On the Secrecy Capacity of 1-2-1 Atomic Networks

Mohammad Milanian, Minoh Jeong, Martina Cardone
University of Minnesota, Minneapolis, MN 55455, USA, Email: {milanian, jeong316, mcardone}@umn.edu

2024 IEEE International Symposium on Information Theory (ISIT) | 979-8-3503-8284-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISIT57864.2024.10619394

***Abstract*—We consider the problem of secure communication over a noiseless 1-2-1 network, an abstract model introduced to capture the directivity characteristic of mmWave communications. We focus on structured networks, which we refer to as 1-2-1 atomic networks. Broadly speaking, these are characterized by a source, a destination, and three layers of intermediate nodes with sparse connections. The goal is for the source to securely communicate to the destination in the presence of an eavesdropper with unbounded computation capabilities, but limited network presence. We derive novel upper and lower bounds on the secrecy capacity of 1-2-1 atomic networks. These bounds are shown to be tighter than existing bounds in some regimes. Moreover, in such regimes, the bounds match and hence, they characterize the secrecy capacity of 1-2-1 atomic networks.**

I. Introduction

Millimeter Wave (mmWave) communication has shown a great potential in overcoming the spectrum scarcity and enabling multi-gigabit services [1], [2]. In [3], the authors introduced the so-called *1-2-1 network* model with the goal to study the information theoretic capacity of mmWave networks. This model abstracts away the physical layer component, while capturing the fundamental directivity characteristic of mmWave communication. In the 1-2-1 network model, in order to activate the communication link from node a to node b, these two nodes need to perform beamforming in a way that their beams face each other (hence, the term 1-2-1).

In this work, similarly to [4] and [5], we study secure communication over 1-2-1 networks. We consider 1-2-1 networks with lossless communication links of unitary capacity, where a source wishes to securely communicate with a destination in the presence of an eavesdropper with limited network coverage, but unbounded computation capabilities (e.g., quantum computer). In particular, the adversary can eavesdrop at most K edges of their choice. This assumption on the limited network presence is reasonable in mmWave networks since the adversary has to be physically present on a link to eavesdrop the high-directional communication over it. We assume that the source and destination have stronger beamforming capabilities than the intermediate nodes, i.e., they can transmit to (the source) and receive from (the destination) at most M nodes, whereas the intermediate nodes have only a single transmit beam and a single receive beam. We focus on a class of 1-2-1 networks, which we refer to as 1-2-1 *atomic* networks, an example of which is shown in Figure 1. Broadly speaking, these are layered networks (no communication links exist between nodes within the same layer). Our main contribution consists of: (1) deriving novel lower and upper bounds on the secrecy capacity of 1-2-1 atomic networks; and (2) providing conditions under which these match, hence characterizing the secrecy capacity in these regimes. The lower bound is obtained through the design of a transmission scheme that suitably leverages the network *multipath* to establish keys and transmit messages (encoded with the keys) between the source and the destination. A surprising result of our work is that, given the same network topology, the source may need to change the transmission strategy as K increases.

We study secure communication over 1-2-1 networks as [4] and [5]. However, our work has key distinguishing features from [4] and [5]. In [5], the 1-2-1 model analyzed is different from the 1-2-1 atomic network considered in this paper. In [4], although the derived lower and upper bounds can be applied to 1-2-1 atomic networks, they are not tight in general.

In order to ensure secrecy, we here leverage the following two aspects: (1) directivity; and (2) multipath. *Directivity* has been investigated for ensuring security in MIMO beamforming [6], [7]. The main idea of these works is to create beams that are narrow enough to significantly weaken the channel of the adversary. However, these works focus on guaranteeing secrecy over channels and not over networks, which is our goal in this paper. *Multipath* has also been leveraged for security in noiseless networks in the context of secure network coding [7–13]. The literature on (linear) secure network coding is rich, with a few examples given by [10, 14–21]. However, these works consider networks in which nodes can simultaneously communicate to all the connected nodes. Differently, in this work we have a directivity (1-2-1) constraint imposed by mmWave communication, which allows each node only to communicate with a limited number of connected nodes.

Paper organization. In Section II, we present the 1-2-1 atomic network model and we review a few existing results on the secrecy capacity of 1-2-1 networks. In Section III, we describe our main results, i.e., we derive novel upper and lower bounds on the secrecy capacity and identify regimes in which they are tight. In Section IV, we provide the proof of our main results.

Notation. For any $m \in \mathbb{N}$, we define $[m] := \{1, 2, \dots, m\}$; $[a : b]$ is the set of integers from a to $b \geq a$; $[x]^+ = \max\{0, x\}$. For a set $\mathcal{X}$, $|\mathcal{X}|$ denotes its cardinality; $\varnothing$ is the empty set. For a real number $x \in \mathbb{R}$, we denote its floor by $\lfloor x \rfloor$. We use $X_{\mathcal{S}}$ to denote $(X_j : j \in \mathcal{S})$.

II. System Model and Known Results

We consider a 1-2-1 network [3], where a source S wishes to securely communicate with a destination D. The network is modeled by a directed acyclic graph $G = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of vertices such that $(\mathsf{S}, \mathsf{D}) \in \mathcal{V}$ and $\mathcal{E}$ is the set of edges. All edges are lossless and have a fixed finite capacity, which we assume to be *unitary*, without loss of generality.

979-8-3503-8284-6/24/$31.00 ©2024 IEEE Authorized licensed use limited to: University of Minnesota. Downloaded on May 12,2025 at 21:32:47 UTC from IEEE Xplore. Restrictions apply.

An edge $e \in \mathcal{E}$ is activated according to the 1-2-1 constraint. Under this constraint, each intermediate node (i.e., each $v \in \mathcal{V}$ except for S and D) can simultaneously receive and transmit, but at each point in time it can receive from at most one incoming edge and transmit through at most one outgoing edge. For instance, with reference to Figure 1, at each point in time, node v_1 can receive from at most one among nodes a, b, c and transmit to at most one among nodes h, i, j. Differently, the source S (respectively, the destination D) can transmit to (respectively, receive from) at most $M \geq 1$ nodes.

We denote by H_e and H_v the maximum numbers of edge-disjoint and vertex-disjoint paths from S to D, respectively. Among arbitrary 1-2-1 networks, our focus in this paper is on structured networks, which we refer to as 1-2-1 *atomic* networks, as formally defined next.

Definition 1. *A 1-2-1 atomic network is one for which its underlying $G = (\mathcal{V}, \mathcal{E})$ can be partitioned into H_v atomic subgraphs*[1] *$G_i = (\mathcal{V}_i, \mathcal{E}_i)$ with $\mathcal{V}_i \subseteq \mathcal{V}$ and $\mathcal{E}_i \subseteq \mathcal{E}$ for all $i \in [H_v]$, such that the three following conditions hold:*

- *The maximum number of vertex disjoint paths (respectively, edge disjoint paths) from* S *to* D *in each G_i is equal to one (respectively, h_i);*
- *All the h_i edge disjoint paths in each G_i from* S *to* D *only share one (intermediate) node, referred to as atom v_i;*
- *Any two G_i and G_j share no nodes other than* S *and* D*, for all $i, j \in [H_v], i \neq j$.*

Throughout the paper, we will represent a 1-2-1 atomic network by a vector $\mathbf{h} = [h_1, \ldots, h_{H_v}]$, where h_i is defined in Definition 1. Figure 1 provides an example of a 1-2-1 atomic network with $H_v = 3$ and $\mathbf{h} = [3, 2, 2]$.

The communication from S to D over a 1-2-1 atomic network takes place in the presence of an *external passive adversary* who can eavesdrop any K edges of their choice (unknown to all the other nodes in the network). If the adversary eavesdrops edges in $\mathcal{Z} \subseteq \mathcal{E}, |\mathcal{Z}| = K$, we require that the communication remains secure from the adversary in the following sense,

$$I(W; T_{\mathcal{Z}}^{[n]}) \leq \varepsilon, \quad \forall \mathcal{Z} \subseteq \mathcal{E}, \ |\mathcal{Z}| = K, \tag{1}$$

where W is the message with entropy rate R that S wishes to transmit to D and $T_{\mathcal{Z}}^{[n]} = \left\{ T_e^{[n]}, e \in \mathcal{Z} \right\}$ denotes the packets transmitted over $e \in \mathcal{Z}$ in n network uses.

In this paper, we seek to characterize the secrecy capacity C_s for 1-2-1 atomic networks. This is defined as the maximum rate at which S can communicate to D with zero error, while satisfying the 1-2-1 constraints of the network and the security constraint in (1). To the best of our knowledge, the tightest bounds on C_s are given by [4],

$$\min\{M, H_v\} \frac{H_v - K}{H_v} \leq \mathsf{C}_s \leq \min\{M, H_e\} \frac{H_e - K}{H_e}. \tag{2}$$

It is worth noting that the lower and the upper bounds in (2) match when $H_e = H_v$. However, when $H_v < H_e$ we will show that, in general, neither the lower bound nor the upper bound in (2) are tight for a 1-2-1 atomic network. For instance, consider the 1-2-1 atomic network in Figure 1 for which $H_e = 7$ and $H_v = 3$. Assume that $K = 1$ and $M = 3$. From the bounds in (2), we obtain that $2 \leq \mathsf{C}_s \leq 18/7$. However, in this paper we will prove that $\mathsf{C}_s = 5/2$.

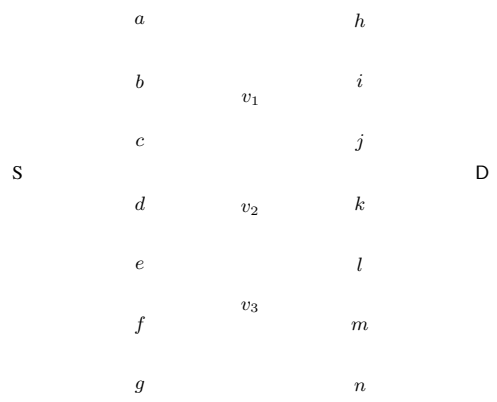

Figure 1: A 1-2-1 atomic network with $H_e = 7$ and $H_v = 3$. The $H_e = 7$ edge-disjoint paths are referred to as $p_i, i \in [7]$ from top to bottom, e.g., $p_4 = \mathsf{S} \to d \to v_2 \to k \to \mathsf{D}$.

III. Main Results

In this section, we present the main results of our work. We start by providing a lower bound on the secrecy capacity C_s of a 1-2-1 atomic network.

Theorem 1. *Define $\widehat{M} := \min(M, H_v)$ and, for all $c \in [0 : \widehat{M} - 1]$, let*

$$R(c) = \begin{bmatrix} \sum_{\eta=0}^{c} (\widehat{M} - \eta) \mathsf{P}_{\widehat{M}-\eta} - K \\ \sum_{\eta=0}^{c} \mathsf{P}_{\widehat{M}-\eta} \end{bmatrix}^{+}, \tag{3}$$

where $\mathsf{P}_{\widehat{M}-\eta} := |\mathcal{P}_{\widehat{M}-\eta}|$ with $\mathcal{P}_{\widehat{M}-\eta}, \eta \in [0 : c]$ being a set[2] *with groups of $\widehat{M} - \eta$ vertex-disjoint paths of $G \setminus \bigcup_{i=0}^{\eta-1} \mathcal{P}_{\widehat{M}-i}$. Each path can appear in at most one group.*

Then, for a 1-2-1 atomic network with K eavesdropped edges, it holds that $\mathsf{C}_s \geq R(c^\star)$ where $c^\star = \arg\max_{c \in [0:\widehat{M}-1]} R(c)$.

Proof: See Section IV-A.

Example 1. *Consider the 1-2-1 atomic network in Figure 1 with $M = 3$. Thus, $\widehat{M} = 3$. Assuming $K = 1$, we have that:*
1) *$\eta = 0 : \mathcal{P}_3 = \{\{p_1, p_4, p_6\}, \{p_2, p_5, p_7\}\}$ and hence, $\mathsf{P}_3 = 2$;*
2) *$\eta = 1 : \mathcal{P}_2 = \varnothing$ and hence, $\mathsf{P}_2 = 0$;*
3) *$\eta = 2 : \mathcal{P}_1 = \{p_3\}$ and hence, $\mathsf{P}_1 = 1$.*

By using the above inside (3)*, we obtain $R(0) = 5/2$, $R(1) = 5/2$, and $R(2) = 2$. Thus, $c^\star = 0$ and $\mathsf{C}_s \geq 5/2$.*

Remark 1. *The value of $c^\star$ in Theorem 1 for a specific 1-2-1 atomic network depends on K. For instance, assume the same setting as in Example 1, but with $K = 5$. Then, we would*

[1] Even though we refer to the G_i's as a partition of G, we assume that S and D are common to all the subgraphs.

[2] Algorithm 1 will provide the detailed construction of $\mathcal{P}_{\widehat{M}-\eta}$.

Authorized licensed use limited to: University of Minnesota. Downloaded on May 12,2025 at 21:32:47 UTC from IEEE Xplore. Restrictions apply.

obtain $R(0) = 1/2$, $R(1) = 1/2$, *and* $R(2) = 2/3$. *Thus,* $c^\star = 2$, *which is different from* $c^\star = 0$ *when* $K = 1$.

We observe that the lower bound on C_s in Theorem 1 depends on $\mathsf{P}_{\widehat{M}-\eta}, \eta \in [0:c]$. Thus, a natural question arises: Is it possible to find an expression to compute $\mathsf{P}_{\widehat{M}-\eta}, \eta \in [0:c]$? The next lemma (the proof of which is in [22, Appendix A]) will be helpful to provide an answer to this question.

Lemma 1. *Consider a 1-2-1 atomic network with underlying graph* G. *Assume, without loss of generality, that* $h_1 \geq h_2 \geq \ldots \geq h_{H_v}$. *Then, there are at least* $\mathsf{P}_\ell(h_{[H_v]})$ *groups of* ℓ *vertex-disjoint paths in* G, *where*

$$\mathsf{P}_1\left(h_{[H_v]}\right) = \sum_{i=1}^{H_v} h_i, \tag{4a}$$

and, for all $\ell \in [2:H_v]$, *it holds that*

$$\mathsf{P}_\ell\left(h_{[H_v]}\right) = \begin{cases} \mathsf{P}_{\ell-1}\left(h_{[2:H_v]}\right) & \text{if } h_1 \geq \mathsf{P}_{\ell-1}\left(h_{[2:H_v]}\right), \\ \left\lfloor \frac{\sum_{i=1}^{H_v} h_i}{\ell} \right\rfloor & \text{otherwise.} \end{cases} \tag{4b}$$

We note that Lemma 1 can be applied $\widehat{M}$ times to compute $\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_{\widehat{M}}$ in Theorem 1. In particular, to compute $\mathsf{P}_{\widehat{M}}$ Lemma 1 is applied over G; then, to compute $\mathsf{P}_{\widehat{M}-1}$ Lemma 1 is applied over $G \backslash \mathcal{P}_{\widehat{M}}$ and so on, until P_1 that can be computed by applying Lemma 1 over $G \setminus \bigcup_{i=0}^{\widehat{M}-2} \mathcal{P}_{\widehat{M}-i}$.

We now focus on deriving an upper bound on the secrecy capacity C_s of a 1-2-1 atomic network.

Theorem 2. *For a 1-2-1 atomic network with* K *eavesdropped edges, it holds that*

$$\mathsf{C}_s \leq \sum_{i=1}^{H_v} \left(1 - \frac{K_i}{h_i}\right), \tag{5a}$$

where, without loss of generality, it is assumed that $h_1 \geq h_2 \geq \ldots \geq h_{H_v}$, *and where*

$$K_i = \min\left\{h_i, K - \sum_{j=i+1}^{H_v} K_j\right\}, \ i \in [H_v]. \tag{5b}$$

Proof: See Section IV-B.

We now leverage the results in Theorem 1 and Theorem 2 to prove the following secrecy capacity result.

Theorem 3. *For a 1-2-1 atomic network with* K *eavesdropped edges and* $M \geq H_v$, *the derived achievability and converse bounds match and hence, under this condition, the secrecy capacity of the considered network is given by* (5).

Proof: See Section IV-C.

Theorem 3 provides a new secrecy capacity result for 1-2-1 networks. In particular, when $M \geq H_v$ our lower and outer bounds in Theorem 1 and Theorem 2 are tighter than those in (2). However, we next show that when $M < H_v$ the bounds in (2) may be tighter. This implies that our bounds in Theorem 1 and Theorem 2 can be further improved, and this is indeed object of current investigation.

Example 2. *Consider a 1-2-1 atomic network with* $\mathbf{h} = [2,1,1,1]$, $M = 3$ *and* $K = 1$. *From Theorem 1, we obtain* $\mathsf{C}_s \geq 2$, *whereas from* (2) *we have that* $\mathsf{C}_s \geq 9/4$. *Thus, our achievable bound in looser than the existing one from [4].*

Example 3. *Consider a 1-2-1 atomic network with* $\mathbf{h} = [4,3,2]$, $M = 2$, *and* $K = 5$. *From Theorem 2, we obtain* $\mathsf{C}_s \leq 1$, *whereas from* (2) *we have that* $\mathsf{C}_s \leq 8/9$. *Thus, our converse bound in looser than the existing one from [4].*

IV. Proof of Main Results

A. Proof of Theorem 1

We here propose a secure transmission scheme for a 1-2-1 atomic network with K eavesdropped edges and we prove that it achieves the secrecy rate in Theorem 1. The scheme consists of four phases, which are next described. The key generation and encoding phases are the same as those in [4].

1) Key generation. We generate K uniform random packets, denoted by $X_{[K]}$ and create H_e linear combinations of them by pre-multiplying $X_{[K]}$ by a maximum distance separable (MDS) code matrix V of size $H_e \times K$, i.e.,

$$f(X) = VX_{[K]}. \tag{6}$$

In what follows, we will refer to each row of $f(X)$ in (6) as a *key*. Note that any K rows of $f(X)$ are linearly independent.

2) Encoding. We take $H_e - K$ message packets $W_j, j \in [H_e - K]$ and we encode them using $f(X)$ in (6). In particular, this encoding operation is as follows,

$$T_i = \begin{cases} f_i(X) & i \in [K], \\ f_i(X) + W_{i-K} & i \in [K+1:H_e], \end{cases} \tag{7}$$

where $f_i(X), i \in [H_e]$ is the ith row of $f(X)$ in (6).

3) Transmission. The transmission phase consists of $c+1$ rounds of sub-transmissions. At each round $\eta \in [0:c]$, we first construct a set $\mathcal{P}_{\widehat{M}-\eta}$ of groups of $\widehat{M}-\eta$ vertex-disjoint paths unused from previous rounds. Then, we transmit packets over the paths $p \in \mathcal{P}_{\widehat{M}-\eta}$. In particular, we construct the set $\mathcal{P}_{\widehat{M}-\eta}$, using Algorithm 1. Once $\mathcal{P}_{\widehat{M}-\eta}$ is constructed, the source S starts sending the packets T_i, $i \in [H_e]$ in (7) sequentially. For instance, for $\eta = 0$, S sends $\widehat{M}$ packets simultaneously

Algorithm 1 Construction of $\mathcal{P}_{\widehat{M}-\eta}$

1: Let $G^{(\eta)} = G \backslash \bigcup_{i=0}^{\eta-1} \mathcal{P}_{\widehat{M}-i}$, which is a graph G with edges that have not been used during rounds $i \in [0:\eta-1]$.
2: Initialize $\mathcal{P}_{\widehat{M}-\eta} = \varnothing$.
3: Return $\mathcal{P}_{\widehat{M}-\eta}$ if step 4 cannot run.
4: Select $\widehat{M}-\eta$ atomic subgraphs of $G^{(\eta)}$ that have the top $\widehat{M}-\eta$ number of non-zero edge-disjoint paths.
5: Select one path from each selected atomic subgraph and let $\mathcal{Q}$ denote them. Note that $|\mathcal{Q}| = \widehat{M}-\eta$.
6: Update $\mathcal{P}_{\widehat{M}-\eta} = \mathcal{P}_{\widehat{M}-\eta} \bigcup \mathcal{Q}$ and remove the paths in $\mathcal{Q}$ from $G^{(\eta)}$, i.e., $G^{(\eta)} = G^{(\eta)} \setminus \mathcal{Q}$.
7: Go to step 3.

Authorized licensed use limited to: University of Minnesota. Downloaded on May 12,2025 at 21:32:47 UTC from IEEE Xplore. Restrictions apply.

(i.e., in one network use) through each of the $|\mathcal{P}_{\widehat{M}}| =: \mathsf{P}_{\widehat{M}}$ groups of paths in $\mathcal{P}_{\widehat{M}}$. Note that this is possible since: (i) at each point in time, S can simultaneously transmit to $\widehat{M}$ nodes, and (ii) each group of paths in $\mathcal{P}_{\widehat{M}}$ are vertex-disjoint. Thus, the 1-2-1 constraint is satisfied. At the end of round $\eta = 0$, S has sent $T_i, i \in [\widehat{M}\mathsf{P}_{\widehat{M}}]$, i.e., round $\eta = 0$ consists of $\mathsf{P}_{\widehat{M}}$ network uses. After this, round $\eta = 1$ starts and S sends $\widehat{M} - 1$ packets simultaneously (i.e., in one network use) through each of the $|\mathcal{P}_{\widehat{M}-1}| =: \mathsf{P}_{\widehat{M}-1}$ groups of paths in $\mathcal{P}_{\widehat{M}-1}$. In particular, round $\eta = 1$ consists of $\mathsf{P}_{\widehat{M}-1}$ network uses. Then, round $\eta = 2$ will start and so on until $\eta = c$. Each round $\eta \in [0 : c]$ consists of $\mathsf{P}_{\widehat{M}-\eta}$ network uses in each of which $\widehat{M} - \eta$ packets are sent by S. Thus, for each $c \in [0 : \widehat{M} - 1]$ a total of $\sum_{\eta=0}^{c}(\widehat{M} - \eta)\mathsf{P}_{\widehat{M}-\eta}$ packets are sent by S in $\sum_{\eta=0}^{c} \mathsf{P}_{\widehat{M}-\eta}$ network uses.

4) Decoding. At the destination D, the decoding is done by first finding the K random packets $X_{[K]}$ and then reconstructing the keys $f(X)$. Specifically, since the first K received packets are just keys without messages (see (7)), the random packets $X_{[K]}$ can be obtained as follows,

$$X_{[K]} = (V_{[K],[K]})^{-1} T_{[K]}, \tag{8}$$

where $V_{[K],[K]}$ is the sub-matrix of V obtained by just retaining the first K rows and all the K columns of V. Then, D can generate the keys $f(X)$ using $X_{[K]}$ in (8) similar to (6). Finally, D decodes the messages $W_j, j \in [H_e - K]$ as follows,

$$\widehat{W}_{i-K} = T_i - f_i(X), \tag{9}$$

where $i \in [K + 1 : H_e]$.

Security. In each network use, the adversary can receive a packet passing through an eavesdropped edge if the eavesdropped edge belongs to the paths used in that particular network use. Since the K eavesdropped edges can at most be part of K paths, the eavesdropper will receive at most K packets, which are linearly independent thanks to the property of MDS codes (see (7)). Thus, the scheme securely transmits a total of $\left[\sum_{\eta=0}^{c}(\widehat{M} - \eta)\mathsf{P}_{\widehat{M}-\eta} - K\right]^+$ message packets in $\sum_{\eta=0}^{c} \mathsf{P}_{\widehat{M}-\eta}$ network uses. This leads to $R(c)$ in (3). The proof of Theorem 1 is concluded by considering the $c^\star \in [0 : \widehat{M} - 1]$ for which $R(c^\star)$ is maximum.

Example 4. *Consider the 1-2-1 atomic network in Figure 1 with $M = 2$. Thus, $\widehat{M} = 2$. Assume $K = 5$. Then, the proposed scheme for $c = 1$ runs as follows,*

1) *We generate $K = 5$ uniform random packets $X_{[5]}$, and extend them to 7 keys, $f_i(X)$, $i \in [7]$ using an MDS code matrix of size 7×5.*
2) *We encode $H_e - K = 2$ messages W_i, $i \in [2]$ as follows,*

$$T_i = \begin{cases} f_i(X) & i \in [5], \\ f_i(X) + W_{i-5} & i \in [6 : 7]. \end{cases} \tag{10}$$

3) *From Algorithm 1, for $c = 1$, we obtain*

$$\mathcal{P}_2 = \{\{p_1, p_4\}, \{p_2, p_6\}, \{p_3, p_5\}\}, \tag{11}$$

$$\mathcal{P}_1 = \{p_7\}. \tag{12}$$

For transmission, we use the network $\mathsf{P}_2 + \mathsf{P}_1 = 3 + 1 = 4$ times: (1) each group of paths in $\mathcal{P}_2$ can be used to simultaneously transmit $\widehat{M} = 2$ packets, e.g., p_1 and p_4 can be used to transmit T_1 and T_2 in the first network use, p_2 and p_6 can be used to transmit T_3 and T_4 in the second network use, and p_3 and p_5 can be used to transmit T_5 and T_6 in the third network use; and (2) each group of paths in $\mathcal{P}_1$ can be used to simultaneously transmit $\widehat{M} - 1 = 1$ packet, e.g., p_7 can be used to transmit T_7 in the fourth network use.

4) *Upon receiving $T_i, i \in [7]$, D recovers W_1 and W_2 using the property of the MDS code matrix (see (8) and (9)).*

The adversary can learn at most 5 packets, which are encoded with independent keys. Thus, the eavesdropper cannot learn anything about W_1 and W_2. For $c = 1$, we hence obtain a secrecy rate $R(1) = \frac{7-5}{4} = \frac{1}{2}$.

B. Proof of Theorem 2

We let $\mathcal{T}_{\mathcal{S}}^{[n]}$ be the set of packets sent over edges $e \in \mathcal{S}$ in n network uses, i.e., $\mathcal{T}_{\mathcal{S}}^{[n]} = \left\{\mathcal{T}_e^{[n]}, \forall e \in \mathcal{S}\right\}$, and we let $\mathcal{E}_{\mathsf{D}}^-$ be the set of all edges incoming into D. We also let $\mathcal{T}_{\mathcal{E}_i}^{[n]}$ be the packets sent to atom $v_i \in \mathcal{V}_i$ over n network uses. We obtain

$$\begin{aligned}
nR &= H(W) \\
&\overset{(a)}{=} H(W) - H\left(W|\mathcal{T}_{\mathcal{E}_{\mathsf{D}}^-}^{[n]}\right) \\
&= I\left(W; \mathcal{T}_{\mathcal{E}_{\mathsf{D}}^-}^{[n]}\right) \\
&\overset{(b)}{\leq} I\left(W; \bigcup_{i=1}^{H_v} \mathcal{T}_{\mathcal{E}_i}^{[n]}\right) \\
&= I\left(W; \mathcal{T}_{\mathcal{Z}}^{[n]}\right) + I\left(W; \bigcup_{i=1}^{H_v} \mathcal{T}_{\mathcal{E}_i \setminus \mathcal{Z}}^{[n]} \,\middle|\, \mathcal{T}_{\mathcal{Z}}^{[n]}\right) \\
&\overset{(c)}{\leq} \varepsilon + H\left(\bigcup_{i=1}^{H_v} \mathcal{T}_{\mathcal{E}_i \setminus \mathcal{Z}}^{[n]} \,\middle|\, \mathcal{T}_{\mathcal{Z}}^{[n]}\right) \\
&\overset{(d)}{\leq} \varepsilon + \sum_{i=1}^{H_v} H\left(\mathcal{T}_{\mathcal{E}_i \setminus \mathcal{Z}_i}^{[n]} \,\middle|\, \mathcal{T}_{\mathcal{Z}_i}^{[n]}\right) \\
&\overset{(e)}{\leq} \varepsilon + \sum_{i=1}^{H_v} \frac{h_i - K_i}{h_i} H\left(\mathcal{T}_{\mathcal{E}_i}^{[n]}\right) \\
&\overset{(f)}{\leq} \varepsilon + \sum_{i=1}^{H_v} \frac{h_i - K_i}{h_i} n,
\end{aligned} \tag{13}$$

where the labeled (in)equalities follow from: (a) the constraint for reliable decoding; (b) the data processing inequality; (c) the security constraint in (1) and the fact that the entropy of a discrete random variable is non-negative; (d) letting $\mathcal{Z}_i = \mathcal{E}_i \cap \mathcal{Z}$ and using the chain rule for the entropy and the fact that conditioning does not increase the entropy; (e) applying [4, Lemma 1]; and (f) the 1-2-1 network constraint.

Authorized licensed use limited to: University of Minnesota. Downloaded on May 12,2025 at 21:32:47 UTC from IEEE Xplore. Restrictions apply.

By dividing both sides of (13) by n and letting $n \to \infty$, we arrive at

$$R \leq \sum_{i=1}^{H_v} \begin{matrix} h_i - K_i \\ h_i \end{matrix}. \tag{14}$$

The above bound holds for any $\mathcal{Z} \subseteq \mathcal{E}$ such that $|\mathcal{Z}| = K$. Thus, we can find the tightest upper bound by minimizing it with respect to K_i's, which yields

$$R \leq \min_{\substack{K_i \in \mathbb{N} \cup \{0\}, i \in [H_v]: \\ \sum_{i=1}^{H_v} K_i = K, \\ K_i \leq h_i,\ i \in [H_v]}} \sum_{i=1}^{H_v} \begin{matrix} h_i - K_i \\ h_i \end{matrix}. \tag{15}$$

Now, recall that the h_i's are assumed (without loss of generality) to be sorted in descending order, i.e., $h_1 \geq h_2 \geq \ldots \geq h_{H_v}$. This implies that a solution to (15) would first fill K_{H_v} with its maximum value, i.e., $K_{H_v} = \min\{h_{H_v}, K\}$. Then, it will fill K_{H_v-1} as $K_{H_v-1} = \min\{h_{H_v-1}, K - K_{H_v}\}$ and so on until $K_1 = \min\left\{h_1, K - \sum_{i=2}^{H_v} K_i\right\}$. This concludes the proof of Theorem 2.

C. Proof of Theorem 3

Without loss of generality, assume that $h_1 \geq h_2 \geq \ldots \geq h_{H_v}$. If $M \geq H_v$, which implies $\widehat{M} = H_v$, it is not difficult to see that (see also Algorithm 1),

$$\mathsf{P}_{\widehat{M}} = \mathsf{P}_{H_v} = h_{H_v}. \tag{16}$$

Then, the representation for $G \setminus \mathcal{P}_{\widehat{M}}$ is given by $[h_1 - h_{H_v}, \ldots, h_{H_v-1} - h_{H_v}, 0]$, which similarly gives

$$\mathsf{P}_{\widehat{M}-1} = \mathsf{P}_{H_v-1} = h_{H_v-1} - h_{H_v}. \tag{17}$$

Iterating the above procedure up to $\mathcal{P}_1$, we obtain

$$\mathsf{P}_\ell = h_\ell - h_{\ell+1},\ \forall \ell \in [H_v], \tag{18}$$

where we let $h_{H_v+1} = 0$. Substituting (18) into (3) yields that for $c \in [0 : H_v - 1]$,

$$\begin{aligned} R(c) &= \begin{bmatrix} \sum_{\eta=0}^{c} (H_v - \eta)(h_{H_v-\eta} - h_{H_v-\eta+1}) - K \\ \sum_{\eta=0}^{c} (h_{H_v-\eta} - h_{H_v-\eta+1}) \end{bmatrix}^+ \\ &= \begin{bmatrix} H_v - c + \dfrac{\sum_{\eta=0}^{c-1} h_{H_v-\eta} - K}{h_{H_v-c}} \end{bmatrix}^+. \end{aligned} \tag{19}$$

Now, we pick $c \in [0 : H_v - 1]$ such that $\sum_{i=0}^{c-1} h_{H_v-i} < K \leq \sum_{i=0}^{c} h_{H_v-i}$. Note that such a c always exists. We define $\alpha_i = \min\left\{h_i, K - \sum_{j=i+1}^{H_v} \alpha_j\right\},\ i \in [H_v]$, that is,

$$\alpha_i = \begin{cases} 0 & \text{if } i < H_v - c - 1, \\ K - \sum_{j=i+1}^{H_v} h_j & \text{if } i = H_v - c, \\ h_i & \text{if } i > H_v - c. \end{cases} \tag{20}$$

The α_i's in (20) imply that

$$\begin{matrix} K - \sum_{\eta=0}^{c-1} h_{H_v-\eta} \\ h_{H_v-c} \end{matrix} + c = \begin{matrix} K - \sum_{\eta=0}^{c-1} h_{H_v-\eta} \\ h_{H_v-c} \end{matrix} + \sum_{i=H_v-c+1}^{H_v} \begin{matrix} h_i \\ h_i \end{matrix}$$

$$= \sum_{i=1}^{H_v} \begin{matrix} \alpha_i \\ h_i \end{matrix}. \tag{21}$$

Substituting (21) into (19), we obtain

$$R(c) = \left[H_v - \sum_{i=1}^{H_v} \begin{matrix} \alpha_i \\ h_i \end{matrix}\right]^+ = \sum_{i=1}^{H_v} \left(1 - \begin{matrix} \alpha_i \\ h_i \end{matrix}\right), \tag{22}$$

where

$$\alpha_i = \min\left\{h_i, K - \sum_{j=i+1}^{H_v} \alpha_j\right\},\ i \in [H_v], \tag{23}$$

which is the upper bound in (5). This concludes the proof of Theorem 3.

ACKNOWLEDGMENT

This research was supported in part by the U.S. National Science Foundation under Grant CCF-2045237.

REFERENCES

[1] X. Wang, L. Kong, F. Kong, F. Qiu, M. Xia, S. Arnon, and G. Chen, "Millimeter Wave Communication: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1616–1653, 2018.

[2] A. N. Uwaechia and N. M. Mahyuddin, "A Comprehensive Survey on Millimeter Wave Communications for Fifth-Generation Wireless Networks: Feasibility and Challenges," *IEEE Access*, vol. 8, pp. 62 367–62 414, 2020.

[3] Y. H. Ezzeldin, M. Cardone, C. Fragouli, and G. Caire, "Gaussian 1-2-1 Networks: Capacity Results for mmWave Communications," *IEEE Transactions on Information Theory*, vol. 67, no. 2, pp. 961–990, 2020.

[4] G. K. Agarwal, Y. H. Ezzeldin, M. Cardone, and C. Fragouli, "Secure Communication over 1-2-1 Networks," in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 196–200.

[5] Y. H. Ezzeldin, M. Cardone, and C. Fragouli, "Multilevel Secrecy over 1-2-1 Networks," in *2020 IEEE Information Theory Workshop (ITW)*, 2020, pp. 1–5.

[6] A. Mukherjee and A. L. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels with Imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2011.

[7] I. Safaka, L. Czap, K. Argyraki, and C. Fragouli, "Creating Secrets out of Packet Erasures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1177–1191, 2016.

[8] N. Cai and R. Yeung, "Secure Network Coding," in *2002 IEEE International Symposium on Information Theory,*, 2002, pp. 323–.

[9] A. Khaleghi, D. Silva, and F. R. Kschischang, "Subspace Codes," in *IMA International Conference on Cryptography and Coding*. Springer, 2009, pp. 1–21.

[10] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient Network Coding in the Presence of

Authorized licensed use limited to: University of Minnesota. Downloaded on May 12,2025 at 21:32:47 UTC from IEEE Xplore. Restrictions apply.

Byzantine Adversaries," in *2007-26th IEEE International Conference on Computer Communications (INFOCOM)*. IEEE, 2007, pp. 616–624.

[11] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. Tolhuizen, "Polynomial Time Algorithms for Multicast Network Code Construction," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, 2005.

[12] G. K. Agarwal, M. Cardone, and C. Fragouli, "Secure Network Coding for Multiple Unicast: On the Case of Single Source," in *Information Theoretic Security: 10th International Conference (ICITS)*. Springer, 2017, pp. 188–207.

[13] T. Cui, T. Ho, and J. Kliewer, "On Secure Network Coding with Nonuniform or Restricted Wiretap Sets," *IEEE Transactions on Information Theory*, vol. 59, no. 1, pp. 166–176, 2012.

[14] N. Cai and R. W. Yeung, "A Security Condition for Multi-Source Linear Network Coding," in *2007 IEEE International Symposium on Information Theory (ISIT)*, 2007, pp. 561–565.

[15] C.-K. Ngai, R. W. Yeung, and Z. Zhang, "Network Generalized Hamming Weight," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1136–1143, 2011.

[16] V. K. Wei, "Generalized Hamming Weights for Linear Codes," *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

[17] R. Koetter, M. Effros, T. Ho, and M. Médard, "Network Codes as Codes on Graphs," in *2004 Annual Conference on Information Sciences and Systems (CISS)*, 2004.

[18] M. Gadouleau and S. Riis, "Graph-Theoretical Constructions for Graph Entropy and Network Coding Based Communications," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6703–6717, 2011.

[19] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger, "Byzantine Modification Detection in Multicast Networks With Random Network Coding," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2798–2803, 2008.

[20] A. Papadopoulos, L. Czap, and C. Fragouli, "LP Formulations for Secrecy over Erasure Networks with Feedback," in *2015 IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 954–958.

[21] L. Czap, V. M. Prabhakaran, S. Diggavi, and C. Fragouli, "Triangle Network Secrecy," in *2014 IEEE International Symposium on Information Theory*, 2014, pp. 781–785.

[22] M. Milanian, M. Jeong, and M. Cardone, "On the Secrecy Capacity of 1-2-1 Atomic Networks," *arXiv preprint arXiv:2405.05823*, 2024.

Authorized licensed use limited to: University of Minnesota. Downloaded on May 12,2025 at 21:32:47 UTC from IEEE Xplore. Restrictions apply.