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

Jianwei Xie Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
xiejw@umd.edu *ulukus@umd.edu*

***Abstract*—In this paper, we study the sum secure degrees of freedom (d.o.f.) of two-unicast layered wireless networks. Without a secrecy constraint, the sum d.o.f. of this class of networks was studied by [1] and shown to take only one of three possible values: $1, 3/2$ and 2, for all network configurations. We consider the setting where the message of each source-destination pair must be kept information-theoretically secure from the unintended receiver. We show that the sum secure d.o.f. can take $0, 1, 3/2, 2$ and at most countably many other positive values, which we enumerate.**

I. Introduction

We consider a two-unicast layered network (see Fig. 1) where two transmitters wish to have reliable and secure communication with their respective receivers simultaneously, by utilizing a layered network between the transmitters and receivers. The single-layer 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]–[9]. In particular, the sum d.o.f. of a fully connected interference channel is 1 [10]. The interference channel has been studied from an information-theoretic security [11], [12] point of view in several settings, e.g., [13], [14].

Two-unicast layered networks have been studied in [15]–[17] where conditions to achieve only one rate pair have been given. Recently, [1] showed that, if the source-destination pairs are connected, with probability 1, two-unicast layered Gaussian networks can only have three possible values for the sum d.o.f.: 1, 3/2 or 2. To achieve this result, [1] divided all possible network structures into five sub-classes, A, A', B, B' and C, and determined the sum d.o.f. in each case.

We extend this line of work to include security in addition to reliability for the end-to-end users. In the first part of this work, we show that although for cases A and A' in [1] the sum d.o.f. is exactly 1, the sum secure d.o.f. can take values 0, 1 and at most countably many other positive values. These values are unknown, but we provide the simplest equivalent channel models whose sum secure d.o.f. give these values. In the second part of this work, we propose schemes to achieve 2 sum secure d.o.f. for cases B and B', and $3/2$ sum secure d.o.f. for case C. For most cases, some nodes perform cooperative jamming [18] to help increase the secrecy rates of the legitimate users. For the $2 \times 2 \times 2$ interference network [19], we prove that the sum secure d.o.f. is 2 and give the corresponding achievable scheme.

This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811.

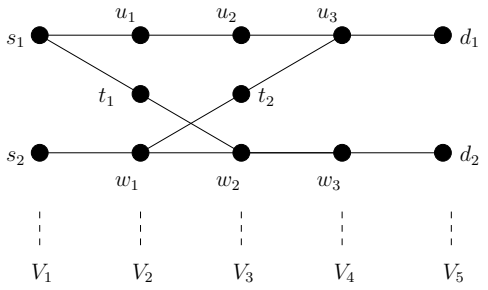

Fig. 1. An example two-unicast layered network.

In our achievable schemes, in most scenarios, we either find a node and utilize it to protect the communication by having it perform cooperative jamming [18] against the unintended receiver, or employ the real interference alignment tool [9] to align the signals at both destination nodes in a desired way. However, in some certain classes of layered networks, such nodes do not exist. To overcome this problem, we use the interference neutralization technique [20] to neutralize the message signal at the unintended destination and even neutralize the artificial noise at the intended receiver to mimic the wiretap channel with cooperative jamming. After discussing all these possibilities, we note that there is still a class of layered wireless networks in which the sum secure d.o.f. is an open problem. Our second contribution is to find the simplest equivalent channel model to characterize this class of networks. Under this classification, once the equivalent problem is solved, the sum secure d.o.f. of layered networks will be resolved. The sum secure d.o.f. of this class of networks can only take at most a countably many number of values. Therefore, we determine the sum secure d.o.f. for all two-unicast layered networks as countably many possible values by utilizing these canonical networks.

II. Definition 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 $V_1, V_2, \cdots, V_r$ 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 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 $i = 1, 2, \cdots, k-1$. And, 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 case, we always assume that $s_1 \rightsquigarrow d_1$ and $s_2 \rightsquigarrow d_2$. In addition, 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.*

To characterize the interference form another pair, the number of the 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 $S \subset V$ 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 Fig. 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 a 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. For the input signal of each node u, we assume that X_u satisfies an average power constraint P, i.e.,

$$\frac{1}{n} \sum_{t=1}^{n} X_u^2(t) \leq P \tag{4}$$

where n is the total number of channel uses and $X_u(t)$ is the input signal sent from node u at time t.

For each source-destination pair (s_i, d_i), the source node s_i intends to transmit a message W_i from a message set $\mathcal{W}_i$ to the destination node d_i, and keep it secure against d_j[1]. For a fixed n, the number of channel uses, we assume that each node in the network is allowed to use any encoding/decoding function. For a fixed but small enough $\epsilon > 0$, the rate $R_i = \frac{1}{n} \log |\mathcal{W}_i|$ is achievable if the probability of decoding error at destination d_i is smaller than ϵ.

The rate R_i will be the secure communication rate R_{s_i} of pair i if it satisfies the secrecy constraint, which is defined as follows: For any $i = 1$ or 2, the uncertainty of message W_i, given the observation of the other destination $Y_{d_j}^n$, is almost equal to the entropy of the message, i.e.,

$$H(W_i|Y_{d_j}^n) \geq H(W_i) - n\epsilon, \quad i = 1, 2 \tag{5}$$

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:

$$D_{s,\Sigma} = \limsup_{P\to\infty} \sup \frac{R_{s_1} + R_{s_2}}{\frac{1}{2} \log P} \tag{6}$$

where the supremum is taken over all possible encoding/decoding functions at the nodes in the network.

The sum d.o.f. of two-unicast layered networks is found as:

Theorem 1 (Sum d.o.f. of two-unicast network [1]) *For a two-unicast layered Gaussian network 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,
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

[1]Here we use the notation $j = \bar{i}$, i.e., $i = 1, j = 2$ or $i = 2, j = 1$.

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.

III. Sum Secure D.O.F. for Case A

The sum d.o.f. capacity result is $D_\Sigma = 1$ for this case, which is an upper bound for the sum secure d.o.f. To find all possible values of sum secure d.o.f., we first characterize the penultimate layer V_{r-1}:

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

where G_is are mutually disjoint sets defined as follows:

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

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 the set G_4 is zero, i.e., $|G_4| = 0$.

We present our results in sub-cases with an ordered series $(A_1, A_2, \cdots)$, which implicitly means that A_i only contains the setting $A_i \cap (\cup_{j=1}^{i-1} A_j)^c$ for all i.

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

Without loss of generality, we give the brief idea of the proof for the condition $|G_3| \geq 1$. There exists at least one node $u \in G_3$. We can utilize node u to cooperatively jam d_2 with average power P. Then, the last hop of the network forms a Gaussian wiretap channel with $h_{d_2,u}^2 P + 1$ as the variance of the effective noise at d_2, which implies that $D_{s,\Sigma} = 1$. The same argument can be applied to $|G_2| \geq 1$.

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

By our assumption, the definition of the setting A_2 is $A_2 \cap A_1^c$, which is $|G_1| = 1$ and $|G_2| = |G_3| = 0$. First of all, note that $|G_2| = |G_3| = 0$ implies $|G_1| \geq 1$ due to the existence of P_{s_i,d_i}. Furthermore, if $|G_1| = 1$ and $|G_2| = |G_3| = 0$, this indicates that $V_{r-1} = G_1 = \{u\}$ and both edges (u, d_1) and (u, d_2) exist. Then, the signals observed at d_1 and d_2 are the same except a constant factor and additive Gaussian noises, which implies that $D_{s,\Sigma}$ must be 0.

C. Sub-case A_3: $D_{s,\Sigma} = 1$ if $|G_1| \geq 2$ and there exist two distinct nodes $u_1, u_2 \in G_1$, $s_i \rightsquigarrow u_1$ and $s_i \rightsquigarrow u_2$ for $i = 1$ or 2.

First, note that the combined conditions $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$ imply that the source nodes s_1 and s_2 do not belong to the layer V_{r-1}, i.e, $V_1 \neq V_{r-1}$ and $r \geq 3$; otherwise, this is not case A. The achievable scheme is based on interference neutralization [20]:

- For a fixed i, the source node s_i sends the message signal to its destination.

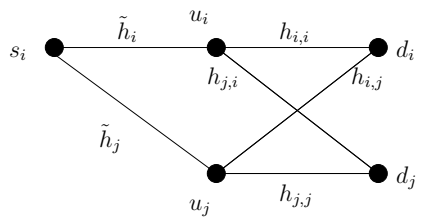

Fig. 2. The condensed network for $s_i \rightsquigarrow u_1$ and $s_i \rightsquigarrow u_2$.

- 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.

We construct the condensed network [1] with three key layers as shown in Fig. 2. Then, the end-to-end transfer matrix $\mathbf{T} = [T_i, T_j]^T$ from s_i to d_i, d_j satisfies

$$\begin{aligned}\begin{pmatrix} Y_{d_i} \\ Y_{d_j} \end{pmatrix} &= \mathbf{T} X_{s_i} + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_i \tilde{h}_i h_{i,i} + \alpha_j \tilde{h}_j h_{i,j} \\ \alpha_i \tilde{h}_i h_{j,i} + \alpha_j \tilde{h}_j h_{j,j} \end{pmatrix} X_{s_i} + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix}\end{aligned} \tag{12}$$

where $\tilde{N}_1$ and $\tilde{N}_2$ are effective dependent noises with finite variances. They are independent of the message signal.

We simply choose $\alpha_i = 1$ and $\alpha_j = -(\tilde{h}_i h_{j,i})/(\tilde{h}_j h_{j,j})$. Then, $T_j = 0$, which indicates that the observation $Y_{d_j}^n$ at d_j and W_i are independent, which means $I(W_i; Y_{d_j}^n) = 0$, i.e., the message W_i is secure.

Meanwhile, the probability that d_i can *decode* W_i with arbitrarily small probability of error is

$$P\left(T_i \neq 0\right) = P\left(h_{j,j} h_{i,i} - h_{i,j} h_{j,i} \neq 0\right) = 1 \tag{13}$$

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 $w \rightsquigarrow u_2$.

For this setting, we propose the following achievable scheme:

- For a fixed i, the source node s_i sends the message signal to $u \in G_1$. All the nodes on the path $P_{s_i,u}$ relay the signal.
- u encodes the message according to a wiretap codebook and sends the codeword to d_i.
- The special node w sends pure Gaussian random noise with average power aP to jam the 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 output signals satisfy the power constraint. a depends on the network topology, but not on the 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.

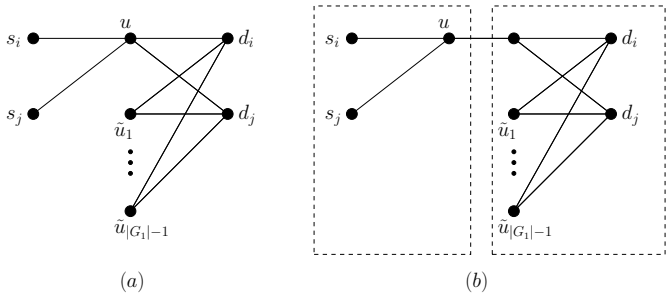

Fig. 3. The condensed network for the sub-case A_5.

- All other nodes including s_j do not send/relay signals.

The idea here 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. Then, the last hop of this condensed network is equivalent to the two-pair one-sided additive interference channel with dependent finite variance noise. Since the noises are independent of the input signals, based on the fact that the secrecy capacity depends only on the marginal distribution of X_i, Y_i and X_i, Y_j, we conclude that the sum secure d.o.f. is $D_{s,\Sigma} = 1$.

E. Sub-case A_5: $D_{s,\Sigma}$ can only be countably many positive values for all other settings in case A.

In this last sub-case of case A, it is known that

- $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$, which implies that the total number of the layers $r \geq 3$.
- For each node $w \in \cup_{i=1}^{r-2} V_i$, there exists at most one $u_w \in G_1$ such that $w \rightsquigarrow u_w$.

We claim that for this setting the sum secure d.o.f. could only be a strictly positive function of the value $|G_1|$. Therefore, $D_{s,\Sigma}$ can only take at most countably many possible values.

It is easy to prove that $u_i = u_j$. We denote $u \stackrel{\triangle}{=} u_i = u_j$. Then, for each other node $\tilde{u} \in G_1, \tilde{u} \neq u$, we have $s_i \not\rightsquigarrow \tilde{u}$, $s_j \not\rightsquigarrow \tilde{u}$. Besides, these $\tilde{u}$'s can only send independent signals because for each node $w \in \cup_{i=1}^{r-2} V_i$ there exists at most one $u_w \in G_1$ such that $w \rightsquigarrow u_w$.

The condensed network is shown in Fig. $3(a)$. Due to the Markov chain $W_i, W_j \rightarrow Y_u^n \rightarrow Y_{d_i}^n, Y_{d_j}^n$, the node u can decode the messages W_i and W_j with arbitrarily small probability of error, which implies that $D_{s,\Sigma} \leq 1$ in the first dashed box of Fig. $3(b)$. The bottleneck is the second box, which is a brodcast channel with confidential messages and M *independent helpers*. Here $M = |G_1| - 1$. We denote the sum secure d.o.f. capacity of this channel as $f'(M)$. We claim that the $D_{s,\Sigma}$ of the original network is $f(M) \stackrel{\triangle}{=} \min\{f'(M), 1\}$. The converse is straight-forward. The achievability of the first box is done by time-sharing.

Finding the function $f(M)$ is an open problem. However, we know its following properties:

1) $f(M) \leq 1$ for all M by definition.
2) $0 < f(1) \leq \frac{2}{3}$ due to [21], [22].
3) $f(M+1) \geq f(M)$ for any M. This is because the $D_{s,\Sigma}$ is potentially larger with one more interferer helper.

TABLE I
CASE A'

Sub-case	$D_{s,\Sigma}$	Condition
A'_1	1	A_1
A'_2	0	$A_2 \cap A_1^C$
A^*	$g(0)$	$V_1 = V_{r-1}$, i.e., $r = 2$
A'_3	1	$r \geq 3$ and $A_3 \cap A_2^C \cap A_1^C$
A'_4	1	$r \geq 3$ $A_4 \cap A_3^C \cap A_2^C \cap A_1^C$

Therefore, for networks in sub-case A_5 of case A, $D_{s,\Sigma}$ is a positive function of $|G_1|$. And, $D_{s,\Sigma}$ can only take at most countably many values.

IV. Sum Secure D.O.F. for Case A'

We use the same ideas presented in Section III to analyze the networks in case A'. The results are shown in Table I. However, there are two differences between case A and A'.

In contrast to case A, for case A', we cannot conclude that $r \geq 3$ if $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$. If $r = 2$, this layered network is a two-pair two-sided Gaussian interference channel with confidential messages. The sum secure d.o.f. of this network is an open problem, and is denoted as $g(0)$.

The other difference is that, if $r \geq 3$ and none of the conditions A_1, A_2, A_3 and A_4 is satisfied, then there are two scenarios. If there exists node $u \in G_1$ such that $s_1 \rightsquigarrow u$ and $s_2 \rightsquigarrow u$, we use the f function to characterize the sum secure d.o.f. If such a node does not exist, which means s_i and s_j "connect" to different nodes in V_{r-1}, then we have to define a new function g, which also takes at most countably many values.

V. Sum Secure D.O.F. for Cases B and B'

As proved in [1], for all the networks belonging to cases B and B', we could either use a simple amplify-and-forward scheme to make the end-to-end transfer matrix diagonal with non-zero diagonal entries, i.e.,

$$\begin{bmatrix} Y_{d_1} \\ Y_{d_2} \end{bmatrix} = \begin{bmatrix} \beta_1 & 0 \\ 0 & \beta_2 \end{bmatrix} \begin{bmatrix} X_{s_1} \\ X_{s_2} \end{bmatrix} + \begin{bmatrix} N_1^{eff} \\ N_2^{eff} \end{bmatrix} \tag{14}$$

or find a $2 \times 2 \times 2$ condensed interference sub-network in the original layered network.

For the diagonal end-to-end transfer matrix, the operations of the nodes in the middle layers are either performing amplify-and-forward or keeping silent, so the effective noises are independent of the input signals, and there is no information leakage from the source node to the unintended destination even when the effective noises N_i^{eff}, $i = 1$ or 2, at d_i are dependent. By interference neutralization, for this class of networks, the sum secure d.o.f. is 2.

The $2 \times 2 \times 2$ interference channel is a cascade of two fully connected one-hop interference channels. Reference [19] employed interference neutralization and real interference alignment to achieve 2 sum d.o.f. We use the same idea to design the auxiliary random variables for the $2 \times 2 \times 2$

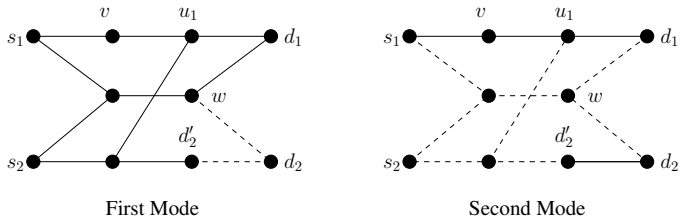

Fig. 4. The condensed network for a special class of the case C. The solid lines mean that signals are intended to be transmitted via that edge in that mode. Dashed lines mean that the edge is not used in that mode.

interference channel, construct the channel inputs, and show that it can asymptotically achieve 2 sum secure d.o.f. Based on this result, for the $2\times2\times2$ condensed interference sub-network in the original layered network, we simply treat all nodes except the nodes belonging to the sub-network as silent nodes and utilize the same achievable scheme. Note that although the equivalent interference sub-network has dependent noise 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 the reliability and security.

Therefore, in both cases, the upper bound 2 is achievable, i.e., $D_{s,\Sigma} = 2$.

VI. Sum Secure D.O.F. for Case C

The converse for this case is $D_{s,\Sigma} \leq D_{\Sigma} \leq \frac{3}{2}$ from [1]. The achievability without secrecy constant is given in [1].

We need to modify the achievable scheme to derive a secrecy rate. To this end, we demonstrate our steps in Fig. 4. In the first mode, the source pair (s_1, s_2) transmits (W_1, W_2) to destination (d_1, d_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' securely by amplify-and-forward. In the second mode, s_1 transmits a new message W_1' to d_1 and d_2' forwards the message W_2 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, d_2 can receive a mixed signal from w, which contains both W_1 and W_2. Note that in this condensed network the noises at each node are dependent, but have finite variances. To transmit message W_1 securely to d_1 against d_2 in the first mode: 1) Node d_2' sends pure Gaussian noise with average power P to jam the unintended receiver d_2. Signals from s_2 via different paths are canceled at d_1 due to the amplify-and-forward scheme. 2) Since the secrecy capacity depends only on the marginal distribution of $X_{s_1}, Y_{d_1}, Y_{d_2}$, with the help of jamming from d_2', we can always design a wiretap code achieving 1 secure d.o.f. for the condensed wiretap channel even when the effective noises at d_1 and d_2 are dependent.

VII. Conclusion

In this paper, we studied the sum secure degrees of freedom of two-unicast layered wireless networks. We used the setting in [1], i.e., cases A, A', B, B' and C, to explore all possible values of sum secure d.o.f. The major challenge is the cases A and A' due to the fact that both destination nodes may decode the messages. To overcome this problem, we classified layered wireless networks into more detailed sub-cases and in almost all the sub-cases utilized the techniques of cooperative jamming and interference neutralization to design an achievable scheme. There is still a scenario where the result is unknown. We provided the simplest equivalent channel models whose sum secure d.o.f. give these values. In all other cases, we proposed modified schemes to achieve 2 sum secure d.o.f. for cases B and B', and $3/2$ sum secure d.o.f. for case C.

References

[1] I. Shomorony and A. S. Avestimehr. Sum degrees of freedom of two-unicast wireless networks. *IEEE ISIT*, 2011.

[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, 1982.

[3] A. B. Carleial. A case where interference does not reduce capacity. *IEEE Trans. Inf. Theory*, 21(5):569–570, 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, 1978.

[5] H. Sato. The capacity of the Gaussian interference channel under strong interference. *IEEE Trans. Inf. Theory*, 27(6):786–788, 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, 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), 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. Submitted to *IEEE Trans. Inf. Theory*, Aug. 2009. Also available at [arXiv:0908.1208].

[10] A. Host-Madsen and A. Nosratinia. The multiplexing gain of wireless networks. *IEEE ISIT*, 2005.

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

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

[13] 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, 2008.

[14] Z. Li, R. D. Yates, and W. Trappe. Secrecy capacity region of a class of one-sided interference channel. *IEEE ISIT*, 2008.

[15] C. C. Wang and N. B. Shroff. Beyond the butterfly - a graph-theoretic characterization of the feasibility of network coding with two simple unicast sessions. *IEEE ISIT*, 2007.

[16] S. Shenvi and B. K. Dey. A simple necessary and sufficient condition for the double unicast problem. *IEEE ICC*, 2010.

[17] K. Cai, K. B. Letaief, P. Fan, and R. Feng. On the solvability of 2-pair unicast networks — a cut-based characterization. Available at [arXiv:1007.0465v1].

[18] 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), June 2008.

[19] 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. Also available at [arXiv:1012.2350].

[20] 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, IL*, 2008.

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

[22] X. He. Cooperation and information theoretic security in wireless networks. Ph.D. dissertation, Dept. Electrical Engineering, the Pennsylvania State University, 2010.