

Secure Error-Correcting (SEC) Network Codes

Chi-Kin Ngai
Chinese University of Hong Kong
Hong Kong SAR
China
Email: cknagai@alumni.cuhk.net

Raymond W. Yeung
Chinese University of Hong Kong
Hong Kong SAR
Hong Kong
Email: whyeung@ie.cuhk.edu.hk

Abstract — We investigate transmission of information in a network in the presence of an adversary that can eavesdrop k channels and inject d errors into the network at the same time. We propose a deterministic construction of a secure error-correcting (SEC) network codes which can transmit information at rate $m - 2d - k$ to all the sink nodes which protecting the information from eavesdropping and contamination by the adversary, where m is the minimum maxflow among all the sink nodes. We also show that this rate is optimal.

I. INTRODUCTION

In a real network, data transmission may suffer from two kinds of adversaries: contamination and eavesdropping. Here contamination refers to the distortion on the transmission, such as random errors, link failures, traffic congestion and malicious modifications. Network coding for combating these two kinds of adversaries have been studied in the literature.

The concept of network error correction coding, a generalization of classical error correction coding, was introduced by Cai and Yeung [3–5]. They generalized the Hamming bound, the Singleton bound and the Gilbert-Varshamov bound in classical error correction coding to network coding. A refined version of these bounds are proved by [10] and [11]. Zhang [6] introduced the minimum rank for linear network codes, which plays a role similar to that of the minimum distance in decoding classical error-correcting codes. Recently, network generalizations of the Hamming weight, the Hamming distance, and the minimum distance of network codes have been obtained by Yang and Yeung [9]. In terms of the minimum distance, the capability of a network code for error correction, error detection, and erasure correction can be fully characterized.

The eavesdropping problem has been addressed by Cai and Yeung [2]. They introduced a communication system on a wiretap network (CSWN), which consists of a collection \mathcal{W} of subsets of channels. A eavesdropper can arbitrarily choose one but only one subset $W \in \mathcal{W}$ and fully access all the channels in the subset W . The communicators over a CSWN know the collection \mathcal{W} but do not know which subset W is chosen by the eavesdropper. They proposed in [2] a secure network coding scheme based on a given decodable linear network code.

In this paper, we consider an adversary that can:

- i) eavesdrop a subset of at most k channels;
- ii) contaminate the transmission on a subset of at most d channels.

The main contribution of this paper is to propose a construction of deterministic network codes which can transmit information to all the sink nodes at rate $m - 2d - k$ with complete reliability and information-theoretic security. We also shown that the rate $m - 2d - k$ is optimal in the presence of such an adversary. We call the codes so constructed *secure error-correcting* (SEC) network codes. The security of the code is rigorously established based on a very general model in which the adversary can use the information obtained through eavesdropping in a causal manner. The details will be explained later.

A similar problem was studied in [7,8] with the *inaction* assumption, i.e., the adversary contaminates the same subset of channels for a long period of time.

II. CODE CONSTRUCTION

In this section, we present a code construction by cascading an error-correcting network code construction with a secure network code construction. The existence of such a code will also be shown while the error-correcting capability and the secure issue of the result network code will be analyzed in the next section. The construction consists of four parts. Part 1 is to utilize a given linear multicast as an error-correcting network code with distance achieving the refined Singleton bound [4] by choosing a suitable input subspace at the source node. The technique involved can also be found in [4]. Parts 2 to 4 involve the steps of transforming the constructed error-correcting network code into a SEC code. This idea is originated in the work [12]. Most of the techniques involved in constructing a secure network code can be found in [2].

For two subsets $V_1, V_2 \subset \mathbb{F}_q^{\omega+k}$, their sum is the set defined by

$$V_1 + V_2 = \{\mathbf{v}_1 + \mathbf{v}_2 : \mathbf{v}_1 \in V_1, \mathbf{v}_2 \in V_2\}, \quad (1)$$

where ω is an integer whose value is to be specified. Denote by \mathcal{W} a collection of subsets W of the edge set \mathcal{E} such that $|W| \leq k$.

Construction 1:

- i) Let an m -dimensional linear multicast with global encoding kernels $\{f_e\}$ be given, and let $\omega + k < m + 1$. In [4], it was shown that by choosing a suitable $(\omega +$

k)-dimensional subspace of \mathbb{F}^m , specified by an $(\omega + k) \times m$ generator matrix G , the linear multicast can be converted into a linear network code with $d_{min} = m - \omega - k + 1 > 0$.

- ii) For all $W \in \mathcal{W}$, define $\mathcal{L}_W = \langle \{Gf_e, e \in W\} \rangle$ where $\langle \cdot \rangle$ is the conventional notation for the linear span of a set of vectors. Then we choose ω linearly independent vectors $b_1, b_2, \dots, b_\omega$ from $\mathbb{F}^{\omega+k}$ such that $\forall W \in \mathcal{W}$,

$$\langle \{b_1, b_2, \dots, b_\omega\} \rangle \cap \mathcal{L}_W = \emptyset. \quad (2)$$

The existence of such a set of vectors will be justified later on. We can extend $b_1, b_2, \dots, b_\omega$ to a linearly independent set with $\omega + k$ vectors, say $b_1, b_2, \dots, b_\omega, b_{\omega+1}, \dots, b_{\omega+k}$, and denote

$$Q = [\begin{array}{cccc} b_1 & b_2 & \dots & b_{\omega+k} \end{array}], \quad (3)$$

which is non-singular.

- iii) The information source X takes values in \mathbb{F}^ω while the independent randomness R takes values in \mathbb{F}^k according to the uniform distribution. Let the message \mathbf{x} be a row vector in \mathbb{F}^ω , and let the outcome \mathbf{r} of R be a row vector in \mathbb{F}^k . Let $X' = (X, R)$ and the outcome of X' be $\mathbf{x}' = (\mathbf{x}, \mathbf{r})$.
- iv) Encode the vector \mathbf{x}' by $Q^{-1}G$ and transmit the encoded vector $\mathbf{x}'Q^{-1}G$ by utilizing the given linear multicast. Therefore the symbol transmitted on each channel e is equal to $\mathbf{x}'Q^{-1}Gf_e$.

The existence of Q can be justified by standard techniques. See for example [13].

III. SECURITY AND ERROR-CORRECTION CAPABILITY

In this section, we show that the code constructed in the previous section can transmit at rate $m - 2d - k$ with reliability and information-theoretic security in the presence of an adversary that can eavesdrop any set of k channels and can inject up to d errors in the network.

Theorem 1. *Given a set of local encoding kernels over a finite field with size q where q is sufficiently large, there exists a message set \mathcal{C} with $|\mathcal{C}| = q^{m-2d-k}$ such that information can be transmitted to all the sink nodes t at the rate $m - 2d - k$ in the presence of d channels with errors, and the network code can prevent eavesdroppings on any set of k channels in the network.*

Proof. In Construction 1, by letting $d_{min} = 2d + 1$, we obtain a linear network code that transmits information at rate $\omega = m - 2d - k$. All we have to show is that the code satisfies the error correcting condition and the security condition. We first verify the error correcting condition. By the result in [9], every sink node can decode

$\mathbf{x}'Q^{-1}$ in the presence of up to d errors. Therefore, the sink nodes can recover \mathbf{x}' and hence \mathbf{x} .

Now, let us check the security condition. We first assume that no error is injected into the network. We first fix an arbitrary set W of $k' \leq k$ channels, $e_1, e_2, \dots, e_{k'}$ such that $\{f_{e_1}, f_{e_2}, \dots, f_{e_{k'}}\}$ forms a set of linear independent vectors and assume that it is the set of eavesdropped channels. Then the information transmitted on the k' channels will be $\mathbf{x}'Q^{-1}Gf_{e_1}, \mathbf{x}'Q^{-1}Gf_{e_2}, \dots, \mathbf{x}'Q^{-1}Gf_{e_{k'}}$, respectively. Or equivalently,

$$\mathbf{x}'Q^{-1}f'_{e_1}, \mathbf{x}'Q^{-1}f'_{e_2}, \dots, \mathbf{x}'Q^{-1}f'_{e_{k'}}, \quad (4)$$

where $f'_{e_l} = Gf_{e_l}, \forall 1 \leq l \leq k'$. Next, we are going to show by contradiction that all the symbols the eavesdropper obtains from the channels are a mixture of the symbols from X and R , and that the eavesdropper cannot recover any information about X , either completely or partially. To extract any kind of information consisting only symbols from X , there must exist at least one vector f in the vector space $\langle f'_{e_1}, f'_{e_2}, \dots, f'_{e_{k'}} \rangle$ such that

$$Q^{-1}f \in V', \quad (5)$$

where V' is the vector space consisting of all $(\omega + k)$ -dimensional column vectors which contain only zeros starting from the $(\omega + 1)$ st position. If such a vector f exists, then

$$f \in V'', \quad (6)$$

where $V'' = \{Qv : v \in V'\}$. Furthermore,

$$V'' = \{Qv : v \in V'\} \quad (7)$$

$$= \langle \{Q\delta_1, Q\delta_2, \dots, Q\delta_\omega\} \rangle \quad (8)$$

$$= \langle \{b_1, b_2, \dots, b_\omega\} \rangle, \quad (9)$$

where $\delta_i, 1 \leq i \leq \omega$ denotes the $(\omega + k)$ -dimensional column vector which contains only zeros except in the i th position which is equal to 1. Therefore,

$$f \in \langle \{b_1, b_2, \dots, b_\omega\} \rangle. \quad (10)$$

This contradicts (2). Hence, such a vector f does not exist, and all the symbols that the eavesdropper obtains from the channels are a mixture of the symbols from X and R .

Let Y_W be the vector of symbols transmitted on the k' eavesdropped channels. Let \mathbf{y}_W be the value of Y_W when $X = (\mathbf{x}, \mathbf{r})$. The information transmitted on the k' eavesdropped channels are

$$Y_W = (\mathbf{x}, \mathbf{r}) [\begin{array}{cccc} Q^{-1}f'_{e_1} & Q^{-1}f'_{e_2} & \dots & Q^{-1}f'_{e_{k'}} \end{array}] \quad (11)$$

$$= (\mathbf{x}, \mathbf{r}) \left[\begin{array}{c} G_1 \\ G_2 \end{array} \right] \quad (12)$$

$$= \mathbf{x}G_1 + \mathbf{r}G_2, \quad (13)$$

where G_1 and G_2 are matrices with dimensions $\omega \times k'$ and $k \times k'$, respectively. Next, we are going to show that

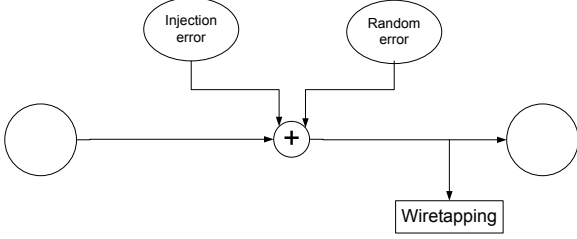


Figure 1: Error components and wiretapping of a channel.

the rank of G_2 must be k' , the number of columns of G_2 . Assume that the rank of G_2 is less than k' . There must exist a k' -dimensional non-zero column vector v such that

$$G_2 v = 0. \quad (14)$$

Then

$$Y_W v = (\mathbf{x}, \mathbf{r}) \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} v \quad (15)$$

$$= (\mathbf{x}, \mathbf{r}) \begin{bmatrix} G_1 v \\ 0 \end{bmatrix} \quad (16)$$

$$= \mathbf{x} G_1 v. \quad (17)$$

This contradicts the fact that all symbols obtained by the eavesdropper are mixture of the symbols from X and R . Therefore, the rank of G_2 must be k' .

For all subset W of k' channels, $\mathbf{y}_W \in \mathbb{F}^{k'}$ and $\mathbf{x} \in \mathbb{F}^\omega$,

$$Pr\{Y_W = \mathbf{y} | X = \mathbf{x}\} \quad (18)$$

$$= Pr\{\mathbf{x} G_1 + R G_2 = \mathbf{y}\} \quad (19)$$

$$= Pr\{R G_2 = \mathbf{y} - \mathbf{x} G_1\} \quad (20)$$

$$= |\mathbb{F}|^{-k'}, \quad (21)$$

which is independent of \mathbf{x} . Therefore,

$$I(X; Y_W) = 0. \quad (22)$$

From now on, we assume that errors can occur on all the edges in the network and we will prove that under this assumption, the eavesdropper still cannot obtain any useful information. Let $\mathcal{E} = \{1, 2, \dots, |\mathcal{E}|\}$, where the indexing is consistent with the partial order of edges in the network.

Assume that on each edge $i \in \mathcal{E}$, the error is an addition of two components, as illustrated in Figure 1. One of the component is called random error Z_i^{ran} which is not under the control of the adversary and satisfies

$$I(X, R; Z^{ran}) = 0, \quad (23)$$

where $Z^{ran} = (Z_i^{ran}, 1 \leq i \leq |\mathcal{E}|)$. And we assume that the adversary is powerful enough to know all the random errors Z^{ran} injected though the value of the random errors are out of adversary's control. The other component of the error is called injection error Z_i^{in} which is a possibly

probabilistic injection of errors based on both the information obtained so far by the adversary and the random errors Z^{ran} , and is under the control of the adversary. We will show that the code we constructed in the last section is indeed secure under this highly advantageous assumption for the eavesdropper.

Let $\{\sigma(1), \sigma(2), \dots, \sigma(k)\}$ be the set of k channels that the adversary chooses to eavesdrop where the indexing is consistent with the partial order of the edges in the network. In order words, $\sigma(i) \leq \sigma(j), \forall i < j$. Assume that $\forall 1 \leq j \leq |\mathcal{E}|$, there exists $1 \leq i_j \leq k$ such that either $\sigma(i_j) < j$ and $j \leq \sigma(i_j + 1)$, or $\sigma(i) < j, \forall 1 \leq i \leq k$. And we assume that the adversary has the ability to decide what errors to be injected into the downstream of the network based on the information it obtained in the upstream.

Let $Y_j, 1 \leq j \leq k$, be the symbols transmitted on the edge $\sigma(j)$ when there is no error injected into the network and let $Y'_j, 1 \leq j \leq k$, be the symbols transmitted on the edge $\sigma(j)$ when there are errors in the network (either random or injected). We further assume that for every channel chosen, the eavesdropper always eavesdrops at the receiving end of the channel, that is, after the errors are injected if there is any. This assumption can be justified because in our model, the adversary are assumed to know not only the injected errors, but also the random errors that are happening on every channels. The information that the adversary can obtain by eavesdropping the receiving end of the channels allows it to calculate the information at the transmitting end of the channels. Therefore $\forall j, 1 \leq j \leq k$,

$$Y'_j = Y_j + g'_j(Z_i^{in}, Z_i^{ran}, \forall i \leq \sigma(j)), \quad (24)$$

where $g'_e(\cdot)$ s are deterministic functions depend only on the local encoding kernels of the network.

Then $\forall j, 1 \leq j \leq k$,

$$\begin{aligned} & I(Z_j^{in}; Y_{i_j+1}, \dots, Y_k | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \\ &= I(Z_j^{in}; Y_{i_j+1}, \dots, Y_k | Y'_1, \dots, Y'_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \end{aligned} \quad (25)$$

$$\leq I(Z_j^{in}; X, R | Y'_1, \dots, Y'_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \quad (26)$$

$$= 0, \quad (27)$$

where the first equality is valid because when $(Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran})$ are all known, the values of Y_1, \dots, Y_{i_j} can always be calculated from Y'_1, \dots, Y'_{i_j} by using (24) and vice versa, the first inequality follows from the fact that Y_{i_j+1}, \dots, Y_k are all functions of X, R and the last equality is true by the construction of our model. Therefore, $\forall j, 1 \leq j \leq k$,

$$I(Z_j^{in}; Y_{i_j+1}, \dots, Y_k | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) = 0. \quad (28)$$

Furthermore, $\forall j, 1 \leq j \leq k$,

$$\begin{aligned} & I(Z_j^{in}; Y_{i_j+1}, \dots, Y_k | X, R, Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \\ & \leq I(Z_j^{in}; X, R | X, R, Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \end{aligned} \quad (29)$$

$$= 0. \quad (30)$$

Therefore, $\forall j, 1 \leq j \leq k$,

$$\begin{aligned} & I(Z_j^{in}; Y_{i_j+1}, \dots, Y_k | X, R, Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \\ & = 0. \end{aligned} \quad (31)$$

Then $\forall j, 1 \leq j \leq k$,

$$\begin{aligned} & I(X, R; Z_j^{in} | Y_1, \dots, Y_{i_j}, Y_{i_j+1}, \dots, Y_k, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \\ & = I(X, R; Z_j^{in} | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) - \end{aligned}$$

$$\begin{aligned} & I(X, R; Z_j^{in}; Y_{i_j+1}, \dots, Y_k | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \\ & = I(X, R; Z_j^{in} | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) - \end{aligned} \quad (32)$$

$$\begin{aligned} & I(X, R; Z_j^{in}; Y_{i_j+1}, \dots, Y_k | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) - \\ & I(Z_j^{in}; Y_{i_j+1}, \dots, Y_k | X, R, Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \end{aligned} \quad (33)$$

$$\begin{aligned} & = I(X, R; Z_j^{in} | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) - \\ & I(Z_j^{in}; Y_{i_j+1}, \dots, Y_k | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \end{aligned} \quad (34)$$

$$= I(X, R; Z_j^{in} | Y_1, \dots, Y_{i_j}, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \quad (35)$$

$$= 0, \quad (36)$$

$$= 0, \quad (36)$$

where (32) follows from

$$I(A; B; C) = I(A; C) - I(A; B|C)^1, \quad (37)$$

(33) follows from (31), (35) follows from (28), and the last equality is valid by the construction of our model. Since $Y_W = (Y_1, \dots, Y_k)$, it follows from (36) that

$$I(X, R; Z_j^{in} | Y_W, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) = 0. \quad (38)$$

Summing over all j and applying the chain rule for mutual information, we get

$$\begin{aligned} & I(X, R; Z^{in} | Y_W, Z^{ran}) \\ & = \sum_j I(X, R; Z_j^{in} | Y_W, Z_1^{in}, \dots, Z_{j-1}^{in}, Z^{ran}) \end{aligned} \quad (39)$$

$$= 0, \quad (40)$$

where $Z^{in} = (Z_i^{in}, 1 \leq i \leq |\mathcal{E}|)$.

On the other hand,

$$\begin{aligned} & I(X; Y_W | Z^{ran}) \\ & = I(X; Y_W) - I(X; Y_W; Z^{ran}) \end{aligned} \quad (41)$$

$$= -I(X; Y_W; Z^{ran}) \quad (42)$$

$$= I(X; Z^{ran} | Y_W) - I(X; Z^{ran}) \quad (43)$$

$$= I(X; Z^{ran} | Y_W) \quad (44)$$

$$\leq I(X, R; Z^{ran} | Y_W) \quad (45)$$

$$= I(X, R; Z^{ran}) - I(XR; Z^{ran}; Y_W) \quad (46)$$

$$= -I(X, R; Z^{ran}; Y_W) \quad (47)$$

$$\leq I(Z^{ran}; Y_W | X, R) \quad (48)$$

$$\leq H(Y_W | X; R) \quad (49)$$

$$= 0, \quad (50)$$

where (42) follows from (22), both (44) and (47) follow from (23) and (48) follows from

$$0 \leq I(Z^{ran}; Y_W) \quad (51)$$

$$= I(X, R; Z^{ran}; Y_W) + I(Z^{ran}; Y_W | X, R). \quad (52)$$

Since $I(X; Y_W | Z^{ran}) \geq 0$, (50) implies

$$I(X; Y_W | Z^{ran}) = 0. \quad (53)$$

Therefore,

$$\begin{aligned} & I(X; Y_W, Z^{in}, Z^{ran}) \\ & = I(X; Z^{ran}) + I(X; Y_W | Z^{ran}) + I(X; Z^{in} | Y_W, Z^{ran}) \end{aligned} \quad (54)$$

$$= I(X; Y_W | Z^{ran}) + I(X; Z^{in} | Y_W, Z^{ran}) \quad (55)$$

$$= I(X; Z^{in} | Y_W, Z^{ran}) \quad (56)$$

$$= 0, \quad (57)$$

where (55) follows from (23), (56) follows from (53), and (57) follows from (40).

Finally,

$$\begin{aligned} & I(X; Y'_W) \\ & \leq I(X; Y'_W, Z^{in}, Z^{ran}) \end{aligned} \quad (58)$$

$$= I(X; Y_W, Z^{in}, Z^{ran}) \quad (59)$$

$$= 0. \quad (60)$$

Therefore,

$$I(X; Y'_W) = 0. \quad (61)$$

That is, the code we constructed in the last section is indeed secure. \square

Next, we prove that $m - 2d - k$ is an upper bound on the rate of a SEC network code in the presence of an adversary that can eavesdrop k channels and inject d errors. The proof here is an extension of the one in [14]. In establishing this result, we need a set of inequalities due to Han [1] stated in the next lemma.

¹See [13], Ch. 3.

Lemma 1. For a subset α of $\mathcal{N} = \{1, 2, \dots, m\}$, let $\bar{\alpha} = \mathcal{N} \setminus \alpha$ and $(X_i, i \in \alpha)$ by X_α . For $1 \leq k \leq m$, let

$$H'_k = \frac{1}{\binom{m-1}{k-1}} \sum_{\alpha: |\alpha|=k} H(X_\alpha | X_{\bar{\alpha}}). \quad (62)$$

Then

$$H'_1 \leq H'_2 \leq \dots \leq H'_m. \quad (63)$$

Theorem 2. The maximum rate at which information can be transmitted from the source node to all the sink nodes with linear network code in the presence of adversary that can eavesdrop k channels and inject d errors at the same time is $m - 2d - k$.

Proof. Let t be the sink node such that there exists a cut U between s and t such that there are exactly m edges across the cut U . Let $\mathcal{E}_t = \{e_1, e_2, \dots, e_m\}$ be the set of edges across the cut U . Assume that the source node transmits ω units of information, $\mathbf{x} = \{x_1, x_2, \dots, x_\omega\}$, to the sink nodes and k' symbols of randomness are introduced.

Consider a fixed linear network code in which all the node will transmit a linear combination of the information that it received from the incoming edges onto the outgoing edges according to the local encoding kernels. Then the information transmitting across the cut is

$$\mathbf{x}G_M + \mathbf{r}G_R, \quad (64)$$

where G_M is a $\omega \times m$ generator matrix for the message and G_R is a $k' \times m$ matrix and the exact value of G_M and G_R depend on the local encoding kernels of the linear network code considered. The rank of G_M must be ω for the message to be decodable at the sink nodes. Furthermore,

$$\langle G_M \rangle \cap \langle G_R \rangle = \{0\}, \quad (65)$$

where $\langle G_M \rangle$ and $\langle G_R \rangle$ are the row vector spaces of G_M and G_R , respectively. Otherwise, there exist $\mathbf{x}, \mathbf{x}' \in \mathbb{F}^\omega$, $\mathbf{x} \neq \mathbf{x}'$, $\mathbf{r}, \mathbf{r}' \in \mathbb{F}^k$, $\mathbf{r} \neq \mathbf{r}'$ such that

$$(\mathbf{x} - \mathbf{x}')G_M = (\mathbf{r} - \mathbf{r}')G_R. \quad (66)$$

This implies

$$\mathbf{x}G_M + \mathbf{r}'G_R = \mathbf{x}'G_M + \mathbf{r}G_R. \quad (67)$$

Then, the sink node t would not be able to decode the message correctly.

Assume information is transmitting at the rate of $L - a$ and a units of randomness, $\mathbf{r} = \{r_1, r_2, \dots, r_a\}$, are introduced where $L > a$. Next we are going to show that at least k symbols of randomness are required for the code to be secured.

We first deal with the case when $L \geq k + 1$. Let $Y_{\mathcal{E}'}$, $\mathcal{E}' \subset \mathcal{E}$, be the vector of symbols transmitted on the edge in \mathcal{E}' . We first assume that G_R is a full rank matrix,

since $\langle G_M \rangle \cap \langle G_R \rangle = \{0\}$, $\begin{bmatrix} G_M \\ G_R \end{bmatrix}$ is a full rank matrix. Therefore, \exists an $L \times L$ submatrix which is invertible. This implies there exists a subset $\mathcal{E}'_t \subset \mathcal{E}_t$, $|\mathcal{E}'_t| = L$ such that

$$H(X, R | Y_{\mathcal{E}'_t}) = 0, \quad (68)$$

which further implies

$$H(X | Y_{\mathcal{E}'_t}) = 0. \quad (69)$$

For the case in which $\text{rank}(G_R) = b < a$, there exists a matrix \hat{G}_R that consists of b rows of G_R such that $\forall \mathbf{x} \in \mathbb{F}^{L-a}$, $\mathbf{r} \in \mathbb{F}^a$, $\exists \mathbf{r}' \in \mathbb{F}^b$ such that

$$(\mathbf{x}, \mathbf{r}) \begin{bmatrix} G_M \\ G_R \end{bmatrix} = (\mathbf{x}, \mathbf{r}') \begin{bmatrix} G_M \\ \hat{G}_R \end{bmatrix}, \quad (70)$$

where the components of \mathbf{r}' is a linear combination of components of \mathbf{r} . Since $\langle G_M \rangle \cap \langle G_R \rangle = \{0\}$, \exists an $(L - a + b) \times (L - a + b)$ submatrix which is invertible. This implies there exists a subset $\mathcal{E}'_t \subset \mathcal{E}_t$, $|\mathcal{E}'_t| = L$ such that

$$H(X, R' | Y_{\mathcal{E}'_t}) = 0, \quad (71)$$

where \mathbf{r}' is the outcome of the random variable R' . This further implies

$$H(X | Y_{\mathcal{E}'_t}) = 0. \quad (72)$$

For any $\mathcal{I} \subset \mathcal{E}'_t$, $|\mathcal{I}| = k$, consider

$$H(X) = H(X | Y_{\mathcal{E}'_t}) + I(Y_{\mathcal{E}'_t}; X) \quad (73)$$

$$= I(Y_{\mathcal{I}}; X) + I(Y_{\mathcal{E}'_t \setminus \mathcal{I}}; X | Y_{\mathcal{I}}) \quad (74)$$

$$= I(Y_{\mathcal{E}'_t \setminus \mathcal{I}}; X | Y_{\mathcal{I}}), \quad (75)$$

where the second equality follows from (69) and the last equality follows from the requirement for the code to be secured. Summing over all \mathcal{I} , we have

$$\begin{aligned} & \binom{L}{k} H(X) \\ &= \sum_{\mathcal{I}} I(Y_{\mathcal{E}'_t \setminus \mathcal{I}}; X | Y_{\mathcal{I}}) \end{aligned} \quad (76)$$

$$\leq \binom{L-1}{L-k-1} \left[\frac{1}{\binom{L-1}{L-k-1}} \sum_{\mathcal{I}} H(Y_{\mathcal{E}'_t \setminus \mathcal{I}} | Y_{\mathcal{I}}) \right] \quad (77)$$

$$\leq \binom{L-1}{L-k-1} H(Y_{\mathcal{E}'_t}), \quad (78)$$

where the last inequality follows from Lemman 1. Hence,

$$H(Y_{\mathcal{E}'_t}) \geq \frac{L}{L-k} H(X). \quad (79)$$

Finally,

$$H(X) + H(R) \geq H(X, R) \quad (80)$$

$$= H(X, R, Y_{\mathcal{E}'_t}) \quad (81)$$

$$\geq H(Y_{\mathcal{E}'_t}) \quad (82)$$

$$\geq \frac{L}{L-k} H(X), \quad (83)$$

where (81) follows from

$$H(Y_{\mathcal{E}'_t}|X, R) = 0. \quad (84)$$

This implies

$$H(R) \geq \frac{k}{L-k}H(X) \geq k, \quad (85)$$

where X is uniformly distributed. Therefore, at least k symbols of randomness need to be introduced.

On the other hand, when $L \leq k$, there exists a subset $\mathcal{E}'_t \subset \mathcal{E}_t, |\mathcal{E}'_t| = k$ such that

$$H(X, R|Y_{\mathcal{E}'_t}) = 0. \quad (86)$$

That is, the code is insecure. Therefore, at least k symbols of randomness again need to be introduced.

Now, assume that k symbols of randomness are introduced. For the network code to correct any d errors injected into $\mathcal{E}_t, \forall \mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}^\omega, \mathbf{x}_1 \neq \mathbf{x}_2, \mathbf{r}_1, \mathbf{r}_2 \in \mathbb{F}^k, \text{ and } \forall z_1, z_2 \in \mathbb{F}^m, |z_1| \leq d, |z_2| \leq d,$

$$\mathbf{x}_1 G_M + \mathbf{r}_1 G_R + z_1 \neq \mathbf{x}_2 G_M + \mathbf{r}_2 G_R + z_2, \quad (87)$$

or equivalently, $\forall \mathbf{x} \in \mathbb{F}^\omega, \mathbf{x} \neq \mathbf{0},$

$$\mathbf{x} G_M \notin \{\mathbf{r} G_R + z : \mathbf{r} \in \mathbb{F}^k, z \in \mathbb{F}^m, |z| \leq 2d\}. \quad (88)$$

Let

$$G'_R = \begin{bmatrix} g_{r,1} \\ g_{r,2} \\ \vdots \\ g_{r,k} \end{bmatrix} \quad (89)$$

be the row-echelon form of G_R . We can always find $2d$ vectors, namely v_1, v_2, \dots, v_{2d} , from the set of standard basis of \mathbb{F}^m such that

$$g_{r,1}, g_{r,2}, \dots, g_{r,k}, v_1, v_2, \dots, v_{2d} \quad (90)$$

form a set of $k+2d$ linear independent vectors. Therefore,

$$|\{\mathbf{r} G_R + z : \mathbf{r} \in \mathbb{F}^k, z \in \mathbb{F}^m, |z| \leq 2d\}| \quad (91)$$

$$\geq |\langle \{g_{r,1}, g_{r,2}, \dots, g_{r,k}, v_1, v_2, \dots, v_{2d}\} \rangle| \quad (92)$$

$$= |\mathbb{F}|^{k+2d}, \quad (93)$$

where (92) follows from the fact that

$$\forall \mathbf{y} \in \langle \{g_{r,i}, 1 \leq i \leq k, v_j, 1 \leq j \leq 2d\} \rangle, \exists \mathbf{r} \in \mathbb{F}^k, z \in \mathbb{F}^m, |z| \leq 2d \text{ such that } \mathbf{y} = \mathbf{r} G_R + z.$$

By (88), the rank of G_M must be less than $m - 2d - k + 1$. Otherwise, the sink node cannot decode the information successfully. Therefore, the maximum rate at which information can be transmitted from the source node to all the sink nodes is at most $m - 2d - k$. \square

IV. CONCLUSION

In this paper, an algorithm in constructing a deterministic secure error-correcting (SEC) network code is proposed. We have shown that in the presence of malicious parties, by combining the idea of secure network code and error-correcting network code, information still can be multicast with complete secrecy and error tolerability at rate $m - 2d - k$, where k and d are the maximum number of channels the adversary can eavesdrop and contaminate, respectively.

REFERENCES

- [1] T. S. Han, "Nonnegative entropy measures of multivariate symmetric correlations," *Info. Contr.*, 36: 133-156, 1978.
- [2] N. Cai and R. W. Yeung, "Secure Network Coding", 2002 IEEE International Symposium on Information Theory.
- [3] N. Cai and R. W. Yeung, "Network coding and error correction," *IEEE Information Theory Workshop*, Bangalore, India, 2002.
- [4] R. W. Yeung and N. Cai, "Network error correction, Part I: basic concepts and upper bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 19-36, 2006.
- [5] N. Cai and R. W. Yeung, "Network error correction, Part II: lower bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp.37-54, 2006.
- [6] Z. Zhang, "Network error correction coding in packetized networks," 2006 IEEE Information Theory Workshop, Oct. 2006.
- [7] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of byzantine adversaries," *IEEE INFOCOM*, 2007.
- [8] S. Jaggi, and M. Langberg, "Resilient network codes in the presence of eavesdropping Byzantine adversaries," 2007 IEEE International Symposium on Information Theory.
- [9] S. Yang and R. W. Yeung, "Characterizations of Network Error Correction/Detection and Erasure Correction," *NetCod 2007*.
- [10] S. Yang, C. K. Ngai and R. W. Yeung, "Construction of Linear Network Codes that Achieve a Refined Singleton Bound," 2007 IEEE International Symposium on Information Theory.
- [11] S. Yang, and R. W. Yeung, "Refined Coding Bounds for Network Error Correction," *IEEE Information Theory Workshop*, Bergen, Norway, 2007.
- [12] C. K. Ngai and S. Yang, "Deterministic Secure Error-Correcting (SEC) Network Codes," *Information Theory Workshop*, Lake Tahoe, USA, 2007.
- [13] R. W. Yeung, *Information Theory and Network Coding*, Springer 2008.
- [14] R. W. Yeung and N. Cai, "On the optimality of a construction of a secure network codes," 2008 IEEE International Symposium on Information Theory.