On the Secure Degrees-of-Freedom of Partially Connected Networks with no CSIT

Mohamed Adel Attia  Ravi Tandon
Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ, 85721
Email: \{madel, tandonr\}@email.arizona.edu

Abstract—In this work, we focus on the partially connected interference network with confidential messages, and study the secure degrees of freedom with no channel state information at the transmitters (CSIT). Prior works on fully connected interference networks with full CSIT have shown that the secure degrees of freedom scales linearly with the number of users. With no CSIT, however, the secure degrees of freedom of fully connected networks collapses to zero. In this work, we show that partial connectivity, a widely prevalent property of wireless networks, can be leveraged to provide secrecy even with no CSIT. We present a systematic approach to first understand the feasibility of secure communication in a partially connected network and develop achievable schemes for a class of regular partially connected networks. Finally, we also provide novel information theoretic outer bounds on the secure degrees of freedom for this class of regular partially connected networks, and approximately characterize the secure degrees of freedom.

I. INTRODUCTION

Over the past several decades, information theoretic approaches for physical layer security have received significant interest, with the goal of achieving confidential data transmission over wireless networks. Starting from the seminal works of Wyner [1] in the 1970s on single-user wiretap channels, significant progress has been made on multiple fronts: several ingenious techniques such as artificial noise injection, secrecy precoding, lattice-based approaches, cooperative jamming have been developed, which in turn have contributed to our understanding of fundamental limits of secure communication in multi-user networks (we refer the reader to [2] for a recent comprehensive survey). Despite this progress, one of the major hurdles in realizing physical layer security is the assumption of timely and accurate availability of channel knowledge, or channel state information at the transmitters (CSIT), which may not be available in practice. To overcome this, several works have started to consider these problems under relaxed CSIT assumptions, including delayed CSIT [3], blind cooperative jamming [4], and recent works on no Channel State Information (CSI) from adversarial nodes [5].

In this paper, we focus on \(K\)-user interference networks with confidential messages and no CSIT. A special case of this problem is the fully connected interference network, i.e., every receiver is connected to every transmitter. For this network, it was recently shown in [6] that the secure sum degrees of freedom (SDoF) with full CSIT is given by \((K^2 - K)/(2K - 1)\), which grows linearly with \(K\). For this fully connected network, with no CSIT, it can be formally argued that the SDoF collapses to zero. This is due to the fact that all the users receive statistically equivalent signals making it impossible to achieve any secure degrees of freedom.

While the above results may appear pessimistic, they make the assumption of full connectivity. In practice, however, differences in wireless channels for different users due to the random placement of the nodes, the path loss, and the existence of obstacles in the wireless medium lead to a partially connected network topology, in which a receiver is effectively connected to only a subset of the transmitters. For such partially connected networks, the problem of reliable communication has been addressed through various Topological Interference Management (TIM) schemes [7–9]. These schemes do not assume any CSIT but only work under the assumption about the knowledge of network topology.

This paper asks the following fundamental questions: Is secure communication feasible in partially connected networks? If yes, is there a principled approach to achieve positive SDoF, and what is the optimal value? To this end, we initiate the study of partially connected interference networks with no CSIT, which can be viewed as the Secure Topological Interference Management problem. To the best of our knowledge, no prior work has considered secrecy for the TIM problem. The contributions of this paper are summarized as follows:

- First, we present a systematic approach to understand when secure communication is possible for any user in a partially connected network with no CSIT. We subsequently generalize this approach for multiple secure transmissions.
- We next apply these ideas to the \((K,d)\) partially connected regular networks with no CSIT, and present a general scheme for any number of users, \(K\) and any node degree \(d\). Our scheme achieves a sum SDoF of \([K/(d + 1)]\), which grows linearly with the number of users \(K\), for a fixed \(d\).
- We also derive an information theoretic upper bound on the sum SDoF for the \((K,d)\) partially connected regular networks as \(K/(d + 1)\), which shows that our scheme is information theoretically optimal within a gap of at most \(d/(d + 1) < 1\). Furthermore, we give some directions on how to close this gap by exploiting side information at the users.

II. SYSTEM MODEL

We consider the \(K \times K\) partially connected Gaussian interference channel, with \(K\) transmitters and \(K\) receivers, each with one antenna. Transmitter \(Tx_k\) has a message \(W_k\) intended for receiver \(Rx_k\). In order to describe the topology of the underlying network, we define \(R_k\) as the connectivity set of the transmitter \(Tx_k\), which contains all the receivers that it is connected to, and \(T_k\) as the connectivity set of the receiver \(Rx_k\), which contains all the transmitters that it is connected to. For example, if \(T_k = \{3, 7\}\), then receiver \(Rx_k\) is connected to the transmitters \(Tx_3\) and \(Tx_7\). We also

This work was supported by NSF Grant CCF 1559758.
define the node degree as the number of nodes connected to it, which is given by the cardinality of its connection set, i.e., the node degrees of \( R_k \) and \( T_k \) are given by \(|T_k|\), and \(|R_k|\), respectively. Now, we notice that the topology of the network is completely characterized by the connectivity sets of all the transmitters and the receivers, and we refer to the topology \( G \) as, \( G \sim (T_1, \ldots, T_K, R_1, \ldots, R_K) \).

In a partially connected network, the received signal at time \( t \) for any receiver \( R_k \) is composed only of signal components coming from \( T_k \), for \( i \in T_k \), and is given by
\[
Y_k(t) = \sum_{i \in T_k} H_{ki}(t) X_i(t) + Z_k(t),
\]
where \( X_i(t) \) is the signal transmitted by transmitter \( T_i \) at time \( t \), for \( i = \{1, \ldots, K\} \). \( H_{ki}(t) \) indicates the random complex channel coefficient between transmitter \( T_i \) and receiver \( R_k \), and \( Z_k(t) \sim N(0,1) \) is the complex Gaussian noise. In order for each receiver \( R_k \) to get the required message \( W_k \), it should be connected to the corresponding transmitter \( T_k \), i.e., \( k \in R_k \) (then \( k \in T_k \)).

We assume the channel coefficients \( H_{ki}(t) \) are generated from a continuous distribution and are assumed to be independent and identically distributed (i.i.d.) across time and users. We define \( H_{ki}^{(n)} \) as the \( n \times n \) diagonal matrix, where its diagonal entries represent the channel coefficients from time \( t = 1 \) to \( t = n \) between \( T_k \) and \( R_k \). We also define \( \Omega = \{ H_{ki}^{(n)} : i \in T_k \}_{k=1}^{K} \) as the set containing all non-zero channel coefficients between any transmitter/receiver pair. We assume that \( \Omega \) is not available at any of the transmitters, while \( \Omega \) is available causally at the receivers. The block received signal at \( R_k \) after a block of length \( n \) is given by
\[
Y_k^n = \sum_{i \in T_k} H_{ki}^{(n)} X_i^n + Z_k^n,
\]
where \( X_i^n, Y_k^n, \) and \( Z_k^n \) are the \( n \times 1 \) column vectors of block length \( n \). We assume the transmitted signal \( X_i^n \) obeys an average power constraint, \( \frac{1}{n} E[\|X_i^n\|^2] < P \).

We say a rate tuple \( (R_1^1(P, G), R_2^1(P, G), \ldots, R_K^1(P, G)) \) is confidentially achievable, if there exist a sequence of decoding and encoding functions such that for some \( \epsilon_n \to 0 \) as \( n \to \infty \), the following two conditions are satisfied:

**Decodability Constraint:** Each receiver should decode the corresponding message reliably from the received signal, i.e.,
\[
\max_k \Pr(W_k \neq \hat{W}_k) \leq \epsilon_n.
\]

**Confidentiality Constraint:** Transmitters are sending confidential messages to the intended receivers such that all messages are kept information-theoretically secure against all unintended receivers, i.e., for \( W_{k_1}^K \subseteq \{W_1, \ldots, W_K\} \setminus W_k \),
\[
I(W_{k_1}^K; Y_k^n) \leq n \epsilon_n, \forall k.
\]

We say a secrecy degree of freedom tuple \( (d_1^k, \ldots, d_k^k) \) is achievable if for any achievable rate \( R_i^k(P, G) \), we have \( d_i^k = \lim_{P \to \infty} \frac{R_i^k(P, G)}{\log(P)} \). Therefore, the sum Secure Degree of Freedom (SDoF) for a partially connected interference channel given by a topology \( G \) is given as
\[
\text{SDoF}^{G} = \sum_{i=1}^{K} d_i^k = \lim_{P \to \infty} \frac{\sum_{i=1}^{K} R_i^k(P, G)}{\log(P)}.
\]

**Notation:** For any two sets \( A \) and \( B \), \( A \setminus B \) is defined as all the elements in the set \( A \) that is not in the set \( B \), i.e., \( A \setminus B = \{i : i \in A, i \notin B\} \). We also denote \( L_i(A, B) \) and \( L_i'(A, B) \) as two different linear combinations of the Random variables \( A \), and \( B \) received at \( R_i \).

### III. MAIN RESULTS AND DISCUSSIONS

We first state two important lemmas, which help in understanding how we can achieve positive secure degrees of freedom using the approach of artificial noise injection and interference avoidance for any arbitrary network topology.

**Lemma 1. (Secure communication for a user)\footnote{This lemma is a direct consequence of the results in [9] and [10].}**
For any receiver \( R_i \), a positive secure degree of freedom can be achieved, i.e., \( d_i^k > 0 \), if \( \forall j \in R_i \setminus \{i\} \), the following condition is satisfied,
\[
T_j \setminus T_i \neq \emptyset.
\]

**Proof:** For secure communication to \( R_i \), one possible approach is to employ artificial noise injection and interference avoidance. To this end, when \( T_i \) transmits to \( R_i \), then other transmitters can send artificial noise in order to immerse the signal seen at every unintended receiver connected to \( T_i \), i.e., for \( j \in R_i \setminus \{i\} \), we should have \( T_j \neq \emptyset \). This condition implies that for every unintended receiver, there must be at least one other transmitter connected to it. However, it may be the case that the protecting transmitters (or the transmitters sending artificial noise) are connected to the legitimate receiver \( R_i \), then the jamming signals are received at \( R_i \) as well. Therefore, the chosen protecting transmitters should not be connected to \( R_i \), i.e., not in \( T_i \), otherwise they will immerse the intended reception. Therefore, the secrecy condition for a single user to transmit becomes \( T_j \setminus T_i \neq \emptyset \), \( \forall j \in R_i \setminus \{i\} \). Whenever the above condition is satisfied, a positive secure degree of freedom is achievable for receiver \( R_i \) through artificial noise injection and interference avoidance.

**Lemma 2. (Multiple simultaneous secrecy transmission)\footnote{This lemma is a direct consequence of the results in [9] and [10].}**
For a set of \( k \) receivers labeled as \( \{R_{i_1}, \ldots, R_{i_k}\} \), positive \( k \)-tuples secure degrees of freedom can be achieved simultaneously, i.e., \( d_i^k = \ldots d_i^k > 0 \), if \( \forall j \in ( \cap_{i_k} i_1 \cup \cap_{i_2} i_2 \cup \ldots \cup \cap_{i_k} i_k \) \), the following condition is satisfied,
\[
T_j \setminus (T_{i_1} \cup T_{i_2} \ldots \cup T_{i_k}) \neq \emptyset.
\]

**Proof:** This lemma takes the single-user approach further and gives sufficient conditions for simultaneous secure transmission of different messages. If \( k \) transmitters send message symbols simultaneously, we therefore require two conditions:

a) each reception must be protected at unintended receivers by artificial noise injection from some other transmitters, and

b) the reception of legitimate signals must not cause interference to each other (i.e., interference must be avoided). Therefore, in order to protect all the \( k \) transmitted messages, then for every unintended receiver \( R_j \) connected to any of the \( k \) transmitters, i.e., \( j \in ( \cap_{i_k} i_1 \cup \cap_{i_2} i_2 \cup \ldots \cup \cap_{i_k} i_k \) \), we have \( T_j \neq \emptyset \). However, we need not affect any of the \( k \) intended receptions, i.e., the protecting transmitters are not in \( (T_{i_1} \cup T_{i_2} \ldots \cup T_{i_k}) \), which leads to the condition in (6).

Next, we give some examples to understand how Lemma 1 and Lemma 2 can be applied for any arbitrary topology.
Example 1 (Fully Connected Topology). In this example, we consider a fully connected network with $K = 4$ transmitter/receiver pairs. In this case, the connectivity sets are given as $T_i = R_i = \{1, 2, 3, 4\}, \forall i \in \{1, 2, 3, 4\}$. Applying Lemma 1 for every transmitter $T_x_i$, $i \in \{1, 2, 3, 4\}$, we have $T_i \setminus T_j = \{\phi\}, \forall j \neq i$. Therefore, if any transmitter $T_x_k$, $k \neq i$, sends artificial noise $N_{k'}$ to imitate $S_i$ at $R_x_j$, it will also hide $S_i$ at the intended receiver $R_x_i$. As a result, security can not be achieved for a fully connected network with no CSIT. That is also due to the fact that for a fully connected network with no CSIT, all the received signals are statistically equivalent. Therefore, with the secrecy requirement we get $I(W_k; Y_k^{t_n}) = I(W_k; Y_k^{t_n}) \leq n \epsilon_n, \forall j \neq k$, which means that the decodability constraint contradicts with the secrecy requirement, i.e., $d_k^t = 0, \forall k$, and SDoF = 0.

Example 2 (Irregular Topology). Consider the partially connected channel shown in Figure 1.

- We first apply Lemma 1 to notice the following:
  - In order for $T_x_1$ to reliably transmit a secure message, say $S_1$, to $R_x_1$, it must be protected from $R_x_3$ which will also receive $S_1$, i.e., $3 \in R_3$. However, we notice that $T_3 \setminus T_1 = \{4, 5\} \neq \{\phi\}$ which means according to Lemma 1 that either $T_x_4$, or $T_x_5$ can protect $S_1$ by sending artificial noise $N_4$, or $N_5$, respectively, which is not seen by $R_x_1$.
  - In order for $T_x_3$ to transmit a secure message, say $S_3$, to $R_x_3$, it must be protected from $R_x_1$ which will also receive $S_3$, i.e., $1 \in R_1$. However, we notice that $T_1 \setminus T_3 = \{\phi\}$ which means according to Lemma 1 that there is no transmitter that can protect $S_3$ at $R_x_1$ without affecting $R_x_3$.
  - Doing the same analysis for the remaining users, we conclude that only transmitters $T_x_1, T_x_2$, and $T_x_5$ can transmit securely to the corresponding receivers, i.e., $d_i^t > 0$ for $i = 1, 2, 5$, while $T_x_3$ and $T_x_4$ can not transmit without revealing their messages to other unintended receivers, i.e., $d_3^t = d_4^t = 0$.
- We next apply Lemma 2 to this example to understand when more than one user can transmit simultaneously.
  - Taking the pair of transmitters $(T_x_1, T_x_2)$, in order to transmit two messages securely, say $(S_1, S_2)$, they must be protected at receivers $R_x_3$, and $R_x_4$ (3 $\in R_1, 4 \in R_3$). Using Lemma 2, we notice that $T_3 \setminus (T_1 \cup T_2) = \{5\}$, and $T_4 \setminus (T_1 \cup T_2) = \{5\}$. Therefore, by sending artificial noise $N_5$ from $T_x_5$, it will hide both $S_1$ and $S_2$ at $R_x_3$, and $R_x_4$ without affecting the intended receptions at $R_x_1$, and $R_x_2$.
  - Taking the pair of transmitters $(T_x_1, T_x_5)$, in order to transmit two messages securely, say $(S_1, S_5)$, they must be protected at receivers $R_x_3$, and $R_x_4$ (3 $\in R_1, 4 \in R_3$). Using Lemma 2, we notice that $T_3 \setminus (T_1 \cup T_5) = \{4\}$, and $T_4 \setminus (T_1 \cup T_5) = \{\phi\}$. Therefore, even if we can protect the messages at $R_x_4$ by sending artificial noise from $T_x_2$, it is impossible to protect them at $R_x_3$ without affecting the intended reception at $R_x_1$, or $R_x_5$.
  - Similarly, it is not feasible to send secure messages simultaneously for the remaining pair $(T_x_2, T_x_5)$.

As a summary, as shown in Figure 1 we can send in the first time slot two secure messages $S_1$ and $S_2$ to $R_x_1$ and $R_x_2$, respectively, and one secure message $S_5$ to $R_x_5$ in the second slot. Therefore, we achieve SDoF = $\frac{3}{2}$.

Now, we define a special class of network topologies named as the regular topology.

**Definition 1.** (Regular Topological Interference Channel)
A $(K, d)$ regular network refers to a symmetric structured network of $K$ users with each node has a degree $d$. In other words, if we consider the adjacency matrix for the network, all the rows and columns are shifted versions of each other, and the sum of each row and column is equal to $d$.

Example 3 (Regular topology). We assume a $(6, 2)$ regular network of $K = 6$ users, and $d = 2$ node degrees, where every transmitter is connected to the corresponding receiver as well as the next $d - 1 = 1$ receivers as shown in Figure 2.

- If we consider $T_x_1$ is sending a symbol $S_1$ to $R_x_1$, it will prevent the next $d - 1 = 1$ users (here $R_x_2$ only) from receiving their own symbols because of receiving $S_1$. In order to protect $S_1$, one way is to send artificial noise $N_2$ from $T_x_2$ to imitate $S_1$ at $R_x_2$ without affecting the reception at $R_x_1$. However, $N_2$ is also received at $R_x_3$ preventing it from receiving $S_3$ while $R_x_1$ is receiving, and we keep $T_x_3$ silent.
- While $T_x_1$ is sending $S_1$, let $T_x_4$ send a symbol $S_4$ to $R_x_4$. This transmission will prevent the next transmitter $T_x_5$ from sending a symbol to $R_x_5$. Instead, $T_x_5$ will send artificial
noise $N_1$ to immerse $S_1$ at $R_X_5$, which will prevent $R_X_6$ from receiving $S_6$ while $R_X_4$ is receiving, and we keep $T_X_6$ silent.

- In the same way, $T_X_2$, and $T_X_5$ (also $T_X_3$, and $T_X_4$) can send two secure symbols simultaneously, while $T_X_3$, and $T_X_6$ ($T_X_1$, and $T_X_4$) are sending artificial noise to protect the reception at unintended receivers $R_X_3$, and $R_X_6$ ($R_X_1$, and $R_X_4$).

- To summarize, we are able to send 6 symbols in 3 time slots, and hence we achieve $SDoF = \frac{6}{2} = 3$.

**Remark 1.** Without loss of generality, when we consider a $(K,d)$ regular network throughout this paper, we assume a topology such that for any transmitter $T_X_k$, the connectivity set including direct links to receivers is given by,

$$R_k = \{k, k+1, \ldots, k+d-1\} \pmod{K}. \quad (7)$$

Equivalently, for any receiver $R_X_k$, the connectivity set is,

$$T_k = \{k-k, k-k+1, \ldots, k-d+1\} \pmod{K}. \quad (8)$$

This structure can be restored for any general $(K,d)$ regular network given by Definition 1, by permuting the set of users (permuting the columns and the rows of the adjacency matrix) to get the same the connectivity sets given by (7) and (8).

**General Scheme for Regular Networks**

Now, we generalize a scheme for any $(K,d)$ regular network. Each transmission between $T_X_i$ and $R_X_i$, say $S_i$, is also received at the next $d-1$ users, $\{R_X_{i+1}, \ldots, R_X_{i+d-1}\}$. For secure transmission, $T_X_{i+1}$ can send artificial noise $N_{i+1}$ that will immerse $S_i$ at all the $d-1$ unintended receivers. However, this noise will also be received at $R_X_{i+d}$. To summarize: “Each secure transmission at $R_X_i$ will affect the next $d$ receivers, $\{R_X_{i+1}, \ldots, R_X_{i+d}\}$, preventing them from receiving their own symbols”. Therefore, for $K$ transmitter/receiver pairs, we can send $\left\lfloor \frac{K}{d+1} \right\rfloor$ messages in one channel use. Starting from $T_X_1$, the following transmitters can transmit in the same time $\{T_X_1, T_X_{i+d+1}, \ldots, T_X_{i+\mu(d+1)}\}$, where $\mu = \left\lfloor \frac{K}{d+1} \right\rfloor$. In order to symmetrize the scheme, we repeat this session $K$ times for $i \in \{1, \ldots, K\}$. As a result we can send $K\left\lfloor \frac{K}{d+1} \right\rfloor$ total symbols in $K$ channel uses, achieving $SDoF = \left\lfloor \frac{K}{d+1} \right\rfloor$.

Therefore, we have our first theorem which gives a lower bound on $SDoF$ for any $(K,d)$ regular network.

**Theorem 1.** (Achievability for Regular Topologies) For any $(K,d)$ regular network, we can achieve an $SDoF$ with no CSIT given as follows,

$$SDoF_{\text{Regular}}(K,d) \geq \begin{cases} \left\lfloor \frac{K}{d+1} \right\rfloor, & \forall d \neq 1 \\ K, & d = 1 \end{cases} \quad (9)$$

We also state the following theorem which gives an Information theoretic upper bound on $SDoF$ for any $(K,d)$ regular network.

**Theorem 2.** (Upper Bound for Regular Topologies) For any $(K,d)$ regular network, the $SDoF$ with no CSIT is upper bounded as follows,

$$SDoF_{\text{Regular}}(K,d) \leq \begin{cases} \left\lfloor \frac{K}{d+1} \right\rfloor, & \forall d \neq \{1, K\} \\ K, & d = 1 \\ 0, & d = K \end{cases} \quad (10)$$

\(^1\)All the indexes in this paper are modulo $K$

**Example 4** (Closing the Gap). Consider a modification of our general scheme as in Figure 4. In the first slot, $T_X_1$ sends a secure message $S_1$ to $R_X_1$. In order to immerse $S_1$ at $R_X_2$, $T_X_2$ sends artificial noise $N_2$. Let $T_X_3$ send an artificial noise $N_3$ while the secure transmission of $T_X_1$ is taking place. This transmission will not affect the decodability at $R_X_1$, and will provide $N_3$ as a side information to $R_X_3$ without revealing $N_3$ to $R_X_3$ (receives $L_3(N_2+N_3)$). Therefore, $N_3$ still can be used to protect a message coming from $T_X_2$ at receiver $R_X_3$.

In the second slot, we send $N_1$ while the secure transmission of $S_3$ to $R_X_3$ is taking place. In a similar way, $N_4$ is received at $R_X_2$ as a useful side information. Using the side information $N_1$, and $N_3$ available at $R_X_2$, and $R_X_4$, respectively, we can securely send in the third slot two symbols, $S_2$, and $S_4$, simultaneously for $R_X_2$, and $R_X_4$, respectively. For decoding, $R_X_2$ uses $L_2(S_1+N_1)$ and the side information $N_1$ to get $S_1$, while $R_X_4$ uses $L_4(S_4+N_3)$ and the side information $N_3$ to get $S_4$. As a result, we are able to securely send 4 symbols in 3 slots achieving $SDoF_{\text{Regular}}(4,2) = \frac{4}{3}$, which satisfies the upper bound in (10) and closes the gap in Figure 3.

**IV. CONCLUSIONS**

In this paper, we considered the partially connected network with confidential messages and no CSIT, where we discussed an approach towards achieving secrecy for any arbitrary topology. As an application, we considered the $(K,d)$ regular topology, where we introduced a general secrecy scheme achieving $SDoF = \left\lfloor \frac{K}{d+1} \right\rfloor$. We also derived an information theoretic upper bound, $SDoF \leq \left\lfloor \frac{K}{d+1} \right\rfloor$, with a gap at most $\frac{d}{d+1}$.

We showed through an example of $(4,2)$ regular network that closing the gap is possible by leveraging side information at the receivers. There are several interesting future directions for this problem, such as closing the gap for any $(K,d)$ regular network, and also generalizing our scheme and outer bound using the approaches presented in this paper towards any arbitrary topology.
t = 3 \hspace{1cm} t = 2 \hspace{1cm} t = 1 \hspace{1cm} t = 2 \hspace{1cm} t = 3

\begin{align*}
N_1 & \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow S_1 \hspace{1cm} L_1(N_1, N_2, L_2(N_1, N_2)) \\
S_1 & \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow S_2 \hspace{1cm} L_2(S_1, N_2, L_2(S_2, N_2)) \\
N_2 & \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow S_3 \hspace{1cm} L_3(N_2, N_3, L_2(S_3, N_2)) \\
S_3 & \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow S_4 \hspace{1cm} L_4(S_3, N_3, L_4(S_4, N_3))
\end{align*}

Fig. 4. Regular interference network with K = 4 transmitter/receiver pairs, and node degree d = 2. We modify our scheme such that Rx\(_2\) and Rx\(_3\) can get side information \(N_1\) and \(N_1\), respectively, which can be used to send two symbols at \(t = 3\), achieving SDoF = \(\frac{4}{7}\).

REFERENCES


APPENDIX A

PROOF OF THEOREM 2

Using Remark 1, the \(n\)-length block received signal at Rx\(_d\) in a \((K, d)\) regular network can be written as \(Y_d^n = \sum_{i=0}^{K-1} H_d^{(i)} X_i^n + Z_d^n\). We first bound the secure rate \(R_d^n\) for Rx\(_d\) as follows,

\[ nR_d^n = H(W_d) \geq I(Y_d^n; W_d) + H(W_d | Y_d^n) \]

\[ = I(Y_d^n; W_d | \Omega) + n\epsilon_n = h(Y_d^n | \Omega) - h(Y_d^n | W_d, \Omega) + n\epsilon_n, \]

where \((a)\) is due to Fano’s inequality using (2), and \(\Omega\) denotes the global CSI as defined in Section II. Since \(\Omega\) appears in all terms in the conditioning, we will omit it for simplicity in all subsequent derivations.

A. Decodability Constraint

We next obtain a lower bound on the term \(h(Y_d^n | W_d)\):

\[ h(Y_d^n | W_d) \geq h(Y_d^n | W_d, X_d^n) \left( a \right) = h(Y_d^n | X_d^n) \]

\[ = h \left( \sum_{i=1}^{d} H_d^{(i)} X_i^n + Z_d^n \right | X_d^n) = h \left( \sum_{i=1}^{d-1} H_d^{(i)} X_i^n + Z_d^n \right), \]

(12)

where \((a)\) follows from the Markov chain \(W_d \rightarrow X_d^n \rightarrow Y_d^n\). In order to bound \(h \left( \sum_{i=1}^{d-1} H_d^{(i)} X_i^n + Z_d^n \right), \) we next define \(L_\ell = \sum_{i=1}^{\ell} H_d^{(i)} X_i^n + Z_d^n\), for \(\ell \in \{1, \ldots, d-1\}\) and develop a recursive relationship for \(h(L_\ell)\) as follows:

\[ h(L_\ell) = h(L_\ell | W_\ell) + H(W_\ell) - H(W_\ell | L_\ell) \]

\[ \geq h(L_\ell | X_\ell^n) + H(W_\ell) - H(W_\ell | L_\ell) \]

\[ \geq h(L_{\ell-1}) + nR_\ell^n - n\epsilon_n, \]

(13)

where \((a)\) follows from the Markov chain \(W_d \rightarrow X_\ell^n \rightarrow Y_\ell^n\), and \((b)\) by noting that \(h(L_\ell | X_\ell^n) = h(L_{\ell-1})\) by removing the contribution of \(X_\ell^n\) from \(L_\ell\) to get \(L_{\ell-1}\), and the fact that \(H(W_\ell | L_\ell) \leq n\epsilon_n\) due to the following remark.

Remark 2. From the decodability constraint (2), \(W_i\) must be decoded from \(Y_i^n\). Now, if we assume a genie providing clean symbols \(X_i, i \in \{K-(\ell-1), \ldots, K\}\) to Rx\(_2\), then it can remove the interference caused by those symbols from \(Y_i^n\) and get a more clean version \(\tilde{Y}_\ell = \sum_{i=1}^{\ell} H_d^{(i)} X_i^n + Z_d^n\). If \(\tilde{Y}_\ell\) is sufficient to decode \(W_\ell\), then \(\tilde{Y}_\ell\) is also sufficient to decode \(W_\ell\). Since \(\tilde{Y}_\ell\) is statistically equivalent to \(L_\ell\) because no CSI is available at the transmitters, then \(L_\ell\) is also sufficient to decode \(W_\ell\), i.e., \(H(W_\ell | L_\ell) \leq n\epsilon_n\).

Therefore, starting from \(h(L_{d-1})\) in (13), we now obtain a lower bound on \(h(Y_d^n | W_d)\) from (12) as,

\[ h(Y_d^n | W_d) \geq h(L_{d-1}) \geq h(L_{d-2}) + nR_{d-1}^n - n\epsilon_n \]

\[ \vdots \]

\[ \geq h(L_1) + n \sum_{i=2}^{d-1} R_i^n - n(d-2)\epsilon_n \]

\[ \geq n \sum_{i=1}^{d-1} R_i^n + h(\tilde{X}_1^n + \tilde{Z}_1^n | W_1) - n(d-1)\epsilon_n, \]

(14)

where \((a)\) follows by lower bounding \(h(L_1)\) through the following arguments.

Remark 3. We first define \(\tilde{X}_1^n = \tilde{H}^{(n)} X_1^n\), for any \(\tilde{H}^{(n)} \in \Omega\), then we note that \(\tilde{X}_1^n + \tilde{Z}_1^n\) is statistically equivalent to \(L_1 = H_d^{(1)} X_1^n + Z_d^n\) due to the no CSIT assumption, where \(\tilde{Z}_1^n\) is independent of and identically distributed as \(Z_d^n\). Therefore, we can write

\[ h(L_1) = h(L_1 | W_1) + H(W_1) - H(W_1 | L_1) \]

\[ \geq h(\tilde{X}_1^n + \tilde{Z}_1^n | W_1) + nR_1^n - n\epsilon_n, \]

(15)

Note that for \(\ell \in \{1, \ldots, d-1\}\), we have \(\ell - d + 1 \pmod{K} = K + (\ell - d + 1) < K\).
where (b) follows from the arguments similar to Remark 2. Now plugging (14) in (11), we obtain

\[ n \sum_{i=1}^{d} R_i^n \leq h(Y_d^n) - h(\bar{X}_1^n + \bar{Z}_d^n|W_i) + nd\epsilon_n. \]  

(16)

If we start in (11) with any user \( k \in \{1, 2, \ldots, K\} \), we get \( K \) different bounds. Then, summing up all these \( K \) bounds,

\[ nK\log(P) - \sum_{i=1}^{K} h(\bar{X}_i^n + \bar{Z}_i^n|W_i) + nKd\epsilon_n \]

\[ \leq nK\log(P) - \sum_{i=1}^{K} h(\bar{X}_i^n + \bar{Z}_i^n|W_i) + nKd\epsilon_n, \]  

(17)

where (a) follows by writing the noise \( \bar{Z}_i^n \) as a sum of i.i.d. noises, \( Z_i^n = Z_{1_i}^n + \cdots + Z_{n_i}^n \), where the individual variances of each noise term are \( 1/d \) times the variance of \( Z_i^n \).

### B. Confidentiality Constraint

In order to use the confidentiality constraint in (3), we start differentially bound in the form in (11) as follows,

\[ nR_d^n \leq h(Y_d^n) - h(Y_d^n|W_d) + n\epsilon_n - I(Y_d^n; W_1, \ldots, W_{d-1}) \]

\[ + I(Y_d^n; W_1, \ldots, W_{d-1}) \leq h(Y_d^n|W_1, \ldots, W_{d-1}) - h(Y_d^n|W_d) + 2n\epsilon_n \]

\[ \leq h(\sum_{i=1}^{d-1} R_i^n - h(\bar{X}_i^n + \bar{Z}_i^n|W_1) + n(d+1)\epsilon_n \]

\[ \sum_{i=1}^{d-1} R_i^n \leq \sum_{i=2}^{d} h(\bar{X}_i^n + \bar{Z}_i^n|W_i) + nR_d^n - n \sum_{i=1}^{d-1} R_i^n \]

\[ + n(d+1)\epsilon_n - n\epsilon_n = -n\epsilon_d^n \]

(18)

where (a) follows from the conditionality requirement in (3), (b) by bounding \( h(Y_d^n|W_d) \) using (14), and (c) by bounding \( h(Y_d^n|W_1, \ldots, W_{d-1}) \) as follows,

\[ h(Y_d^n|W_1, \ldots, W_{d-1}) \leq h(\sum_{i=1}^{d} \bar{X}_i^n + \bar{Z}_i^n|W_1, \ldots, W_{d-1}) \]

\[ = h(\sum_{i=1}^{d} (\bar{X}_i^n + \bar{Z}_i^n)|W_1, \ldots, W_{d-1}) \]

\[ \leq \sum_{i=1}^{d} h(\bar{X}_i^n + \bar{Z}_i^n|W_1, \ldots, W_{d-1}) - n\epsilon_n \]

\[ \leq \sum_{i=1}^{d} h(\bar{X}_i^n + \bar{Z}_i^n|W_1) + h(\bar{X}_i^n + \bar{Z}_i^n) - n\epsilon_n \]

\[ = H(W_d) + \sum_{i=1}^{d} h(\bar{X}_i^n + \bar{Z}_i^n|W_i) - n\epsilon_n \]

\[ = nR_d^n + \sum_{i=1}^{d} h(\bar{X}_i^n + \bar{Z}_i^n|W_i) - n\epsilon_n, \]

where (a) following the same arguments in Remark 2, and (b) follows by bounding \( h(\sum_{i=1}^{d} U_i^n) \) for \( U_i^n = \bar{X}_i^n + \bar{Z}_i^n \) as

\[ h(\sum_{i=1}^{d} U_i^n) = h(\sum_{i=1}^{d} U_i^n, U_{i+1}, \ldots, U_d) \]

\[ \leq h(U_i^n, U_{i+1}, \ldots, U_d) \]

\[ \leq \sum_{i=1}^{d} h(U_i^n) - h(\bar{Z}_{i+1}^n, \ldots, \bar{Z}_d^n|\bar{Z}_i^n) \]

\[ \leq \sum_{i=1}^{d} h(\bar{Z}_i^n) + h(\bar{Z}_i^n) \]

\[ = d \sum_{i=1}^{d} h(U_i^n) - n\epsilon_n + n\epsilon_n \]

(19)

where (a) because conditioning reduces entropy, and (b) and (c) because \( \bar{Z}_i^n \)'s are i.i.d. and independent from \( X_i^n \)'s. Therefore, from (18), we get,

\[ \sum_{i=2}^{d} h(\bar{X}_i^n + \bar{Z}_i^n|W_i) \geq n \sum_{i=1}^{d-1} R_i^n - n(d+1)\epsilon_n + n\epsilon_n \]

(20)

Now, starting in (18) from any user \( k \in \{1, 2, \ldots, K\} \), we get different \( K \) relations. Then, summing up all the \( K \) relations and then dividing by \( d-1 \) we finally get,

\[ \sum_{i=1}^{K} h(\bar{X}_i^n + \bar{Z}_i^n|W_i) \geq n \sum_{i=1}^{K} R_i^n - nK(d+1)\epsilon_n - nK\epsilon_n \]

(21)

Eventually, using the bound (22) in (17) we can get the upper bound on the secrecy sum rate as follows,

\[ \sum_{i=1}^{K} R_i^n \leq \frac{K}{d+1} \log(P) + \frac{K(d+1)\epsilon_n - nK\epsilon_n}{d+1}. \]

(23)

Therefore, using (23) and the definition in (4), taking the limits \( n \to \infty \) and \( P \to \infty \), we arrive at the following upper bound on the SDoF for any \( (K, d) \) regular topology,

\[ \text{SDoF}_{\text{regular}}(K, d) \leq \frac{K}{d+1}. \]

(24)

This completes the proof of Theorem 2.