Network Codes Resilient to Jamming and Eavesdropping

Hongyi Yao, Tsinghua University
Danilo Silva, State University of Campinas
Sidharth Jaggi, Chinese University of Hong Kong
Michael Langberg, The Open University of Israel

***Abstract*—We consider the problem of communicating information over a network secretly and reliably in the presence of a hidden adversary who can eavesdrop and inject malicious errors. We provide polynomial-time, rate-optimal distributed network codes for this scenario, improving on the rates achievable in [1]. Our main contribution shows that as long as the sum of the adversary's jamming rate Z_O and his eavesdropping rate Z_I is less than the network capacity C, (*i.e.,* $Z_O + Z_I < C$), our codes can communicate (with vanishingly small error probability) a single bit correctly and without leaking any information to the adversary. We then use this to design codes that allow communication at the optimal source rate of $C - Z_O - Z_I$, while keeping the communicated message secret from the adversary. Interior nodes are oblivious to the presence of adversaries and perform random linear network coding; only the source and destination need to be tweaked. In proving our results we correct an error in prior work [2] by a subset of the authors in this work.**

I. Introduction

A source Alice wishes to transmit information to a receiver Bob over a network containing a malicious adversary Calvin. Such scenarios face at least two challenges – Calvin might eavesdrop on private communications, or he might disrupt communications by injecting fake information into the network. In the network coding model this second danger may be even more pronounced since all nodes, including honest ones, mix information. In this case, even a small number of fake packets injected by Calvin may end up corrupting *all* the information flowing in the network, causing decoding errors.

In this work we consider the *secrecy* and *error control* issues together. Namely, we design schemes that allow reliable network communications in the presence of an adversary that can both jam and eavesdrop, without leaking information to him. In particular, suppose the network's min-cut from Alice to Bob is C, and Calvin eavesdrops on Z_I links and corrupts Z_O links[1]. We demonstrate schemes that are distributed, computationally efficient to design and implement, and can be used to communicate a *single* bit secretly and without error. We then use this scheme as a tool to improve on prior work [3], and achieve a provably optimal rate of $C - Z_O - Z_I$.

Related problems have been considered in the past. Prior results may be classified in the following three categories.

For networks containing adversaries that only eavesdrop on some links (without jamming transmissions), the work of [4] provided a tight information-theoretic characterization of the *secrecy capacity*, *i.e.*, the optimal rate achievable without leaking any of Alice's information to Calvin. Efficient schemes achieving this performance were proposed by [5]–[7]. Cryptographically (but not information-theoretically) secret schemes for this scenario were also considered in [8].

For networks containing adversaries with unlimited eavesdropping capabilities and limited jamming capabilities, prior related work has focused primarily on the detection of Byzantine errors [9], non-constructive bounds on the achievable *zero-error* rates [10], [11], and network error-correcting codes [12] (which have high design complexity) and [2], [3], [13], [14] (which have low design complexity). Results for this setting are also available under cryptographic assumptions [15], [16].

The scenario closest to the one considered in this work, with limitations on both Calvin's eavesdropping power Z_I and his jamming power Z_O, have been considered in [1]–[3], [17], [18]. Under the requirement of *zero* error probability, the maximum rate of secret and reliable communication is given by $C - 2Z_O - Z_I$. Schemes achieving this rate have been proposed in [1], [18] (high design complexity schemes) and [17], [19], [20] (low design complexity schemes). The optimality of such a rate has been shown in [1] for single-letter coding and in [20] for block coding.

If the requirement of zero error probability is relaxed to *vanishingly small* error probability, as considered here, then higher rates may be achieved. In particular, the work in [3] provided computationally efficient communication schemes (but with no guarantees on secrecy) at rate $C - Z_O$ as long as the technical requirement $C > 2Z_O + Z_I$ was satisfied. Work by a subset of the authors of this paper claimed in [2] to improve this technical requirement to $C > Z_O + Z_I$. As we demonstrate in Section VIII, prior proof of the claim was incorrect, and Section II gives a correct proof of the claim. Combining these results with the secrecy scheme of [7] allows us to obtain the optimal rate of $C - Z_O - Z_I$ when secrecy constraints are incorporated.

The work of Hongyi Yao was supported in part by National Natural Science Foundation of China Grant 60553001, the National Basic Research Program of China Grant 2007CB807900 and 2007CB807901. The work of Danilo Silva was supported by FAPESP grant 2009/15771-7. The work of Sidharth Jaggi was supported RGC GRF grant 412608, 411008, and 411209, RGC AoE grant on Institute of Network Coding, established under the University Grant Committee of Hong Kong, CUHK MoE-Microsoft Key Laboratory of Humancentric Computing and Interface Technologies, Direct Grant (Project Number 2050397) of The Chinese University of Hong Kong, and two gift grants from Microsoft and Cisco. The work of Michael Langberg was supported in part by ISF grant 480/08.

[1]We consider a model where network links rather than nodes are eavesdropped and corrupted; eavesdropping on a node is equivalent to eavesdropping on links incoming to it, and corrupting a node is equivalent to corrupting the links outgoing from it.

978-1-4244-7190-4/10/$26.00 ©2010 IEEE

II. Main Results

The main results of this work are Theorems 1 and 2.

Theorem 1: If $C > Z_O - Z_I$ then Alice can communicate a single bit correctly to Bob (while keeping it secret from Calvin) using codes of computational complexity $O(\text{poly}(C, \log_2 q))$ and error probability $O(q^{-C})$.

Combining the codes in Theorem 1 with the "shared-secret" codes in [3] then gives us the following theorem.

Theorem 2: No rate higher than $C - Z_O - Z_I$ is achievable. A rate of $C - Z_O - Z_I$ is achievable with codes of computational complexity $O(n\text{poly}(C, \log_2 q))$.

Note: In [1], Ngai et al show that $C - 2Z_O - Z_I$ is an upper bound on the rate, assuming no error events, and single-letter coding (respectively equations (87) and (65) in their proof). Our work achieves higher rates by instead assuming asymptotically negligible probability of error, and block coding.

A. High-level overview of proofs and techniques

We first show in Section IV that $C - Z_O - Z_I$ is an upper bound on the rate at which a secret message can be correctly transmitted from Alice to Bob, by demonstrating an attack that Calvin can use to successfully disrupt communication if Alice tries to communicate at any higher rate. We then construct efficient codes that essentially achieve rate $C - Z_O - Z_I$. Our codes consist of the three layers described below. All the three layers are embedded along with Alice's message into her packets and then transmitted through the network using random linear network codes.

Secret-sharing layer: In Section VI we first prove Theorem 1 by showing how to communicate a single bit secretly and correctly over a network containing adversaries that can jam and eavesdrop, as long as $C > Z_I + Z_O$. This layer is important for the error-control layer described later, and can be implemented via a "small" header appended to each network coded packet. When k secret bits are to be shared, the scheme is repeated k times in each transmitted packet header, for a secret-sharing header of total length $C + kC(C - Z_I)$. The secret-sharing layer consisting of the following components:

1. *Identity matrix:* As standard in random linear network coding [21], [13], the identity matrix I_C is appended to convey to the receiver information about the linear transform induced by the random linear network code.

2. *Bit matrices:* For each secret bit, $i \in \{1, \ldots, k\}$, if the ith secret bit equals 0, the $(C - Z_I) \times C(C - Z_I)$ matrix S^i (over $\mathbb{F}_q$) is chosen as a zero matrix; otherwise, S^i is chosen independently and uniformly at random from all $(C - Z_I) \times C(C - Z_I)$ matrices. We refer to S^i as a *bit matrix*. The idea is that the rank of the matrices corresponding to bit 0 is much smaller than the rank of the matrices corresponding to bit 1—due to the limitation on the numbers of packets Calvin can observe or inject, with high probability he cannot change the rank of the corresponding received matrix by too much. Details are given in Lemma 3.

3.*Random matrix:* Alice adapts the scheme of [7] to keep the bit matrices secret from Calvin. That is, for each secret bit i that Alice wishes to communicate to Bob, she combines the bit matrix S^i with a random noise matrix N^i (at rate Z_I). It can be shown that it is impossible for Calvin to glean any useful information (since it can only eavesdrop at rate Z_I).

Section VII combines the secrecy layer with the two other layers described below to complete our code construction.

Secrecy layer: As done with the random matrices N^i in the secret-sharing layer above, a random matrix N is used to preserve the secrecy of the source message S (of rate $C - Z_O - Z_I$), yielding a encoded matrix M (of rate $C - Z_O$).

Error control layer: In this layer Alice uses the "shared-secret" scheme outlined in Theorem 1 of [3]. That is, Alice first takes a secret linear hash to her secrecy-encoded message M to generate a small hash value. Both the linear hash and the resulting hash value (say k bits in all) are transmitted to Bob using the secret-sharing layer. Alice then combines her data with a zero-value matrix (of rate Z_O), such that Bob can use the secret hash to *distill* Alice's codeword M from the corrupted information reaching the destination.

Vis-a-vis our secret-sharing scheme of Section VI, the work of [2] (by a subset of the authors of this work) claimed to have the same result. However, we show in Section VIII that the scheme proposed in [2] is incorrect by giving an attack that Calvin can use to ensure that Bob has a significant probability of decoding error.

III. Network Model and Problem Statement

We use the general model proposed in [3]. To simplify notation we consider only the problem of communicating from a single source to a single destination[2].

A. Network Model

Alice communicates to Bob over a network with an attacker (adversary) Calvin hidden somewhere in it. Calvin aims to disrupt the transfer of information from Alice to Bob and in the meantime eavesdrop the information Alice sends. He can observe some of the transmissions, and can inject his own fake transmissions.

Calvin is computationally unbounded, knows the encoding and decoding schemes of Alice and Bob, and the network code implemented by the interior nodes. He also knows the network topology, and he gets to choose which network links to eavesdrop on and which ones to corrupt.

The network is modeled as a directed and delay-free graph whose edges each have capacity equal to one symbol of a finite field of size q, $\mathbb{F}_q$, per unit time[3]. All computations are over $\mathbb{F}_q$. The *network capacity*, denoted by C, is the *min-cut from source to destination*[4].

[2]Similarly to many network coding algorithms, our techniques generalize to multicast problems.

[3]For ease of presentation edges with non-unit capacities are not considered here (as in [3], they may be modeled via block coding and parallel edges).

[4]For the corresponding multicast case, C is defined as the minimum of the min-cuts over all destinations. It is well-known that C also equals the time-average of the maximum number of packets that can be delivered from Alice to Bob, assuming no adversarial interference, i.e., the *max flow*.

Each packet contains n symbols from $\mathbb{F}_q$. Alice's message is denoted $S \in \mathcal{S}$. To send this to Bob over the network, Alice encodes it into a matrix $X \in \mathbb{F}_q^{C\times n}$, possibly using a *stochastic encoder*[5]. The i^{th} row in X is Alice's i^{th} packet. As in [21], Alice and internal nodes in take random linear combinations of their observed packets to generate their transmitted packets.

Analogously to how Alice generates X, Bob organizes received packets into a matrix Y. The i^{th} received packet corresponds to the i^{th} row of Y. The random linear network code used by Alice and all internal nodes induces a linear transform A from X to Y, such that $Y = AX$ when no error is induced by the adversary[6]. Thus Y is a matrix in $\mathbb{F}_q^{C\times n}$, and $A \in \mathbb{F}_q^{C\times C}$. Hereafter we assume that the matrix A is invertible, which happens with high probability if q is sufficiently large [21].

Calvin can eavesdrop on Z_I edges, and can inject (possibly fake) information at Z_O locations[7], in the network. The matrix received by Bob is then $Y = AX + Z$, where Z corresponds to the information injected by Calvin as seen by Bob. Note that the limitation of Calvin's jamming capacity implies that $\mathsf{rank}(Z) \leq Z_O$. Similarly, Calvin's observation can be described as a matrix $W = BX$, where $B \in \mathbb{F}_q^{Z_I\times C}$ is the linear transform undertaken by X as seen by Calvin.

B. Problem Statement

Alice wishes to communicate with Bob with perfect secrecy and vanishingly small error probability. That is, Alice's scheme is *perfectly secret* if

$$I(S;W) = 0 \quad \forall B \in \mathbb{F}_q^{Z_I\times C} \tag{1}$$

i.e., Calvin obtains no information about Alice's message. The *error probability* is the probability that Bob's reconstruction $\hat{S}$ of Alice's information S is inaccurate, i.e., $P[\hat{S} \neq S]$. We consider the error probability of the worst-case scenario[8]. Namely, a scheme has error probability less than ϵ if $P[\hat{S} \neq S] < \epsilon \quad \forall A, Z$, where A is assumed to be nonsingular, and $\mathsf{rank}(Z) \leq Z_O$. The *rate* R of a scheme is the number of information bits of information Alice transmits to Bob, amortized by the size of a packet in bits, i.e., $R = \frac{1}{n}\log_q|\mathcal{S}|$. The rate R is said to be *achievable* if for any $\epsilon > 0$, any $\delta > 0$, and sufficiently large n, there exists a perfectly secret block-length-n network code with rate at least $R - \delta$ and a probability of error less than ϵ.

IV. Converse for Theorem 2

We start by presenting an attack that Calvin may use to force the achievable rate to at most $C - Z_O - Z_I$, thereby demonstrating that this is indeed an upper bound on the achievable rate. Let $\{e_1, e_2, ..., e_C\}$ be a set of edges that form a cut from Alice to Bob. Calvin jams the edges in $\{e_1, e_2, ..., e_{Z_O}\}$ by adding random errors on them. Further, Calvin eavesdrops on edges in $\{e_{Z_O+1}, e_{Z_O+2}, ..., e_{Z_O+Z_I}\}$. Let $\mathbf{X}$ be the random variable denoting Alice's information. Let $\mathbf{Y}_j$, $\mathbf{Y}_e$, and $\mathbf{Y}_u$ be the random variables denoting the packets carried by the jammed edges $\{e_1, e_2, ..., e_{Z_O}\}$, eavesdropped edges $\{e_{Z_O+1}, e_{Z_O+2}, ..., e_{Z_O+Z_I}\}$, and untouched edges $\{e_{Z_O+Z_I+1}, e_{Z_O+Z_I+2}, ..., e_C\}$ respectively. Let $\mathbf{Y}$ be the random variable denoting the packets received by Bob. Then

$$\begin{aligned}
nR &= H(\mathbf{X}) = H(\mathbf{X}|\mathbf{Y}) + I(\mathbf{X};\mathbf{Y}) && (2)\\
&\leq 1 + \epsilon nR + I(\mathbf{X};\mathbf{Y}) && (3)\\
&\leq 1 + \epsilon nR + I(\mathbf{X};\mathbf{Y}_j,\mathbf{Y}_e,\mathbf{Y}_u) && (4)\\
&= 1 + \epsilon nR + I(\mathbf{X};\mathbf{Y}_e,\mathbf{Y}_u) && (5)\\
&= 1 + \epsilon nR + I(\mathbf{X};\mathbf{Y}_e) + I(\mathbf{X};\mathbf{Y}_u|\mathbf{Y}_e) && (6)\\
&= 1 + \epsilon nR + I(\mathbf{X};\mathbf{Y}_u|\mathbf{Y}_e) && (7)\\
&\leq 1 + \epsilon nR + H(\mathbf{Y}_u) && (8)\\
&\leq n\left[(C - Z_I - Z_O) + \epsilon R + \frac{1}{n}\right]. && (9)
\end{aligned}$$

Here (2) follows from the fact that Alice's message is uniformly distributed over $\mathbf{X}$, (3) from Fano's inequality, (4) from the data processing inequality, (5) since Calvin adds random noise on the edges he jams and so $\mathbf{Y}_j$ is independent of $(\mathbf{X}, \mathbf{Y}_e, \mathbf{Y}_u)$, (6) by the chain rule for mutual information, (7) from the fact that information-theoretic secrecy is required and so $I(\mathbf{X};\mathbf{Y}_e) = 0$, (8) by the fact that conditioning reduces entropy and the definition of mutual information, and finally (9) by the fact that there are at most $C - Z_I - Z_O$ links corresponding to the random variable $\mathbf{Y}_u$ and the alphabet-size upper bound on entropy. Requiring $\epsilon \to 0$ as $n \to \infty$ gives the required result.

TABLE I
Summary of commonly used notation

Notation	Meaning
C	Capacity
Z_I	Eavesdropping rate
Z_O	Jamming rate
n	Packet length
q	Field size
$Q = q^C$	Extension field size

V. Auxiliary Tools

A. Secrecy Coding

Consider a special case of the problem where Calvin can eavesdrop $Z_I < C$ packets but cannot jam any packets ($Z_O = 0$). Below, we review a construction of a perfectly secret scheme that asymptotically achieves the maximum possible rate (i.e., the secrecy capacity) $R = C - Z_I$. The scheme, proposed in [7], is based on MRD codes. (For more details on MRD codes, see [7].)

[5]The random coin tosses made by Alice as part of her encoding scheme are not known to either Calvin or Bob.

[6]For the ease of notation we assume Bob removes redundant incoming edges so that the number of edges reaching Bob equals the min-cut capacity C from Alice to Bob.

[7]We assume throughout that the information injected into the network by Calvin is *added* to the original information transmitted (here we consider addition over our field $\mathbb{F}_q$).

[8]Our interest is to design communication schemes that do not rely on the specific network topology or network code used.

Let $Q = q^C$ and let $\mathbb{F}_Q$ be an extension field of $\mathbb{F}_q$. Let $\phi : \mathbb{F}_Q \to \mathbb{F}_q^{1\times C}$ be a vector space isomorphism. In addition, let $\phi_{m,n} : \mathbb{F}_Q^{m\times n} \to \mathbb{F}_q^{m\times Cn}$ be a vector space isomorphism such that the ith row of $\phi_{m,n}(X)$ is given by $\begin{bmatrix}\phi(X_{i,1}) & \cdots & \phi(X_{i,n})\end{bmatrix}$. In other words, we expand each element of $X \in \mathbb{F}_Q^{m\times n}$ as a length-C row vector over $\mathbb{F}_q$ (with the number of columns in matrix increasing accordingly). We will omit the subscript from $\phi_{m,n}$ when the dimensions of the argument are clear from the context.

Let $H \in \mathbb{F}_Q^{(C-Z_I)\times C}$ be the parity-check matrix of a $[C, Z_I]$ linear MRD code over $\mathbb{F}_Q$. Let $T \in \mathbb{F}_Q^{C\times C}$ be an invertible matrix chosen such that the first $C-Z_I$ rows of T^{-1} are equal to H. Assume that n is divisible by C and let $n' = n/C - 1$.

In order to encode a given message $S \in \mathbb{F}_Q^{(C-Z_I)\times n'}$, Alice first generates a random matrix $N \in \mathbb{F}_Q^{Z_I\times n'}$ uniformly and independently from any other variables. Then, she computes $X = \begin{bmatrix}I_C & \phi(x)\end{bmatrix}$, where $x = T\begin{bmatrix}S\\N\end{bmatrix}$.

After receiving $Y = AX = \begin{bmatrix}A & A\phi(x)\end{bmatrix}$, Bob computes $X = A^{-1}Y$ to recover $x = \phi^{-1}(\phi(x))$. Then, Bob can easily obtain S since, by construction, $S = Hx$.

Recall that Calvin's observation is given by $W = BX$, where $B \in \mathbb{F}_q^{Z_I\times C}$. According to Theorem 4 of [7], we have that $I(S;W) = 0$ for all B, and therefore (1) is satisfied. Thus, the scheme is indeed perfectly secret.

The decoding complexity is given by $O(nC^2)$ operations in $\mathbb{F}_Q$, which can be done in $O(nC^4)$ operations in $\mathbb{F}_q$.

B. Error Control under a Shared Secret Model

Consider now the case where Calvin can jam $Z_O < C$ packets and eavesdrop *any* number of packets he choose. However, we drop the requirement of secret communication, i.e., all we require is that Bob can decode correctly. In addition, suppose the existence of a *low* rate side channel, which Calvin cannot access, that enables Alice to transmit to Bob a small secret $\mathbb{S}$. Below, we review a coding scheme presented in [3] that can asymptotically achieve the maximum possible rate $R = C - Z_O$.

Let $b = C - Z_O$. We first describe how Alice produces the secret bit string $\mathbb{S}$ based on a given message $M \in \mathbb{F}_q^{b\times(n-b)}$. To begin with, she generates $\alpha = bC+1$ symbols $\rho_1, \rho_2, ..., \rho_\alpha \in \mathbb{F}_q$ independently and uniformly at random. Let $P \in \mathbb{F}_q^{n\times\alpha}$ be the matrix given by $P_{(i,j)} = (\rho_j)^i$. Then, she computes a matrix $\mathbb{H} = \bar{X}P \in \mathbb{F}_q^{b\times\alpha}$, where $\bar{X} = \begin{bmatrix}I_b & M\end{bmatrix}$. The tuple $(\rho_1, \rho_2, ..., \rho_\alpha, \mathbb{H})$, consisting in total of $\alpha(b+1)$ symbols in $\mathbb{F}_q$, comprises the message "hash" that should be secretly transmitted to Bob. The bit representation of this tuple yields the string $\mathbb{S} \in \{0,1\}^k$, consisting of $k = \alpha(b+1)\log_2 q$ bits. Over the main channel, Alice transmits the $C \times n$ matrix $X = \begin{bmatrix}\bar{X}\\0\end{bmatrix} = \begin{bmatrix}I_b & M\\0 & 0\end{bmatrix}$.

Assuming that $(\rho_1, \rho_2, \ldots, \rho_\alpha, \mathbb{H})$ is secretly and correctly received by Bob, let us proceed to the description of Bob's decoder. First, Bob reconstructs the matrix P. Bob obtains $Y = AX + Z$, where $Z \in \mathbb{F}_q^{C\times n}$ has rank at most Z_O. This can also be written as $Y = \tilde{A}\bar{X} + Z$, where $\tilde{A}$ consists of the first b columns of A. Let $\bar{Y}$ be the reduced row echelon form of Y. It is shown in [3] that, with probability at least $1 - O(1/q)$ for any fixed network, $\bar{X}$ can be written as $\bar{X} = U\bar{Y}$ for some $U \in \mathbb{F}_q^{b\times C}$. It is also shown in [3] that, with probability at least $1 - n^\alpha/q$, the system $U\bar{Y}P = \mathbb{H}$ has a unique solution in U. Bob solves this system to find U, computes $\bar{X} = U\bar{Y}$ and finally recovers M.

Overall, the probability of error of the scheme is at most $n^\alpha/q + O(1/q) = O(n^{C^2}/q)$, while the decoding complexity is $O(nC^3)$ operations in $\mathbb{F}_q$.

VI. Sending a Single Bit Secretly and Reliably

Let $C' = C - Z_I$. In this section, we show how Alice can transmit a secret bit reliably to Bob when $C > Z_I + Z_O$. We assume that $n = C(1 + C')$, as this is the smallest packet length required for the scheme to work. Larger packet lengths can be easily handled by zero-padding the transmitted packets.

Let $T \in \mathbb{F}_Q^{C\times C}$ and $H \in \mathbb{F}_Q^{C'\times C}$ be as given in Section V-A.

A. Alice's encoder

Initially, Alice chooses a matrix $S \in \mathbb{F}_Q^{C'\times C'}$ according to her secret bit: if the bit is 1, she picks S uniformly at random; otherwise, if the bit is 0, she sets $S = 0$. Then, she sends S to Bob using the secrecy scheme described in Section V-A. More precisely, she transmits $X = \begin{bmatrix}I_C & \phi(x)\end{bmatrix}$, where $x = T\begin{bmatrix}S\\N\end{bmatrix}$ and $N \in \mathbb{F}_Q^{Z_I\times C'}$ is a uniformly random matrix chosen independently from S.

B. Bob's decoder

Recall that Bob receives a matrix $Y = AX + Z$, where $A \in \mathbb{F}_q^{C\times C}$ is nonsingular and $Z \in \mathbb{F}_q^{C\times C(1+C')}$ has rank at most Z_O. Let $\bar{Y}$ denote the reduced row echelon form of Y. Consider first the case where $\bar{Y} = \begin{bmatrix}I & \phi(r)\end{bmatrix}$, for some $r \in \mathbb{F}_Q^{C\times C'}$. It is possible to show that $Hr = S + E$, where $E \in \mathbb{F}_Q^{C'\times C'}$ is a matrix of rank at most Z_O. As will be shown later, with high probability, Hr is full-rank if and only if Alice's secret bit is 1. Thus, Bob can decode by computing the rank of Hr.

In general, however, $\bar{Y}$ may not have the form described above. Nevertheless, as shown in [13], [17], it is possible to extract from $\bar{Y}$ some matrices $r \in \mathbb{F}_Q^{C\times C'}$, $\hat{L} \in \mathbb{F}_q^{C\times\mu}$ and $\hat{V} \in \mathbb{F}_Q^{\delta\times C'}$ such that

$$r = x + \hat{L}V^1 + L^2\hat{V} + L^3V^3$$

for some $V^1 \in \mathbb{F}_Q^{\mu\times C'}$, $L^2 \in \mathbb{F}_q^{C\times\delta}$, $L^3 \in \mathbb{F}_q^{C\times\epsilon}$ and $V^3 \in \mathbb{F}_Q^{\epsilon\times C'}$. Moreover, it is shown in [17] that $\mu, \delta \le Z_O$ and

$$\epsilon \le Z_O - \max\{\mu, \delta\}.$$

Note that $\epsilon < C' - \max\{\mu, \delta\}$, since $Z_O < C'$.

In possession of r, $\hat{L}$ and $\hat{V}$, Bob is now ready to decode the secrecy layer that has been applied to x.

We have

$$\begin{aligned} Hr &= Hx + H\hat{L}V^1 + HL^2\hat{V} + HL^3V^3 \\ &= S + \hat{\Lambda}V^1 + \Lambda^2\hat{V} + \Lambda^3V^3 \end{aligned} \tag{10}$$

where $\hat{\Lambda} = H\hat{L}$, $\Lambda^2 = HL^2$ and $\Lambda^3 = HL^3$. Note that $\hat{\Lambda} \in \mathbb{F}_Q^{C' \times \mu}$ and $\hat{V} \in \mathbb{F}_Q^{\delta \times C'}$ are known.

Now, let $J \in \mathbb{F}_Q^{(C'-\mu)\times C'}$ and $K \in \mathbb{F}_Q^{C' \times (C'-\delta)}$ be full-rank matrices such that $J\hat{\Lambda} = 0$ and $\hat{V}K = 0$. Then Bob can further simplify (10) by computing

$$JHrK = JSK + J\Lambda^3 V^3 K.$$

Note that $\mathsf{rank}(J\Lambda^3 V^3 K) \leq \epsilon < C' - \max\{\mu, \delta\}$.

Thus, Bob performs the following test. If $JHrK$ is full-rank, then Bob concludes that bit 1 was sent; otherwise, Bob concludes that bit 0 was sent.

With respect to complexity, computing $\bar{Y}$ takes $O(C^2 n) = O(C^4)$ operations in $\mathbb{F}_q$. Computing J, K, $JHrK$ and the rank of $JHrK$ each take $O(C^3)$ operations in $\mathbb{F}_Q$, which amounts to $O(C^5)$ in $\mathbb{F}_q$. Thus, the overall decoding complexity is $O(C^5)$ operations in $\mathbb{F}_q$.

C. Probability of error analysis

When bit 0 is sent, Bob never makes an error; he makes an error if and only if bit 1 is sent and $JHrK$ is not full-rank. Recall that, when bit 1 is sent, S is uniformly distributed over $\mathbb{F}_Q^{C' \times C'}$. Due to the secrecy encoding, Calvin has no information about S, and therefore S is statistically independent from $\Lambda^3 V^3$. It follows that $S' = S + \Lambda^3 V^3$ is also uniformly distributed over $\mathbb{F}_Q^{C' \times C'}$. Thus, the probability of error when bit 1 is sent is equal to the probability that $JS'K \in \mathbb{F}_Q^{(C'-\mu)\times(C'-\delta)}$ is not full-rank for a uniform S'.

Lemma 3: If $S' \in \mathbb{F}_Q^{C' \times C'}$ is uniformly distributed then, for any $J \in \mathbb{F}_Q^{(C'-\mu)\times C'}$ and any $K \in \mathbb{F}_Q^{C' \times (C'-\delta)}$, the matrix $JS'K$ is full-rank with probability at least $1 - C'/Q$.

Proof: Without loss of generality, assume $\mu \geq \delta$. It suffices to prove the statement for $\mu = \delta$; if $\mu > \delta$, then removing $\mu - \delta$ columns from K cannot possibly increase the rank of $JS'K$.

For any fixed J and K, consider the entries of S' as variables taking values in $\mathbb{F}_Q$. Then each entry of $JS'K$ is a multivariate polynomial over $\mathbb{F}_Q$ with degree at most 1. It follows that $\det(JS'K)$ is a multivariate polynomial over $\mathbb{F}_Q$ with degree at most $C' - \mu \leq C'$. Note that, if $Q \leq C'$, the statement follows trivially, so assume $Q > C'$. From [21, Lemma 4], we have that $P[\det(JS'K) = 0] \leq C'/Q$. ∎

Thus, the probability of error of the scheme is upper bounded by $C'/Q \leq C/q^C$, which can be made arbitrarily small by choosing q sufficiently large. This proves Theorem 1.

VII. Achievability for Theorem 2

We now describe a coding scheme that achieves rate $R = C - Z_I - Z_O$ asymptotically in the packet length n.

As before, assume that n is divisible by C and let $n' = n/C - (1 + kC')$, where $k = (bC + 1)(b + 1)\log_2 q$.

Let $H \in \mathbb{F}_Q^{C' \times C}$ be the parity-check matrix of a $[C, Z_I]$ linear MRD code over $\mathbb{F}_Q$. Let $T \in \mathbb{F}_Q^{C \times C}$ be an invertible matrix such that the first $C - Z_I$ rows of T^{-1} are equal to H.

Similarly, let $H_0 \in \mathbb{F}_Q^{R \times b}$ be the parity-check matrix of a $[b, Z_I]$ linear MRD code over $\mathbb{F}_Q$, and let $T_0 \in \mathbb{F}_Q^{b \times b}$ be an invertible matrix such that the first R rows of T_0^{-1} are equal to H_0.

A. Alice's encoder

First, given a message $S \in \mathbb{F}_Q^{R \times n'}$, Alice computes $x = T_0 \begin{bmatrix} S \\ N \end{bmatrix}$, where $N \in \mathbb{F}_Q^{Z_I \times n'}$ is chosen independently and uniformly at random. Then, she sets $M = \phi(x)$ and generates a string $\mathbb{S} \in \{0,1\}^k$ of k bits according to the scheme described in Section V-B. Next, for each ith bit of $\mathbb{S}$, Alice produces a matrix $S^i \in \mathbb{F}_Q^{C' \times C'}$ according to the scheme described in Section VI. Then, for each $i = 1, \ldots, k$, she computes $x^i = T \begin{bmatrix} S^i \\ N^i \end{bmatrix}$, where each $N^i \in \mathbb{F}_Q^{Z_I \times C'}$ is chosen uniformly at random and independently from any other variables. Finally, she produces a transmission matrix

$$X = \begin{bmatrix} I_C & \phi(x^1) & \phi(x^2) & \cdots & \phi(x^k) & \begin{bmatrix} M \\ 0 \end{bmatrix} \end{bmatrix}.$$

B. Bob's decoder

For each $i = 1, \ldots, k$, Bob extracts a submatrix Y^i from Y corresponding to the submatrix $\begin{bmatrix} I_C & \phi(x^i) \end{bmatrix}$ from X (i.e., columns $1, \ldots, C, C + (i-1)C' + 1, \ldots, C + iC'$). He then applies on Y^i the decoder described in Section VI to obtain each ith bit of $\mathbb{S}$.

Similarly, Bob extracts a submatrix Y^0 consisting of the first b and the last $n'C$ rows of Y. Note that $Y^0 = AX^0 + Z^0$, where $X^0 = \begin{bmatrix} I_b & M \\ 0 & 0 \end{bmatrix} \in \mathbb{F}_q^{C \times (b + n'C)}$ and Z^0 has rank at most Z_O. Then, Bob applies the decoder described in Section V-B to obtain M.

Finally, Bob computes $x = \phi^{-1}(M)$ and $S = H_0 x$.

C. Overall Analysis

1) Secrecy analysis: The secrecy of the message is guaranteed by the scheme of Section V-A.

2) Error probability analysis: By the union bound, the probability that Bob makes an error when decoding the k-bit secret $\mathbb{S}$ is at most $kC/q^C \leq C^4(\log_2 q)/q^C = O(\frac{\log_2 q}{q^C})$. Given that the secret is decoded correctly, the probability that Bob makes an error when decoding the message is at most $O(n^{C^2}/q)$. Thus, the overall probability of error is at most $O(n^{C^2}/q)$.

3) Rate analysis: The rate of the scheme is given by $Rn'C/n = R(1 - (1 + kC')C/n) \leq R - RC^5(\log_2 q)/n$. Thus, the rate loss is $O(\frac{\log_2 q}{n})$.

4) Complexity analysis: Decoding all the secret bits takes $O(kC^5) = O(C^8 \log_2 q)$ operations in $\mathbb{F}_q$, while decoding the message is dominated by the secrecy decoding step with $O(C^4 n)$ operations in $\mathbb{F}_q$.

Note: Both the rate loss and the error probability can be made asymptotically small by choosing q to grow faster than polynomially but slower than exponentially in n. For instance, we may choose $q = 2^{\lfloor \sqrt{n} \rfloor}$.

VIII. Errata for [2]

We briefly reprise the scheme of [2] before demonstrating the flaw in the proof. In what follows, all operations are over $\mathbb{F}_q$.

In the scheme of [2] there exist two hash matrices D_0 and D_1 which are chosen independently and uniformly at random $C^2(C-Z_O)\times C^2$ *Vandermonde matrices*, *i.e.*, each column of D_0 and D_1 is of the form $\mathbf{h}(u)=[u,u^2,...,u^{C^2(C-Z_O)}]^T$, where the generator u is chosen independently and uniformly at random from $\mathbb{F}_q$. Both D_0 and D_1 are publicly known to all parties, including Bob and Calvin.

Alice's Encoder: Alice first chooses a random length-$(C^2(C-Z_O)-C^2)$ row vector $\mathbf{u}$. Let $I\in\{0,1\}$ be the secret bit that Alice wishes to send to Bob. Alice then constructs the length-$1\times C^2$ row vector $\mathbf{r}$ such that $[\mathbf{u},\mathbf{r}]D_I=0$. Note that such $\mathbf{r}$ exists since the last C^2 rows of D_I form an invertible matrix. Finally the vector $[\mathbf{u},\mathbf{r}]$ is rearranged into a $(C-Z_O)\times C^2$ matrix which is sent through the network via random linear network coding.

Bob's Decoder: After receiving the $C\times C^2$ matrix Y, for each $I\in\{0,1\}$ Bob check whether there exists $C-Z_O$ length-C vectors $\{\mathbf{x}_i, i\in[1,C-Z_O]\}$ such that $[\mathbf{x}_1Y,\mathbf{x}_2Y,...,\mathbf{x}_{C-Z_O}Y]D_I=0$. If so, Bob decodes the secret bit as I. The idea is that if I is Alice's bit, such $\{\mathbf{x}_i, i\in[1,C-Z_O]\}$ exists for D_I with high probability [3].

Calvin's successful attack: When Calvin corrupts $Z_O\geq C-Z_O$ edges, Calvin could mimic Alice's behaviour when she wishes to transmit a particular bit, say 1. As a result Bob would always find length-C row vectors $\{\mathbf{x}_i, i\in[1,C-Z_O]\}$ such that $[\mathbf{x}_1Y,\mathbf{x}_2Y,...,\mathbf{x}_{C-Z_O}Y]D_1=0$. In this case Bob cannot determine whether the bit 1 is from Alice or from Calvin.

Even if Calvin can only inject $Z_O<C-Z_O$ errors, if $Z_O+Z_I\geq C-Z_O$, there is another successful attack for Calvin. To see that, without loss of generality let $Z_O+Z_I=C-Z_O$. Since Calvin can eavesdrop on Z_I packets $\{\mathbf{y}_i, i\in[1,Z_I]\}$, he can carefully choose his Z_O injected error packets $\{\mathbf{z}_i, i\in[1,Z_O]\}$ so that $[\mathbf{y}_1,...,\mathbf{y}_{Z_I},\mathbf{z}_1,...,\mathbf{z}_{Z_O}]D_1=0$. In this case, Bob also always decodes its bit as 1. Thus the scheme in [2] only works for the case where $C>2Z_O+Z_I$, which does not improve the result in [3].

Why our scheme works: In our scheme Section VI, instead of distinguishing the bit by the hash matrices, Alice hides her secret in the rank of the bit matrix she transmits. In particular, there is a rank gap $C-Z_I$ between the bit matrix for bit 0 and the one for bit 1. Thus as long as $C-Z_I>Z_O$, Calvin cannot mimic Alice any more, since he can only inject Z_O errors. As a result Bob can determine Alice's bit by examining the rank of the matrix he decodes.

IX. Conclusion

In this work we considered the problem of communicating information secretly and reliably over a network containing a malicious eavesdropping and jamming adversary. Under the assumptions that vanishingly small probabilities of error and block coding are allowed, we substantially improve on the best achievable rates in prior work [1], and also prove the optimality of our achievable rates. A key component of our code design is a scheme that allows a small amount of information to be transmitted secretly and reliably over the network, as long as the total number of packets that the adversary can either eavesdrop on or jam is less than the communication capacity of the network. In proving this scheme we correct an error in the proof of prior work [2] by a subset of the authors of this work.

References

[1] C.-K. Ngai and R. W. Yeung, "Secure error-correcting (sec) network codes," in *Proc. Workshop on Network Coding Theory and Applications*, Lausanne, Switzerland, Jun. 15-16, 2009, pp. 98–103.

[2] S. Jaggi and M. Langberg, "Resilient network codes in the presence of eavesdropping Byzantine adversaries," in *Proc. IEEE Int. Symp. Information Theory*, 24–29 June 2007, pp. 541–545.

[3] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard, and M. Effros, "Resilient network coding in the presence of Byzantine adversaries," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2596–2603, Jun. 2008.

[4] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, Jun. 30–Jul. 5, 2002, p. 323.

[5] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the capacity of secure network coding," in *Proc. 42nd Annual Allerton Conf. on Commun., Control, and Computing*, Sep. 2004.

[6] S. Y. E. Rouayheb and E. Soljanin, "On wiretap networks II," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jun. 24–29, 2007, pp. 551–555.

[7] D. Silva and F. R. Kschischang, "Security for wiretap networks via rank-metric codes," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, Canada, Jul. 6–11, 2008, pp. 176–180.

[8] P. F. Oliveira and J. Barros, "A network coding approach to secret key distribution," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 414–423, 2008.

[9] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks using randomized network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2798–2803, 2008.

[10] 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.

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

[12] R. Matsumoto, "Construction algorithm for network error -correcting codes attaining the singleton bound," Oct 2006.

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

[14] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[15] D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," in *Proc. of The 27th Conference on Computer Communications*, 2008.

[16] F. Zhao, T. Kalker, M. Medard, and J. K. Han, "Signatures for content distribution with network coding," in *Proc. of ISIT*, 2007.

[17] D. Silva, "Error control for network coding," Ph.D. dissertation, University of Toronto, Toronto, Canada, 2009.

[18] C.-K. Ngai and S. Yang, "Deterministic secure error-correcting (sec) network codes," in *Proc. IEEE Information Theory Workshop*, Tahoe City, CA, Sep. 2–6, 2007, pp. 96–101.

[19] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inf. Theory*, 2008, submitted for publication. [Online]. Available: http://arxiv.org/abs/0809.3546

[20] ——, "Universal secure error control schemes for network coding," in *Proc. IEEE Int. Symp. Information Theory*, 2010, to be published.

[21] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.