On Secure Topological Interference Management for Half-rate-feasible Networks

Jean de Dieu Mutangana   Ravi Tandon
Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ, USA
E-mail: {*mutangana, tandonr*}@email.arizona.edu

***Abstract*— The topological interference management (TIM) problem is a framework for studying partially connected interference networks with no channel state information at transmitters (CSIT), except network topology. TIM is a more pragmatic setting as CSIT is often available imperfectly, or may not be available at all. In this paper, we study the TIM problem with confidential messages, denoted in short by the *secure TIM* (STIM) problem. More specifically, we focus on the STIM problem for *half-rate-feasible* (HRF) networks. Half-rate-feasible networks are a class of partially connected interference networks whose sum degrees of freedom (DoF) have been characterized by $K/2$, without any secrecy constraints. The main contribution of this paper is as follows: We design achievable schemes for HRF networks subject to secrecy constraints, and present a lower bound on the secure degrees of freedom (SDoF). To this end, we first show the necessity of classifying HRF networks into two sub-categories based on some properties of the underlying network topology. As it turns out, the division of HRF networks into these sub-categories is critical for the design of secure transmission schemes. We then leverage the underlying topological properties along with ideas from secure interference alignment (SIA) in order to design achievable schemes for both subclasses of HRF networks.**

I. Introduction

Significant progress has been made on understanding the capacity of multi-user wireless interference networks under the assumption of *full connectivity*, with or without secrecy constraints [1]–[6]. Moreover, as indicated in [1] and related works therein, the majority of the results on fully connected networks have been derived under the assumption that channel state information is available to the transmitters (CSIT). However, in practice, the inherent randomness, path loss, and fading properties of the wireless medium naturally lead to *partial connectivity*, where each receiver is only connected to a subset of transmitters and vice versa. Furthermore, in practice, CSIT may be delayed/noisy, statistical in nature, or even completely absent. The topological interference management (TIM) problem is a framework for studying partially connected interference networks, where only the network topology is known to the transmitters [7]–[9]. The TIM problem is also closely related to the index coding problem [7].

In this paper, we study the *secure* TIM (STIM) problem, an important avenue which has largely remained unexplored. We first observe that for a fully connected interference network with i.i.d. channel gains, with no CSIT, the secure degrees of freedom (SDoF) is in fact *zero*. This is due to the fact that all receivers are statistically equivalent, and thus decodability and confidentiality constraints are in direct conflict. Thus, the nontrivial setting is that of *Partially connected networks*. Motivated by the above discussion, we focus on the following fundamental question: Can we achieve positive SDoF for K-user partially connected interference networks without any CSIT, except topological knowledge?

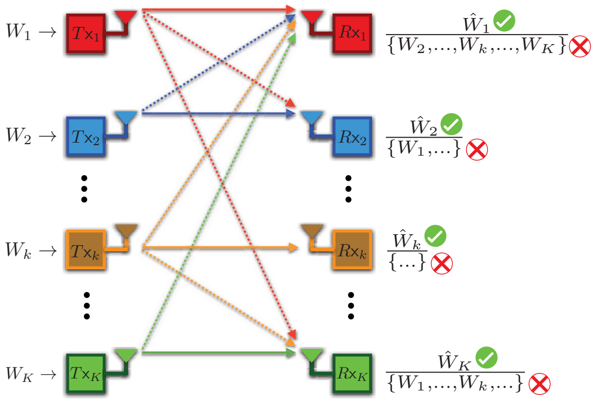

Fig. 1: STIM problem, where each user Rx_k should only decode its dedicated message W_k and the remaining messages must remain confidential.

In particular, we focus on the STIM problem for the so-called *half-rate-feasible* (HRF) networks. HRF networks are a class of partially connected interference networks which are well understood without secrecy constraints. In particular, it was shown in [7], that the optimal sum degrees of freedom (DoF) of HRF networks is $K/2$, without any secrecy constraints [7]. Our main contribution in this paper is to show that the answer to the above question is in fact affirmative for HRF networks. To achieve this, we divide the class of HRF networks into two subclasses based on interplay between the interference sets and the alignment sets resulting from the network topology. We then devise two different secure transmission schemes, one for each subclass, by leveraging ideas from secure interference alignment (SIA) and obtain lower bounds on SDoF for both categories of HRF networks. The contrast from the non-secure setting is that the achievable SDoF for HRF networks is dependent on topology (unlike the optimal DoF of $K/2$ which does not depend on the topology).

II. System Model for STIM

We consider a K-user single-input single-output (SISO) partially connected network with confidential messages as

This work was supported by NSF grants CNS-1715947 and CAREER-1651492.

978-1-7281-5089-5/20/$31.00 ©2020 IEEE

depicted by Fig. 1. We use $\mathcal{T}_k$ to denote the set of *all transmitters* that are *connected* to Receiver k, for $k \in \{1, 2, \dots, K\}$. Similarly, we use $\mathcal{R}_k$ to denote the set of *all receivers* that are *connected* to Transmitter k, for $k \in \{1, 2, \dots, K\}$. Therefore, the network topology is described by $\mathcal{G} = (\mathcal{T}_1, \mathcal{T}_2, \dots, \mathcal{T}_K, \mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_K)$. We also use $\mathcal{I}_k$ to represent the set of signals from transmitters that *cause interference* at Receiver k. For a given topology $\mathcal{G}$, the signal received at Receiver k at time t is given by

$$Y_k(t) = \sum_{i \in \mathcal{T}_k} h_{ki}(t) X_i(t) + Z_k(t), \tag{1}$$

where $h_{ki}(t)$ represents the channel coefficient between transmitter i to receiver k at time t, assumed to be i.i.d. and drawn from a continuous distribution. $Z_k(t)$ is the zero-mean unit-variance complex Gaussian channel noise. $X_i(t)$ is the signal sent by transmitter i under power constraint $\mathbb{E}(||X_i(t)||^2) \le P$, where P is the average transmit power.

CSIT/CSIR assumptions: Within STIM framework, there is no CSIT, except that the transmitters possess the network channel topology $\mathcal{G}$. For coherent detection, we assume that each Receiver k knows the channel coefficients corresponding to the set of transmitters in $\mathcal{T}_k$ and the network topology $\mathcal{G}$.

Transmitter k wants to send a message W_k (uniformly distributed in $\mathcal{W}_k = \{1, 2, \dots, 2^{nR_k}\}$) to the kth receiver. A secure rate of communication $R_k(P, \mathcal{G}) = \frac{\log(|\mathcal{W}_k|}{n}$ is achievable, if there exist sequence of encoding/decoding functions that, for $n \to \infty$ and $\epsilon \to 0$, satisfy the next two constraints:

Definition 1 *(Decodability Constraint):*

$$Pr[W_k \neq \hat{W}_k] \le \epsilon. \tag{2}$$

Definition 2 *(Secrecy Constraint):*

$$\frac{1}{n} I(\mathcal{W}_{\{k\}}; Y_k^{(n)} | W_k) \le \epsilon, \tag{3}$$

where $\mathcal{W}_{\{k\}} = \mathcal{W} \backslash \{W_k\}$, $\mathcal{W} = \{W_1, W_2, \dots, W_K\}$, and $Y_k^{(n)}$ is the observed signal at the kth receiver over the n-length transmission block.

The sum secrecy capacity C_s is defined as the supremum of all achievable sum secure rates $R_s = \sum_{k=1}^{K} R_k(P, \mathcal{G})$.

Definition 3 *(SDoF): We define sum secure degrees of freedom (SDoF) as the pre-log of the sum secrecy capacity*

$$\mathsf{SDoF} = \lim_{P \to \infty} \frac{C_s}{\log(P)}. \tag{4}$$

III. Half-rate-feasible (HRF) Networks

Consider the composite messages set $\mathcal{W} = \{W_1, W_2, \dots, W_K\}$, the interference message sets $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_K$ respectively seen at the K receivers, and the union set $\mathcal{I} = \{\mathcal{I}_1 \cup \mathcal{I}_2 \cup \dots \cup \mathcal{I}_K\}$. Moreover, consider the composite set $\mathcal{W}_{\{-\mathcal{I}\}} = \mathcal{W} \backslash \mathcal{I}$ of all messages that are not seen as interference at any other (unintended) receivers, i.e., only seen at the intended receivers. We can define an alignment set $\mathcal{A}_j$, for $j \in \{1, 2, \dots, N\}$, in *two ways:*

Definition 4 *(Alignment Set): 1) For messages that belong to the set $\mathcal{I}$, an alignment set is any set consisting of a union of one or more of the above K interference sets (e.g., say r sets, for $1 \le r \le K$) that can be aligned together along a unique direction in order to affect decodability of its elements at one or more receivers where its elements are observed [10]. 2) For any other messages in the network that don't belong to $\mathcal{I}$, i.e., the messages that belong to the set $\mathcal{W}_{\{-\mathcal{I}\}}$, an alignment is any set consisting of one or more of these messages that can be aligned along a unique direction in order to affect their decodability only at their respectively intended receivers.*

We now define related parameters: 1) $I \le N$ is the number of alignment sets which are a union of one or more interference sets, i.e., when $\mathcal{A}_j = \bigcup_{(r)} \mathcal{I}_i^{(r)}$ for $1 \le r \le K$. 2) $\mathcal{C}_j(r) = \{$Set of transmitters for the elements in $\mathcal{A}_j = \bigcup_{(r)} \mathcal{I}_i^{(r)} : |C_j(r) \cap \mathcal{I}_i^{(r)}| \ge 1\}, \forall\, r$, and 3) $Q_j = \min_r |C_j(r)|$.

Definition 5 *(No Internal Conflict): Messages belonging to the same alignment set $\mathcal{A}_j$ "have no internal conflicts," if they do not interfere at each other's desired destinations [7].*

This definition is clarified by Examples A and B below.

Example A. *($K = 6$-user STIM Network):* Consider the network shown by Fig. 2(a). We now illustrate how its alignment sets are created along with their internal conflict properties.

As it can be directly observed from Fig. 2(a) and the resulting topology $\mathcal{G} = (\mathcal{T}_1, \mathcal{T}_2, \dots, \mathcal{T}_6, \mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_6)$, we have six interference sets $\mathcal{I}_1 = \{W_2\}$, $\mathcal{I}_2 = \{W_3, W_4, W_6\}$, $\mathcal{I}_3 = \{W_1, W_5\}$, $\mathcal{I}_4 = \{W_1, W_5\}$, $\mathcal{I}_5 = \{W_3, W_4, W_6\}$, and $\mathcal{I}_6 = \{W_1, W_5\}$ that are respectively seen at $K = 6$ receivers. We create the alignment sets using the following *search steps*:

Step 1: Consider any set $\mathcal{I}_k$, for $k \in \{1, 2, \dots, 6\}$. a) If the elements of $\mathcal{I}_k$ belong to any other interference set $\mathcal{I}_i$, for $i \neq k$ and $i \in \{1, 2, \dots, 6\}$, then create an alignment set $\mathcal{A}_j$ which is a union of $\mathcal{I}_k$ with all $r-1$ interference sets with a nonempty intersection with $\mathcal{I}_k$. E.g., $\mathcal{A}_1 = \{W_1, W_5\} = \{\mathcal{I}_3 \cup \mathcal{I}_4 \cup \mathcal{I}_6\}$ has $r = 3$ interference sets. $\mathcal{A}_2 = \{W_3, W_4, W_6\} = \{\mathcal{I}_2 \cup \mathcal{I}_5\}$ and has $r = 2$ sets. b) Otherwise, create an alignment set $\mathcal{A}_j = \mathcal{I}_k$. E.g., $\mathcal{A}_3 = \{W_2\}$ and has $r = 1$. Therefore, we have $I = 3$ unique alignment sets, i.e., those whose elements are seen as interference at one or more unintended receivers.

Step 2: Consider the composite set $\mathcal{W}_{\{-\mathcal{I}\}}$ of all messages that are not seen as interference at any other (unintended) receivers. a) If the set $\mathcal{W}_{\{-\mathcal{I}\}}$ is nonempty, then create an alignment set $\mathcal{A}_j = \mathcal{W}_{\{-\mathcal{I}\}}$. b) Otherwise, do nothing. We note that, for this Example, $\mathcal{W}_{\{-\mathcal{I}\}} = \mathcal{W} \backslash \mathcal{I} = \{\,\}$ because $\mathcal{W} = \mathcal{I} = \{\mathcal{I}_1 \cup \mathcal{I}_2 \cup \dots \cup \mathcal{I}_6\}$. Thus, we do nothing.

Therefore, as shown by Steps 1 and 2, we have a total of $N = 3$ unique alignment sets, namely $\mathcal{A}_1 = \{W_1, W_5\}$, $\mathcal{A}_2 = \{W_3, W_4, W_6\}$, and $\mathcal{A}_3 = \{W_2\}$. Here, we point out that $N = I$ for the current Example. This is not required in general. Moreover, note that none of the signals belonging to the same alignment set interfere at each other's desired destinations, i.e., there are *no internal conflicts*. For example, $W_1 \in \mathcal{A}_1$ does not interfere at W_5's desired destination (which is Receiver 5). Also, $W_5 \in \mathcal{A}_1$ does not interfere at W_1's desired destination (which is Receiver 1). This property applies to all three alignment sets of this Example.

Example B. *($K = 10$-user STIM Network):* Consider the net-

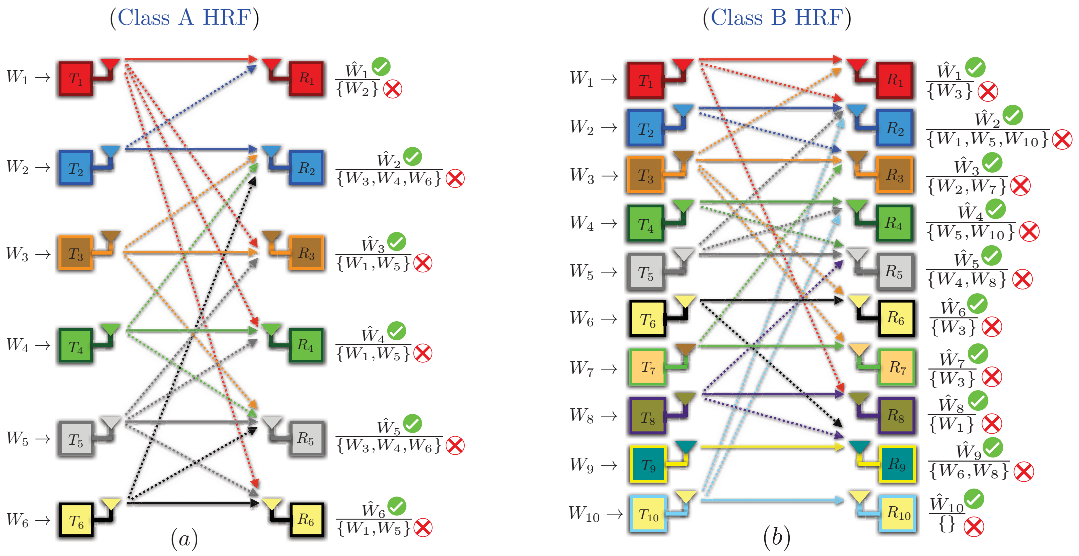
(Class A HRF)
$W_1 \rightarrow$ T_1
$W_2 \rightarrow$ T_2
$W_3 \rightarrow$ T_3
$W_4 \rightarrow$ T_4
$W_5 \rightarrow$ T_5
$W_6 \rightarrow$ T_6
R_1 $\hat{W}_1$ ✓ $\{W_2\}$ ✗
R_2 $\hat{W}_2$ ✓ $\{W_3,W_4,W_6\}$ ✗
R_3 $\hat{W}_3$ ✓ $\{W_1,W_5\}$ ✗
R_4 $\hat{W}_4$ ✓ $\{W_1,W_5\}$ ✗
R_5 $\hat{W}_5$ ✓ $\{W_3,W_4,W_6\}$ ✗
R_6 $\hat{W}_6$ ✓ $\{W_1,W_5\}$ ✗
(a)
(Class B HRF)
$W_1 \rightarrow$ T_1
$W_2 \rightarrow$ T_2
$W_3 \rightarrow$ T_3
$W_4 \rightarrow$ T_4
$W_5 \rightarrow$ T_5
$W_6 \rightarrow$ T_6
$W_7 \rightarrow$ T_7
$W_8 \rightarrow$ T_8
$W_9 \rightarrow$ T_9
$W_{10} \rightarrow$ T_{10}
R_1 $\hat{W}_1$ ✓ $\{W_3\}$ ✗
R_2 $\hat{W}_2$ ✓ $\{W_1,W_5,W_{10}\}$ ✗
R_3 $\hat{W}_3$ ✓ $\{W_2,W_7\}$ ✗
R_4 $\hat{W}_4$ ✓ $\{W_5,W_{10}\}$ ✗
R_5 $\hat{W}_5$ ✓ $\{W_4,W_8\}$ ✗
R_6 $\hat{W}_6$ ✓ $\{W_3\}$ ✗
R_7 $\hat{W}_7$ ✓ $\{W_3\}$ ✗
R_8 $\hat{W}_8$ ✓ $\{W_1\}$ ✗
R_9 $\hat{W}_9$ ✓ $\{W_6,W_8\}$ ✗
R_{10} $\hat{W}_{10}$ ✓ $\{\}$ ✗
(b)

Fig. 2: (a) Example A: $K = 6$-user *Class A HRF* Network. (b) Example B: $K = 10$-user *Class B HRF* Network.

work shown by Fig. 2(b). We now illustrate how its alignment sets are created along with their internal conflict properties.

As it can be directly observed from Fig. 2(b) and the resulting topology $\mathcal{G} = (\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_{10}, \mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_{10})$, we have ten interference sets $\mathcal{I}_1 = \{W_3\}$, $\mathcal{I}_2 = \{W_1, W_5, W_{10}\}$, $\mathcal{I}_3 = \{W_2, W_7\}$, $\mathcal{I}_4 = \{W_5, W_{10}\}$, $\mathcal{I}_5 = \{W_4, W_8\}$, $\mathcal{I}_6 = \{W_3\}$, $\mathcal{I}_7 = \{W_3\}$, $\mathcal{I}_8 = \{W_1\}$, $\mathcal{I}_9 = \{W_6, W_8\}$, and $\mathcal{I}_{10} = \{\ \}$ that are respectively seen at $K = 10$ receivers. We now create alignment sets using the following *search steps*:

Step 1: Consider any set $\mathcal{I}_k$, for $k \in \{1, 2, \ldots, 10\}$. a) If the elements of $\mathcal{I}_k$ belong to any other interference set $\mathcal{I}_i$, for $i \neq k$ and $i \in \{1, 2, \ldots, 10\}$, then create an alignment set $\mathcal{A}_j$ which is a union of $\mathcal{I}_k$ with all $r - 1$ interference sets with a nonempty intersection with $\mathcal{I}_k$. E.g., $\mathcal{A}_1 = \{W_1, W_5, W_{10}\} = \{\mathcal{I}_2 \cup \mathcal{I}_5 \cup \mathcal{I}_8\}$ and $r = 3$, $\mathcal{A}_3 = \{W_3\} = \{\mathcal{I}_1 \cup \mathcal{I}_6 \cup \mathcal{I}_7\}$ and $r = 3$, whereas $\mathcal{A}_4 = \{W_4, W_6, W_8\} = \{\mathcal{I}_5 \cup \mathcal{I}_9\}$ and $r = 2$. b) Otherwise, create an alignment set $\mathcal{A}_j = \mathcal{I}_k$. E.g., $\mathcal{A}_2 = \{W_2, W_7\} = \mathcal{I}_3$ and $r = 1$. Therefore, we have $I = 4$ unique alignment sets, i.e., whose elements are seen as interference at other (unintended) receivers.

Step 2: Consider the composite set $\mathcal{W}_{\{-\mathcal{I}\}}$ of all messages that are not seen as interference at any other (unintended) receivers. a) If the set $\mathcal{W}_{\{-\mathcal{I}\}}$ is nonempty, then create an alignment set $\mathcal{A}_j = \mathcal{W}_{\{-\mathcal{I}\}}$. b) Otherwise, do nothing. We note that, for the current Example, $\mathcal{W}_{\{-\mathcal{I}\}} = \mathcal{W} \backslash \mathcal{I} = \{W_9\}$ because $\mathcal{W} = \{W_1, W_2, \ldots, W_{10}\}$ whereas $\mathcal{I} = \{\mathcal{I}_1 \cup \mathcal{I}_2 \cup \cdots \cup \mathcal{I}_{10}\} = \{W_1, W_2, \ldots, W_8, W_{10}\}$. Thus, we create the alignment set $\mathcal{A}_5 = \mathcal{W}_{\{-\mathcal{I}\}} = \{W_9\}$.

Thus, for the current Example as shown by Steps 1 and 2, we have a total of $N = 5$ unique alignment sets, namely $\mathcal{A}_1 = \{W_1, W_5, W_{10}\}$, $\mathcal{A}_2 = \{W_2, W_7\}$, $\mathcal{A}_3 = \{W_3\}$, $\mathcal{A}_4 = \{W_4, W_6, W_8\}$, and $\mathcal{A}_5 = \{W_9\}$. We point out here that $N > I$. This is not required in general. Moreover, there are *no internal conflicts*. For example, $W_2 \in \mathcal{A}_2$ does not interfere at W_7's desired destination (which is Receiver 7). Also, $W_7 \in \mathcal{A}_2$ does not interfere at W_2's desired destination (which is Receiver 2). The same property applies to all five alignment sets of this Example.

Definition 6 *(Half-rate-feasible (HRF) Networks): A topology where all alignment sets $\mathcal{A}_j$, for $j \in \{1, 2, \ldots, N\}$, satisfy the above "no internal conflict" condition is said to form an HRF network. This is because, under such settings, as shown by [7] for the nonsecure TIM model, each Receiver k, for $k \in \{1, 2, \ldots, K\}$, can get "half the cake". That is, each of the K receivers achieves DoF of $\frac{1}{2}$ and hence, a sum DoF of $\frac{K}{2}$ for the whole network.*

Thus, both Examples A and B satisfy Definition 6, because each of them has alignment sets without any internal conflicts.

Although it was not necessary to do so for the nonsecure TIM model [7], for the STIM model of this paper, it is important to divide the class of HRF networks into two subclasses in order to achieve secure transmission:

Definition 7 *(Class A HRF: Alignment Sets with No Proper Interference Subsets): Consider a network with K interference sets $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_K$ and with N unique alignment sets $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_N$. A network topology is said to belong to "Class A HRF" networks, if none of its alignment sets has "proper subset", i.e., no subset besides its exact equals, among the interference sets.*

This definition is clarified by the running Example A.

Example A. *($K = 6$-user Class A HRF Network):* Consider the STIM network shown by Fig. 2(a), the six corresponding interference sets, and the resulting three alignment sets above. We observe the following fact: *None* of the alignment sets has a proper subset among interference sets. This is due to equalities $\mathcal{A}_1 = \mathcal{I}_3 = \mathcal{I}_4 = \mathcal{I}_6$, $\mathcal{A}_2 = \mathcal{I}_2 = \mathcal{I}_5$, and $\mathcal{A}_3 = \mathcal{I}_1$.

Definition 8 *(Class B HRF: Alignment Sets with Proper Interference Subsets): A network topology is said to belong to "Class B HRF" networks, if some of its alignment sets have "proper subsets" among the interference sets.*

This definition is clarified by the running Example B.

Example B. *($K = 10$-user Class B HRF Network):* Consider the STIM network shown by Fig. 2(b), the ten corresponding interference sets, and the resulting five alignment sets as derived above. We observe the following fact: *Some* of these alignment sets have proper subsets among the interference sets. More specifically, for the alignment set $\mathcal{A}_1 = \{W_1, W_5, W_{10}\}$, we have $\mathcal{I}_4 = \{W_5, W_{10}\} \subset \mathcal{A}_1$ and $\mathcal{I}_8 = \{W_1\} \subset \mathcal{A}_1$. Similarly, for $\mathcal{A}_4 = \{W_4, W_6, W_8\}$, we have $\mathcal{I}_5 = \{W_4, W_8\} \subset \mathcal{A}_4$ and $\mathcal{I}_9 = \{W_6, W_8\} \subset \mathcal{A}_4$. A slight difference to note here (and to be used later) is that the *subsets of $\mathcal{A}_1$ do not intersect*, whereas the *subsets of $\mathcal{A}_4$ do indeed intersect*.

IV. Main Results

A. Class A HRF Networks

The following Theorem, which is proved in Section V-A , states our result for *Class A HRF* networks.

Theorem 1. *Let N be the number of unique alignment sets, i.e., $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_N$, created from the elements of $\mathcal{I}$ and $\mathcal{W}_{\{-\mathcal{I}\}}$ according to the network topology $\mathcal{G}$ and Definition 4. The following SDoF is achievable for* Class A HRF *networks:*

$$\mathsf{SDoF} \geq \frac{K - I}{2}, \tag{5}$$

where $K = \sum_{j=1}^{N} |\mathcal{A}_j|$ and $I \leq N$ is the total number of alignment sets which are a union of one or more interference sets, i.e., when $\mathcal{A}_j = \bigcup_{(r)} \mathcal{I}_i^{(r)}$ for $1 \leq r \leq K$.

We next use the running Example A to highlight key principles behind Theorem 1, but first, we remark the following:

Remark 1. *SIA has three objectives: 1) Align interference signals in the smallest subspace possible at the unintended receivers. 2) Keep the desired signal separate from interference at the intended receiver. 3) Keep interference signals protected at unintended receivers while using minimal channel resources.*

Example A. *($K = 6$-user Class A HRF Network):*

Consider the STIM network shown by Fig. 2(a) and the corresponding alignment sets as derived in Section III. Moreover, the transmitters only know the network topology $\mathcal{G}$. Our goal is to show that SDoF of $\frac{3}{2}$ is achievable through our scheme.

Transmission: The proposed transmission for the Class A HRF network of the current Example entails *two conditions:*

(Condition 1): In order to guarantee *decodability* at each intended receiver, we need to align the $N = 3$ alignment sets $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$ respectively along three 2×1 sized *pairwise independent* vectors V_1, V_2, and V_3, i.e, any randomly chosen two are linearly independent. For example, we can choose $V_1 = [1 \;\; 0]^\top$, $V_2 = [0 \;\; 1]^\top$, and $V_3 = [1 \;\; 1]^\top$. At the *intended receive nodes*, this ensures that each desired signal occupies a separate subspace from that occupied by interference signals.

(Condition 2): In order to guarantee *secrecy* at the unintended receivers, we need to protect all the $I = 3$ alignment sets $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$, i.e., whose elements are seen as interference, by ensuring that each of them *contains one* artificial noise signal. For example, we can let Transmitters 2, 3, and 5 act as cooperative jammers by sending artificial noise signals to respectively protect the elements of $\mathcal{A}_3$, $\mathcal{A}_2$, and $\mathcal{A}_1$. We then let the remaining nodes 1, 4, and 6 send information signals.

SDoF Calculation: As a result of this transmission, each of the six receivers observes independent equations, and is thus able to solve for its intended signal– be it information or artificial noise, and not able to solve for any interference signals. Therefore, over $|V_1| = |V_2| = |V_3| = 2$ time slots, we can achieve SDoF of $\frac{\text{SymbolsSent}-\text{NoiseSymbols}}{\text{TimeSlots}} = \frac{K-I}{2} = \frac{3}{2}$.

B. Class B HRF Networks

The following Theorem, which is proved in Section V-B, states our result for *Class B HRF* networks.

Theorem 2. *Let N be the number of unique alignment sets, i.e., $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_N$, created from the elements of $\mathcal{I}$ and $\mathcal{W}_{\{-\mathcal{I}\}}$ according to the network topology $\mathcal{G}$ and Definition 4. The following SDoF is achievable for* Class B HRF *networks:*

$$\mathsf{SDoF} \geq \frac{K - \sum_{j=1}^{I} |Q_j|}{2}, \tag{6}$$

where $K = \sum_{j=1}^{N} |\mathcal{A}_j|$ and $I \leq N$ is the number of alignment sets which are a union of one or more interference sets, i.e., when $\mathcal{A}_j = \bigcup_{(r)} \mathcal{I}_i^{(r)}$ for $1 \leq r \leq K$. Here $\mathcal{C}_j(r) = \{$Set of transmitters for the elements in $\mathcal{A}_j = \bigcup_{(r)} \mathcal{I}_i^{(r)} : |C_j(r) \cap \mathcal{I}_i^{(r)}| \geq 1\}$, $\forall\, r$, and $Q_j = \min_r |C_j(r)|$.

We now use the running Example B to highlight key principles behind Theorem 2.

Example B. *($K = 10$-user Class B HRF Network):*

Consider the STIM network shown by Fig. 2(b) and the corresponding alignment sets as derived in Section III. Moreover, the transmitters only know the network topology $\mathcal{G}$. Our goal is to show that SDoF of $\frac{5}{2}$ is achievable through our scheme.

Transmission: The proposed transmission for the Class B HRF network of the current Example entails *two conditions:*

(Condition 1): In order to guarantee *decodability* at each intended receiver, we need to align all $N = 5$ alignment sets $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_5$ along five 2×1 sized vectors, that are pairwise independent. E.g., we can choose $V_1 = [1 \;\; 0]^\top$, $V_2 = [0 \;\; 1]^\top$, $V_3 = [1 \;\; 1]^\top$, $V_4 = [1 \;\; 2]^\top$, and $V_5 = [2 \;\; 1]^\top$.

(Condition 2): In order to guarantee *secrecy* at the unintended receivers, we need to protect all $I = 4$ alignment sets $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$, $\mathcal{A}_4$, i.e., whose elements are seen as interference at unintended receivers, by ensuring that each of them *contains enough* artificial noise symbols. We next take a closer look at these alignment sets and their interference subsets, then divide them into three types: Those that *don't have proper subsets*, *have nonintersecting subsets*, *have intersecting subsets*.

Step 1: Consider each of the $I = 4$ interference alignment sets. a) If a given alignment set does not have proper subsets among the interference sets $\mathcal{I}_1$, $\mathcal{I}_2$, $\ldots$, $\mathcal{I}_{10}$, then randomly pick one of the corresponding transmitters to act as a cooperative jammer by sending artificial noise. E.g., for this Example, this statement is true for the alignment sets $\mathcal{A}_2 = \{W_2, W_7\}$ and $\mathcal{A}_3 = \{W_3\}$. E.g., we can let Transmitters 7 and 3 act as cooperative jammers. Note that $\{W_7\}$ can be thought of as the smallest cooperative jamming subset $\mathcal{C}_j(r)$ of $\mathcal{A}_2$. Note that, as indicated in Section III, $\mathcal{A}_2$ consists of $r = 1$ interference sets and $\mathcal{C}_j(r)$ has cardinality $Q_j = \min_r |\mathcal{C}_j(r)| = |\{W_7\}| = 1$. Similarly, $\mathcal{C}_j(r) = \{W_3\}$ is the smallest jamming subset of $\mathcal{A}_3$, consists of $r = 3$ interference sets, and has $Q_j = \min_r |C_j(r)| = 1$. b) Otherwise, use Step 2.

Step 2: Consider each alignment set with proper interference subsets, i.e., each alignment set $\mathcal{A}_j$, where $\mathcal{A}_j = \bigcup_{(r)} \mathcal{I}_i^{(r)}$ for $2 \leq r \leq 10$ and $\mathcal{A}_j \neq \mathcal{I}_i^{(r)}$ for some $\mathcal{I}_i^{(r)} \in \mathcal{A}_j$. a) If its interference subsets have a nonempty intersection, then randomly pick one of the transmitters corresponding to the intersection set's elements to act as a cooperative jammer. E.g., for the current Example, this is true for the alignment set $\mathcal{A}_4 = \{W_4, W_6, W_8\} = \{\mathcal{I}_5 \cup \mathcal{I}_9\}$ because its $r = 2$ subsets intersect. More specifically $\{\mathcal{I}_4 \cap \mathcal{I}_8\} = \{W_8\}$. Thus, we can let Transmitter 8 act as a cooperative jammer. Note that $\{W_8\}$ can be thought of as the smallest cooperative jamming subset $\mathcal{C}_j(r)$ of $\{\mathcal{I}_5 \cap \mathcal{I}_9\}$. Moreover, since there is an intersection between all interference subsets of $\mathcal{A}_4$, this smallest subset has cardinality $Q_j = \min_r |\mathcal{C}_j(r)| = |\{W_8\}| = 1$.

b) Otherwise, if its subsets have an empty intersection, then randomly pick two or more transmitters corresponding to the smallest subset $\mathcal{C}_j(r)$ of the alignment set $\mathcal{A}_j$, which has a nonempty intersection with its interference subsets, to act as the smallest cooperative jamming subset. That is, have all $|\mathcal{C}_j(r)| \geq 2$ transmitters corresponding to the elements of $\mathcal{C}_j(r)$ send artificial noise. For this Example, this is true for the alignment set $\mathcal{A}_1 = \{W_1, W_5, W_{10}\} = \{\mathcal{I}_2 \cup \mathcal{I}_5 \cup \mathcal{I}_8\}$ which is a union of $r = 3$ sets. E.g., we can pick the subset $\mathcal{C}_j(r) = \{W_1, W_5\}$ with cardinality $Q_j = \min_r |\mathcal{C}_j(r)| = 2$, i.e., let the corresponding nodes 1 and 5 send artificial noise.

We can then have the remaining nodes, i.e., Transmitters 2, 4, 6, 9, and 10 send information signals.

SDoF Calculation: As a result of this transmission, each of the ten receivers observes independent equations, and is thus able to solve for its intended signal– be it information or artificial noise, and not able to solve for any interference signals. Thus, over $|V_1| = |V_2| = \cdots = |V_5| = 2$ time slots, we achieve achieve SDoF of $\frac{\text{SymbolsSent}-\text{NoiseSymbols}}{\text{TimeSlots}} = \frac{K-\sum_{j=1}^{I}|\mathcal{C}_j|}{2} = \frac{5}{2}$.

Remark 2. *In [11], the authors derived upper and lower bounds on SDoF for "regular" STIM networks, i.e., a setting with an assumption that all receivers are connected to a fixed (and equal) number of (interfering) transmitters beyond their uniquely dedicated transmitters. In this paper, we study the STIM networks without this "regularity" restriction.*

V. Proof Sketches of Main Results

A. Theorem 1 Proof: Transmission and SDoF Calculation

The proposed transmission scheme for Theorem 1 works over two time slots. This is done by: a) Aligning each of the N unique alignment sets, which are directly inferred from the network topology $\mathcal{G}$, along N pairwise independent vectors of size 2×1 each. b) Ensuring that the messages from each alignment set are protected by artificial noise at unintended receivers. Transmitters only know the network topology.

Topology vs. Alignment: Consider the composite messages set $\mathcal{W} = \{W_1, W_2, \ldots, W_K\}$, the interference message sets $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_K$ respectively seen at the K receivers, and the union set $\mathcal{I} = \{\mathcal{I}_1 \cup \mathcal{I}_2 \cup \cdots \cup \mathcal{I}_K\}$.

We first need to create a total of N unique alignment sets through the following two *search steps*:

Step 1: From the above K interference sets, while obeying the network topology $\mathcal{G}$, we can create $I \leq N$ *interference* alignment sets as follows. a) If any of the elements of $\mathcal{I}_k$, for $k \in \{1, 2, \ldots, K\}$, belong to any other interference set $\mathcal{I}_i$, for $i \neq k$ and $i \in \{1, 2, \ldots, K\}$, then create an alignment set $\mathcal{A}_j$ which is a union of $\mathcal{I}_k$ with all $(r-1)$ interference sets with a nonempty intersection with $\mathcal{I}_k$, i.e., $\mathcal{A}_j = \bigcup_{(r)} \mathcal{I}_i^{(r)}$ for $2 \leq r \leq K$. b) Otherwise, create an alignment set $\mathcal{A}_j = \mathcal{I}_k$. This step alone leads to a total of I unique alignment sets, i.e., whose elements are seen as interference at one (for $r = 1$) or more (for $2 \leq r \leq K$) receivers.

Step 2: Consider the composite set $\mathcal{W}_{\{-\mathcal{I}\}} = \mathcal{W} \backslash \mathcal{I}$ of all messages that are not seen as interference at any other (unintended) receivers, i.e., only seen at the intended receivers. From the elements of the set $\mathcal{W}_{\{-\mathcal{I}\}}$, while obeying the network topology $\mathcal{G}$, we can create the remaining $N - I$ alignment sets as follows. a) If the set $\mathcal{W}_{\{-\mathcal{I}\}}$ is nonempty, then create an alignment set $\mathcal{A}_j = \mathcal{W}_{\{-\mathcal{I}\}}$. b) Otherwise, do nothing. This step alone leads to a total of $N - I = 1$ unique alignment sets, i.e., the alignment set whose elements are only observed at their respectively intended receivers. We point out here that all the elements the is nonempty set $\mathcal{W}_{\{-\mathcal{I}\}}$ lead to just one alignment set. This in turn means that they are aligned along a single alignment vector. Thus, it is not necessary to use more than one alignment vector for all the messages that are not seen as interference at the other (unintended) receivers.

Therefore, by considering both Steps 1 and 2, we obtain:

1) $N = I + 1$ alignment sets in total, if $\mathcal{W}_{\{-\mathcal{I}\}}$ is nonempty.
2) $N = I$ alignment sets in total, if $\mathcal{W}_{\{-\mathcal{I}\}}$ is empty.

Transmission Scheme: The proposed transmission for the Class A HRF networks of Theorem 1 entails *two conditions:*

(Condition 1): In order to guarantee *decodability* at the intended receivers, we need to align the N alignment sets $\mathcal{A}_1$, $\mathcal{A}_2, \ldots, \mathcal{A}_N$ respectively along N vectors of size 2×1, each. That is, vectors $V_1, V_2, \ldots, V_N$, that are *pairwise independent*. At the *intended receive nodes*, this ensures that each desired signal occupies a separate subspace from that occupied by interference signals.

(Condition 2): In order to guarantee *secrecy* at the unintended receivers, we need to protect all I alignment sets, i.e., whose elements are seen as interference at unintended receivers, by ensuring that each set *contains one* artificial noise signal. This implies that, within each interference alignment set, *random transmitter choice guarantees secrecy:* We can randomly pick any transmitter to act as a cooperative jammer (i.e., by sending artificial noise) as long as it corresponds to one of the elements of the alignment set whose information signals we need to protect. Hence, at *unintended receivers*, the subspace occupied by interference signals is completely immersed in artificial noise, which ensures confidentiality.

SDoF Calculation: As a result of the above transmission, I transmitters send artificial noise signals and the remaining $K-I$ send information signals. Moreover, this takes place over a total of $|V_1| = |V_2| = \cdots = |V_N|$ time slots. Combining all steps, we thus obtain the expression of Theorem 1. ■

B. Theorem 2 Proof: Transmission and SDoF Calculation

As we will show, the main difference between Theorem 1 and Theorem 2 lies in the way secrecy is achieved.

Topology vs. Alignment: The process for creating aligement sets for Theorem 2 follows similar steps as those used in the proof of Theorem 1. Thus, we omit further repetition.

Transmission Scheme: The proposed transmission for the Class B HRF networks of Theorem 2 entails *two conditions: (Condition 1):* In order to guarantee decodability at the intended receivers, we follow the steps in *Condition 1* of the transmission scheme for Theorem 1. Thus, we omit repetition.

(Condition 2): In order to guarantee secrecy at the unintended receivers, we need to protect all *I interference* alignment sets, by ensuring that each one *contains enough* artificial noise signals. Here, *random transmitter choice does not guarantees secrecy*. We now take a closer look at these alignment sets and their interference subsets, then divide them into three categories: Those that 1) *don't have proper subsets*, 2) *have intersecting subsets*, 3) *have nonintersecting subsets*.

Step 1: Consider each of the I *interfering* alignment sets. From these I sets and their corresponding transmitters, while obeying the network topology $\mathcal{G}$, we can decide on which transmitters should act as cooperative jammers as shown next.

a) If a given *alignment set does not have proper subsets* among the interference sets $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_K$, then randomly pick one of the corresponding transmitters to act as a cooperative jammer by sending artificial noise. We note that, for all alignment sets that satisfy this property, this can be thought of as picking the smallest cooperative jamming subset $\mathcal{C}_j(r)$ of $\mathcal{A}_j$. Moreover, for this case, each $\mathcal{C}_j(r)$ has cardinality, $Q_j = \min_r |\mathcal{C}_j(r)| = 1$. Thus, a single transmitter suffices in protecting the alignment set's elements at unintended receivers. This is the case where $\mathcal{A}_j = \mathcal{I}_i^{(r)}$, for $i \in \{1, 2, \ldots, K\}$ and $1 \leq r \leq K$, i.e., the jamming subset $\mathcal{C}_j(r)$ is a singleton in order to avoid wastefulness. b) Otherwise, follow Step 2.

Step 2: Consider each alignment set with proper subsets among the interference sets, i.e., the alignment set $\mathcal{A}_j$, where $\mathcal{A}_j = \bigcup_{(r)} \mathcal{I}_i^{(r)}$ for $2 \leq r \leq K$ and $\mathcal{A}_j \neq \mathcal{I}_i^{(r)}$ for some $\mathcal{I}_i^{(r)} \in \mathcal{A}_j$. a) If its *subsets have a nonempty intersection*, then randomly pick one of the transmitters corresponding to the intersection set's elements to act as a cooperative jammer, i.e., any randomly chosen transmitter corresponding to the elements in the set $\bigcap_{(r)} \mathcal{I}_i^{(r)}$ for $2 \leq r \leq K$. We note here that, for all alignment sets that satisfy this property, this can be thought of as picking smallest cooperative jamming subset $\mathcal{C}_j(r)$ of the set $\bigcap_{(r)} \mathcal{I}_i^{(r)}$. Moreover, for this case, each possible $\mathcal{C}_j(r)$ has cardinality $Q_j = \min_r |\mathcal{C}_j(r)| = 1$ since there is a nonempty intersection between all interference subsets of $\mathcal{A}_j$.

b) Otherwise, consider each alignment set with proper subsets. a) If its *subsets have an empty intersection*, then randomly pick two or more transmitters corresponding to the smallest subset $\mathcal{C}_j(r)$ of the alignment set $\mathcal{A}_j$, which has a nonempty intersection with its interference subsets, to act as the smallest cooperative jamming subset. That is, for each alignment $\mathcal{A}_j$, have all the $Q_j = \min_r |\mathcal{C}_j(r)| \geq 2$ transmitters corresponding to the elements of each interference set $\mathcal{I}_i^{(r)} \subset \mathcal{A}_j$ satisfying $\mathcal{C}_j(r) \cap \mathcal{I}_i^{(r)} \geq 1$, for $2 \leq r \leq K$, send artificial noise. At the *unintended receive nodes*, the above two steps ensure that the subspace occupied by interference signals is completely immersed in artificial noise, which guarantees confidentiality.

SDoF Calculation: As a result of the above transmission, $\sum_{j=1}^{I} \mathcal{Q}_j$ transmitters, where $Q_j = \min_r |\mathcal{C}_j(r)|$, send artificial noise and the remaining $K - \sum_{j=1}^{I} \mathcal{Q}_j$ send information. This takes place over $|V_1| = |V_2| = \cdots = |V_N|$ time slots. Combining all steps, we get the expression of Theorem 2. ■

VI. Conclusion

In this paper, we investigated the STIM problem: Secure multi-user partially connected networks without CSIT, except network topology. We showed that secure transmission for the HRF networks requires separation into complimentary subclasses based on intersection properties between interference sets and their corresponding alignment sets. Specifically, through careful interference alignment and cooperative jamming, we derived lower bounds on achievable SDoF for Class A and Class B HRF networks. We aim to further investigate whether the alignment and jamming methods used herein can be extended to network topologies other than the HRF ones.

References

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

[2] 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, 2015.

[3] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3323–3332, 2011.

[4] J. d. D. Mutangana and R. Tandon, "Interference channels with confidential messages: Scaling up the secure degrees of freedom with no CSIT," in *Proc. 52nd Asilomar Conference on Signals, Systems, and Computers*, 2018.

[5] ——, "Interference channels with confidential messages: Leveraging OFDM transmission to scale up secure degrees of freedom with no CSIT," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, 2019.

[6] M. Seif, R. Tandon, and M. Li, "On the secure degrees of freedom of the K-user interference channel with delayed CSIT," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, 2018.

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

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

[9] H. Maleki, V. R. Cadambe, and S. A. Jafar, "Index coding-An interference alignment perspective," *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5402–5432, 2014.

[10] S. A. Jafar, "Blind interference alignment," *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 3, pp. 216–227, 2012.

[11] M. A. Attia and R. Tandon, "On the secure degrees-of-freedom of partially connected networks with no CSIT," in *Proc. IEEE International Conference on Communications (ICC)*, 2017.