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.

This work was supported by NSF Grant CCF 1559758.

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 $\lfloor K/(d+1) \rfloor$, 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 $\mathcal{R}_k$ as the connectivity set of the transmitter Tx_k, which contains all the receivers that it is connected to, and $\mathcal{T}_k$ as the connectivity set of the receiver Rx_k, which contains all the transmitters that it is connected to. For example, if $\mathcal{T}_k = \{3,7\}$, then receiver Rx_k is connected to the transmitters Tx_3 and Tx_7. We also

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 Rx_k, and Tx_k are given by $|\mathcal{T}_k|$, and $|\mathcal{R}_k|$, 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 $\mathcal{G}$ as, $\mathcal{G} \sim (\mathcal{T}_1, \ldots, \mathcal{T}_K, \mathcal{R}_1, \ldots, \mathcal{R}_K)$.

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

We assume the channel coefficients $H_{kj}(t)$ are generated from a continuous distribution and are assumed to be independent and identically distributed (i.i.d.) across time and users. We define $\mathbf{H}_{ki}^{(n)}$ as the $n \times n$ diagonal matrix, where its diagonal entries represent the channel coefficients from time $t = 1$ to $t = n$ between Tx_i and Rx_k. We also define $\Omega = \left\{ \mathbf{H}_{ki}^{(n)} : i \in \mathcal{T}_k \right\}_{k=1}^{K}$, as the set containing all non-zero channel coefficients between any transmitter/receiver pair. We assume that Ω is not available at any of the transmitters, while Ω is available causally at the receivers. The block received signal at Rx_k after a block of length n is given by,

$$Y_k^n = \sum_{i \in \mathcal{T}_k} \mathbf{H}_{ki}^{(n)} X_i^n + Z_k^n, \tag{1}$$

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 $(R_1^s(P,\mathcal{G}), R_2^s(P,\mathcal{G}), \ldots, R_K^s(P,\mathcal{G}))$ 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.,

$$\max_k \Pr(W_k \neq \hat{W}_k) \leq \epsilon_n. \tag{2}$$

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 $W_{-k}^K = \{W_1, \ldots, W_K\} \setminus W_k$,

$$I(W_{-k}^K; Y_k^n) \leq n\epsilon_n, \ \forall k. \tag{3}$$

We say a secrecy degree of freedom tuple $(d_1^s, \ldots, d_K^s)$ is achievable if for any achievable rate $R_i^s(P,\mathcal{G})$, we have $d_i^s = \lim_{P\to\infty} \frac{R_i^s(P,\mathcal{G})}{\log(P)}$. Therefore, the sum Secure Degree of Freedom (SDoF) for a partially connected interference channel given by a topology $\mathcal{G}$ is given as,

$$\text{SDoF}^{\mathcal{G}} = \sum_{i=1}^{K} d_i^s = \lim_{P\to\infty} \frac{\sum_{i=1}^{K} R_i^s(P,\mathcal{G})}{\log(P)}. \tag{4}$$

Notation: For any two sets $\mathcal{A}$ and $\mathcal{B}$, $\mathcal{A} \setminus \mathcal{B}$ is defined as all the elements in the set $\mathcal{A}$ that is not in the set $\mathcal{B}$, i.e., $\mathcal{A} \setminus \mathcal{B} = \{i : i \in \mathcal{A}, i \notin \mathcal{B}\}$. 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 Rx_i.

III. Main Results and Discussions

We first state two important lemmas, which help in understanding when 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)*
For any receiver Rx_i, a positive secure degree of freedom can be achieved, i.e., $d_i^s > 0$, if $\forall j \in \mathcal{R}_i \setminus \{i\}$, the following condition is satisfied,

$$\mathcal{T}_j \setminus \mathcal{T}_i \neq \{\phi\}. \tag{5}$$

Proof: For secure communication to Rx_i, one possible approach is to employ artificial noise injection and interference avoidance. To this end, when Tx_i transmits to Rx_i, then other transmitters can send artificial noise in order to immerse the signal seen at every unintended receiver connected to Tx_i, i.e., for $j \in \mathcal{R}_i \setminus \{i\}$, we should have $\mathcal{T}_j \neq \{\phi\}$. 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 Rx_i, then the jamming signals are received at Rx_i as well. Therefore, the chosen protecting transmitters should not be connected to Rx_i, i.e., not in $\mathcal{T}_i$, otherwise they will immerse the intended reception. Therefore, the secrecy condition for a single user to transmit becomes $\mathcal{T}_j \setminus \mathcal{T}_i \neq \{\phi\}, \forall j \in \mathcal{R}_i \setminus \{i\}$. Whenever the above condition is satisfied, a positive secure degree of freedom is achievable for receiver Rx_i through artificial noise injection and interference avoidance. ■

Lemma 2. *(Multiple simultaneous secrecy transmission)*
For a set of k receivers labeled as $\{\mathsf{Rx}_{i_1}, \ldots, \mathsf{Rx}_{i_k}\}$, positive k-tuples secure degrees of freedom can be achieved simultaneously, i.e., $d_{i_1}^s, \ldots, d_{i_k}^s > 0$, if $\forall j \in (\mathcal{R}_{i_1} \setminus \{i_1\}) \cup (\mathcal{R}_{i_2} \setminus \{i_2\}) \ldots \cup (\mathcal{R}_{i_k} \setminus \{i_k\})$, the following condition is satisfied,

$$\mathcal{T}_j \setminus (\mathcal{T}_{i_1} \cup \mathcal{T}_{i_2} \ldots \cup \mathcal{T}_{i_k}) \neq \{\phi\}. \tag{6}$$

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 Rx_j connected to any of the k transmitters, i.e., $j \in (\mathcal{R}_{i_1} \setminus \{i_1\}) \cup (\mathcal{R}_{i_2} \setminus \{i_2\}) \ldots \cup (\mathcal{R}_{i_k} \setminus \{i_k\})$, we have $\mathcal{T}_j \neq \{\phi\}$. However, we need not to affect any of the k intended receptions, i.e., the protecting transmitters are not in $(\mathcal{T}_{i_1} \cup \mathcal{T}_{i_2} \ldots \cup \mathcal{T}_{i_k})$, 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.

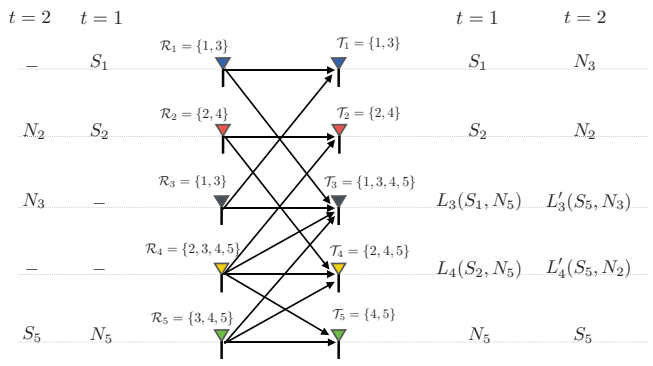

Fig. 1. Irregular partially connected interference network with $K=5$ transmitter/receiver pairs. Applying Lemma 1, Only Rx_1, Rx_2, and Rx_5 can securely send their messages S_1, S_2, and S_5, respectively. Applying Lemma 2, we can even send S_1, and S_2 securely in the same time.

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 $\mathcal{T}_i=\mathcal{R}_i=\{1,2,3,4\}$, $\forall i\in\{1,2,3,4\}$. Applying Lemma 1 for every transmitter Tx_i, $i\in\{1,2,3,4\}$, we have $\mathcal{T}_j\setminus\mathcal{T}_i=\{\phi\}$, $\forall j\neq i$. Therefore, if any transmitter Tx_k, $k\neq i$, sends artificial noise N_k to immerse S_i at Rx_j, it will also hide S_i at the intended receiver Rx_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 $I(W_k;Y_k^n)=I(W_k;Y_j^n)\leq n\epsilon_n$, $\forall j\neq k$, which means that the decodability constraint contradicts with the secrecy requirement, i.e., $d_k^s=0$, $\forall k$, 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 Tx_1 to reliably transmit a secure message, say S_1, to Rx_1, it must be protected from Rx_3 which will also receive S_1, i.e., $3\in\mathcal{R}_1$. However, we notice that $\mathcal{T}_3\setminus\mathcal{T}_1=\{4,5\}\neq\{\phi\}$ which means according to Lemma 1 that either Tx_4, or Tx_5 can protect S_1 by sending artificial noise N_4, or N_5, respectively, which is not seen by Rx_1.

– In order for Tx_3 to transmit a secure message, say S_3, to Rx_3, it must be protected from Rx_1 which will also receive S_3, i.e., $1\in\mathcal{R}_3$. However, we notice that $\mathcal{T}_1\setminus\mathcal{T}_3=\{\phi\}$ which means according to Lemma 1 that there is no transmitter that can protect S_3 at Rx_1 without affecting Rx_3.

– Doing the same analysis for the remaining users, we conclude that only transmitters Tx_1, Tx_2, and Tx_5 can transmit securely to the corresponding receivers, i.e., $d_i^s>0$ for $i=1,2,5$, while Tx_3, and Tx_4 can not transmit without revealing their messages to other unintended receivers, i.e., $d_3^s=d_4^s=0$.

• We next apply Lemma 2 to this example to understand when more than one user can transmit simultaneously.

– Taking the pair of transmitters (Tx_1,Tx_2), in order to transmit two messages securely, say (S_1,S_2), they must be protected at receivers Rx_3, and Rx_4 ($3\in\mathcal{R}_1$, $4\in\mathcal{R}_5$). Using Lemma 2, we notice that $\mathcal{T}_3\setminus(\mathcal{T}_1\cup\mathcal{T}_2)=\{5\}$, and $\mathcal{T}_4\setminus(\mathcal{T}_1\cup\mathcal{T}_2)=\{5\}$. Therefore, by sending artificial noise N_5 from Tx_5 it will hide both S_1, and S_2 at Rx_3, and Rx_4 without affecting the intended receptions at Rx_1, and Rx_2.

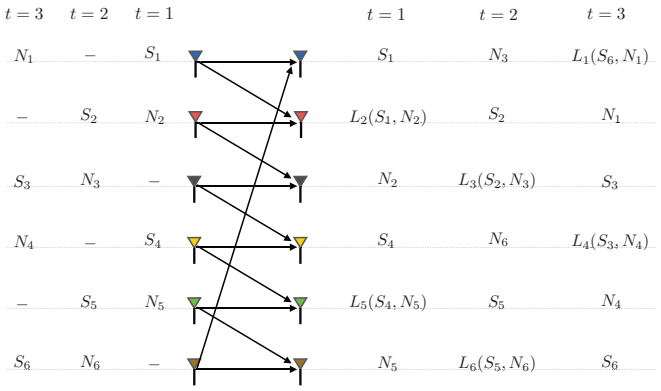

Fig. 2. A $(6,2)$ Regualr network with $K=5$ transmitter/receiver pairs, and $d=2$ node degrees. Every transmission affects the next two receivers, and therefore, we only send $\frac{6}{3}=2$ symbols per time slot.

– Taking the pair of transmitters (Tx_1,Tx_5), in order to transmit two messages securely, say (S_1,S_5), they must be protected at receivers Rx_3, and Rx_4 ($3\in\mathcal{R}_1$, $\{3,4\}\in\mathcal{R}_5$). Using Lemma 2, we notice that $\mathcal{T}_3\setminus(\mathcal{T}_1\cup\mathcal{T}_5)=\{\phi\}$, and $\mathcal{T}_4\setminus(\mathcal{T}_1\cup\mathcal{T}_5)=\{2\}$. Therefore, even if we can protect the messages at Rx_4 by sending artificial noise from Tx_2, it is impossible to protect them at Rx_3 without affecting the intended reception at Rx_1, or Rx_5.

– Similarly, it is not feasible to send secure messages simultaneously for the remaining pair (Tx_2,Tx_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 Rx_1 and Rx_2, respectively, and one secure message S_5 to Rx_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 Tx_1 is sending a symbol S_1 to Rx_1, it will prevent the next $d-1=1$ users (here Rx_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 Tx_2 to immerse S_1 at Rx_2 without affecting the reception at Rx_1. However, N_2 is also received at Rx_3 preventing it from receiving S_3 while Rx_1 is receiving, and we keep Tx_3 silent.

• While Tx_1 is sending S_1, let Tx_4 send a symbol S_4 to Rx_4. This transmission will prevent the next transmitter Tx_5 from sending a symbol to Rx_5. Instead, Tx_5 will send artificial

noise N_5 to immerse S_4 at Rx_5, which will prevent Rx_6 from receiving S_6 while Rx_4 is receiving, and we keep Tx_6 silent.

• In the same way, Tx_2, and Tx_5 (also Tx_3, and Tx_6) can send two secure symbols simultaneously, while Tx_3, and Tx_6 (Tx_1, and Tx_4) are sending artificial noise to protect the reception at unintended receivers Rx_3, and Rx_6 (Rx_1, and Rx_4).

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

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 Tx_k, the connectivity set including direct links to receivers is given by,

$$\mathcal{R}_k = \{k, k+1, \ldots, k+d-1\} (\text{mod } \mathsf{K}). \tag{7}$$

Equivalently, for any receiver Rx_k, the connectivity set is,

$$\mathcal{T}_k = \{k, k-1, \ldots, k-d+1\} (\text{mod } \mathsf{K}). \tag{8}$$

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 Tx_i and Rx_i, say S_i, is also received at the next $d-1$ users, $\{\mathsf{Rx}_{i+1}, \ldots \mathsf{Rx}_{i+d-1}\}$. For secure transmission, Tx_{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 Rx_{i+d}. To summarize: "Each secure transmission at Rx_i will affect the next d receivers, $\{\mathsf{Rx}_{i+1}, \ldots \mathsf{Rx}_{i+d}\}$, preventing them from receiving their own symbols". Therefore, for K transmitter/receiver pairs, we can send $\lfloor \frac{K}{d+1} \rfloor$ messages in one channel use. Starting from Tx_i, the following transmitters can transmit in the same time $\{\mathsf{Tx}_i, \mathsf{Tx}_{i+d+1}, \ldots, \mathsf{Tx}_{i+\mu(d+1)}\}$[1], where $\mu = \lfloor \frac{K}{d+1} \rfloor$. In order to symmetrize the scheme, we repeat this session K times for $i \in \{1, \ldots, K\}$. As a result we can send $K\lfloor \frac{K}{d+1} \rfloor$ total symbols in K channel uses, achieving $\text{SDoF} = \lfloor \frac{K}{d+1} \rfloor$.

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,*

$$\mathit{SDoF}^{\mathit{regular}}(K, d) \geq \begin{cases} \left\lfloor \frac{K}{d+1} \right\rfloor, & \forall d \neq 1 \\ K, & d = 1 \end{cases} \tag{9}$$

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,*

$$\mathit{SDoF}^{\mathit{regular}}(K, d) \leq \begin{cases} \frac{K}{d+1}, & \forall d \neq \{1, K\} \\ K, & d = 1 \\ 0, & d = K \end{cases} \tag{10}$$

[1]All the indexes in this paper are modulo K

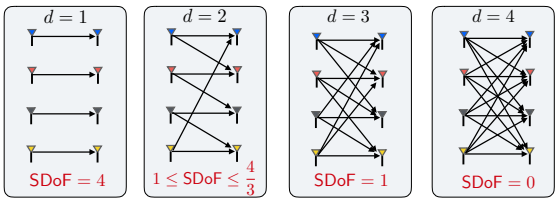

Fig. 3. Regular interference network with $K = 4$ transmitter/receiver pairs, and different node degrees. Applying Theorems 1 and 2, we can get the bounds on SDoF for different node degrees, which is found optimal for $d \in \{1, 3, 4\}$, while for $d = 2$ we have a gap of $\frac{1}{3}$.

The proof of Theorem 2 can be found in Appendix A. We notice that this bound is tight for $\frac{K}{d+1}$ is integer and that the gap is at most $\frac{d}{d+1} < 1$ for any value of K. The case $d = 1$ is trivial which is the interference free K parallel channels, where we can optimally achieve $\text{SDoF} = K$. When $d = K$, $\text{SDoF} = 0$ optimally as discussed in Example 1. In order to study the gap between the bounds found in Theorems 1 and 2, we consider the case of $K = 4$ transmitter/receiver pairs, with any value of node degree $d = \{1, 2, 3, 4\}$. As shown in Figure 3, we have tight bounds for node degrees $d = \{1, 3, 4\}$. In the next example, we study the case when $d = 2$ in order to close the gap $1 \leq \text{SDoF}^{\text{regular}}(4, 2) \leq \frac{4}{3}$.

Example 4 (Closing the Gap)**.** Consider a modification of our general scheme as in Figure 4. In the first slot, Tx_1 sends a secure message S_1 to Rx_1. In order to immerse S_1 at Rx_2, Tx_2 sends artificial noise N_2. Let Tx_3 send an artificial noise N_3 while the secure transmission of Tx_1 is taking place. This transmission will not affect the decodability at Rx_1, and will provide N_3 as a side information to Rx_4 without revealing N_3 to Rx_3 (receives $L_3(N_2+N_3)$). Therefore, N_3 still can be used to protect a message coming from Tx_2 at receiver Rx_3.

In the second slot, we send N_1 while the secure transmission of S_3 to Rx_3 is taking place. In a similar way, N_1 is received at Rx_2 as a useful side information. Using the side information N_1, and N_3 available at Rx_2, and Rx_4, respectively, we can securely send in the third slot two symbols, S_2, and S_4, simultaneously for Rx_2, and Rx_4, respectively. For decoding, Rx_2 uses $L'_2(S_1 + N_1)$ and the side information N_1 to get S_1, while Rx_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 $\text{SDoF}^{\text{regular}}(4, 2) = \frac{4}{3}$, 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 $\text{SDoF} = \lfloor \frac{K}{d+1} \rfloor$. We also derived an information theoretic upper bound, $\text{SDoF} \leq \frac{K}{d+1}$, 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.

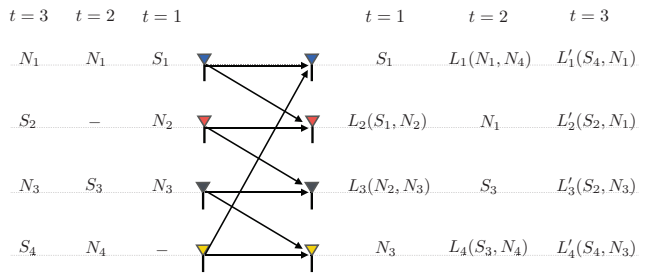

Fig. 4. Regular interference network with $K=4$ transmitter/receiver pairs, and node degree $d=2$. We modify our scheme such that Rx_2, and Rx_4 can get side information N_1, and N_3, respectively, which can be used to send two symbols at $t=3$, achieving SDoF $=\frac{4}{3}$.

REFERENCES

[1] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] S. Ulukus and A. Yener, "Wireless Physical Layer Security: Lessons Learned from Information Theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[3] R. Tandon, P. Piantanida, and S. Shamai, "On Multi-User MISO Wiretap Channels with Delayed CSIT," in *Proceedings of the EEE International Symposium on Information Theory (ISIT), Honolulu, HI*, 2014.

[4] J. Xie and S. Ulukus, "Secure Degrees of Freedom of the Gaussian Wiretap Channel with Helpers and No Eavesdropper CSI: Blind Cooperative Jamming," in *Proceedings of the Conference on Information Sciences and Systems (CISS), Baltimore, MD*, Mar. 2013.

[5] T. Liu and P. Mukherjee and S. Ulukus and S. Lin and Y. Hong, "Secure Degrees of Freedom of MIMO Rayleigh Block Fading Wiretap Channels With No CSI Anywhere," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2655–2669, May 2015.

[6] 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, May 2015.

[7] S. A. Jafar, "Topological interference management through index coding," *IEEE Transactions on Information Theory*, vol. 60, no. 1, pp. 529–568, Jan. 2014.

[8] N. Naderializadeh and A. S. Avestimehr, "Interference networks with no csit: Impact of topology," *IEEE Transactions on Information Theory*, vol. 61, no. 2, pp. 917–938, Febl. 2015.

[9] X. Yi and D. Gesbert, "Topological interference management with transmitter cooperation," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6107–6130, Nov. 2015.

APPENDIX A
PROOF OF THEOREM 2

Using Remark 1, the n-length block received signal at Rx_k in a (K,d) regular network can be written as $Y_k^n = \sum_{i=k-d+1}^{k} \mathbf{H}_{ki}^{(n)} X_i^n + Z_k^n$. We first bound the secure rate R_d^s for Rx_d as follows,

$$nR_d^s = H(W_d) = H(W_d|\Omega) = I(Y_d^n; W_d|\Omega) + H(W_d|Y_d^n,\Omega)$$
$$\overset{(a)}{\leq} I(Y_d^n; W_d|\Omega) + n\epsilon_n = h(Y_d^n|\Omega) - h(Y_d^n|W_d,\Omega) + n\epsilon_n, \tag{11}$$

where (a) is due to Fano's inequality using (2), and Ω denotes the global CSI as defined in Section II. Since Ω 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 $h(Y_d^n|W_d)$:

$$h(Y_d^n|W_d) \geq h(Y_d^n|W_d, X_d^n) \overset{(a)}{=} h(Y_d^n|X_d^n)$$
$$= h\left(\sum_{i=1}^{d} \mathbf{H}_{di}^{(n)} X_i^n + Z_d^n \,\middle|\, X_d^n\right) = h\left(\sum_{i=1}^{d-1} \mathbf{H}_{di}^{(n)} X_i^n + Z_d^n\right), \tag{12}$$

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

$$h(L_\ell) = h(L_\ell|W_\ell) + H(W_\ell) - H(W_\ell|L_\ell)$$
$$\overset{(a)}{\geq} h(L_\ell|X_\ell^n) + H(W_\ell) - H(W_\ell|L_\ell)$$
$$\overset{(b)}{\geq} h(L_{\ell-1}) + nR_\ell^s - n\epsilon_n, \tag{13}$$

where (a) follows from the Markov chain $W_d \to X_d^n \to Y_d^n$, and (b) by noting that $h(L_\ell|X_\ell^n) = h(L_{\ell-1})$ by removing the contribution of X_ℓ^n from L_ℓ 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_ℓ must be decoded from Y_ℓ^n. Now, if we assume a genie providing clean symbols X_i, $i \in \{K+(\ell-d+1),\ldots,K\}$ to Rx_ℓ[2], then it can remove the interference caused by those symbols from Y_ℓ^n and get a more clean version $\widetilde{Y}_\ell^n = \sum_{i=1}^{\ell} \mathbf{H}_{\ell i}^{(n)} X_i^n + Z_\ell^n$. If Y_ℓ^n is sufficient to decode W_ℓ, then $\widetilde{Y}_\ell^n$ is also sufficient to decode W_ℓ. Since $\widetilde{Y}_\ell^n$ is statistically equivalent to L_ℓ because no CSI is available at the transmitters, then L_ℓ is also sufficient to decode W_ℓ, 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,

$$h(Y_d^n|W_d) \geq h(L_{d-1}) \geq h(L_{d-2}) + nR_{d-1}^s - n\epsilon_n$$
$$\vdots$$
$$\geq h(L_1) + n\sum_{i=2}^{d-1} R_i^s - n(d-2)\epsilon_n$$
$$\overset{(a)}{\geq} n\sum_{i=1}^{d-1} R_i^s + h(\widetilde{X}_1^n + \widetilde{Z}^n|W_1) - n(d-1)\epsilon_n, \tag{14}$$

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

Remark 3. *We first define $\widetilde{X}_1^n = \widetilde{\boldsymbol{H}}^{(n)} X_1^n$, for any $\widetilde{\boldsymbol{H}}^{(n)} \in \Omega$, then we note that $\widetilde{X}_1^n + \widetilde{Z}^n$ is statistically equivalent to $L_1 = \boldsymbol{H}_{d1}^{(n)} X_1^n + Z_d^n$ due to the no CSIT assumption, where $\widetilde{Z}^n$ is independent of and identically distributed as Z_d^n. Therefore, we can write*

$$h(L_1) = h(L_1|W_1) + H(W_1) - H(W_1|L_1)$$
$$\overset{(b)}{\geq} h(\widetilde{X}_1^n + \widetilde{Z}^n|W_1) + nR_1^s - n\epsilon_n, \tag{15}$$

[2]Note that for $\ell \in \{1,\ldots,d-1\}$, we have $\ell - d + 1 (\mathsf{mod}\ K) = K + (\ell - d + 1) < K$.

where (b) follows from the arguments similar to Remark 2. Now plugging (14) in (11), we obtain

$$n\sum_{i=1}^{d} R_i^s \leq h(Y_d^n) - h(\widetilde{X}_1^n + \widetilde{Z}^n|W_1) + nd\epsilon_n. \tag{16}$$

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,

$$\begin{aligned}
nd\sum_{i=1}^{K} R_i^s &\leq \sum_{i=1}^{K} h(Y_d^n) - \sum_{i=1}^{K} h(\widetilde{X}_i^n + \widetilde{Z}^n|W_i) + nKd\epsilon_n \\
&\overset{(a)}{=} nK\log(P) - \sum_{i=1}^{K} h(\widetilde{X}_i^n + \widetilde{Z}_1^n + \cdots + \widetilde{Z}_d^n|W_i) + nKd\epsilon_n \\
&\leq nK\log(P) - \sum_{i=1}^{K} h(\widetilde{X}_i^n + \widetilde{Z}_i^n|W_i) + nKd\epsilon_n,
\end{aligned} \tag{17}$$

where (a) follows by writing the noise $\widetilde{Z}^n$ as a sum of i.i.d. noises, $\widetilde{Z}^n = \widetilde{Z}_1^n + \cdots + \widetilde{Z}_d^n$, where the individual variances of each noise term are $1/d$ times the variance of $\widetilde{Z}^n$.

B. Confidentiality Constraint

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

$$\begin{aligned}
nR_d^s &\leq h(Y_d^n) - h(Y_d^n|W_d) + n\epsilon_n - I(Y_d^n; W_1, \ldots, W_{d-1}) \\
&\quad + I(Y_d^n; W_1, \ldots, W_{d-1}) \\
&\overset{(a)}{\leq} h(Y_d^n|W_1, \ldots, W_{d-1}) - h(Y_d^n|W_d) + 2n\epsilon_n \\
&\overset{(b)}{\leq} h(Y_d^n|W_1, \ldots, W_{d-1}) - n\sum_{i=1}^{d-1} R_i^s - h(\widetilde{X}_1^n + \widetilde{Z}^n|W_1) \\
&\quad + n(d+1)\epsilon_n \quad \leq \quad h(Y_d^n|W_1, \ldots, W_{d-1}) - n\sum_{i=1}^{d-1} R_i^s \\
&\quad - h(\widetilde{X}_1^n + \widetilde{Z}_1^n|W_1) \quad + n(d+1)\epsilon_n \\
&\overset{(c)}{\leq} \sum_{i=2}^{d} h(\widetilde{X}_i^n + \widetilde{Z}_i^n|W_i) + nR_d^s - n\sum_{i=1}^{d-1} R_i^s \\
&\quad + n(d+1)\epsilon_n - no(\log(P))
\end{aligned} \tag{18}$$

where (a) follows from the confidentiality 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,

$$\begin{aligned}
h(Y_d^n|W_1, \ldots, W_{d-1}) &\overset{(a)}{=} h\left(\sum_{i=1}^{d} \widetilde{X}_i^n + \widetilde{Z}^n|W_1, \ldots, W_{d-1}\right) \\
&= h\left(\sum_{i=1}^{d} (\widetilde{X}_i^n + \widetilde{Z}_i^n)|W_1, \ldots, W_{d-1}\right) \\
&\overset{(b)}{\leq} \sum_{i=1}^{d} h\left(\widetilde{X}_i^n + \widetilde{Z}_i^n|W_1, \ldots, W_{d-1}\right) - no(\log(P)) \\
&= \sum_{i=1}^{d-1} h\left(\widetilde{X}_i^n + \widetilde{Z}_i^n|W_i\right) + h(\widetilde{X}_d^n + \widetilde{Z}_d^n) - no(\log(P)) \\
&= H(W_d) + \sum_{i=1}^{d} h\left(\widetilde{X}_i^n + \widetilde{Z}_i^n|W_i\right) - no(\log(P)) \\
&= nR_d^s + \sum_{i=1}^{d} h\left(\widetilde{X}_i^n + \widetilde{Z}_i^n|W_i\right) - no(\log(P)),
\end{aligned} \tag{19}$$

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

$$\begin{aligned}
h\left(\sum_{i=1}^{d} U_i^n\right) &= h\left(\sum_{i=1}^{d} U_i^n, U_2^n, \ldots, U_d^n\right) \\
&\quad - h\left(U_2^n, \ldots, U_d^n \middle| \sum_{i=1}^{d} U_i^n\right) \\
&\overset{(a)}{\leq} h\left(U_1^n, U_2^n, \ldots, U_d^n\right) \\
&\quad - h\left(U_2^n, \ldots, U_d^n \middle| \sum_{i=1}^{d} U_i^n, \widetilde{X}_1^n, \ldots, \widetilde{X}_d^n\right) \\
&\overset{(b)}{=} \sum_{i=1}^{d} h\left(U_i^n\right) - h\left(\widetilde{Z}_2^n, \ldots, \widetilde{Z}_d^n \middle| \widetilde{Z}^n\right) \\
&\overset{(c)}{=} \sum_{i=1}^{d} h\left(U_i^n\right) - \sum_{i=1}^{d} h(\widetilde{Z}_i^n) + h\left(\widetilde{Z}^n\right) \\
&= \sum_{i=1}^{d} h\left(U_i^n\right) - no(\log(P)),
\end{aligned} \tag{20}$$

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

$$\sum_{i=2}^{d} h(\widetilde{X}_i^n + \widetilde{Z}_i^n|W_i) \geq n\sum_{i=1}^{d-1} R_i^s - n(d+1)\epsilon_n + no(\log(P)). \tag{21}$$

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,

$$\begin{aligned}
&\sum_{i=1}^{K} h(\widetilde{X}_i^n + \widetilde{Z}_i^n|W_i) \\
&\geq n\sum_{i=1}^{K} R_i^s - \frac{nK(d+1)\epsilon_n - nKo(\log(P))}{d-1}.
\end{aligned} \tag{22}$$

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

$$\sum_{i=1}^{K} R_i^s \leq \frac{K}{d+1}\log(P) + \frac{Kd(d+1)\epsilon_n - Ko(\log(P))}{d^2-1}. \tag{23}$$

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,

$$\text{SDoF}^{\text{regular}}(K, d) \leq \frac{K}{d+1}. \tag{24}$$

This completes the proof of Theorem 2.