On the Effect of Colluding Eavesdroppers on Secrecy Scaling

O. Ozan Koyluoglu, C. Emre Koksal, and Hesham El Gamal
Department of Electrical and Computer Engineering
The Ohio State University, Columbus, Ohio
Email: {koyluogo,koksal,helgamal}@ece.osu.edu

***Abstract*—In a powerful secrecy attack, eavesdroppers can *collude*, i.e., they can share their observations. Securing information in such a scenario will be an even more challenging task compared to non-colluding case. We here analyze the effect of eavesdropper collusion on the achievable performance in both the path loss and ergodic multi-path fading models. We provide two results: 1) If the legitimate nodes have unit intensity ($\lambda = 1$) and the colluding eavesdroppers have an intensity of $\lambda_e = O\left((\log n)^{-2(1+p)}\right)$ for any $p > 0$ in a random extended network, almost all of the nodes can achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$; and 2) In the K-user Gaussian interference channel with K_e external colluding eavesdroppers, a secure degrees of freedom (DoF) of $\eta = \left[\frac{1}{2} - \frac{K_e}{K}\right]^+$ per frequency-time slot is achievable for each user in the ergodic setting (in the absence of the eavesdropper CSI).**

I. Introduction

Due to the broadcast nature of wireless medium, transmissions are susceptible to eavesdropping and secrecy of the transmission arises as another quality of service (QoS) constraint. Therefore, users in a wireless network need to take some precaution to achieve a desired secrecy level.

For the path loss model, secrecy capacity scaling in an extended network is recently studied in [1]. In that model, the legitimate and eavesdropper nodes are assumed to be placed according to Poisson point processes in a square region of area n. It is shown that, when the legitimate nodes have unit intensity, $\lambda = 1$, and the eavesdroppers have an intensity of $\lambda_e = O\left((\log n)^{-2}\right)$, almost all of the nodes achieve a perfectly secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$. The frequency/time selective scenario is studied in [2], where the authors show how the interference alignment technique can be utilized to achieve secrecy in frequency selective channels. For the K-user Gaussian interference channel with an external eavesdropper, a secure DoF of $\eta = \frac{1}{2} - \frac{1}{K}$ per frequency-time slot is shown to be achievable for each user in the ergodic setting (in the absence of the eavesdropper CSI).

In a more powerful attack, eavesdroppers can *collude*, i.e., they can share their observations. Securing information in such a scenario will be an even more challenging task compared to non-colluding case. We here analyze the effect of eavesdropper collusion on the achievable performance in both the path loss and multi-path fading models.

II. Path Loss Model

The set of legitimate nodes is denoted by $\mathcal{L}$, whereas the set of eavesdroppers is represented by $\mathcal{E}$. During time slot t, the set of transmitting nodes are denoted by $\mathcal{T}(t) \subset \mathcal{L}$, where each transmitting user $i \in \mathcal{T}(t)$ transmits the signal $X_i(t)$. The received signals at listening node $j \in \mathcal{L} - \mathcal{T}(t)$ and at eavesdropper $e \in \mathcal{E}$ are denoted by $Y_j(t)$ and $Y_e(t)$, respectively:

$$\begin{aligned} Y_j(t) &= \sum_{i \in \mathcal{T}(t)} \sqrt{d_{i,j}^{-\alpha}} X_i(t) + N_j(t) \\ Y_e(t) &= \sum_{i \in \mathcal{T}(t)} \sqrt{d_{i,e}^{-\alpha}} X_i(t) + N_e(t), \end{aligned}$$

where $N_j(t)$ and $N_e(t)$ are i.i.d. $\mathcal{N}(0, N_0)$ noise samples at the legitimate node j and at the eavesdropper e, respectively, d_{ij} represents the distance between nodes i and j and $\alpha > 2$ is the path loss exponent. Finally, the set of all observations at eavesdropper e is denoted by $\mathbf{Y}_e$, and we define $\mathbf{Y}_\mathcal{E} = \{\mathbf{Y}_e, \forall e \in \mathcal{E}\}$. In the multi-hop strategy, each transmission consists of N channel uses. We denote the observations at the eavesdroppers corresponding to hop h as $\mathbf{Y}_\mathcal{E}(h)$.

Now, consider any random source-destination pair, where the source s wishes to transmit the message $w_{s,d}$ securely to the intended destination d. We say that the secret rate of R is achievable for almost all the source-destination pairs, (s, d) if

- The error probability of decoding the intended message at the intended receiver can be made arbitrarily small as $N \to \infty$.
- The information leakage rate associated with the transmissions of the message over the entire path, i.e., $\frac{I(W_{s,d}; \mathbf{Y}_\mathcal{E})}{N}$, can be made arbitrarily small as $N \to \infty$.

If there are only H hops carrying the message $w_{s,d}$, one only needs to consider the associated channel observations at the eavesdroppers when evaluating our security constraint. Hence, our second condition is satisfied if $\frac{I(W_{s,d}; \mathbf{Y}_\mathcal{E}(1), \cdots, \mathbf{Y}_\mathcal{E}(H))}{N}$ can be made arbitrarily small for sufficiently large block lengths.

A. Analysis

The achievable scheme is based on highways, a set of nodes crossing the network area horizontally and vertically that carry the messages of sources to destinations. Using the approach

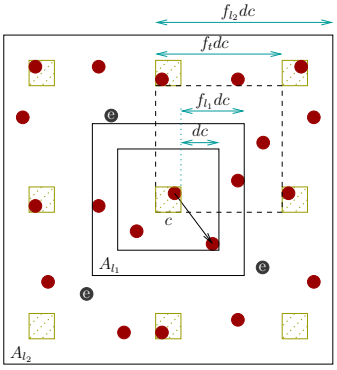

Fig. 1. The time division approach is represented by denoting the squares that are allowed for transmission. It is evident from the dotted square that the time division requires $(f_t\, d)^2$ time slots. The transmitter located at the center of the figure wishes to communicate with a receiver that is d squares away. The second square surrounding the transmitter is the first secrecy zone level, which is the region of points that are at most $f_{l_1}\ d$ squares away from the transmitter. Side length of each square is denoted by c.

of [1], we divide the achievability argument into the following four (modified) key steps:

1) Lemma 1 uses the idea of **secrecy zones** to guarantee the secrecy of the communication over a single hop.
2) In Lemma 2, we show that the multi-hop forwarding strategy, which injects independent randomization signal in each hop, allows for hiding the information from colluding eavesdroppers which listen to the transmissions over **all** hops.
3) We characterize the rate assigned to each node on the highway in Lemma 4.
4) The accessibility of highways for **almost** all the nodes in the networks with the appropriate rates is established in Lemma 5.

The main result is then proved by combining the aforementioned steps with a multi-hop routing scheme.

We partition the network area into squares of constant side length c. We further divide the area into larger squares of side $f_t dc$, each of which contains $(f_t d)^2$ small squares. These small squares take turn over a Time-Division-Multiple-Access (TDMA) frame of size $(f_t d)^2$ slots. In each slot, a transmitter within a small square can transmit to a receiver that is located at most d squares away as illustrated in Fig. 1. On the same figure, we also show the *secrecy zones*, around a transmitting square: Secrecy zone of level k has an area of A_{l_k} (the distance is denoted with $f_{l_k} dc$). Note that, we take f_{l_k} as a design parameter. We will choose f_{l_k} differently, depending on whether a node is forwarding data over a highway or accessing/accessed by a highway. Furthermore, $d, f_{l,k}$ and f_t all depend on the number, n, of nodes.

Our first result establishes an achievable *secure* rate per *a single hop*, active over N channel uses, under the assumption of eavesdroppers on the boundary of *each* secrecy zone level.

Lemma 1 (Secure Rate per Hop): In a communication scenario depicted in Fig. 1 (no eavesdroppers at the first secrecy zone), the rate

$$R_{TR} = \frac{1}{(f_t d)^2}\left[\frac{1}{2}\log(1+\text{SNR}_{TR}) - \frac{1}{2}\log(1+\overline{\text{SNR}_{\mathcal{E}^*}})\right]^+, \tag{1}$$

where

$$\text{SNR}_{TR} \geq \underline{\text{SNR}_{TR}} \triangleq \frac{P(d+1)^{-\alpha}c^{-\alpha}(\sqrt{2})^{-\alpha}}{N_o + P8(f_t)^{-\alpha}d^{-\alpha}c^{-\alpha}S(\alpha)}, \tag{2}$$

$$S(\alpha) \triangleq \sum_{i=1}^{\infty} i(i-1)^{-\alpha}, \tag{3}$$

$$\overline{\text{SNR}_{\mathcal{E}^*}} \triangleq \frac{P(1+\epsilon)5c^2c^{-\alpha}d^{-\alpha}}{N_0}\lambda_e d^2 \sum_{k=2}^{L}(f_{l_k})^2(f_{l_{k-1}})^{-\alpha}, \tag{4}$$

$$f_t \geq \frac{d+1}{d}, \tag{5}$$

is w.h.p. securely and simultaneously achievable between any transmitter-receiver pair if f_{l_k} is chosen such that

$$\lambda_e d^2 (f_{l_k})^2 \to \infty, \text{ as } n \to \infty, \text{ for } k = 2, 3, \cdots. \tag{6}$$

Proof: The steps of the proof similar to that of the proof provided for [1, Lemma 1]. We only need to extend the upper bound on the colluding eavesdropper SNR. In our case, secrecy is guaranteed assuming that the eavesdroppers are located on the boundary of each secrecy zone level. We first bound the number of eavesdroppers at each level. We have

$$A_{l_k} \leq (2df_{l_k}+1)^2c^2 \leq 5d^2(f_{l_k})^2c^2 \tag{7}$$

and hence the number of eavesdroppers in layer l_k can be bounded, using the Chebyshev's inequality, by

$$|\mathcal{E}^*_{l_k}| \leq (1+\epsilon)\lambda_e 5c^2d^2(f_{l_k})^2 \tag{8}$$

w.p. 1 given $\epsilon > 0$ as long as we choose f_{l_k} to satisfy

$$\lambda_e d^2(f_{l_k})^2 \to \infty, \text{ as } n \to \infty.$$

Now, we place $|\mathcal{E}^*_{l_k}|$ number of eavesdroppers from layer k at distance $f_{l_{k-1}}$ for $k = 2, 3, \cdots$. This is referred to as configuration $\mathcal{E}^*$. These colluding eavesdroppers can do maximal ratio combining (this gives the best possible SNR for them) to achieve the following SNR.

$$\begin{aligned}\text{SNR}_{\mathcal{E}^*} &= \frac{P\sum_{k=2}^{L}|\mathcal{E}^*_{l_k}|(f_{l_{k-1}})^{-\alpha}c^{-\alpha}d^{-\alpha}}{N_0} \\ &\leq \frac{P(1+\epsilon)5c^2c^{-\alpha}d^{-\alpha}}{N_0}\lambda_e d^2\sum_{k=2}^{L}(f_{l_k})^2(f_{l_{k-1}})^{-\alpha} \\ &\triangleq \overline{\text{SNR}_{\mathcal{E}^*}}. \end{aligned} \tag{9}$$

■

Note that the challenge here is to choose f_{l_k} such that $\overline{\text{SNR}_{\mathcal{E}^*}} < \infty$, but at the same time satisfy (6).

Lemma 2 (Securing a Multi-Hop Path): Securing each hop from the colluding eavesdroppers in configuration $\mathcal{E}^*$ that

listen only the corresponding hop implies that the secrecy constraint is w.h.p. satisfied for the colluding eavesdroppers $\mathcal{E}$ (which listen the transmissions from all the hops and lie outside the first level secrecy zones).

Proof:

Proof follows by following the steps given in the proof of [1, Lemma 2], where the transmitter of hop i is now required to inject randomness at a higher rate of $R_i^x = I(X_i; Y_{e_1{}^*(i)}, \cdots, Y_{e_{|\mathcal{E}|}{}^*(i)}) = I(X_i; Y_{\mathcal{E}^*(i)})$. This rate loss is still finite and upper bounded by $\overline{\text{SNR}_{\mathcal{E}^*}}$ as shown in the previous theorem.

■

We now state our relevant percolation theory results. We say that each square is "open" if the square has at least one legitimate node and there are no eavesdroppers in the first secrecy zone around the square. We denote the probability of having at least one legitimate node in a square by p. It is evident that

$$p = 1 - e^{-c^2},$$

and hence, p can be made arbitrarily close to 1 by increasing c. For any given transmitting square, we denote the probability of having an eavesdropper-free secrecy zone by q. The number of eavesdroppers within the first secrecy zone is a Poisson random variable with parameter $\lambda_e(2f_{l_1}d+1)^2c^2$, and hence,

$$q = e^{-\lambda_e(2f_{l_1}d+1)^2c^2}.$$

Thus, q gets arbitrarily close to 1, as $n \to \infty$, if $\lambda_e(f_{l_1})^2 \to 0$ with n (d and c are some finite numbers for the highway construction).

Lemma 3 (Lemma 3 of [1]): There exist a sufficient number of *secure* vertical and horizontal highways such that, as $n \to \infty$, each secure highway is required to serve $O(\sqrt{n})$ nodes and an entry (exit) point has w.h.p. a distance of at most $\kappa' \log n$ away from each source (respectively, destination), where κ' can be made arbitrarily small, if

$$\lambda_e(2f_{l_1}d+1)^2c^2 \leq \delta$$

for some constant $\delta << 1$, for sufficiently large n.

We refer to [1, Lemma 3] for the proof of this lemma. Next, we have the following result regarding the secure rate over highways.

Lemma 4 (Rate per Node on the Highways): If $\lambda_e = O((\log n)^{-2})$, each node on the constructed highways can transmit to their next hop at a constant secure rate. Furthermore, as the number of nodes each highway serves is $O(\sqrt{n})$, each highway can w.h.p. carry a per-node throughput of $\Omega\left(\frac{1}{\sqrt{n}}\right)$.

Proof:

We show the result for $\lambda_e = \Theta\left((\log n)^{-2}\right)$, which will imply the desired result (as lowering the eavesdropper density can not degrade the performance). Consequently, there exists constants $\underline{\Lambda}$, $\overline{\Lambda}$, and n_1 such that

$$\underline{\Lambda}(\log n)^{-2} \leq \lambda_e \leq \overline{\Lambda}(\log n)^{-2}, \text{ for } n \geq n_1, \tag{10}$$

where $\underline{\Lambda} < \overline{\Lambda}$.

We choose each secrecy zone over the highways by setting

$$f_{l_k} = \left(\frac{\delta}{5\overline{\Lambda}c^2d^2}\right)^{\frac{1}{2}} (\log n)^{(\frac{\alpha}{2})^{k-1}}. \tag{11}$$

Here,

$$\begin{aligned} \lambda_e(2f_{l_1}d+1)^2c^2 &\leq \lambda_e 5(f_{l_1})^2d^2c^2 && (12)\\ &= \lambda_e \frac{\delta(\log n)^2}{\overline{\Lambda}} && (13)\\ &\leq \delta, \text{ for } n \geq n_1. && (14)\end{aligned}$$

Therefore, due to our percolation result, i.e., Lemma 3, each member of a given highway does not have any eavesdropper within their first level secrecy zone. Now, as the above choice also satisfies

$$\lambda_e d^2 (f_{l_k})^2 \to \infty, \text{ as } n \to \infty, \text{ for } k = 2, 3, \cdots,$$

we can utilize Lemma 1 to achieve a secrecy rate of

$$R_{TR} = \frac{1}{(f_t d)^2}\left[\frac{1}{2}\log(1+\text{SNR}_{TR}) - \frac{1}{2}\log(1+\overline{\text{SNR}_{\mathcal{E}^*}})\right]. \tag{15}$$

Now, we provide an upper bound for $\overline{\text{SNR}_{e^*}}$. First, note that our setup results in

$$(f_{l_k})^2 (f_{l_{k-1}})^{-\alpha} = \left(\frac{\delta}{5\overline{\Lambda}c^2d^2}\right)^{\frac{2-\alpha}{2}}.$$

Hence,

$$\begin{aligned} \overline{\text{SNR}_{e^*}} &= \frac{P(1+\epsilon)5}{N_0}\lambda_e(L-1)\left(\frac{\delta}{5\overline{\Lambda}}\right)^{\frac{2-\alpha}{2}} && (16)\\ &\leq \frac{P(1+\epsilon)5}{N_0}\overline{\Lambda}(\log n)^{-2}(L-1)\left(\frac{\delta}{5\overline{\Lambda}}\right)^{\frac{2-\alpha}{2}}, \\ &\quad \text{for } n \geq n_1 && (17)\\ &\to 0, \text{ as } n \to \infty, && (18)\end{aligned}$$

where the last step is due to the observation that the number of levels can be upper bounded by

$$L - 1 \leq \frac{\log(\log n)}{\frac{\alpha}{2}}. \tag{19}$$

Therefore, there exists n_2 such that for all $n \geq n_2$, the rate expression satisfies $R_{TR} \geq R$ for some constant R. The second claim follows from Lemma 3.

■

Our final step is to show that almost all the nodes can access the highways simultaneously with high probability with a rate scaling higher than $\Omega\left(\frac{1}{\sqrt{n}}\right)$.

Lemma 5 (Access Rate to the Highways): Almost all source (destination) nodes can w.h.p. simultaneously transmit (receive) their messages to (from) highways with a secure rate of $\Omega\left((\log n)^{-3-\alpha}\right)$, if $\lambda_e = O\left((\log n)^{-2(1+p)}\right)$ for any $p > 0$.

Proof:

We show the result for $\lambda_e = \Theta\left((\log n)^{-2(1+p)}\right)$, which will imply the desired result (as lowering the eavesdropper density

can not degrade the performance). Consequently, there exists constants $\underline{\Lambda}$, $\overline{\Lambda}$, and n_3 such that

$$\underline{\Lambda}(\log n)^{-2(1+p)} \leq \lambda_e \leq \overline{\Lambda}(\log n)^{-2(1+p)}, \text{ for } n \geq n_3, \tag{20}$$

where $\underline{\Lambda} < \overline{\Lambda}$.

At this point, we can upper bound the fraction of nodes that can not access to a highway due to an existence of an eavesdropper in their first secrecy zone. Following the analysis in [1, Lemma 5], as long as we satisfy

$$\lambda_e (f_{l_1})^2 d^2 \to 0, \text{ as } n \to \infty, \tag{21}$$

almost all the nodes can access to the highways. To compute the achievable secrecy rate with Lemma 1, we need to satisfy

$$\lambda_e (f_{l_k})^2 d^2 \to \infty, \text{ as } n \to \infty, \text{ for } k = 2, 3, \cdots. \tag{22}$$

Further, we can show that as long as we satisfy

$$\lambda_e d^2 \sum_{k=2}^{L} (f_{l_k})^2 (f_{l_{k-1}})^{-\alpha} \leq C, \text{ as } n \to \infty, \tag{23}$$

for some constant C, the achievable rate R_{TR} in Lemma 1 scales like $\Omega\left((\log n)^{-2-\alpha}\right)$. Due to time-division among the legitimate nodes accessing the highways (there are w.h.p. $O(\log n)$ nodes within small squares), the secrecy rate per user satisfies $\Omega\left((\log n)^{-3-\alpha}\right)$.

Here, to satisfy (21), (22), (23) with $d = \kappa' \log(n)$, where κ' is some constant that can be arbitrarily chosen small (Lemma 3), we choose the secrecy zones as

$$f_{l_k} = (\log n)^{r(\frac{\alpha}{2})^{k-1}}, \tag{24}$$

with some r satisfying $\frac{2}{\alpha} p < r < p$. ■

We hence obtained the following result.

Theorem 6: If the legitimate nodes have unit intensity ($\lambda = 1$) and the colluding eavesdroppers have an intensity of $\lambda_e = O\left((\log n)^{-2(1+p)}\right)$ for any $p > 0$ in an extended network, almost all of the nodes can achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$.

III. Multi-path Fading Model

We generalize the system model given in [2] to multi-eavesdropper scenario. We assume the existence of K_e external eavesdroppers each observe the signals of the K sources. The eavesdropper set is denoted with $\mathcal{K}_e = \{e_1, \cdots, e_K\}$, whereas the legitimate node set is denoted by $\mathcal{K} = \{1, \cdots, K\}$. We consider an ergodic setting where the channel gains are fixed during a block of n_1 symbol times and then randomly change to another value for the next block. Hence, transmission time of n time slots is divided into B fading blocks with $n = n_1 B$. We denote the received signals at receiver $i \in \{1, \cdots, K, e_1, \cdots, e_{K_e}\}$ using the extended channel notation as follows

$$\begin{aligned} \bar{\mathbf{Y}}_i(j + (b-1)n_1) &= \sum_{k=1}^{K} \mathbf{H}_{i,k}(b) \bar{\mathbf{X}}_k(j + (b-1)n_1) \\ &\quad + \bar{\mathbf{Z}}_i(j + (b-1)n_1), \end{aligned} \tag{25}$$

where $b \in \{1, \cdots, B\}$ denotes the fading block b, $j \in \{1, \cdots, n_1\}$ denotes the j^{th} time instant of the corresponding fading block, $\mathbf{H}_{i,k}(b)$ is the $F \times F$ diagonal matrix of channel coefficients between transmitter k and receiver i during fading block b, and $\bar{\mathbf{X}}_k(j + (b-1)n_1)$ is the transmitted vector of user k at j^{th} symbol of the b^{th} fading block. We further define $\mathbf{H} \triangleq \{\mathbf{H}_{i,k}(b) : i, k \in \mathcal{K}, b \in \{1, \cdots, B\}\}$ and $\mathbf{H}_e \triangleq \{\mathbf{H}_{e,k}(b) : e \in \mathcal{K}_e, k \in \mathcal{K}, b \in \{1, \cdots, B\}\}$. We assume that $\mathbf{H}$ is known at all the nodes in the network, whereas $\mathbf{H}_e$ is known only at the eavesdropper (only the statistical knowledge about the eavesdropper CSI is available to the network users). The channel coefficients are i.i.d. samples of a zero-mean unit variance complex Gaussian distribution.

We denote the observation at the eavesdropper e as $\mathbf{Y}_e = \{\bar{\mathbf{Y}}_e(1), \cdots, \bar{\mathbf{Y}}_e(n)\}$ for any $e \in \mathcal{K}_e$, and define $\mathbf{Y}_{\mathcal{K}_e} = \{\mathbf{Y}_e, \forall e \in \mathcal{K}\}$. In this scenario, we measure the secrecy level with the following information leakage rate to *colluding eavesdroppers*

$$\frac{1}{n} I\left(W_{\mathcal{K}}; \mathbf{Y}_{\mathcal{K}_e} | \mathbf{H}, \mathbf{H}_e\right). \tag{26}$$

We say that the secrecy tuple $(R_1, \cdots, R_K)$ is achievable for the Gaussian interference channel with colluding eavesdroppers, if, for any given $\epsilon > 0$, there exits an $(n, F, M_1, \cdots, M_K)$ secret codebook such that

$$\frac{1}{nF} \log_2 M_k = R_k, \ \forall k \in \mathcal{K}, \tag{27}$$

$$\max\{P_{e,1}, \cdots, P_{e,K}\} \leq \epsilon, \tag{28}$$

and

$$\frac{1}{n} I\left(W_{\mathcal{K}}; \mathbf{Y}_{\mathcal{K}_e} | \mathbf{H}, \mathbf{H}_e\right) \leq \epsilon. \tag{29}$$

Here, the error probability for user k is denoted by $P_{e,k}$. (Please refer to [2] for details of the secrecy codebook.)

We finally say that the symmetric secure degrees of freedom (per orthogonal frequency-time slot) of η is achievable, if the rate tuple $(R_1, \cdots, R_K)$ is achievable and

$$\eta = \lim_{\rho \to \infty} \frac{R_k}{\log(\rho)}, \forall k \in \mathcal{K}. \tag{30}$$

A. Analysis

In [2], the authors show how the interference alinement technique can be utilized to achieve secrecy in frequency selective channels. Interference alignment [3] is a recently proposed precoding technique and can be described as follows: Lets assume that we employ interference alignment precoding using the matrices $\bar{\mathbf{V}}_k$ of [3], so that the transmitted signals are of the form $\bar{\mathbf{X}}_k(t) = \bar{\mathbf{V}}_k \tilde{\mathbf{X}}_k(t)$, where $\tilde{\mathbf{X}}_k(t)$ represents the vector of m_k streams transmitted from user k. According to the interference alignment principle, the beamforming matrices $\bar{\mathbf{V}}_k$ are constructed to satisfy the following two properties:

1) The non-intended signals seen by each receiver are aligned within some low dimensionality subspace. More precisely, the column space of the matrices $\mathbf{H}_{i,k} \bar{\mathbf{V}}_k$ for $k \in \mathcal{K} - i$ lie in a subspace of dimension $F - m_i$ at receiver i.

2) The intended streams span the orthogonal subspace, i.e., the columns of $\mathbf{H}_{i,i}\bar{\mathbf{V}}_i$ are independent and are orthogonal to that of $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k$ for each user $k \in \mathcal{K}-i$.

Exploiting the channel ergodicity and utilizing the interference alignment scheme, the following result is given in [2].

Theorem 7 (Theorem 3 of [2]): For the K-user Gaussian interference channel with an external eavesdropper, a secure DoF of $\eta = \frac{1}{2} - \frac{1}{K}$ per frequency-time slot is achievable for each user in the ergodic setting (in the absence of the eavesdropper CSI).

We remark that as the ergodicity exploited in the achievability, the above result will also hold for any number of *non-colluding* eavesdroppers, as each one will observe statistically the same signals. For the collusion case, we generalize the above result as follows.

Theorem 8: For the K-user Gaussian interference channel with K_e external colluding eavesdroppers, a secure DoF of $\eta = \left[\frac{1}{2} - \frac{K_e}{K}\right]^+$ per frequency-time slot is achievable for each user in the ergodic setting (in the absence of the eavesdropper CSI).

Proof:

We provide a sketch of the proof here. (Please refer to [2] for details.) Let $m \in \mathbb{N}$ and $F = (m+1)^M + m^M$, where $M = (K-1)(K-2)-1$. We set $m_1 = (m+1)^M$ and $m_k = m^M$ for $k \neq 1$. We employ the same codebook construction of [2], where each code consists of $2^{nF(R+R^x)}$ codewords. Here, R corresponds to secure rate per orthogonal dimension, whereas R^x refers to the randomization rate (the rate loss experienced to achieve secrecy). At each fading block, we re-order users (for the construction of the interference alignment matrices) to achieve statistical symmetry across users; and choose the rates as follows.

$$R_k = \frac{1}{KF}\left(K\mathbb{E}[I(\tilde{\mathbf{X}};\bar{\mathbf{Y}}|\mathbf{H})] - \max_{p(\bar{\mathbf{X}}_{\mathcal{K}})} \mathbb{E}[I(\bar{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_{\mathcal{K}_e}|\mathbf{H},\mathbf{H}_e)]\right) \quad (31)$$

$$R_k^x = \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_{\mathcal{K}_e}|\mathbf{H},\mathbf{H}_e)], \quad (32)$$

Decodability: Due to the maximization in (31), we have $R_k + R_k^x \leq \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}};\bar{\mathbf{Y}}|\mathbf{H})]$, from which we conclude that each user in the interference network can decode its own secrecy and randomization indices as $n_1 \to \infty$ and as $B \to \infty$ using almost all codebooks in the ensemble.

Secrecy: Generalizing the equivocation computation to multiple eavesdroppers, we have

$$\begin{aligned}\frac{1}{n}H(W_{\mathcal{K}}|\mathbf{Y}_{\mathcal{K}_e},\mathbf{H},\mathbf{H}_e) &= \frac{1}{n}H(W_{\mathcal{K}}) + \frac{1}{n}H(W_{\mathcal{K}}^x) \quad (33)\\ &\quad - \frac{1}{n}I(W_{\mathcal{K}},W_{\mathcal{K}}^x;\mathbf{Y}_{\mathcal{K}_e},\mathbf{H},\mathbf{H}_e)\\ &\quad - \frac{1}{n}H(W_{\mathcal{K}}^x|W_{\mathcal{K}},\mathbf{Y}_{\mathcal{K}_e},\mathbf{H},\mathbf{H}_e).\end{aligned}$$

Here, we observe

$$\frac{1}{n}H(W_{\mathcal{K}}^x) = \frac{1}{n}\sum_{k=1}^{K} nFR_k^x = \mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_{\mathcal{K}_e}|\mathbf{H},\mathbf{H}_e)], \quad (34)$$

and

$$\begin{aligned}&\lim_{n\to\infty}\frac{1}{n}I(W_{\mathcal{K}},W_{\mathcal{K}}^x;\mathbf{Y}_{\mathcal{K}_e},\mathbf{H},\mathbf{H}_e) \quad (35)\\ &\leq \lim_{n\to\infty}\frac{1}{n}I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\cdots,\tilde{\mathbf{X}}_{\mathcal{K}}(n);\mathbf{Y}_{\mathcal{K}_e},\mathbf{H},\mathbf{H}_e)\\ &= \mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_{\mathcal{K}_e}|\mathbf{H},\mathbf{H}_e)].\end{aligned}$$

At this point, we remark that [2, Lemma 8] can be generalized to the multiple eavesdropper scenario: The choice $R_k^x = \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_{\mathcal{K}_e}|\mathbf{H},\mathbf{H}_e)]$ satisfies

$$\sum_{k\in\mathcal{S}} R_k^x \leq \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_{\mathcal{K}_e}|\tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)], \forall \mathcal{S}\subseteq\mathcal{K}, \quad (36)$$

and hence randomization messages are decodable at the colluding eavesdropper with this rate assignment. Therefore, averaging over the ensemble of codes and messages, we have

$$\frac{1}{n}H(W_{\mathcal{K}}^x|W_{\mathcal{K}},\mathbf{Y}_{\mathcal{K}_e},\mathbf{H},\mathbf{H}_e) \leq \epsilon, \quad (37)$$

where $\epsilon \to 0$ as $n \to \infty$. Now, combining (33), (34), (35), and (37), and taking the limit we obtain

$$\frac{1}{n}I(W_{\mathcal{K}};\mathbf{Y}_{\mathcal{K}_e}|\mathbf{H},\mathbf{H}_e) \leq \epsilon \quad (38)$$

for sufficiently large n.

Finally, we compute the achievable secure DoF with this scheme. We observe

$$\lim_{\rho\to\infty}\frac{\mathbb{E}[I(\tilde{\mathbf{X}};\bar{\mathbf{Y}}|\mathbf{H})]}{\log(\rho)} = \left(\frac{1}{K}m_1 + \frac{K-1}{K}m_2\right), \quad (39)$$

which follows from the random permutation and the ergodicity, and

$$\lim_{\rho\to\infty}\frac{\max_{p(\bar{\mathbf{X}}_{\mathcal{K}})}\mathbb{E}[I(\bar{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_{\mathcal{K}_e}|\mathbf{H},\mathbf{H}_e)]}{\log(\rho)} = F\min\{K,K_e\}. \quad (40)$$

Now, combining (31), (39), and (40), we conclude

$$\begin{aligned}\lim_{m\to\infty}\lim_{\rho\to\infty}\frac{R_k}{\log(\rho)} &= \lim_{m\to\infty}\left[\frac{1}{KF}\left(m^M + (m+1)^M(K-1)\right.\right. \quad (41)\\ &\left.\left. - F\min\{K,K_e\}\right)\right]^+ = \frac{[K-2K_e]^+}{2K}.\end{aligned}$$

■

We remark that colluding eavesdroppers degrade the achievable performance. For $K_e \geq K/2$, we can not achieve any positive secure DoF per user with this scheme. However, we note that, in the limit of $\frac{K_e}{K} \to 0$, this scheme achieves $\eta \to \frac{1}{2}$ secure DoF per user. We can readily conclude that adding more users to the network enhances security in this scenario.

REFERENCES

[1] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," Aug. 2009. [Online]. Available: http://arxiv.org/abs/0908.0898

[2] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, submitted for publication. [Online]. Available: http://arxiv.org/abs/0810.1187

[3] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom for the k-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.