On the Secure Degrees of Freedom of the K-user Interference Channel with Delayed CSIT

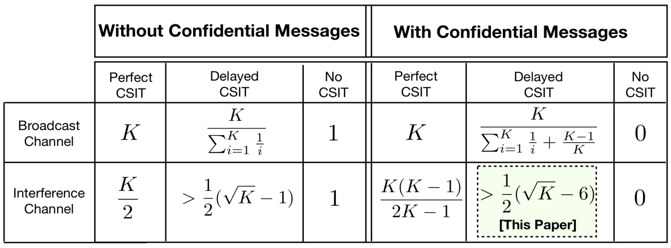
Mohamed Seif   Ravi Tandon   Ming Li
Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ, 85721
Email: $\{$*mseif, tandonr, lim*$\}$@email.arizona.edu

Abstract—**In this paper, the K-user interference channel with confidential messages is considered with delayed channel state information at transmitters (CSIT). We propose a novel secure transmission scheme in which the transmitters carefully mix information symbols with artificial noises to ensure confidentiality. Achieving confidentiality is challenging due to the delayed nature of CSIT, and the distributed nature of the transmitters. Our scheme works over two phases: phase one in which each transmitter sends information symbols mixed with artificial noises, and repeats such transmission over multiple rounds. In the next phase, each transmitter uses delayed CSIT of the previous phase and sends a function of the net interference and artificial noises (generated in previous phase), which is simultaneously useful for all receivers. These phases are designed to ensure the decodability of the desired messages while satisfying the confidentiality constraints. The proposed scheme achieves a sum secure degrees of freedom (SDoF) of at least $\frac{1}{2}(\sqrt{K}-6)$. To the best of our knowledge, this is the first result on the K-user interference channel with confidential messages and delayed CSIT that achieves a SDoF which scales with K.**

I. Introduction

Delayed CSIT can impact the spectral efficiency of wireless networks, and this problem has received significant recent attention. Maddah-Ali and Tse in [1] studied the K-user broadcast channel (BC) with delayed CSIT, and showed that the optimal sum degrees of freedom (DoF) is given by $K/(1+\frac{1}{2}+\cdots+\frac{1}{K})$ which is strictly greater than one DoF (with no CSIT) and less than K DoF (with perfect CSIT). Interference channels (IC) with delayed CSIT have been studied in several works such as [2], [3]. The main drawback of these schemes is that the achievable DoF *does not* scale with the number of users. In a recent work [4], a novel transmission scheme is presented which achieves $\frac{\lfloor\sqrt{K}\rfloor}{2}$ DoF for the K-user IC with delayed CSIT. The result in [4] is particularly interesting, as it shows that the sum DoF for the K-user IC *does* scale with the number of users, even with delayed CSIT.

Another important aspect in wireless networks is ensuring secure communication between transmitters and receivers. Many seminal works in the literature studied the secure capacity regions for multi-user settings such as wiretap, broadcast and interference channels (see comprehensive surveys [5]–[7]).



	Without Confidential Messages			With Confidential Messages		
	Perfect CSIT	Delayed CSIT	No CSIT	Perfect CSIT	Delayed CSIT	No CSIT
Broadcast Channel	K	$\frac{K}{\sum_{i=1}^{K}\frac{1}{i}}$	1	K	$\frac{K}{\sum_{i=1}^{K}\frac{1}{i}+\frac{K-1}{K}}$	0
Interference Channel	$\frac{K}{2}$	$>\frac{1}{2}(\sqrt{K}-1)$	1	$\frac{K(K-1)}{2K-1}$	$>\frac{1}{2}(\sqrt{K}-6)$ **[This Paper]**	0

Table 1: Summary of results on the K-user BC and IC with and without confidential messages.

Since the exact secure capacity regions for many multi-user networks are not known, secure degrees of freedom (SDoF) for a variety of models have been studied (e.g., [8], [9]). More specifically, for the K-user BC with confidential messages (CM), the authors in [9] showed that the optimal sum SDoF with delayed CSIT is given by $K/(1+\frac{1}{2}+\cdots+\frac{1}{K}+\frac{K-1}{K})$. The achievability scheme is based on a modification of the scheme in [1] along with a key generation method which uses delayed CSIT. For the K-user interference channel with confidential messages under perfect CSIT, Xie and Ulukus showed in [10] that the optimal sum SDoF is $\frac{K(K-1)}{2K-1}$. There are various other works for different CSIT assumptions, such as wiretap channel with no eavesdropper CSIT [11], and broadcast channel with alternating CSIT [12].

Contributions: In this work, we consider the K-user interference channel with confidential messages (IC-CM) and delayed CSIT. We focus on answering two fundamental questions: (a) are positive SDoF achievable for the IC with delayed CSIT?, and (b) if yes, then does the SDoF scale with K? We answer the above two questions in the affirmative by showing that positive SDoF are indeed achievable, and the achievable sum SDoF is at least $\frac{1}{2}(\sqrt{K}-6)$. This result highlights the fact that in presence of delayed CSIT, there is almost no DoF scaling loss due to confidentiality constraints compared to the no secrecy case [4]. Our transmission scheme is inspired by the work of [4] in terms of the organization of the transmission phases. One of the main differences is that the transmitters mix their information symbols with artificial noises so that the signals at each unintended receiver are completely immersed in the space spanned by artificial noise. However, this mixing must be done with only delayed CSIT, and it should also allow successful decoding at the respective receiver. The equivocation analysis of the proposed scheme is

The work of M. Seif and R. Tandon was supported by the U.S. NSF through grants CCF-1559758 and CNS-1715947. The work of M. Seif and M. Li was supported in part by the U.S. NSF grant CNS-1564477, and ONR YIP grant N00014-16-1-2650.

non-trivial due to the multi-phase nature of the scheme using delayed CSIT. Table 1 summarizes the main results for the BC and IC models under two scenarios: (a) without confidential messages, (b) with confidential messages, under three CSIT assumptions (perfect, delayed and no CSIT).

II. System Model

We consider the K-user interference channel with confidential messages and delayed CSIT (shown in Fig. 1). The input-output relationship at time slot t is

$$y_k(t) = h_{kk}(t)x_k(t) + \sum_{j=1, j\neq k}^{K} h_{kj}(t)x_j(t) + n_k(t), \quad (1)$$

where $y_k(t)$ is the signal received at receiver k at time t, $h_{kj}(t) \sim \mathcal{CN}(0,1)$ is the channel coefficient at time t between transmitter j and receiver k, and $x_k(t)$ is the transmitted signal from transmitter k at time t with an average power constraint $\mathbb{E}\{|x_k(t)|^2\} \leq P$. The additive noise $n_k(t) \sim \mathcal{CN}(0,1)$ at receiver k is also i.i.d. across users and time. The channel coefficients are assumed to be i.i.d. across time and users and we assume perfect CSI at all the receivers. We further assume that the CSIT is delayed, i.e., CSI is available at each transmitter after one time slot without error.

Let $R_k = \frac{\log_2(|\mathcal{W}_k|)}{n}$ denote the rate of message W_k intended for receiver k, where $|\mathcal{W}_k|$ is the cardinality of the kth message. A $(2^{nR_1}, 2^{nR_2}, \ldots, 2^{nR_K}, n)$ code is described by the set of encoding and decoding functions as follows: the set of encoders at the transmitters are given as: $\{\psi_t^{(k)} : W_k \times \{H(t')\}_{t'=1}^{t-1} \to x_k(t)\}_{t=1}^{n}, \forall k = 1, \ldots, K$, where the message W_k is uniformly distributed over the set $\mathcal{W}_k$, and $H(t') \triangleq \{h_{kj}(t')\}_{k=1,j=1}^{K}$ is the set of all channel gains at time t'. The transmitted signal from transmitter k at time slot t is given as: $x_k(t) = \psi_t(W_k, \{H(t')\}_{t'=1}^{t-1})$. The decoding function at receiver k is given by the following mapping: $\phi^{(k)} : y_k^{(n)} \times \{H(t)\}_{t=1}^{n} \to W_k$, and the estimate of the message at receiver k is defined as: $\hat{W}_k = \phi^{(k)}(\{y_k(t), H(t)\}_{t=1}^{n})$. The rate tuple $(R_1, \ldots, R_K)$ is achievable if there exists a sequence of codes which satisfy the decodability constraints at the receivers and the confidentiality constraints, i.e.,

$$\lim_{n\to\infty} \sup \text{Prob}\left[\hat{W}_k \neq W_k\right] \leq \epsilon_n, \forall k = 1, \ldots, K, \quad (2)$$

$$\lim_{n\to\infty} \sup \frac{1}{n} I\left(W_{-k}^{K}; y_k^{(n)} | W_k, \Omega\right) \leq \epsilon_n, \forall k = 1, \ldots, K, \quad (3)$$

where $\epsilon_n \to 0$ as $n \to 0$, $W_{-k}^{K} \triangleq \{W_1, W_2, \ldots, W_K\} \backslash \{W_k\}$, and $\Omega \triangleq \{H(t)\}_{t=1}^{n}$ is the set of all channel gains over the channel uses. The supremum of the achievable sum rate, $R_s \triangleq \sum_{k=1}^{K} R_k$, is defined as the secrecy sum capacity C_s. The optimal secure degrees of freedom (SDoF) is defined as:

$$\text{SDoF}_{\text{sum}}^{*} \triangleq \lim_{P\to\infty} \frac{C_S}{\log(P)}. \quad (4)$$

In the next section, we present our main results on sum SDoF with confidential messages and delayed CSIT.

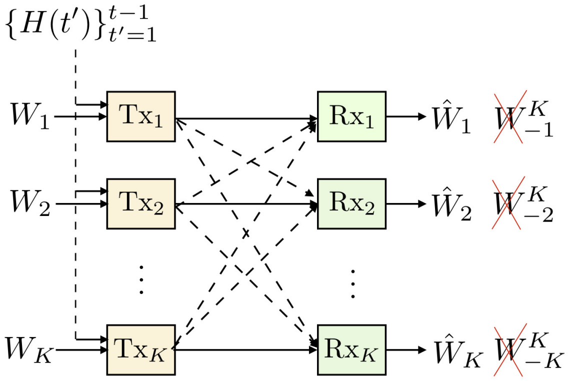


Fig. 1: K-user interference channel with confidential messages and delayed CSIT.

III. Main Results and Discussions

Theorem 1: For the K-user interference channel with confidential messages and delayed CSIT, the following secure sum degrees of freedom is achievable:

$$\text{SDoF}_{\text{sum}}^{\text{ach.}} = \frac{KR(K - R - 2)}{(K - 1) \times [R(R + 1) + K]}, \quad (5)$$

where,

$$R = \left\lfloor \frac{-K + K \times \sqrt{1 + \frac{(K-1)(K-2)}{K}}}{K - 1} \right\rfloor. \quad (6)$$

In the next Corollary, we simplify the above expression and present a lower bound on the $\text{SDoF}_{\text{sum}}^{\text{ach.}}$. Complete proofs of all the results are given in the full version of the paper in [13].

Corollary 1: For the K-user IC-CM with delayed CSIT , the achievable SDoF in (5) is lower bounded as

$$\text{SDoF}_{\text{sum}}^{\text{ach.}} > \frac{1}{2}(\sqrt{K} - 6). \quad (7)$$

Remark 1: We next compare the secure sum DoF of Theorem 1 to that of [4] (i.e., without confidential messages). For the K-user interference channel without secrecy constraints, the achievable sum DoF in [4] is given as:

$$\text{DoF}_{\text{sum}}^{\text{ach.}} \geq \frac{\lfloor\sqrt{K}\rfloor}{2} > \frac{1}{2}(\sqrt{K} - 1). \quad (8)$$

Comparing this result with (7), we can conclude that the scaling behavior of the sum SDoF is still attainable and there is almost no scaling loss in the sum SDoF compared to the no secrecy case, especially as K becomes large.

IV. Proof of Theorem 1

In this Section, we present the main steps behind the proof of Theorem 1 (for full details, we refer the reader to [13]).

A. *Achievability scheme:*

In this subsection, we present our secure transmission scheme. We consider a transmission block of length $RT + K(n+1)^N = R(Rn^N + (n+1)^N) + K(n+1)^N$, where R denotes the number of transmission rounds and $N = RK(K-1)$, and n is an integer. The transmission scheme works over two phases. The goal of each transmitter is to

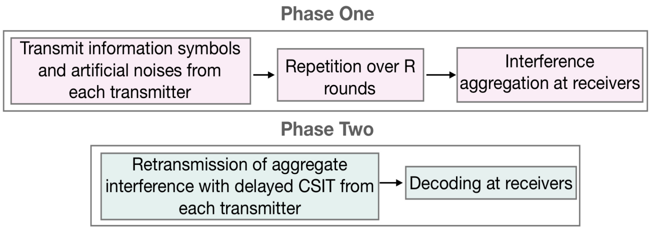

Phase One
Transmit information symbols and artificial noises from each transmitter
Repetition over R rounds
Interference aggregation at receivers
Phase Two
Retransmission of aggregate interference with delayed CSIT from each transmitter
Decoding at receivers

Fig. 2: Summary of two-phase transmission scheme.

securely send $T_1 = Rn^n + (n+1)^N - \lceil \frac{RT+(K-1)(n+1)^N}{K-1} \rceil$ information symbols to its corresponding receiver. In the first phase, each transmitter sends random linear combinations of the T_1 information symbols and the $T_2 = \lceil \frac{RT+(K-1)(n+1)^N}{K-1} \rceil$ artificial noise symbols in T time slots. Each transmitter repeats such transmission for R rounds, and hence, phase one spans RT time slots. By the end of phase one, each receiver applies local interference alignment on its signals to reduce the dimension of the aggregate interference. In the second phase, each transmitter knows the channel coefficients of phase one due to delayed CSIT. Subsequently, each transmitter sends a function of the net interference and artificial noises (generated in previous phase) which is simultaneously useful to all receivers. More specifically, each transmitter seperately sends $(n+1)^N$ linear equations of the past interference to all receivers. Therefore, phase 2 spans $K(n+1)^N$ time slots. By the end of both phases, each receiver is able to decode its desired T_1 information symbols while satisfying the confidentiality constraints. Therefore, the transmission scheme spans $RT + K(n+1)^N$ time slots. We next calculate the achievable sum SDoF of this scheme as follows:

$$\begin{aligned}
\text{SDoF}_{\text{sum}}^{\text{ach.}} &= \lim_{n\to\infty} \frac{KT_1}{R(Rn^N + (n+1)^N) + K(n+1)^N}, \\
&\overset{(a)}{>} \lim_{n\to\infty} \frac{K\left[Rn^n + (n+1)^N \times (\frac{K-R-1}{K-1}) - (n+1)^N - 1\right]}{R(Rn^N + (n+1)^N) + K(n+1)^N}, \\
&\overset{(b)}{=} \frac{KR(K-R-2)}{(K-1)\times[R(R+1)+K]}, \qquad (9)
\end{aligned}$$

where in (a), we substituted the value of T_1 and used the property that $\lceil x \rceil < x+1$, and (b) follows by taking the limit $n \to \infty$. Before we present the details of the scheme, we first optimize the achievable SDoF with respect to the number of rounds R and also simplify the above expression, which leads to the expression in Corollary 1.

Lemma 1: The optimal R^* which maximizes (9) is given by

$$R^* = \left\lfloor \frac{-K + K \times \sqrt{1 + \frac{(K-1)(K-2)}{K}}}{K-1} \right\rfloor. \qquad (10)$$

See [13] for proof of Lemma 1. Fig. 2 depicts an overview of the two transmission phases.

We now present the transmission scheme in full detail. For our scheme, we collectively denote the L symbols transmitted over L time slots as a super symbol and call this as the L symbol extension of the channel. For the extended channel, the signal at receiver k is given as

$$\mathbf{y}_k = \sum_{j=1}^{K} \mathbf{H}_{kj}\mathbf{x}_j + \mathbf{n}_k, \qquad (11)$$

where $\mathbf{x}_k$ is a $L \times 1$ column vector representing the L symbols transmitted by transmitter k in L time slots. $\mathbf{H}_{kj}$ is a $L \times L$ diagonal matrix representing the L symbol extension of the channel as follows: $\mathbf{H}_{kj} = \text{diag}(h_{kj}(1), h_{kj}(2), \dots, h_{kj}(L))$. Now we proceed to the description of the proposed scheme.

<u>Phase 1</u>– Interference creation with information symbols and artificial noises

Recall that the goal of each transmitter is to send T_1 information symbols securely to its respective receiver. This phase is comprised of R rounds, where, in each round, every transmitter j sends linear combinations of the T_1 information symbols $\mathbf{s}_j \in \mathbb{C}^{T_1 \times 1}$, mixed with T_2 artificial noises $\mathbf{u}_j \in \mathbb{C}^{T_2 \times 1}$, where the elements of $\mathbf{u}_j$ are drawn from complex-Gaussian distribution with average power P. Hence, the signal sent by transmitter j in each round r can be written as

$$\mathbf{x}_j = \mathbf{V}_j \begin{bmatrix} \mathbf{s}_j \\ \mathbf{u}_j \end{bmatrix}, \ \forall j = 1, 2, \dots, K, \qquad (12)$$

where $\mathbf{V}_j, \forall j = 1, 2, \dots, K$ is a random *mixing* matrix of dimension $T \times T$ whose elements are i.i.d. drawn from complex-Gaussian distribution with zero mean and unit variance at transmitter j. The matrix $\mathbf{V}_j, \forall j = 1, 2, \dots, K$ is known at all the terminals. The received signal at receiver k for round $r \in \{1, 2, \dots, R\}$ is given by

$$\mathbf{y}_k^r = \sum_{j=1}^{K} \mathbf{H}_{kj}^r \mathbf{x}_j + \mathbf{n}_k^r. \qquad (13)$$

Hence, phase one spans RT time slots.

Interference aggregation at receivers

At the end of phase one, each receiver k has the signals $\mathbf{y}_k = \{\mathbf{y}_k^r\}_{r=1}^R$, over R rounds. Each receiver performs a linear post-processing of its received signals in order to align the aggregate interference (generated from symbols and artificial noises) from the $(K-1)$ unintended transmitters. In particular, each receiver multiplies its received signals in the rth block with a matrix $\mathbf{W}$ (of dimension $T \times n^N$) as follows:

$$\begin{aligned}
\tilde{\mathbf{y}}_k^r = \mathbf{W}^H \mathbf{y}_k^r &= \mathbf{W}^H \Big(\sum_{j=1}^{K} \mathbf{H}_{kj}^r \mathbf{x}_j + \mathbf{n}_k^r \Big), \qquad (14) \\
&= \mathbf{W}^H \mathbf{H}_{kk}^r \mathbf{x}_k + \sum_{j\neq k} \mathbf{W}^H \mathbf{H}_{kj}^r \mathbf{x}_j + \mathbf{W}^H \mathbf{n}_k^r. \qquad (15)
\end{aligned}$$

The goal is to design the matrix $\mathbf{W}$ and a matrix $\mathbf{X}$, so that

$$\mathbf{W}^H \mathbf{H}_{kj}^r \prec \mathbf{X}, \ \forall k = 1, \dots, K, k \neq j, \forall r = 1, \dots, R, \quad (16)$$

where $\mathbf{X} \in \mathbb{C}^{(n+1)^N \times T}$. Here the notation $\mathbf{A} \prec \mathbf{B}$ means that the set of row vectors of matrix $\mathbf{A}$ is a subset of row vectors of $\mathbf{B}$. To this end, we choose $\mathbf{W}$ and $\mathbf{X}$ as follows:

$$\mathbf{W} = \left[\prod_{(r,m,i)\in\mathcal{S}} (\mathbf{H}_{mi}^{r^{(n_{mi}^r)}})^H \mathbb{1} : 0 \leq n_{mi}^r \leq n-1 \right], \quad (17)$$

$$\mathbf{X} = \left[\prod_{(r,m,i)\in\mathcal{S}} (\mathbf{H}_{mi}^{r^{(n_{mi}^r)}})^H \mathbb{1} : 0 \leq n_{mi}^r \leq n \right]^H, \quad (18)$$

where $\mathbb{1}$ is the all ones column vector and the set $\mathcal{S} = \{(r,m,i) : \forall r \in \{1,\ldots,R\}, \forall m \neq i \in \{1,\ldots,K\}\}$. Note that the set $\mathcal{S}$ does not contain the channel matrix $\mathbf{H}_{kk}^r$ that carries the information symbols intended to receiver k. However, multiplying with any channel gain that appears in $\mathbf{W}$ results in aligning this signal within the matrix $\mathbf{X}$ asymptotically. It is worth noting that, the matrix $\mathbf{X}$ defines all the possible interference generated by the transmitters at all receivers. Hence, this choice of $\mathbf{X}$ and $\mathbf{W}$ guarantees that the alignment condition (16) is satisfied. Therefore, the processed signal in round r at receiver k can be written as

$$\tilde{\mathbf{y}}_k^r = \mathbf{W}^H \mathbf{H}_{kk}^r \mathbf{x}_k + \sum_{j\neq k} \mathbf{W}^H \mathbf{H}_{kj}^r \mathbf{x}_j + \mathbf{W}^H \mathbf{n}_k^r, \quad (19)$$

$$= \mathbf{W}^H \mathbf{H}_{kk}^r \mathbf{x}_k + \sum_{j\neq k} \Pi_{kj}^r \mathbf{X} \mathbf{x}_j + \mathbf{W}^H \mathbf{n}_k^r, \quad (20)$$

where $\Pi_{kj}^r \in \mathbb{C}^{n^N \times (n+1)^N}$ is a selection and permutation matrix. After phase 1, receiver k has Rn^N equations of T desired symbols (composed of T_1 information symbols and T_2 artificial noises generated by the transmitter k) plus $(K-1)$ interference terms, which are of dimension $(n+1)^N$.

<u>Phase 2</u>*– Re-transmission of aggregate interference with delayed CSIT*

For the second phase, each transmitter k uses $(n+1)^N$ time slots to re-transmit the aggregated interference $(\mathbf{X}\mathbf{x}_k)$ generated in the first phase at the receivers, which is sufficient to cancel out the interference term at receiver $j \neq k$, and to provide additional $(n+1)^N$ equations of the desired symbols to receiver k. Hence, this phase spans $K(n+1)^N$ time slots. The transmitted signal from transmitter k is as follows:

$$\mathbf{z}_k = \mathbf{X}\ \mathbf{x}_k, \forall k = 1, 2, \ldots, K. \quad (21)$$

Decoding at receivers:

At the end of phase 2, the interference at receiver k can be removed by subtracting the terms $\sum_{j=1,j\neq k} \Pi_{kj}^r \mathbf{X}\ \mathbf{x}_j$ from the equalized signal $\tilde{\mathbf{y}}_k^r$, i.e., (ignoring the additive noise $\mathbf{n}_k^r$)

$$\mathbf{W}^H \mathbf{H}_{kk}^r \mathbf{x}_k = \tilde{\mathbf{y}}_k^r - \sum_{j=1,j\neq k} \Pi_{kj}^r \mathbf{X}\ \mathbf{x}_j. \quad (22)$$

Canceling the interference terms leaves each receiver $k, \forall k \in \{1,\ldots,K\}$ with Rn^N useful linear equations in addition to the $(n+1)^N$ useful equations from transmitter k (from phase 2). At the end of phase 2, receiver k will collectively obtain the following signal,

$$\underbrace{\left[\mathbf{X}^H, (\mathbf{W}^H \mathbf{H}_{kk}^1)^H, \ldots, (\mathbf{W}^H \mathbf{H}_{kk}^R)^H\right]^H}_{\mathbf{B}_k} \mathbf{V}_k \begin{bmatrix} \mathbf{s}_k \\ \mathbf{u}_k \end{bmatrix}. \quad (23)$$

Therefore, at the end of phase 2, each receiver has enough linear equations of the desired symbols. To ensure decodability, we need to prove that the matrix $\mathbf{B}_k \mathbf{V}_k$ is full rank and hence each receiver will be able to decode its desired T_1 information symbols. First, we notice that $\mathbf{V}_k$ is full rank matrix and hence $\text{rank}(\mathbf{B}_k \mathbf{V}_k) = \text{rank}(\mathbf{B}_k)$. In [13], it is shown that the matrix $\mathbf{B}_k$ is full rank which in turn ensures decodability.

B. Equivocation Analysis

We next present the equivocation analysis of the scheme. The parameters T_1 (number of information symbols) and T_2 (number of artificial noises) are chosen carefully so that the confidentiality constraints are satisfied as we prove next.

Lemma 2: For the proposed transmission scheme, the confidentiality constraints are satisfied at each receiver, i.e.,

$$I(\{\mathbf{s}_j\}_{j=1,j\neq i}^K; \mathbf{y}_i | \Omega) = o(\log(P)), \forall i = 1, 2, \ldots, K, \quad (24)$$

where $o(\log(P))$ *represents a funtion of* P *such that* $\lim_{P\to\infty} o(\log(P))/\log(P) = 0$. *This means that the mutual information between the un-intended data symbols and the received signal at receiver* i *is within* $o(\log(P))$.

Without loss of generality, let us consider the first receiver. We bound the mutual information between the unintended information symbols of transmitters $2,\ldots,K$ and the signal seen at receiver 1 given the knowledge of the channel coefficients Ω, as follows:

$$\begin{aligned} I(\mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K; \mathbf{y}_1 | \Omega) &\leq I(\mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K; \mathbf{y}_1, \mathbf{s}_1, \mathbf{u}_1 | \Omega), \\ &\overset{(a)}{=} I(\mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K; \mathbf{y}_1 | \Omega, \mathbf{s}_1, \mathbf{u}_1), \\ &\overset{(b)}{=} I(\mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K; \bar{\mathbf{y}}_1 | \Omega), \end{aligned} \quad (25)$$

where in (a), the term $I(\mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K; \mathbf{s}_1, \mathbf{u}_1 | \Omega)$ equals zero since the information symbols $\mathbf{s}_1$ and artificial noise symbols $\mathbf{u}_1$ are independent of the information symbols $\{\mathbf{s}_j\}_{j=2}^K$. In (b), $\bar{\mathbf{y}}_1$ is the effective remaining signal at receiver 1 after removing the contributions of $(\mathbf{s}_1, \mathbf{u}_1)$. We compactly write the signal $\bar{\mathbf{y}}_1$ at receiver 1 over $RT + (K-1)(n+1)^N$ time slots as follows:

$$\bar{\mathbf{y}}_1 = \mathbf{A}_1 \mathbf{V} \mathbf{q} + \mathbf{n}_1, \quad (26)$$

where the matrix $\mathbf{A}_1$ is written as a vertical concatenation of matrices $\mathbf{C}$ and $\mathbf{D}$, corresponding to the two transmission phases as follows:

$$\mathbf{A}_1 = \left[\begin{array}{c} \mathbf{C} \\ \hline \mathbf{D} \end{array}\right], \ \mathbf{C} = \begin{bmatrix} \mathbf{H}_{12}^1 & \mathbf{H}_{13}^1 & \cdots & \mathbf{H}_{1K}^1 \\ \mathbf{H}_{12}^2 & \mathbf{H}_{13}^2 & \cdots & \mathbf{H}_{1K}^2 \\ \vdots & \vdots & \ldots & \vdots \\ \mathbf{H}_{12}^R & \mathbf{H}_{13}^R & \cdots & \mathbf{H}_{1K}^R \end{bmatrix},$$

$$\mathbf{D} = \text{blkdiag}(\tilde{\mathbf{H}}_{12}\mathbf{X}, \ldots, \tilde{\mathbf{H}}_{1K}\mathbf{X}). \quad (27)$$

The matrix $\mathbf{C}$ (of dimensions $RT \times (K-1)T$) corresponds to phase one, whose elements are i.i.d., and drawn from a continuous distribution and hence, it is full rank almost surely (i.e., $\text{rank}(C) = RT$). The matrix $\mathbf{D}$ has a block diagonal structure (each block matrix has dimensions of $(n+1)^N \times T$) since the transmission in phase two is done in TDMA fashion. Furthermore, each block is a full rank matrix (i.e., $\text{rank}(\tilde{\mathbf{H}}_{1j}\mathbf{X}) = \text{rank}(\mathbf{X}) = (n+1)^N, \forall j = 2, \ldots, K$) [13]. Hence, the matrix $\mathbf{A}_1$ has dimensions $(RT + (K-1)(n+1)^N) \times (K-1)T = (K-1)T_2 \times (K-1)T$ (see [13]). The matrix $\mathbf{V}$ in (26) is defined as $\mathbf{V} = \text{blkdiag}(\mathbf{V}_2, \mathbf{V}_3, \ldots, \mathbf{V}_K)$, which is a block diagonal matrix of dimensions $(K-1)T \times (K-1)T$, comprised of the $(K-1)$ mixing matrices used by the $(K-1)$ transmitters. Furthermore, we write $\mathbf{q} = \begin{bmatrix} \mathbf{s}_2^T & \mathbf{u}_2^T & \mathbf{s}_3^T & \mathbf{u}_3^T & \cdots & \mathbf{s}_K^T & \mathbf{u}_K^T \end{bmatrix}^T$, as a column vector of length $(K-1)T$, which contains the information symbols and the artificial noises sent by transmitters $2, \ldots, K$.

Starting from (25), and (26), our goal is to show that $I(\mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K; \bar{\mathbf{y}}_1 | \Omega) \leq o(\log(P))$. Before we proceed, we state two Lemmas which are proved in [13].

Lemma 3: Let $\mathbf{A}$ *be a matrix with dimension* $M \times N$ *and* $\mathbf{X} = (x_1, \ldots, x_N)^T$ *be a zero-mean jointly Gaussian random vector with covariance matrix* $P\mathbf{I}$*. Also, let* $\mathbf{N} = (n_1, \ldots, n_M)^T$ *be a zero-mean jointly Gaussian random vector with covariance matrix* $\sigma^2\mathbf{I}$*, independent of* $\mathbf{X}$, then

$$h(\mathbf{AX} + \mathbf{N}) = \text{rank}(\mathbf{A}) \log(P) + o(\log(P)). \tag{28}$$

Lemma 4: Consider two matrices $\mathbf{A}_{M \times N}$ *and* $\mathbf{B}_{N \times M}$ *where* $M \leq N$*. The elements of matrix* $\mathbf{B}$ *are chosen independently from the entries of* $\mathbf{A}$ *at random from a continuous distribution. Then, rank*$(\mathbf{AB})$ = *rank*$(\mathbf{A})$ *almost surely.*

Use the definitions in (26), we now bound (25) as follows

$$\begin{aligned}
& I(\mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K; \mathbf{y}_1 | \Omega) \leq I(\mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K; \bar{\mathbf{y}}_1 | \Omega), \\
& = h(\bar{\mathbf{y}}_1 | \Omega) - h(\bar{\mathbf{y}}_1 | \mathbf{s}_2, \mathbf{s}_3, \ldots, \mathbf{s}_K, \Omega), \\
& \overset{(a)}{=} h(\mathbf{A}_1 \mathbf{V} \mathbf{q} + \mathbf{n}_1) - h(\mathbf{A}_1 \tilde{\mathbf{V}} \tilde{\mathbf{q}} + \mathbf{n}_1), \\
& \overset{(b)}{=} \Big(\text{rank}(\mathbf{A}_1 \mathbf{V}) - \text{rank}(\mathbf{A}_1 \tilde{\mathbf{V}})\Big) \log(P) + o(\log(P)), \\
& \overset{(c)}{=} \Big(\text{rank}(\mathbf{A}_1) - \text{rank}(\mathbf{A}_1 \tilde{\mathbf{V}})\Big) \log(P) + o(\log(P)), \\
& \overset{(d)}{=} o(\log(P)),
\end{aligned} \tag{29}$$

where in (a), we defined $\tilde{\mathbf{q}} = \begin{bmatrix} \mathbf{u}_2^T & \mathbf{u}_3^T & \cdots & \mathbf{u}_K^T \end{bmatrix}^T$ as the column vector of length $(K-1)T_2$, containing the artificial noises of transmitters $2, \ldots, K$, and $\tilde{\mathbf{V}} = \text{blkdiag}(\mathbf{V}_{2,u}, \mathbf{V}_{3,u}, \ldots, \mathbf{V}_{K,u})$, which is a block diagonal matrix of dimensions $(K-1)T \times (K-1)T_2$, where each $\mathbf{V}_{i,u}$ (of size $T \times T_2$) is a sub-matrix of $\mathbf{V}_i$ corresponding to the artificial noises. In step (b), we invoke Lemma 3 to express the differential entropy terms in terms of rank(s) $\text{rank}(\mathbf{A}_1\mathbf{V})$ and $\text{rank}(\mathbf{A}_1\tilde{\mathbf{V}})$, and in step (c), we used the fact that since $\mathbf{V}$ is a random square (invertible) matrix, generated independently from the entries of $\mathbf{A}_1$, hence $\text{rank}(\mathbf{A}_1\mathbf{V}) = \text{rank}(\mathbf{A}_1)$ almost surely. Finally, for step (d), we invoke Lemma 4, which allows us to claim that $\text{rank}(\mathbf{A}_1\tilde{\mathbf{V}}) = \text{rank}(\mathbf{A}_1)$ almost surely. The step (d) is perhaps the most critical step in the equivocation analysis, and central to the choice of parameters of the scheme. In particular, to ensure that $\text{rank}(\mathbf{A}_1\tilde{\mathbf{V}}) = \text{rank}(\mathbf{A}_1)$, where $\tilde{\mathbf{V}}$ is a non-square random matrix, we must satisfy $RT + (K-1)(n+1)^N \leq (K-1)T_2$. The value for T_2 (number of artificial noise symbols) is therefore chosen to satisfy the above bound with equality, giving the intuition behind its choice. Hence, from (29), we arrive at the proof of Lemma 2, showing that the scheme satisfies confidentiality constraints, and completing the proof of Theorem 1.

V. Conclusion

In this paper, we studied the K-user interference channel with confidential messages and delayed CSIT. We showed that the sum secure degrees of freedom (SDoF) is at least $\frac{1}{2}(\sqrt{K} - 6)$, which scales with the number of users. To achieve this result, we have proposed a novel secure transmission scheme which satisfies both confidentiality and decodability constraints at receivers. To the best of our knowledge, this is the first result showing scaling of SDoF for the interference channel with confidential messages and delayed CSIT. An interesting open problem is to obtain upper bounds on SDoF with delayed CSIT.

References

[1] M. A. Maddah-Ali and D. Tse, "Completely stale transmitter channel state information is still very useful," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4418–4431, Apr. 2012.

[2] M. J. Abdoli, A. Ghasemi, and A. K. Khandani, "On the degrees of freedom of K-user SISO interference and X channels with delayed CSIT," *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6542–6561, Jun. 2013.

[3] H. Maleki, S. A. Jafar, and S. Shamai, "Retrospective interference alignment over interference networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 3, pp. 228–240, Dec. 2012.

[4] D. Castanheira, A. Silva, and A. Gameiro, "Retrospective interference alignment: Degrees of freedom scaling with distributed transmitters," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1721–1730, Jan. 2017.

[5] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Sep. 2015.

[6] P. Mukherjee, R. Tandon, and S. Ulukus, *Physical layer security with delayed, hybrid and alternating channel state knowledge, information theoretic security and privacy of information sources*. Eds., Cambridge Univ. Press, to appear, 2016.

[7] Y. Liang, H. V. Poor, S. Shamai *et al.*, "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, Jun. 2009.

[8] X. He and A. Yener, "K-user interference channels: Achievable secrecy rate and degrees of freedom," in *IEEE Information Theory Workshop (ITW) on Networking and Information Theory*, Jul. 2009, pp. 336–340.

[9] S. Yang and M. Kobayashi, "Secure communication in K-user multi-antenna broadcast channel with state feedback," in *IEEE International Symposium on Information Theory (ISIT)*, Oct. 2015, pp. 1976–1980.

[10] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2647–2661, Mar. 2015.

[11] P. Mukherjee and S. Ulukus, "Secrecy in MIMO networks with no eavesdropper CSIT," *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4382–4391, May 2017.

[12] P. Mukherjee, J. Xie, and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1898–1922, Oct. 2017.

[13] M. Seif, R. Tandon, and M. Li, "Secure retrospective interference alignment," *e-print arXiv: 1801.03494*, Jan. 2018.