Routing for Security in Networks with Adversarial Nodes

Pak Hou Che*, Minghua Chen*, Tracey Ho†, Sidharth Jaggi*, and Michael Langberg‡

*Department of Information Engineering, The Chinese University of Hong Kong
†Department of Electrical Engineering, California Institute of Technology
‡Department of Mathematics and Computer Science, The Open University of Israel

***Abstract*—[1] We consider the problem of secure unicast transmission between two nodes in a directed graph, where an adversary eavesdrops/jams a subset of nodes. This adversarial setting is in contrast to traditional ones where the adversary controls a subset of links. In particular, we study, in the main, the class of routing-only schemes (as opposed to those allowing coding inside the network). Routing-only schemes usually have low implementation complexity, yet a characterization of the rates achievable by such schemes was open prior to this work. We first propose an LP based solution for secure communication against eavesdropping, and show that it is information-theoretically rate-optimal among all routing-only schemes. The idea behind our design is to balance information flow in the network so that no subset of nodes observe "too much" information. Interestingly, we show that the rates achieved by our routing-only scheme are always at least as good as, and sometimes better, than those achieved by "naïve" network coding schemes (*i.e.* the rate-optimal scheme designed for the traditional scenario where the adversary controls links in a network rather than nodes.) We also demonstrate non-trivial network coding schemes that achieve rates at least as high as (and again sometimes better than) those achieved by our routing schemes, but leave open the question of characterizing the optimal rate-region of the problem under all possible coding schemes. We then extend these routing-only schemes to the adversarial node-jamming scenarios and show similar results. During the journey of our investigation, we also develop a new technique that has the potential to derive non-trivial bounds for general secure-communication schemes.**

I. Introduction

The secure network coding problem, introduced by Cai and Yeung [1], considers communication of a secret message in the presence of a computationally-unlimited adversary that eavesdrops on a limited but unknown portion of the network. Most existing work in the literature concerns the multicast uniform link-based adversary case, where all links have equal capacity and the adversary can eavesdrop on a limited number of links. In this case, the maximum secure rate achievable when only the source generates randomness has a simple cut-set characterization [1], and is achieved by a number of existing coding schemes, *e.g.* [2–4].

In this paper we consider the node-based adversary case, where a computationally-unlimited adversary can eavesdrop on a limited number of nodes. Much less is known about this problem. Motivated by complexity considerations, we focus on the class of routing-only schemes for unicast, in which only the source performs coding while non-source nodes perform routing. We formulate a linear program (LP) that balances the amount of information flowing through any subset of nodes, and show that its solution, which involves only simple forwarding, achieves the optimal capacity within the class of routing-only schemes. This class includes schemes involving replication (transmitting multiple copies of a received packet); our result shows that such replication does not improve rate. We further show that our LP-based routing-only schemes achieve rates that are always at least and sometimes higher than rates achieved by naïve application of secure network coding schemes designed for the uniform link-adversary case. Related work by Cui *et al.* [5] considers the link-based secrecy problem with unequal link capacities and/or restricted eavesdropping sets, and give some achievable coding schemes where random keys may be injected or canceled at intermediate nodes. These approaches can sometimes achieve higher rates than our routing-only schemes, though at the expense of higher design and implementation complexity.

We further extend our routing-only schemes to the problem of coding against a node-based jamming adversary that can introduce arbitrary errors at nodes under his control. The problem of network error correction coding against a jamming adversary was introduced by Yeung and Cai [6, 7]. Like the eavesdropping problem, network error correction for the multicast uniform link-based adversary case has been extensively studied, with various existing capacity-achieving code constructions *e.g.* [7–9], while much less is known about the node-based adversary case. Similarly, we show that our routing-only schemes, obtained using the same LP formulation, achieve rates that are never lower and sometimes higher compared to that achieved by naïve application of network error correction codes designed for the uniform link-adversary

The work of S. Jaggi was partially supported by a grant from University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-02/08), and a Direct Grant.

The work of M. Chen was partially supported by a grant from University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-02/08), and a Direct Grant, General Research Fund Project No. 411010 and 411011, from the University Grants Committee of the Hong Kong Special Administrative Region, China and China National 973 projects (grant No. 2012CB315904 and 2013CB336700).

The work of T. Ho was partially supported by NSF grant CNS 0905615.

The work of M. Langberg was partially supported by ISF grant 480/08 and BSF grant 2010075. Work done in part while M. Langberg was at the California Institute of Technology.

[1]The authors are listed in alphabetical order.

case. However, unlike the eavesdropping case, we show that replication can improve rate in the jamming case. Kosut *et al.* [10] also consider node-based jamming adversaries, and introduce non-linear network codes called "polytope codes" in which intermediate nodes carry out comparison and signaling operations. These codes can sometimes achieve higher rates than routing-only schemes, but are more complex.

One "natural" restriction we consider in the jamming scenario, in contrast to most work in the network error-correction literature, is that the adversary is "causal". That is, his jamming actions cannot be based on future transmissions on the network. Under this reasonable assumption, we note that the power of the adversary is significantly weakened compared to the "non-causal" scenario. Specifically, we show that ideas in [11] lead to code designs in which the same rates can be achieved against a *causal omniscient* adversary (one who can see all causal transmissions in the network, and base his jamming strategy as a function of these observations), as are achieved by our schemes against a *localized* adversary (one who can see only see transmissions on edges incoming to him, and base his jamming strategy as a function of these observations).

A. Notational Conventions

Calligraphic symbols such as $\mathcal{N}$ denote sets. Boldface symbols such as $\mathbf{x}$ denote vectors, boldface upper-case symbols such as $\mathbf{X}$ denote random variables, non-boldface lower-case symbols such as x denote particular instantiations of those random variables and non-boldface upper-case symbols such as X denote matrices.

II. Model

A. Network Model

We denote a network by a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the vertex set, and $\mathcal{E}$ is the edge set. There are two pre-specified nodes in $\mathcal{V}$ – specifically s denotes the *source node*, and t denotes the *terminal node*. For notational convenience, we denote by $\overline{\mathcal{V}}$ the set of *internal nodes* $\mathcal{V} \setminus \{s, t\}$, *i.e.*, the subset of nodes of $\mathcal{V}$ excluding the source and terminal nodes. As is common in the network coding literature [12], we assume each edge has unit capacity.[2] For any nodes $v \in \overline{\mathcal{V}}$, let $\mathcal{E}_{in}(v)$ denote the *set of incoming edges* of node v and $\mathcal{E}_{out}(v)$ denote the *set of outgoing edges* of node v. We also define $\mathcal{E}_{in}(\mathcal{A})$ and $\mathcal{E}_{out}(\mathcal{A})$ be the set of incoming and outgoing edges of the nodes $v \in \mathcal{A}$ respectively. For directed edge $e = (v, v') \in \mathcal{E}$, let $head(e)$ denote the head node of the edge e, *i.e.*, $head(e) = v'$, and $tail(e)$ denote the tail node of the edge e, *i.e.*, $tail(e) = v$. The *min-cut of the network between the source s and the terminal t* is denoted by C.

[2]In the node-adversary case this unit-capacity assumption is without loss of generality (not so in the case when the adversary controls edges – see, for instance, [5]).

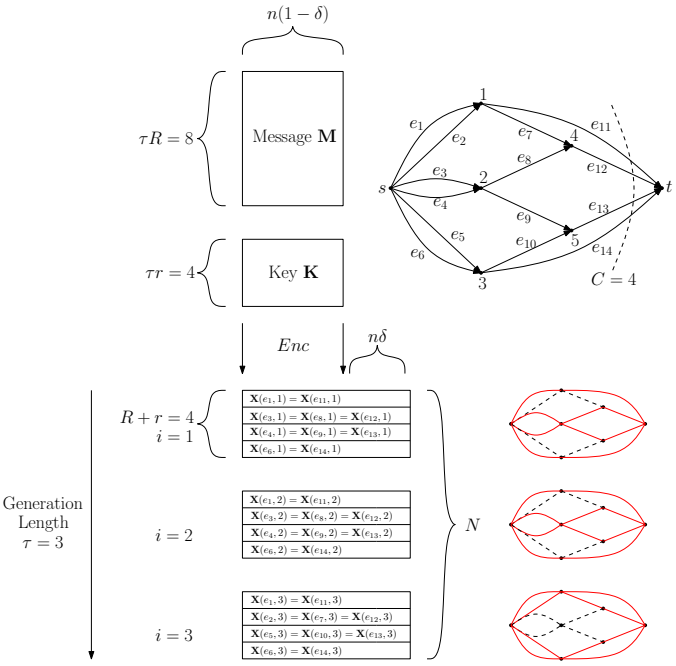

Fig. 1. **Illustrating example for our code parameters:** The source s wishes to transmit a messge $\mathbf{M}$ to the terminal t over a network $\mathcal{G} = (\mathcal{E}, \mathcal{V})$ with min-cut C (in this example $C = 4$), specifically the so-called "cockroach network" example first described in [10], and replicated on the upper right of this figure. To this end, it first organizes $\mathbf{M}$ into $\tau R = 8$ packets (in this example, the generation length $\tau = 3$, and the rate $R = 8/3$), each containing $n(1-\delta)$ symbols over $\mathbb{F}_q$. It then generates a uniformly random key $\mathbf{K}$ which it organizes into τr packets (in this example $r = 4/3$), each containing $n(1-\delta)$ symbols over $\mathbb{F}_q$. Next, the source uses Enc to encode $\mathbf{M}$ and $\mathbf{K}$ into N packets (in this example $N = 12$), each containing n symbols over $\mathbb{F}_q$. In each coding instant i within the generation of length τ the source then injects at most C of these packets into the network (in this example $i \in \{1, 2, 3\}$, the outputs of the encoder are denoted $\mathbf{X}(e, i)$, for appropriate e and i, and routed over the network according to the red paths denoted in the three figures on the right). Finally, the terminal uses Dec to decode $\mathbf{M}$ as $\hat{\mathbf{M}}$. The set of all node encoders, along with the decoder, together comprise the code $\mathcal{C}$.

B. Source Encoding

A *packet* is defined as a length-n vector in the field $\mathbb{F}_q$. Here the *field-size* q, the *number of packets in a generation* N, the *rate* R, the *redundancy* δ, and the *key rate* r are code-design parameters to be specified later. We also define τ to be the *generation length*, which satisfies $N \leq \tau C$, *i.e.*, the number of packets in a generation is at most the generation length times the min-cut. A visual presentation of these parameters are given in Figure 1. The source s has a *message* $\mathbf{M}$ drawn arbitrarily from the set $\{1, 2, \ldots, q^{RNn(1-\delta)}\}$, and a random variable *key* $\mathbf{K}$ distributed uniformly from the set $\{1, 2, \ldots, q^{rNn(1-\delta)}\}$. The source s then encodes the message $\mathbf{M}$ and the key $\mathbf{K}$ by the *source encoder* $Enc(s)$, and generates Nn symbols over $\mathbb{F}_q$, *i.e.*, $Enc : \{1, 2, \ldots, q^{RNn(1-\delta)}\} \times \{1, 2, \ldots, q^{rNn(1-\delta)}\} \to \{1, 2, \ldots, q^{(R+r)Nn}\}$.

C. Linear Network Encoding

[3] There are two types of nodes in the network – "uncorrupted nodes" and "eavesdropping nodes". Nodes in the first category are entirely honest, perform the encoding operations specified in this section, and do not aim to eavesdrop on communications. Nodes in the second category also perform the encoding operations specified in this section, but in addition attempt to eavesdrop on communication as specified in Section II-D.

The random variable $\mathbf{X}(e,i)$ denotes the packet on edge $e \in \mathcal{E}$ at time $i \in \{1,\ldots,\tau\}$. For simplicity, we sometimes omit the time index, and use $\mathbf{X}(e)$ to denote the set of *all* packets going over an edge in a generation. We also denote $\mathbf{X}(\mathcal{E}',i)$ to be set of packets $\{e \in \mathcal{E}' : \mathbf{X}(e,i)\}$ at time $i \in \{1,\ldots,\tau\}$, where $\mathcal{E}' \subseteq \mathcal{E}$.

Each node in the network also has an encoder. As mentioned before, in this work we restrict the internal nodes in the network to "simple" operations, specifically causal linear operations[4] over $\mathbb{F}_q$. That is, the packets transmitted on each outgoing edge of a node v are linear functions of the packets arriving on incoming edges of v.

We distinguish two types of network encoding schemes:

Routing schemes: In a *routing scheme*, the set of packets leaving a node v are subsets of packets incoming to that node. That is, any packet $\mathbf{X}(e,i)$ transmitted on an edge $e \in \mathcal{E}_{out}(v)$ at time $i \in \{1,\ldots,\tau\}$ equals a packet $\mathbf{X}(e',j)$ transmitted on an edge $e' \in \mathcal{E}_{in}(v)$ at time $j \leq i$. Note that this includes "replication", *i.e.*, a node is allowed to transmit multiple copies of a packet it has observed.

Coding schemes: In a *coding scheme*[5], the set of packets leaving a node v are linear combinations of packets incoming to that node[6] that in fact such a strategy can sometimes increase the throughput of networks. These linear combinations can be of two types. In *scalar linear network coding schemes*, each outgoing packet corresponds to a causal linear combination (over $\mathbb{F}_q$) of the packets that v has already observed. That is, for any packet $\mathbf{X}(e,i)$ with $tail(e) \in \overline{\mathcal{V}}$, we have

$$\mathbf{X}(e,i) = \sum_{j \leq i} \sum_{e' : head(e') = tail(e)} \beta(e',e,j)\mathbf{X}(e',j), \quad (1)$$

where the linear network *coding coefficients* $\beta(e,e',j)$ are scalars from $\mathbb{F}_q$.

The choice of coding coefficients is part of the code design, and is explicitly specified later in the schemes we construct. In general they may be chosen either deterministically (as a function of $\mathcal{G}$) or randomly[7]. We define the *network code* $\mathcal{C}$ to be a triple that contains source encoder $Enc(s)$, intermediate node encoders $Enc(v)$ for all $v \in \overline{\mathcal{V}}$ and terminal decoder $Dec(t)$. That is, $\mathcal{C} = (Enc(s), Enc(\overline{\mathcal{V}}), Dec(t))$ – here $Enc(\overline{\mathcal{V}})$ is $Enc(v)$ where $v \in \overline{\mathcal{V}}$.

D. Eavesdropping Model

The *set of nodes eavesdropped by the adversary* $\mathcal{Z}_E$ is a set of at most z_E nodes in $\overline{\mathcal{V}}$, chosen by the adversary as a function of his knowledge of $\mathcal{G}$ and $\mathcal{C}$, prior to the start of communication. That is, $\mathcal{Z}_E \subseteq \overline{\mathcal{V}} : \mathcal{G} \times \mathcal{C} \to \mathcal{P}_{z_E}(\overline{\mathcal{V}})$, where $\mathcal{P}_{z_E}(\overline{\mathcal{V}})$ denotes the set of all subsets of $\overline{\mathcal{V}}$ of size less than or equal to z_E. Given this choice, at time i the adversary observes packets $\mathbf{X}(\mathcal{E}_{in}(\mathcal{Z}_E), j)$ with $j \leq i$, the information on edges incoming to nodes in $\mathcal{Z}_E$ at time $j \leq i$. Given these packets, the adversary's estimate $\hat{\mathbf{M}}$ of $\mathbf{M}$ is allowed to be an arbitrary (possibly probabilistic) function of the packets he observes, the network $\mathcal{G}$, and the network code $\mathcal{C}$.

Adversarial Communication Goals Against a Localized Eavesdropper: Prior to the communication commencing, both $\mathbf{M}$ and $\mathbf{K}$ are known only to the source s itself, and not to any other party. s wishes to transmit the message $\mathbf{M}$ to t over the network $\mathcal{G}$, such that the secrecy and decodability requirements described in (3) and (2) in II-E below are satisfied.

E. Terminal Decoding

1) **Decodability:** We define the *decoding function* of terminal t to be Dec, where $Dec : \{1,2,\ldots,q^{(R+r)Nn}\} \to \{1,2,\ldots,q^{RNn(1-\delta)}\}$. Let $\widehat{\mathbf{M}} = Dec(Enc(\mathbf{M}))$ be the message that the terminal t decodes. The terminal t is required to be able to decode the original message $\mathbf{M}$ with arbitrarily high probability. That is, we need
$$\Pr_{\mathcal{C}}(\widehat{\mathbf{M}} \neq \mathbf{M}) < \epsilon_1. \quad (2)$$
for arbitrarily small ϵ_1.
2) **Secrecy:** The source s transmits the message $\mathbf{M}$ with Δ-*securely* to the terminal t. That is, we require the mutual information between the source's message and the adversary's estimate of it to be "small", that is,
$$I\left(\mathbf{M}; \mathbf{X}(\mathcal{E}_{in}(\mathcal{Z}_E))\right) \leq \Delta.^{8} \quad (3)$$
In particular, if $\Delta = 0$, we say the message $\mathbf{M}$ is *perfectly secure*.

The *overall probability of error*[9] $\Pr_e$ of a transmission scheme can be separated into two parts. The *probability of decoding error* and the *probability of leakage*. The probability of decoding error, denoted by ϵ_1, is $\Pr_{\mathcal{C}}(\widehat{\mathbf{M}} \neq \mathbf{M})$. The

[3] In some models, non-linear coding outperforms linear coding [10]. For complexity reasons, we restrict our attention to linear codes.

[4] In most of the network coding literature, we do not explicitly worry about causality, since a "limited" amount of non-causality can be simulated by pipelining (buffering at each node).

[5] Vector linear network coding schemes are more general than scalar linear network coding schemes – see [13]. In general, all the achievability schemes we present in this paper are based on scalar linear network coding schemes. However, some of the non-achievability results we present work even for vector linear network coding schemes.

[6] In this model we disallow the possibility that an internal node in the network generates private randomness, and uses this to generate outgoing packets. It can be shown in [5].

[7] Each node chooses its linear network coding coefficients uniformly at random over $\mathbb{F}_q$, for instance [14].

[8] Intuitively, this inequality means that the communication scheme leaks at most Δ units of information.

[9] These definitions are for *maximal* probability of error (over all messages $\mathbf{M}$) and hence also work *averaged* over $\mathbf{M}$. The converses we prove *also* work *averaged* over $\mathbf{M}$, and hence are also true for the *worst-case* $\mathbf{M}$.

probability of leakage error, denoted by ϵ_2, is defined as $\Pr_{\mathcal{C}}(I(\mathbf{M};\mathbf{X}(\mathcal{E}_{in}(\mathcal{Z}))) > \Delta)$.

F. Code Parameters

The rate $R = \frac{1}{nN}\log_q|\mathcal{M}|$ is *achievable* if for any $\epsilon > 0$, there exists $\delta > 0$ such that there is a coding scheme with rate at least $R - \delta$ with the overall probability of error $P_e = \Pr_{\mathcal{C}}(\widehat{\mathbf{M}} \neq \mathbf{M}) + \Pr_{\mathcal{C}}(I(\mathbf{M};\mathbf{X}(\mathcal{E}_{in}(\mathcal{Z}))) > \Delta) < \epsilon$ for large enough nN and q.

III. Preliminaries

A. Routing Linear Program

We first introduce the linear program that gives us a baseline routing scheme.

Let $\mathcal{P}$ be the set of all paths from s to t. For path $p \in \mathcal{P}$, a natural internal variable in the **Linear Program 1** (defined in Equations (4) – (6)) is the *flow through path* p, denoted by $F(p)$.

Linear Program 1

$$F(z) = \max \quad \sum_{p\in\mathcal{P}} F(p) - \lambda(z), \tag{4}$$

$$\text{subject to} \quad \forall e \in \mathcal{E}, \quad \sum_{p:p\ni e} F(p) \le 1, \tag{5}$$

$$\forall \mathcal{Z} \subset \overline{\mathcal{V}}, |\mathcal{Z}| \le z, \quad \sum_{p:|p\cap\mathcal{Z}|>0} F(p) \le \lambda(z). \tag{6}$$

In LP1, the maximum value of the objective function in (4) is denoted by $F(z)$. Equation (5) says that the flows passing through a link are bounded by its capacity (which equals 1). Equation (6) bounds the flow through any set of nodes with $|\mathcal{Z}| \le z$. This flow is bounded from above by $\lambda(z)$ – the LP attempts to ensure that not *too much* flow passes through any set of z nodes, while simultaneously maximizing the overall flow. Here, $\lambda(z)$ is also a variable of LP1. The choice of rate R and key-rate r for each of our routing scheme depends critically on $\lambda(z)$.

Remark 1. In this linear program the rate of the key is set of $r = \lambda(z)$, but the key rate in [1] equals the maximum number of incoming links of any subset of z intermediate nodes $\max\Gamma_{in}(z)$. Since $\lambda(z) \le \max\Gamma_{in}(z)$ for any subset of z intermediate nodes, the rate obtained by this LP is never worse (and often significantly better than) that obtained in [1].

Lemma 1. *If the optimal solution for LP1 is with* $\sum_{p\in\mathcal{P}} F(p) < C$. *Then, there is another optimal solution satisfying* $\sum_{p\in\mathcal{P}} F(p) = C$.

Proof. Suppose the optimal solution of LP1 is $((\forall p \in \mathcal{P}, F_0(p)), \lambda_0)$ such that the sum of all flows $\sum_{p\in\mathcal{P}} F_0(p) < C$ and let $F_0 = \sum_{p\in\mathcal{P}} F_0(p)$. So, the optimal objective function is $F_0 - \lambda_0$. Note that in this network, we can still inject $F_{in} = C - F_0$ fraction of flows into the network since the sum of all flows $F_0 < C$. Then, we have the sum of all flows $\sum_{p\in\mathcal{P}} F'(p) = C$, where $F'(p)$ is the new flow assignment after F_{in} injections on the original flow F_0. Denote the increment of λ_0 after inject F_{in} into the original λ_{in}, we have $\lambda_{in} \le F_{in}$. Also, we have $\forall \mathcal{Z} \subset \overline{\mathcal{V}}$, $\sum_{p:p\ni v_i, i\in\mathcal{Z}} F'(p) \le \lambda_0 + \lambda_{in}$, where $\lambda_{in} \le F_{in}$. This means, the increment of the flows that passing through $\mathcal{Z}$ is λ_{in}. So, the objective function after the flow injection is $C - (\lambda_0 + \lambda_{in}) \ge C - (\lambda_0 + F_{in}) = F - \lambda_0$. Since $F - \lambda_0$ is optimal, and so as $C - (\lambda_0 + \lambda_{in})$. ∎

By Lemma 1, LP1 can be reduced into the following linear program.

Linear Program 1'

$$\begin{aligned} \max \quad & C - \lambda(z) \\ \text{subject to} \quad & \forall e \in \mathcal{E}, \quad \sum_{p:p\ni e} F(p) \le 1 \\ & \forall \mathcal{Z} \subset \overline{\mathcal{V}}, |\mathcal{Z}| \le z, \sum_{p:p\ni i, i\in Z} F(p) \le \lambda(z) \\ & \sum_{p\in\mathcal{P}} F(p) = C \end{aligned}$$

Note that the size of $\mathcal{P}$ is exponential in the network size, having an exponential number of variables. In order to reduce the complexity of solving the linear program, we consider the following linear program which is equivalent to LP1'. As in the max-flow min-cut theorem, instead of using the flow $F(p)$ on the paths $p \in \mathcal{P}$ as the variables, we use the flow $F(e)$ on the edges $e \in \mathcal{E}$ as the variables in the following linear program.

Linear Program 2

$$\begin{aligned} \max \quad & C - \lambda(z) \\ \text{subject to} \quad & \forall v \in \overline{\mathcal{V}}, \sum_{e:e\in\mathcal{E}_{in}(v)} F(e) = \sum_{e:e\in\mathcal{E}_{out}(v)} F(e) \\ & \forall \mathcal{Z} \subset \overline{\mathcal{V}}, |\mathcal{Z}| \le z, \sum_{e:e\in\mathcal{E}_{in}(v), v\in\mathcal{Z}} F(e) \le \lambda(z) \\ & \sum_{e:e\in\mathcal{E}_{out}(s)} F(e) = \sum_{e:e\in\mathcal{E}_{in}(t)} F(e) = C \end{aligned}$$

Remark 2. Due to the condition $|\mathcal{Z}| \le z$, there are $\binom{|\overline{\mathcal{V}}|}{z}$ constraints in LP2, which is still exponential in z. However, the number of variables is linear in $|\mathcal{E}|$. In comparison, in LP1', there are exponentially many constraints and exponential variables in the linear program.

IV. Main Results

We characterize the performance of routing solutions to the secure communication problem with adversarial nodes. The routing solution is provided by LP1'. An adversary is said be to *localized* if it only has a casual "localized" view of network traffic, depending on the nodes in $\mathcal{Z}$ it controls. An adversary is said to be *omniscient* if it has a "global" view of the network traffic. For localized eavesdropping, we use Vandermonde matrix as the encoding matrix at the source. We use the encoding procedure of [11] in the localized jamming/localized eavesdropping and jamming/omniscient jamming cases.

Theorem 1. *$R = C - \lambda(z)$, where $\lambda(z)$ is obtained by an optimal solution from LP1', is achievable for localized eavesdropping.*

We further show that this achievable scheme, which does not involve replication, is optimal for localized eavesdropping among the class of all routing schemes, which in general allow replication.

Theorem 2. *The achievable scheme for localized eavesdropping is optimal among routing schemes.*

V. Proofs

A. Eavesdropping

Proof of Theorem 1:

By LP1', each path p is assigned a flow $F(p)$. It is clear that $F(p)$ is rational for any $p \in \mathcal{P}$ since all the coefficients in LP1' are rational. Let τ be the minimum positive integer such that $\tau F(p) \in \mathbf{Z}^+$. One may consider τ as a factor by which the capacity of each link is scaled, or as the time in a generation, that is, there are C packets transmitted at time i for $i \in \{1, 2, \ldots, \tau\}$ and there are $N = \tau C$ packets transmitted to terminal t in each section. Now, let us consider the following scheme with rate $R = C - \lambda$.

Source: Let $\mathbf{m} = (m_1, \ldots, m_{\tau R})$ be the message transmitted, and $\mathbf{k} = (k_1, \ldots, k_{\tau\lambda})$ be the *keys*. The keys are uniformly random over $\mathbb{F}_q$, and are unknown to the eavesdropper. The messages and the keys are coded together at the source before transmission over the network. Let $\mathbf{V}$, a Vandermonde matrix with size $N \times N$, be the source encoder matrix. Let $\mathbf{x} = (\mathbf{m}\ \mathbf{k})^T$ and the information to be transmitted from s be $\mathbf{Vx}$. Each encoded packet corresponds to an entry of $\mathbf{Vx}$.

Intermediate Nodes: The encoded packets are transmitted via the routes given by LP1'.

Terminal: At terminal t, the terminal t simply multiplies $\mathbf{V}^{-1}$ with the received information $\mathbf{Vx}$. Hence, $\mathbf{x}$ is recovered.

For any $\mathcal{Z} \subset \overline{\mathcal{V}}$, the total amount of flow passing through $\mathcal{Z}$ is at most $\tau\lambda$, which are linearly independent combinations of $\tau\lambda$ uniform random symbols that are not known by the eavesdropper. Thus, the eavesdropper does not obtain any information about the original message no matter which set of $\mathcal{Z}$ nodes he observes. Therefore, the rate $R = C - \lambda$ is achievable by the above scheme. ∎

Due to space limitation, we only give a sketch proof of Theorem 2. The full proof is given in [17].

Sketch Proof of Theorem 2:

The proof involves two main steps:

Step 1: We first show that there is a routing scheme *without* replicating that performs at least as well as any routing scheme *with replicating*.[10]

Step 2: Next, we give a more nuanced argument to show that in fact, for an optimal routing scheme, even the packets leaving the source must be essentially (statistically) independent by the Slepian-Wolf Theorem [15]. Let $p_1, p_2, \ldots, p_k$ be all the paths from the source s to the terminal t. Denote a new random variable $\widehat{\mathbf{P}}(j)$ for each path p_j from the source s to the terminal t with certain properties.

[10]We defined replicating routing schemes as those in which an internal node transmits the same incoming packet at least twice on outgoing edges.

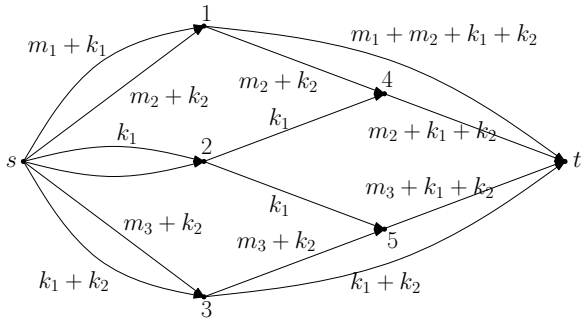

Fig. 2. An example, for the cockroach network, of a "careful coding" scheme that beats any routing scheme in the **Localized Eavesdropping** model. It can be verified by solving **Linear Program 1** that the routing-only rate equals $8/3$. However, it can be verified that in the scenario that $z = 1$, *i.e.*, at most one node is eavesdropped on, the scheme outlined in this figure ensures that a rate R of 3 is perfectly securely achievable.

We now use the properties of the new routing scheme to argue that in fact the rate specified by the solution of LP1 is also an outer bound on the achievable rate for routing-only schemes.

$$
\begin{aligned}
mR &= H\left(\mathbf{M}^m\right) && (7)\\
&\le H\left(\mathbf{M}^m, \widehat{\mathbf{P}}(\mathcal{Z})^m\right) && (8)\\
&\le H\left(\mathbf{M}^m|\widehat{\mathbf{P}}(\mathcal{Z})^m\right) + I\left(\mathbf{M}^m; \widehat{\mathbf{P}}(\mathcal{Z})^m\right) && (9)\\
&\le H\left(\mathbf{M}^m|\widehat{\mathbf{P}}(\mathcal{Z})^m\right) - H\left(\mathbf{M}^m|\widehat{\mathbf{P}}(\mathcal{Z})^m, \overline{\widehat{\mathbf{P}}(\mathcal{Z})}^m\right)\\
&\quad + H\left(\mathbf{M}^m|\widehat{\mathbf{P}}(\mathcal{Z})^m, \overline{\widehat{\mathbf{P}}(\mathcal{Z})}^m\right) + m\Delta && (10)\\
&\le I\left(\mathbf{M}; \overline{\widehat{\mathbf{P}}(\mathcal{Z})}^m|\widehat{\mathbf{P}}(\mathcal{Z})^m\right)\\
&\quad + 1 + \epsilon mR + m\Delta && (11)\\
&\le H\left(\overline{\widehat{\mathbf{P}}(\mathcal{Z})}^m\right) + 1 + \epsilon mR + m\Delta && (12)\\
&= mC - mH\left(\widehat{\mathbf{P}}(\mathcal{Z})\right) + 1 + \epsilon mR + m\Delta && (13)
\end{aligned}
$$

where $\overline{\widehat{\mathbf{P}}(\mathcal{Z})}$ denotes the random variables $\{\widehat{\mathbf{P}}(1), \ldots, \widehat{\mathbf{P}}(k)\} \setminus \widehat{\mathbf{P}}(\mathcal{Z})$. Inequality (11) holds by Fano's inequality, and the last equality holds due to the "near-independence" of $\widehat{\mathbf{P}}(j)$, as argued in Step 1 (the remaining steps follow from standard information identities and inequalities). Hence $R \le \frac{1}{1-\epsilon}\left[C - H\left(\widehat{\mathbf{P}}(\mathcal{Z})\right) + \frac{1}{m} + \Delta\right]$. But this entropy inequality must hold for each set $\mathcal{Z}$. But these, along with the entropy inequalities constraining the rate on each edge to be at most 1, match the corresponding achievable rate given by LP1'. ∎

B. Encoding Complexity versus Rate-optimal Loss

Note that the size of encoding matrix is determined by $N = \tau C$. Since τ is the parameter determined by LP1', the encoding complexity is large when τ is also large. In this section, we will give the rate loss when we fix τ.

	A. Eavesdropper	B. Localized jammer	C. Localized eavesdropper/jammer	D. Omniscient jammer
1.1 Naïve coding	$C-\Gamma_{in}(\mathcal{Z})$ [1]	$C-\Gamma_{out}(\mathcal{Z})$ [11] if $\Gamma_{out}(\mathcal{Z})<C/2$	$C-\Gamma_{in}(\mathcal{Z})-\Gamma_{out}(\mathcal{Z})$ [16] if $\Gamma_{in}(\mathcal{Z})+\Gamma_{out}(\mathcal{Z})<C$	$C-\Gamma_{out}(\mathcal{Z})$ [11] if $\Gamma_{out}(\mathcal{Z})<C/2$
1.2 Toy example	2	0	0	0
2.1 Routing	$=C-\lambda(z)$	$\geq C-\lambda(z)$ if $\lambda(z)<C/2$	$\geq C-2\lambda(z)$ if $\lambda(z)<C/2$	$\geq C-\lambda(z)$ if $\lambda(z)<C/2$
2.2 Toy example	$8/3$	$8/3$	$4/3$	$8/3$
3.1 Coding	$\geq C-\lambda(z)$ [5]	$\geq C-\lambda(z)$	$\geq C-2\lambda(z)$	$\geq C-\lambda(z)$
3.2 Toy example	3	3	open	3

Fig. 3. Here, $\lambda(z)$ is the optimal value of the variable λ in LP1'. Eavesdropping: In the cockroach network that first describe in [10], 1 eavesdropped node can be regarded as 2 eavesdropping links (since each node has 2 incoming links). So, the best achievable rate for this example is 2 by [1]. In our routing scheme, the rate $R=8/3$ is achievable for the cockroach network example – see Figure 1. We Further show that the rate $R=3$ is achievable in the cockroach network example if smart coding is allowed – see Figure 2. A more general achievable scheme is shown in [5]. More examples are shown in [17] for localized jamming, localized eavesdropping and jamming, and omniscient jamming cases.

Lemma 2. *For τ' fixed, denote the corresponding rate to be R'. We have $R-R'<\frac{|\mathcal{E}|}{\tau'}$.*

Proof. Solving the bf Linear Program 2 of network $\mathcal{G}$ gives us the flow value $F(e)$ on each link $e\in\mathcal{E}$. Reduce the network $\mathcal{G}$ by setting each link to be capacity $F(e)$ and multiply τ' to each link of the network $\mathcal{G}$. So, each link has capacity equals to $\tau' F(e)$, denote this scaled network to be $\mathcal{G}'$. Denote the network $\mathcal{G}''$ to be the quantization on each link e to be integer value, *i.e.*, taking $\lfloor \tau' F(e) \rfloor$. So, the capacity on each link e is reduced by a value at most 1. Therefore, the capacity of the network $\mathcal{G}''$ is reduced at most $|\mathcal{E}|$ from the network $\mathcal{G}'$. Therefore, the capacity of the network $\mathcal{G}$ by fixing τ' reduced is at most $\frac{|\mathcal{E}|}{\tau'}$. Hence, $R-R'<\frac{|\mathcal{E}|}{\tau'}$. ∎

VI. Further Extensions

In our full technical report (see [17]), we defined 3 types of jamming adversaries: **localized jamming**, **localize eavesdropping and jamming** and **omniscient jamming**. Using the same routing scheme provided by LP1', we obtained the following results.

Theorem 3. *$R=C-\lambda(z)$, where $\lambda(z)$ is the variable of LP1', is achievable for localized jamming.*

Theorem 4. *$R=C-2\lambda(z)$, where $\lambda(z)$ is the variable of LP1', is achievable for localized eavesdropping and jamming.*

Theorem 5. *$R=C-\lambda(z)$, where $\lambda(z)$ is the variable of LP1', is achievable for omniscient jamming.*

References

[1] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. 2002 IEEE Int. Symp. Information Theory (ISIT 2002)*, Lausanne, Switzerland, Jun./Jul. 2002, p. 323.

[2] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the capacity of secure network coding," in *Proc. 42nd Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Sep./Oct. 2004.

[3] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, 2011.

[4] S. E. Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type ii," *IEEE Transactions on Information Theory*, vol. 58, no. 3, 2012.

[5] T. Cui, T. Ho, and J. Kliewer, "Achievable strategies for secure network coding for general networks," in *Information Theory and Applications Workshop*, 2010.

[6] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 19–36, 2006.

[7] N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 37–54, 2006.

[8] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard, and M. Effros, "Resilient network coding in the presence of byzantine adversaries," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2596 –2603, June 2008.

[9] D. Silva, F. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3951–3967, Sept. 2008.

[10] O. Kosut, L. Tong, and D. Tse, "Nonlinear network coding is necessary to combat general byzantine attacks," in *Proc. of the 47th annual Allerton conference on Communication, control, and computing*, September 2009, pp. 593 – 599.

[11] S. Jaggi, M. Langberg, T. Ho, and M. Effros, "Correction of adversarial errors in networks," in *Proc. 2002 IEEE Int. Symp. Information Theory (ISIT 2002)*, Adelaide, Australia, 2005.

[12] R. Kötter and M. Médard, "An algebraic approach to network coding," *IEEE Transactions on Networking*, vol. 11, no. 5, pp. 793–795, Oct. 2003.

[13] S. Jaggi, M. Effros, T. Ho, and M. Médard, "On linear network coding," 2004, invited talk, 42nd annual Allerton conference on Communication, control, and computing.

[14] T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, and B. Leung, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[15] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[16] H. Yao, D. Silva, S. Jaggi, and M. Langberg, "Network codes resilient to jamming and eavesdropping," in *2010 IEEE International Symposium on Network Coding (NetCod)*, June 2010.

[17] P. H. Che, M. Chen, T. Ho, S. Jaggi, and M. Langberg, "Routing for security in networks with adversarial nodes", Project website: http://personal.ie.cuhk.edu.hk/~cph010/project-node_security.html