Sum Secure Degrees of Freedom of Two-Unicast Layered Wireless Networks

Jianwei Xie and Sennur Ulukus, *Member, IEEE*

***Abstract*—In this paper, we study the sum secure degrees of freedom (d.o.f.) of two-unicast layered wireless networks. Without any secrecy constraints, the sum d.o.f. of this class of networks was studied by [1] and shown to take only one of three possible values: $1, \frac{3}{2}$ and 2, for all network configurations. We consider the setting where, in addition to being reliably transmitted, each message is required to be kept information-theoretically secure from the unintended receiver. We show that the sum *secure* d.o.f. can only take one of five possible values: $0, \frac{2}{3}, 1, \frac{3}{2}, 2$, for all network configurations. To determine the sum secure d.o.f., we divide the class of two-unicast layered networks into several sub-classes, and propose an achievable scheme based on the specific structure of the networks in each sub-class. Our achievable schemes are based on real interference alignment, cooperative jamming, interference neutralization and cooperative jamming neutralization techniques.**

***Index Terms*—Information-theoretic security, layered wireless networks, interference alignment, cooperative jamming.**

I. Introduction

WE CONSIDER a two-unicast layered network (see Figure 1) where two transmitters wish to have reliable and secure communication with their respective receivers simultaneously, by utilizing a layered network in between. The two-layer (i.e., single-hop) version of this network is an interference channel, whose capacity is unknown in general; it is known only in certain special cases, e.g., a class of deterministic interference channels [2], a class of strong interference channels [3]–[5], a class of degraded interference channels [6]. The degrees of freedom (d.o.f.) characterizations have been found for the interference channel in several different settings, e.g., [7]–[10]. In particular, the sum d.o.f. of a fully connected two-user interference channel is 1 [11]. Recently, reference [1] showed that, if the source-destination pairs are *connected*, then with probability one, the sum d.o.f. of two-unicast layered Gaussian networks can take only one of three possible values: 1, $\frac{3}{2}$ and 2.

We extend this line of work to include security in addition to reliability for the end-to-end users. The security we use is in the information-theoretic sense, which is measured by the conditional equivocation of the messages at the unintended receivers. Wyner introduced the wiretap channel [12], in which the transmitter wishes to send a message to the receiver secret from the eavesdropper. The capacity-equivocation region was originally found for the degraded wiretap channel by Wyner [12], and then was generalized to the general wiretap channel by Csiszar and Korner [13], and extended to the Gaussian wiretap channel by Leung-Yan-Cheong and Hellman [14]. For two-layer (i.e., single-hop) wireless networks, different multi-user settings have been studied recently, e.g., broadcast channels with confidential messages [15], [16], multi-receiver wiretap channels [17]–[19] (see also a survey on extensions of these to MIMO channels [20]), two-user interference channels with confidential messages [15], [21], two-user interference channels with one external eavesdropper [22], multiple access wiretap channels [23]–[27], relay eavesdropper channels [28]–[33], compound wiretap channels [34], [35]. Since in most multi-user scenarios it is difficult to obtain the exact secrecy capacity region, achievable secure d.o.f. at high signal-to-noise ratio (SNR) cases has been studied for several channel structures, such as the K-user Gaussian interference channel with confidential messages [36], [37] ($K = 2$ was studied in [38]), the K-user interference channel with external eavesdroppers [37], [39], the Gaussian wiretap channel with helpers [38], [40]–[42], the Gaussian multiple access wiretap channel [38], [43], [44], and the wireless X network [45].

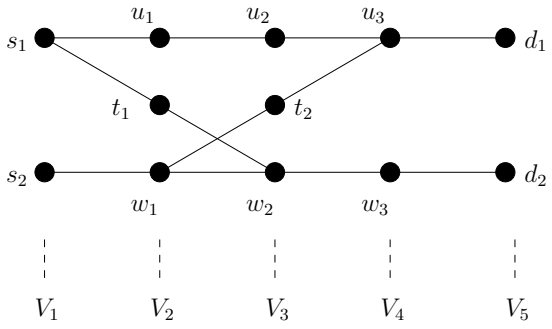


Fig. 1. An example two-unicast layered network.

To determine the sum d.o.f. of two-unicast layered networks, reference [1] divided all network structures into five cases: A, A', B, B' and C, and found the sum d.o.f. in each case. In particular, the sum d.o.f. of all networks in cases A and A' is 1, in cases B and B' is 2, and in case C is $\frac{3}{2}$. The main challenge of determining the sum *secure* d.o.f. is in cases A and A'. In the first part of this work, we show that although for these two cases the sum d.o.f. is exactly 1, the sum *secure* d.o.f. can take one of three possible values: $0, \frac{2}{3}$ and 1. To determine the secure d.o.f. in all possible cases, we further divide the layered networks in case A and A' into

Manuscript received September 15, 2012; revised March 10, 2013. This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811, and presented in part at the IEEE International Symposium on Information Theory, Boston, MA, July 2012.

J. Xie and S. Ulukus are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA (e-mail: xiejw@umd.edu, ulukus@umd.edu).

Digital Object Identifier 10.1109/JSAC.2013.130924.

five sub-cases, e.g., A_1 through A_5. In the first four sub-cases, we explicitly utilize the properties of the layered network in each sub-case, and either find a node and employ it to protect the communication by having it perform cooperative jamming [23], [24] against the unintended receiver, or use the interference neutralization technique [46] to neutralize the message signal at the unintended destination and even neutralize the cooperative jamming signal at the intended receiver to mimic the wiretap channel with cooperative jamming. Achievable schemes we develop based on these two techniques match the corresponding upper bounds, giving the exact sum secure d.o.f. for the layered networks in these four sub-cases.

In the last sub-case of the cases A and A', i.e., in A_5, we note that there is an independence structure in the last layer of the network before the destination nodes. Specifically, the nodes in this last layer have mutually independent observations, and therefore as transmitters in the last hop of the network, they can only send independent signals. Due to this independence structure, we cannot simply utilize cooperative jamming and/or interference neutralization to achieve the optimal sum secure d.o.f., which makes this sub-case most challenging. To overcome this difficulty, we first reduce this problem into two simplest equivalent channel models, which are $(\mathbf{P1})$ the two-user Gaussian interference channel with confidential messages and $M \geq 0$ helper(s) and $(\mathbf{P2})$ the Gaussian broadcast channel with confidential messages and $M \geq 1$ helper(s). Finding the sum secure d.o.f. of these two channel models has been hard and open for a long time. For example, for the two-user Gaussian interference channel with confidential messages, which is the special case $M = 0$ of $(\mathbf{P1})$, the best known upper bound was 1 which was due to the channel model without secrecy constraints. On the other hand, if we consider symmetric rates, the best known inner bound for the sum secure d.o.f. was $\frac{1}{3}$ [45]; if we consider one individual rate as a lower bound for the sum rate, the individual secure d.o.f. of $\frac{1}{2}$ was achieved in [47] and [42, Theorem 5.4] in the context of the wiretap channel with a helper (for the class of algebraic irrational channel gains). Recently, we have shown that $\frac{2}{3}$ is the exact sum secure d.o.f. for the two-user Gaussian interference channel with confidential messages, i.e., for the case $M = 0$ in $(\mathbf{P1})$, and 1 is the exact sum secure d.o.f. for the cases $M \geq 1$ in $(\mathbf{P1})$ and $(\mathbf{P2})$ [38]. Utilizing these recent results in the context of this two-unicast layered network, we are able to provide a complete sum secure d.o.f. characterization for all two-unicast layered networks in cases A and A'.

For the cases B and B', reference [1] showed that the trivial upper bound of 2 for the sum d.o.f. can be achieved by either obtaining a diagonal end-to-end transfer matrix with non-zero diagonal entries, or by constructing a $2 \times 2 \times 2$ condensed interference network in which the d.o.f.-optimal achievable scheme is based on real interference alignment [48]. For the first scenario, we have secrecy for free, due to the diagonal nature of the end-to-end transfer matrix. For the second scenario, we propose a modified achievable scheme for the $2\times2\times2$ interference network to achieve the upper bound of 2 for the sum secure d.o.f. The challenge in the equivocation calculation in this case is that we need to provide a precise performance analysis in terms of both reliability and secrecy. In this case, the nodes in the middle layer of the $2 \times 2 \times 2$ interference network perform hard decisions to decode the original channel inputs from the previous layer. If these hard decisions have no error, then due to the special construction of the channel inputs based on interference neutralization and interference alignment, the messages are secure. However, if errors occur during decoding in the middle layer, then the mixed signals containing both messages observed by both destination nodes may leak information. To show the optimality of the proposed achievable scheme, we observe that the message rate scales with $\log P$, but the probability of hard decision error decreases exponentially fast with P, which makes the information leakage rate negligible in the high SNR regime.

Finally, reference [1] showed that all layered networks in case C can be operated in a time-sharing mode between two networks which belong to cases B and B', i.e., after selecting a temporary node d' in the network, in both modes, we can find a sub-network which has the structure of case B or case B' to transmit 2 sum d.o.f. reliably, in which, node d' is one of the destinations for the first mode, which stores the information and serves as the source node in the second mode. Therefore, on average, we can achieve $\frac{3}{2}$ sum d.o.f. To achieve $\frac{3}{2}$ sum secure d.o.f. for case C, we study all possibilities for the layered network in this case, and find a node to cooperatively jam the unintended receiver to protect the messages.

II. Definitions and Notations

Let V be the node set and $E \subset V \times V$ be the edge set. A two-unicast layered network $N = (G, L_2)$ is a directed graph $G = (V, E)$ with two source-destination pairs $L_2 = \{(s_1, d_1), (s_2, d_2)\} \subset V \times V$. The network has a layered structure which means that the node set V can be partitioned into r mutually disjoint subsets $V_1, V_2, \cdots, V_r$, denoting the nodes in each layer, such that $V_1 = \{s_1, s_2\}, V_r = \{d_1, d_2\}$ and

$$E \subset \bigcup_{i=1}^{r-1} V_i \times V_{i+1} \tag{1}$$

Since each node only belongs to one layer and each layer has an index, we define the index function $l(v)$ as the index of the layer containing the node v, i.e., $v \in V_{l(v)}$. Next, we give several definitions on graphs.

Definition 1 (Path) A path P_{v_1,v_k} is an ordered set of nodes $\{v_1, v_2, \cdots, v_k\}$ provided that $(v_i, v_{i+1}) \in E$ for $i = 1, 2, \cdots, k-1$. Further, we denote $u \rightsquigarrow v$ if there exists at least one path $P_{u,v}$ from u to v.

Two paths are disjoint provided that the two sets of nodes are disjoint. To avoid the trivial cases, we always assume that $s_1 \rightsquigarrow d_1$ and $s_2 \rightsquigarrow d_2$. In contrast to the assumption in [1], we cannot remove nodes v which do not belong to any path, since we may employ them to perform cooperative jamming.

Definition 2 For a subset of nodes $S \subset V$, we denote by $G[S]$ the graph induced by S on G provided that $G[S] = (S, E_s)$ where $E_s = \{(v, u) \in E : v, u \in S\}$.

Reference [1] defines interference and manageable interference as follows:

Definition 3 (Interference) For $i = 1$ or 2, a node $v \notin P_{s_i,d_i}$ causes interference on P_{s_i,d_i} and we write $v \overset{I}{\rightsquigarrow} P_{s_i,d_i}$ if there exist a node $u \in P_{s_i,d_i}$ such that $(v,u) \in E$ and a path $P_{s_j,v}$ such that P_{s_i,d_i} and $P_{s_j,v}$ are disjoint.

In Definition 3 and in the sequel, we use the notation $j = \bar{i}$ to denote the index of the other transmitter-receiver pair, i.e., $i = 1, j = 2$ or $i = 2, j = 1$. In order to characterize the interference from another pair, the number of nodes causing interference is defined as follows:

$$n_i(G[S], P_{s_i,d_i}) \triangleq n_i(G[S]) \triangleq \Big|\{v \in S : v \overset{I}{\rightsquigarrow} P_{s_i,d_i}, \exists P_{s_j,v} \subset S \text{ and } P_{s_i,d_i} \cap P_{s_j,v} = \phi\}\Big| \tag{2}$$

for some subset $S \subset V$ and $(P_{s_1,d_1} \cup P_{s_2,d_2}) \subset S$.

Definition 4 (Manageable interference) Two disjoint paths P_{s_1,d_1} and P_{s_2,d_2} have **manageable interference** if we can find $S \subset V$, such that $(P_{s_1,d_1} \cup P_{s_2,d_2}) \subset S$, $n_1(G[S]) \neq 1$ and $n_2(G[S]) \neq 1$.

An example two-unicast layered network is shown in Figure 1. This network has $r = 5$ layers and two disjoint paths $P_{s_1,d_1} = \{s_1, u_1, u_2, u_3, d_1\}$ and $P_{s_2,d_2} = \{s_2, w_1, w_2, w_3, d_2\}$. Node t_1 causes interference on P_{s_2,d_2}, since we can find $w_2 \in P_{s_2,d_2}$ such that $(t_1, w_2) \in E$ and a path $P_{s_1,t_1} = \{s_1, t_1\}$ such that P_{s_1,t_1} and P_{s_2,d_2} are disjoint. This implies that $n_2(G[V]) = 1$. It is also easy to see that $n_1(G[V]) = 1$ due to node t_2. However, if we choose $S = V \backslash \{t_1, t_2\}$, then, for the graph $G[S]$ induced by S, $n_1(G[S]) = n_2(G[S]) = 0$. By definition, P_{s_1,d_1} and P_{s_2,d_2} have manageable interference.

Regarding the channel model, each node v observes the signals through a memoryless additive Gaussian channel, i.e.,

$$Y_v = \sum_{u:(u,v)\in E} h_{v,u} X_u + N_v \tag{3}$$

where N_v is an additive zero-mean unit-variance Gaussian noise and X_u is the input signal sent from node u provided that the edge (u,v) exists. All the channel gains $h_{v,u}$ in the network are fixed during the communication session and known at all nodes. Channel gains are independently drawn from continuous distributions. The input signal of each node u, X_u, satisfies an average power constraint P, i.e., $\mathrm{E}[X_u^2] \leq P$.

The source node s_1 has a message W_1 uniformly chosen from set $\mathcal{W}_1$ for destination d_1. The rate of the message is $R_1 \triangleq \frac{1}{n}\log|\mathcal{W}_1|$. The source node s_1 uses a stochastic function $f_1 : \mathcal{W}_1 \to X_{s_1}^n$ to encode the message, where n is the number of channel uses. Similarly, source node s_2 has message W_2 (independent of W_1) uniformly chosen from set $\mathcal{W}_2$ for destination d_2. The rate of the message is $R_2 \triangleq \frac{1}{n}\log|\mathcal{W}_2|$. Source node s_2 uses a stochastic function $f_2 : \mathcal{W}_2 \to X_{s_2}^n$ to encode the message. The messages are said to be transmitted reliably and securely if only the intended destination node can decode each message, i.e., each destination node is an eavesdropper for the other. Formally, for $i = 1$ or 2, a secrecy rate R_i is said to be achievable if for any $\epsilon > 0$ there exists an n-length code such that destination node d_i can decode the message as $\hat{W}_i$ reliably based on its observation $Y_{d_i}^n$, i.e., the probability of decoding error is less than ϵ,

$$\Pr\left[W_i \neq \hat{W}_i\right] \leq \epsilon \tag{4}$$

and the message is kept information-theoretically secure against the other receiver,

$$\frac{1}{n}H(W_i|Y_{d_j}^n) \geq \frac{1}{n}H(W_i) - \epsilon \tag{5}$$

This definition implicitly implies that the source nodes trust all the intermediate relay nodes, but the unintended destination node. The sum secure d.o.f. is defined as:

$$D_{s,\Sigma} = \lim_{P\to\infty} \sup \frac{R_1 + R_2}{\frac{1}{2}\log P} \tag{6}$$

where the supremum is over all achievable secrecy rate pairs (R_1, R_2). The sum d.o.f. of two-unicast layered networks was found in [1] as:

Theorem 1 (Sum d.o.f. of two-unicast networks [1]) For a two-unicast layered Gaussian network $N = (G = (V,E), L_2 = \{(s_1,d_1),(s_2,d_2)\})$ where the channel gains are chosen according to independent continuous distributions, with probability 1, D_Σ is given by
A) 1, if N contains a node v whose removal disconnects d_i from $\{s_i, s_j\}$ and s_j from $\{d_i, d_j\}$, for $i = 1$ or 2, $j = \bar{i}$,
A') 1, if N contains an edge (v_2, v_1) such that the removal of v_1 disconnects d_i from $\{s_i, s_j\}$ and the removal of v_2 disconnects s_j from $\{d_i, d_j\}$, for $i = 1$ or 2, $j = \bar{i}$,
B) 2, if N contains two disjoint paths P_{s_1,d_1} and P_{s_2,d_2} with manageable interference,
B') 2, if N or any sub-network does not contain two disjoint paths P_{s_1,d_1} and P_{s_2,d_2}, but is not in case (A),
C) $3/2$, in all other cases.

By considering secrecy for the end-to-end users in addition to reliability, the main result of our paper is the characterization of the sum *secure* d.o.f. of two-unicast layered networks as stated in the following theorem.

Theorem 2 (Sum secure d.o.f. of two-unicast networks) For a two-unicast layered Gaussian network $N = (G = (V,E), L_2 = \{(s_1,d_1),(s_2,d_2)\})$ where the channel gains are chosen according to independent continuous distributions, with probability 1, $D_{s,\Sigma}$ can take one of the following five possible values: $0, \frac{2}{3}, 1, \frac{3}{2}, 2$.

We will prove Theorem 2 in the following three sections. In particular, in Section III, we will show that for two-unicast layered networks in cases A and A', the sum secure d.o.f. can take one of three values: $0, \frac{2}{3}, 1$. Next, in Section IV, we will show that for two-unicast layered networks in cases B and B', the sum secure d.o.f. is 2. Finally, in Section V, we will show that for two-unicast layered networks in case C, the sum secure d.o.f. is $\frac{3}{2}$.

In order to prove Theorem 2, we characterize the penultimate layer V_{r-1}, i.e., the last layer of the network before the

layer of destinations, as:

$$V_{r-1} = G_1 \cup G_2 \cup G_3 \cup G_4 \tag{7}$$

where G_is are mutually disjoint sets defined as follows:

$$G_1 = \{u \in V_{r-1} : (u, d_1) \in E \text{ and } (u, d_2) \in E\} \tag{8}$$
$$G_2 = \{u \in V_{r-1} : (u, d_1) \in E \text{ and } (u, d_2) \notin E\} \tag{9}$$
$$G_3 = \{u \in V_{r-1} : (u, d_1) \notin E \text{ and } (u, d_2) \in E\} \tag{10}$$
$$G_4 = \{u \in V_{r-1} : (u, d_1) \notin E \text{ and } (u, d_2) \notin E\} \tag{11}$$

That is, we group the nodes in the penultimate layer V_{r-1} into four disjoint sets: G_1 through G_4. These are the sets of nodes that may or may not be connected to the destinations: G_1 is the set of all nodes in this layer which are connected to both destinations, G_2 is the set of all nodes that are connected to the first destination (d_1) but not to the second destination (d_2), G_3 is the set of all nodes which are connected to the second destination (d_2) but not to the first destination (d_1), and G_4 is the set of nodes that are not connected to d_1 or d_2. Since the last layer V_r only contains d_1, d_2, it is safe to remove the nodes belonging to G_4 from the network. For the rest of this paper, we assume that the cardinality of set G_4 is zero, i.e., $|G_4| = 0$.

III. Sum Secure d.o.f. for Cases A and A'

In this section, we consider two-unicast layered networks in cases A and A', i.e., each network N contains an edge (v_2, v_1) such that removal of v_1 disconnects d_i from $\{s_i, s_j\}$ and removal of v_2 disconnects s_j from $\{d_i, d_j\}$, for $i = 1$ or 2, $j = \bar{i}$. If $v_1 = v_2$, then the "*edge*" downgrades to a node, and this is case A; otherwise, this is case A'.

The sum d.o.f. capacity is $D_\Sigma = 1$ for this case, which is an upper bound for the sum secure d.o.f., $D_{s,\Sigma}$. We present our results by dividing all the networks in cases A and A' into 5 sub-cases, A_1 through A_5. We implicitly mean that, for each i, the sub-case A_i does not include the setting in A_j for any $j < i$, i.e., the sub-case A_2 does not include the setting in A_1, the sub-case A_3 does not include the settings in A_1 or A_2, etc. We start with a sub-case (sub-case A_1) where there exists at least one node in G_2 or G_3, i.e., $|G_2| \geq 1$ or $|G_3| \geq 1$. In this case, cooperative jamming is sufficient to achieve 1 secure d.o.f. if there exists a helper in the set $G_2 \cup G_3$. If the union of G_2 and G_3 is empty, then all the nodes in layer V_{r-1} are connected to both destinations, i.e., $V_{r-1} = G_1$. Since the signals from any node in G_1 are received by both destination nodes, we investigate the structure of the network and the set G_1 to find the exact sum secure d.o.f. based on interference neutralization and real interference alignment in sub-cases A_2 through A_5. Our result for cases A and A' is stated in the following theorem.

Theorem 3 With probability 1, the sum secure d.o.f. of layered networks in cases A and A' is

$$D_{s,\Sigma} = \begin{cases} 0 & \text{if } |G_1| = 1 \text{ and } |G_2 \cup G_3| = 0 \\ \frac{2}{3} & (*) \\ 1 & o.w. \end{cases} \tag{12}$$

where the condition $(*)$ is either of the following two conditions:

1) $(\mathbf{C1})$ $r = 2$ and $|G_2 \cup G_3| = 0$,
2) $(\mathbf{C2})$ $r \geq 3, |G_1| = 2$, $|G_2 \cup G_3| = 0$, for each w there exists at most one $u_w \in G_1$ such that $w \rightsquigarrow u_w$, and the layered network is not in case A.

We can interpret Theorem 3 in the following way. The first condition $|G_1| = 1$ and $|G_2 \cup G_3| = 0$ means that $V_{r-1} = G_1 = \{u\}$ has only one node u which is connected to both d_1 and d_2. Both destinations receive almost the same signals at high SNR, which implies that $D_{s,\Sigma} = 0$. This case is considered in detail in Section III-B. Next, condition $(\mathbf{C1})$, i.e., $r = 2$ and $|G_2 \cup G_3| = 0$, implies that $|G_1| = 2$ due to the assumption $V_1 = \{s_1, s_2\}$. Therefore, this layered network is a fully-connected two-user Gaussian interference channel with confidential messages, for which the sum secure d.o.f. is $\frac{2}{3}$ [38]. Such networks belong to case A'. Since this result follows from [38], we will not consider it further in the following sub-sections. Next, condition $(\mathbf{C2})$ is a variant of condition $(\mathbf{C1})$, thereby the corresponding $D_{s,\Sigma}$ is also $\frac{2}{3}$. We will show this in Section III-E. For all other network configurations, $D_{s,\Sigma}$ is 1. We will give the corresponding achievable schemes in Sections III-A, III-C, III-D, and III-E.

A. Sub-case A_1: $D_{s,\Sigma} = 1$ if $|G_2| \geq 1$ or $|G_3| \geq 1$.

Without loss of generality, we prove $D_{s,\Sigma} = 1$ for the setting $|G_3| \geq 1$. The same argument can be applied to $|G_2| \geq 1$. The cardinality of set G_3 is nonzero which means that there exists at least one node $u \in G_3$. There are two possibilities. The first possibility is that we can find some node $u \in G_3$ and u belongs to the path P_{s_2,d_2}. Since by definition the edge (u, d_1) does not exist, if the message signal of the transmitter-receiver pair 2 is going through the path P_{s_2,d_2}, by keeping other nodes in the network silent, there is no information leakage to d_1, i.e., this message (message W_2) is secure and $D_{s,\Sigma} = 1$.

If we cannot find such node u (which is the second possibility), then we can utilize node u to perform cooperative jamming. Transmitter 1 transmits a message carrying 1 d.o.f. along the existing path P_{s_1,d_1}. All nodes on this path, except the node $\tilde{s} \in V_{r-1}$, simply relay the signal. Node u, which is connected to d_2 only, sends i.i.d. Gaussian cooperative jamming signal [23], [24] with average power P, which is independent of message W_1, to ensure the secrecy of the message from transmitter-receiver pair 1. The final hop becomes a Gaussian wiretap channel with an independent helper which is only connected to the eavesdropper. Due to the fact that the signal from node u is an artificial i.i.d. Gaussian noise, the source-destination pair $(\tilde{s}, d_1)$ can achieve the (maximum) secrecy rate, which is known [14]

$$\frac{1}{2}\log\left(1 + h^2_{d_1,\tilde{s}}P\right) - \frac{1}{2}\log\left(1 + \frac{h^2_{d_2,\tilde{s}}P}{1 + h^2_{d_2,u}P}\right) \tag{13}$$

and from (6) the secure d.o.f. is $D_{s,\Sigma} = 1$.

B. Sub-case A_2: $D_{s,\Sigma} = 0$ if $|G_1| = 1$.

In this section, we consider the sub-case A_2 and prove that $D_{s,\Sigma} = 0$. After ruling out the setting in sub-case A_1, the setting of layered networks in A_2 is $|G_1| = 1$

and $|G_2| = |G_3| = 0$. First, note that $|G_2| = |G_3| = 0$ implies $|G_1| \geq 1$ due to the existence of P_{s_i,d_i} for some i. Furthermore, if $|G_1| = 1$ and $|G_2| = |G_3| = 0$, this indicates that $V_{r-1} = G_1 = \{u\}$ has only one node u which is connected to both d_1 and d_2. The last hop of the layered network in this sub-case is a Gaussian broadcast channel with confidential messages, in which the transmitter is node u, and d_1, d_2 are the two receivers. The sum secure d.o.f. is 0: due to the degradedness of the underlying Gaussian broadcast channel, one of the users (stronger) has the secrecy capacity which is the secrecy capacity of the Gaussian wiretap channel, and the other user (weaker) has zero secrecy capacity. It is well-known that the secrecy capacity of the Gaussian wiretap channel does not scale with $\log P$, therefore, for both users, the secure d.o.f. is zero, implying that the sum secure d.o.f. is zero. This concludes that $D_{s,\Sigma} = 0$ if $|G_1| = 1$ and $|G_2| = |G_3| = 0$.

C. Sub-case A_3: $D_{s,\Sigma} = 1$ if there exist two distinct nodes $u_1, u_2 \in G_1$ and a source node s such that $s \rightsquigarrow u_1$ and $s \rightsquigarrow u_2$.

In this section, we consider the sub-case A_3 in which layer V_{r-1} contains several nodes, which are connected to both destinations. In addition, by excluding the settings in A_1 and A_2, we note that the layered networks in A_3 must have $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$. Since the condition (**C1**), i.e., $r = 2$ and $|G_2 \cup G_3| = 0$, has already been discussed and excluded in the present discussion, we know that the networks with $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$ must have at least three layeres, i.e., $r \geq 3$.

We propose an achievable scheme for this sub-case based on interference neutralization [46]. The source node s, say s_i, which connects to u_1 and u_2, sends the message signal carrying 1 d.o.f. to its destination. All the nodes on the two paths P_{s_i,u_1} and P_{s_i,u_2} just relay the signal. The two nodes u_1 and u_2 perform amplify-and-forward with factors α_1 and α_2, respectively. The values of α_1 and α_2 will be specified later. All other nodes, including s_j, do not send/relay signals.

To show the achievable sum secure d.o.f. for this scheme, we construct the condensed network [1] with three key layers as shown in Figure 2. Then, the end-to-end transfer matrix $\mathbf{T} = [T_i, T_j]^T$ from s_i to d_i, d_j satisfies

$$\begin{aligned}\begin{pmatrix} Y_{d_i} \\ Y_{d_j} \end{pmatrix} &= \mathbf{T} X_{s_i} + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_i \tilde{h}_i h_{i,i} + \alpha_j \tilde{h}_j h_{i,j} \\ \alpha_i \tilde{h}_i h_{j,i} + \alpha_j \tilde{h}_j h_{j,j} \end{pmatrix} X_{s_i} + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix}\end{aligned} \tag{14}$$

where $\tilde{N}_1$ and $\tilde{N}_2$ are effective dependent noises with finite variances. However, they are independent of the message signal due to the linear construction.

If we choose $\alpha_i = 1$ and $\alpha_j = -(\tilde{h}_i h_{j,i})/(\tilde{h}_j h_{j,j})$, then the signal X_{s_i} from the source node s_i is perfectly canceled at the destination node d_j due to the fact $T_j = 0$, which also makes the observation $Y_{d_j}^n$ at d_j and W_i independent, i.e., $I(W_i; Y_{d_j}^n) = 0$. This indicates that message W_i is secure. On the other hand, for reliability, the probability that d_i can decode W_i with arbitrarily small probability of decoding error is

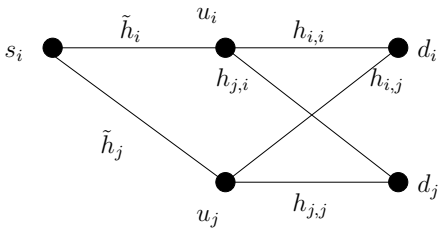


Fig. 2. The condensed network for $s_i \rightsquigarrow u_1$ and $s_i \rightsquigarrow u_2$.

$$\begin{aligned}P(T_i \neq 0) &= P\left(\tilde{h}_i h_{i,i} - \tilde{h}_j h_{i,j} \frac{\tilde{h}_i h_{j,i}}{\tilde{h}_j h_{j,j}} \neq 0\right) \\ &= P(h_{j,j} h_{i,i} - h_{i,j} h_{j,i} \neq 0) = 1\end{aligned} \tag{15}$$

which means that $D_{s,\Sigma} = 1$ with probability one.

D. Sub-case A_4: $D_{s,\Sigma} = 1$ if there exist two distinct nodes $u_1, u_2 \in G_1$ and a node w such that $w \rightsquigarrow u_1$ and $w \rightsquigarrow u_2$.

In this section, we show that, if there is a node which is connected to at least two nodes in G_1, even though it is not a source node, we still can achieve 1 sum secure d.o.f. After excluding all previous sub-cases, in addition to the definition of A_4, the layered networks in this sub-case must have the following properties: $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$, $r \geq 3$, and, for each source node s_i $(i = 1, 2)$, there exists one and only one $\tilde{u}_i \in G_1$ such that $s_i \rightsquigarrow \tilde{u}_i$.

For sub-case A_4, we propose the following achievable scheme. For any source node, say s_i, and a path $P_{s_i,u}$, where $u \in G_1$, the source node s_i sends the message signal carrying 1 d.o.f. to node u. All the nodes on path $P_{s_i,u}$ just relay the signal. Node u encodes the message according to a secrecy capacity achieving code, which will be specified later, and sends the codeword to d_i. The special node w sends artificial i.i.d. Gaussian random noise with average power aP to jam the unintended destination d_j through the two nodes u_1 and u_2. The linear factor a is a constant to coordinate with the nodes in the network such that all the channel inputs satisfy the power constraint. The value of a depends on the network topology, but not on power P. All the nodes on two paths P_{w,u_1}, P_{w,u_2} relay the signals. Nodes u_1 and u_2 perform amplify-and-forward with factors α_1 and α_2, respectively. All other nodes, including s_j, do not send/relay signals.

The intuition behind this achievable scheme is similar to the previous sub-case. However, we carefully choose the factors α_1 and α_2 to neutralize the artificial noise at the legitimate destination d_i, and thereby utilize node w to perform cooperative jamming. After removing all unnecessary nodes, there are only two possibilities for sub-case A_4 as shown in Figure 3. If $u_i = \tilde{u}_i$ as shown in Figure 3(a), then this node u_i has to relay the message carrying signal and also the jamming signal. After scaling all signals in the network with a constant factor to satisfy the average power constraint, u_i sends a superposition of the two signals. Under this setting, we disregard the difference between the two possibilities and thereby focus on the cooperative jamming signal. In both

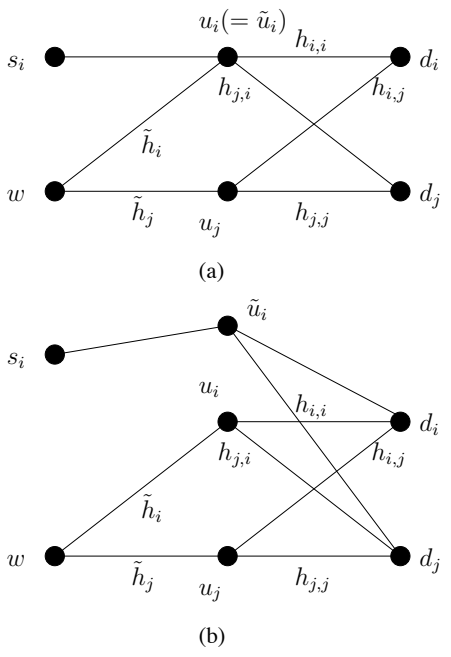


Fig. 3. The two possible condensed networks for the sub-case A_4: $w \rightsquigarrow u_1$ and $w \rightsquigarrow u_2$.

condensed networks in Figure 3, if we consider the source node s_i as the transmitter, d_i as the legitimate receiver, and d_j as the eavesdropper, the networks are equivalent to Gaussian wiretap channels with dependent noises. Due to the fact that the secrecy capacity depends only on the marginal distributions (but not on the joint), to show that 1 sum secure d.o.f. is achievable, it suffices to prove that with proper design of α_i and α_j, the jamming noise with average power aP from node w can be perfectly canceled at the legitimate receiver d_i, but not at the eavesdropper d_j.

Consider the end-to-end transfer matrix $\mathbf{T} = [T_i, T_j]^T$ from w to d_i, d_j:

$$\begin{aligned}\begin{pmatrix} Y_{d_i}^w \\ Y_{d_j}^w \end{pmatrix} &= \mathbf{T}N_w + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_i \tilde{h}_i h_{i,i} + \alpha_j \tilde{h}_j h_{i,j} \\ \alpha_i \tilde{h}_i h_{j,i} + \alpha_j \tilde{h}_j h_{j,j} \end{pmatrix} N_w + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix}\end{aligned} \tag{16}$$

If we choose $\alpha_i = 1$ and $\alpha_j = -(\tilde{h}_i h_{i,i})/(\tilde{h}_j h_{i,j})$, then $T_i = 0$ and receiver d_i will have a clean view of the signal from s_i. Meanwhile, the probability that T_j is non-zero is

$$P\left(T_j \neq 0\right) = P\left(h_{j,j}h_{i,i} - h_{i,j}h_{j,i} \neq 0\right) = 1 \tag{17}$$

which concludes that $D_{s,\Sigma} = 1$ with probability one for sub-case A_4.

E. Sub-case A_5: All other settings in cases A and A'.

In this section, we consider the layered networks in cases A and A', which are not in any of the previous sub-cases. In this sub-case, by excluding the settings of all previous sub-cases, we know that $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$, the number of layers $r \geq 3$, and there is an independence structure in layer V_{r-1}. By an independence structure, we mean that all the channel inputs from nodes belonging to $G_1 = V_{r-1}$ in the last hop must be mutually independent. This is because, for each node w in the network before V_{r-1}, there exists at most one $u_w \in G_1$ such that $w \rightsquigarrow u_w$.

Since we can precisely characterize the structure of the layered network in this sub-case, we claim that $D_{s,\Sigma} = \frac{2}{3}$ if condition (**C2**) is satisfied and is 1 otherwise. The proof is developed in three steps. The first step is to explore the structure of the network. The second step is to reduce the network to an equivalent Gaussian broadcast channel with confidential messages and $M \geq 1$ helper(s) or a two-user Gaussian interference channel with confidential messages and $M \geq 0$ helper(s). The final step is to use recent sum secrecy capacity result in terms of d.o.f. in [38].

First, we show that $D_{s,\Sigma} = 1$ if the network belongs to case A. Let $s_i \rightsquigarrow u_i$ and $s_j \rightsquigarrow u_j$ for some $u_i, u_j \in V_{r-1}$. We prove $u_i = u_j$ by contradiction. Assuming $u_i \neq u_j$. Since, by the definition of case A, removal of v disconnects d_i from s_1, s_2, we must have $s_i \rightsquigarrow v$. Again, since the removal of v disconnects s_j from d_1, d_2, it must be that $s_j \rightsquigarrow v \rightsquigarrow u_j$, which implies $s_i \rightsquigarrow v \rightsquigarrow u_j$, i.e., $s_i \rightsquigarrow u_j$ and $s_i \rightsquigarrow u_i$, which is sub-case A_3. This leads to a contradiction. Denote $u \triangleq u_i = u_j$. Then, for each other node $\tilde{u} \in G_1, \tilde{u} \neq u$, we must have $s_i \not\rightsquigarrow \tilde{u}$, $s_j \not\rightsquigarrow \tilde{u}$. The condensed network is shown in Figure $4(a)$, which is equivalent to the channel model in Figure $4(b)$. Due to the Markov chain $W_i, W_j \rightarrow Y_u^n \rightarrow Y_{d_i}^n, Y_{d_j}^n$, node u can decode messages W_i and W_j with arbitrarily small probability of error, which implies that $D_\Sigma = 1$ in the first dashed box of Figure $4(b)$. The bottleneck for the sum secure d.o.f. is the second box, which is a Gaussian broadcast channel with confidential messages and M independent helpers. Here $M = |G_1| - 1 \geq 1$. Finally, by utilizing real interference alignment based scheme [38], we know that the sum secure d.o.f. of Gaussian broadcast channels with confidential messages and $M \geq 1$ helper(s) is 1 with probability one. Hence, for the networks belonging to the intersection of case A_5 and case A, $D_{s,\Sigma}$ is 1 with probability one.

Second, we consider the networks in which s_i and s_j connect to different nodes in layer V_{r-1}. We show that these networks belong to case A'. We again prove this by contradiction. Let $s_i \rightsquigarrow u_i$ and $s_j \rightsquigarrow u_j$ for some $u_i, u_j \in V_{r-1}$. If $u_i = u_j \triangleq u$, then due to the independence structure, these networks are equivalent to the network shown in Figure 4. Clearly, the removal of u disconnects d_1 from $\{s_1, s_2\}$ and s_2 from $\{d_1, d_2\}$. By definition, this is case A. This leads to a contradiction, and s_i and s_j connect to different nodes in layer V_{r-1}. The condensed network of this setting as shown in Figure 5 also becomes two concatenated networks, in which the sum secure d.o.f is dominated by the last hop due to the independence structure in layer V_{r-1}. The last hop is a two-user Gaussian interference channel with confidential messages and M independent helpers. Here $M = |G_1| - 2 \geq 0$. Finally, by [38], we know the sum secure d.o.f. of this hop:

$$D_{s,\Sigma} = \begin{cases} \frac{2}{3} & \text{if } M = 0 \\ 1 & \text{if } M \geq 1 \end{cases} \tag{18}$$

where $M = 0$ corresponds to condition (**C2**) which gives

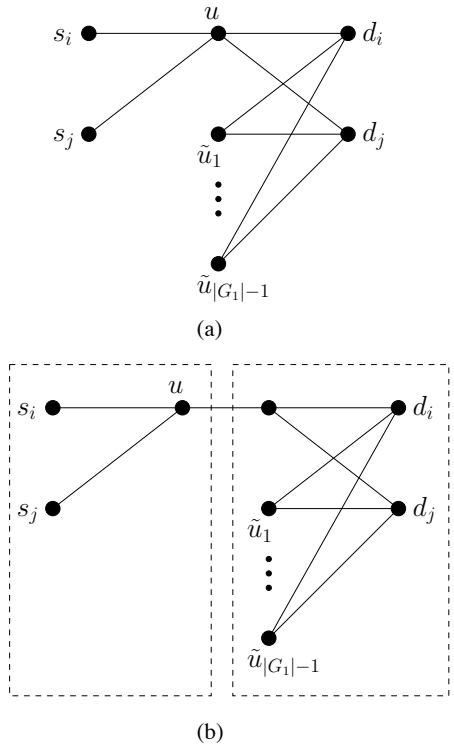


Fig. 4. The condensed network for the equivalent Gaussian broadcast channel of the sub-case A_5.

a two-user Gaussian interference channel with confidential messages, and $M \geq 1$ corresponds to the same channel model with $M \geq 1$ independent helpers.

IV. Sum Secure d.o.f. for Cases B and B'

In this section, we consider the layered networks in cases B and B'. As proven in [1], for all network configurations belonging to cases B and B', two achievable schemes are sufficient to achieve 2 sum d.o.f., where we either use a simple amplify-and-forward scheme to make the end-to-end transfer matrix diagonal with non-zero diagonal entries, i.e.,

$$\begin{bmatrix} Y_{d_1} \\ Y_{d_2} \end{bmatrix} = \begin{bmatrix} \beta_1 & 0 \\ 0 & \beta_2 \end{bmatrix} \begin{bmatrix} X_{s_1} \\ X_{s_2} \end{bmatrix} + \begin{bmatrix} N_1^{eff} \\ N_2^{eff} \end{bmatrix} \tag{19}$$

or find a $2 \times 2 \times 2$ condensed interference sub-network in the original layered network. In this section, we will show that the sum secure d.o.f is the same as the sum d.o.f., i.e., $D_{s,\Sigma} = 2$.

For the diagonal end-to-end transfer matrix, the operations of the nodes in the middle layers are either to perform amplify-and-forward or be silent, therefore, the effective noises are independent of the input signals. Moreover, due to the fact that the end-to-end transfer matrix is diagonal, for each $i = 1$ or 2, we have $I(W_i; Y_{d_j}^n) = 0$, i.e., there is no information leakage from the source node to the unintended destination node even when the effective noises at the destination nodes are dependent. By interference neutralization, for this class of networks, the sum secure d.o.f. is exactly equal to the sum d.o.f., which is 2.

For the $2 \times 2 \times 2$ interference channel, which is a cascade of two fully connected one-hop interference channels, [48] employed interference neutralization and real interference alignment to achieve 2 sum d.o.f. Here, we use this idea to design the auxiliary random variables for the $2 \times 2 \times 2$ interference channel, construct the channel inputs, and show that it can asymptotically achieve 2 sum secure d.o.f.

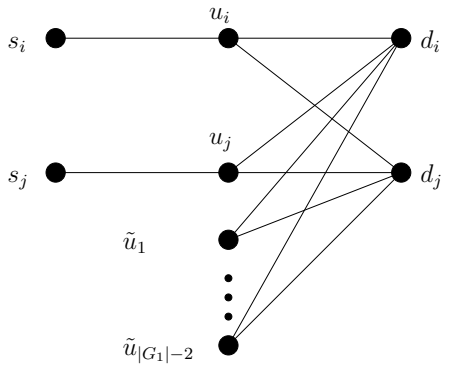


Fig. 5. The condensed network for the equivalent Gaussian interference channel of the sub-case A_5.

Theorem 4 For $2 \times 2 \times 2$ Gaussian interference channels with confidential messages, the sum secure d.o.f. is 2, with probability one.

The proof of this theorem is given in Appendix. Based on this result, for the $2 \times 2 \times 2$ condensed interference sub-network in the original layered network, we simply treat all nodes except the nodes belonging to this sub-network as silent nodes and utilize this achievable scheme. Note that although the equivalent interference sub-network has dependent noises at each node, due to the fact that the noises are independent of the message and have finite variances, the difference between these two models will not affect the performance in terms of reliability or security. Therefore, in both cases, the upper bound of 2 sum secure d.o.f. is achievable, i.e., $D_{s,\Sigma} = 2$.

V. Sum Secure d.o.f. for Case C

In this section, we consider the layered networks in case C. The converse for this case is $D_{s,\Sigma} \leq D_{\Sigma} \leq \frac{3}{2}$ from [1]. The achievability scheme proposed in [1] operates in two modes: First, a temporary node d' is chosen. In both modes, we could find a sub-network which has two disjoint paths with manageable interference to transmit 2 sum d.o.f. Node d' is one of the destinations of the first mode, which stores the information and serves as the source node in the second mode.

An example of case C is shown in Figure 6. The network in both modes are the same. In each mode, the solid lines show the links over which information is transmitted, and dashed lines show the edges that are not used. In this example, node d_1' is the temporary node, which is the last node on path P_{s_1,d_1} before the interference. In the first mode, source s_1 sends message W_1 to node d_1' and s_2 sends message W_2 to destination d_2. Since the two paths $P_{s_1,d_1'}$ and P_{s_2,d_2} are disjoint and interference free, 2 sum d.o.f. worth of information can be sent reliably and node d_1' stores message W_1. In the second mode, d_1' forwards message W_1 to d_1 and s_2 sends a new message W_2 to d_2. Since the sub-network

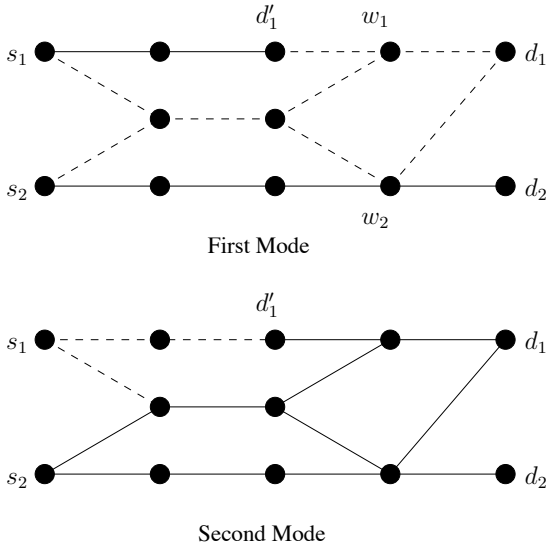


Fig. 6. The condensed network for an example of case C. Solid lines show the edges over which signals are transmitted. Dashed lines show the edges that are not used in that mode.

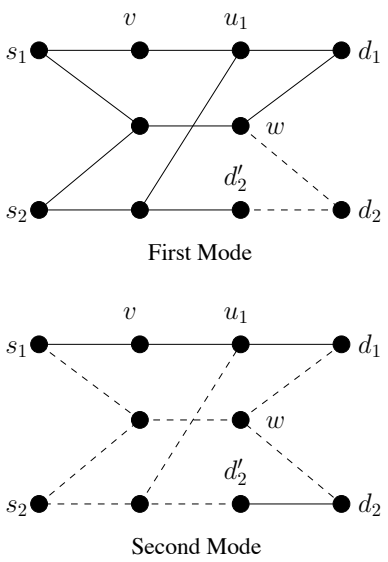


Fig. 7. The condensed network for an example of case C. Solid lines show the edges over which signals are transmitted. Dashed lines show the edges that are not used in that mode.

in solid lines between source nodes (d_1', s_2) and destination nodes (d_1, d_2) form a layered network in case B, the sum d.o.f. is 2. Finally, by choosing the number of channel uses in both modes to be the same, the achieved overall sum d.o.f. is $\frac{3}{2}$.

Reference [1] concluded that all network configurations in case C can be classified into two sub-cases C_1 and C_2. Further, in each sub-case, there are up to two different settings for the layered networks, which are given in Figures 6 and 7 for sub-case C_1, and Figures 8 and 9 for sub-case C_2. All other networks in case C have the same structure, and the same achievable scheme can be applied. In this section, we provide modified schemes for each setting of each sub-case to incorporate security in addition to reliability. In each case, we will achieve a sum secure d.o.f that is the same as the sum d.o.f., i.e., $D_{s,\Sigma} = D_\Sigma = \frac{3}{2}$.

A. Modified Scheme for Figure 6

We modify the achievable scheme described above to meet the secrecy constraint. The only issue of the original scheme is that the signal sent by w_2 in the first mode could be captured by the destination node d_1 if d_1 is in the next layer after w_2. To solve this problem, we use node w_1 on the path P_{s_1,d_1} and in the same layer as w_2 to jam the destination node d_1. Then, this hop simply becomes a Gaussian wiretap channel with a cooperative jammer, where the cooperative jammer is connected to the unintended receiver, but not to the intended receiver. This network has 1 secure d.o.f., i.e., node w_2 decodes the message it received and transmits the message based on a wiretap codebook to keep the message secure against the unintended destination d_1.

B. Modified Scheme for Figure 7

The other setting for layered networks in sub-case C_1 is shown in Figure 7. In the first mode, the source pair (s_1, s_2) transmits (W_1, W_2) to the destination pair (d_1, d_2'), where d_2' is the temporary node to store message W_2. Clearly, P_{s_1,d_1} and $P_{s_2,d_2'}$ are disjoint paths with manageable interference, i.e., case B. We can transmit W_1 to d_1 and W_2 to d_2' reliably and achieve 2 sum d.o.f. In the second mode, s_1 transmits a new message $\tilde{W}_1$ to d_1 and d_2' forwards message W_2 it received in the first mode to d_2. This scheme can achieve $\frac{3}{2}$ sum d.o.f., but the messages are not securely transmitted. The reason is that, in the first mode, if the destination node d_2 is in the next layer of w, it can receive a mixed signal from w, which contains both W_1 and W_2.

To ensure the secrecy of both messages, we need to modify the achievable scheme and form an effective Gaussian wiretap channel with finite-variance noises. To this end, node d_2' sends pure Gaussian noise with average power P to jam the unintended receiver d_2. Signals from s_2 through different paths are canceled at d_1 due to the amplify-and-forward scheme used in case B. Since d_2 can decode W_2 after the second mode, it is safe to assume that in the first mode the signal relayed by node w does not contain the channel input of s_2. Therefore, the source-destination pair (s_1, d_1) forms a wiretap channel, where d_2 is the eavesdropper. Since the secrecy capacity depends only on the marginal distribution of $X_{s_1}, Y_{d_1}, Y_{d_2}$, but not the joint distribution, with the help of cooperative jamming from d_2', we can always achieve 1 secure d.o.f. for the condensed wiretap channel even when the effective Gaussian additive noises at d_1 and d_2 are dependent.

C. Modified Scheme for Figure 8

The first setting of sub-case C_2 is shown in Figure 8. For the disjoint paths P_{s_1,d_1} and P_{s_2,d_2} in layered networks of sub-case C_2, there always exists a direct interference, i.e., two nodes v_1 and v_2 satisfy $v_1 \in P_{s_1,d_1}, v_2 \in P_{s_2,d_2}$ and $(v_2, v_1) \in E$ which implies $v_2 \overset{I}{\rightsquigarrow} P_{s_1,d_1}$. Meanwhile, as proven in [1], for this sub-case, there also exists a path Q_{s_1,d_1} such that $Q_{s_1,d_1} \cap P_{s_2,d_2} = \phi$ and $v_1 \notin Q_{s_1,d_1}$. This implies $v_1 \neq d_1$,

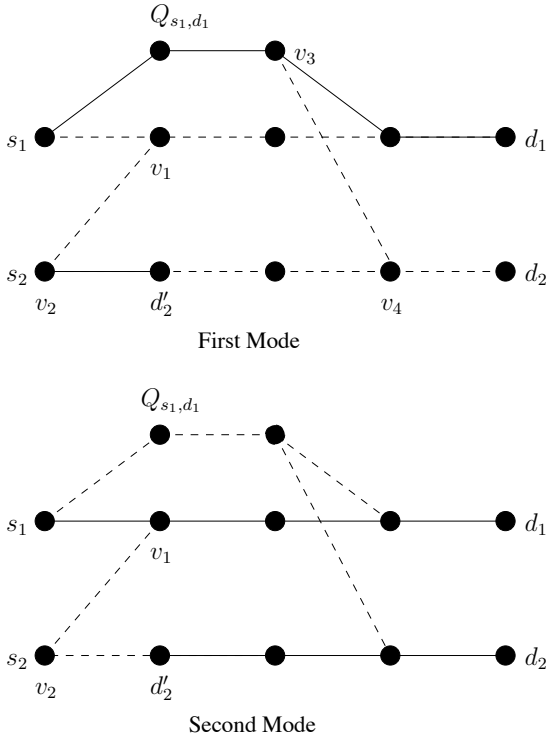


Fig. 8. The condensed network for one of two cases in C_2. Solid lines show the edges over which signals are transmitted. Dashed lines show the edges that are not used in that mode.

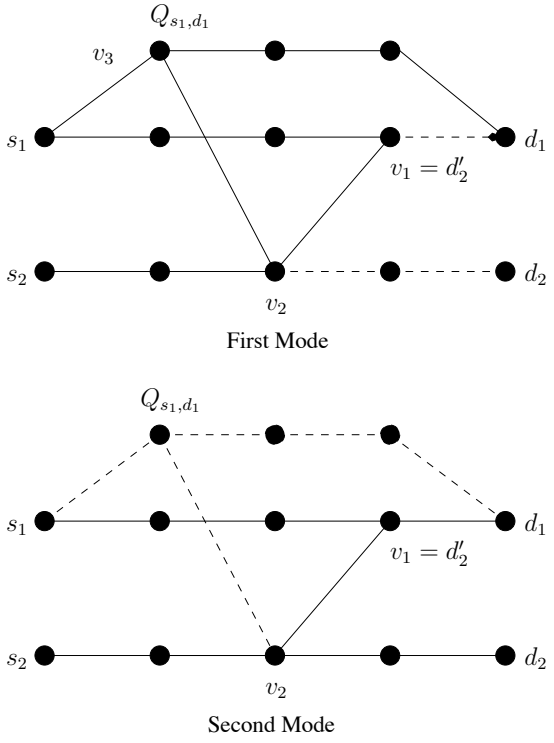


Fig. 9. The condensed network for one of two cases in C_2. Solid lines show the edges over which signals are transmitted. Dashed lines show the edges that are not used in that mode.

and the $d_2' \neq d_2$, where d_2' is the temporary node on the path P_{s_2,d_2} and in the same layer with v_1.

To achieve $\frac{3}{2}$ sum secure d.o.f., we use the following modified achievable scheme. In the first mode, s_1 transmits message W_1 along the path Q_{s_1,d_1} to d_1, and s_2 transmits message W_2 along the path $P_{s_2,d_2'}$. If $d_2 = v_4$ which may receive the signal from v_3, we can always find a node on the path P_{s_2,d_2} to cooperatively jam d_2 due to the fact $d_2' \neq d_2$. In the second mode, s_1 transmits a new message $\tilde{W}_1$ along the path P_{s_1,d_1} to d_1, and d_2' relays message W_2 stored in the first mode along the path P_{d_2',d_2}. The two paths P_{s_1,d_1} and P_{d_2',d_2} are interference free, and therefore, the transmission is reliable and secure.

D. Modified Scheme for Figure 9

The second setting of sub-case C_2 is shown in Figure 9. The temporary node d_2' is chosen to be v_1. In this configuration, we also have $v_1 = d_2' \neq d_1$ and $l(d_2) > l(v_2) + 1$. In the first mode, s_1 transmits message W_1 along the path Q_{s_1,d_1} to d_1, and s_2 transmits message W_2 along the path $P_{s_2,d_2'}$. This sub-network belongs to case B, which has 2 sum d.o.f. Since $d_2' \neq d_1$ and d_2 is not in the next layer of v_2, by keeping v_1 silent, messages W_1 and W_2 are secure. In the second mode, s_1 transmits a new message $\tilde{W}_1$ along the path P_{s_1,d_1} to d_1, and s_2 transmits message W_2 along the path P_{s_2,d_2}. Since d_2' has message W_2, it can decode message W_1 and only relay W_1 to d_1, which implies that $D_{s,\Sigma} = \frac{3}{2}$.

VI. Conclusion

In this paper, we considered the sum secure d.o.f. of two-unicast layered wireless networks. We used the setting in [1] and studied the cases in A, A', B, B' and C separately to incorporate security in addition to reliability. The major challenge was in cases A and A', where the sum d.o.f. is 1, due to the fact that both destination nodes can decode the message signals. While this is inconsequential for the reliability problem in [1], it is a major problem when security is considered. To overcome this problem, we classified layered wireless networks into more detailed sub-cases, and in all sub-cases proposed modified achievable schemes that guarantee both reliability and security. In almost all sub-cases, we utilized the cooperative jamming and interference neutralization techniques to design an appropriate achievable scheme. A remaining challenge was a special configuration, where all of the nodes in the last layer before the destination layer were allowed to send only independent signals. We reduced the layered networks in this category into equivalent channel models and determined their secure d.o.f. using the recent results in [38]. As a result, we showed that all networks in cases A and A' have sum secure d.o.f. of $0, \frac{2}{3}$, or 1. We proposed modified schemes to achieve 2 sum secure d.o.f. for cases B and B' (which included the achievable scheme for the $2 \times 2 \times 2$ interference networks), and $\frac{3}{2}$ sum secure d.o.f. for case C.

Appendix

In this section, we will show that sum secure d.o.f. of 2 can be achieved in the $2 \times 2 \times 2$ interference network with constant channel gains. The $2 \times 2 \times 2$ interference network is a concatenation of two fully connected two-user Gaussian interference channels. The main idea is to design a

wiretap channel with proper auxiliary random variables, and to show that with such a choice of random variables, the achievable secrecy rate can asymptotically approach 1 secure d.o.f. for each user. Our achievability is mainly based on the real interference alignment [10] based scheme in [48]. There are two differences: 1) In [48], M signals are employed for transmitter 1 and $M-1$ signals are employed for transmitter 2. The integer M is chosen sufficiently large such that 1 d.o.f. can be achieved asymptotically for each user. Due to the fact that the last signal of transmitter 1, $x_{1,M}$, can be decoded by transmitter 2, this scheme is insecure. Here, we use only $M-1$ signals in the transmission by choosing $x_{1,M}=0$. 2) To achieve 2 sum d.o.f. in the $2\times 2\times 2$ interference network, in addition to scaling the signals with proper coefficients based on real interference alignment, the nodes in the middle layer of the $2\times 2\times 2$ interference network perform hard decisions to decode the original channel inputs from the previous layer and resend the signals again with well-designed coefficients. If these hard decisions have no error, then due to the special construction of the channel inputs based on interference neutralization and interference alignment, the messages are secure. However, if errors occur during decoding in the middle layer, then the mixed signals containing both messages observed by both destination nodes may leak information. To show the optimality of the proposed achievable scheme, we observe that the message rate scales with $\log P$, but the probability of hard decision error decreases exponentially fast with P, which makes the information leakage rate negligible in the high SNR regime. We provide a precise performance analysis in terms of both reliability and secrecy.

We use the notation in [48] for the channel model. In the first hop, the received signal at relay $R_k, k\in\{1,2\}$ is

$$Y_{R_k}=F_{k1}X_1+F_{k2}X_2+Z_k \tag{20}$$

where F_{kj} is the channel gain from source S_j to relay R_k, X_j is the input signal from S_j, Y_{R_k} is the received signal at relay R_k, and Z_k is an additive zero-mean unit-variance Gaussian noise. In the second hop, the received signal at destination $D_k, k\in\{1,2\}$ is given by

$$Y_k=G_{k1}X_{R_1}+G_{k2}X_{R_2}+N_k \tag{21}$$

where G_{kj} is the channel gain from relay R_j to destination D_k, X_{R_j} is the input signal from relay R_j, Y_k is the received signal at D_k and N_k is an additive zero-mean unit-variance Gaussian noise. All the channel gains in the network are fixed during the communication session and known at all nodes.

In contrast to separating the message W_i into M independent sub-messages $W_{i,k_i}(k_i\in\{1,2,\cdots,M\})$ in [48], we need to construct a virtual wiretap channel to achieve the sum secure d.o.f. For each user i, we separate the channel input signal x_i into M independent sub-signals $\{x_{i,k_i}\}_{k_i=1}^M$. The constellation of each sub-signal x_{i,k_i} is defined as follows

$$C(Q)=\{-Q,-Q+1,\cdots,Q-1,Q\} \tag{22}$$

If x_{i,k_i}'s are independent and uniform, each of them carries $\log(2Q+1)$ bits. The real channel input x_i is set to be the linear combination of $\{x_{i,k_i}\}$ with the rationally independent coefficients[1] $\{t_{i,k_i}\}$, i.e.,

$$x_i=a\sum_{k_i=1}^{M}t_{i,k_i}x_{i,k_i} \tag{23}$$

where a is a constant to normalize the input signal power, and $t_{2,M}=0$ since we only need $M-1$ data signals for x_2. The average power of this channel input is

$$\mathrm{E}[x_i^2]\le a^2\left(\sum_{k_i=1}^{M}|t_{i,k_i}x_{i,k_i}|\right)^2\le\left(\sum_{k_i=1}^{M}|t_{i,k_i}|\right)^2a^2Q^2 \tag{24}$$

When M is fixed, which will be specified later, we denote $\xi=\max_{i=1,2}\left(\sum_{k_i=1}^{M}|t_{i,k_i}|\right)^2$, and, for any $\epsilon>0$, we choose

$$Q=P^{\frac{1-\epsilon}{2(M+\epsilon)}},\quad a=\frac{1}{\sqrt{\xi}}P^{\frac{M-1+2\epsilon}{2(M+\epsilon)}} \tag{25}$$

Then, the signals x_1 and x_2 both satisfy the average power constraint, i.e.,

$$\mathrm{E}[x_i^2]\le P,\quad \text{for } i=1,2 \tag{26}$$

Furthermore, from [10], the minimum distance d_{min} between the points in the combined constellation can be lower bounded as follows:

$$d_{min}\ge\frac{k_\epsilon a}{(2Q)^{M-1+\epsilon}}=\frac{k_\epsilon}{2^{M-1+\epsilon}\sqrt{\xi}}P^{\frac{\epsilon}{2}} \tag{27}$$

for some constant k_ϵ, which depends on ϵ, but not on P. This result implies that the error probability of hard decisions to recover the PAM signals decreases exponentially with the power P^ϵ.

We use the scheme in [48] to design the coefficients t_{i,k_i}s. At the relay node R_1, the received signal is as follows

$$Y_{R_1}=F_{1,1}t_{1,1}x_{1,1}+\sum_{i=1}^{M-1}F_{1,1}t_{1,i+1}(x_{1,i+1}+x_{2,i})+Z_1 \tag{28}$$

We denote

$$x_{R_1,1}=x_{1,1} \tag{29}$$

$$x_{R_1,i+1}=x_{1,i+1}+x_{2,i},\quad \text{for } i=1,\cdots,M-1 \tag{30}$$

It is easy to see that $x_{R_1,1}\in C(Q)$ and $x_{R_1,i+1}\in C(2Q)$ for $i=1,\cdots,M-1$.

Relay node R_1 performs hard decision to get $\hat{x}_{R_1,i}$ for $i=1,\cdots,M$. The probability of decoding error $\mathrm{P}_e(R_1)$ decreases exponentially with power P^ϵ and the channel input of the relay node R_1 is:

$$x_{R_1}=b\sum_{k_1=1}^{M}t_{R_1,k_1}\hat{x}_{R_1,k_1} \tag{31}$$

where b is again a constant to normalize the input signal power. Similarly, relay node R_2 makes the hard decision $\hat{x}_{R_2,i}$ of the signals $x_{R_2,i}$,

$$x_{R_2,i}=x_{1,i}+x_{2,i},\quad \text{for } i=1,\cdots,M-1 \tag{32}$$

$$x_{R_2,M}=x_{1,M} \tag{33}$$

[1] $a_1,a_2,\ldots,a_L$ are rationally independent if whenever $q_1,q_2,\ldots,q_L$ are integer numbers then $\sum_{i=1}^{L}q_ia_i=0$ implies $q_i=0$ for all i.

and the probability of error $\mathrm{P}_e(R_2)$ exponentially decreases with power P^ϵ. The channel input of the relay node R_2 is:

$$x_{R_2} = b\sum_{k_2=1}^{M-1} t_{R_2,k_2}\hat{x}_{R_2,k_2} \tag{34}$$

The selection of $\{t_{R_1,k_1}\}$ and $\{t_{R_2,k_2}\}$ can be found in [48].

The observations of the two receivers in the final layer are

$$Y_1 = b\sum_{i=1}^{M} G_{1,1}t_{R_1,i}x_{D_1,i} + N_1 \tag{35}$$

$$Y_2 = bG_{2,1}t_{R_1,M}x_{D_2,M} + b\sum_{i=1}^{M-1} G_{2,2}t_{R_2,i}x_{D_2,i} + N_2 \tag{36}$$

where

$$x_{D_1,1} = \hat{x}_{R_1,1} \tag{37}$$

$$x_{D_1,i+1} = \hat{x}_{R_1,i+1} - \hat{x}_{R_2,i}, \quad \text{for } i = 1,\cdots,M-1 \tag{38}$$

$$x_{D_2,i} = \hat{x}_{R_2,i} - \hat{x}_{R_1,i}, \quad \text{for } i = 1,\cdots,M-1 \tag{39}$$

$$x_{D_2,M} = \hat{x}_{R_1,M} \tag{40}$$

Denote by A the event that the hard decisions at relay nodes 1 and 2 are both correct. Then, the probability of the complement event $\bar{A}$ decreases exponentially with power P^ϵ due to the following inequality

$$\begin{aligned}
&1-\Pr(A)\\
&\quad= \Pr(\bar{A}) && (41)\\
&\quad= \Pr(\text{hard decision error occurs at } R_1 \text{ and/or } R_2) && (42)\\
&\quad\le \mathrm{P}_e(R_1)+\mathrm{P}_e(R_2) && (43)\\
&\quad\le 2\exp(-c_0P^\epsilon) && (44)
\end{aligned}$$

for some constant c_0 independent of P. If event A happens, which indicates that the hard decisions at both relay nodes are correct, then it is clear that

$$x_{D_1,1} = \hat{x}_{R_1,1} = x_{1,1} \tag{45}$$

$$\begin{aligned}
x_{D_1,i+1} &= \hat{x}_{R_1,i+1} - \hat{x}_{R_2,i}\\
&= x_{1,i+1} + x_{2,i} - x_{1,i} - x_{2,i}\\
&= x_{1,i+1} - x_{1,i}, \qquad \text{for } i = 1,\cdots,M-1
\end{aligned} \tag{46}$$

and

$$\begin{aligned}
x_{D_2,1} &= \hat{x}_{R_2,1} - \hat{x}_{R_1,1}\\
&= x_{1,1} + x_{2,1} - x_{1,1}\\
&= x_{2,1}
\end{aligned} \tag{47}$$

$$\begin{aligned}
x_{D_2,i} &= \hat{x}_{R_2,i} - \hat{x}_{R_1,i}\\
&= x_{1,i} + x_{2,i} - x_{1,i} - x_{2,i-1}\\
&= x_{2,i} - x_{2,i-1}, \qquad \text{for } i = 2,\cdots,M-1
\end{aligned} \tag{48}$$

$$\begin{aligned}
x_{D_2,M} &= \hat{x}_{R_1,M}\\
&= x_{1,M} + x_{2,M-1}
\end{aligned} \tag{49}$$

which means that the observation Y_1 and $\{x_{2,i}\}_{i=1}^{M-1}$ are independent and, except the item $x_{1,M}$, the observation Y_2 and $\{x_{1,i}\}_{i=1}^{M-1}$ are independent[2].

To design the wiretap code, we choose the auxiliary random variables $v_{1,i}$ and $v_{2,i}$ as

$$v_{1,i} = x_{1,i} \text{ and } v_{2,i} = x_{2,i}, \quad \text{for } i = 1,\cdots,M-1 \tag{50}$$

with uniform distribution in $C(Q)$ and choose $x_{1,M} = 0$. Since for different channel uses the signals are i.i.d., and W_1, W_2 are independent, the following secrecy rate pair is achievable [15, Theorem 2]:

$$I(\bar{v}_i;Y_i) - I(\bar{v}_i;Y_j|\bar{v}_j) \tag{51}$$

where $\bar{v}_i \triangleq (v_{i,1}, v_{i,2}, \cdots, v_{i,M-1})$ and $\bar{v}_j \triangleq (v_{j,1}, v_{j,2}, \cdots, v_{j,M-1})$ for $i = 1,2$, and $j = \bar{i}$. By [48], information rate part, i.e., the first item in (51), is given by

$$I(\bar{v}_i;Y_i) \ge \frac{(M-1)(1-\epsilon)}{2(M+\epsilon)}\log P + o(\log P) \tag{52}$$

To upper bound the second item in (51), we define the binary random variable Z_A as

$$Z_A = \mathbb{1}_{\{A\}} \tag{53}$$

where $\mathbb{1}_{\{\cdot\}}$ is the indicator function. As shown above, when event A happens,

$$\bar{v}_i \to \bar{v}_j \to Y_j \tag{54}$$

forms a Markov chain for $i = 1,2$ and $j = \bar{i}$, i.e.,

$$I(\bar{v}_i;Y_j|\bar{v}_j, Z_A = 1) = 0 \tag{55}$$

The difficulty to analyze the achievable secrecy rate is that when the hard decisions at relay nodes are in error, the mixed signals at the unintended receiver will not be aligned in the *perfect* way, which will introduce dependence between the Y_j and $v_{i,1\ldots M-1}$. However, we can upper bound the mutual information for each i as follows:

$$\begin{aligned}
I(\bar{v}_i;Y_j|\bar{v}_j) &= H(\bar{v}_i) - H(\bar{v}_i|Y_j,\bar{v}_j) && (56)\\
&\le H(\bar{v}_i) - H(\bar{v}_i|Y_j,Z_A,\bar{v}_j) && (57)
\end{aligned}$$

where the latter item can be rewriten as

$$\begin{aligned}
&H(\bar{v}_i|Y_j,Z_A,\bar{v}_j)\\
&\quad= \sum_{z\in\{0,1\}} P(Z_A=z)H(\bar{v}_i|Y_j,Z_A=z,\bar{v}_j) && (58)\\
&\quad\ge P(Z_A=1)H(\bar{v}_i|Y_j,Z_A=1,\bar{v}_j) && (59)\\
&\quad= P(Z_A=1)H(\bar{v}_i|Z_A=1,\bar{v}_j) && (60)
\end{aligned}$$

(60) is due to (55). The former item in (57) can be upper bounded by

$$\begin{aligned}
H(\bar{v}_i) &= H(\bar{v}_i|Z_A,\bar{v}_j) + H(Z_A,\bar{v}_j) - H(Z_A,\bar{v}_j|\bar{v}_i) && (61)\\
&= H(\bar{v}_i|Z_A,\bar{v}_j) + H(\bar{v}_j) + H(Z_A|\bar{v}_j)\\
&\qquad - H(\bar{v}_j|\bar{v}_i) - H(Z_A|\bar{v}_j,\bar{v}_i) && (62)\\
&= H(\bar{v}_i|Z_A,\bar{v}_j) + H(Z_A|\bar{v}_j) - H(Z_A|\bar{v}_j,\bar{v}_i) && (63)\\
&\le H(\bar{v}_i|Z_A,\bar{v}_j) + 1 && (64)\\
&= \sum_{z\in\{0,1\}} P(Z_A=z)H(\bar{v}_i|Z_A=z,\bar{v}_j) + 1 && (65)
\end{aligned}$$

[2]Note that $\{x_{1,i}\}_{i=1}^{M}$ are i.i.d.

Substituting (60) and (65) in (57), we have

$$I(\bar{v}_i;Y_j|\bar{v}_j) \leq \sum_{z\in\{0,1\}} P(Z_A=z)H(\bar{v}_i|Z_A=z,\bar{v}_j)+1 - P(Z_A=1)H(\bar{v}_i|Z_A=1,\bar{v}_j) \quad (66)$$

$$\leq P(Z_A=0)H(\bar{v}_i|Z_A=0,\bar{v}_j)+1 \quad (67)$$

$$\leq P(\bar{A})H(\bar{v}_i|Z_A=0,\bar{v}_j)+1 \quad (68)$$

$$\leq o(\log P) \quad (69)$$

The last inequality is due to (44) and the finite alphabet of the vector $\bar{v}_i=(v_{i,1},v_{i,2},\cdots,v_{i,M-1})$, which is maximized by uniform distribution, i.e.,

$$H(\bar{v}_i|Z_A=0,\bar{v}_j) \leq \log|C|^{M-1} \quad (70)$$

$$= \frac{(M-1)(1-\epsilon)}{2(M+\epsilon)}\log P + o(\log P) \quad (71)$$

which means that the achievable rate (51) is lower bounded by

$$\frac{(M-1)(1-\epsilon)}{2(M+\epsilon)}\log P + o(\log P) \quad (72)$$

If we choose M large enough, then the sum secure d.o.f. will approach 2 arbitrarily close, completing the proof.

REFERENCES

[1] I. Shomorony and A. S. Avestimehr. Two-unicast wireless networks: Characterizing the degrees of freedom. *IEEE Trans. Inf. Theory*, 59(1):353–383, January 2013.

[2] A. El Gamal and M. Costa. The capacity region of a class of deterministic interference channels. *IEEE Trans. Inf. Theory*, 28(2):343–346, March 1982.

[3] A. B. Carleial. A case where interference does not reduce capacity. *IEEE Trans. Inf. Theory*, 21(5):569–570, September 1975.

[4] H. Sato. On the capacity region of a discrete two-user channel for strong interference. *IEEE Trans. Inf. Theory*, 24(3):377–379, March 1978.

[5] H. Sato. The capacity of the Gaussian interference channel under strong interference. *IEEE Trans. Inf. Theory*, 27(6):786–788, November 1981.

[6] N. Liu and S. Ulukus. The capacity region of a class of discrete degraded interference channels. *IEEE Trans. Inf. Theory*, 54(9):4372–4378, September 2008.

[7] V. R. Cadambe and S. A. Jafar. Interference alignment and degrees of freedom of the K-user interference channel. *IEEE Trans. Inf. Theory*, 54(8):3425–3441, August 2008.

[8] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani. Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis. *IEEE Trans. Inf. Theory*, 54(8):3457–3470, Aug. 2008.

[9] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani. Real interference alignment with real numbers. *IEEE Trans. Inf. Theory*, submitted August 2009. Also available at [arXiv:0908.1208].

[10] A. S. Motahari, S. Oveis-Gharan, M. A. Maddah-Ali, and A. K. Khandani. Real interference alignment: Exploiting the potential of single antenna systems. *IEEE Trans. Inf. Theory*, submitted November 2009. Also available at [arXiv:0908.2282].

[11] A. Host-Madsen and A. Nosratinia. The multiplexing gain of wireless networks. In *IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[12] A. D. Wyner. The wiretap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, January 1975.

[13] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[14] S. K. Leung-Yan-Cheong and M. E. Hellman. Gaussian wiretap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, July 1978.

[15] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, June 2008.

[16] J. Xu, Y. Cao, and B. Chen. Capacity bounds for broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 55(10):4529–4542, October 2009.

[17] A. Khisti, A. Tchamkerten, and G. W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, June 2008.

[18] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, March 2009.

[19] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. Secure broadcasting: The secrecy rate region. In *46th Annual Allerton Conference on Communications, Control and Computing*, Monticello, IL, September 2008.

[20] E. Ekrem and S. Ulukus. Secure broadcasting using multiple antennas. *J. Communications and Networks*, 12(5):411–432, October 2010.

[21] X. He and A. Yener. A new outer bound for the Gaussian interference channel with confidential messages. In *43rd Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2009.

[22] O. O. Koyluoglu and H. El Gamal. Cooperative encoding for secrecy in interference channels. *IEEE Trans. Inf. Theory*, 57(9):5681–5694, September 2011.

[23] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, December 2008.

[24] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54(6):2735–2751, June 2008.

[25] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.

[26] Y. Liang and H. V. Poor. Multiple-access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, March 2008.

[27] E. Ekrem and S. Ulukus. Cooperative secrecy in wireless communications. *Securing Wireless Communications at the Physical Layer*, W. Trappe and R. Liu, Eds., Springer-Verlag, 2009.

[28] Y. Oohama. Relay channels with confidential messages. *IEEE Trans. Inf. Theory, Special issue on Information Theoretic Security*, submitted Nov 2006. Also available at [arXiv:cs/0611125v7].

[29] L. Lai and H. El Gamal. The relay-eavesdropper channel: cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, September 2008.

[30] M. Yuksel and E. Erkip. The relay channel with a wiretapper. In *41st Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2007.

[31] M. Bloch and A. Thangaraj. Confidential messages to a cooperative relay. In *IEEE Information Theory Workshop*, Porto, Portugal, May 2008.

[32] X. He and A. Yener. Cooperation with an untrusted relay: A secrecy perspective. *IEEE Trans. Inf. Theory*, 56(8):3807–3827, August 2010.

[33] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. *IEEE Trans. Inf. Theory*, 57(1):137–155, January 2011.

[34] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz). Compound wiretap channels. *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, March 2009.

[35] E. Ekrem and S. Ulukus. Degraded compound multi-receiver wiretap channels. *IEEE Trans. Inf. Theory*, 58(9):5681–5698, September 2012.

[36] X. He and A. Yener. K-user interference channels: Achievable secrecy rate and degrees of freedom. In *IEEE Information Theory Workshop on Networking and Information Theory*, Volos, Greece, June 2009.

[37] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. Interference alignment for secrecy. *IEEE Trans. Inf. Theory*, 57(6):3323–3332, June 2011.

[38] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. Submitted to *IEEE Trans. on Information Theory*, September 2012. Also available at [arXiv:1209.5370].

[39] J. Xie and S. Ulukus. Real interference alignment for the K-user Gaussian interference compound wiretap channel. In *48th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2010.

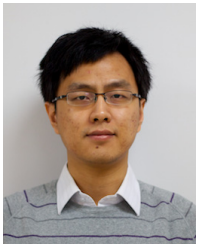
[40] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers. In *50th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, October 2012.

[41] X. He and A. Yener. Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels. *IEEE Trans. Inf. Theory*, submitted July 2009. Also available at [arXiv:0907.5388].

[42] X. He. *Cooperation and information theoretic security in wireless networks*. Ph.D. dissertation, Pennsylvania State University, Pennsylvania, 2010.

[43] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure degrees-of-freedom of the multiple-access-channel. *IEEE Trans. Inf. Theory*, submitted March 2010. Also available at [arXiv:1003.0729].

[44] R. Bassily and S. Ulukus. Ergodic secret alignment. *IEEE Trans. Inf. Theory*, 58(3):1594–1611, March 2012.
[45] T. Gou and S. A. Jafar. On the secure Degrees of Freedom of wireless X networks. In *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.
[46] S. Mohajer, S. N. Diggavi, C. Fragouli, and D. Tse. Transmission techniques for relay-interference networks. In *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.
[47] X. He and A. Yener. Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling. In *IEEE Global Telecommunications Conference*, Honolulu, Hawaii, December 2009.
[48] T. Gou, S. A. Jafar, and S. Chung S. Jeon. Aligned interference neutralization and the degrees of freedom of the $2 \times 2 \times 2$ interference channel. *IEEE Trans. Inf. Theory*, 58(7):4381–4395, July 2012.



Jianwei Xie received the B.S. and M.S. degrees in electronic engineering from the Tsinghua University, Beijing, China, in 2006 and 2008, respectively. Currently, he is working toward the Ph.D. degree in the department of electrical and computer engineering at the University of Maryland, College Park. He received the Distinguished Dissertation Fellowship from the ECE Department at the University of Maryland, College Park, in 2013. His research interests include information theory and wireless communications.

Sennur Ulukus is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, information-theoretic physical-layer security, and energy-harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, an 2005 NSF CAREER Award, the 2010-2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 George Corcoran Education Award. She served as an Associate Editor for the IEEE Transactions on Information Theory (2007-2010) and IEEE Transactions on Communications (2003-2007). She served as a Guest Editor for the Journal of Communications and Networks for the special issue on energy harvesting in wireless networks (2012), IEEE Transactions on Information Theory for the special issue on interference networks (2011), IEEE Journal on Selected Areas in Communications for the special issue on multiuser detection for advanced communication systems and networks (2008). She served as the TPC co-chair of the Communication Theory Symposium at 2013 IEEE ICC, Physical-Layer Security Workshop at 2011 IEEE Globecom, Physical-Layer Security Workshop at 2011 IEEE ICC, 2011 Communication Theory Workshop (IEEE CTW), Wireless Communications Symposium at 2010 IEEE ICC, Medium Access Control Track at 2008 IEEE WCNC, and Communication Theory Symposium at 2007 IEEE Globecom. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007-2009.