Achievable Strategies for General Secure Network Coding

Tao Cui and Tracey Ho
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125, USA
Email: {taocui, tho}@caltech.edu

Jörg Kliewer
Klipsch School of Electrical and Computer Engineering
New Mexico State University
Las Cruces, NM 88003, USA
Email: jkliewer@nmsu.edu

***Abstract*—This paper considers secure network coding over networks with restricted wiretapping sets and unequal link capacities in the presence of a wiretapper that can wiretap any subset of k links. In particular, we consider networks with point-to-point erasure channels. Existing results for wireline networks show that for the case of both unrestricted wiretapping sets and equal (unit) link capacities, the secrecy capacity is given by the cut-set bound, whether or not the location of the wiretapped links is known, and can be achieved by injecting k random keys at the source which are decoded at the sink along with the message. In contrast, for restricted wiretapping sets and unequal link capacities we show that this global key strategy is suboptimal. In particular, we propose achievable strategies where random keys are canceled at intermediate non-sink nodes, injected at intermediate non-source nodes, or a combination of both strategies is considered.**

I. Introduction

Information-theoretically secure communication uses coding to ensure that an adversary eavesdropping on a subset of network links obtains no information about the secure message. A theoretical basis for information-theoretic security was given in the seminal paper by Wyner [1] using Shannon's notion of perfect secrecy [2], where a coset coding scheme based on a linear maximum distance separable code was used to achieve security for a wiretap channel. More recently, information-theoretic security has been studied in networks with general topologies. The secure network coding problem was introduced in [3] for multicast wireline networks where each link has equal capacity, and a wiretapper can observe an unknown (unrestricted) set of up to k network links. For this problem, constructions of information-theoretically secure linear network codes are proposed in e.g. [3]–[5]. In [6], secure communication is considered for wireless erasure networks.

In the case of throughput optimization without security requirements, the assumption that all links have unit capacity is made without loss of generality, since links of larger capacity can be modeled as multiple unit capacity links in parallel. However, in the secure communication problem, such an assumption cannot be made without loss of generality. Indeed, we show in this paper that there are significant differences between the equal capacity and unequal capacity cases and that these differences also exist if unrestricted or unrestricted wiretapping sets are considered. In particular, for the case of equal (unit) link capacities and unrestricted wiretapping sets, the secrecy capacity is given by the cut set bound, whether or not the location of the wiretapped links is known. This capacity can be achieved by injecting k random keys at the source which are decoded at the sink along with the message [3]. We refer to this approach as the global key strategy. In contrast, the restricted wiretapping set case is more complicated, even for a single source and sink. We propose new achievable strategies where random keys are canceled at intermediate non-sink nodes, injected at intermediate non-source nodes, or where a combination of both strategies is applied, and show that these approaches can outperform the global key strategy.

II. Network Model and Problem Formulation

In this paper we focus on acyclic graphs for simplicity; we expect that our results can be generalized to cyclic networks using the approach in [7], [8] of working over fields of rational functions in an indeterminate delay variable.

For each node $i \in \mathcal{V}$, $\mathcal{N}_{\mathcal{O}}(i)$ and $\mathcal{N}_{\mathcal{I}}(i)$ denote the set of in-neighbors and out-neighbors of i, i.e.,

$$\mathcal{N}_{\mathcal{I}}(i) = \{j|(j,i) \in \mathcal{E}\}, \quad \mathcal{N}_{\mathcal{O}}(i) = \{j|(i,j) \in \mathcal{E}\}. \tag{1}$$

A cut for $x, y \in \mathcal{V}$ is a partition of $\mathcal{V}$ into two sets $\mathcal{V}_x$ and $\mathcal{V}_y = \mathcal{V}_x^c$ such that $x \in \mathcal{V}_x$ and $y \in \mathcal{V}_y$. For the $x-y$ cut given by $\mathcal{V}_x$, the cut-set $[\mathcal{V}_x, \mathcal{V}_y]$ is the set of edges going from $\mathcal{V}_x$ to $\mathcal{V}_y$, i.e.,

$$[\mathcal{V}_x, \mathcal{V}_y] = \{(u,v)|(u,v) \in \mathcal{E},\, u \in \mathcal{V}_x,\, v \in \mathcal{V}_y\}. \tag{2}$$

In the most general network model that we consider, each edge $(i,j) \in \mathcal{E}$ represents a memoryless erasure channel from node i to node j with erasure probability $p_{i,j}$. As in [3], there is an eavesdropper, who can wiretap any k edges of this network. For any wiretapped edge $(i,j) \in \mathcal{E}$, the wiretapper can receive the symbols sent by node i to node j via another memoryless erasure channel with erasure probability $q_{i,j}$. Note that our model includes those in [3], [6] as special cases. When $p_{i,j} = q_{i,j} = 0$ for all links (i,j), our model reduces to that in [3]. When $p_{i,j} = q_{i,j}$ takes different values for different links (i,j), with appropriate capacity scaling, the network is equivalent to an network with unequal capacity links where the wiretapper fully observes transmissions on the links it wiretaps.

An eavesdropper can wiretap a set $\mathcal{A}$ of links chosen from a known collection $\mathcal{W}$ of possible wiretap sets. Without loss of generality we can restrict our attention to maximal wiretap sets, i.e. no set in $\mathcal{W}$ is a subset of another. The choice of wiretap set $\mathcal{A}$ is unknown to the communicating nodes, except where otherwise specified in this paper. The secrecy capacity is the highest possible source-sink communication rate such that the message communicated is information theoretically secret regardless of the choice of $\mathcal{A}$, i.e. has zero mutual information with the wiretapper's observations.

The strategies we describe below apply to the general problem with unequal link capacities and restricted wiretapping sets, but the examples we provide focus on two special cases:

1) Scenario 1 is a wireline network with *equal* link capacities, where the wiretapper can wiretap an unknown subset of k links from a known collection of vulnerable network links.
2) Scenario 2 is a wireline network with *unequal* link capacities, where the wiretapper can wiretap an unknown subset of k links from the entire network.

Although, for the sake of simplicity, we only discuss single-source single-sink networks in the following, the cut-set bound and strategy 2 in the next section can be easily extended to multicast networks.

III. Cut-Set Bound and Achievable Strategies

In this section, we consider the general wireline problem with unequal link capacities where the eavesdropper can wiretap an unknown set $\mathcal{A}$ of links chosen from a known collection $\mathcal{W}$ of possible wiretap sets. We state a cut-set upper bound on capacity, and give two new achievable strategies and examples in which they outperform the existing global key strategy.

A. Cut-Set Bound

Let $\mathcal{S}^c$ denote the set complement of a set $\mathcal{S}$. A cut for $x, y \in \mathcal{V}$ is a partition of $\mathcal{V}$ into two sets $\mathcal{V}_x$ and $\mathcal{V}_x^c$ such that $x \in \mathcal{V}_x$ and $y \in \mathcal{V}_x^c$. For the $x-y$ cut given by $\mathcal{V}_x$, the cut-set $[\mathcal{V}_x, \mathcal{V}_x^c]$ is the set of edges going from $\mathcal{V}_x$ to $\mathcal{V}_x^c$, i.e.,

$$[\mathcal{V}_x, \mathcal{V}_x^c] = \{(u,v) | (u,v) \in \mathcal{E},\, u \in \mathcal{V}_x,\, v \in \mathcal{V}_x^c\}. \quad (3)$$

Before stating the theorem, we briefly review the results in [1], where a wiretap channel with one source, one sink and one wiretapper is considered. Let X be the secret message sent by the source, and let Y and Z be the received signal at the sink and wiretapper, respectively. By using a coset coding scheme based on a linear maximum distance separable code, Wyner showed that the secrecy capacity of the wiretap channel is

$$C_s = \max_{p_X(x)} I(Y;X) - I(Z;X), \quad (4)$$

with $H(X|Z) = H(X)$, where $p_X(x)$ is the pdf of X.

Theorem 1. *Consider a single source and single sink wireline erasure network in which a secret message M is delivered from source s to destination d. There exists a wiretapper in the network that can wiretap at most k links and the wiretapped messages are denoted as $\mathbf{Z}$. Assuming that the destination has complete knowledge of the erasure locations on each link of the network and the locations of the wiretapped links, the secrecy capacity is given by*

$$C_s = \min_{\{\mathcal{V}_s:\, \mathcal{V}_s \text{ is an } s-d \text{ cut}\}} \min_{\{\mathcal{A} | \mathcal{A} \subseteq [\mathcal{V}_s, \mathcal{V}_s^c],\, |\mathcal{A}| \le k\}} \sum_{(i,j) \in [\mathcal{V}_s, \mathcal{V}_s^c] - \mathcal{A}} (1 - p_{i,j}) + \sum_{(i,j) \in \mathcal{A}} \max\left(q_{i,j} - p_{i,j}, 0\right), \quad (5)$$

where

$$H(M|\mathbf{Z}) = H(M). \quad (6)$$

Proof: **Achievability.** We show the achievability of (5) by applying the coding scheme of [1] on each link individually. Let $X_{i,j}$, $Y_{i,j}$ and $Z_{i,j}$ be the local message, channel output, and wiretapper's output on link $(i,j) \in \mathcal{A}$. From (4), we know that as long as the rate of $X_{i,j}$ is less than

$$\begin{aligned} \max_{P_{i,j}(x_{i,j})} I(X_{i,j}; Y_{i,j}) - I(X_{i,j}; Z_{i,j}) &= \max_{\pi} (q_{i,j} - p_{i,j}) H(\pi) \\ &= \max\left(q_{i,j} - p_{i,j}, 0\right), \end{aligned} \quad (7)$$

node j can receive $X_{i,j}$ securely, i.e., $I(X_{i,j}; Z_{i,j}) = 0$. As $M \to \mathbf{X} \to \mathbf{Z}$ forms a Markov chain, we have

$$\begin{aligned} I(M;\mathbf{Z}) &\le I(\mathbf{X};\mathbf{Z}) = H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{X}) \\ &\le \sum_{(i,j) \in \mathcal{A}} H(Z_{i,j}) - \sum_{(i,j) \in \mathcal{A}} H(Z_{i,j}|X_{i,j}) \\ &= \sum_{(i,j) \in \mathcal{A}} I(X_{i,j}; Z_{i,j}) = 0, \end{aligned} \quad (8)$$

where the second inequality follows since conditioning reduces entropy [9] and that $Z_{i,j}$ is conditionally independent of the local messages and wiretapped observations at other nodes given $X_{i,j}$. As mutual information is nonnegative, we have $I(M;\mathbf{Z}) = 0$ and perfect secrecy is achieved. Therefore, given the wiretapping set $\mathcal{A}$, we can decouple the secrecy coding from the routing or network coding, i.e., routing or network coding is oblivious to the secrecy coding. We simply replace the capacity of each link with the secrecy capacity of each link. Therefore, the following cut-set bound is achievable

$$\min_{\{\mathcal{V}_s:\, \mathcal{V}_s \text{ is an } s-d \text{ cut}\}} \sum_{(i,j) \in [\mathcal{V}_s, \mathcal{V}_s^c] - \mathcal{A}} (1 - p_{i,j}) + \sum_{(i,j) \in \mathcal{A}} \max\left(q_{i,j} - p_{i,j}, 0\right). \quad (9)$$

The wiretapper chooses the set $\mathcal{A}$ to minimize the secrecy rate in (9), which gives (5). This concludes the achievability part.

Converse. Let $\mathcal{V}_s$ be a cut of the network and $\mathcal{A} \subseteq [\mathcal{V}_s, \mathcal{V}_s^c]$, $|\mathcal{A}| \le k$ be the set of wiretapping edges. Denote by $\mathbf{X}$ the transmitted signals from nodes in $\mathcal{V}_s$ over links in $[\mathcal{V}_s, \mathcal{V}_s^c]$ and denote by $\mathbf{Z}$ and $\mathbf{Y}$ the observed signals from links in $\mathcal{A}$ and in $[\mathcal{V}_s, \mathcal{V}_s^c]$, respectively. Let $\mathcal{A}_h$ be the set of links (i,j) such that $p_{i,j} \ge q_{i,j}$, and let $\mathbf{Y}_h$ and $\mathbf{Y}_d$ contain the observations from links in $\mathcal{A}_h$ and $[\mathcal{V}_s, \mathcal{V}_s^c] - \mathcal{A}_h$, respectively. $\mathbf{Z}_h$ and $\mathbf{Z}_d$ are defined similarly, where $\mathbf{Z}_d$ is a degraded version of $\mathbf{Y}_d$

while $\mathbf{Y}_h$ is a degraded version of $\mathbf{Z}_h$. We consider block coding with block length n. We have

$$\begin{aligned}
nR_s \leq & H(M|\mathbf{Z}^n) \\
\overset{(a)}{\leq} & H(M|\mathbf{Z}^n) - H(M|\mathbf{Y}^n) + n\epsilon_n \\
\overset{(b)}{=} & H(M|\mathbf{Z}_d^n, \mathbf{Z}_h^n) - H(M|\mathbf{Y}_d^n, \mathbf{Y}_h^n) + n\epsilon_n \\
\overset{(c)}{\leq} & H(M|\mathbf{Z}_d^n, \mathbf{Y}_h^n) - H(M|\mathbf{Y}_d^n, \mathbf{Y}_h^n) + n\epsilon_n \\
\overset{(d)}{\leq} & H(M|\mathbf{Z}_d^n, \mathbf{Y}_h^n) - H(M|\mathbf{Z}_d^n, \mathbf{Y}_d^n, \mathbf{Y}_h^n) + n\epsilon_n \\
= & I(M; \mathbf{Y}_d^n|\mathbf{Z}_d^n, \mathbf{Y}_h^n) + n\epsilon_n \\
\overset{(e)}{\leq} & I(\mathbf{X}^n; \mathbf{Y}_d^n|\mathbf{Z}_d^n, \mathbf{Y}_h^n) + n\epsilon_n, \\
= & \sum_{i=1}^{n} H(\mathbf{Y}_{d,i}|\mathbf{Z}_d^n, \mathbf{Y}_h^n) - \sum_{i=1}^{n} H(\mathbf{Y}_{d,i}|\mathbf{X}^n, \mathbf{Z}_d^n, \mathbf{Y}_h^n) \\
& + n\epsilon_n, \\
\overset{(f)}{\leq} & \sum_{i=1}^{n} H(\mathbf{Y}_{d,i}|\mathbf{Z}_{d,i}, \mathbf{Y}_{h,i}) - \sum_{i=1}^{n} H(\mathbf{Y}_{d,i}|\mathbf{X}_i, \mathbf{Z}_{d,i}, \mathbf{Y}_{h,i}) \\
& + n\epsilon_n, \\
= & nI(\mathbf{X}; \mathbf{Y}_d|\mathbf{Z}_d, \mathbf{Y}_h) + n\epsilon_n, \\
= & n\left(I(\mathbf{X}; \mathbf{Y}_d, \mathbf{Y}_h) - I(\mathbf{X}; \mathbf{Z}_d, \mathbf{Y}_h)\right) + n\epsilon_n, \\
\leq & n \max_{p(\mathbf{X})} \left(I(\mathbf{X}; \mathbf{Y}_d, \mathbf{Y}_h) - I(\mathbf{X}; \mathbf{Z}_d, \mathbf{Y}_h)\right) + n\epsilon_n, \\
\overset{(g)}{=} & n\left(\sum_{(i,j)\in[\mathcal{V}_s, \mathcal{V}_s^c]} (1-p_{i,j}) - \sum_{(i,j)\in\mathcal{A}_d} (1-q_{i,j}) - \right. \\
& \left. \sum_{(i,j)\in\mathcal{A}_h} (1-p_{i,j})\right) + n\epsilon_n, \\
= & n\left(\sum_{(i,j)\in[\mathcal{V}_s, \mathcal{V}_s^c]-\mathcal{A}} (1-p_{i,j}) + \right. \\
& \left. \sum_{(i,j)\in\mathcal{A}} \max(q_{i,j} - p_{i,j}, 0)\right) + n\epsilon_n,
\end{aligned} \tag{10}$$

where $\epsilon_n \to 0$ as $n \to +\infty$ and

- (a) comes from Fano's inequality.
- (b) follows from the definition of $\mathbf{Y}_d, \mathbf{Y}_h, \mathbf{Z}_d, \mathbf{Z}_h$.
- (c) comes from the fact that $M \to \mathbf{X}^n \to (\mathbf{Z}_d^n, \mathbf{Z}_h^n) \to (\mathbf{Z}_d^n, \mathbf{Y}_h^n)$ forms a Markov chain.
- (d) follows from conditioning reduces entropy.
- (e) comes from the fact that $M \to \mathbf{X}^n \to (\mathbf{Y}_d^n, \mathbf{Y}_h^n) \to (\mathbf{Z}_d^n, \mathbf{Y}_h^n)$ forms a Markov chain and $A \to B \to C \to D \Rightarrow I(A;C|D) \leq I(B;C|D)$. To show this inequality, we have

$$\begin{aligned}
I(A;C|D) - I(B;C|D) = & I(A;C,D) - I(A;D) - \\
& I(B;C,D) + I(B;D) \\
= & I(B;D|A) - I(B;C|A) \\
= & -I(B;C|A,D) \leq 0.
\end{aligned}$$

- (f) follows from the fact that conditioning reduces entropy and that $\mathbf{Y}_{d,i}$ is independent of other variables given $\mathbf{X}_i, \mathbf{Z}_{d,i}, \mathbf{Y}_{h,i}$.
- (g) is because both $I(\mathbf{X}; \mathbf{Y}_d, \mathbf{Y}_h)$ and $I(\mathbf{X}; \mathbf{Z}_d, \mathbf{Y}_h)$ are maximized when the entries of $\mathbf{X}$ are i.i.d. Bernoulli(1/2).

■

By decoupling the secrecy coding from the routing or network coding as in the achievability proof of Theorem 1, Theorem 1 can be readily extended to the multicast case. The proof is similar to the unicast case. We thus give the following theorem without proof.

Theorem 2. *Consider a multicast problem in a wireline erasure network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with a single source $s \in \mathcal{V}$ and a set of destinations $\mathcal{D} \subseteq \mathcal{V}$. A secret message M is multicast from s to all nodes in $\mathcal{D}$. There exists a wiretapper in the network that can wiretap at most k links, and the wiretapped messages are denoted as $\mathbf{Z}$. Assuming that the destination has complete knowledge of the erasure locations on each link of the network and the locations of the wiretapped links, the secrecy multicast capacity of the network is given by*

$$\begin{aligned}
C_s = & \min_{d\in\mathcal{D}} \min_{\{\mathcal{V}_s: \mathcal{V}_s \text{ is an } s-d \text{ cut}\}} \\
& \min_{\{\mathcal{A}|\mathcal{A}\subseteq[\mathcal{V}_s, \mathcal{V}_s^c], |\mathcal{A}|\leq k\}} \sum_{(i,j)\in[\mathcal{V}_s, \mathcal{V}_s^c]-\mathcal{A}} (1-p_{i,j}) + \\
& \sum_{(i,j)\in\mathcal{A}} \max\left(q_{i,j} - p_{i,j}, 0\right),
\end{aligned} \tag{11}$$

where

$$H(M|\mathbf{Z}) = H(M). \tag{12}$$

B. Achievable Strategies for Unknown Wiretap Set

In the case of unrestricted wiretapping sets, unit link capacities, and $p_{i,j} = q_{i,j}$ on every edge (i,j), the secrecy capacity can be achieved using global keys generated at the source and decoded at the sink [3]. The source transmits r secret information symbols and k random key symbols, where $r+k$ is equal to the min-cut of the network. This scheme does not achieve capacity in general networks. Intuitively, this is because the total rate of random keys is limited by the min cut from the source to the sink, whereas more random keys may be required to fully utilize large capacity cuts with large capacity links.

In this case, capacity can be improved by using a combination of local and global random keys. A local key is injected at a non-source node and/or canceled at a non-sink node. However, it is complicated to optimize over all possible combinations of nodes at which keys are injected and canceled. Thus, we propose the following more tractable family of constructions, which we will use in subsequent sections. In the following, we focus on the case of a single source and a single sink. Let $z_{i,j}$ be the actual flow on link (i,j).

For the case where $q_{i,j} \neq p_{i,j}$, by using random linear coding on each link, node i sends $\frac{z_{i,j}}{(1-p_{i,j})}$ random linear combinations over link (i,j) to guarantee that j can decode

$z_{i,j}$ symbols with high probability for large $z_{i,j}$. The wiretapper can get $\min\left(\frac{1-q_{i,j}}{1-p_{i,j}}, 1\right) z_{i,j}$ linearly independent random combinations from link (i,j) with high probability.

Strategy 1: Random keys injected at the source and possibly canceled at intermediate nodes

Connect each subset of links $\mathcal{A} \in \mathcal{W}$ in the network $\mathcal{G}$ to a virtual node $t^{\mathcal{A}}$, and connect both $t^{\mathcal{A}}$ and the actual sink to a virtual sink $d^{\mathcal{A}}$. Let $R_{s\to\mathcal{A}}$ be the total flow between s and $t^{\mathcal{A}}$. The virtual link between $t^{\mathcal{A}}$ and $d^{\mathcal{A}}$ has capacity $R_{s\to\mathcal{A}}$, and the virtual link between the actual sink and $d^{\mathcal{A}}$ has capacity R_s. This is illustrated in Fig. 1. The source multicasts a secret message $\mathbf{v} = [v_1, \ldots, v_{R_s}]^T$ with R_s symbols plus R_w random key symbols $\mathbf{w} = [w_1, \ldots, w_{R_w}]$. We want to choose the secrecy rate R_s and the random key rate R_w such that the virtual receiver $d^{\mathcal{A}}$ can decode $R_s + R_{s\to\mathcal{A}}$ message and key symbols from the source, and the original receiver can decode the R_s message symbols.

If the rate $R_s + R_{s\to\mathcal{A}}$ satisfies the min-cut between the source and the virtual receiver $d^{\mathcal{A}}$ and $R_{s\to\mathcal{A}} \le R_w$, by using [10, Corollary 19.21], there exists a network code such that $d^{\mathcal{A}}$ receives $R_s + R_{s\to\mathcal{A}}$ linearly independent combinations of $\mathbf{v}$ and $\mathbf{w}$ when the finite field size is sufficiently large. Let the signals received at a particular virtual sink $d^{\mathcal{B}}$ be denoted as $\mathbf{M}_{\mathcal{B}}[\mathbf{v}^T, \mathbf{w}^T]^T$, where $\mathbf{M}_{\mathcal{B}}$ is an $R_s + R_{s\to\mathcal{A}}$ by $R_s + R_w$ received coding matrix with full row rank[1]. We can add $R_w - R_{s\to\mathcal{B}}$ rows to $\mathbf{M}_{\mathcal{B}}$ to get a full rank $(R_s + R_w) \times (R_s + R_w)$ square matrix $\tilde{\mathbf{M}}_{\mathcal{B}}$. We thus precode the secret message and keys using $\tilde{\mathbf{M}}_{\mathcal{B}}^{-1}$, i.e., the source transmits $\tilde{\mathbf{M}}_{\mathcal{B}}^{-1}[\mathbf{v}^T, \mathbf{w}^T]^T$. This results in the actual sink receiving the message $\mathbf{v}$, which is transmitted to each virtual sink by the corresponding virtual link.

For any virtual sink $d^{\mathcal{A}}$, the received coding matrix after precoding is $\mathbf{M}_{\mathcal{A}}\tilde{\mathbf{M}}_{\mathcal{B}}^{-1}$, which is a full row rank matrix. As $\mathbf{M}_{\mathcal{A}}\tilde{\mathbf{M}}_{\mathcal{B}}^{-1}$ is a full row rank matrix, the coding vectors of the received signals from the set $\mathcal{A}$ of wiretapping links span a rank $R_{s\to\mathcal{A}}$ subspace that is linearly independent of the set of coding vectors of message $\mathbf{v}$ which is received from the actual sink d. Therefore, perfect secrecy with rate R_s can be achieved provided that the finite field size $q > \binom{|\mathcal{E}|}{k}$. Note that by applying $\tilde{\mathbf{M}}_{\mathcal{B}}^{-1}$, the random keys injected by the source are either implicitly canceled at intermediate nodes or decoded by the sink.

Since computing $R_{s\to\mathcal{A}}$ involves a separate linear optimization in $z_{i,j}$, to simplify the computation, we can replace $R_{s\to\mathcal{A}}$ with an upper bound $\sum_{(i,j)\in\mathcal{A}} z_{i,j} \min\left(\frac{1-q_{i,j}}{1-p_{i,j}}, 1\right)$. This gives a lower bound on the achievable secrecy rate using key cancellation, for which we can write a linear program (LP)

[1]We assume that R_s and $R_{s\to\mathcal{B}}$ are integers, which can be approximated arbitrarily closely by scaling the capacity of all links by the same factor.

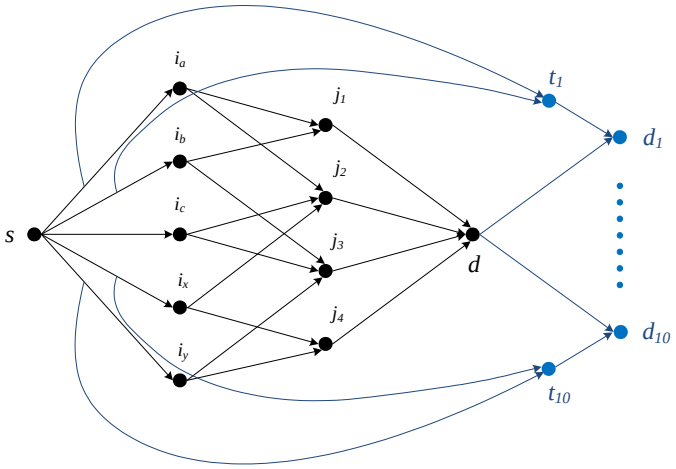

Fig. 1. Illustration of Strategy 1, an achievable construction where random keys are injected by the source and possibly canceled at intermediate nodes. In this figure, $k = 2$ and only the 5 links in the first layer can be wiretapped.

as follows:

$$\begin{aligned}
&\max\ R_s \\
&\text{subject to} \sum_{(i,j)\in\mathcal{E}} f_{i,j}^{\mathcal{A}} - \sum_{(i,j)\in\mathcal{E}} f_{j,i}^{\mathcal{A}} = \\
&\qquad \begin{cases} R_s + \sum_{(i,j)\in\mathcal{A}} z_{i,j} \min\left(\frac{1-q_{i,j}}{1-p_{i,j}}, 1\right), & \text{if } i = s, \\ -R_s - \sum_{(i,j)\in\mathcal{A}} z_{i,j} \min\left(\frac{1-q_{i,j}}{1-p_{i,j}}, 1\right), & \text{if } i = d^{\mathcal{A}}, \\ 0, & \text{otherwise,} \end{cases} \\
&\qquad \forall \mathcal{A} \in \mathcal{W}, \\
&\qquad f_{i,j}^{\mathcal{A}} \le z_{i,j} \le c_{i,j},\ \forall (i,j) \in \mathcal{E}, \mathcal{A} \in \mathcal{W},
\end{aligned} \tag{13}$$

where $f_{i,j}^{\mathcal{A}}$ is the virtual flow on link (i,j) for the virtual sink corresponding to wiretapping set $\mathcal{A}$ and $z_{i,j}$ is the actual flow on link (i,j). The optimal value of (14) gives an achievable secrecy rate.

An alternative simplification is to redefine $R_{s\to\mathcal{A}}$ as the minimum cut capacity between s and $t^{\mathcal{A}}$ on the graph (as opposed to the capacity associated with the chosen flow variables). This gives another achievable region for which we can write an LP:

$$\begin{aligned}
&\max\ R_s \\
&\text{subject to} \sum_{(i,j)\in\mathcal{E}} f_{i,j}^{\mathcal{A}} - \sum_{(i,j)\in\mathcal{E}} f_{j,i}^{\mathcal{A}} = \\
&\qquad \begin{cases} R_s + R_{s\to\mathcal{A}}, & \text{if } i = s, \\ -R_s - R_{s\to\mathcal{A}}, & \text{if } i = d^{\mathcal{A}}, \\ 0, & \text{otherwise,} \end{cases} \\
&\qquad \forall \mathcal{A} \in \mathcal{W}, \\
&\qquad f_{i,j}^{\mathcal{A}} \le z_{i,j} \le c_{i,j},\ \forall (i,j) \in \mathcal{E}, \mathcal{A} \in \mathcal{W}.
\end{aligned} \tag{14}$$

An illustration of the Strategy 1 construction in Scenario 1 is given in Fig. 1 for $p_{i,j} = q_{i,j}$ for all edges (i,j) where the number of wiretapped links is $k = 2$, and only the first layer of the three layer network is allowed to be wiretapped. Each link

in the network has unit capacity. Let c denote the minimum cut after deleting any k links in the first layer of the graph. As the wiretapped links are connected to the source directly, the min-cut between each virtual sink and the source is at least $c+k$. Since c is the cut-set upper bound on the secrecy rate, by using the key cancelation scheme the secrecy rate c is achievable, which is equal to the secrecy rate when the location of wiretap links is known. For the example in Fig. 1, the secrecy rate $c = 3$ is achievable. When key cancelation is not applied, let r and w be the secrecy rate and the random key rate at the source, respectively. Let x be the total actual flow on the first layer. To achieve secrecy, we must have $w \geq \frac{2}{5}x$, where the min-cut condition on the first layer requires $r + w \leq x$. Since the sink needs to decode both message and random key symbols from the source, the min-cut condition on the last layer requires $r + w \leq 4$. Combining these we obtain $r \leq \frac{12}{5}$, which is strictly less than 3.

This example can be converted into a Scenario 2 example with unequal link capacities where the adversary can wiretap any $k = 2$ links, where Strategy 1 outperforms the global key strategy. Each link in the second and third layers is divided into $1/\epsilon$ links of ϵ capacity each, where ϵ is an arbitrarily small constant. Since the set of possible wiretapping link sets is strictly larger in this case, the maximum rate under the global key strategy is also at most $\frac{12}{5}$. By allocating 2ϵ of the capacity of each first layer link to carry an additional global random key, a rate arbitrarily close to 3 can be achieved.

Strategy 2: Random keys injected at the source and/or intermediate nodes and decoded at the sink

Connect each subset of links $\mathcal{A} \in \mathcal{W}$ in the network $\mathcal{G}$ to a virtual receiver $d^{\mathcal{A}}$. If the rate of linearly independent keys received at $d^{\mathcal{A}}$ is greater or equal than the rate for the data received through the corresponding wiretap links, perfect secrecy can be achieved. Let $R_{w,v}$ be the secret key injection rate at node v and R_s be the secrecy rate at the source. We want to maximize R_s subject to the condition that the sink can decode the random keys injected at all nodes plus the message, and each wiretap set gets total key rate greater than or equal to its received flow. We then have the following LP:

$$
\begin{aligned}
&\max\ R_s \\
&\text{subject to } \sum_j f^{\mathcal{A}}_{i,j} - \sum_j f^{\mathcal{A}}_{j,i} \\
&\quad \begin{cases} = -\sum_{(i,j)\in\mathcal{A}} g_{i,j} \min\left(\frac{1-q_{i,j}}{1-p_{i,j}}, 1\right), & \text{if } i = d^{\mathcal{A}}, \\ \leq R_{w,i}, & \text{otherwise}, \end{cases} \\
&\quad \forall \mathcal{A} \in \mathcal{W}, \\
&\quad \sum_j g_{i,j} - \sum_j g_{j,i} = \\
&\quad \begin{cases} R_s + R_{w,s}, & \text{if } i = s, \\ -\left(R_s + \sum_{v\in\mathcal{V}, v\neq d} R_{w,v}\right), & \text{if } i = d, \\ R_{w,i}, & \text{otherwise}, \end{cases} \\
&\quad f^{\mathcal{A}}_{i,j} \leq g_{i,j}, \quad g_{i,j} \leq c_{i,j}, \forall (i,j) \in \mathcal{E}, \mathcal{A} \in \mathcal{W},
\end{aligned}
\tag{15}
$$

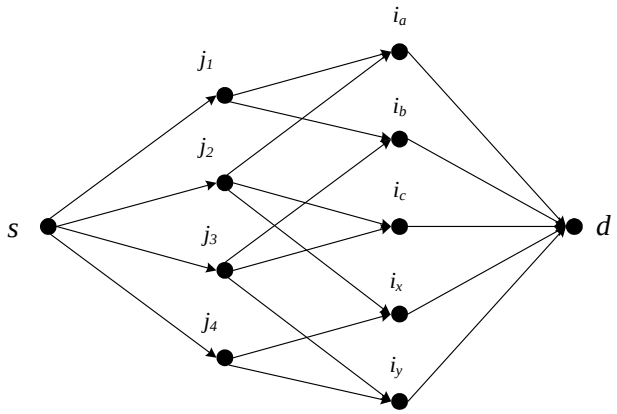

Fig. 2. Example of usefulness of Strategy 2.

where the first equality is the flow conservation for the random keys intended to the virtual sink $d^{\mathcal{A}}$, $f^{\mathcal{A}}_{i,j}$ is the random key flow on link (i,j) for $d^{\mathcal{A}}$, and $g_{i,j}$ is the actual flow on link (i,j); the second equality is the flow conservation for the secret data and random keys; the third set of inequalities requires that the the key flow on each link is less than or equal to the actual flow. The actual flow on each link is constrained by the capacity of each link. Note that under the assumption that different nodes do not have common randomness here we cannot apply the key cancelation and precoding idea in Strategy 1, as after applying the precoding matrix each node may potentially be required to transmit a mixture of all the random keys in the network. Precoding can be applied only if the various key sources can share random keys.

A Scenario 1 example where this strategy is useful is given in Fig. 2, which is obtained by interchanging the source and the sink as well as reversing all the links in Fig. 1. For the sake of simplicity we again assume $p_{i,j} = q_{i,j}$ for all edges (i,j). At most three links in the last layer can be wiretapped. By injecting one local key at node j_2 and two global keys at the source, Strategy 2 can achieve secrecy rate 2. On the other hand, if random keys are only injected at the source, the secrecy rate is at most $\frac{8}{5}$. Let r and w be the secrecy rate and the random key rate at the source, respectively. Let x be the total actual flow on the last layer. To achieve secrecy, we must have $w \geq \frac{3}{5}x$, where the min-cut condition on the last layer requires $r + w \leq x$. Since the source injects all the random keys, the min-cut condition on the first layer requires $r+w \leq 4$. Combining these we obtain $r \leq \frac{8}{5}$, which is strictly less than 2.

This example can be converted to a Scenario 2 example where Strategy 2 outperforms the global key strategy, using a construction similar to that in the previous example for Strategy 1.

Strategy 3: Random keys injected at the source and/or intermediate nodes and some keys from the source are possibly canceled at intermediate nodes and all other keys are decoded at the sink (combination of Strategy 2 and Strategy 3)

From the proposed two strategies, we can see that Strategy

1 seems to be useful if the wiretapped links are upstream of the min-cut while Strategy 2 is useful if the wiretapped links are downstream of the min-cut. In general, these two strategies can be combined to obtain a higher secrecy rate.

We can partition the graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ into two graphs $\mathcal{G}_1 = (\mathcal{V}, \mathcal{E}_1)$ and $\mathcal{G}_2 = (\mathcal{V}, \mathcal{E}_2)$, where each edge e in $\mathcal{V}$ is partitioned into two parallel edges $e^{(1)} \in \mathcal{E}_1$ and $e^{(2)} \in \mathcal{E}_2$ with capacity $c_e^{(1)}$ and $c_e^{(2)}$ ($c_e = c_e^{(1)} + c_e^{(2)}$), respectively. We then apply strategy 1 on graph $\mathcal{G}_1$ and strategy 2 on graph $\mathcal{G}_2$. Combining (14) and (15), we get

$$
\begin{aligned}
&\max\ R_s^{(1)} + R_s^{(2)} \\
&\text{subject to} \sum_{(i,j)\in\mathcal{E}} f_{i,j}^{(1),\mathcal{A}} - \sum_{(i,j)\in\mathcal{E}} f_{j,i}^{(1),\mathcal{A}} = \\
&\quad \begin{cases} R_s^{(1)} + \sum_{(i,j)\in\mathcal{A}} z_{i,j} \min\left(\frac{1-q_{i,j}}{1-p_{i,j}}, 1\right), & \text{if } i = s, \\ -R_s^{(1)} - \sum_{(i,j)\in\mathcal{A}} z_{i,j} \min\left(\frac{1-q_{i,j}}{1-p_{i,j}}, 1\right), & \text{if } i = d^{\mathcal{A}}, \\ 0, & \text{otherwise,} \end{cases} \\
&\quad \forall \mathcal{A} \in \mathcal{W}, \\
&\quad f_{i,j}^{(1),\mathcal{A}} \le z_{i,j} \le c_{i,j}^{(1)},\ \forall (i,j) \in \mathcal{E}, \\
&\quad \sum_j f_{i,j}^{(2),\mathcal{A}} - \sum_j f_{j,i}^{(2),\mathcal{A}} \\
&\quad \begin{cases} = -\sum_{(i,j)\in\mathcal{A}} g_{i,j}^{(2)} \min\left(\frac{1-q_{i,j}}{1-p_{i,j}}, 1\right), & \text{if } i = d^{\mathcal{A}}, \\ \le R_{w,i}, & \text{otherwise,} \end{cases} \\
&\quad \forall \mathcal{A} \in \mathcal{W}, \\
&\qquad \sum_j g_{i,j}^{(2)} - \sum_j g_{j,i}^{(2)} = \\
&\qquad \begin{cases} R_s^{(2)} + R_{w,s}, & \text{if } i = s, \\ -\left(R_s + \sum_{v\in\mathcal{V}, v\neq d} R_{w,v}\right), & \text{if } i = d, \\ R_{w,i}, & \text{otherwise,} \end{cases} \qquad (16) \\
&\quad f_{i,j}^{(2),\mathcal{A}} \le g_{i,j}^{(2)}, \quad g_{i,j}^{(2)} \le c_{i,j}^{(2)},\ \forall (i,j) \in \mathcal{E}, \\
&\quad c_{i,j}^{(1)} + c_{i,j}^{(2)} = c_{i,j},\ \forall (i,j) \in \mathcal{E}.
\end{aligned}
$$

Consider the example in Fig. 2, where all links have unit capacity and $p_{i,j} = q_{i,j}$ for all edges (i,j). Let the middle layer links be 1-5 (from top to bottom) and the last layer links be 6-8 (from top to bottom). Any three of the five links in the middle layer can be wiretapped. We show that the optimal solution must inject random keys at the source and random keys at the second layer nodes and some random keys are canceled at the fifth layer. At the beginning of Strategy 2, we have shown that only global keys at the source is not sufficient. We next consider when random keys are only injected at the second layer nodes. It is clear that if the source does not inject any random key the second layer nodes must inject some random keys otherwise perfect secrecy cannot be achieved. As the maximum secrecy rate is two obtained by the cut-set bound, we can move some portion of random keys from the second layer to the source. Therefore, there are random keys injected at both the source and the second layer nodes. By solving the linear programs (14) and (15), we find that both strategy 1 and strategy 2 achieve a rate 1.2. For strategy 3, a rate 1.3846 is achievable. Even though strategy 3 cannot achieve the outer bound 5/3 given in [11], it outperforms both both strategy 1 and strategy 2. This also shows that strategy 3 is not simply a time sharing strategy between strategy 1 and strategy 2 over the whole network.

For numerical computation of achievable rates in scenarios 1 and 2, we note that the number of possible wiretapping sets, and thus the size of the LPs, are exponential in the size k of each wiretap set, so they are useful for small k.

IV. Conclusion

We have considered the secrecy capacity of wireline networks with restricted wiretapping sets and for unequal capacity links. For such a scenario we have shown that inserting global keys at the source represents a suboptimal strategy. This is in contrast to the case of unrestricted wiretapping sets and equal capacity links where a global key strategy achieves the secrecy capacity. In particular, we have proposed achievable strategies where random keys are canceled at intermediate non-sink nodes, injected at intermediate non-source nodes, or where a combination of these strategies is considered.

References

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

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst.Tech. J.*, vol. 28, pp. 656–715, 1948.

[3] N. Cai and R. Yeung, "Secure network coding," in *Proc. of IEEE ISIT*, June 2002, p. 323.

[4] J. Feldman, T. Malkin, R. Servedio, and C. Stein, "On the capacity of secure network coding," in *Proc. of Allerton Conference on Communication, Control, and Computing*, Sept. 2004.

[5] S. Y. El Rouayheb and E. Soljanin, "On wiretap networks II," in *Proc. of IEEE ISIT*, Nice, France, June 2007, pp. 551–555.

[6] A. Mills, B. Smith, T. Clancy, E. Soljanin, and S. Vishwanath, "On secure communication over wireless erasure networks," in *Proc. of IEEE ISIT*, July 2008, pp. 161–165.

[7] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[8] T. Ho, M. Médard, J. Shi, M. Effros, and D. R. Karger, "On randomized network coding," in *Proc. of Allerton Conference on Communication, Control, and Computing*, Sept. 2003.

[9] T. Cover and J. Thomas, *Elements of Information Theory*, 1991.

[10] R. W. Yeung, *Information Theory and Network Coding*. Springer, August 2008.

[11] T. Cui, T. Ho, and J. Kliewer, "On secure network coding over networks with unequal link capacities," Submitted to IEEE Transactions on Information Theory. Online: arxiv.org, arXiv:0911.467v1, 2009.