A B] - \text{rank}[B] = \text{dim}(\text{span}([\vec{s}^0] | [\vec{s}^0] \in \text{rowspan}[A B])); \)

Using the second identity in Claim 1 and using some simple linear algebra, one can show the following Corollary.

**Corollary 1.** Consider four matrices \( A, B, C, D \), where \( A, B \) have the same number of rows; \( C, D \) have the same number of rows; \( A, C \) have the same number of columns; and \( B, D \) have the same number of columns. Then,

\[
\text{rank}[A B] - \text{rank}[B] \leq \text{rank}[A B C D] - \text{rank}[B D],
\] (14)

where \( [B；D] \) denotes the vertical concatenation of matrices \( B \) and \( D \) (i.e., \( \begin{bmatrix} B \\ D \end{bmatrix} \)).

Using Claim 1 the decodability condition in (7) can be rewritten as

\[
\text{rank}[G_{11}^n V_1^n G_{12}^n U_1^n G_{12}^n U_2^n] - \text{rank}[G_{11}^n U_1^n G_{12}^n U_2^n] = \text{rank}[V_1^n] = m_1(n).
\] (15)

Suppose \( d \in D \), i.e., there exists a sequence \( \{f_1(n), f_2(n)\}_{n=1}^\infty \) resulting in satisfying (7), (9) with probability 1, and \( d = 3 \).

Note that the original lemma in [17] is stated for the case where transmitters have delayed CSIT of all the channels; however, the same analysis and result holds when transmitters have delayed CSIT with respect to the channels of only \( \text{Rx}_1 \).
Transmit Signals

\begin{align*}
\begin{array}{ccc}
\text{time} & a_1 & b_1 \\
& a_1 & b_2 \\
& \text{x} & \text{L}(b_1, b_2)
\end{array}
\end{align*}

Received Signals

\begin{align*}
\begin{array}{ccc}
\text{time} & L_1(a_1, b_1) & L_2(a_1, b_2) \\
& L_3(a_1, b_2) & L_4(x, L(b_1, b_2))
\end{array}
\end{align*}

\begin{itemize}
\item L(b_1, b_2) is an equation derived by combining \(L_1(a_1, b_1)\) and \(L_2(a_1, b_2)\) to remove \(a_1\).
\item X can be recovered
\end{itemize}

\section*{Fig. 2. The achievable scheme for the blind cooperative wiretap channel with delayed CSIT uses 3 timeslots, where in the first 2 timeslots only artificial noise is being transmitted. In the third timeslot Tx_1 sends the secret symbol x, while Tx_2 sends a noise equation that Rx_1 has already recovered, but not the eavesdroppers.}

\[
\lim_{n \to \infty} m_1(n) = \frac{m_{1,n}}{n}. \quad \text{Hence, for each } n, \text{ by the decodability condition in (E), we have}
\]

\[
\text{rank}[G_{11}^n V_1^n \ G_{11}^n U_1^n \ G_{12}^n U_2^n] = \text{rank}[G_{11}^n V_1^n \ G_{11}^n U_1^n \ G_{12}^n U_2^n] = m_1(n).
\]

\[
\text{Furthermore, we define}
\]

\[
eaveses(n) \triangleq \text{rank}[G_{21}^n V_1^n \ G_{21}^n U_1^n \ G_{22}^n U_2^n] - \text{rank}[G_{21}^n U_1^n \ G_{22}^n U_2^n].
\]

\[
\text{It is easy to see that by Claim 1,}
\]

\[
eaveses(n) = \text{dim} \left( \text{Proj}_{Z_1} \text{colspan}(G_{11}^n V_1^n) \right),
\]

\[
\text{with } j = 2, \text{ where } I_j \text{ is defined in (6). Therefore, by Equivocation in (G), we have}
\]

\[
\lim_{n \to \infty} \frac{eaveses(n)}{n} = 0.
\]

\section*{C. Proof of Lemma 2}

Let us fix \( n \), and consider a fixed linear coding strategy \( \{e_1(n), e_2(n)\} \), with the corresponding \( V_1^n \in \mathbb{C}^{m_1 \times m_1(n)}, U_1^n \in \mathbb{C}^{m_2 \times m_2(n)}, U_2^n \in \mathbb{C}^{m_3 \times m_3(n)} \) as defined in (2)-(4). For ease of notation, we define \([V_1^n \ U_1^n] \text{ by } [W_1^n]\). Hence, we need to show\([G_{11}^n W_1^n G_{12}^n U_2^n] \leq \text{rank}[G_{21}^n W_1^n G_{22}^n U_2^n]. We also define \(m \triangleq m_1(n) + m_2(n) + m_3(n)\). We now state a lemma that will be useful later in the proof of Lemma 2.

\section*{Lemma 3. (22)} A multi-variate polynomial function on \( \mathbb{C}^n \rightarrow \mathbb{C} \), is either identically 0, or non-zero almost everywhere.

We now prove Lemma 2. Let us denote by \([1 : n]\) the set \(\{1, \ldots, n\}\). For any matrix \(B_{n \times m}\) and \(I_1 \subseteq [1 : n]\), and \(I_2 \subseteq [1 : m]\), we denote by \(B_{I_1 I_2}\) the sub-matrix of \(B\) whose rows and columns are specified by \(I_1\) and \(I_2\), respectively. Define the set of realizations \(\mathcal{A}\) as:

\[
\mathcal{A} \triangleq \{G^n | \text{rank}[G_{11}^n W_1^n G_{12}^n U_2^n] > \text{rank}[G_{21}^n W_1^n G_{22}^n U_2^n]\}
\]

Note that in order to prove \(\text{rank}[G_{11}^n W_1^n G_{12}^n U_2^n] \leq \text{rank}[G_{21}^n W_1^n G_{22}^n U_2^n]\), we only need to show \(\Pr(A) = 0\).

Since a matrix \(B_{n \times m}\) has rank \(r\) if and only if the maximum size of a square sub-matrix of \(B\) with non-zero determinant is \(r\), we have:

\[
A \subseteq \{G^n | \exists I_1 \subseteq [1 : n], I_2 \subseteq [1 : m], |I_1| = |I_2|, \text{s.t.} \det([G_{11}^n W_1^n G_{12}^n U_2^n]_{I_1, I_2}) \neq 0, \det([G_{21}^n W_1^n G_{22}^n U_2^n]_{I_1, I_2}) = 0\},
\]

which can be rewritten as

\[
A \subseteq \bigcup_{I_1 \subseteq [1 : n]} \{G^n | \det([G_{11}^n W_1^n G_{12}^n U_2^n]_{I_1, I_2}) \neq 0, \det([G_{21}^n W_1^n G_{22}^n U_2^n]_{I_1, I_2}) = 0\}.
\]

Let \(X^n \triangleq \text{diag}(x_1, \ldots, x_n)\) and \(Y^n \triangleq \text{diag}(y_1, \ldots, y_n)\), where \(x_1, \ldots, x_n, y_1, \ldots, y_n\) are variables in \(\mathbb{C}\). Then, for any \(I_1 \subseteq [1 : n], I_2 \subseteq [1 : m]\), where \(|I_1| = |I_2|\), \(\det([X^n W^n Y^n]_{I_1, I_2})\) is a multi-variate polynomial function in \(x_1, \ldots, x_n, y_1, \ldots, y_n\). Note that if for some realization \(X^n = G_{11}^n\) and \(Y^n = G_{12}^n\), \(\det([X^n W^n Y^n]_{I_1, I_2}) \neq 0\), then the polynomial function defined by \(\det([X^n W^n Y^n]_{I_1, I_2})\) is not identical to zero \(\det([X^n W^n Y^n]_{I_1, I_2}) \neq 0\). So, by (21), we have:

\[
\text{det}([X^n W^n Y^n]_{I_1, I_2}) = 0.
\]
have

\[ A \subseteq \bigcup_{I_1 \subseteq [1:n]} \{ G^n | \det([X^n W_1^n \ Y^n U^n_2^n]_{I_1 I_2}) \neq 0 \}, \]

\[ \det([G^n_{21} W_1^n \ G^n_{22} U^n_2^n]_{I_1 I_2}) = 0 \}

\[ = \bigcup_{I_1 \subseteq [1:n]} \{ G^n | \det([X^n W_1^n \ Y^n U^n_2^n]_{I_1 I_2}) \neq 0, \]

\[ G_{21}, G_{22} \text{ are roots of } \det([X^n W_1^n \ Y^n U^n_2^n]_{I_1 I_2}) \}. \] (22)

Note that by Lemma 3, for every \( I_1 \in [1 : n], I_2 \in [1 : m], |I_1| = |I_2| \), we have

\[ \Pr(\{ G^n | \det([X^n W_1^n \ Y^n U^n_2^n]_{I_1 I_2}) \neq 0, \]

\[ G_{21}, G_{22} \text{ are roots of } \det([X^n W_1^n \ Y^n U^n_2^n]_{I_1 I_2}) \}) = 0. \] (23)

So, since finite union of measure-zero sets has measure zero,

\[ \Pr(\{ G^n | \det([X^n W_1^n \ Y^n U^n_2^n]_{I_1 I_2}) \neq 0, \]

\[ G_{21}, G_{22} \text{ roots of } \det([X^n W_1^n \ Y^n U^n_2^n]_{I_1 I_2}) \}) = 0, \] (24)

which by (22) implies that \( \Pr(A) = 0. \)

**Remark 5.** Using the same line of argument as in the proof of Lemma 2 one can prove Lemma 2 in a more general network setting where there are arbitrary number of transmitters, and the transmitters have arbitrary number of antennas. In addition, the assumption of delayed CSIT of channels to Rx1 can be relaxed to any form of CSIT of channels to Rx1 (e.g. instantaneous CSIT, or partial delayed CSIT). Furthermore, the statement in Lemma 2 holds as long as the number of antennas in Rx1 and Rx2 are equal.

IV. BLIND MIMO WIRETAP CHANNEL WITH DELAYED CSIT

In this section we study the blind MIMO wiretap channel with delayed CSIT. To this aim, we first briefly describe the system model, and then we provide complete characterization of the linear secure degrees of freedom.

**A. System Model & Main Results**

We consider the multiple-input multiple-output (MIMO) Gaussian wiretap channel depicted in Fig. 3, which consists of a transmitter (Tx) and \( k + 1 \) receivers, where Tx has a secret message for Rx1 (legitimate receiver); and Rx2, . . . , Rx\( k+1 \) are the eavesdroppers. Tx is equipped with \( M \) antennas, and for each \( j, j \in \{1, \ldots, k+1\} \), Rx\( j \) has \( N_j \) antennas.

The received signal at Rx\( j \) (\( j \in \{1, \ldots, k+1\} \)) at time \( t \) is given by

\[ \tilde{y}_j(t) = g_j(t) x(t) + \tilde{z}_j(t), \] (25)

where \( x(t) \in \mathbb{C}^M \) is the transmit signal vector of Tx; \( g_j(t) \in \mathbb{C}^{N_j \times M} \) indicates the channel matrix from Tx to Rx\( j \); and \( \tilde{z}_j(t) \sim \mathcal{CN}(0, I_{N_j}) \). The channel coefficients comprising \( g_j(t) \) are i.i.d across time and antennas, and they are drawn from a continuous distribution. We denote by \( \mathcal{G}(t) \) the set of all channel coefficients at time \( t \). In addition, we denote by \( \mathcal{G}^n \) the set of all channel coefficients from time 1 to \( n \), i.e.,

\[ \mathcal{G}^n \triangleq \{ g_j(t) : j \in \{1, \ldots, k+1\}, t \in \{1, \ldots, n\} \}. \]

We assume delayed channel state information at the transmitters (CSIT) with respect to channels to the legitimate receiver (Rx1); however, the transmitter has no knowledge of channels to the eavesdroppers. In other words, at time \( t \), only the states of the past \( \mathcal{G}_0^{t-1} \triangleq \{ g_i(t) : h = 1, \ldots, t-1 \} \) are known to the transmitter.

Similar to the model presented in Section II, we consider linear coding strategies. In particular, we consider a communication scheme with block length \( n \), in which Tx wishes to communicate a vector \( \tilde{x} \in \mathbb{C}^{m_1(n)} \) of \( m_1(n) \in \mathbb{N} \) information symbols to Rx1. The information symbols are then modulated at time \( t \), \( t = 1, \ldots, n \), with precoding matrix \( v(t) \in \mathbb{C}^{M \times m_1(n)} \). In addition, Tx is allowed to use a vector \( \tilde{w} \in \mathbb{C}^{m_2(n)} \) of \( m_2(n) \in \mathbb{N} \) noise symbols, modulated with precoding matrix \( u(t) \in \mathbb{C}^{M \times m_2(n)} \) at time \( t \), \( t = 1, 2, \ldots, n \). Note that the precoding matrices \( v(t), u(t) \) depend only upon the outcome of \( \mathcal{G}_0^{t-1} \) due to the delayed channel knowledge constraint.

We denote the precoding functions used by Tx by \( f(n) \). In addition, we denote by \( \mathcal{V}^n \in \mathbb{C}^{nM \times m_1(n)} \), and \( \mathcal{U}^n \in \mathbb{C}^{nM \times m_2(n)} \) the overall precoding matrices such that \( v(t) \) occupies the rows \( 1 + (t-1)M, \ldots, tM \) of \( \mathcal{V}^n \), and \( u(t) \) occupies the rows \( 1 + (t-1)M, \ldots, tM \) of \( \mathcal{U}^n \). Moreover, we denote by \( \mathcal{G}_j^n \in \mathbb{C}^{N_j \times nM} \) the block diagonal channel coefficients matrix where the channel coefficients of timeslot \( t \) are in the rows \( 1 + (t-1)N_j, \ldots, tN_j \), and in the columns \( 1 + (t-1)M, \ldots, tM \).

Based on the above setting, the received signal at Rx\( j \) (\( j \in \{1, \ldots, k+1\} \)) after the \( n \) time steps of the communication will be

\[ y_j^n = \mathcal{G}_j^n \mathcal{V}^n \tilde{x} + \mathcal{G}_j^n \mathcal{U}^n \tilde{w} + \tilde{z}_j^n. \] (26)

Now, consider decoding \( \tilde{x} \) at Rx\( j \) for \( j = 1, \ldots, k+1 \). The interference subspace at Rx\( j \) will be

\[ \mathcal{I}_j = \text{colspan} \left( \{ \mathcal{G}_j^n \mathcal{U}^n \} \right). \] (27)

The decodability condition for information symbols of Tx at
\[ \text{dim} \left( \text{Proj}_{x_1} \text{colspan} \left( G^n \right) \right) = \text{dim} \left( \text{colspan} \left( V^n \right) \right) = m_1(n). \tag{28} \]

Based on this setting, we now define the linear secure degrees of freedom (LSDoF) of the blind MIMO wiretap channel with delayed CSIT.

**Definition 2.** Secure degrees of freedom are linearly achievable if there exists a sequence \( \{f(n)\}_{n=1}^\infty \) such that for each \( n \), \( V^n \) satisfies the decodability condition of (28) with probability 1, and

\[ d = \lim_{n \to \infty} \frac{m_1(n)}{n}, \tag{29} \]

and (Equivocation Condition):

\[ \lim_{n \to \infty} \frac{\text{dim} \left( \text{Proj}_{x_j} \text{colspan} \left( G^n \right) \right)}{n} \xrightarrow{a.s.} 0, \quad 2 \leq j \leq k + 1. \tag{30} \]

We define \( D \) to be the set of all achievable \( d \)'s. We also define linear secure degrees of freedom (LSDoF) to be the supremum of all \( d \in D \).

Our main result in this section is the characterization of the LSDoF of the blind MIMO wiretap channel with delayed CSIT, as stated in Theorem 2. We restate the Theorem here for convenience.

**Theorem 2.** For the blind MIMO wiretap channel with delayed CSIT and with \( M \) antennas at the transmitter and \( N \) antennas at Rx, let \( N_{\text{max}} \) denote the maximum of \( N_2, \ldots, N_{k+1} \). Then, LSDoF is characterized as following:

- If \( M \leq \max(N_1, N_{\text{max}}) \),

\[ \text{LSDoF} = [M - N_{\text{max}}]^+ \]

- If \( N_{\text{max}} \leq N_1 < M \),

\[ \text{LSDoF} = \frac{N_1(\min(M, N_1 + N_{\text{max}}) - N_{\text{max}})}{\min(M, N_1 + N_{\text{max}})} \]

- If \( N_1 \leq N_{\text{max}} < M < N_1 + N_{\text{max}} \),

\[ \text{LSDoF} = \frac{N_1(M - N_{\text{max}})}{M + N_1 - N_{\text{max}}} \]

- If \( N_1 \leq N_{\text{max}}, M \geq N_1 + N_{\text{max}} \),

\[ \text{LSDoF} = \frac{N_1}{2}, \]

where \([x]^+ = \max(x, 0)\).

**B. Proof of Achievability**

In this section we present the achievable schemes for different antenna configurations. The first two cases (i.e. \( M \leq \max(N_1, N_{\text{max}}) \) and \( N_{\text{max}} \leq N_1 < M \)) are presented in [16]; so, we briefly state them here.

Let us denote by Rx_{\text{max}} the eavesdropper with \( N_{\text{max}} \) antennas.

1) Case of \( M \leq \max(N_1, N_{\text{max}}) \): Note that for the case where \( M \leq N_{\text{max}} \), Theorem 2 suggests that LSDoF = 0; so there is nothing to prove on the achievability side. So, let us consider the case where \( N_{\text{max}} < M \leq N_1 \). In this case we securely deliver \( M - N_{\text{max}} \) information symbols to Rx_1 in each timeslot. In particular, in each timeslot, each of the first \( N_{\text{max}} \) transmit antennas sends a distinct new noise symbol, while each of the antennas with index \( N_{\text{max}} + 1, \ldots, M - 1 \) sends a distinct new information symbol. Consequently, Rx_2 decodes all symbols almost surely, including the \( M - N_{\text{max}} \) information symbols, since it receives \( N_1 \) equations in \( M \) unknowns, where \( M \leq N_1 \). On the other hand, the Equivocation condition in (30) for Rx_{\text{max}} is satisfied. This is due to the following: note that Claim 1 provides an alternative representation for the Equivocation condition. Therefore, for the Equivocation condition in (30) to hold for Rx_{\text{max}}, it is sufficient to have \( \text{rank}[G^n_{\text{max}}(V^n, U^n)] \xrightarrow{a.s.} \text{rank}[G^n_{\text{max}}(U^n)] \). But note that for each \( n \), \( \text{rank}[G^n_{\text{max}}(V^n, U^n)] \xrightarrow{a.s.} \text{rank}[G^n_{\text{max}}(U^n)] = nN_{\text{max}}, \) which means the Equivocation condition holds for Rx_{\text{max}}. Similarly, one can argue that the Equivocation condition (30) holds for other eavesdroppers with less number of antennas as well. Hence, LSDoF \( \geq M - N_{\text{max}} \).

2) Case of \( N_{\text{max}} \leq N_1 < M \): In this case the scheme securely delivers \( N_1(\min(M, N_1 + N_{\text{max}}) - N_{\text{max}}) \) information symbols over \( \min(M, N_1 + N_{\text{max}}) \) timeslots. The scheme is presented in two phases.

**Phase 1:** For \( t = 1, 2, \ldots, N_{\text{max}} \), each of the first \( \min(M, N_1 + N_{\text{max}}) \) antennas of the transmitter sends a distinct new noise symbol. Hence, Rx_1 obtains \( \min(M, N_1 + N_{\text{max}}) \) linearly independent noise equations in each timeslot that are almost surely not known by Rx_{\text{max}} (for instance, what Rx_1 receives on its first \( \min(M, N_1 + N_{\text{max}}) - N_{\text{max}} \) antennas are not recoverable by Rx_{\text{max}}). Hence, by the end of Phase 1, Rx_1 obtains \( N_{\text{max}}(\min(M, N_1 + N_{\text{max}}) - N_{\text{max}}) \) linearly independent noise equations that are not known by Rx_{\text{max}}.

**Phase 2:** In each of the timeslots \( t \in \{N_{\text{max}} + 1, \ldots, \min(M, N_1 + N_{\text{max}})\} \), the first \( N_{\text{max}} \) transmit antennas each send a linearly independent noise equation known by Rx_1 (which is not recoverable by other receivers) plus a distinct information symbol. In addition, each of the transmit antennas with index \( N_{\text{max}} + 1, \ldots, N_1 \) sends a distinct information symbol. In each timeslot of Phase 2, Rx_1 cancels the noise equations that are being sent from its received signal, and recovers \( N_1 \) information symbols. Therefore, Rx_1 recovers \( N_1(\min(M, N_1 + N_{\text{max}}) - N_{\text{max}}) \) information symbols in total. On the other hand, the rank of interference matrix (i.e. \( \text{rank}[G^n_{\text{max}}(U^n)] \)) in Rx_{\text{max}} is the same as the rank of the total received signal in that receiver (i.e. \( \text{rank}[G^n_{\text{max}}(V^n, U^n)] \)) almost surely. This together with Claim 1 means that the Equivocation condition (i.e. (30)) holds for Rx_{\text{max}} (similarly the Equivocation condition also holds for other eavesdroppers).

Hence, overall \( N_1(\min(M, N_1 + N_{\text{max}}) - N_{\text{max}}) \) information symbols are delivered securely to Rx_1 over \( \min(M, N_1 + N_{\text{max}}) \) timeslots. The scheme consists of two phases.
For $t = 1, 2, \ldots, N_1$, each antenna sends a distinct new noise symbol. Hence, Rx$_1$ obtains $(M - N_{max})$ linearly independent noise equations in each timeslot that are almost surely not known by Rx$_{max}$ (for instance, what Rx$_1$ receives on its first $(M - N_{max})$ antennas are not recoverable by Rx$_{max}$). Also, note that in each of the timeslots of this phase the noise equations received on the first $(M - N_{max})$ antennas of Rx$_1$ are almost surely not recoverable by other eavesdroppers either. Hence, by the end of Phase 1, Rx$_1$ obtains $N_1(M - N_{max})$ linearly independent noise equations that are not known by any of the eavesdroppers almost surely.

**Phase 2:** In each of the timeslots $t \in \{N_1 + 1, \ldots, M + N_1 - N_{max}\}$, $N_1$ transmit antennas are active, each sending a linearly independent noise equation known by Rx$_1$ (which is not recoverable by other receivers) plus a distinct information symbol. In each timeslot of Phase 2, Rx$_1$ cancels the noise equations that are being sent from its received signal, and recovers $N_1$ information symbols. Therefore, Rx$_1$ recovers $N_1(M - N_{max})$ information symbols in total. On the other hand, the Equivocation condition in (30) for Rx$_{max}$ is satisfied. This is due to the following: note that Claim 1 provides an alternative representation for the Equivocation condition. Therefore, for the Equivocation condition in (30) to hold for Rx$_{max}$, it is sufficient to have, for $n = M + N_1 - N_{max}$, \( \text{rank}[G_{max}^n[V^n \ U^n]] \overset{a.s.}{=} \text{rank}[G_{max}^n U^n] \). But note that \( \text{rank}[G_{max}^n[V^n \ U^n]] \overset{a.s.}{=} \text{rank}[G_{max}^n U^n] \overset{a.s.}{=} N_1 N_{max} + N_1(M - N_{max}) = N_1 M \), which means the Equivocation condition holds for Rx$_{max}$. Similarly, one can argue that the Equivocation condition holds for other eavesdroppers with less number of antennas as well. Hence, overall $N_1(M - N_{max})$ information symbols are delivered securely to Rx$_1$ over $M + N_1 - N_{max}$ timeslots.

The achievable scheme for a simple configuration of this case, which outperforms the state-of-the-art scheme, is presented in Fig. 5.

**C. Proof of Converse**

Note that for any antenna configuration $(M, N_1, N_2, \ldots, N_{k+1})$, if some of the eavesdroppers are removed from the network, LSDoF will be no less than its value before removing those eavesdroppers, and this is due to dropping some of the constraints on maximizing LSDoF. Hence, to prove the converse we first remove all the eavesdroppers except Rx$_{max}$ from the network.

For each antenna configuration $(M, N_1, N_2, \ldots, N_{k+1})$, using Claim 1 the decodability condition in (28) can be rewritten as

\[
\text{rank}[G_i^n[V^n \ U^n]] - \text{rank}[G_i^n U^n] = \text{rank}[V^n] = m_1(n). \quad (31)
\]

Suppose $d$ linear secure DoF can be achieved, i.e., there exists a sequence \( \{f^{(n)}\}_{n=1}^{\infty} \) resulting in satisfying (7), (9) with probability 1, and $d = \lim_{n \to \infty} m_1(n)$. Hence, for each $n$, by the decodability condition in (31) we have

\[
\text{rank}[G_i^n[V^n \ U^n]] - \text{rank}[G_i^n U^n] \overset{a.s.}{=} \text{rank}[V^n] \overset{a.s.}{=} m_1(n). \quad (32)
\]
Furthermore, we define
\[
eaves(n) \triangleq \text{rank}[G_{\text{max}}^n [V^n \ U^n]] - \text{rank}[G_{\text{max}}^n U^n].
\] (33)

It is easy to see that by Claim [1]
\[
eaves(n) = \dim \left( \text{Proj}_{\text{max}} \ \text{colspan} (G_{\text{max}}^n V^n) \right),
\]
where \( I_{\text{max}} \) is as defined in (27). Therefore, by Equivocation in (30), we have
\[
\lim_{n \to \infty} \frac{\eaves(n)}{n} \overset{a.s.}{=} 0.
\] (34)

The following lemma is the MIMO version of the Rank Ratio Inequality (Lemma [1]). In particular, Lemma [1] considers the SISO 2-transmitter 2-receiver network with delayed CSIT, while in the following Lemma the focus is on the rank ratio for the network with a single multi-antenna transmitter and 2 multi-antenna receivers.

**Lemma 4. (MIMO RRI)** For any fixed \( n \), and any linear coding strategy \( \{f^{(n)}\} \), with corresponding \( U^n \) as defined in Section \([1]A\)

\[
\begin{align*}
\frac{\text{rank}[G_{\text{max}}^n U^n]}{N_{\text{max}}} & \overset{a.s.}{\geq} \frac{\text{rank}[G_1^n U^n; G_{\text{max}}^n U^n]}{\min(M, N_1 + N_{\text{max}})}; \\
\frac{\text{rank}[G_1^n U^n]}{N_1} & \overset{a.s.}{\geq} \frac{\text{rank}[G_1^n U^n; G_{\text{max}}^n U^n]}{\min(M, N_1 + N_{\text{max}})},
\end{align*}
\]

where \([B; D]\) denotes the vertical concatenation of matrices \( B \) and \( D \) (i.e., \([B; D]\)).

The proof for Lemma [4] follows from channel symmetry; it follows the same steps as the proof of Lemma 1 in [16]; and therefore, it has been omitted for brevity.

We will now use the above derivations to prove the converse for each specific choice of antenna configuration \((M, N_1, N_2, \ldots, N_{k+1})\). Note that the above derivations do not depend on which \((M, N_1, N_2, \ldots, N_{k+1})\) is considered.

1) Case of \( M \leq \max(N_1, N_{\text{max}}) \): By the decodability assumption \([32]\),
\[
m(n) \overset{a.s.}{=} \text{rank}[G_1^n [V^n \ U^n]] - \text{rank}[G_1^n U^n] \leq \text{rank}[G_1^n [V^n \ U^n]; G_{\text{max}}^n [V^n \ U^n]] - \text{rank}[G_1^n U^n] \leq \text{rank}[G_1^n [V^n \ U^n]; G_{\text{max}}^n [V^n \ U^n]] - \text{rank}[G_{\text{max}}^n U^n]
\]
\[
= \text{rank}[G_1^n [V^n \ U^n]; G_{\text{max}}^n [V^n \ U^n]] - \text{rank}[G_{\text{max}}^n [V^n \ U^n]]
\]
\[
- \text{rank}[G_{\text{max}}^n [V^n \ U^n]] + \text{eaves}(n)
\]

\([\text{Lemma } 1, \overset{a.s.}{\leq} \text{min}(M, N_1 + N_{\text{max}} - N_{\text{max}}) + \text{eaves}(n) \]
\[
\times \text{rank}[G_{\text{max}}^n [V^n \ U^n]] + \text{eaves}(n)
\]
\[
\leq \frac{\text{min}(M, N_1 + N_{\text{max}} - N_{\text{max}}) + nN_{\text{max}}}{N_{\text{max}}}
\]
\[
\times \text{eaves}(n)
\]
\[
= \text{min}(M, N_1 + N_{\text{max}}) + n \text{eaves}(n).
\]

Hence, by dividing both sides of the above inequality by \( n \) and taking the limit \( n \to \infty \), the result follows.

2) Case of \( N_{\text{max}} \leq N_1 < M \): Let us first consider a hypothetical receiver \( \text{Rx}_0 \) with \( N_1 \) antennas for which there is no CSIT available to the transmitter. Hence, following similar arguments as in the proof of Lemma [2] we obtain the following inequality, which is the extension of Lemma [2] to the MIMO case (see Remark [5]).
\[
\text{rank}[G_1^n [V^n \ U^n]] \overset{a.s.}{=} \text{rank}[G_{\text{max}}^n [V^n \ U^n]].
\] (35)

Moreover, since \( N_1 \geq N_{\text{max}} \) and there is no CSIT with respect to any of \( \text{Rx}_0, \text{Rx}_{\text{max}} \), using the same steps as in the proof of Lemma 1 in [16] one can show that
\[
\frac{\text{rank}[G_0^n [V^n \ U^n]]}{N_1} \overset{a.s.}{\leq} \frac{\text{rank}[G_{\text{max}}^n [V^n \ U^n]]}{N_{\text{max}}}. 
\] (36)
Therefore, by combining the inequalities in (35), we get
\[
\text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n] \right]_{a.s.} \leq \frac{N_1}{N_{\max}} \text{rank} \left[ \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right].
\] (37)

Hence, we have
\[
m(n) \lesssim \frac{N_1}{N_{\max}} \text{rank} \left[ \mathbf{G}_1^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_i^*[\mathbf{U}^n] \right].
\] (38)

3) Case of \( N_1 \leq N_{\max} < M < N_1 + N_{\max} \): Let us first partition the rows of \( \mathbf{G}_{\max}^n \) to two sets of rows \( \mathbf{G}_{\max,1}^n, \mathbf{G}_{\max,2}^n \), where \( \mathbf{G}_{\max,1}^n \) comprises rows which contain the channel coefficients from the transmitter to the first \( N_1 \) antennas of \( \mathbf{Rx}_1 \), and \( \mathbf{G}_{\max,2}^n \) corresponds to rows which contain the channel coefficients from the transmitter to the remaining \( N_{\max} - N_1 \) antennas of \( \mathbf{Rx}_2 \). In addition, let us denote by \( \mathbf{G}_{\max,3}^n \) the channel to a virtual receiver with \( M - N_{\max} \) antennas from whom the transmitter has no CSIT.

Similarly, we partition \( \mathbf{G}_i^n \) to two sets of rows \( \mathbf{G}_{i,1}^n, \mathbf{G}_{i,2}^n \), where \( \mathbf{G}_{i,1}^n \) comprises rows which contain the channel coefficients from the transmitter to the first \( M - N_{\max} \) antennas of \( \mathbf{Rx}_1 \), and \( \mathbf{G}_{i,2}^n \) corresponds to rows which contain the channel coefficients from the transmitter to the remaining \( N_1 + N_{\max} - M \) antennas of \( \mathbf{Rx}_1 \).

Before going to the proof of converse, we first present a claim which is going to be used in the proof. The proof of the following claim is provided in Appendix A.

**Claim 2.**
\[
\frac{1}{M - N_{\max}} \left( \text{rank} \left[ \mathbf{G}_{i,1}^n[\mathbf{V}^n \mathbf{U}^n]; \mathbf{G}_{\max}^n[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_{i,1}^n[\mathbf{V}^n \mathbf{U}^n] \right] \right) \lesssim \frac{1}{N_{\max} - N_1} \left( \text{rank} \left[ \mathbf{G}_{\max,1}^n[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_{\max,1}^n[\mathbf{V}^n \mathbf{U}^n] \right] \right).
\] (39)

We now prove the converse. By the decodability assumption in (32) we have
\[
m(n) \lesssim \text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_i^*[\mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right] + eaves(n) \]
\[
\text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n] \right] - \frac{N_1}{M} \text{rank} \left[ \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right] + eaves(n) \]
\[
\text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n] \right] - \frac{N_1}{M} \text{rank} \left[ \mathbf{G}_{\max,1}^*[\mathbf{V}^n \mathbf{U}^n] \right] + eaves(n) \]
\[
\text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n] \right] - \frac{N_1}{M} \text{rank} \left[ \mathbf{G}_{\max,2}^*[\mathbf{V}^n \mathbf{U}^n] \right] + eaves(n) \]
\[
\text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n] \right] - \frac{N_1}{M} \text{rank} \left[ \mathbf{G}_{\max,3}^*[\mathbf{V}^n \mathbf{U}^n] \right].
\] (40)

Moreover, by the decodability assumption in (32),
\[
m(n) \lesssim \text{rank} \left[ \mathbf{G}_1^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_1^*[\mathbf{U}^n] \right].
\] (41)

**Corollary 1.**
\[
\text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n]; \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_i^*[\mathbf{U}^n]; \mathbf{G}_{\max}^*[\mathbf{U}^n] \right] \leq \text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n]; \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_i^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right] - \text{rank} \left[ \mathbf{G}_{\max}^*[\mathbf{V}^n \mathbf{U}^n] \right] + eaves(n).
\] (42)
We multiply both sides of (39) by \( \frac{M(M - N_{\text{max}})}{(M - N_1)(M + N_1 - N_{\text{max}})} \),
and multiply both sides of (40) by \( \frac{N_1(N_{\text{max}} - N_1)}{(M - N_1)(M + N_1 - N_{\text{max}})} \),
and sum the resulting inequalities together. Hence, we will have,

\[
m(n) \overset{a.s.}{\leq} \frac{M(M - N_{\text{max}})}{(M - N_1)(M + N_1 - N_{\text{max}})} (1 - N_1) M \times \text{rank} [G_1^n | V^n \ U^n] + eaves(n)
\]

\[
\leq \frac{M(M - N_{\text{max}})}{(M - N_1)(M + N_1 - N_{\text{max}})} (1 - \frac{N_1}{M}) nN_1 + eaves(n)
\]

\[
= \frac{(M - N_{\text{max}})}{(M + N_1 - N_{\text{max}})} nN_1 + eaves(n).
\]

Hence, by dividing both sides of the above inequality by \( n \)
and taking the limit \( n \to \infty \), the result follows.

4) Case of \( N_1 \leq N_{\text{max}} \), \( M \geq N_1 + N_{\text{max}} \): Let us partition the rows of \( G_{\text{max},1}^n \) again to two sets of rows \( G_{\text{max},1}^n, G_{\text{max},2}^n \) similar to the previous case, where \( G_{\text{max},1}^n \) comprises rows which contain the channel coefficients from the transmitter to the first \( N_1 \) antennas of Rx_{max}, and \( G_{\text{max},2}^n \) corresponds to rows which contain the channel coefficients from the transmitter to the remaining \( N_{\text{max}} - N_1 \) antennas of Rx_{max}.

Hence, following similar arguments as in the proof of Lemma 2, we get the following (for the MIMO case).

\[
\text{rank} [G_1^n | V^n \ U^n] \overset{a.s.}{\leq} \text{rank} [G_{\text{max},1}^n | V^n \ U^n]. \quad (41)
\]

We now prove the converse for this case. By decodability
assumption in (22), we have,

\[
m(n) \overset{a.s.}{=} \text{rank} [G_1^n | V^n \ U^n] - \text{rank} [G_{\text{max},1}^n | V^n \ U^n] 
\]

\[
\overset{(\text{Lemma 2})}{\leq} \text{rank} [G_{\text{max},1}^n | V^n \ U^n] - \text{rank} [G_{\text{max},1}^n | V^n \ U^n] 
\]

\[
\overset{(\text{Corollary 2})}{\leq} \frac{1}{2} \text{rank} [G_{\text{max},1}^n | V^n \ U^n] + \frac{1}{2} \text{rank} [G_{\text{max},1}^n | V^n \ U^n] + 1 \frac{eaves(n)}{2}
\]

\[
\leq \frac{1}{2} nN_1 + \frac{1}{2} eaves(n).
\]

Hence, by dividing both sides of the above inequality by \( n \)
and taking the limit \( n \to \infty \), the result follows.

V. CONCLUSION & FINAL REMARKS

In this paper we have considered the wiretap channel
consisting of a legitimate receiver and arbitrary number of
eavesdroppers, with delayed CSIT of the legitimate receiver
and no eavesdroppers CSIT. We considered two scenarios:
(i) the case where the secure communication is aided via a
distributed jammer (blind cooperative wiretap channel), and
(ii) the case where all nodes in the network are equipped with
multiple antennas (blind MIMO wiretap channel with delayed
CSIT). We characterize the secure Degrees of Freedom (SDoF)
in both scenarios, when assuming linear coding strategies at the
transmitter(s). In order to obtain the results we have
utilized the Rank Ratio Inequality developed in [17] along
with a new lemma (Least Alignment Lemma) which implies
that once the transmitters in a network have no CSIT with
respect to a receiver, the least amount of alignment will occur
at that receiver, meaning that transmit signals will occupy the
maximal signal dimensions at that receiver.

We conjecture that the results are true for general encoding
schemes as well. In particular, we conjecture the following
generalization of Least Alignment Lemma (Lemma 2) for
general encoding strategies.

**Conjecture 1.** For any coding strategy, denoted by encoding
functions \( \{P_n\}_{n=1}^\infty \), and the corresponding received signals
\( \bar{y}_1^n, \bar{y}_2^n \), we have

\[
h(\bar{y}_1^n | \mathbf{g}^n) \leq h(\bar{y}_2^n | \mathbf{g}^n) + n \times o(\log(P)) \quad \text{for } \mathbf{g}^n.
\]

Therefore, a future direction would be to remove the linearity
restriction on the encoding schemes, and prove/disprove
the conjecture, which if true would lead to the converse proof
for SDoF of blind MIMO wiretap channel with delayed CSIT.

**APPENDIX A**

**PROOF OF CLAIM 2**

Let us first consider Lemma 3 in [16]. Using the same
proof steps as in the proof of Lemma 3 one can show the
following extension of the lemma (using the same notation):
Let \( x_{L+N_1} = (x_1, \ldots, x_{L+N_1}) \) be entropy-symmetric such that
\( h(x_j : j \in J \} = h(x_k : k \in K) \} \) for any \( |J| = |K| \leq L \). Then, for any \( L \geq M \geq N \),

\[
M h(x_1^n | x_{L+1}, \ldots, x_{L+N_1}) \geq Nh(x_1^n | x_{L+1}, \ldots, x_{L+N_1}).
\]

In other words, if \( L \geq M \geq N \),

\[
\frac{1}{M} \left[ h(x_1^n | x_{L+1}, \ldots, x_{L+N_1}) - h(x_{L+1}, \ldots, x_{L+N_1}) \right] \leq \frac{1}{N} \left[ h(x_1^n | x_{L+1}, \ldots, x_{L+N_1}) - h(x_{L+1}, \ldots, x_{L+N_1}) \right].
\]

The same argument can be used for rank-symmetric vectors
(analogous to entropy-symmetric variables). In particular,

\[
\frac{1}{M - N_1} \left[ \text{rank} [G_{\text{max},1}^n | V^n \ U^n] \right] - \text{rank} [G_{\text{max},1}^n | V^n \ U^n] \leq \frac{1}{N_{\text{max}} - N_1} \left[ \text{rank} [G_{\text{max},1}^n | V^n \ U^n] \right] - \text{rank} [G_{\text{max},1}^n | V^n \ U^n].
\]

\[
\overset{a.s.}{\leq} \frac{1}{N_{\text{max}} - N_1} \left[ \text{rank} [G_{\text{max},1}^n | V^n \ U^n] \right] - \text{rank} [G_{\text{max},1}^n | V^n \ U^n]. \quad \text{(43)}
\]
By rewriting the above inequality we get
\[
(N_{\text{max}} - N_1) \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n ; G_{\text{max},3}^{n} | V^n U^n \right] \\
\leq (M - N_1) \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n \right] \\
- (M - N_{\text{max}}) \text{rank} \left[ G_{\text{max},1}^{n} | V^n U^n \right].
\]
(44)

Again, by rewriting the above inequality, we get
\[
(N_{\text{max}} - N_1)( \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n ; G_{\text{max},3}^{n} | V^n U^n \right] \\
- \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n \right]) \\
\leq (M - N_{\text{max}})( \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n \right] \\
- \text{rank} \left[ G_{\text{max},1}^{n} | V^n U^n \right]).
\]
(45)

Since the number of antennas corresponding to $G_{\text{max},3}^{n}$ and $G_{1,1}^{n}$ are equal, and since Tx has no CSIT with respect to channels comprising $G_{\text{max},3}^{n}$ and $G_{\text{max}}^{n}$ by using a variant of Lemma 2, we have
\[
\text{rank} \left[ G_{\text{max}}^{n} | V^n U^n ; G_{\text{max},3}^{n} | V^n U^n \right] \geq \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n ; G_{1,1}^{n} | V^n U^n \right].
\]
(46)

Therefore, by (45), (46),
\[
(N_{\text{max}} - N_1)( \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n ; G_{\text{max},3}^{n} | V^n U^n \right] \\
- \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n \right]) \\
\leq (M - N_{\text{max}})( \text{rank} \left[ G_{\text{max}}^{n} | V^n U^n \right] \\
- \text{rank} \left[ G_{\text{max},1}^{n} | V^n U^n \right]),
\]
and hence the desired result follows.

Acknowledgement

The authors would like to thank Dr. Ravi Tandon for his motivating discussions on this problem.

References

[1] S. Lashgari and A. S. Avestimehr, “Blind Wiretap Channel with Delayed CSIT,” Proc. of IEEE ISIT, 2014.
[2] A. D. Wyner, “The wire-tap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.
[3] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339–348, 1978.
[4] Y. Liang and H. V. Poor, “Information theoretic security,” Foundations and Trends in Communications and Information Theory, 2009.
[5] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” IEEE Transactions on Information Theory, vol. 24, no. 4, pp. 451–456, 1978.
[6] X. He and A. Yener, “MIMO wiretap channels with arbitrarily varying eavesdropper channel states,” arXiv preprint arXiv:1007.4801, 2010.
[7] A. Khisti and G. Wornell, “Secure transmission with multiple antennas I: The MISO/M wiretap channel,” IEEE Transactions on Information Theory, vol. 56, no. 7, pp. 3088–3104, 2010.
[8] A. Khisti and D. Zhang, “Artificial-noise alignment for secure multicast using multiple antennas,” arXiv preprint:1211.4649, 2012.
[9] J. Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks,” arXiv preprint, arXiv:1209.5370, 2012.
[10] J. Xie and S. Ulukus, “Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming,” arXiv preprint, arXiv:1302.6570, 2013.
[11] R. Tandon, S. Ulukus, and K. Ramchandran, “Secure source coding with a helper,” IEEE Transactions on Information Theory, 2012.
[12] G. Bagherikaram, A. Motahari, and A. Khandani, “On the secure Degrees-of-Freedom of the multiple-access-channel,” arXiv preprint arXiv:1003.0729, 2010.
[13] A. Zaidi, H. Awan, S. Shamai, and L. Vandendorpe, “Secure degrees of freedom of x-channel with output feedback and delayed csit,” in IEEE International Workshop on Information Theory, ITW, 2013.
[14] A. Zaidi, H. Awan, S. Shamai, and L. Vandendorpe, “Secure Degrees of Freedom of MIMO X-Channels With Output Feedback and Delayed CSIT,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1760–1774, 2013.
[15] A. Khisti, “Interference alignment for the multiantenna compound wiretap channel,” IEEE Transactions on Information Theory, vol. 57, no. 5, pp. 2976–2993, 2011.
[16] S. Y. et. al., “Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT,” Information Theory, IEEE Transactions on 59:9, 5244–5256, 2013.
[17] S. Lashgari, A. S. Avestimehr, and C. Suh, “Linear degrees of freedom of the X-channel with delayed CSIT,” IEEE Transactions on Information Theory, vol. 60, no. 4, pp. 2180–2189, 2014.
[18] S. Yang, P. Plantanida, M. Kobayashi, and S. Shamai, “On the secrecy degrees of freedom of multi-antenna wiretap channels with delayed csit,” in Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on Information Theory, pp. 2866–2870, IEEE, 2011.
[19] M. Kobayashi, P. Plantanida, S. Yang, and S. Shamai, “On the Secrecy Degrees of Freedom of the Multiantenna Block Fading Wiretap Channels,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 703–711, 2011.
[20] G. Bresler, D. Cartwright, and D. N. Tse, “Interference alignment for the MIMO interference channel,” arXiv:1303.5678, 2013.
[21] S. Lashgari, A. S. Avestimehr, and C. Suh, “A rank ratio inequality and the linear degrees of freedom of X-channel with delayed CSIT,” Allerton Conference on Communication, Control, and Computing, 2013.
[22] H. Federer, “Geometric Measure Theory,” Reprint of the 1969 Edition. Springer, 1996.