# Topological Interference Management With Confidential Messages

Jean de Dieu Mutangana, *Member, IEEE*, and Ravi Tandon, *Senior Member, IEEE*

***Abstract*— The topological interference management (TIM) problem refers to the study of the $K$-user partially connected interference networks with no channel state information at the transmitters (CSIT), except for the knowledge of network topology. In this paper, we study the *TIM problem with confidential messages* (TIM-CM), where message confidentiality must be satisfied in addition to reliability constraints. In particular, each transmitted message must be decodable at its intended receiver and remain confidential at the remaining $(K-1)$ receivers. Our main contribution is to present a comprehensive set of results for the TIM-CM problem by studying the symmetric secure degrees of freedom (SDoF). To this end, we first characterize necessary and sufficient conditions for feasibility of positive symmetric SDoF for any arbitrary topology. We next present two achievable schemes for the TIM-CM problem: For the first scheme, we use the concept of *secure partition* and, for the second one, we use the concept of *secure independent sets*. We also present outer bounds on symmetric SDoF for any arbitrary network topology. Using these bounds, we characterize the optimal symmetric SDoF of all $K = 2$-user and $K = 3$-user network topologies.**

***Index Terms*— Topological interference management, confidential messages, channel state information uncertainty at transmitters, network topology, multi-user interference networks, partially connected networks, secure degrees of freedom.**

## I. Introduction

PHYSICAL layer security (PHY-SEC) exploits the inherent randomness of the wireless channel such as fading or noise in order to establish secure communication between the legitimate network users. It was introduced by Wyner in his seminal work on the degraded wiretap channel [55]. Wyner's model was extended to the nondegraded wiretap channel in [9], and then to the Gaussian wiretap channel in [20]. Numerous extensions to other multi-terminal problems ensued, including secrecy constrained broadcast channels (BC), multiple access channels (MAC), multiple-input multiple-output (MIMO) channels, and multi-user interference channels (IC), e.g., references [4], [10]–[12], [18], [21]–[24], [35], [37], [38], [41], [48], [56], [57]. For an overview of PHY-SEC research progress and potential applications in next generation wireless systems, we refer the reader to comprehensive surveys [34], [44], [54], [58].

A large body of works in PHY-SEC have been achieved under the assumption that channel state information at the transmitters (CSIT) is available –be it instantaneous [18], [24], [41], delayed [19], [31], [46], [52], or alternating [35], [51]. Moreover, a major portion of prior works on multi-user interference networks (with or without secrecy constraints) have assumed that the network is *fully connected*, i.e., that each transmitter in a given network is connected to every receiver in the same network and vice versa, e.g., [10], [31], [56]. For instance, in [56] the authors studied the $K$-user fully connected interference channel with confidential messages (IC-CM) and showed that when CSIT is perfectly available, then the sum secure degrees of freedom (sum SDoF) scales linearly with $K$. Additionally, it is known that, for the fully connected interference networks, SDoF is zero when CSIT is not available. This is due to the fact that, under such settings, all receivers are statistically equivalent from each transmitter's perspective which puts decodability and secrecy constraints in direct conflict.

As indicated in [34], [44], [54], [58], a considerable portion of works on PHY-SEC have also studied secrecy constrained wireless channels in the absence of CSIT. For instance, in [57] the authors characterized sum SDoF for the MIMO wiretap channel with no CSI anywhere for $T \geq 2\min(n_t, n_r)$, where parameters $n_t$, $n_r$, and $T$ respectively represent the number of antennas at the transmitter, number of antennas at the receiver, and coherence time. In [10] the authors showed that positive sum SDoF is achievable for the $K$-user fully connected IC-CM with no CSIT by leveraging the intersymbol interference (ISI) heterogeneity which is inherently present within the subclass of channels with memory. Therein, it was shown that the achievable sum SDoF scales linearly with $K$ under some ISI heterogeneity conditions. Note that, in reality, the signals propagating over the wireless medium face several physical obstacles in addition to signal energy dissipation over traveled distance [15], [53]. Particularly, in multi-user interference networks, the above physical phenomena lead to the presence of *weak channels*, i.e., channels whose signal strength is at noise floor levels or below a preset minimum power threshold for reliable signal detection at the receivers. It is thus reasonable to model multi-user wireless networks by discarding the weak channels, a setting referred to as that of

Manuscript received 26 October 2020; revised 23 May 2022; accepted 12 June 2022. Date of publication 27 June 2022; date of current version 21 October 2022. This work was supported by NSF under Grant CNS-1715947, Grant CCF-2100013, and Grant CAREER-1651492. *(Corresponding author: Ravi Tandon.)*

The authors are with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721 USA (e-mail: mutangana@email.arizona.edu; tandonr@email.arizona.edu).

Communicated by A. W. Eckford, Associate Editor for Communications.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2022.3186238.

Digital Object Identifier 10.1109/TIT.2022.3186238

*partially connected* networks, i.e., where each transmitter is only connected to a subset of receivers and vice versa.

Motivated by the above reasons, research considerations from the other extreme in terms of CSIT availability and network connectivity have recently gained traction under the framework of topological interference management (TIM) [1], [14], [17], [28], [32], [36], [47], [59]–[61]. In particular, the TIM problem studies partially connected multi-user interference networks with no CSIT, except for the knowledge of network topology and channel statistics. In other words, research on the TIM problem seeks to exploit the inherent heterogeneity due to the partial connectivity in order to ensure network reliability in the absence of CSIT. We note here that the TIM problem is closely related to the index coding (ICOD) problem [2], [3], [5], [6], [16], a framework under which the messages from all transmitters pass through a single common node (or equivalently, a server) which encodes them into a common function, that it then broadcasts to all receivers. Each receiver then applies its side information (also known as antidotes) to the broadcast function in order to decode its intended message. The authors in [17] and [32] have shown that the TIM problem can be reformulated into the ICOD problem and vice versa. Moreover, due to the fact that the common node has access to all messages and the presence of antidotes at the receivers, the channel capacity for a given ICOD problem is an upper bound on the capacity of its TIM network counterpart. Note that the general ICOD and the general TIM are both still open problems. We refer the reader to [3] and references therein for an overview of fundamentals of ICOD. A variant of the ICOD problem called pliable index coding (PICOD) was recently proposed [7], [27], [49], [50]. PICOD is a slightly more relaxed problem where each receiver is satisfied by decoding any one arbitrary message (not belonging to its side information set) from the broadcast function.

In this paper, we study the TIM problem with an additional secrecy constraint, a framework that we refer to as *TIM with confidential messages* (TIM-CM). Here, each transmitted message must be decodable at its intended receiver and remain confidential at the remaining $(K-1)$ receivers. The Besides a small number of recent results, e.g., [4], [12], the TIM-CM problem has largely remained unexplored. The work in [4] derived a lower and an upper bound on sum SDoF for the *regular* TIM-CM problem. This is the secrecy constrained version of the well understood *regular* TIM problem, where each user is assumed to receive signals from a constant number of transmitters [60], and whose sum degrees of freedom (DoF) has been derived in [60] through interference avoidance based on fractional graph coloring. The work in [12] derived a lower bound on sum SDoF for the *half-rate-feasible* TIM-CM problem. This is the secrecy constrained version of the well understood *half-rate-feasible* TIM problem whose upper bound on symmetric DoF has been shown in [17], [32] to be $1/2$ per user, hence the name "half-rate-feasible."

Just as there is a direct relationship between the general TIM problem and the general ICOD problem, one can also reformulate the TIM-CM problem of the current paper into an *ICOD problem with confidential messages* (private-ICOD) and vice versa. The main difference between TIM-CM and private-ICOD is that, unlike in TIM-CM, each receiver in private-ICOD has an arbitrary subset of transmitted messages and jamming signals as side information, i.e., requiring that each receiver be only able to decode its intended message and nothing more beyond its side information set. Under the private-ICOD settings, all messages and jamming signals (from the transmitters) are assumed to be available to the common node which encodes them into a common function to broadcast to all receivers. Each receiver can use its side information to decode its indented message. As a consequence of the possible reformulation, we also consider the literature on secrecy constrained index coding, e.g., [13], [25], [26], [29], [30], [33], [39], [40], [42], [43], [45], to get a comprehensive picture of works related to TIM-CM.

The majority of results on secrecy constrained ICOD problems can be broadly placed in two major categories: $(i)$ ICOD problems with secrecy constraints against external eavesdroppers, i.e., requiring secrecy against any illegitimate network users that may eavesdrop on the broadcast function. This is a problem also referred to as secure index coding (secure-ICOD), e.g., [30], [33], [42], [43]. $(ii)$ ICOD problems with secrecy constraints against other legitimate users within the same network. This second category can be further subdivided into two problem subclasses, namely, private-ICOD (also defined above) and private pliable index coding (private-PICOD), which focuses on a slightly more relaxed setting where each receiver is satisfied by decoding any one arbitrary message from the transmitted messages and nothing more beyond its side information set. For example, in recent work [30], the authors studied the $K$-user secure-ICOD problem and characterized the optimal capacity region for $K \leq 4$. On the other hand, in a recent paper [39] and its long version [40], the authors studied the $K$-user private-ICOD problem and settled the capacity region for $K \leq 3$. In order to obtain this result, there is an additional assumption made in [39]: a key sharing mechanism enables the common node to share secret keys with arbitrarily subsets of receivers in addition to the broadcast of the common function. Moreover, it is proved in [39] that, due to the presumption of existence of this secret key sharing mechanism, the achievable secrecy rate matches that of the nonsecrecy constrained ICOD problem, i.e., there is no rate penalty for secrecy. In the absence of the secrect key sharing mechanism between the server and receivers, the authors [39] also studied a resulting *weak secrecy private-ICOD* (WS-ICOD) model and provided necessary conditions for the feasibility of positive secrecy rate. For this model, no achievable schemes were proposed and capacity region was not derived for any value of $K$. A direct reformulation of the TIM-CM problem of the current paper would lead to a WS-ICOD model because WS-ICOD precludes the assumption of the secret key sharing mechanism beyond the broadcast function. Moreover, there is a rate penalty for secrecy under TIM-CM settings. In regards to the private-PICOD problem, recent works derived lower bounds on secrecy rate [25], [26], [45].

Motivated by the above discussion, in this paper, we focus on the following question: What are the bounds on symmetric

SDoF for the $K$-user partially connected interference networks with confidential messages in the absence of CSIT, except for the knowledge of network topology and channel statistics? In other words, our aim is to explore how much this topology knowledge alone can be exploited in order to manage interference and establish limits on symmetric SDoF for the TIM-CM problem.

*Contributions:* We summarize our main contributions as follows:

(i) *(Necessary and Sufficient Conditions for Symmetric SDoF Feasibility):* We characterize necessary and sufficient conditions under which non-zero SDoF is feasible for any topology. These feasibility conditions for TIM-CM are related to conditions of its WS-ICOD counterpart [40, Lemma 8] since its graph is a complementary of the network coding graph of WS-ICOD.

(ii) *(Inner Bounds on Symmetric SDoF):* We propose achievable symmetric SDoF schemes for the general TIM-CM problem by introducing two transmission schemes, namely, *secure partition* for the first lower bound and *secure independent* sets for the second one.

(iii) *(Outer Bounds on Symmetric SDoF):* We also obtain upper bounds on symmetric SDoF for the general TIM-CM problem. To this end, we first show how to obtain a nontrivial upper bound on symmetric SDoF through a careful analysis of the received signal structures at all $K$ receivers and their respective interference components with regard to the underlying topology. We next present a second upper bound which we show to be tighter for some examples. The main difference between this upper bound and the first one is that here we leverage the potential presence of *fractional signal generators* within the network, a concept that was introduced in [36], [60] for the nonsecrecy constrained TIM problem. This is a paradigm where the interference signal component of the received signal at some receiver can generate either a statistically equivalent version of the received signal at some other receiver or its cleaner version (i.e., with less interference).

(iv) *(Optimal Symmetric SDoF for All $K$-User TIM-CM Topologies With $K \leq 3$):* Finally, we apply the proposed upper and lower bounds to characterize the optimal symmetric SDoF for all $K$-user TIM-CM topologies with $K \leq 3$.

## II. System Model

We consider the $K$-user partially connected single-input single-output (SISO) interference network with confidential messages as depicted in Fig. 1. We use $\mathcal{T}_k$ to denote the index set of all transmitters that are connected to receiver $R\mathsf{x}_k$, for $k \in \{1, 2, \ldots, K\}$. Similarly, we use $\mathcal{R}_k$ to denote the index set of all receivers that are connected to transmitter $T\mathsf{x}_k$, for $k \in \{1, 2, \ldots, K\}$. Therefore, the network can be fully described by its topology $\mathcal{G} = (\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_K, \mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_K)$. Additionally, we use $\mathcal{I}_k$ to represent the index set of all transmitters that cause interference at $R\mathsf{x}_k$. In turn, this implies that $\mathcal{T}_k = \{k\} \cup \mathcal{I}_k$. For a given topology $\mathcal{G}$, the signal received at $R\mathsf{x}_k$ at time $t$ is given by

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

where $h_{ki}$ represents the channel coefficient between Transmitter $i$ and Receiver $k$, assumed be time invariant and i.i.d. across users. $Z_k(t)$ is the zero-mean unit-variance complex Gaussian channel noise. We next provide the adjacency matrix definition which will be useful later.

*Definition 1 (Adjacency Matrix):* For a network topology $\mathcal{G}$, we define an adjacency matrix $\mathbf{B}$ as:

$$\mathbf{B}_{(j,i)} = \begin{cases} 1, & h_{ji} \neq 0 \\ 0, & otherwise, \end{cases}$$

where the matrix $\mathbf{B}$ is of size $K \times K$. Here, $h_{ji} \neq 0$ ($h_{ji} = 0$) indicates whether there is a connection (no connection) between Transmitter $i$ and Receiver $j$ [17], [60].

*CSIT/CSIR Assumptions*: Under the TIM-CM framework, there is no CSIT, except that the transmitters have the statistics of the channel coefficients and full access to the network topology $\mathcal{G}$. For coherent signal detection, in addition to having access to $\mathcal{G}$, we assume that there is global CSI at the receivers (CSIR). That is, each receiver $R\mathsf{x}_k$, for $k \in \{1, 2, \ldots, K\}$, has casual access to the set of all non-zero channel coefficients denoted by $\mathcal{H} = \{h_{ki} : i \in \mathcal{T}_k\}_{k=1}^{K}$.

Each transmitter $T\mathsf{x}_k$, for $k \in \{1, 2, \ldots, K\}$, uses the knowledge of $\mathcal{G}$ to encode its message $W_k$ into an $n$-length vector $X_k^n = [X_k(1), X_k(2), \ldots, X_k(n)]^\top$ via an encoding function $f_{_{Enc}}(W_k|\mathcal{G})$. The vector $X_k^n$ is subject to the following power constraint:

$$\frac{1}{n}\mathbb{E}(||X_k^n||^2) \leq P, \tag{2}$$

where $P$ is the average transmit power. Each receiver $R\mathsf{x}_k$ receives a vector $Y_k^n = [Y_k(1), Y_k(2), \ldots, Y_k(n)]^\top$ and uses the knowledge of both $\mathcal{G}$ and $\mathcal{H}$ to recover its intended message $W_k$ via a decoding function $f_{_{Dec}}(Y_k^n|\mathcal{G}, \mathcal{H})$. The considered system model is subject to reliability and secrecy constraints as we explain next.

Transmitter $T\mathsf{x}_k$ wants to securely send a message $W_k$, which is uniformly distributed in $\mathcal{W}_k = \{1, 2, \ldots, 2^{nR_k}\}$, to receiver $R\mathsf{x}_k$. Here, $\mathcal{W}_k$ represents the index set of all message at $T\mathsf{x}_k$. A secure rate of communication $R_k(P, \mathcal{G}) = \frac{\log(|\mathcal{W}_k|)}{n}$ is achievable, if there exists a sequence of encoding and decoding functions $f_{_{Enc}}(W_k|\mathcal{G})$, $f_{_{Dec}}(Y_k^n|\mathcal{G}, \mathcal{H})$ such that, as $n \to \infty$, both the decodability and confidentiality constraints are satisfied:

*Decodability Constraint:* Each receiver $R\mathsf{x}_k$ must be able to decode its intended message $W_k$,

$$Pr[W_k \neq \hat{W}_k] = o(n). \tag{3}$$

*Confidentiality Constraints:* All messages seen as interference at receiver $R\mathsf{x}_k$ must remain confidential,

$$\frac{1}{n}I(W_{\mathcal{I}_k}; Y_k^n|W_k, \mathcal{H}) = o(n), \quad \forall k \in \{1, 2, \ldots, K\}. \tag{4}$$

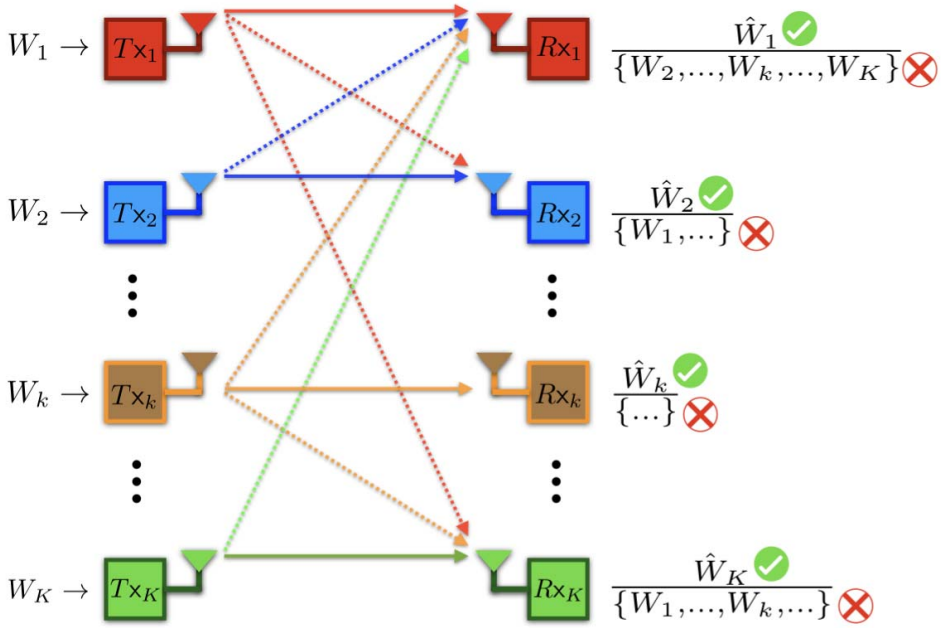


Fig. 1. TIM-CM problem where each user $R\mathsf{x}_k$ should only decode its intended message $W_k$ and the remaining (interfering) messages must remain confidential.

Here, $W_{\mathcal{I}_k} = \{W_i : i \in \mathcal{I}_k, i \neq k\}$ is the set of all messages seen as interference at $R\mathsf{x}_k$, and $Y_k^n$ is the signal received at $R\mathsf{x}_k$ over the $n$-length transmission block.

*Definition 2 (Secure Degrees of Freedom (SDoF) Tuple):* Consider a network topology $\mathcal{G}$ and the defined above average signal transmission power parameter $P$. We say that an SDoF $K$-tuple $\left(\mathsf{SDoF}^{(1)}, \mathsf{SDoF}^{(2)}, \ldots, \mathsf{SDoF}^{(K)}\right)$ is achievable, if there exist achievable rates $(R_1(P,\mathcal{G}), R_2(P,\mathcal{G}), \ldots, R_K(P,\mathcal{G}))$, for each $P$, such that

$$\mathsf{SDoF}^{(k)} = \lim_{P\to\infty} \frac{R_k(P,\mathcal{G})}{\log(P)}, \quad k \in \{1,2,\ldots,K\}, \tag{5}$$

where $\mathsf{SDoF}^{(k)}$ is the achievable SDoF for user $k$.

In this paper, we focus on the *symmetric SDoF* which we define next.

*Definition 3 (Symmetric SDoF):* The symmetric SDoF, $\mathsf{SDoF}^{\mathsf{sym}}$ is defined as follows:

$$\begin{aligned}\mathsf{SDoF}^{\mathsf{sym}} &= \sup\left\{D : \left(\mathsf{SDoF}^{(1)}, \mathsf{SDoF}^{(2)}, \ldots, \mathsf{SDoF}^{(K)}\right)\right.\\ &\left.= (D,\ldots,D) \text{ is achievable.}\right\}\end{aligned} \tag{6}$$

## III. Main Results and Discussion

In this Section, we present our main results and an accompanying discussion together with illustrative examples. In Section III-A, we present necessary and sufficient conditions for the feasibility of positive symmetric SDoF for the general TIM-CM problem, the first inner bound on symmetric SDoF based on secure partition, and the second inner bound based on secure independent sets, respectively in Theorems 1, 2, and 3. In Section III-B, we present our first and second upper bounds on symmetric SDoF, respectively in Theorems 4 and 5. Finally, in Section III-C, we present two case studies where we respectively characterize the optimal symmetric SDoF for all 2-user and 3-user TIM-CM topologies.

### A. Feasibility of Positive Symmetric SDoF and Inner Bounds

Consider the $K$-user TIM-CM model defined by equation (1). The following Theorem, which is proved in Appendix IV, answers the question: When is symmetric SDoF zero for a given TIM-CM network?

*Theorem 1:* For a network topology $\mathcal{G}$, the symmetric SDoF is zero if and only if there exists a pair $i, j \in \{1,2,\ldots,K\}$, for $i \neq j$, such that

(i) $i \in \mathcal{I}_j$
(ii) $j \in \mathcal{I}_i$
(iii) $\mathcal{I}_j \setminus \{i\} \subseteq \mathcal{I}_i \setminus \{j\}$ or $\mathcal{I}_i \setminus \{j\} \subseteq \mathcal{I}_j \setminus \{i\}$.

Consequently, as also detailed in Appendix IV, for any TIM-CM network that does not satisfy the conditions of Theorem 1, positive symmetric SDoF is feasible. In the Appendix, we present a simple scheme satisfying positive symmetric SDoF through *secure* time division multiple access (secure TDMA), which leads to the smallest achievable symmetric SDoF of $\frac{1}{K}$ per user. We use Examples 1 and 2 to highlight the principles behind Theorem 1.

*Example 1 (5-User TIM-CM Network: Zero Symmetric SDoF):* Consider the network topology in Fig. 2 (a). At receiver $R\mathsf{x}_1$, we have $\mathcal{I}_1 = \{2,3,4\}$ and $\mathcal{T}_1 = \{1\} \cup \mathcal{I}_1 = \{1,2,3,4\}$. At receiver $R\mathsf{x}_2$, we have $\mathcal{I}_2 = \{1,3\}$ and $\mathcal{T}_2 = \{2\} \cup \mathcal{I}_2 = \{1,2,3\}$. Consider the user pair $(i,j) = (1,2)$. Therefore, for this pair, the conditions of Theorem 1 are satisfied because $(i)$ $1 \in \mathcal{I}_2$, $(ii)$ $2 \in \mathcal{I}_1$, and

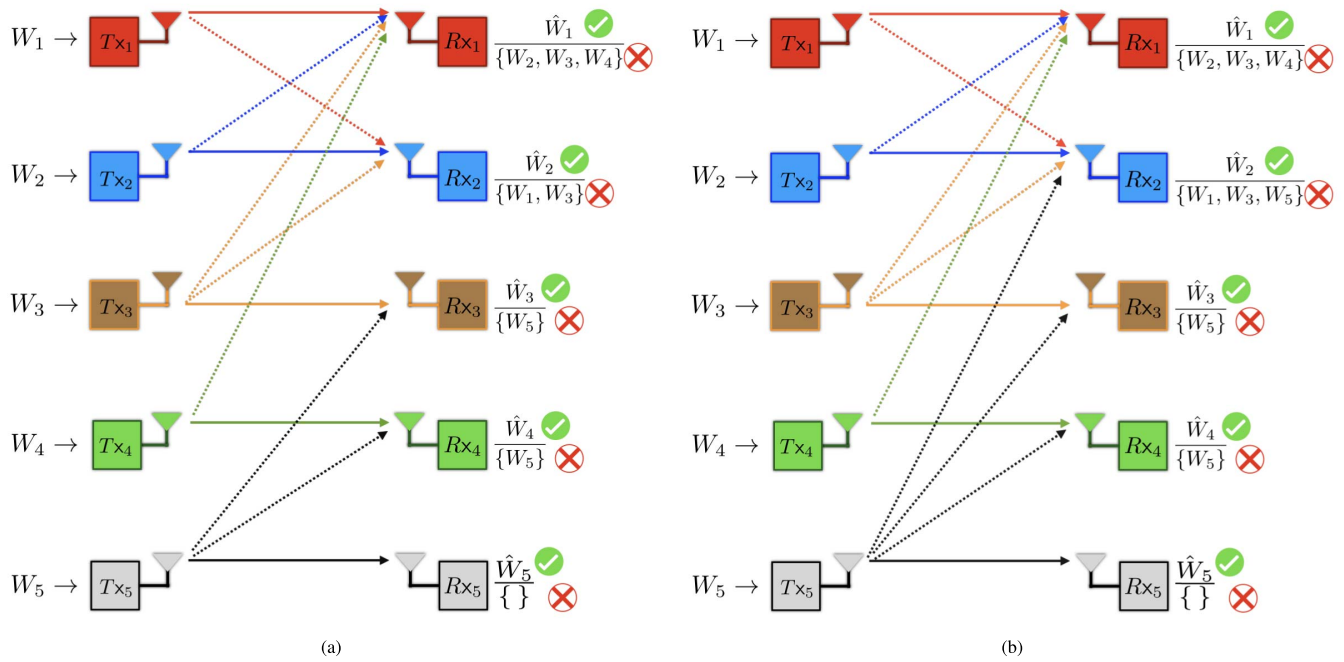


Fig. 2. 5-user TIM-CM networks depicting: (a) When symmetric SDoF is *zero* versus (b) When it is *nonzero*.

$(iii)$ $\mathcal{I}_2 \setminus \{1\} \subseteq \mathcal{I}_1 \setminus \{2\}$. Since the conditions of Theorem 1 are satisfied, then symmetric SDoF is zero for this network.

The intuition behind the infeasibility of positive symmetric SDoF for this topology is as follows: Suppose transmitter $T\mathsf{x}_1$ wants to send its message during a given time slot. Then, transmitters $T\mathsf{x}_2$, $T\mathsf{x}_3$, and $T\mathsf{x}_4$, which are all seen at its intended receiver $R\mathsf{x}_1$ have to remain silent in order to avoid causing interference and thus preventing it from decoding the message sent by $T\mathsf{x}_1$. Moreover, any message sent by $T\mathsf{x}_1$ will be seen as interference at $R\mathsf{x}_2$. Therefore, a separate transmitter that is seen at $R\mathsf{x}_2$ but not seen at $R\mathsf{x}_1$ is needed to protect the message from $T\mathsf{x}_1$ by jamming $R\mathsf{x}_2$. However, there is no such transmitter within the network topology of Fig. 2 (a), thereby leading to zero secure communication rate for the transmit receive pair $T\mathsf{x}_1 - R\mathsf{x}_1$. The proof of Theorem 1 essentially formalizes the above logical arguments.

*Example 2 (5-User TIM-CM Network: Nonzero Symmetric SDoF):* Consider the network topology in Fig. 2 (b). It can easily be verified that for all user pairs $i, j \in \{1, 2, \ldots, 5\}$, for $i \neq j$, the conditions of Theorem 1 are not satisfied. Therefore, we can achieve a positive symmetric SDoF of at least $\frac{1}{K} = \frac{1}{5}$ over five time slots as we show next.

The proposed transmission works over $T = 5$ *sub-blocks*, where each sub-block is of length $n_B$. This leads to the transmission block of length $n = n_B T$. Moreover, we assume that $n_B$ is large enough to satisfy the decodability and confidentiality constraints in (3)-(4). From here onward in the achievable schemes of this paper, with a slight abuse of notation, we refer to a sub-block of length $n_B$ as a *time slot*. Under the same convention, we will refer to $T$ as the *transmission blocklength*. Furthermore, we assume that the transmitted signals are observed at discrete and synchronous time slots at the receivers.

(i) In the first sub-block (time slot), transmitter $T\mathsf{x}_1$ sends its message signal using a wiretap code [55], whereas $T\mathsf{x}_5$ acts as a cooperative jammer by sending an artificial noise signal. All the other transmitters remain silent. Hence, the received signals at the first and second receivers are respectively given by $Y_1 = h_{11}X_1 + Z_1$ and $Y_2 = h_{21}X_1 + h_{25}X_5 + Z_2$. The following secrecy rate is achievable at $R\mathsf{x}_1$: $R_1 = I(X_1; Y_1|\mathcal{H}) - I(X_1; Y_2|\mathcal{H})$. In particular, by assuming that the transmitters use Gaussian codebooks [21]–[23], [57], it can be readily verified that the achievable SDoF at $R\mathsf{x}_1$ is $\mathsf{SDoF}^{(1)} = \lim_{P\to\infty} \frac{R_1}{\log(P)} = 1$. Transmission for the remaining four users follows the same logic as the first one and we summarize it next.

(ii) In time slot $t = 2$, let $T\mathsf{x}_2$ transmit its message and let $T\mathsf{x}_4$ jam $R\mathsf{x}_1$.

(iii) In time slot $t = 3$, let $T\mathsf{x}_3$ transmit its message and let $T\mathsf{x}_1$ simultaneously jam $R\mathsf{x}_1$ and $R\mathsf{x}_2$.

(iv) In time slot $t = 4$, let $T\mathsf{x}_4$ transmit its message and let $T\mathsf{x}_2$ jam $R\mathsf{x}_1$.

(v) In time slot $t = 5$, let $T\mathsf{x}_5$ transmit its message and let $T\mathsf{x}_3$ and $T\mathsf{x}_4$ collectively jam $R\mathsf{x}_2$, $R\mathsf{x}_3$, and $R\mathsf{x}_4$. Hence, each receiver gets its intended message over five time slots, i.e., $\mathsf{SDoF}^{\mathsf{sym}} \geq \frac{1}{5}$.

We next present general transmission schemes beyond the (greedy) secure TDMA approach. We show how to achieve lower bounds on symmetric SDoF that are greater than or equal to $\frac{1}{K}$ under feasible topology conditions. Clearly, this implies that, under such schemes, the transmission blocklength may be less than the number of users in the whole network. As we explain later, transmission is done through the process of *secure interference avoidance*. Let us first define *interference avoidance*.

*Definition 4 (Interference Avoidance):* In order to enable decodability at its intended receiver, each transmitter $T\mathsf{x}_k$, for $k \in \{1,2,\ldots,K\}$, uses time slot $t$, for $t \in \{1,2,\ldots,T\}$, to transmit an information message $W_k$, for $k \in \{1,2,\ldots,K\}$, if and only if both those users that it causes interference to and those users that cause interference at its intended receiver $R\mathsf{x}_k$ are not using the same time slot $t$ to transmit any signals. This principle is called interference avoidance.

The above transmission principle would suffice, if we were only concerned with decodability, i.e., under the TIM model. However, for the TIM-CM problem, we are additionally required to preserve secrecy. Thus, more restrictions on transmission have to be imposed beyond interference avoidance as we explain next.

*Definition 5 (Secure Interference Avoidance):* In order to enable both decodability and secrecy, $T\mathsf{x}_k$ can transmit its message $W_k$ by following the defined above interference avoidance plus a new requirement that there must exist a set $\mathcal{C}$ of cooperative jamming transmitters (that do not interfere at $R\mathsf{x}_k$) to protect $W_k$ at all receive nodes where it is seen as interference by sending artificial noise.

The above described (secure) interference avoidance principles are closely related to the notion of (secure) *independent sets* and *secure partition* as we explain next.

*Definition 6 (Independent Set (IS)):* Consider a $K$-user TIM-CM network. A set of users $\mathcal{U}_{IS} \subseteq \{1,2,\ldots,K\}$, is an *independent set*, if for all $i \neq j \in \mathcal{U}_{IS}$, $\mathbf{B}_{(i,j)} = \mathbf{B}_{(j,i)} = 0$. This implies that, for all $i \neq j \in \mathcal{U}_{IS}$, transmitter $T\mathsf{x}_j$ is not connected to receiver $R\mathsf{x}_i$ and transmitter $T\mathsf{x}_i$ is not connected to receiver $R\mathsf{x}_j$. This can simply be represented as $j \notin \mathcal{T}_i$ and $i \notin \mathcal{T}_j$.

*Definition 7 (Secure Independent Set (SIS)):* A set of users $\mathcal{U}_{SIS} \subseteq \{1,2,\ldots,K\}$, is a *secure independent set*, if $\mathcal{U}_{SIS}$ is an independent set, and there exists a set $\mathcal{C} \subseteq \{1,2,\ldots,K\} \setminus \mathcal{U}_{SIS}$, such that:

(i) $\mathcal{U}_{SIS} \cap \mathcal{R}_{\mathcal{C}} = \emptyset$
(ii) $\mathcal{R}_{\mathcal{U}_{SIS}} \setminus \mathcal{U}_{SIS} \subseteq \mathcal{R}_{\mathcal{C}}$,

where $\mathcal{R}_{\mathcal{U}_{SIS}}$ and $\mathcal{R}_{\mathcal{C}}$ respectively represent the set of all receivers that are connected to transmitters in $\mathcal{U}_{SIS}$ and $\mathcal{C}$.

In other words, condition $(i)$ implies that the intended receivers for the transmitters in $\mathcal{U}_{SIS}$ do not see the cooperative jamming signals from the transmitters in $\mathcal{C}$; and condition $(ii)$ implies that all unintended receivers that see signals from the transmitters in $\mathcal{U}_{SIS}$ should be in the coverage of the cooperative jamming set $\mathcal{C}$.

The intuition behind the above definition is that each transmitter in the secure independent set $\mathcal{U}_{SIS}$ will also be able to achieve confidentiality, as it will be simultaneously protected by artificial noise signal(s) that are sent by the cooperative jamming transmitters in $\mathcal{C}$.

*Definition 8 (Secure Partition (SP)):* A partition $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_T\}$, where $\mathcal{P}_t \neq \emptyset$ for all $t \in \{1,2,\ldots,T\}$, $\mathcal{P}_m \cap \mathcal{P}_n \neq \emptyset$ for all $m \neq n \in \{1,2,\ldots,T\}$, and $\bigcup_{t=1}^{T} \mathcal{P}_t = \{1,2,\ldots,K\}$, is a secure partition, if every subset $\mathcal{P}_t$, for $t = 1,2,\ldots,T$, is a secure independent set.

The following Theorem states our first lower bound on the symmetric SDoF.

*Theorem 2:* The symmetric SDoF for the $K$-user TIM-CM network is lower bounded as follows:

$$\begin{aligned} &\mathsf{SDoF}^{\mathsf{sym}} \geq \max_{\mathcal{P}} \frac{1}{|\mathcal{P}|}, \\ &\text{such that } \mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_T\}, \text{ for } |\mathcal{P}| = T, \\ &\text{is a secure partition of } \{1,2,\ldots,K\}. \end{aligned} \tag{7}$$

*Proof:* To prove the above result, we need to argue that for any secure partition $\mathcal{P}$, a symmetric SDoF of $1/|\mathcal{P}|$ is achievable. The result then follows by maximizing over all secure partitions. Since by Definition 8, each subset $\mathcal{P}_t$ is a secure independent set, we can schedule all users in $\mathcal{P}_t$ in a single time slot $t$, for $t \in \{1,2,\ldots,T\}$, while satisfying decodability (3) and secrecy (4). To this end, we also simultaneously schedule all transmitters in a separate set $\mathcal{C}_t$, for $t \in \{1,2,\ldots,T\}$, to act as cooperative jammers by transmitting artificial noise symbols during time slot $t$ in order to protect all the information signals from the $|\mathcal{P}_t|$ transmitters at the receivers where they are seen as interference. Thus, by separately scheduling $|\mathcal{P}|$ subsets over $|\mathcal{P}|$ slots, and the fact a user only appears in a single subset, we achieve a lower bound of $1/|\mathcal{P}|$. Clearly, under this transmission scheme, each user is only assigned a single secure interference free channel use per transmission blocklength $|\mathcal{P}| = T$ and the achievable SDoF is maximized when all receivers can be served with their intended messages over the minimum cardinality of $\mathcal{P}$. ■

We use Examples 3.A and 4.A to highlight the principles behind Theorem 2.

*Example 3.A (6-User TIM-CM Network: Transmission via SP):* Consider the network topology $\mathcal{G} = (\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_6, \mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_6)$ depicted in Fig. 3. From this topology, we can directly deduce the following:

- *(Independent Sets)*: Consider a set of transmitters $\mathcal{U}_{IS} = \{1,5,6\}$. It can be verified that, for all $i,j \in \mathcal{U}_{IS}$, the adjacency matrix of this network satisfies $\mathbf{B}_{(i,j)} = \mathbf{B}_{(j,i)} = 0$. Therefore, by Definition 6, Transmitters 1, 5, and 6 form an independent set $\{1,5,6\}$. In other words, $T\mathsf{x}_1$, $T\mathsf{x}_5$, and $T\mathsf{x}_6$ are not connected to each other's desired destinations $R\mathsf{x}_1$, $R\mathsf{x}_5$, and $R\mathsf{x}_6$. Similarly, we can show that the sets $\{3\}$, $\{4,6\}$, and $\{2,5,6\}$ are also independent sets.
- *(Secure Independent Sets)*: Consider a set of transmitters $\mathcal{U}_{SIS} = \{5,6\}$. Clearly, for all $i,j \in \mathcal{U}_{SIS}$, $\mathbf{B}_{(i,j)} = \mathbf{B}_{(j,i)} = 0$. Moreover, consider a set $\mathcal{C} = \{4\}$. This is a set of transmitter(s) such that, for a set of receivers $\mathcal{R}_{\mathcal{C}} = \{1,2,4\}$ that can see signals from $\mathcal{C}$ and the set of receivers $\mathcal{R}_{\mathcal{U}_{SIS}} = \{4,5,6\}$ that can see signals from $\mathcal{U}_{SIS}$, the following conditions are satisfied: $(i)$ $\mathcal{U}_{SIS} \cap \mathcal{R}_{\mathcal{C}} = \emptyset$ and $(ii)$ $\mathcal{R}_{\mathcal{U}_{SIS}} \setminus \mathcal{U}_{SIS} \subseteq \mathcal{R}_{\mathcal{C}}$. Therefore, by Definition 7, the set $\mathcal{U}_{SIS} = \{5,6\}$ is a secure independent set. Similarly, we can show that the sets $\{1\}$, $\{3\}$, $\{2,6\}$, and $\{4,6\}$ are also secure independent sets.
- *(Secure Partition)*: From the above secure independent sets and Definition 8, we can create a secure partition $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_5\}$, where $\mathcal{P}_1 = \{2,6\}$, $\mathcal{P}_2 = \{1\}$, $\mathcal{P}_3 = \{3\}$, $\mathcal{P}_4 = \{4\}$, and $\mathcal{P}_5 = \{5\}$.

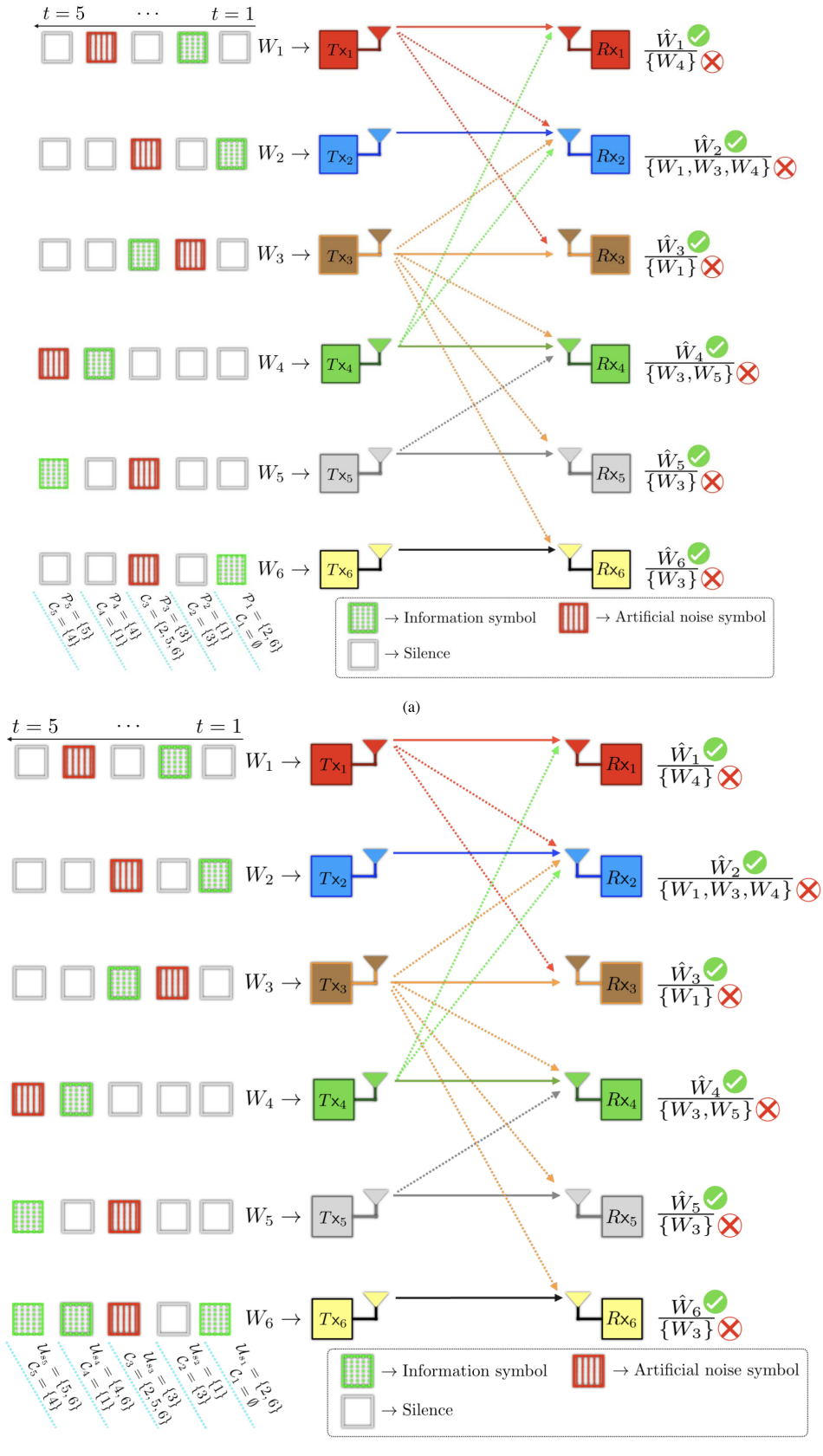


Fig. 3. 6-user TIM-CM network contrasting: (a) Transmission via secure partition versus (b) Transmission via secure independent sets.

As depicted in Fig. 3(a), we can schedule transmitters in secure partition subsets $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_5$ respectively over $T = |\mathcal{P}| = 5$ time slots and have the following sets of transmitters serve as their respective cooperative jamming sets: $\mathcal{C}_1 = \emptyset$, $\mathcal{C}_2 = \{3\}$, $\mathcal{C}_3 = \{2, 5, 6\}$, $\mathcal{C}_4 = \{1\}$, and $\mathcal{C}_5 = \{4\}$. Therefore, we are able to separately schedule $|\mathcal{P}| = 5$ subsets respectively over $|\mathcal{P}| = 5$ time slots, which leads to a symmetric SDoF of $\frac{1}{|\mathcal{P}|} = \frac{1}{5}$.

*Example 4.A (5-User TIM-CM Network: Transmission via SP):* Consider the network depicted in Fig. 4(a). Following a similar analogy as in Example 3.A, we can use its topology $\mathcal{G} = (\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_5, \mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_5)$ to obtain three secure partition subsets that collectively contain all five users once. For example, as also shown in Fig. 4(a), we can schedule transmitters in $\mathcal{P}_1 = \{2, 3, 5\}$, $\mathcal{P}_2 = \{1\}$, and $\mathcal{P}_3 = \{4\}$ respectively over $T = |\mathcal{P}| = |\{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}| = 3$ time slots and have the following sets serve as their respective cooperative jamming sets: $\mathcal{C}_1 = \{1\}$, $\mathcal{C}_2 = \{4\}$, and $\mathcal{C}_3 = \emptyset$. Therefore, this leads to a symmetric SDoF of $\frac{1}{|\mathcal{P}|} = \frac{1}{3}$.

Depending on the underlying network topology, it may be possible to achieve more symmetric SDoF than the secure partition scheme of Theorem 2, which allows each user to have only one secure interference free channel use per transmission block. In particular, each user may be able to use more than one secure interference free channel per transmission block. We will clarify this fact later on using concrete examples.

The following Theorem states our second lower bound on the symmetric SDoF.

*Theorem 3:* The symmetric SDoF for the $K$-user TIM-CM network is lower bounded as follows:

$$\mathsf{SDoF}^{\mathsf{sym}} \geq \sup_{T\in\mathbb{N}} \max_{\mathcal{U}_{s_1},\mathcal{U}_{s_2},\ldots,\mathcal{U}_{s_T}\in\mathcal{U}^{SIS}} \min_{k\in\{1,2,\ldots,K\}} \frac{\sum_{t=1}^{T} \mathbf{1}(k \in \mathcal{U}_{s_t})}{T}, \quad (8)$$

where $\mathcal{U}^{SIS} = \{\mathcal{U}_{s_1}, \mathcal{U}_{s_2}, \ldots, \mathcal{U}_{s_M}\}$ is the set of all secure independent sets for the network topology $\mathcal{G}$. Here, $\mathbf{1}(k \in \mathcal{A}) \triangleq 1$, if $k \in \mathcal{A}$ and 0 otherwise.

*Proof:* We can take $T$ secure independent sets $\mathcal{U}_{s_1}, \mathcal{U}_{s_2}, \ldots, \mathcal{U}_{s_T} \in \mathcal{U}^{SIS}$ and proceed with transmission, while preserving decodability (3) and confidentiality (4), as follows. Let all $|\mathcal{U}_{s_t}|$ transmitters in the set $\mathcal{U}_{s_t}$ send information messages during the same time slot $t \in \{1, 2, \ldots, T\}$. Since $\mathcal{U}_{s_t}$ is a secure independent set, there exists a set $\mathcal{C}_t$, $t \in \{1, 2, \ldots, T\}$, of cooperative jammers so that all transmitters in $\mathcal{U}_{s_t}$ can be simultaneously scheduled while satisfying both the decodability and confidentiality constraints. By doing this for all $T$ sets respectively over $T$ time slots, this implies that each user $k$ will get a total of $\sum_{t=1}^{T} \mathbf{1}(k \in \mathcal{U}_{s_t})$ secure interference free channels to use over transmission block $T$. This gives each user $k \in \{1, 2, \ldots, K\}$, a total of $\frac{\sum_{t=1}^{T} \mathbf{1}(k\in\mathcal{U}_{s_t})}{T}$ secure degrees of freedom. Since we are interested in the achievable symmetric SDoF, the largest SDoF that all users can simultaneously achieve for a given choice of $T$ and $\mathcal{U}_{s_1}, \mathcal{U}_{s_2}, \ldots, \mathcal{U}_{s_T}$ is given by $\min_{k\in\{1,2,\ldots,K\}} \frac{\sum_{t=1}^{T} \mathbf{1}(k\in\mathcal{U}_{s_t})}{T}$. Therefore, by optimizing the above over $T$ and $\mathcal{U}_{s_1}, \mathcal{U}_{s_2}, \ldots, \mathcal{U}_{s_T}$, we obtain $\sup_{T\in\mathbb{N}} \max_{\mathcal{U}_{s_1},\mathcal{U}_{s_2},\ldots,\mathcal{U}_{s_T}} \min_{k\in\{1,2,\ldots,K\}} \frac{\sum_{t=1}^{T} \mathbf{1}(k\in\mathcal{U}_{s_t})}{T}$, which is the symmetric SDoF lower bound in Theorem 3. Clearly, under this transmission scheme, each user may be assigned one or more secure interference free channel uses per transmission blocklength $T$. ■

We use Examples 3.B and 4.B to highlight the principles behind Theorem 3.

*Example 3.B (6-User TIM-CM Network: Transmission via SIS):* Consider the network of Fig. 3. From the topology of this network, we can readily infer the following:

- *(Independent Sets)*: According to Definition 6, this topology leads to independent sets $\{3\}$, $\{4, 6\}$, $\{1, 5, 6\}$, and $\{2, 5, 6\}$.
- *(Secure Independent Sets)*: According to Definition 7, this topology leads to secure independent sets $\{1\}$, $\{3\}$, $\{2, 6\}$, $\{4, 6\}$, and $\{5, 6\}$.

Transmission works as follows: In the first time slot, we can pick any of the three largest secure independent sets $\{2, 6\}$, $\{4, 6\}$, and $\{5, 6\}$ and schedule its users. Let us, for example, schedule the users in the SIS set $\mathcal{U}_{s_1} = \{2, 6\}$. Note that, as it is also depicted in Fig. 3(b), signals sent by Transmitters 2 and 6 are only observed at their respectively intended Receivers 2 and 6 and not seen at any other receivers as interference. Therefore, the messages from these two transmitter do not need protection at any other receivers. In other words, there is no need for any of the remaining four transmitters in the same network to act as a cooperative jammer during the first time slot. Thus, the cooperative jamming set in the first time slot is the empty set denoted by $\mathcal{C}_1 = \emptyset$.

In total, following the same logic, we can obtain five (not necessarily unique) secure independent sets that collectively contain each of the five users at least once, namely $\mathcal{U}_{s_1} = \{2, 6\}$, $\mathcal{U}_{s_2} = \{1\}$, $\mathcal{U}_{s_3} = \{3\}$, $\mathcal{U}_{s_4} = \{4, 6\}$, and $\mathcal{U}_{s_5} = \{5, 6\}$. Accordingly, the following (not necessarily unique) sets of transmitters can serve as cooperative jammers, respectively over five time slots: $\mathcal{C}_1 = \emptyset$, $\mathcal{C}_2 = \{3\}$, $\mathcal{C}_3 = \{2, 5, 6\}$, $\mathcal{C}_4 = \{1\}$, and $\mathcal{C}_5 = \{4\}$. As depicted in Fig. 3(b), by allowing the transmitters in the secure independent sets (cooperative jamming sets) to respectively send their messages (artificial noise symbols) over $T = 5$ time slots, one set per time slot, we can achieve a symmetric SDoF of $\frac{1}{5}$. We note here that this SDoF value is equivalent to the $\frac{1}{5}$ that we achieved in Example 3.A for the same topology through the secure partition scheme of Theorem 2.

Note that: $(i)$ In Example 4.A, we transmit using the SP scheme of Theorem 2 and, thus, only allow one secure interference free channel use per user over the whole transmission blocklength. $(ii)$ On the other hand (for the same exact topology as in Example 4.A), in Example 4.B below, we transmit using the SIS scheme of Theorem 3 which allows more than one secure interference free channel uses per user.

*Example 4.B (5-User TIM-CM Network: Transmission via SIS):* Consider the network in Fig. 4.

Following a similar analogy as in Example 3.B, we can use its topology $\mathcal{G} = (\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_5, \mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_5)$ to obtain five (not necessarily unique) secure independent sets that collectively contain each of the five users at least once. For example, as also shown in Fig. 4(b), we can schedule

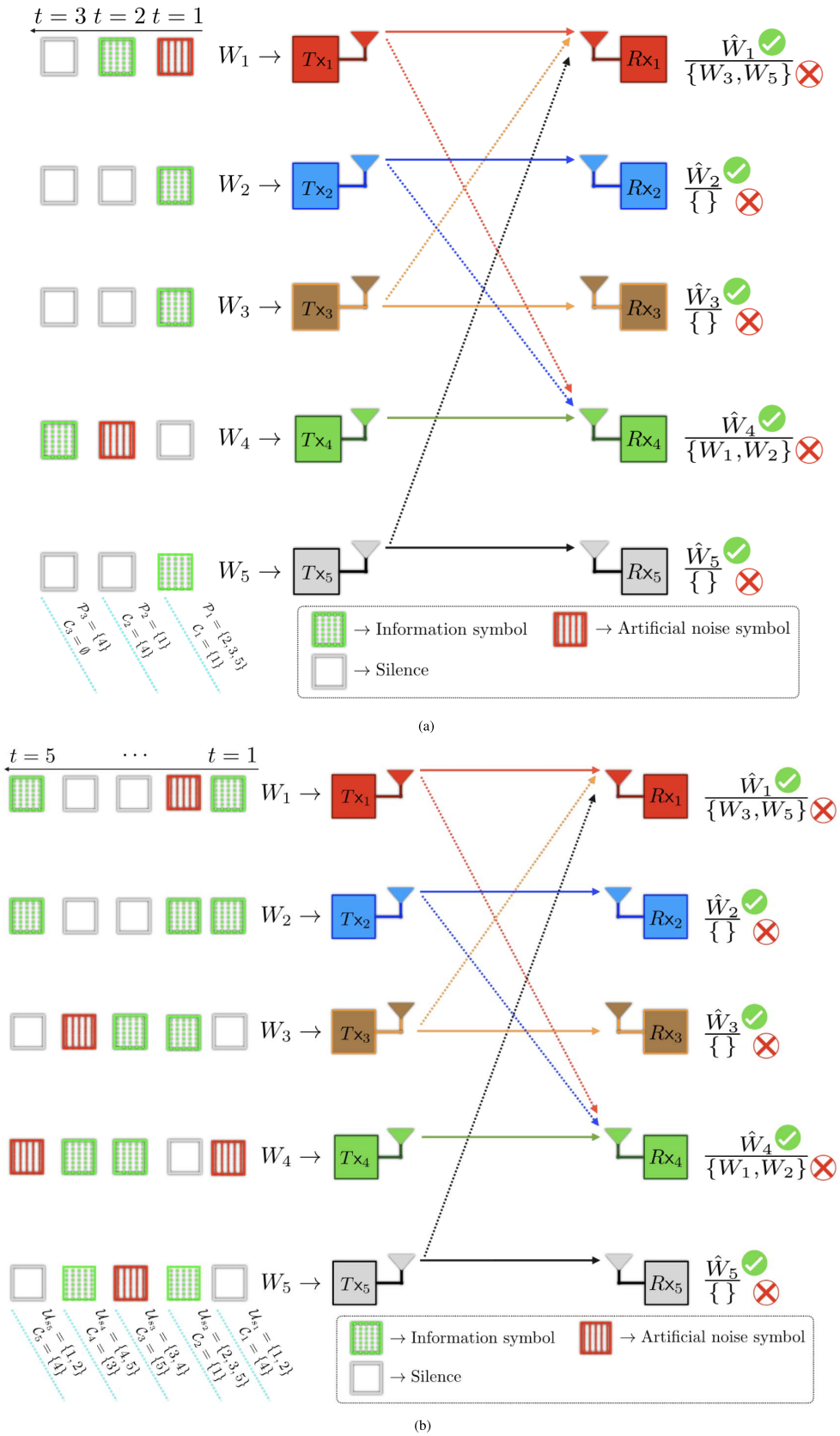


Fig. 4. 5-user TIM-CM network contrasting: (a) Transmission via secure partition versus (b) Transmission via secure independent sets.

transmitters in $\mathcal{U}_{s_1} = \{1, 2\}$, $\mathcal{U}_{s_2} = \{2, 3, 5\}$, $\mathcal{U}_{s_3} = \{3, 4\}$, $\mathcal{U}_{s_4} = \{4, 5\}$, and $\mathcal{U}_{s_5} = \{1, 2\}$ respectively over $T = 5$ time slots and have the following (not necessarily unique) sets serve as their respective cooperative jamming sets: $\mathcal{C}_1 = \{4\}$, $\mathcal{C}_2 = \{1\}$, $\mathcal{C}_3 = \{5\}$, $\mathcal{C}_4 = \{3\}$, and $\mathcal{C}_5 = \{4\}$. Therefore, we are able to allow two secure interference free channels

uses for each user over the transmission block $T$, leading to a symmetric SDoF of $\frac{2}{5}$. We note here that this symmetric SDoF value is greater than the $\frac{1}{3}$ that we achieved in Example 4.A for the same network through the secure partition scheme of Theorem 2.

*Remark 1:* (Transmission without secrecy): For the topology in Fig. 4, the TIM scheme of [36] achieves a DoF of $\frac{1}{2}$. To achieve this, in the absence of secrecy constraints, we can schedule the transmitters in the two independent sets $\{1,2\}$ and $\{3,4,5\}$ to respectively transmit over $T=2$ time slots, one set per time slot, thereby achieving a (nonsecure) symmetric DoF of $\frac{1}{2}$. Moreover, we note here that, this DoF matches the upper bound derived by [17] and [32].

### *B. Outer Bounds on Symmetric SDoF*

In this Section, we present upper bounds on symmetric SDoF for the TIM-CM problem. The Theorem below states our first upper bound on the symmetric SDoF and its proof is provided in Appendix IV-B. Here, we first provide a few important definitions before stating the Theorem.

Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two arbitrary and disjoint subsets of receivers, i.e., such that $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$ and $\mathcal{S}_1, \mathcal{S}_2 \subseteq \{1,2,\ldots,K\}$. Suppose $\mathcal{S}_2 = \{m_1, m_2, \ldots, m_{|\mathcal{S}_2|}\}$ and let $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_{m_q}\}_{q=1}^{|\mathcal{S}_2|}$ be the collection of all index sets of transmitters whose signals are respectively seen at the receivers in $\mathcal{S}_2$. Furthermore, define $\mu(\mathcal{S}_1,\mathcal{S}_2) \triangleq \min_{\mathcal{V}_2(\mathcal{S}_2),\mathcal{V}_1(\mathcal{S}_1)} |(\mathcal{U}(\mathcal{S}_2) \setminus \mathcal{V}_2(\mathcal{S}_2)) \setminus \mathcal{V}_1(\mathcal{S}_1)|$. Suppose $\mathcal{S}_2 = \{m_1, m_2, \ldots, m_{|\mathcal{S}_2|}\}$, where $\mathcal{V}_2(\mathcal{S}_2) = \{j_1, j_2, \ldots, j_{|\mathcal{S}_2|}\}$ is an arbitrary set of indexes $j_q \in \mathcal{I}_{m_q}$ for $m_q \in \mathcal{S}_2$ and $\mathcal{V}_1(\mathcal{S}_1) = \{\ell_1, \ell_2, \ldots, \ell_{|\mathcal{S}_1|}\}$ is an arbitrary set of indexes $\ell_p \in \mathcal{I}_{r_p}$ for $r_p \in \mathcal{S}_1 = \{r_1, r_2, \ldots, r_{|\mathcal{S}_1|}\}$. Moreover, let $\mathcal{I}_k$ be the index set of all signals that are seen as interference at receiver $R\mathsf{x}_k$ and $\mathcal{T}_k = \{k\} \cup \mathcal{I}_k$.

*Theorem 4:* The symmetric SDoF for the $K$-user TIM-CM network is upper bounded as follows:

$$\mathsf{SDoF}^{\mathsf{sym}} \leq \min_{\mathcal{S}1,\mathcal{S}_2} \frac{|\mathcal{S}_1| + \mu(\mathcal{S}_1,\mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) + \sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset)}. \quad (9)$$

As detailed in Appendix IV-B, the upper bound in Theorem 4 is based on the analysis of the received signal structures at all $K$ receivers and their respective interference components. To prove the Theorem, we first show how to get a nontrivial upper bound on secrecy rate by discarding all but one interference components from the received signal. Next, we show that the secrecy rate of the resulting signal can be bounded in two different ways, using which we then deduce the desired upper bound. We use Examples 3.C and 4.C to highlight the principles behind Theorem 4.

*Example 3.C (6-User TIM-CM Network: Upper Bound on Symmetric SDoF):* Let us revisit the 6-user TIM-CM network in Fig. 3. Our aim is to show that we can obtain a symmetric SDoF upper bound of $\frac{1}{3}$. To this end, we can now proceed as follows: Let us pick two disjoint subsets of receivers $\mathcal{S}_1 = \{2,4,6\}$ and $\mathcal{S}_2 = \{1,3,5\}$. We note here that the users in $\mathcal{S}_1$ have interference sets $\mathcal{I}_2 = \{1,3,4\}$, $\mathcal{I}_4 = \{3,5\}$ and $\mathcal{I}_6 = \{3\}$, whereas the users in $\mathcal{S}_2$ have interference sets $\mathcal{I}_1 = \{4\}$, $\mathcal{I}_3 = \{1\}$ and $\mathcal{I}_5 = \{3\}$, respectively. Therefore, $\sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) = \sum_{r_p \in \mathcal{S}_1 = \{2,4,6\}} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) = 3$ and $\sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset) = \sum_{m_q \in \mathcal{S}_2 = \{1,3,5\}} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset) = 3$. Moreover, we can, for example, pick the multi-set $\mathcal{U}(\mathcal{S}_2)$ and the two sets $\mathcal{V}_2(\mathcal{S}_2)$ and $\mathcal{V}_1(\mathcal{S}_1)$ as follows:

- $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_1, \mathcal{T}_3, \mathcal{T}_5\} = \{\{1,4\},\{1,3\},\{3,5\}\} = \{1,1,3,3,4,5\}$.
- $\mathcal{V}_2(\mathcal{S}_2) = \{4,1,3\}$, where $4 \in \mathcal{I}_1$, $1 \in \mathcal{I}_3$, and $3 \in \mathcal{I}_5$.
- $\mathcal{V}_1(\mathcal{S}_1) = \{1,5,3\}$, where $1 \in \mathcal{I}_2$, $5 \in \mathcal{I}_4$, and $3 \in \mathcal{I}_6$.

Thus, using its definition, we can calculate $\mu(\mathcal{S}_1,\mathcal{S}_2)$ as follows:

$$\begin{aligned}\mu(\mathcal{S}_1,\mathcal{S}_2) &= |(\mathcal{U}(\mathcal{S}_2) \setminus \mathcal{V}_2(\mathcal{S}_2)) \setminus \mathcal{V}_1(\mathcal{S}_1)| \\ &= |(\{1,1,3,3,4,5\} \setminus \{4,1,3\}) \setminus \{1,5,3\}| = 0.\end{aligned}$$

Therefore, using the above, we obtain the following upper bound on symmetric SDoF:

$$\begin{aligned}&\mathsf{SDoF}^{\mathsf{sym}} \\ &\leq \min_{\mathcal{S}1,\mathcal{S}_2} \frac{|\mathcal{S}_1| + \mu(\mathcal{S}_1,\mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) + \sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset)} \\ &\leq \frac{1}{3}.\end{aligned}$$

*Example 4.C (5-User TIM-CM Network: Upper Bound on Symmetric SDoF):* Let us revisit the 5-user TIM-CM network in Fig. 4. Our aim is to show that we can obtain a symmetric SDoF upper bound of $\frac{1}{2}$, which is thus close to the achievable lower bound of $\frac{2}{5}$ that we derived in Example 4.B for the same topology (via secure independent sets). To this end, we can now proceed as follows: Let us pick two disjoint subsets of receivers $\mathcal{S}_1 = \{1,4\}$ and $\mathcal{S}_2 = \{2,3\}$. We note here that the users in $\mathcal{S}_1$ have interference sets $\mathcal{I}_1 = \{3,5\}$ and $\mathcal{I}_4 = \{1,2\}$, whereas the users in $\mathcal{S}_2$ have interference sets $\mathcal{I}_2 = \emptyset$ and $\mathcal{I}_3 = \emptyset$, respectively. Therefore, $\sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) = \sum_{r_p \in \mathcal{S}_1 = \{1,4\}} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) = 2$ and $\sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset) = \sum_{m_q \in \mathcal{S}_2 = \{2,3\}} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset) = 0$. Moreover, we can, for example, pick the multi-set $\mathcal{U}(\mathcal{S}_2)$ and the two sets $\mathcal{V}_2(\mathcal{S}_2)$ and $\mathcal{V}_1(\mathcal{S}_1)$ as follows:

- $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_2, \mathcal{T}_3\} = \{\{2\},\{3\}\} = \{2,3\}$.
- $\mathcal{V}_2(\mathcal{S}_2) = \{3,2\}$, where $3 \in \mathcal{I}_1$ and $2 \in \mathcal{I}_4$.
- $\mathcal{V}_1(\mathcal{S}_1) = \emptyset$, because $\mathcal{I}_2 = \emptyset$ and $\mathcal{I}_3 = \emptyset$.

Thus, using its definition, we can calculate $\mu(\mathcal{S}_1,\mathcal{S}_2)$ as follows:

$$\begin{aligned}\mu(\mathcal{S}_1,\mathcal{S}_2) &= |(\mathcal{U}(\mathcal{S}_2) \setminus \mathcal{V}_2(\mathcal{S}_2)) \setminus \mathcal{V}_1(\mathcal{S}_1)| \\ &= |(\{2,3\} \setminus \{3,2\}) \setminus \emptyset| = 0.\end{aligned}$$

Therefore, using the above, we obtain the following upper bound on symmetric SDoF:

$$\begin{aligned}&\mathsf{SDoF}^{\mathsf{sym}} \\ &\leq \min_{\mathcal{S}1,\mathcal{S}_2} \frac{|\mathcal{S}_1| + \mu(\mathcal{S}_1,\mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) + \sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset)} \\ &\leq \frac{1}{2}.\end{aligned}$$

We next present our second upper bound in Theorem 5, which we later show to be tighter for some examples compared

to the results of Theorem 4. The main difference between this upper bound and the first one is that we now exploit the potential presence of *fractional signal generators* within the network, a concept that was introduced in [36], [60] for the nonsecrecy constrained TIM problem. This is a paradigm where the interference signal component of the received signal at some receiver can generate either a statistically equivalent version of the received signal at some other receiver or its cleaner version, i.e., with less interference. To this end, let us first define a fractional signal generator.

*Definition 9 (Fractional Signal Generator):* Let $\mathcal{I}_k$ be the index set of all signals that are seen as interference at receiver $R\mathsf{x}_k$ and $\mathcal{T}_k = \{k\} \cup \mathcal{I}_k$. We say that a receiver $R\mathsf{x}_k$ is a fractional signal generator of $\mathcal{G}_k$, if $\mathcal{G}_k \subseteq \mathcal{I}_k$ and there exists a permutation $\Pi^{(k)} = (\Pi_1, \Pi_2, \dots \Pi_{|\mathcal{G}_k|})$ of the set $\mathcal{G}_k$ such that $\mathcal{G}_k \setminus \{\Pi_1, \Pi_2, \dots, \Pi_i\} \subseteq \mathcal{I}_{\Pi_i}$, for $i = 1, 2, \dots, |\mathcal{G}_k|$.

Consider the 6-user network topology depicted in Fig. 3. In this network, $R\mathsf{x}_2$ receives signals from Transmitters 1, 2, 3, and 4. This fact can be equivalently denoted as $\mathcal{T}_2 = \{2\} \cup \mathcal{I}_2 = \{1, 2, 3, 4\}$. The main idea behind Definition 9 is that, by following a not necessarily unique successive order, $R\mathsf{x}_2$ can generate the signal index set $\mathcal{G}_2 = \{3, 4\}$ because $\mathcal{G}_2 \subseteq \mathcal{I}_2 = \{1, 3, 4\}$. More specifically, we next demonstrate why $R\mathsf{x}_2$ is called a fractional signal generator for the signal index set $\mathcal{G}_2$:

- First, we show how $R\mathsf{x}_2$ can generate the second element of $\mathcal{G}_2$, i.e., 4. Because the order of signal generation matters, we denote this fact by $(\{3, 4\} \setminus \{4\}) = \{3\} \subseteq \mathcal{I}_4 = \{3, 5\}$. This indicates that by first generating 4, we only remain with $\{3\}$ which is a subset of the interference set $\mathcal{I}_4 = \{3, 5\}$ at $R\mathsf{x}_4$. As we will show in the second step below, this order of signal generation will enable the generation of the first element of $\mathcal{G}_2$, i.e., 3. To this end, assume that the interference component $X_1^n$ seen from $T\mathsf{x}_1$ is provided by a genie to $R\mathsf{x}_2$. In turn, this allows $R\mathsf{x}_2$ to discard this interference signal component from its composite interference component in order to generate a signal $\tilde{Y}_4^n$ with components $\{3, 4\}$, which is an enhanced version of the original signal $Y_4^n$, whose components are $\mathcal{T}_4 = \{3, 4, 5\}$. In other words, the newly generated signal $\tilde{Y}_4^n$ is the enhanced version $Y_4^n$ because $\tilde{Y}_4^n$ has only one interference term, i.e., sees signals from $T\mathsf{x}_3$, whereas the original signal $Y_4^n$ has two interference terms, i.e., sees signals from $T\mathsf{x}_3$ and $T\mathsf{x}_5$. Therefore, if $R\mathsf{x}_4$ can decode its intended message $W_4$ from the original signal $Y_4^n$, then its enhanced version $\tilde{R}\mathsf{x}_4$ can also decode $W_4$ from $\tilde{Y}_4^n$.
- Second, we show how further processing of the signal at $R\mathsf{x}_2$ can generate the first element of the $\mathcal{G}_2$, i.e., 3. We denote this by $(\{3\} \setminus \{3\}) = \emptyset$ to indicate that 3 is the element of $\mathcal{G}_2$ which is generated the last. The intuition behind this second step is as follows: From the interference subset $\{3, 4\}$ at $R\mathsf{x}_2$ (i.e., having already removed the interference term from $T\mathsf{x}_1$ in the above step), one can next discard the (genie provided) interference component seen from $T\mathsf{x}_4$ in order to generate a signal $\tilde{Y}_3^n$ with a single component $\{3\}$, which is the enhanced version of the original signal $Y_3^n$, whose components are $\mathcal{T}_3 = \{1, 3\}$. Therefore, if $R\mathsf{x}_3$ can decode its intended message $W_3$ from the original signal $Y_3^n$, then $\tilde{R}\mathsf{x}_3$ can also decode $W_3$ from $\tilde{Y}_3^n$.

Therefore, successive decodability of $W_3$ and $W_4$, from the signals generated by the interference signal at $R\mathsf{x}_2$, follows the sequence $\Pi^{(2)} = (4, 3)$, which satisfies Definition 9.

The Theorem below states our second upper bound on the symmetric SDoF and its proof is provided in Appendix IV-B. Here, we first provide a few important definitions before stating the Theorem.

Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two arbitrary and disjoint subsets of receivers, i.e., such that $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$ and $\mathcal{S}_1, \mathcal{S}_2 \subseteq \{1, 2, \dots, K\}$. Suppose $\mathcal{S}_2 = \{m_1, m_2, \dots, m_{|\mathcal{S}_2|}\}$ and let $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_{m_q}\}_{q=1}^{|\mathcal{S}_2|}$ be the collection of all index sets of transmitters whose signals are respectively seen at the receivers in $\mathcal{S}_2$. Consider a collection of sets $\mathcal{G}^{\mathcal{S}_2} = \{\mathcal{G}_{m_1}^{(2)}, \mathcal{G}_{m_2}^{(2)}, \dots, \mathcal{G}_{m_{|\mathcal{S}_2|}}^{(2)}\}$ such that Receiver $m_q$ is a generator of $\mathcal{G}_{m_q}^{(2)} \subseteq \mathcal{I}_{m_q}$ for all $q \in \{1, 2, \dots, |\mathcal{S}_2|\}$, with a permutation $\Pi^{(m_q)} = \{\Pi_1^{(m_q)}, \Pi_2^{(m_q)}, \dots \Pi_{|\mathcal{G}_{m_q}^{(2)}|}^{(m_q)}\}$ according to Definition 9. Then, let $\tilde{\mathcal{V}}(\mathcal{S}_2) = \{\Pi_{|\mathcal{G}_{m_1}^{(2)}|}^{(m_1)}, \Pi_{|\mathcal{G}_{m_2}^{(2)}|}^{(m_2)}, \dots \Pi_{|\mathcal{G}_{m_{|\mathcal{S}_2|}}^{(2)}|}^{(m_{|\mathcal{S}_2|})}\}$ be an arbitrary set of indexes $\Pi_{|\mathcal{G}_{m_q}^{(2)}|}^{(m_q)} \in \mathcal{I}_{m_q}$ for $m_q \in \mathcal{S}_2$. Similarly, suppose $\mathcal{S}_1 = \{r_1, r_2, \dots r_{|\mathcal{S}_1|}\}$ and consider a collection of sets $\mathcal{G}^{\mathcal{S}_1} = \{\mathcal{G}_{r_1}^{(1)}, \mathcal{G}_{r_2}^{(1)}, \dots, \mathcal{G}_{r_{|\mathcal{S}_1|}}^{(1)}\}$ such that Receiver $r_p$ is a generator of $\mathcal{G}_{r_p}^{(1)} \subseteq \mathcal{I}_{r_p}$ for all $p \in \{1, 2, \dots, |\mathcal{S}_1|\}$, with a permutation $\Pi^{(r_p)} = \{\Pi_1^{(r_p)}, \Pi_2^{(r_p)}, \dots \Pi_{|\mathcal{G}_{r_p}^{(1)}|}^{(r_p)}\}$ according to Definition 9. Then, let $\tilde{\mathcal{V}}_1(\mathcal{S}_1)) = \{\Pi_{|\mathcal{G}_{r_1}^{(1)}|}^{(r_1)}, \Pi_{|\mathcal{G}_{r_2}^{(1)}|}^{(r_2)}, \dots \Pi_{|\mathcal{G}_{r_{|\mathcal{S}_1|}}^{(1)}|}^{(r_{|\mathcal{S}_1|})}\}$ be an arbitrary set of indexes $\Pi_{|\mathcal{G}_{r_p}^{(1)}|}^{(r_p)} \in \mathcal{I}_{r_p}$ for $r_p \in \mathcal{S}_1$. Define $\tilde{\mu}(\mathcal{S}_1, \mathcal{S}_2) \triangleq |(\mathcal{U}(\mathcal{S}_2) \setminus \tilde{\mathcal{V}}_2(\mathcal{S}_2)) \setminus \tilde{\mathcal{V}}_1(\mathcal{S}_1))|$ and let $\mathcal{I}_k$ be the index set of all signals that are seen as interference at receiver $R\mathsf{x}_k$ and $\mathcal{T}_k = \{k\} \cup \mathcal{I}_k$.

*Theorem 5:* The symmetric SDoF for the $K$-user TIM-CM network is upper bounded as follows:

$$\mathsf{SDoF}^{\mathsf{sym}} \leq \min_{(\mathcal{S}1, \mathcal{S}_2)} \min_{(\mathcal{G}^{\mathcal{S}_1}, \mathcal{G}^{\mathcal{S}_2})} \frac{|\mathcal{S}_1| + \tilde{\mu}(\mathcal{S}_1, \mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} |\mathcal{G}_{r_p}^{(1)}| + \sum_{q=1}^{|\mathcal{S}_2|} |\mathcal{G}_{m_q}^{(2)}|}. \tag{10}$$

As detailed in Appendix IV-B, the upper bound in Theorem 5 is also based on the analysis of the received signal structures at all $K$ receivers and their respective interference components with regard to the underlying arbitrary topology. To prove the Theorem, we first show how to get a nontrivial bound on secrecy rate by discarding all the interference components in the received signal, except for those that can be sequentially generated from the interference signal according to Definition 9. Next, we show that the secrecy rate of the resulting signal can be bounded using two types of bounds from which we are then able to deduce the desired upper bound. We use Example 3.D to highlight the principles behind Theorem 5.

*Example 3.D (6-User TIM-CM Network: Upper Bound on Symmetric SDoF):* Let us revisit the 6-user TIM-CM network in Fig. 3. Our aim is to show that we can obtain a symmetric SDoF upper bound of $\frac{1}{4}$ which is a tighter bound compared to the $\frac{1}{3}$ obtained in Example 3.C. We note here that $\frac{1}{4}$ is close to the achievable lower bound of $\frac{1}{5}$ that we derived in Example 3.A (via secure partition) and 3.B (via secure sets) for the same network topology.

We can now proceed as follows: Let us, for example, pick two disjoint subsets receivers $\mathcal{S}_1 = \{2\}$ and $\mathcal{S}_2 = \{3\}$. According to Definition 9 of fractional signal generators, Receiver $2 \in \mathcal{S}_1$ (which has the interference set $\mathcal{I}_2 = \{1,3,4\}$), can generate the following (not necessarily unique) set $\mathcal{G}_2^{(1)} = \{3,4\}$, with a permutation sequence $\Pi^{(2)} = (4,3)$. Therefore, this leads to the multi-set $\mathcal{G}^{\mathcal{S}_1} = \mathcal{G}_2^{(1)} = \{3,4\}$, which is the collection of all signal sets generated by receivers in $\mathcal{S}_1$. Following a similar analogy, Receiver $3 \in \mathcal{S}_2$ (which has the interference set $\mathcal{I}_3 = \{1\}$) can only generate $\mathcal{G}_3^{(2)} = \{1\}$. Therefore, $\mathcal{G}^{\mathcal{S}_2} = \mathcal{G}_3^{(2)} = \{1\}$. This implies that $\sum_{p=1}^{|\mathcal{S}_1|} |\mathcal{G}_{r_p}^{(1)}| = \sum_{r_p \in \mathcal{S}_1 = \{2\}} |\mathcal{G}_{r_p}^{(1)}| = 2$, whereas $\sum_{q=1}^{|\mathcal{S}_2|} |\mathcal{G}_{m_q}^{(2)}| = \sum_{m_q \in \mathcal{S}_2 = \{3\}} |\mathcal{G}_{m_q}^{(2)}| = 1$. Moreover, we can, for example, pick the multi-set $\mathcal{U}(\mathcal{S}_2)$ and the two sets $\tilde{\mathcal{V}}(\mathcal{S}_2)$ and $\tilde{\mathcal{V}}_1(\mathcal{S}_1)$ as follows:

- $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_3\} = \{1,3\}$.
- $\tilde{\mathcal{V}}(\mathcal{S}_2) = \{\Pi^{(m_{|\mathcal{S}_2|})}_{|\mathcal{G}^{(2)}_{m_{|\mathcal{S}_2|}}|}\} = \{\Pi^{(3)}_{|\mathcal{G}_3^{(2)}|}\} = \{1\}$, where $1 \in \mathcal{G}_3^{(2)} \subseteq \mathcal{I}_3$.
- $\tilde{\mathcal{V}}_1(\mathcal{S}_1)) = \{\Pi^{(r_{|\mathcal{S}_1|})}_{|\mathcal{G}^{(1)}_{r_{|\mathcal{S}_1|}}|}\} = \{\Pi^{(2)}_{|\mathcal{G}_2^{(1)}|}\} = \{3\}$, where $3 \in \mathcal{G}_2^{(1)} \subseteq \mathcal{I}_2$.

Thus, using its definition, we can calculate $\tilde{\mu}(\mathcal{S}_1, \mathcal{S}_2)$ as follows:

$$\begin{aligned}\tilde{\mu}(\mathcal{S}_1,\mathcal{S}_2) &= |(\mathcal{U}(\mathcal{S}_2) \setminus \tilde{\mathcal{V}}_2(\mathcal{S}_2)) \setminus \tilde{\mathcal{V}}_1(\mathcal{S}_1))| \\ &= |(\{1,3\} \setminus \{1\}) \setminus \{3\}| = 0.\end{aligned}$$

Therefore, using the above, we obtain the following upper bound on symmetric SDoF:

$$\begin{aligned}&\mathsf{SDoF}^{\mathsf{sym}} \\ &\leq \min_{(\mathcal{S}1,\mathcal{S}_2)} \min_{(\mathcal{G}^{\mathcal{S}_1},\mathcal{G}^{\mathcal{S}_2})} \frac{|\mathcal{S}_1| + \tilde{\mu}(\mathcal{S}_1,\mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} |\mathcal{G}_{r_p}^{(1)}| + \sum_{q=1}^{|\mathcal{S}_2|} |\mathcal{G}_{m_q}^{(2)}|} \\ &\leq \frac{1}{4}.\end{aligned}$$

We now remark the following regarding the 5-user example network topology of Fig. 4.

*Remark 2:* Since the topology of Fig. 4 that we used in Example 4.C does not contain nontrivial fractional signal generators (i.e., where some of the receivers can generate more than one signal), applying the principles of Theorem 5 would also lead to the symmetric SDoF upper bound of $\frac{1}{2}$.

### C. Case Studies: Settling Symmetric SDoF for 2-User and 3-User Topologies

In this Section, we present two case studies: In the first one, we study the 2-user TIM-CM networks and, in the second one, we study the 3-user TIM-CM networks. To this end, we enumerate all possible (non-isomorphic) topologies for the 2-user and 3-user TIM-CM networks as respectively depicted in Fig. 5 and Fig. 6. We then apply the result of Theorem 1 to eliminate all topologies where positive symmetric SDoF is not feasible. To find the outer bounds for the remaining networks, i.e., where positive symmetric SDoF is feasible, we apply the upper bound results of Theorems 4 and 5. We then verify the optimality of symmetric SDoF by showing that these upper bounds match the lower bounds by applying the achievable result of Theorem 2 or 3, thereby settling the $K$-user TIM-CM problem for $K \leq 3$.

Our results can be readily applied to calculate the exact symmetric SDoF for all (nonisomorphic) 2-user TIM-CM topologies as respectively given in Fig. 5 (a)-(c). To avoid repetitiveness, here, we only show how to find the exact symmetric SDoF for all 3-user TIM-CM topologies. To this end, we first consider all the 3-user TIM-CM networks for which symmetric SDoF is zero, i.e., the topologies that satisfy the conditions of Theorem 1. As indicated in Fig. 6, symmetric SDoF is zero for networks in Fig. 6 (d), (g), (j), (k), (l), (m), (n), (o), and (p). As an illustrative example, we provide calculation of the exact symmetric SDoF for the network of Fig. 6 (o). The calculations for the other topologies (for which symmetric SDoF is zero) follow a similar analogy and are thus omitted here to avoid repetition.

Consider the network of Fig. 6 (o). At receiver $R\mathsf{x}_2$, we have $\mathcal{I}_2 = \{1,3\}$ and $\mathcal{T}_2 = \{2\} \cup \mathcal{I}_2 = \{1,2,3\}$. At receiver $R\mathsf{x}_3$, we have $\mathcal{I}_3 = \{1,2\}$ and $\mathcal{T}_3 = \{3\} \cup \mathcal{I}_3 = \{1,2,3\}$. We note here that for the two transmit-receive pairs $T\mathsf{x}_2 - R\mathsf{x}_2$ and $T\mathsf{x}_3 - R\mathsf{x}_3$, the conditions of Theorem 1 are satisfied because $(i)$ $2 \in \mathcal{I}_3$, $(ii)$ $3 \in \mathcal{I}_2$, and $(iii)$ $\mathcal{I}_3 \setminus \{2\} = \mathcal{I}_2 \setminus \{3\}$. Since the conditions of Theorem 1 are satisfied, then symmetric SDoF is zero for this network.

Second, we consider all the 3-user TIM-CM networks for which SDoF is nonzero, i.e., the topologies that do not satisfy the conditions of Theorem 1. As indicated in Fig. 6, symmetric SDoF is nonzero for networks in Fig. 6 (a), (b), (c), (e), (f), (h), and (i). It can easily be verified that for each of these topologies, except for the topology of Fig. 6 (h), the lower bound achieved using the secure partition scheme of Theorem 2 matches the upper bound obtained through the result of Theorem 4, thereby leading to their exact symmetric SDoF. For the network of Fig. 6 (h), we apply the result of Theorem 2 to find the lower bound. However, we use the result of Theorem 5 to find its matching upper bound instead of Theorem 4 because the latter leads to a loose bound.

As illustrative examples, we provide calculations of exact symmetric SDoF for the networks of Fig. 6 (e) and (h). The calculations for the other topologies (for which symmetric SDoF is nonzero) follow a similar analogy and are thus omitted here to avoid repetition.

Consider the 3-user network of Fig. 6 (e). At receiver $R\mathsf{x}_1$, we have $\mathcal{I}_1 = \emptyset$ and $\mathcal{T}_1 = \{1\} \cup \mathcal{I}_1 = \{1\}$. At $R\mathsf{x}_2$, we have $\mathcal{I}_2 = \{1,3\}$ and $\mathcal{T}_2 = \{2\} \cup \mathcal{I}_2 = \{1,2,3\}$. At $R\mathsf{x}_3$, we have $\mathcal{I}_3 = \emptyset$ and $\mathcal{T}_3 = \{3\} \cup \mathcal{I}_3 = \{3\}$. Then, we can apply the scheme of Theorem 2 by creating a secure partition $\mathcal{P} = \{\mathcal{P}_1 = \{1,3\}, \mathcal{P}_2 = \{2\}\}$ and scheduling the transmitters in $\mathcal{P}_1$ to send their respective messages over the first time

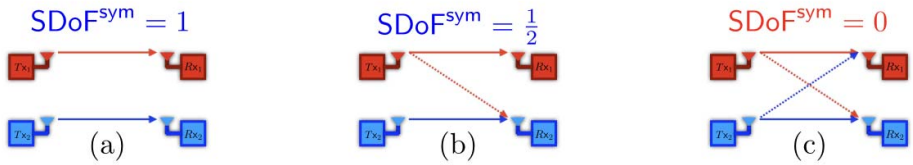


Fig. 5. Case study A: Application of current results to all 2-user TIM-CM networks.

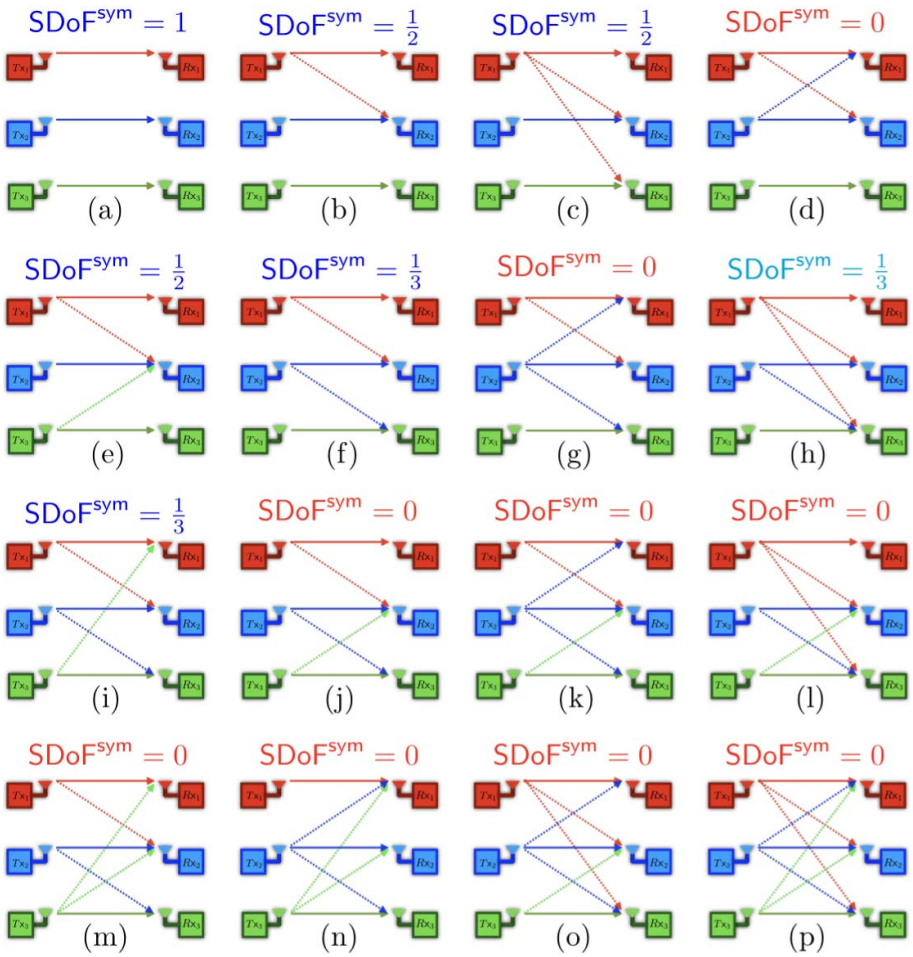


Fig. 6. Case study B: Application of current results to all 3-user TIM-CM networks.

slot (while the second transmitter $T\mathbf{x}_2$ acts as a cooperative jammer by sending an artificial noise symbol over the first time slot, i.e., $\mathcal{C}_1 = \{2\}$). We schedule the transmitter in $\mathcal{P}_2$ to send its message over the second time slot (while $T\mathbf{x}_1$ and $T\mathbf{x}_3$ remain silent over the second time slot, i.e., $\mathcal{C}_2 = \emptyset$). Therefore, we achieve a symmetric SDoF of $\frac{1}{|\mathcal{P}|} = \frac{1}{2}$ per user.

To find the upper bound on symmetric SDoF for the network of Fig. 6 (e), we apply the result of Theorem 4 as shown next. Let us pick two disjoint subsets of receivers $\mathcal{S}_1 = \{2\}$ and $\mathcal{S}_2 = \{3\}$. We note here that the user in $\mathcal{S}_1$ has interference set $\mathcal{I}_2 = \{1, 3\}$, whereas the user in $\mathcal{S}_2$ has interference set $\mathcal{I}_3 = \emptyset$. Therefore, $\sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) = \sum_{r_p \in \mathcal{S}_1 = \{2\}} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) = 1$ and $\sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset) = \sum_{m_q \in \mathcal{S}_2 = \{3\}} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset) = 0$. Moreover, we can, for example, pick the multi-set $\mathcal{U}(\mathcal{S}_2)$ and the two sets $\mathcal{V}_2(\mathcal{S}_2)$ and $\mathcal{V}_1(\mathcal{S}_1)$ as follows: $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_3\} = \{3\}$. $\mathcal{V}_2(\mathcal{S}_2) = \emptyset$ because $\mathcal{I}_3 = \emptyset$. $\mathcal{V}_1(\mathcal{S}_1) = \{3\}$, where $3 \in \mathcal{I}_2 = \{1, 3\}$. Thus, using its definition, we can calculate $\mu(\mathcal{S}_1, \mathcal{S}_2)$ as follows: $\mu(\mathcal{S}_1, \mathcal{S}_2) = |(\mathcal{U}(\mathcal{S}_2) \setminus \mathcal{V}_2(\mathcal{S}_2)) \setminus \mathcal{V}_1(\mathcal{S}_1)| = |(\{3\} \setminus \emptyset) \setminus \{3\}| = 0$. Therefore, using the above, we obtain the following upper bound on symmetric SDoF:

$$\begin{aligned} &\mathsf{SDoF}^{\mathsf{sym}} \\ &\leq \min_{\mathcal{S}1, \mathcal{S}_2} \frac{|\mathcal{S}_1| + \mu(\mathcal{S}_1, \mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) + \sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset)} \\ &\leq \frac{1}{2}. \end{aligned}$$

Thus, for this network, the upper bound matches the lower bound. This implies that its exact symmetric SDoF is $\frac{1}{2}$.

Consider the 3-user network of Fig. 6 (h). At receiver $R\mathsf{x}_1$, we have $\mathcal{I}_1 = \emptyset$ and $\mathcal{T}_1 = \{1\} \cup \mathcal{I}_1 = \{1\}$. At $R\mathsf{x}_2$, we have $\mathcal{I}_2 = \{1\}$ and $\mathcal{T}_2 = \{2\} \cup \mathcal{I}_2 = \{1, 2\}$. At $R\mathsf{x}_3$, we have $\mathcal{I}_3 = \{1, 3\}$ and $\mathcal{T}_3 = \{3\} \cup \mathcal{I}_3 = \{1, 2, 3\}$. Then, we can apply the scheme of Theorem 2 by creating a secure partition $\mathcal{P} = \{\mathcal{P}_1 = \{1\}, \mathcal{P}_2 = \{2\}, \mathcal{P}_3 = \{3\}\}$. In turn, this implies that we can schedule the transmitter in $\mathcal{P}_1$ to send its message over the first time slot (while $T\mathsf{x}_2$ acts as a cooperative jammer by sending an artificial noise symbol and $T\mathsf{x}_3$ remains silent over the first time slot, i.e., $\mathcal{C}_1 = \{2\}$) and schedule the transmitter in $\mathcal{P}_2$ to send its message over the second time slot (while $T\mathsf{x}_1$ remains silent and $T\mathsf{x}_3$ acts as a cooperative jammer by sending an artificial noise symbol over the second time slot, i.e., $\mathcal{C}_2 = \{3\}$). Over the third time slot, we schedule the transmitter in $\mathcal{P}_3$ to send its message (while $T\mathsf{x}_1$ and $T\mathsf{x}_2$ remain silent, i.e., $\mathcal{C}_3 = \emptyset$). Therefore, we achieve a symmetric SDoF of $\frac{1}{|\mathcal{P}|} = \frac{1}{3}$ per user.

Finding the upper bound on symmetric SDoF for the network of Fig. 6 (h) by applying the result of Theorem 4 leads to a symmetric SDoF of $\frac{1}{2}$, which is greater than the achieved above lower bound. Since this network contains fractional signal generators (as in Definition 9), we can improve the upper bound by applying the result of Theorem 5. As we show next, this leads to an upper bound that matches the above lower bound.

Let us, for example, pick two disjoint subsets of receivers $\mathcal{S}_1 = \{3\}$ and $\mathcal{S}_2 = \{1\}$. According to Definition 9 of fractional signal generators, Receiver $3 \in \mathcal{S}_1$ (which has the interference set $\mathcal{I}_2 = \{1, 2\}$), can generate the set $\mathcal{G}_3^{(1)} = \{1, 2\}$, with a permutation sequence $\Pi^{(3)} = (2, 1)$. Therefore, this leads to the multi-set $\mathcal{G}^{\mathcal{S}_1} = \mathcal{G}_3^{(1)} = \{1, 2\}$, which is the collection of all signal sets generated by the receivers in $\mathcal{S}_1$. Following a similar analogy, Receiver $1 \in \mathcal{S}_2$ (which has the interference set $\mathcal{I}_1 = \emptyset$) does not generate any signals sets, i.e., $\mathcal{G}_1^{(2)} = \emptyset$. Therefore, $\mathcal{G}^{\mathcal{S}_2} = \mathcal{G}_1^{(2)} = \emptyset$. This implies that $\sum_{p=1}^{|\mathcal{S}_1|} |\mathcal{G}_{r_p}^{(1)}| = \sum_{r_p \in \mathcal{S}_1 = \{3\}} |\mathcal{G}_{r_p}^{(1)}| = 2$, whereas $\sum_{q=1}^{|\mathcal{S}_2|} |\mathcal{G}_{m_q}^{(2)}| = \sum_{m_q \in \mathcal{S}_2 = \{1\}} |\mathcal{G}_{m_q}^{(2)}| = 0$. Moreover, we can, for example, pick the multi-set $\mathcal{U}(\mathcal{S}_2)$ and the two sets $\tilde{\mathcal{V}}(\mathcal{S}_2)$ and $\tilde{\mathcal{V}}_1(\mathcal{S}_1))$ as follows: $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_1\} = \{1\}$. $\tilde{\mathcal{V}}(\mathcal{S}_2) = \{\Pi^{(m_{|\mathcal{S}_2|})}_{|\mathcal{G}^{(2)}_{m_{|\mathcal{S}_2|}}|}\} = \emptyset$ because $\mathcal{G}_1^{(2)} = \emptyset$. $\tilde{\mathcal{V}}_1(\mathcal{S}_1)) = \{\Pi^{(r_{|\mathcal{S}_1|})}_{|\mathcal{G}^{(1)}_{r_{|\mathcal{S}_1|}}|}\} = \{\Pi^{(3)}_{|\mathcal{G}_3^{(1)}|}\} = \{1\}$, where $1 \in \mathcal{G}_3^{(1)} = \mathcal{I}_3$. Thus, using its definition, we can calculate $\tilde{\mu}(\mathcal{S}_1, \mathcal{S}_2)$ as follows: $\tilde{\mu}(\mathcal{S}_1, \mathcal{S}_2) = |(\mathcal{U}(\mathcal{S}_2) \setminus \tilde{\mathcal{V}}_2(\mathcal{S}_2)) \setminus \tilde{\mathcal{V}}_1(\mathcal{S}_1))| = |(\{1\} \setminus \emptyset) \setminus \{1\}| = 0$. Therefore, using the above, we obtain the following upper bound on symmetric SDoF:

$$\begin{aligned}
&\mathsf{SDoF}^{\mathsf{sym}} \\
&\leq \min_{(\mathcal{S}1, \mathcal{S}_2)} \min_{(\mathcal{G}^{\mathcal{S}_1}, \mathcal{G}^{\mathcal{S}_2})} \frac{|\mathcal{S}_1| + \tilde{\mu}(\mathcal{S}_1, \mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} |\mathcal{G}_{r_p}^{(1)}| + \sum_{q=1}^{|\mathcal{S}_2|} |\mathcal{G}_{m_q}^{(2)}|} \\
&\leq \frac{1}{3}.
\end{aligned}$$

Thus, for this network, the upper bound matches the lower bound. This implies that its exact symmetric SDoF is $\frac{1}{3}$.

## IV. Conclusion

In this paper, we studied the impact of network topology on symmetric SDoF for the $K$-user partially connected interference networks with confidential messages in the absence of CSIT, except for the knowledge of network topology and channel statistics, a setting we named the general TIM-CM problem. We first presented necessary and sufficient conditions for the feasibility of positive symmetric SDoF for any topology. We then presented inner bounds on symmetric SDoF for the TIM-CM problem. For the first lower bound, we introduced and demonstrated how to utilize the concept of secure partition. For the second one, we introduced and showed how to utilize the concept of secure independent sets. We also presented outer bounds on symmetric SDoF. First, we showed how to collectively manage the interference components of the received signals at all receivers in order to obtain the first nontrivial upper bound. Then, through our second outer bound, we demonstrated that the first one can be made tighter in the presence of fractional signal generators. We also provided several examples to further clarify the principles behind each of our proposed results and their application in calculating symmetric SDoF. In the end, we presented case studies through which we characterized the optimal symmetric SDoF for all $K$-user TIM-CM topologies with $K \leq 3$. To the best of our knowledge, this is the first work to do a comprehensive study of the general TIM-CM problem.

This work opens up several avenues for future research directions. The main one is that of finding the exact symmetric SDoF for the general TIM-CM problem. Another avenue is to investigate the topology conditions under which the secure partition based transmission scheme is better than the secure independent sets scheme in terms of spectral efficiency or vice versa.

## Appendix A
## Proof of Theorem 1

In this Section, we present the proof of Theorem 1: Its converse is provided in Appendix IV-A, whereas the achievability is provided in Appendix IV-B.

### A. Converse Proof

Consider the $K$-user TIM-CM network and suppose there exists a pair of users $i, j \in \{1, 2, \ldots, K\}$, for $i \neq j$, such that $(i)$ $i \in \mathcal{I}_j$, $(ii)$ $j \in \mathcal{I}_i$, and $(iii)$ $\mathcal{I}_i \setminus \{j\} \subseteq \mathcal{I}_j \setminus \{i\}$, i.e., satisfying the conditions of Theorem 1. The signals seen at receivers $R\mathsf{x}_i$ and $R\mathsf{x}_j$ at time $t$ can then be written as follows:

$$Y_i(t) = h_{ii} X_i(t) + \sum_{m \in \mathcal{I}_i} h_{im} X_m(t) + Z_i(t), \tag{11}$$

$$Y_j(t) = h_{jj} X_j(t) + \sum_{m \in \mathcal{I}_j} h_{jm} X_m(t) + Z_j(t). \tag{12}$$

We next show that since the considered user pair $i, j$ satisfies the conditions of Theorem 1, then positive symmetric SDoF is not feasible, i.e, it is zero. To this end, we now create a virtual receiver $\tilde{R}\mathsf{x}_j$ which is a genie-enhanced version of the

original receiver $R\mathsf{x}_j$. Note that $\mathcal{I}_j = (\mathcal{I}_j \setminus \{i\}) \cup \{i\}$, and by condition $(iii)$ $\mathcal{I}_i \setminus \{j\} \subseteq \mathcal{I}_j \setminus \{i\}$. Therefore, $(\mathcal{I}_i \setminus \{j\}) \cup \{i\} \subseteq (\mathcal{I}_j \setminus \{i\}) \cup \{i\} = \mathcal{I}_j$. Since $(\mathcal{I}_i \setminus \{j\}) \cup \{i\}$ is a subset of $\mathcal{I}_j$, we can let receiver $\tilde{R}\mathsf{x}_j$ be as shown next. Consider the received signal at $R\mathsf{x}_j$ and let a genie provide the interfering signals set $X^n_{\mathcal{I}_j \setminus \mathcal{I}_i}$ (i.e., corresponding to the interference index set $\mathcal{I}_j \setminus \mathcal{I}_i$) to receiver $R\mathsf{x}_j$. This leads to an enhanced receiver $\tilde{R}\mathsf{x}_j$ with the following output at time $t$:

$$\tilde{Y}_j(t) = h_{jj}X_j(t) + \sum_{m \in (\mathcal{I}_i \setminus \{j\}) \cup \{i\}} h_{jm}X_m(t) + Z_j(t). \tag{13}$$

We note here that, if receiver $R\mathsf{x}_j$ can decode so can receiver $\tilde{R}\mathsf{x}_j$ because $(\mathcal{I}_i \setminus \{j\}) \cup \{i\}$ is a subset of $\mathcal{I}_j$. The above enhancement leads to a statistically equivalent receive pair $(R\mathsf{x}_i, \tilde{R}\mathsf{x}_j)$ that can be represented by a 2-user symmetric interference network defined by:

$$Y_i(t) = \sum_{m \in \mathcal{T}_i} h_{im}X_m(t) + Z_i(t) \tag{14}$$

$$\tilde{Y}_j(t) = \sum_{m \in \tilde{\mathcal{T}}_j} h_{jm}X_m(t) + Z_j(t), \tag{15}$$

where $\tilde{\mathcal{T}}_j = \{j\} \cup (\mathcal{I}_i \setminus \{j\}) \cup \{i\} = \mathcal{T}_i$. To complete the proof, we use the remaining steps to show that the SDoF at the original receiver $R\mathsf{x}_j$ is upper bounded by the SDoF at the enhanced receiver $\tilde{R}\mathsf{x}_j$, which is zero. To this end, we start by upperbounding the secrecy rate $R_j$ at $R\mathsf{x}_j$ as follows:

$$\begin{aligned}
nR_j &= H(W_j|\mathcal{H}) && (16)\\
&= I(W_j; Y^n_j|\mathcal{H}) + H(W_j|Y^n_j, \mathcal{H}) && (17)\\
&= I(W_j; Y^n_j|\mathcal{H}) + no(n), && (18)\\
&\leq I(W_j; Y^n_j, X^n_{\mathcal{I}_j \setminus \mathcal{I}_i}|\mathcal{H}) + no(n) && (19)\\
&= I(W_j; X^n_{\mathcal{I}_j \setminus \mathcal{I}_i}|\mathcal{H}) + I(W_j; Y^n_j|X^n_{\mathcal{I}_j \setminus \mathcal{I}_i}, \mathcal{H}) + no(n) && (20)\\
&= I(W_j; Y^n_j|X^n_{\mathcal{I}_j \setminus \mathcal{I}_i}, \mathcal{H}) + no(n) && (21)\\
&= I(W_j; \tilde{Y}^n_j|\mathcal{H}) + no(n) && (22)\\
&= I(W_j; Y^n_i|\mathcal{H}) + no(n) && (23)\\
&= no(n), && (24)
\end{aligned}$$

where (18) is due to the decodability constraint in (3), (19) is due to the enhancement by a genie providing the interfering signals set $X^n_{\mathcal{I}_j \setminus \mathcal{I}_i}$ to receiver $R\mathsf{x}_j$, and (20) follows from the chain rule of mutual information. Equation (21) is due to the independence of $W_j$ from $X^n_{\mathcal{I}_j \setminus \mathcal{I}_i}$, whereas (22) follows from the fact that $\tilde{Y}^n_j$ is the enhanced version of $Y^n_j$. Equation (23) is due to the fact that the joint distribution of $(W_j, \tilde{Y}^n_j)$ is the same as the joint distribution of $(W_j, Y^n_i)$, whereas (24) is due to the secrecy constraint in (4). Taking the limit of (24) as $n \to \infty$, we get $R_j = 0$. This implies that the symmetric secrecy rate is zero. Therefore, by Definition 3, symmetric SDoF is also zero. ■

### *B. Achievability Proof*

Our aim is to show that symmetric SDoF is nonzero, if the conditions of Theorem 1 are not met. Consider the $K$-user TIM-CM network and suppose there is no single pair of users $i, j \in \{1, 2, \ldots, K\}$, for $i \neq j$, within the network that satisfies the conditions of Theorem 1. We next provide a simple secure TDMA algorithm that achieves SDoF of $\frac{1}{K}$.

The proposed secure transmission works as follows: Let $\mathcal{C}_t$ be the index set of transmitters that have to act as cooperative jammers (by sending artificial noise symbols) during the $t$th time slot. The following steps show how each transmitter $T\mathsf{x}_k$, for $k \in \{1, 2, \ldots, K\}$, can securely transmit its message $W_k$ during time slot $t \in \{1, 2, \ldots, T\}$:

(i) Let $T\mathsf{x}_k$ send $W_k$ over the $t$th time slot.
(ii) Let all transmitters in $\{\{T\mathsf{x}_i\}^K_{i \neq k}: i \in \mathcal{C}_t\}$ send artificial noise symbols during time slot $t$.
(iii) Let all transmitters $\{\{T\mathsf{x}_i\}^K_{i \neq k}: i \notin \mathcal{C}_t\}$ remain silent during time slot $t$.
(iv) Repeat steps $(i) - (iii)$ for a total of $T = K$ times.

We are thus able to separately serve the $K$ users over a transmission block of length $T = K$ time slots, which leads to a symmetric SDoF of $\frac{1}{K}$ per user. Note that $\frac{1}{K}$ is the least symmetric SDoF that can be achieved for any TIM-CM topology that is symmetric SDoF feasible. ■

## APPENDIX B
## PROOF OF THEOREM 4

Consider the signal $Y^n_k$ received at $R\mathsf{x}_k$ over transmission blocklength $n$. For simplicity of notation, we denote $\mathbf{H}^n_{ki} = h_{ki}\mathbf{I}_n$ as the channel matrix between transmitter $T\mathsf{x}_i$ and receiver $R\mathsf{x}_k$ over a block of length $n$, where $h_{ki}$ is the time-invariant channel coefficient and $\mathbf{I}_n$ is the $n \times n$ identity matrix. We invoke decodability and confidentiality constraints to upper bound the secrecy rate $R_k$ at $R\mathsf{x}_k$ as follows:

$$\begin{aligned}
nR_k &= H(W_k|\mathcal{H}) && (25)\\
&= I(W_k; Y^n_k|\mathcal{H}) + H(W_k|Y^n_k, \mathcal{H}) && (26)\\
&= I(W_k; Y^n_k|\mathcal{H}) + no(n) && (27)\\
&= I(W_k; Y^n_k|\mathcal{H}) - I(W_{\mathcal{I}_k}; Y^n_k|\mathcal{H}) \\
&\quad + I(\mathcal{W}_{\mathcal{I}_k}; Y^n_k|\mathcal{H}) + no(n) && (28)\\
&= h(Y^n_k|W_{\mathcal{I}_k}, \mathcal{H}) - h(Y^n_k|W_k, \mathcal{H}) \\
&\quad + I(\mathcal{W}_{\mathcal{I}_k}; Y^n_k|\mathcal{H}) + no(n) && (29)\\
&= h(Y^n_k|W_{\mathcal{I}_k}, \mathcal{H}) \\
&\quad - h(Y^n_k|W_k, \mathcal{H}) + no(n) && (30)\\
&\leq h(Y^n_k|W_{\mathcal{I}_k}, \mathcal{H}) \\
&\quad - h(Y^n_k|W_k, X^n_k, \mathcal{H}) + no(n) && (31)\\
&= h(Y^n_k|W_{\mathcal{I}_k}, \mathcal{H}) \\
&\quad - h(Y^n_k|X^n_k, \mathcal{H}) + no(n) && (32)\\
&= h(Y^n_k|W_{\mathcal{I}_k}, \mathcal{H}) \\
&\quad - h\left(\sum_{i \in \mathcal{T}_k} \mathbf{H}^n_{ki}X^n_i + Z^n_k \middle| X^n_k, \mathcal{H}\right) + no(n) && (33)\\
&= h(Y^n_k|W_{\mathcal{I}_k}, \mathcal{H}) \\
&\quad - h\left(\sum_{i \in \mathcal{I}_k} \mathbf{H}^n_{ki}X^n_i + Z^n_k \middle| \mathcal{H}\right) + no(n) && (34)\\
&\leq h(Y^n_k|W_{\mathcal{I}_k}, \mathcal{H})
\end{aligned}$$

$$- h\left(\sum_{i\in\mathcal{I}_k}\mathbf{H}_{ki}^n X_i^n + Z_k^n \Big| X_{\mathcal{I}_k\setminus\{i\}}^n, \mathcal{H}\right) + no(n) \quad (35)$$

$$= h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - h(\mathbf{H}_{ki}^n X_i^n + Z_k^n|\mathcal{H}) + no(n), \quad (36)$$

for all $i \in \mathcal{I}_k$. Here, (27) is due to Fano's inequality, (29) comes from the identity $I(X;Y) - I(X;Z) = h(X|Z) - h(X|Y)$, (30) is due to the secrecy constraint in (4), (31) is due to the fact that conditioning reduces entropy, (32) follows from the Markov chain $W_k \to X_k^n \to Y_k^n$, and (35) is due to the fact that conditioning reduces entropy. Starting with (36), we can then proceed as follows.

$$\begin{aligned} nR_k &\le h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - h(\mathbf{H}_{ki}^n X_i^n + Z_k^n|\mathcal{H}) + no(n) \\ &= h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - h(\tilde{Y}_i^n|\mathcal{H}) + no(n) \quad (37)\\ &= h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - I(W_i;\tilde{Y}_i^n|\mathcal{H}) \\ &\quad - h(\tilde{Y}_i^n|W_i,\mathcal{H}) + no(n) \quad (38)\\ &= h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - H(W_i|\mathcal{H}) + H(W_i|\tilde{Y}_i^n,\mathcal{H}) \\ &\quad - h(\tilde{Y}_i^n|W_i,\mathcal{H}) + no(n) \quad (39)\\ &= h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - nR_i + H(W_i|\tilde{Y}_i^n,\mathcal{H}) \\ &\quad - h(\tilde{Y}_i^n|W_i,\mathcal{H}) + no(n) \quad (40)\\ &= h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - nR_i - h(\tilde{Y}_i^n|W_i,\mathcal{H}) + no(n), \quad (41)\end{aligned}$$

for all $i \in \mathcal{I}_k$ and where (37) follows from substitution $\tilde{Y}_i^n = \mathbf{H}_{ki}^n X_i^n + Z_k^n$. Here, (41) is due to the fact that $\tilde{Y}_i^n$ is the enhanced version of the signal $Y_i^n$ seen at receiver $R\mathsf{x}_i$, and therefore due to the decodability constraint, $H(W_i|\tilde{Y}_i^n,\mathcal{H}) = o(n)$.

We now bound (41) in two different ways. We start with the first type of bound as follows:

$$\begin{aligned} n(R_i+R_k) &\le h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - h(\tilde{Y}_i^n|W_i,\mathcal{H}) + no(n) \quad (42)\\ &\le h(Y_k^n|\mathcal{H}) - h(\tilde{Y}_i^n|W_i,\mathcal{H}) + no(n) \quad (43)\\ &\le n\log(P) - h(\tilde{Y}_i^n|W_i,\mathcal{H}) \\ &\quad + no(n) + no(\log(P)), \quad (44)\end{aligned}$$

for all $i \in \mathcal{I}_k$. Here, (42) follows from rearranging the terms in (41), (43) is due to the fact that conditioning reduces entropy, and (44) follows from the fact that Gaussian distribution maximizes entropy [8]. We note here that, for any receiver $R\mathsf{x}_k$ with interference set $\mathcal{I}_k = \emptyset$, we would get the following bound instead of (44): $nR_k \le n\log(P) + no(\log(P))$.

We next derive the second type of bound. We start by bounding (42) as follows:

$$\begin{aligned} n(R_i+R_k) &\le h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) - h(\tilde{Y}_i^n|W_i,\mathcal{H}) + no(n) \\ &\le nR_k + \sum_{j\in\mathcal{T}_k} h(\tilde{Y}_j^n|W_j,\mathcal{H}) - h(\tilde{Y}_i^n|W_i,\mathcal{H}) \\ &\quad + no(\log(P)) + no(n), \quad (45)\end{aligned}$$

for all $i \in \mathcal{I}_k$ and where $\mathcal{T}_k = \{k\} \cup \mathcal{I}_k$. Here, (45) follows from bounding $h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H})$ using Lemma 1 below whose proof is in Appendix IV-B.

*Lemma 1:* Let $\tilde{Y}_i^n = \mathbf{H}_{ki}^n X_i^n + Z_k^n$, for all $i \in \mathcal{T}_k = \{k\} \cup \mathcal{I}_k$, then we have the following:

$$\begin{aligned} h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) &\le nR_k + \sum_{j\in\mathcal{T}_k} h(\tilde{Y}_j^n|W_j,\mathcal{H}) \\ &\quad + no(\log(P)). \quad (46)\end{aligned}$$

By simplifying (45), we then obtain the desired second type of bound:

$$\begin{aligned} nR_i &\le \sum_{j\in\mathcal{T}_k} h(\tilde{Y}_j^n|W_j,\mathcal{H}) - h(\tilde{Y}_i^n|W_i,\mathcal{H}) \\ &\quad + no(\log(P)) + no(n). \quad (47)\end{aligned}$$

Similarly, we note that for any $R\mathsf{x}_k$ with $\mathcal{I}_k = \emptyset$, we would get the following bound instead of (47): $0 \le \sum_{j\in\mathcal{T}_k} h(\tilde{Y}_j^n|W_j,\mathcal{H}) = h(\tilde{Y}_k^n|W_k,\mathcal{H})$.

For the purpose of the current paper, we are interested in symmetric SDoF. Therefore, we can now drop the indexing and instead use the notation $R_i = R^{\mathsf{sym}}, \forall i \in \{1,2,\ldots,K\}$, which represents the symmetric secrecy rate at any receiver. Moreover, as shown by (44) and (47), we get two types of bounds on $R^{\mathsf{sym}}$. Consider the receiver $R\mathsf{x}_k$. Then, from (44), we directly obtain the following first type of bound:

$$\begin{aligned} 2nR^{\mathsf{sym}} &\le n\log(P) - h(\tilde{Y}_i^n|W_i,\mathcal{H}) \\ &\quad + no(n) + no(\log(P)), \quad (48)\end{aligned}$$

for all $i \in \mathcal{I}_k$. We again note here that, for any receiver $R\mathsf{x}_k$ with $\mathcal{I}_k = \emptyset$, we would get $nR^{\mathsf{sym}} \le n\log(P) + no(\log(P))$ instead of (48). The second type of bound follows from (47) and is given by:

$$\begin{aligned} nR^{\mathsf{sym}} &\le \sum_{j\in\mathcal{T}_k} h(\tilde{Y}_j^n|W_j,\mathcal{H}) - h(\tilde{Y}_i^n|W_i,\mathcal{H}) \\ &\quad + no(\log(P)) + no(n), \quad (49)\end{aligned}$$

for all $i \in \mathcal{I}_k$ and where $\mathcal{T}_k = \{k\} \cup \mathcal{I}_k$. Similarly, we note that, for any $R\mathsf{x}_k$ with $\mathcal{I}_k = \emptyset$, we would get $0 \le \sum_{j\in\mathcal{T}_k} h(\tilde{Y}_j^n|W_j,\mathcal{H}) = h(\tilde{Y}_k^n|W_k,\mathcal{H})$ instead of (49).

We now remark the following fact which is heavily used in the subsequent steps of this proof.

*Remark 3:* Due to the absence of CSI at the transmitters, i.e., no CSIT under the TIM-CM framework, and the fact that the channel coefficients are i.i.d., the enhanced signal $\tilde{Y}_i^n = \mathbf{H}_{ki}^n X_i^n + Z_k^n$ is statistically equivalent to the enhanced signal $\tilde{Y}_i{}^n = \mathbf{H}_{ji}^n X_i^n + Z_j^n$, for all $k \ne j \in \{1,2,\ldots,K\}$.

We can now proceed as follows: Pick any two arbitrary and disjoint subsets of receivers $\mathcal{S}_1$ and $\mathcal{S}_2$, i.e., such that $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$ and $\mathcal{S}_1, \mathcal{S}_2 \subseteq \{1,2,\ldots,K\}$. For all receivers in $\mathcal{S}_1$, we can apply the first type of bound (48), and for all receivers in $\mathcal{S}_2$, we apply the second type of bound (49). Then, we can add up the resulting $|\mathcal{S}_1| + |\mathcal{S}_2|$ equations and see the resulting cancellation possible as a function of the set choices $(\mathcal{S}_1, \mathcal{S}_2)$. Moreover, suppose $\mathcal{S}_1 = \{r_1, r_2, \ldots, r_{|\mathcal{S}_1|}\}$ and $\mathcal{S}_2 = \{m_1, m_2, \ldots, m_{|\mathcal{S}_2|}\}$. Thus, by adding up all the

equations and rearranging terms, we obtain the following:

$$\begin{aligned} nR^{\mathsf{sym}} &\left( |\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) \right) \\ &+ nR^{\mathsf{sym}} \sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset) \\ &\leq |\mathcal{S}_1| n \log(P) + no(\log(P)) + no(n) \\ &+ \underbrace{\sum_{m_q \in \mathcal{S}_2} \sum_{i \in \mathcal{I}_{m_q}} h(\tilde{Y}_i^n | W_i, \mathcal{H})}_{\mathcal{U}(\mathcal{S}_2)} \\ &- \underbrace{\sum_{j_q \in \mathcal{I}_{m_q} : m_q \in \mathcal{S}_2} h(\tilde{Y}_{j_q}^n | W_{j_q}, \mathcal{H})}_{\mathcal{V}_2(\mathcal{S}_2)} \\ &- \underbrace{\sum_{\ell_p \in \mathcal{I}_{r_p} : r_p \in \mathcal{S}_1} h(\tilde{Y}_{\ell_p}^n | W_{\ell_p}, \mathcal{H})}_{\mathcal{V}_1(\mathcal{S}_1)}. \end{aligned} \tag{50}$$

Starting with the last three terms in (50), it is clear that the aim should be to choose the indexes for signal components corresponding to the set choices $\mathcal{S}_1$ and $\mathcal{S}_2$ in a way that allows the maximum cancellation of the entropy terms, while taking advantage of the signal distribution properties stated in Remark 3. Depending upon the network topology $\mathcal{G}$, this cancellation will then result in zero or more positive entropy terms. We calculate the number of these remaining positive entropy terms as shown next.

To calculate the number of (positive) entropy terms resulting from $\sum_{m_q \in \mathcal{S}_2} \sum_{i \in \mathcal{I}_{m_q}} h(\tilde{Y}_i^n | W_i, \mathcal{H})$, we can use the cardinality of the collection of all index sets of transmitters whose signals are respectively seen at the receivers in $\mathcal{S}_2 = \{m_1, m_2, \ldots, m_{|\mathcal{S}_2|}\}$. We denote this multi-set of transmitter indexes as $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_{m_q}\}_{q=1}^{|\mathcal{S}_2|}$. To calculate the number of (negative) entropy terms resulting from $\sum_{j_q \in \mathcal{I}_{m_q} : m_q \in \mathcal{S}_2} h(\tilde{Y}_{j_q}^n | W_{j_q}, \mathcal{H})$, we use the cardinality of the set denoted by $\mathcal{V}_2(\mathcal{S}_2) = \{j_1, j_2, \ldots, j_{|\mathcal{S}_2|}\}$, which is an arbitrary set of indexes $j_q \in \mathcal{I}_{m_q}$ for $m_q \in \mathcal{S}_2$. Similarly, to calculate the number of (negative) entropy terms resulting from $\sum_{\ell_p \in \mathcal{I}_{r_p} : r_p \in \mathcal{S}_1} h(\tilde{Y}_{\ell_p}^n | W_{\ell_p}, \mathcal{H})$, we use the cardinality of the set denoted by $\mathcal{V}_1(\mathcal{S}_1) = \{\ell_1, \ell_2, \ldots, \ell_{|\mathcal{S}_1|}\}$, which is an arbitrary set of indexes $\ell_p \in \mathcal{I}_{r_p}$ for $r_p \in \mathcal{S}_1 = \{r_1, r_2, \ldots, r_{|\mathcal{S}_1|}\}$.

From the defined above three sets, we can then calculate the resulting number of (positive) entropy terms as follows:

$$\mu(\mathcal{S}_1, \mathcal{S}_2) = \min_{\mathcal{V}_2(\mathcal{S}_2), \mathcal{V}_1(\mathcal{S}_1)} |(\mathcal{U}(\mathcal{S}_2) \setminus \mathcal{V}_2(\mathcal{S}_2)) \setminus \mathcal{V}_1(\mathcal{S}_1)|. \tag{51}$$

As indicated in (2), each signal is transmitted with an average power constraint $P$. Thus, each of the $\mu(\mathcal{S}_1, \mathcal{S}_2)$ entropy terms can be upper bounded by $n \log(P)$. Therefore, using (50) and (51), we can upper bound the secrecy rate as follows:

$$\begin{aligned} &nR^{\mathsf{sym}} \\ &\leq \frac{|\mathcal{S}_1| n \log(P) + \mu(\mathcal{S}_1, \mathcal{S}_2) n \log(P)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) + \sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset)} \\ &+ \frac{no(\log(P)) + no(n)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) + \sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset)}. \end{aligned} \tag{52}$$

Then, by dividing both sides of (52) by $n \log(P)$, minimizing over all choices of $(\mathcal{S}_1, \mathcal{S}_2)$, and taking the limit as $n \to \infty$ and $P \to \infty$, we obtain the following upper bound on symmetric SDoF:

$$\begin{aligned} &\mathsf{SDoF}^{\mathsf{sym}} \\ &\leq \min_{\mathcal{S}1, \mathcal{S}_2} \frac{|\mathcal{S}_1| + \mu(\mathcal{S}_1, \mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} \mathbf{1}(\mathcal{I}_{r_p} \neq \emptyset) + \sum_{q=1}^{|\mathcal{S}_2|} \mathbf{1}(\mathcal{I}_{m_q} \neq \emptyset)}, \end{aligned} \tag{53}$$

which completes the proof of Theorem 4. ■

## Appendix C
## Proof of Theorem 5

We now present the proof of Theorem 5. As it will be demonstrated by the steps below, the main difference between Theorem 4 and Theorem 5 lies in the way, for a given receiver $R\mathsf{x}_k$, we lower bound the entropy of the interfering signals' component $h\left(\sum_{i \in \mathcal{I}_k} \mathbf{H}_{ki}^n X_i^n + Z_k^n | \mathcal{H}\right)$ from (34) when receiver $R\mathsf{x}_k$ is fractional signal generator as given by Definition 9.

Consider the signal $Y_k^n$ received at $R\mathsf{x}_k$ over transmission blocklength $n$. Starting with (34), we can upper bound the symmetric secrecy rate $R^{\mathsf{sym}}$ as follows:

$$\begin{aligned} nR^{\mathsf{sym}} &\leq h(Y_k^n | W_{\mathcal{I}_k}, \mathcal{H}) \\ &\quad - h\left(\sum_{i \in \mathcal{I}_k} \mathbf{H}_{ki}^n X_i^n + Z_k^n \Big| \mathcal{H}\right) + no(n) \\ &\leq h(Y_k^n | W_{\mathcal{I}_k}, \mathcal{H}) - n|\mathcal{G}_k| R^{\mathsf{sym}} \\ &\quad - h(\tilde{Y}_{\Pi_{|\mathcal{G}_k|}}^n | W_{\Pi_{|\mathcal{G}_k|}}, \mathcal{H}) + no(n), \end{aligned} \tag{54}$$

where $\Pi_{|\mathcal{G}_k|} \in \mathcal{G}_k \subseteq \mathcal{I}_k$ and (54) follows from Lemma 2 below whose proof is in Appendix IV-B.

*Lemma 2:* Let $\tilde{Y}_i^n = \mathbf{H}_{ki}^n X_i^n + Z_k^n$, for all $i \in \mathcal{T}_k = \{k\} \cup \mathcal{I}_k$, and consider any set $\mathcal{G}_k \subseteq \mathcal{I}_k$ and a permutation sequence $\Pi^{(k)} = (\Pi_1, \Pi_2, \ldots \Pi_{|\mathcal{G}_k|})$ of the elements of $\mathcal{G}_k$ satisfying Definition 9, then

$$\begin{aligned} h\left(\sum_{i \in \mathcal{I}_k} \mathbf{H}_{ki}^n X_i^n + Z_k^n \Big| \mathcal{H}\right) &\geq n|\mathcal{G}_k| R^{\mathsf{sym}} \\ &\quad + h(\tilde{Y}_{\Pi_{|\mathcal{G}_k|}}^n | W_{\Pi_{|\mathcal{G}_k|}}, \mathcal{H}) + no(n). \end{aligned} \tag{55}$$

We now bound (54) in two different ways. We start with the first type of bound as follows:

$$\begin{aligned} nR^{\mathsf{sym}} &\leq h(Y_k^n | W_{\mathcal{I}_k}, \mathcal{H}) - n|\mathcal{G}_k| R^{\mathsf{sym}} \\ &\quad - h(\tilde{Y}_{\Pi_{|\mathcal{G}_k|}}^n | W_{\Pi_{|\mathcal{G}_k|}}, \mathcal{H}) + no(n) \\ &\leq h(Y_k^n | \mathcal{H}) - n|\mathcal{G}_k| R^{\mathsf{sym}} \\ &\quad - h(\tilde{Y}_{\Pi_{|\mathcal{G}_k|}}^n | W_{\Pi_{|\mathcal{G}_k|}}, \mathcal{H}) + no(n) \qquad (56) \\ &\leq n \log(P) - n|\mathcal{G}_k| R^{\mathsf{sym}} \\ &\quad - h(\tilde{Y}_{\Pi_{|\mathcal{G}_k|}}^n | W_{\Pi_{|\mathcal{G}_k|}}, \mathcal{H}) \\ &\quad + no(n) + no(\log(P)), \qquad (57) \end{aligned}$$

where $\Pi_{|\mathcal{G}_k|} \in \mathcal{G}_k \subseteq \mathcal{I}_k$, (56) is due to the fact that conditioning reduces entropy, and (57) follows from the fact that Gaussian distribution maximizes entropy [8]. By rearranging the terms in (57), we then obtain the desired first type of bound:

$$nR^{\mathsf{sym}}(1+|\mathcal{G}_k|) \leq n\log(P) - h(\tilde{Y}^n_{\Pi_{|\mathcal{G}_k|}}|W_{\Pi_{|\mathcal{G}_k|}},\mathcal{H}) + no(n), \tag{58}$$

where $\Pi_{|\mathcal{G}_k|} \in \mathcal{G}_k \subseteq \mathcal{I}_k$. We next derive the second type of bound. To this end, we start with (54) as follows:

$$\begin{aligned} nR^{\mathsf{sym}} &\leq h(Y^n_k|W_{\mathcal{I}_k},\mathcal{H}) - n|\mathcal{G}_k|R^{\mathsf{sym}} \\ &\quad - h(\tilde{Y}^n_{\Pi_{|\mathcal{G}_k|}}|W_{\Pi_{|\mathcal{G}_k|}},\mathcal{H}) + no(n) \\ &\leq nR^{\mathsf{sym}} + \sum_{i\in\mathcal{T}_k} h(\tilde{Y}^n_i|W_i,\mathcal{H}) + no(\log(P)) \\ &\quad - n|\mathcal{G}_k|R^{\mathsf{sym}} - h(\tilde{Y}^n_{\Pi_{|\mathcal{G}_k|}}|W_{\Pi_{|\mathcal{G}_k|}},\mathcal{H}) + no(n), \end{aligned} \tag{59}$$

where $\Pi_{|\mathcal{G}_k|} \in \mathcal{G}_k \subseteq \mathcal{I}_k$ and (59) follows from upperbounding $h(Y^n_k|W_{\mathcal{I}_k},\mathcal{H})$ using Lemma 1. By simplifying and rearranging the terms in (59), we then obtain the desired second type of bound:

$$\begin{aligned} nR^{\mathsf{sym}}|\mathcal{G}_k| &\leq \sum_{i\in\mathcal{T}_k} h(\tilde{Y}^n_i|W_i,\mathcal{H}) \\ &\quad - h(\tilde{Y}^n_{\Pi_{|\mathcal{G}_k|}}|W_{\Pi_{|\mathcal{G}_k|}},\mathcal{H}) + no(\log(P)) + no(n), \end{aligned} \tag{60}$$

where $\Pi_{|\mathcal{G}_k|} \in \mathcal{G}_k \subseteq \mathcal{I}_k$.

We can now proceed as follows: Pick any two arbitrary and disjoint subsets of receivers $\mathcal{S}_1$ and $\mathcal{S}_2$, i.e., such that $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$ and $\mathcal{S}_1, \mathcal{S}_2 \subseteq \{1,2,\ldots,K\}$. Suppose $\mathcal{S}_1 = \{r_1, r_2, \ldots r_{|\mathcal{S}_1|}\}$. Consider a collection of sets $\mathcal{G}^{\mathcal{S}_1} = \{\mathcal{G}^{(1)}_{r_1}, \mathcal{G}^{(1)}_{r_2}, \ldots, \mathcal{G}^{(1)}_{r_{|\mathcal{S}_1|}}\}$ such that Receiver $r_p$ is a generator of $\mathcal{G}^{(1)}_{r_p} \subseteq \mathcal{I}_{r_p}$ for all $p \in \{1,2,\ldots,|\mathcal{S}_1|\}$, with a permutation $\Pi^{(r_p)} = \{\Pi^{(r_p)}_1, \Pi^{(r_p)}_2, \ldots \Pi^{(r_p)}_{|\mathcal{G}^{(1)}_{r_p}|}\}$ according to Definition 9. Similarly, suppose $\mathcal{S}_2 = \{m_1, m_2, \ldots m_{|\mathcal{S}_2|}\}$. Consider a collection of sets $\mathcal{G}^{\mathcal{S}_2} = \{\mathcal{G}^{(2)}_{m_1}, \mathcal{G}^{(2)}_{m_2}, \ldots, \mathcal{G}^{(2)}_{m_{|\mathcal{S}_2|}}\}$ such that Receiver $m_q$ is a generator of $\mathcal{G}^{(2)}_{m_q} \subseteq \mathcal{I}_{m_q}$ for all $q \in \{1,2,\ldots,|\mathcal{S}_2|\}$, with a permutation $\Pi^{(m_q)} = \{\Pi^{(m_q)}_1, \Pi^{(m_q)}_2, \ldots \Pi^{(m_q)}_{|\mathcal{G}^{(2)}_{m_q}|}\}$ according to Definition 9. Then, for all receivers in $\mathcal{S}_1$, we can apply the first type of bound (58), and for all receivers in $\mathcal{S}_2$, we apply the second type of bound (60). Then, we add up the resulting $|\mathcal{S}_1| + |\mathcal{S}_2|$ equations, and see the resulting cancellation possible as a function of the choice of $(\mathcal{S}_1, \mathcal{S}_2, \mathcal{G}^{\mathcal{S}_1}, \mathcal{G}^{\mathcal{S}_2})$. Thus, by adding up all the equations and rearranging terms, we obtain the following:

$$\begin{aligned} &nR^{\mathsf{sym}}\left(|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|}|\mathcal{G}^{(1)}_{r_p}|\right) + nR^{\mathsf{sym}}\sum_{q=1}^{|\mathcal{S}_2|}|\mathcal{G}^{(2)}_{m_q}| \\ &\leq |\mathcal{S}_1|n\log(P) + no(\log(P)) + no(n) \\ &\quad + \underbrace{\sum_{m_q\in\mathcal{S}_2}\sum_{i\in\mathcal{T}_{m_q}} h(\tilde{Y}^n_i|W_i,\mathcal{H})}_{\mathcal{U}(\mathcal{S}_2)} \\ &\quad \underbrace{- \sum_{\Pi^{(m_q)}_{|\mathcal{G}^{(2)}_{m_q}|}\in\mathcal{I}_{m_q}:m_q\in\mathcal{S}_2} h\left(\tilde{Y}^n_{\Pi^{(m_q)}_{|\mathcal{G}^{(2)}_{m_q}|}}\Big|W_{\Pi^{(m_q)}_{|\mathcal{G}^{(2)}_{m_q}|}},\mathcal{H}\right)}_{\tilde{\mathcal{V}}_2(\mathcal{S}_2)} \\ &\quad \underbrace{- \sum_{\Pi^{(r_p)}_{|\mathcal{G}^{(1)}_{r_p}|}\in\mathcal{I}_{r_p}:r_p\in\mathcal{S}_1} h\left(\tilde{Y}^n_{\Pi^{(r_p)}_{|\mathcal{G}^{(1)}_{r_p}|}}\Big|W_{\Pi^{(r_p)}_{|\mathcal{G}^{(1)}_{r_p}|}},\mathcal{H}\right)}_{\tilde{\mathcal{V}}_1(\mathcal{S}_1)}. \end{aligned} \tag{61}$$

Starting with the last three terms in (61), we follow the same logic as in the proof of Theorem 4. Clearly, the aim here should be to choose the indexes for signal components corresponding to the set choices $\mathcal{S}_1$ and $\mathcal{S}_2$ in a way that allows the maximum cancellation of the entropy terms, while taking advantage of the signal distribution properties stated in Remark 3. Depending upon the network topology $\mathcal{G}$, this cancellation will then result in zero or more positive entropy terms. We calculate the number of these remaining positive entropy terms as shown next.

To calculate the number of (positive) entropy terms resulting from $\sum_{m_q\in\mathcal{S}_2}\sum_{i\in\mathcal{T}_{m_q}} h(\tilde{Y}^n_i|W_i,\mathcal{H})$, we can use the cardinality of the collection of all index sets of transmitters whose signals are respectively seen at the receivers in $\mathcal{S}_2 = \{m_1, m_2, \ldots, m_{|\mathcal{S}_2|}\}$. We denote this multi-set of transmitter indexes as $\mathcal{U}(\mathcal{S}_2) = \{\mathcal{T}_{m_q}\}_{q=1}^{|\mathcal{S}_2|}$. To calculate the number of (negative) entropy terms resulting from $\sum_{\Pi^{(m_q)}_{|\mathcal{G}^{(2)}_{m_q}|}\in\mathcal{I}_{m_q}:m_q\in\mathcal{S}_2} h(\tilde{Y}^n_{\Pi^{(m_q)}_{|\mathcal{G}^{(2)}_{m_q}|}}|W_{\Pi^{(m_q)}_{|\mathcal{G}^{(2)}_{m_q}|}},\mathcal{H})$, we use the cardinality of the set denoted by $\tilde{\mathcal{V}}_2(\mathcal{S}_2) = \{\Pi^{(m_1)}_{|\mathcal{G}^{(2)}_{m_1}|}, \Pi^{(m_2)}_{|\mathcal{G}^{(2)}_{m_2}|}, \ldots \Pi^{(m_{|\mathcal{S}_2|})}_{|\mathcal{G}^{(2)}_{m_{|\mathcal{S}_2|}}|}\}$, which is an arbitrary set of indexes $\Pi^{(m_q)}_{|\mathcal{G}^{(2)}_{m_q}|} \in \mathcal{I}_{m_q}$ for $m_q \in \mathcal{S}_2$. Similarly, to calculate the number of (negative) entropy terms resulting from $\sum_{\Pi^{(r_p)}_{|\mathcal{G}^{(1)}_{r_p}|}\in\mathcal{I}_{r_p}:r_p\in\mathcal{S}_1} h(\tilde{Y}^n_{\Pi^{(r_p)}_{|\mathcal{G}^{(1)}_{r_p}|}}|W_{\Pi^{(r_p)}_{|\mathcal{G}^{(1)}_{r_p}|}},\mathcal{H})$, we use the cardinality of the set denoted by $\tilde{\mathcal{V}}_1(\mathcal{S}_1)) = \{\Pi^{(r_1)}_{|\mathcal{G}^{(1)}_{r_1}|}, \Pi^{(r_2)}_{|\mathcal{G}^{(1)}_{r_2}|}, \ldots \Pi^{(r_{|\mathcal{S}_1|})}_{|\mathcal{G}^{(1)}_{r_{|\mathcal{S}_1|}}|}\}$, which is an arbitrary set of indexes $\Pi^{(r_p)}_{|\mathcal{G}^{(1)}_{r_p}|} \in \mathcal{I}_{r_p}$ for $r_p \in \mathcal{S}_1$. From the defined above three sets, we can then calculate the resulting number of (positive) entropy terms as follows:

$$\tilde{\mu}(\mathcal{S}_1,\mathcal{S}_2) = |(\mathcal{U}(\mathcal{S}_2) \setminus \tilde{\mathcal{V}}_2(\mathcal{S}_2)) \setminus \tilde{\mathcal{V}}_1(\mathcal{S}_1))|. \tag{62}$$

As indicated in (2), each signal is transmitted with an average power constraint $P$. Thus, each of the $\tilde{\mu}(\mathcal{S}_1,\mathcal{S}_2)$ entropy terms can be upper bounded by $n\log(P)$. Therefore, using (61) and (62), we can upper bound the secrecy rate as follows:

$$\begin{aligned} nR^{\mathsf{sym}} &\leq \frac{|\mathcal{S}_1|n\log(P) + \tilde{\mu}(\mathcal{S}_1,\mathcal{S}_2)n\log(P)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|}|\mathcal{G}^{(1)}_{r_p}| + \sum_{q=1}^{|\mathcal{S}_2|}|\mathcal{G}^{(2)}_{m_q}|} \\ &\quad + \frac{no(\log(P)) + no(n)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|}|\mathcal{G}^{(1)}_{r_p}| + \sum_{q=1}^{|\mathcal{S}_2|}|\mathcal{G}^{(2)}_{m_q}|}. \end{aligned} \tag{63}$$

Then, by dividing both sides of (63) by $n\log(P)$, minimizing over all choices of $(\mathcal{S}_1, \mathcal{S}_2, \mathcal{G}^{\mathcal{S}_1}, \mathcal{G}^{\mathcal{S}_2})$, and taking the limit as

$n \to \infty$ and $P \to \infty$, we obtain the following upper bound on symmetric SDoF:

$$\mathsf{SDoF}^{\mathsf{sym}} \leq \min_{(\mathcal{S}1,\mathcal{S}_2)} \min_{(\mathcal{G}^{\mathcal{S}_1},\mathcal{G}^{\mathcal{S}_2})} \frac{|\mathcal{S}_1| + \tilde{\mu}(\mathcal{S}_1,\mathcal{S}_2)}{|\mathcal{S}_1| + \sum_{p=1}^{|\mathcal{S}_1|} |\mathcal{G}_{r_p}^{(1)}| + \sum_{q=1}^{|\mathcal{S}_2|} |\mathcal{G}_{m_q}^{(2)}|}, \tag{64}$$

which completes the proof of Theorem 5. ■

## Appendix D
## Proof of Lemma 1

Let $\tilde{Y}_i^n = \mathbf{H}_{ki}^n X_i^n + Z_k^n$, for $i \in \mathcal{T}_k = \{k\} \cup \mathcal{I}_k$. To prove Lemma 1, we proceed as follows:

$$\begin{aligned}
h(Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) &= I(W_k;Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (65)\\
&\leq I(W_k;Y_k^n,\tilde{Y}_{\mathcal{I}_k}^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (66)\\
&= I(W_k;Y_k^n|W_{\mathcal{I}_k},\mathcal{H}) + I(W_k,\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (67)\\
&= H(W_k|W_{\mathcal{I}_k},\mathcal{H}) - H(W_k|Y_k^n,W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad + I(W_k,\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,W_{\mathcal{I}_k},\mathcal{H}) + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (68)\\
&= H(W_k|\mathcal{H}) - H(W_k|Y_k^n,\mathcal{H}) \\
&\quad + I(W_k,\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,W_{\mathcal{I}_k},\mathcal{H}) + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (69)\\
&= nR_k + no(n) + I(W_k,\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (70)\\
&= nR_k + no(n) + h(\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad - h(\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (71)\\
&\leq nR_k + no(n) + h(\tilde{Y}_{\mathcal{I}_k}^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad - h(\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (72)\\
&\leq nR_k + no(n) + h(\tilde{Y}_{\mathcal{I}_k}^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad - h(\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,W_{\{k\}\cup\mathcal{I}_k},X_{\mathcal{I}_k}^n,\mathcal{H}) \\
&\quad + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (73)\\
&= nR_k + no(n) + h(\tilde{Y}_{\mathcal{I}_k}^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad - h(\tilde{Y}_{\mathcal{I}_k}^n|Y_k^n,X_{\mathcal{I}_k}^n,W_k,\mathcal{H}) + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (74)\\
&= nR_k + no(n) + h(\tilde{Y}_{\mathcal{I}_k}^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad - h(Z_{\mathcal{I}_k}^n|Y_k^n,W_k,\mathcal{H}) + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (75)\\
&\leq nR_k + no(n) + h(\tilde{Y}_{\mathcal{I}_k}^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad - h(Z_{\mathcal{I}_k}^n) + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (76)\\
&= nR_k + no(n) + h(\tilde{Y}_{\mathcal{I}_k}^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad + no(\log(P)) + h(Y_k^n|W_{\{k\}\cup\mathcal{I}_k},\mathcal{H}) && (77)\\
&\leq nR_k + no(n) + h(\tilde{Y}_{\mathcal{I}_k}^n|W_{\mathcal{I}_k},\mathcal{H}) \\
&\quad + no(\log(P)) + h(Y_k^n|W_k,\mathcal{H}) && (78)\\
&= nR_k + no(n) + \sum_{j\in\mathcal{I}_k} h(\tilde{Y}_j^n|W_j,\mathcal{H}) \\
&\quad + no(\log(P)) + h(Y_k^n|W_k,\mathcal{H}) && (79)\\
&= nR_k + \sum_{j\in\mathcal{T}_k} h(\tilde{Y}_j^n|W_j,\mathcal{H}) + no(\log(P)) + no(n), && (80)
\end{aligned}$$

where (67) is due to the chain rule of mutual information, (69) follows from the independence of the message $W_k$ from the interfering message set $W_{\mathcal{I}_k}$, (70) is due to the decodability constraint in (3), (72) and (73) follow from the fact that conditioning reduces entropy, (74) is due to the Markov chain $W_{\mathcal{I}_k} \to X_{\mathcal{I}_k}^n \to \tilde{Y}_{\mathcal{I}_k}^n$, (76) and (78) follow from the fact that conditioning reduces entropy, (79) is due to the independence of $W_j$ from the message set $W_{\mathcal{I}_k\setminus\{j\}}$, and (80) follows because $\mathcal{T}_k = \{k\} \cup \mathcal{I}_k$. ■

## Appendix E
## Proof of Lemma 2

Let $\tilde{Y}_i^n = \mathbf{H}_{ki}^n X_i^n + Z_k^n$, for all $i \in \mathcal{T}_k = \{k\} \cup \mathcal{I}_k$, and consider any set $\mathcal{G}_k \subseteq \mathcal{I}_k$ and a permutation sequence $\Pi^{(k)} = (\Pi_1, \Pi_2, \ldots \Pi_{|\mathcal{G}_k|})$ of the elements of $\mathcal{G}_k$ satisfying Definition 9. We proceed with the proof of Lemma 2 as follows:

$$\begin{aligned}
&h\left(\sum_{i\in\mathcal{I}_k} \mathbf{H}_{ki}^n X_i^n + Z_k^n \Big| \mathcal{H}\right) \\
&\geq h\left(\sum_{i\in\mathcal{I}_k} \mathbf{H}_{ki}^n X_i^n + Z_k^n \Big| X_{\mathcal{I}_k\setminus\mathcal{G}_k}, \mathcal{H}\right) && (81)\\
&= h\left(\sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n \Big| \mathcal{H}\right) && (82)\\
&= I\left(W_{\Pi_1}; \sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n \Big| \mathcal{H}\right) \\
&\quad + h\left(\sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n \Big| W_{\Pi_1}, \mathcal{H}\right) && (83)\\
&= H(W_{\Pi_1}|\mathcal{H}) \\
&\quad - H\left(W_{\Pi_1} \Big| \sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n, \mathcal{H}\right) \\
&\quad + h\left(\sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n \Big| W_{\Pi_1}, \mathcal{H}\right) && (84)\\
&= nR^{\mathsf{sym}} - H\left(W_{\Pi_1} \Big| \sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n, \mathcal{H}\right) \\
&\quad + h\left(\sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n \Big| W_{\Pi_1}, \mathcal{H}\right) && (85)\\
&= nR^{\mathsf{sym}} + no(n) \\
&\quad + h\left(\sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n \Big| W_{\Pi_1}, \mathcal{H}\right) && (86)\\
&\geq nR^{\mathsf{sym}} + no(n) \\
&\quad + h\left(\sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n \Big| W_{\Pi_1}, X_{\Pi_1}, \mathcal{H}\right) && (87)\\
&= nR^{\mathsf{sym}} + no(n) \\
&\quad + h\left(\sum_{\Pi_i\in\mathcal{G}_k} \mathbf{H}_{k\Pi_i}^n X_{\Pi_i}^n + Z_k^n \Big| X_{\Pi_1}, \mathcal{H}\right) && (88)\\
&= nR^{\mathsf{sym}} + no(n)
\end{aligned}$$

$$+ h\left(\sum_{\Pi_i \in \mathcal{G}_k \setminus \Pi_1} \mathbf{H}^n_{k\Pi_i} X^n_{\Pi_i} + Z^n_k \Big| \mathcal{H}\right) \tag{89}$$

$$\geq n|\mathcal{G}_k| R^{\mathsf{sym}} + h(\tilde{Y}^n_{\Pi_{|\mathcal{G}_k|}} | W_{\Pi_{|\mathcal{G}_k|}}, \mathcal{H}) + no(n), \tag{90}$$

where $\Pi_{|\mathcal{G}_k|} \in \mathcal{G}_k \subseteq \mathcal{I}_k$ (81) follows from the fact that conditioning reduces entropy, (86) is due to Definition 9's fractional signal generator condition $\mathcal{G}_k \setminus \{\Pi_1, \Pi_2, \ldots, \Pi_i\} \subseteq \mathcal{I}_{\Pi_i}$, for $i = 1, 2, \ldots, |\mathcal{G}_k|$, and the decodability constraint in (3), (87) is due to the fact that conditioning reduces entropy, (88) is due to the Markov chain $W_{\Pi_1} \rightarrow X^n_{\Pi_1} \rightarrow Y^n_{\Pi_1}$, whereas (90) is obtained by repeatedly applying steps (82)-(89) for a total of $|\mathcal{G}_k|$ times. ■

## REFERENCES


[1] P. Aquilina and T. Ratnarajah, "On the degrees of freedom of interference broadcast channels with topological interference management," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1477–1489, Apr. 2016.

[2] F. Arbabjolfaei, B. Bandemer, Y.-H. Kim, E. Sasoglu, and L. Wang, "On the capacity region for index coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 962–966.

[3] F. Arbabjolfaei and Y.-H. Kim, "Fundamentals of index coding," *Found. Trends Commun. Inf. Theory*, vol. 14, nos. 3–4, pp. 163–346, 2018.

[4] M. A. Attia and R. Tandon, "On the secure degrees-of-freedom of partially connected networks with no CSIT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[5] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, "Index coding with side information," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.

[6] Y. Birk and T. Kol, "Informed-source coding-on-demand (ISCOD) over broadcast channels," in *Proc. Conf. Comput. Commun. 17th Annu. Joint Conf. IEEE Comput. Commun. Societies Gateway 21st Century (INFOCOM)*, Mar. 1998, pp. 1257–1264.

[7] S. Brahma and C. Fragouli, "Pliable index coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6192–6203, Nov. 2015.

[8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.

[9] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] J. de Dieu Mutangana and R. Tandon, "Interference channels with confidential messages: Leveraging OFDM transmission to scale up secure degrees of freedom with no CSIT," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 747–751.

[11] J. de Dieu Mutangana and R. Tandon, "Blind MIMO cooperative jamming: Secrecy via ISI heterogeneity without CSIT," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 447–461, 2020.

[12] J. de Dieu Mutangana and R. Tandon, "On secure topological interference management for half-rate-feasible networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[13] S. H. Dau, V. Skachek, and Y. M. Chee, "On the security of index coding with side information," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3975–3988, Jun. 2012.

[14] S. Doumiati, M. Assaad, and H. A. Artail, "A framework of topological interference management and clustering for D2D networks," *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7856–7871, Nov. 2019.

[15] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[16] X. Huang and S. El Rouayheb, "Index coding and network coding via rank minimization," in *Proc. IEEE Inf. Theory Workshop-Fall (ITW)*, Oct. 2015, pp. 14–18.

[17] S. A. Jafar, "Topological interference management through index coding," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 529–568, Jan. 2014.

[18] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[19] S. Lashgari and A. S. Avestimehr, "Secrecy DoF of blind MIMOME wiretap channel with delayed CSIT," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 478–489, Feb. 2018.

[20] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[21] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[22] S.-C. Lin and C.-L. Lin, "On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3293–3306, Jun. 2014.

[23] S.-C. Lin and P.-H. Lin, "On secrecy capacity of fast fading multiple-input wiretap channels with statistical CSIT," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 414–419, Feb. 2013.

[24] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[25] T. Liu and D. Tuninetti, "Private pliable index coding," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Aug. 2019, pp. 1–5.

[26] T. Liu and D. Tuninetti, "Secure decentralized pliable index coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 1729–1734.

[27] T. Liu and D. Tuninetti, "Tight information theoretic converse results for some pliable index coding problems," *IEEE Trans. Inf. Theory*, vol. 66, no. 5, pp. 2642–2657, May 2020.

[28] W. Liu, Y. Han, J. Li, and Y. Ma, "Topological interference management with transmitter cooperation for MIMO interference channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10564–10573, Nov. 2018.

[29] Y. Liu, P. Sadeghi, N. Aboutorab, and A. Sharififar, "Secure index coding with security constraints on receivers," 2020, *arXiv:2001.07296*.

[30] Y. Liu, B. N. Vellambi, Y.-H. Kim, and P. Sadeghi, "On the capacity region for secure index coding," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2018, pp. 1–5.

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

[32] H. Maleki, V. R. Cadambe, and S. A. Jafar, "Index coding—An interference alignment perspective," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5402–5432, Sep. 2014.

[33] M. M. Mojahedian, A. Gohari, and M. R. Aref, "Perfectly secure index coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 1432–1436.

[34] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[35] P. Mukherjee, R. Tandon, and S. Ulukus, "Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3823–3853, Jun. 2017.

[36] N. Naderializadeh and A. S. Avestimehr, "Interference networks with, no., CSIT: Impact of topology," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 917–938, Feb. 2015.

[37] M. Nafea and A. Yener, "Secure degrees of freedom of N× N× M wiretap channel with a K-antenna cooperative jammer," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 4169–4174.

[38] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wiretap channel with a multi-antenna cooperative jammer," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7420–7441, Nov. 2017.

[39] V. Narayanan, V. M. Prabhakaran, J. Ravi, V. K. Mishra, B. K. Dey, and N. Karamchandani, "Private index coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 596–600.

[40] V. Narayanan, J. Ravi, V. K. Mishra, B. Kumar Dey, N. Karamchandani, and V. M. Prabhakaran, "Private index coding," 2020, *arXiv:2006.00257*.

[41] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Oct. 2007.

[42] L. Ong, J. Kliewer, and B. N. Vellambi, "Secure network-index code equivalence: Extension to non-zero error and leakage," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 841–845.

[43] L. Ong, B. N. Vellambi, P. L. Yeoh, J. Kliewer, and J. Yuan, "Secure index coding: Existence and construction," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2834–2838.

[44] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, 2017.

[45] S. Sasi and B. S. Rajan, "Code construction for pliable index coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 527–531.

[46] 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 Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 201–205.

[47] Y. Shi, J. Zhang, and K. B. Letaief, "Low-rank matrix completion for topological interference management by Riemannian pursuit," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4703–4717, Jul. 2016.

[48] N. Shlezinger, D. Zahavi, Y. Murin, and R. Dabora, "The secrecy capacity of Gaussian MIMO channels with finite memory," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1874–1897, Mar. 2017.
[49] L. Song and C. Fragouli, "A polynomial-time algorithm for pliable index coding," *IEEE Trans. Inf. Theory*, vol. 64, no. 2, pp. 979–999, Feb. 2018.
[50] Y.-S. Su, "Optimal pliable fractional repetition codes that are locally recoverable: A bipartite graph approach," *IEEE Trans. Inf. Theory*, vol. 65, no. 2, pp. 985–999, Feb. 2019.
[51] R. Tandon, S. A. Jafar, S. Shamai (Shitz), and H. V. Poor, "On the synergistic benefits of alternating CSIT for the MISO broadcast channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4106–4128, Jul. 2013.
[52] R. Tandon, P. Piantanida, and S. Shamai (Shitz), "On multi-user MISO wiretap channels with delayed CSIT," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 211–215.
[53] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[54] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.
[55] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, May 1975.
[56] J. Xie and S. Ulukus, "Secure degrees of freedom of $K$-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.
[57] T. Y. Liu, P. Mukherjee, S. Ulukus, S. C. Lin, and Y. W. P. Hong, "Secure degrees of freedom of MIMO Rayleigh block fading wiretap channels with no CSI anywhere," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2655–2669, May 2015.
[58] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.
[59] X. Yi and G. Caire, "Topological interference management with decoded message passing," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3842–3864, May 2018.
[60] X. Yi and D. Gesbert, "Topological interference management with transmitter cooperation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6107–6130, Nov. 2015.
[61] X. Yi and H. Sun, "Opportunistic topological interference management," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 521–535, Jan. 2020.

**Jean de Dieu Mutangana** (Member, IEEE) received the B.S. degree in systems engineering (telecommunications) from the University of Arkansas at Little Rock in 2012, the M.S. degree in electrical and computer engineering (control, communications, and signal processing) from the University of California, Santa Barbara, in 2014, and the Ph.D. degree in the electrical and computer engineering (communications and signal processing) from The University of Arizona in 2021. Prior to joining The University of Arizona in Fall 2016, he was an Electrical Product Design and Development Engineer (RF connectivity and signal integrity) at Panduit Corporation, Chicago, from 2014 to 2016. He has spent Summer 2018 as a Systems Engineer Intern (mobile communications) at Intel Corporation, Santa Clara. He is currently a Wireless Systems Engineer at Ford Motor Company. His research interests include wireless communications, network information and coding theory, and signal processing.

**Ravi Tandon** (Senior Member, IEEE) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur (IIT Kanpur), in 2004, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park (UMCP), in 2010. He is currently the Litton Industries John M. Leonis Distinguished Associate Professor with the Department of ECE, The University of Arizona. Prior to joining The University of Arizona in Fall 2015, he was a Research Assistant Professor at Virginia Tech with positions at the Bradley Department of ECE, Hume Center for National Security and Technology; and the Discovery Analytics Center, Department of Computer Science. From 2010 to 2012, he was a Post-Doctoral Research Associate at Princeton University. His current research interests include information theory and its applications to wireless networks, signal processing, communications, security and privacy, machine learning, and data mining. He was a recipient of the 2018 Keysight Early Career Professor Award, the NSF CAREER Award in 2017, and the Best Paper Award at IEEE GLOBECOM 2011. He serves as an Editor for IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and IEEE TRANSACTIONS ON COMMUNICATIONS.