On Secure Capacity of Multiple Unicast Traffic over Separable Networks

Gaurav Kumar Agarwal*, Martina Cardone†, Christina Fragouli*
* UCLA, CA 90095, USA, Email: {gauravagarwal, christina.fragouli}@ucla.edu
† University of Minnesota, Minneapolis, MN 55404, USA, Email: cardo089@umn.edu

***Abstract*—This paper studies the problem of information theoretic secure communication when a source has private messages to transmit to m destinations, in the presence of a passive adversary who eavesdrops an unknown set of k edges. The information theoretic secure capacity is derived over unit-edge capacity separable networks, for the cases when $k = 1$ and m is arbitrary, or $m = 3$ and k is arbitrary. This is achieved by first showing that there exists a secure polynomial-time code construction that matches an outer bound over two-layer networks, followed by a deterministic mapping between two-layer and arbitrary separable networks.**

I. Introduction

Today, a large portion of exchanged data over communication networks is inherently *sensitive and private* (e.g., banking, professional, health). Moreover, given the recent progress in quantum computing, we can no longer exclusively rely on computational security: we need to explore unconditionally (information theoretic) secure schemes. In this paper, we present new results for information theoretic security over networks with multiple unicast sessions.

We assume that a source has m private messages to send to m destinations over a network modeled as a directed graph with unit capacity edges. This communication occurs in the presence of a passive external adversary who has unbounded computational capabilities (e.g., quantum computer), but limited network presence, i.e., she can wiretap (an unknown set of) at most k edges of her choice. We seek to characterize the information theoretic secure capacity for this setup.

Our results apply to the class of *separable* networks that, broadly speaking, are networks that can be partitioned into a number of edge disjoint subnetworks that satisfy certain properties (see Definition 3). We establish a direct mapping between the secure capacity for separable networks, and the secure capacity for two-layer networks constructed as follows. The source is connected to a set of relays via direct edges. These relays are then connected to the m destinations, such that each destination is directly connected to an (arbitrary) subset of the relays. An example of such a two-layer network with 6 relays and 3 destinations is shown in Fig. 1.

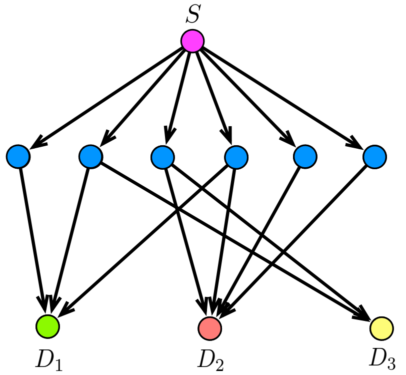

Fig. 1: Example of a two-layer network. For $k = 1$, the joint scheme achieves the rate triple $(2, 2, 1)$. This rate triple cannot be achieved by spatially separating the transmissions of the keys and the encoded messages.

In [1], we characterized the secure capacity region for separable networks having $m = 2$ destinations, and we derived an outer bound on the secure capacity region for networks having an arbitrary number of destinations m. We showed that for $m = 2$ it is optimal to use different parts of the network to transmit the keys and the encoded messages. However, as we also pointed out in [2], such a scheme is not optimal when $m > 2$. We proved this by constructing a joint scheme for two-layer networks that mixes the transmission of keys and encoded messages over the network, and showing that it can achieve higher secure rates than spatially separating the transmissions of the keys and the encoded messages. For instance in Fig. 1, the joint scheme achieves the rate triple $(2, 2, 1)$, which is not possible otherwise.

In this paper, we prove that we can leverage the polynomial-time joint scheme in [2] for two-layer networks, to prove capacity results for separable networks for the following additional cases: (i) networks where $m = 3$ and k is arbitrary; (ii) networks where $k = 1$ and m is arbitrary; (iii) networks where k and m are arbitrary, but the network has some special structure in terms of minimum cut. To prove optimality in these new cases, we need new proof techniques, that include calculating the dimension of the sum of $m = 3$ subspaces in a form that matches a modified outer bound. We also prove that the secure capacity region of any separable network can be characterized from the secure capacity region of the corresponding two-layer network, referred to as the child two-layer network. In particular, we provide a deterministic mapping from a secure scheme for the child two-layer network to a secure scheme for the corresponding separable network. We note that for $m = 2$ every network is separable [1]; however this is no longer the case for $m \geq 3$ [2].

The work was partially supported by NSF grant 1740047 and UC-NL grant LFR-18-548554.

978-1-5386-6900-6/19/$31.00 ©2019 IEEE

Related Work. Shannon [3] proved that the one-time pad can provide perfect information theoretic security with pre-shared keys. For degraded point-to-point channels, Wyner [4] showed that information theoretic security can be achieved without pre-shared keys. With feedback, Maurer [5] proved that secure communication is possible, even when the adversary has a channel of better quality than the legitimate receiver. Multicast traffic over networks of unit capacity edges was analyzed by Cai et al. in [6], and followed by several other works, such as [7], [8]. In [6], the information theoretic secure capacity was characterized for networks where a source multicasts the same information to a number of destinations in the presence of a passive external adversary eavesdropping any k edges of her choice. In [9], the authors studied adaptive and active attacks and also considered multiple multicast traffic over a layered network structure, with arbitrary number of layers. However, different to this paper, every node in one layer is connected to every node in the next layer. It therefore follows that, for the case of two layers, our setting encompasses the one in [9].

Paper Organization. In Section II we define two-layer and separable networks, and formulate the problem. In Section III, we review the secure scheme proposed in [2] and in Section IV, we characterize its achieved rate region. In Section IV we also show the mapping between separable and two-layer networks. In Section V and Section VI, we prove that the scheme achieves the secure capacity when $k = 1$ and $m = 3$, respectively. In Section VI, we also provide sufficient conditions for the scheme to be optimal for arbitrary k and m.

II. System Model and Problem Formulation

Notation: Calligraphic letters indicate sets; $\emptyset$ is the empty set; $\mathcal{A}_1 \sqcup \mathcal{A}_2$ indicates the disjoint union of $\mathcal{A}_1$ and $\mathcal{A}_2$; $\mathcal{A}_1 \backslash \mathcal{A}_2$ is $\mathcal{A}_1 \cap \mathcal{A}_2^C$; $[n] := \{1, 2, \ldots, n\}$; $[x]^+ := \max\{0, x\}$ for $x \in \mathbb{R}$.

A two-layer network consists of one source S that wishes to communicate with m destinations, by hopping information through one layer of t relays. As such, a two-layer network is parameterized by: (i) the integer t, which denotes the number of relays in the first layer; (ii) the integer m, which indicates the number of destinations in the second layer; (iii) m sets $\mathcal{M}_i,\ i \in [m]$, such that $\mathcal{M}_i \subseteq [t]$, where $\mathcal{M}_i$ contains the indexes of the relays connected to destination D_i. An example of a two-layer network is shown in Fig. 1, for which $t = 6$, $m = 3$, $\mathcal{M}_1 = \{1, 2, 4\}$, $\mathcal{M}_2 = \{3, 4, 5, 6\}$ and $\mathcal{M}_3 = \{2, 3\}$.

We represent a two-layer wireline network with a directed acyclic graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of edges. The edges represent orthogonal and interference-free communication links, which are discrete noiseless memoryless channels of unit capacity over a common alphabet. If an edge $e \in \mathcal{E}$ connects a node i to a node j, we denote, tail$(e) = i$ and head$(e) = j$. $\mathcal{I}(v)$ and $\mathcal{O}(v)$ are the set of all incoming and outgoing edges of node v, respectively.

Source S has a message W_i for destination $D_i, i \in [m]$. These m messages are assumed to be independent. Thus, the network consists of multiple unicast traffic, where m unicast sessions take place simultaneously and share the network resources. A passive external eavesdropper Eve is also present and can wiretap any k edges of her choice. The symbol transmitted over n channel uses on $e \in \mathcal{E}$ is denoted as X_e^n. In addition, for $\mathcal{E}_t \subseteq \mathcal{E}$ we define $X_{\mathcal{E}_t}^n = \{X_e^n : e \in \mathcal{E}_t\}$. We assume that S has infinite sources of randomness Θ, while the other nodes in the network do not have any randomness.

Over this network, we seek to reliably communicate (with zero error) the message $W_i, i \in [m]$ to destination D_i so that Eve receives no information about the content of the messages. In particular, we are interested in ensuring perfect information theoretic secure communication, and we aim at characterizing the secure capacity region, which is next formally defined.

Definition 1 (Secure Capacity Region)**.** *A rate m-tuple $(R_1, R_2, \ldots, R_m)$ is said to be securely achievable if there exist a block length n with $R_i = \frac{1}{n} H(W_i)$, $\forall i \in [m]$ and encoding functions $f_e, \forall e \in \mathcal{E}$, over a finite field $\mathbb{F}_q$ with*

$$X_e^n = \begin{cases} f_e\left(W_{[m]}, \Theta\right) & \text{if } tail(e) = S, \\ f_e\left(\{X_\ell^n : \ell \in \mathcal{I}(tail(e))\}\right) & \text{otherwise}, \end{cases}$$

such that each destination D_i can reliably decode the message W_i i.e., $H\left(W_i | \{X_e^n : e \in \mathcal{I}(D_i)\}\right) = 0,\ \forall i \in [m]$.

*We also require perfect secrecy, i.e., $I\left(W_{[m]}; X_{\mathcal{E}_\mathcal{Z}}^n\right) = 0,\ \forall\ \mathcal{E}_\mathcal{Z} \subseteq \mathcal{E}$ such that $|\mathcal{E}_\mathcal{Z}| \leq k$. The **secure capacity region** is the closure of all such feasible rate m-tuples.*

In order to prove that our designed scheme meets the perfect secrecy requirement in Definition 1, we will use the "matrix rank" condition on perfect secrecy proved in [10, Lemma 3.1].

We now provide a couple of definitions that will be used in the remaining part of the paper, and we state a remark that highlights some properties of the networks of interest.

Definition 2 (Min-Cut)**.** *We denote by $M_\mathcal{A}$ the capacity of the min-cut between the source S and the set of destinations $D_\mathcal{A} := \{D_i,\ i \in \mathcal{A}\}$, and refer to it as the min-cut capacity.*

Definition 3 (Separable Graph)**.** *A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with a source and m destinations is said to be **separable** if it can be partitioned into $2^m - 1$ edge disjoint graphs (graphs with empty edge sets are also allowed). In particular, these graphs are denoted as $\mathcal{G}'_\mathcal{J} = (\mathcal{V}, \mathcal{E}'_\mathcal{J}), \mathcal{J} \subseteq [m], \mathcal{J} \neq \emptyset$ and are such that $\mathcal{E}'_\mathcal{J} \subseteq \mathcal{E}$ and $\mathcal{E}'_\mathcal{J} \cap \mathcal{E}'_\mathcal{L} = \emptyset,\ \forall \mathcal{J} \neq \mathcal{L} \subseteq [m]$. Moreover, their min-cut capacities satisfy the following condition*

$$M_\mathcal{A} = \sum_{\substack{\mathcal{J} \subseteq [m] \\ \mathcal{J} \cap \mathcal{A} \neq \emptyset}} M'_\mathcal{J},\ \forall \mathcal{A} \subseteq [m], \tag{1}$$

where, for $\mathcal{G}$, $M_\mathcal{A}$ is defined in Definition 2, and the graph $\mathcal{G}'_\mathcal{J}$ has the following min-cut capacities: (i) $M'_\mathcal{J}$ from the source S to any non-empty subset of destinations in $\mathcal{J}$, and (ii) zero from the source S to the set of destinations $\{D_i : i \in [m] \backslash \mathcal{J}\}$ (see Figure 1 in [2] for an illustration).

Remark 1. *For two-layer networks, we have $M_\mathcal{A} = |\cup_{i \in \mathcal{A}} \mathcal{M}_i|$. For notational convenience, we let $M_{\cap\{i,j\}} = |\mathcal{M}_i \cap \mathcal{M}_j|$ and $M_{\cap\{i,\mathcal{A}\}} = |\mathcal{M}_i \cap (\cup_{j \in \mathcal{A}} \mathcal{M}_j)|$. Moreover, we also assume that $M_{\{i\}} > k, \forall i \in [m]$ (otherwise secure communication is not possible) with $M_\emptyset := k$ for consistency.*

III. Secure Transmission Scheme

We here review the secure polynomial-time scheme for two-layer networks that we recently proposed in [2]. The source S encodes the message packets with k random packets and transmits these packets on its outgoing edges to the t relays. We can write the received symbols at the t relays as

$$\begin{bmatrix} X_1 \\ \vdots \\ X_t \end{bmatrix} = \left[\begin{array}{c|c} \quad M \quad & \quad V \quad \end{array} \right] \begin{bmatrix} W_1 \\ \vdots \\ W_m \\ K \end{bmatrix}, \qquad (2)$$

where: (i) $W_i, i \in [m]$ is a column vector of R_i message packets for destination D_i, (ii) K is a column vector which contains the k random packets, (iii) M is a matrix of dimension $t \times (\sum_{i=1}^{m} R_i)$ (the matrix M is constructed so that all the destinations correctly decode their intended message), and (iv) V is a Vandermonde matrix of size $t \times k$, chosen to guarantee security as per [10, Lemma 3.1]; hence, Eve learns nothing about the messages $W_{[m]}$ by eavesdropping any k edges.

Each relay $i \in [t]$ forwards the received symbol X_i in (2) to the destinations it is connected. As such, each destination will observe a subset of symbols from $\{X_1, X_2, \ldots, X_t\}$. Finally, destination $D_i, i \in [m]$ selects R_i decoding vectors and performs the inner product with $[X_1, X_2, \ldots, X_t]$. The decoding vectors are chosen such that: (1) they are in the left null space of V, i.e., in the right null space of V^T; this ensures that each destination is able to cancel out the random packets (encoded with the message packets); (2) they have zeros in the positions corresponding to the relays D_i is not connected to; this ensures that each destination uses only the symbols that it observes. In other words, all the decoding vectors that D_i can choose belong to the null space of the matrix V_i defined as

$$V_i^T = \begin{bmatrix} V & C_i^T \end{bmatrix}, \qquad (3)$$

where C_i is a matrix of dimension $\bar{t} \times t$, with $\bar{t}$ being the number of relays to which D_i is not connected to (see [2] for details and the construction of the matrix M). In particular, each row of C_i has all zeros except a one in the position corresponding to a relay to which D_i is not connected to. For instance, with reference to the network in Fig. 1, we have

$$C_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad C_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

IV. Achieved Secure Rate Region

In this section, we first derive the rate region achieved by the secure scheme in Section III, and then present the mapping between separable and two-layer networks. In particular, we have the following lemma (see proof in [11, Appendix A]).

Lemma 1. *The secure rate region achieved by the proposed scheme is given by*

$$0 \leq \textstyle\sum_{i \in \mathcal{A}} R_i \leq dim \left(\sum_{i \in \mathcal{A}} N_i \right), \ \forall \mathcal{A} \subseteq [m], \qquad (4)$$

where N_i is the right null space of the matrix V_i in (3).

A. Secure Scheme for any Separable Network

We will here first show that for any separable network, a corresponding two-layer network can be created such that both networks have the same min-cut capacities $M_{\mathcal{A}}$ for all $\mathcal{A} \subseteq [m]$. We will then show that a secure scheme designed for a two-layer network can be converted to a secure scheme on the corresponding separable network.

By Definition 3, a separable network $\mathcal{G}$ with m destinations, can be separated into $2^m - 1$ networks $\mathcal{G}'_{\mathcal{J}}, \ \mathcal{J} \subseteq [m], \mathcal{J} \neq \emptyset$ where $\mathcal{G}'_{\mathcal{J}}$ has min-cut capacity $M'_{\mathcal{J}}$ to every subset of destinations in $\mathcal{J}$. To construct the corresponding two-layer network, we use the following iterative procedure: (1) we place the source node S in layer 0 of our network, and the m destination nodes $D_i, i \in [m]$, in layer 2 of our network; (2) for each $\mathcal{J} \subseteq [m]$, we add $M'_{\mathcal{J}}$ relays in layer 1 of our network; (3) for each $\mathcal{J} \subseteq [m]$, we connect: (i) the source in layer 0 with all the added $M'_{\mathcal{J}}$ relays, and (ii) all the added $M'_{\mathcal{J}}$ relays with the destinations $D_i, i \in \mathcal{J}$ in layer 2. By following the above procedure, for each $\mathcal{A} \subseteq [m]$, the min-cut capacity in the constructed two-layer network is $M_{\mathcal{A}}$ as given in (1). As such, the new constructed two-layer network has the same min-cut capacity $M_{\mathcal{A}}$ of the corresponding separable network.

In what follows, we refer to the original separable network as *parent* separable network, and to the corresponding two-layer network as *child* two-layer network. We now show that a secure scheme designed for the child two-layer network can be converted to a secure scheme for the corresponding parent separable network. Towards this end, we assume that we have a secure scheme for the child two-layer network as described in (2), and proceed as follows. On every graph $\mathcal{G}'_{\mathcal{J}}$ in the parent separable network, we transmit (multicast) the symbols that were transmitted in the child two-layer network from the source S in layer 0 to the set of $M'_{\mathcal{J}}$ relays in layer 1 that were added when constructing the child two-layer network for $\mathcal{G}'_{\mathcal{J}}$. Note that this multicast towards all destinations $D_i, i \in \mathcal{J}$, is possible since $\mathcal{G}'_{\mathcal{J}}$ has min-cut capacity $M'_{\mathcal{J}}$. With such a strategy, at the end of the transmissions every destination in the parent separable graph still receives the same set of packets as it would have received in the child two-layer network. Thus, all the destinations can still decode their respective messages. In [11, Appendix C] we also prove that this scheme satisfies the security condition in [10, Lemma 3.1], and hence it is secure. Moreover, since the child two-layer and the parent separable networks have equal min-cut capacities, they have the same outer bound on the secure capacity region [1]. Thus, an optimal scheme on a child two-layer network results in an optimal scheme on the corresponding parent separable network.

V. Secure Capacity for $k = 1$

In this section, we consider the case when Eve wiretaps any $k = 1$ edge of her choice, and characterize the secure capacity region. In particular, we prove the following theorem.

Theorem 2. *For the two-layer network when Eve wiretaps any $k = 1$ edge of her choice, the secure capacity region is*

$$\textstyle\sum_{i \in \mathcal{A}} R_i \leq M_{\mathcal{A}} - C_{\mathcal{A}}, \ \forall \mathcal{A} \subseteq [m], \qquad (5)$$

with $C_{\mathcal{A}}$ being the number of connected components in an undirected graph where: (i) there are $|\mathcal{A}|$ nodes, i.e., one for each $i \in \mathcal{A}$; (ii) an edge between node i and node j, $\{i,j\} \in \mathcal{A}$, $i \neq j$, exists if $\mathcal{M}_i \cap \mathcal{M}_j \neq \emptyset$.

Outer Bound: The secure capacity region is contained in [1]:

$$\textstyle\sum_{i \in \mathcal{A}} R_i \leq M_{\mathcal{A}} - k, \ \forall \mathcal{A} \subseteq [m]. \tag{6}$$

We now show that the outer bound in (6) can be equivalently written as in (5). Let $\mathcal{V}_i$, $i \in [C_{\mathcal{A}}]$, represent the set of nodes in the i-th component of the graph constructed as explained in Theorem 2. Then, clearly $\mathcal{A} = \bigsqcup_{i=1}^{C_{\mathcal{A}}} \mathcal{V}_i$ and we can write

$$\begin{aligned}\textstyle\sum_{i \in \mathcal{A}} R_i &= \textstyle\sum_{j=1}^{C_{\mathcal{A}}} \left(\sum_{i \in \mathcal{V}_j} R_i \right) \overset{\text{(a)}}{\leq} \sum_{j=1}^{C_{\mathcal{A}}} \left(M_{\mathcal{V}_j} - k \right) \\ &\overset{\text{(b)}}{=} M_{\mathcal{V}_1 \cup \mathcal{V}_2 \cup \ldots \cup \mathcal{V}_{C_{\mathcal{A}}}} - kC_{\mathcal{A}} \overset{\text{(c)}}{=} M_{\mathcal{A}} - C_{\mathcal{A}},\end{aligned}$$

where: (i) the inequality in (a) follows by applying (6) for each set $\mathcal{V}_i, i \in [C_{\mathcal{A}}]$, (ii) the equality in (b) follows since, by construction, $\mathcal{M}_i \cap \mathcal{M}_j = \emptyset$ for all $i \in \mathcal{V}_x$ and $j \in \mathcal{V}_y$ with $x \neq y$, and (iii) the equality in (c) follows since $\mathcal{A} = \bigsqcup_{i=1}^{C_{\mathcal{A}}} \mathcal{V}_i$ and $k = 1$. Thus, (6) implies (5). Moreover, since $C_{\mathcal{A}} \geq 1$, (5) implies (6). This shows that the rate region in Theorem 2 is an outer bound on the secure capacity region when $k = 1$.

We now consider an example of a two-layer network and show how the upper bound derived above applies to it.

Example: Let $\mathcal{A} = \{2,3,4\}$, and assume that $\mathcal{M}_1 = \{1,2\}$, $\mathcal{M}_2 = \{3,4\}$, $\mathcal{M}_3 = \{4,5,6\}$ and $\mathcal{M}_4 = \{7,8\}$. Then, we construct an undirected graph such that: (i) it has 3 nodes since $|\mathcal{A}| = 3$ and (ii) has an edge between node 2 and node 3 since $\mathcal{M}_2 \cap \mathcal{M}_3 = \{4\} \neq \emptyset$. It therefore follows that this graph has $C_{\mathcal{A}} = 2$ components. In particular, we have

$$\textstyle\sum_{i \in \mathcal{A}} R_i = \sum_{i \in \mathcal{V}_1} R_i + \sum_{i \in \mathcal{V}_2} R_i \leq M_{\{2,3,4\}} - 2 = 4, \tag{7}$$

where $\mathcal{V}_1 = \{2,3\}$ and $\mathcal{V}_2 = \{4\}$.

Achievable Rate Region: We here show that the rate region in Theorem 2 is achieved by the scheme described in Section III. In particular, we show

$$\begin{aligned} M_{\mathcal{A}} - C_{\mathcal{A}} \leq \dim \left(\textstyle\sum_{i \in \mathcal{A}} N_i \right) &\overset{\text{(a)}}{=} \dim \left(\left(\cap_{i \in \mathcal{A}} V_i \right)^{\perp} \right) \\ &= t - \dim \left(\cap_{i \in \mathcal{A}} V_i \right), \end{aligned}$$

where recall that $\dim \left(\sum_{i \in \mathcal{A}} N_i \right)$ is the secure rate performance of our proposed scheme in Section III (see Lemma 1). Note that the equality in (a) follows by using the property of the dual space and the rank nullity theorem, and $V_i, i \in \mathcal{A}$ is defined in (3). In other words, we next show that

$$\forall \mathcal{A} \subseteq [m], \ \dim \left(\cap_{i \in \mathcal{A}} V_i \right) \leq t - M_{\mathcal{A}} + C_{\mathcal{A}}. \tag{8}$$

Towards this end, we would like to count the number of linearly independent vectors $x \in \mathbb{F}_q^t$ that belong to $(\cap_{i \in \mathcal{A}} V_i)$.

We note that, by our construction: (i) V^T consists of one row of t ones, and (ii) C_i has zeros in the positions indexed by $\mathcal{M}_i$. Hence, if a vector belongs to V_i, then all its components indexed by $\mathcal{M}_i$ have to be the same, i.e., either they are all zeros, or they are all equal to a multiple of one. Thus, we have q choices to fill these positions indexed by $\mathcal{M}_i$.

Now, consider V_j with $j \in \mathcal{A}$ and $j \neq i$. By using the same logic as above, if a vector belongs to V_j, then all its components indexed by $\mathcal{M}_j$ have to be the same and we have q choices to fill these. We now need to count the number of such choices that are consistent with the choices made to fill the positions indexed by $\mathcal{M}_i$.

Towards this end, we consider two cases:

- **Case 1:** $\mathcal{M}_i \cap \mathcal{M}_j = \emptyset$. In this case, there is no overlap in the elements indexed by $\mathcal{M}_i$ and $\mathcal{M}_j$ and hence we can use all the available q choices to fill the positions indexed by $\mathcal{M}_j$;
- **Case 2:** $\mathcal{M}_i \cap \mathcal{M}_j \neq \emptyset$. There is an overlap in the elements indexed by $\mathcal{M}_i$ and $\mathcal{M}_j$. Since we have already fixed the elements indexed by $\mathcal{M}_i$, there is no choice for the elements indexed by $\mathcal{M}_j$ (as all the elements have to be the same).

By iterating the same reasoning as above for all $i \in \mathcal{A}$, we conclude that we can fill all the positions indexed by $\cup_{i \in \mathcal{A}} \mathcal{M}_i$ of a vector $x \in \mathbb{F}_q^t$ and make sure that $x \in (\cap_{i \in \mathcal{A}} V_i)$ in $q^{C_{\mathcal{A}}}$ ways. This is because, there are $C_{\mathcal{A}}$ connected components, and for each of these components we have only q choices to fill the corresponding positions in the vector x (i.e., the positions that correspond to the relays to which at least one of the destinations inside that component is connected). Once we fix any position inside a component, in fact all the other positions inside that component have to be the same, and thus we have no more freedom in choosing the other positions. Moreover, the remaining $t - M_{\mathcal{A}}$ positions of x can be filled with any value in $\mathbb{F}_q$ and for this we have $q^{t-M_{\mathcal{A}}}$ possible choices. Therefore, the number of vectors $x \in \mathbb{F}_q^t$ that belong to $(\cap_{i \in \mathcal{A}} V_i)$ is at most $q^{C_{\mathcal{A}}+t-M_{\mathcal{A}}}$, which implies $\forall \mathcal{A} \subseteq [m], \ \dim (\cap_{i \in \mathcal{A}} V_i) \leq t - M_{\mathcal{A}} + C_{\mathcal{A}}$. This proves that the secure scheme in Section III achieves the rate region in Theorem 2. We now illustrate our method of identifying vectors that belong to $\cap_{i \in \mathcal{A}} V_i$ through an example.

Example: Let $t = 8$, $m = 4$, $\mathcal{M}_1 = \{1,2\}$, $\mathcal{M}_2 = \{3,4\}$, $\mathcal{M}_3 = \{4,5,6\}$ and $\mathcal{M}_4 = \{7,8\}$. Let $\mathcal{A} = \{2,3,4\}$.

We want to count the number of vectors $x \in \mathbb{F}_q^8$ such that $x \in V_2 \cap V_3 \cap V_4$. We use the following iterative procedure:

- For x to belong to V_2 its elements in the 3rd and 4th positions have to be the same since $\mathcal{M}_2 = \{3,4\}$. Thus, we have q choices to fill the 3rd and 4th positions.
- For x to belong to V_3, its elements in the 4th, 5th and 6th positions have to be equal since $\mathcal{M}_3 = \{4,5,6\}$. However, the element in the 4th position has already been fixed in selecting vectors that belong to V_2. Thus, there is no further choice in filling the 5th and 6th positions.
- For x to belong to V_4, its elements in the 7th and 8th positions have to be the same since $\mathcal{M}_4 = \{7,8\}$. Since in the previous two steps, we have not filled yet the elements in these positions, then we have q possible ways to fill the elements in the 7th and 8th positions.
- Moreover, we can fill the elements in the 1st and 2nd positions of x in q^2 possible ways.

With the above procedure we get that $\dim \left(\cap_{i \in \{2,3,4\}} V_i \right) = 4$, which is equal to the upper bound that we computed in (7) for the same example.

VI. Secure Capacity For $m = 3$

In this section, we consider the case $m = 3$, and we characterize the secure capacity region through the theorem below.

Theorem 3. *For a two-layer network with $m = 3$ destinations, the secure capacity region is given by*

$$\textstyle\sum_{i\in\mathcal{A}} R_i \leq M_{\mathcal{A}} - k, \ \forall \mathcal{A} \subseteq [m]. \tag{9}$$

Clearly the rate region in (9) is an outer bound on the secure capacity region [1] and can be equivalently written as

$$\textstyle\sum_{i\in\mathcal{A}} R_i \leq \min_{\mathcal{P}\,:\,\bigsqcup\limits_{\mathcal{Q}\in\mathcal{P}} \mathcal{Q}=\mathcal{A}} \left\{ \sum\limits_{\mathcal{Q}\in\mathcal{P}} M_{\mathcal{Q}} - |\mathcal{P}|k \right\}, \ \forall \mathcal{A} \subseteq [m],$$

where $\mathcal{P}$ is a partition of $\mathcal{A}$. We will show that $\forall \mathcal{A} \subseteq [m]$,

$$\dim\left(\textstyle\sum_{i\in\mathcal{A}} N_i\right) \geq \min_{\mathcal{P}\,:\,\bigsqcup\limits_{\mathcal{Q}\in\mathcal{P}} \mathcal{Q}=\mathcal{A}} \left\{ \sum\limits_{\mathcal{Q}\in\mathcal{P}} M_{\mathcal{Q}} - |\mathcal{P}|k \right\}. \tag{10}$$

We prove (10) by considering three different cases.

Case 1: $|\mathcal{A}| = 1$, i.e., $\mathcal{A} = \{i\}, \forall i \in [3]$. For this case, V_i in (3) has $k + t - M_{\{i\}}$ rows. All these rows are linearly independent since: (i) the rows of V^T are linearly independent as V is a Vandermonde matrix, (ii) C_i is full row rank by construction, and (iii) any linear combination of the rows of V^T will have a weight of at least $t - k + 1$ (from the Vandermonde property), whereas any linear combination of the rows of C_i will have a weight of at most $t - M_{\{i\}} \leq t - k$. It therefore follows that, $\forall i \in [3]$, we have that $\dim(N_i) = t - \dim(V_i) = t - (k + t - M_{\{i\}}) = M_{\{i\}} - k$, where the first equality follows by using the rank-nullity theorem. Thus, (10) is satisfied.

Case 2: $|\mathcal{A}| = 2$, i.e., $\mathcal{A} = \{i, j\}$. $\forall (i, j) \in [3]^2, i \neq j$,

$$\begin{aligned} \dim(N_i + N_j) &= \dim(N_i) + \dim(N_j) - \dim(N_i \cap N_j) \\ &= M_{\{i\}} + M_{\{j\}} - 2k - \dim(N_i \cap N_j), \end{aligned} \tag{11}$$

where the second equality follows by using $\dim(N_i)$ derived in Case 1. Thus, we need to compute $\dim(N_i \cap N_j)$. Note that, by definition, $N_i \cap N_j$ is the right null space of

$$V_{ij}^{\star} = \begin{bmatrix} V_i \\ V_j \end{bmatrix} \overset{(3)}{=} \begin{bmatrix} V^T \\ C_i \\ C_j \end{bmatrix} = \begin{bmatrix} V^T \\ C_{ij} \end{bmatrix},$$

where in the last equality, C_{ij} is a matrix of dimension $(t - M_{\cap\{i,j\}}) \times t$, with all unique rows. Using a similar argument as in Case 1 the number of linearly independent rows of $V_{ij}^{\star}$ is $\min\{t, t - M_{\cap\{i,j\}} + k\}$. Thus,

$$\begin{aligned} \dim(N_i \cap N_j) &= t - \min\{t, t - M_{\cap\{i,j\}} + k\} \\ &= \max\{0, M_{\cap\{i,j\}} - k\} = [M_{\cap\{i,j\}} - k]^+, \end{aligned}$$

where the first equality follows from the rank-nullity theorem. We can now write $\dim(N_i + N_j)$ from (11) as $\dim(N_i + N_j) = \min\left\{M_{\{i\}} + M_{\{i\}} - 2k, M_{\{i,j\}} - k\right\}$, and the condition in (10) is satisfied.

Case 3: $\mathcal{A} = \{1, 2, 3\}$. We will compute

$$\dim(N_1 + N_2 + N_3) = t - \dim(V_1 \cap V_2 \cap V_3), \tag{12}$$

that is, the number of linearly independent vectors $x \in \mathbb{F}_q^t$ that belong to $V_1 \cap V_2 \cap V_3$. Similar to the case $k = 1$, we have $t - M_{\{1,2,3\}}$ degrees of freedom to fill the positions of x corresponding to $[t] \setminus \cup_{i\in[3]} \mathcal{M}_i$. We now select a permutation (i, j, ℓ) of $(1, 2, 3)$. In order for x to belong to V_i, the positions of x corresponding to $\mathcal{M}_i$ can be filled with k degrees of freedom. This is because: (i) C_i in (3) has zeros in the positions specified by $\mathcal{M}_i$, and (ii) V^T has k rows. Then, to fill the positions of x specified by $\mathcal{M}_j$ so that $x \in V_j$, we have at most $[k - M_{\cap\{i,j\}}]^+$ degrees of freedom. This is because the positions of x corresponding to $\mathcal{M}_i \cap \mathcal{M}_j$ are already fixed. Finally, to fill the positions of x corresponding to $\mathcal{M}_\ell$ so that $x \in V_\ell$, we have at most $[k - M_{\cap\{\ell,\{i,j\}\}}]^+$ degrees of freedom. This is because the positions of x corresponding to $\mathcal{M}_\ell \cap (\mathcal{M}_i \cup \mathcal{M}_j)$ are already fixed. Thus, we obtain $\dim(V_1 \cap V_2 \cap V_3) \leq k + [k - M_{\cap\{i,j\}}]^+ + [k - M_{\cap\{\ell,\{i,j\}\}}]^+ + t - M_{\{1,2,3\}}$, which when substituted in (12), satisfies (10) (see [11, Appendix B]). This proves Theorem 3.

We now conclude this section with the following lemma.

Lemma 4. *The scheme in Section III achieves the secure capacity region of a two-layer network with arbitrary values of k and m whenever $\mathcal{M}_{\cap\{i,j\}} \geq k$ for all $(i, j) \in [m]^2, i \neq j$.*

Proof. We can compute $\dim(\cap_{i=1}^m V_i)$ as follows:

$$\begin{aligned} \dim(\cap_{i\in\mathcal{A}} V_i) &\overset{\text{(a)}}{\leq} t - M_{\mathcal{A}} + k + [k - \mathcal{M}_{\cap\{i_1,i_2\}}]^+ \\ &\quad + \textstyle\sum_{j=3}^{m} [k - \mathcal{M}_{\cap\{i_j,\{i_1,i_2,\ldots,i_{j-1}\}\}}]^+ \\ &\overset{\text{(b)}}{\leq} k + t - M_{\mathcal{A}}, \end{aligned}$$

where: (a) follows by extending to arbitrary m the iterative algorithm for Case 3 above to select $x \in \cap_{i=1}^m V_m$, and (b) follows since $\mathcal{M}_{\cap\{i_j,\{i_1,i_2,\ldots,i_{j-1}\}\}} \geq \mathcal{M}_{\cap\{i_j,i_{j-1}\}} \geq k$. By using the property of the dual space and the rank-nullity theorem, we obtain $\dim(\sum_{i\in\mathcal{A}} N_i) \geq M_{\mathcal{A}} - k$, which satisfies (10) $\forall \mathcal{A} \subseteq [m]$. This proves Lemma 4. □

References

[1] G. K. Agarwal, M. Cardone, and C. Fragouli, "Secure network coding for multiple unicast: On the case of single source," in *Information Theoretic Security*, 2017, pp. 188–207.

[2] ——, "On secure network coding for multiple unicast traffic," *arXiv:1901.02787v1*, January 2019.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory,*, vol. 39, no. 3, pp. 733–742, 1993.

[6] N. Cai and R. W. Yeung, "Secure network coding," in *IEEE International Symposium on Information Theory*, 2002, p. 323.

[7] J. Feldman, T. Malkin, C. Stein, and R. Servedio, "On the capacity of secure network coding," in *42nd Annual Allerton Conference on Communication, Control, and Computing*, 2004, pp. 63–68.

[8] S. Y. El Rouayheb and E. Soljanin, "On wiretap networks II," in *IEEE International Symposium on Information Theory*, 2007, pp. 551–555.

[9] N. Cai and M. Hayashi, "Secure network code for adaptive and active attacks with no-randomness in intermediate nodes," *arXiv:1712.09035*.

[10] N. Cai and R. W. Yeung, "A security condition for multi-source linear network coding," in *2007 IEEE International Symposium on Information Theory*, June 2007, pp. 561–565.

[11] G. K. Agarwal, M. Cardone, and C. Fragouli, "On secure capacity of multiple unicast traffic over separable networks," *arXiv:1901.03216*, January 2019.