Universal Secure Error-Correcting Schemes for Network Coding

Danilo Silva
School of Electrical and Computer Engineering
State University of Campinas (Unicamp), Brazil
danilo@decom.fee.unicamp.br

Frank R. Kschischang
Department of Electrical and Computer Engineering
University of Toronto, Canada
frank@comm.utoronto.ca

Abstract—This paper considers the problem of securing a linear network coding system against an adversary that is both an eavesdropper and a jammer. The network is assumed to transport n packets from source to each receiver, and the adversary is allowed to eavesdrop on μ arbitrarily chosen links and also to inject up to t erroneous packets into the network. The goal of the system is to achieve *zero-error* communication that is information-theoretically secure from the adversary. Moreover, this goal must be attained in a universal fashion, i.e., regardless of the network topology or the underlying network code. An upper bound on the achievable rate under these requirements is shown to be $n - \mu - 2t$ packets per transmission. A scheme is proposed that can achieve this maximum rate, for any n and any field size q, provided the packet length m is at least n symbols. The scheme is based on rank-metric codes and admits low-complexity encoding and decoding. In addition, the scheme is shown to be optimal in the sense that the required packet length is the smallest possible among all universal schemes that achieve the maximum rate.

I. INTRODUCTION

Consider a network implementing linear network coding for multicast [1]. The network may be subject to two types of attacks: a malicious user injects corrupt packets into the network in order to disrupt communication; an unauthorized eavesdropper intercepts packet transmissions in order to obtain as much information as possible about the transmitted messages. The linear mixing performed by network coding presents challenges to coding schemes in both scenarios, and has motivated a significant amount of research.

This paper considers the problem of dealing with the aforementioned attacks in a universal fashion, i.e., in a way that is completely independent of the network topology and the specific network code. This has the advantage of producing schemes that are compatible with noncoherent (random) network coding [2]. Also, we focus on the most stringent requirements of *zero* error probability and *zero* information leakage, i.e., perfectly reliable and perfectly secure (in the information-theoretic sense) communication.

Most of the previous work on this problem deals with the special cases where only error control or only security is required. A dividing assumption among these works refers to the constraints on the packet length m. For a system that is required to work under any packet length (in particular, under $m = 1$), the error control problem has been extensively discussed in [3]–[5] (see references therein) and the security problem has also received significant attention [6]–[8]. In all of these works, the proposed solutions require knowledge of the network code, and therefore are not universal. On the other hand, universal schemes have been proposed for the case where m is required to be sufficiently large; this is the approach taken in [9], [10] for error control and in [11] for security.

When both requirements of error control and security are combined, the problem becomes harder, and a simple concatenation of an error control scheme and a security scheme may not necessarily work. The reason is that, if error control coding is followed by security coding, the overall codeword may not be robust to errors and, similarly, if security coding is followed by error control coding, the overall codeword may not be robust to eavesdropping. Previous work on this problem has been limited[1] to non-universal schemes [13], [14], which require knowledge of the network code.

In this paper, we propose a *universal* scheme that achieves perfectly reliable and perfectly secure communication. Namely, in a network with a maxflow of n packets, if at most t error packets are injected in the network, and at most μ packets are observed by an eavesdropper, then our scheme can provide perfectly secure and reliable communication while achieving a rate of $k = n - 2t - \mu$ packets per transmission. This rate is shown to be optimal. Note that a similar upper bound on rate has been shown [14] in the context of non-universal network coding with $m = 1$, but it does not apply to the problem considered here (since it ignores the possibility of exploiting $m > 1$ in the coding scheme).

A requirement of our scheme is that the packet length m must be at least n symbols. We show that this value is optimal, in the sense that it is the smallest packet length of a universal scheme achieving the maximum rate.

A main tool in the design and analysis of our scheme is the theory of rank-metric codes [15]. We show that our scheme can benefit from existing efficient algorithms for rank-metric codes [10], [16], and therefore can be encoded and decoded with low complexity.

[1]except for an earlier, suboptimal version of this work [12]. There, a compatible concatenation of error control coding and security coding is used over an extension of an extension field. However, the packet length required is on the order of n^2, which is far from optimal.

It is worth mentioning that there is another line of work that relaxes the assumption of zero error probability (requiring, instead, vanishingly small error probability) [17]–[19]. In this case, even higher rates can be achieved [19], however, the packet length must be asymptotically large.

The remainder of the paper is organized as follows. Section II establishes the notation used and reviews background material on rank-metric codes and linear network coding. In Section III, we define the problem of combined error control and security. In Section IV, we review existing techniques for the special cases of either error control or security only. We also provide new results and insights for these scenarios, which will be useful for our proposed scheme. In Section V, we present our scheme and show that it achieves the desired goals. In Section VI, we prove that our scheme is optimal both in the sense of maximal rate and smallest packet length. In Section VII, we discuss how the scheme can be extended to the case of noncoherent network coding. Finally, Section VIII presents our conclusions.

The full version of this work has been incorporated in [20].

II. BACKGROUND

A. Notation

Let $\mathbb{F}_q$ be a finite field. Let $\mathbb{F}_q^{n \times m}$ denote the set of all $n \times m$ matrices over $\mathbb{F}_q$, and set $\mathbb{F}_q^n = \mathbb{F}_q^{n \times 1}$. Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$. Recall that $\mathbb{F}_{q^m}$ is an m-dimensional vector space over $\mathbb{F}_q$. Thus, by fixing a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, elements of $\mathbb{F}_{q^m}$ may be viewed as (row) vectors in $\mathbb{F}_q^{1 \times m}$ and vice-versa. This identification will be used extensively throughout the paper. In particular, we may view a column vector in $\mathbb{F}_{q^m}^n$ as a matrix in $\mathbb{F}_q^{n \times m}$ and vice-versa.

B. Rank-Metric Codes

Let $X, Y \in \mathbb{F}_q^{n \times m}$ be matrices. The *rank distance* between X and Y is defined as $d_{\mathrm{R}}(X, Y) \triangleq \mathrm{rank}(Y - X)$. As observed in [15], the rank distance is indeed a *metric*.

A *rank-metric code* $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ is a matrix code (i.e., a nonempty set of matrices) used in the context of the rank metric. The *minimum rank distance* of $\mathcal{C}$, denoted $d_{\mathrm{R}}(\mathcal{C})$, is the minimum rank distance between all pairs of distinct codewords of $\mathcal{C}$.

There is a rich coding theory for rank-metric codes that is analogous to the classical coding theory in the Hamming metric. In particular, the Singleton bound for the rank metric [10], [15] states that every rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with minimum rank distance d must satisfy

$$|\mathcal{C}| \leq q^{\max\{n,m\}(\min\{n,m\}-d+1)}. \quad (1)$$

Codes that achieve this bound are called *maximum-rank-distance* (MRD) codes and they are known to exist for all choices of parameters q, n, m and $d \leq \min\{n, m\}$ [15].

In the context of the bijection between $\mathbb{F}_q^{1 \times m}$ and $\mathbb{F}_{q^m}$, a rank-metric code may described as a block code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of length n over $\mathbb{F}_{q^m}$. (Note that, differently from classical coding theory, here we treat each codeword as a *column vector*. However, to avoid confusion, we will keep the standard notation on generator and parity-check matrices of linear codes.)

It is particularly useful to consider *linear* block codes over $\mathbb{F}_{q^m}$. For $m \geq n$, an important family of such codes was proposed by Gabidulin [15]. A *Gabidulin code* is an $[n, k]$ linear code over $\mathbb{F}_{q^m}$ defined by the generator matrix

$$G = [G_{ij}] = \left[g_{(j-1)}^{q^{(i-1)}} \right], \quad i = 1, \ldots, k, \, j = 1, \ldots, n \quad (2)$$

where the elements $g_0, \ldots, g_{n-1} \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$. It is shown in [15] that the minimum rank distance of a Gabidulin code is $d = n - k + 1$, so the code is MRD.

C. Linear Network Coding

The basic model for a (multicast) communication system using linear network coding is that of a finite-field matrix channel. At each channel use (generation) a source node transmits a batch of n packets, each consisting of m symbols from a finite field $\mathbb{F}_q$, which can be regarded as the rows of a matrix $X \in \mathbb{F}_q^{n \times m}$. Each link in the network transports a packet free of errors, and each node creates outgoing packets as $\mathbb{F}_q$-linear combinations of incoming packets. The specification of all such linear combinations defines the network code. The packets received by a (specific) destination node can be regarded as the rows of an $N \times m$ matrix $Y = AX$, where $A \in \mathbb{F}_q^{N \times n}$ is the transfer matrix that describes the linear transformations incurred by packets on route to the destination. The system is said to be *coherent* if A is known to each corresponding destination; otherwise, it is said to be *noncoherent*. The linear network code is said to be *feasible* if every transfer matrix to a destination has rank n (so that, in a coherent system, each destination is able to recover X).

The system described above is referred to as an $(n \times m, k)_q$ *linear coded network*, where k denotes the minimum rank among all transfer matrices. Thus, an $(n \times m, n)_q$ linear coded network contains a feasible network code.

III. PROBLEM STATEMENT

For simplicity, we restrict attention to a single destination, since all the results in this paper can be immediately extended to multiple destinations. In addition, we focus on the fundamental case of coherent network coding; extensions to noncoherent network coding are described in Section VII.

The basic model for linear network coding described in Section II-C can be extended to incorporate packet errors. Suppose that at most t errors can occur in any of the links, causing the corresponding packets to become corrupted. In this case, we will say that the network *is subject to t errors*. Assuming, without loss of generality, an additive error model, the matrix received by the destination can be expressed as

$$Y = AX + DZ$$

where $Z \in \mathbb{F}_q^{t \times m}$ is a matrix consisting of the error packets injected and $D \in \mathbb{F}_q^{N \times t}$ is the transfer matrix from the affected links to the destination. Note that D depends on the set of links in error.

This model can be further extended to include an eavesdropper adversary, in the spirit of the wiretap channel II of Ozarow and Wyner [21]. The eavesdropper is assumed to have access to the packets transmitted on any μ arbitrarily chosen links in the network. In this case, we will say that the network *is subject to μ observations*. Let $W \in \mathbb{F}_q^{\mu \times m}$ be a matrix consisting of the packets observed by the eavesdropper. Then W can be expressed as

$$W = BX$$

where $B \in \mathbb{F}_q^{\mu \times n}$ is the transfer matrix from the source node to the eavesdropper. Note that B depends on the set of intercepted links.

To ensure secure and reliable communication, the source node chooses the matrix X as the (possibly stochastic) encoding of some message $S \in \mathcal{S}$ (which should be recovered by the destination but not by the eavesdropper). The coding scheme is said to be *zero-error* if S can be uniquely determined from Y, i.e., $H(S|Y) = 0$. Here we assume that A is a constant known to all, while $D \in \mathbb{F}_q^{N \times t}$ and $Z \in \mathbb{F}_q^{t \times m}$ are unknown random variables with unknown distributions (which may depend on X). A zero-error scheme, in this context, may also be called *t-error-correcting* scheme. A scheme is said to be *universally t-error-correcting* if it satisfies

$$H(S|Y) = 0, \quad \forall A\colon \text{rank } A = n \qquad (3)$$

for any arbitrary distributions on D and Z. In other words, a universally t-error-correcting scheme must provide reliable communication for any of the choice of the (feasible) linear network code.

The coding scheme is said to be *(perfectly) secret* if the eavesdropper gets no information about the message, i.e., if $I(S;W) = 0$. Note that this requirement depends on the choice of B. A scheme is said to be *universally (perfectly) secret* under μ observations if it satisfies

$$I(S;W) = 0, \quad \forall B \in \mathbb{F}_q^{\mu \times m}. \qquad (4)$$

In other words, a universally secret scheme must guarantee secrecy for any choice of the linear network code.

In this paper, we are interested in schemes that are both universally t-error-correcting and universally secret under μ observations, i.e., schemes that satisfy both (3) and (4).

IV. SPECIAL CASES

A. Error Control Only

Consider an $(n \times m, n)_q$ linear network subject to t errors but $\mu = 0$ observations. In this case, condition (4) can be ignored.

In the case of a deterministic encoding, the following characterization is given in [22].

Theorem 1 ([22]): Consider a deterministic encoder mapping $S \in \mathcal{S}$ to $X \in \mathbb{F}_q^{n \times m}$ whose image is given by $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$. There exists a universally t-error-correcting scheme with this encoder if and only if $d_{\mathrm{R}}(\mathcal{C}) \geq 2t + 1$.

From the Singleton bound (1), it can be seen that the maximum rate achievable by a universally t-error-correcting scheme is given by $\max\{n, m\}(\min\{n, m\} - 2t)$ symbols per transmission, and it is achieved by an MRD code. In particular, the rate of $n - 2t$ packets per transmission is achievable only if $m \geq n$.

In the case of a stochastic encoding, the result above does not necessarily hold, since it is conceivable that recovering S from Y does not necessarily enable the receiver to recover X. Still, it is possible to obtain the following equivalence result, which will be very useful in the sequel.

Theorem 2: Consider a stochastic encoding from $S \in \mathcal{S}$ to $X \in \mathbb{F}_q^{n \times m}$. The encoding admits a universally t-error-correcting scheme if and only if it admits a zero-error scheme for the coherent channel $Y = AX$, for all full-rank $A \in \mathbb{F}_q^{(n-2t) \times n}$.

Proof: See [20]. ∎

Essentially, Theorem 2 shows that any coding scheme that corrects t packet errors can be modified at the decoder to instead correct $2t$ "packet erasures" (i.e., rank deficiency), and vice-versa.

B. Security Only

Consider an $(n \times m, n)_q$ linear coded network subject to μ observations but $t = 0$ errors. In this case, $H(X|Y) = 0$; thus, condition (3) can be replaced by $H(S|X) = 0$.

It is shown in [20] that the maximum number of symbols per transmission that can be reliably communicated with a universally secret scheme is upper bounded by $m(n - \mu)$. Moreover, this rate is achievable only if $m \geq n$.

A scheme is proposed in [11], [20] that is able to achieve this maximum rate. The scheme uses Ozarow-Wyner coset coding [21] based on linear MRD codes. In order to describe the scheme, it is convenient to use the bijection described in Section II-A and think of vectors in $\mathbb{F}_q^{1 \times m}$ as elements of the extension field $\mathbb{F}_{q^m}$. Note that this is used solely to perform the encoding and decoding operations at the source and destination nodes, and has no impact in the $\mathbb{F}_q$-linear network coding operations performed at the internal nodes.

Let $\mathcal{C}$ be an $[n, \mu]$ linear code over $\mathbb{F}_{q^m}$ with parity-check matrix $H \in \mathbb{F}_{q^m}^{k \times n}$, where $k = n - \mu$. Let the message be given by $S \in \mathbb{F}_{q^m}^k$. Encoding is performed by choosing $X \in \mathbb{F}_{q^m}^n$ uniformly at random such that $S = HX$. In other words, S is viewed as a syndrome specifying a coset of $\mathcal{C}$, and X is chosen as a random word from that coset. Decoding is performed simply by computing $S = HX$. It is shown in [20] that this scheme is universally secret if and only if $\mathcal{C}$ is an MRD code and $m \geq n$.

We now describe a convenient way to perform the encoding process. Let $T \in \mathbb{F}_{q^m}^{n \times n}$ be an invertible matrix such that H corresponds to the first k rows of T^{-1}. Given a message $S \in \mathbb{F}_{q^m}^k$, the encoder chooses $V \in \mathbb{F}_{q^m}^{(n-k)}$ uniformly at random and independently from S, and produces $X \in \mathbb{F}_{q^m}^n$ by computing

$$X = T \begin{bmatrix} S \\ V \end{bmatrix}.$$

Note that $S = HX$. It is easy to show that $H(X|S) = n - k$, i.e., X is chosen uniformly at random given S. Thus, this encoder indeed implements a coset coding approach.

We now give a security condition based directly on the matrix T rather than its inverse.

Proposition 3: The encoder described above is universally secure under $\mu \leq n - k$ observations if the last $n - k$ rows of T^T form a generator matrix of an $[n, n - k]$ linear MRD code over $\mathbb{F}_{q^m}$ with $m \geq n$.

Proof: Let $G \in \mathbb{F}_{q^m}^{(n-k) \times n}$ and $G_1 \in \mathbb{F}_{q^m}^{k \times n}$ be such that $T^T = \begin{bmatrix} G_1 \\ G \end{bmatrix}$. Then

$$\begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} = T^{-1}T = \begin{bmatrix} H \\ H_1 \end{bmatrix} \begin{bmatrix} G_1^T & G^T \end{bmatrix} = \begin{bmatrix} HG_1^T & HG^T \\ H_1 G_1^T & H_1 G^T \end{bmatrix}.$$

Thus, $HG^T = 0$. Since both G and H are full-rank, it follows that G and H are generator and parity-check matrices, respectively, for exactly the same code. ∎

V. PROPOSED SCHEME

In this section, we propose a scheme that is universally t-error-correcting and universally secret under μ observations. The scheme achieves a rate of $n - \mu - 2t$ packets per transmission and requires the packet length m to be at least n symbols. The scheme can be seen as a combination of the strategies for error control and security described in Section IV, designed in such a way that they can be coupled without violating conditions (3) and (4). In what follows we make use of the identification between $\mathbb{F}_q^{1 \times m}$ and $\mathbb{F}_{q^m}$ described in Section II-A.

Assume that $m \geq n$ and $0 < k \leq n - \mu - 2t$. Let $G \in \mathbb{F}_{q^m}^{(k+\mu) \times n}$ be a generator matrix of an $[n, k + \mu]$ linear MRD code over $\mathbb{F}_{q^m}$. Suppose that the last μ rows of G form a generator matrix $G_{\text{sec}} \in \mathbb{F}_q^{\mu \times n}$ of an $[n, \mu]$ linear MRD code over $\mathbb{F}_{q^m}$.

Encoding proceeds as follows. Given a message $S \in \mathbb{F}_{q^m}^k$, the encoder first produces an auxiliary variable

$$U = \begin{bmatrix} S \\ V \end{bmatrix}$$

by choosing $V \in \mathbb{F}_{q^m}^\mu$ is uniformly at random and independently from S. Then, the encoder computes

$$X = G^T U.$$

Note that the mapping from U to X is a deterministic mapping whose image is (a subset of) $\mathcal{C} = \{G^T u, u \in \mathbb{F}_{q^m}^{(k+\mu)}\}$. It follows from Theorem 1 that, when X is transmitted over an $(n \times m, n)_q$ linear coded network subject to t errors, the receiver can uniquely determine U (and therefore S) if $d_R(\mathcal{C}) > 2t$. Since $\mathcal{C}$ is an $[n, k + \mu]$ linear MRD code over $\mathbb{F}_{q^m}$, with $m \geq n$, we have that $d_R(\mathcal{C}) = n - k - \mu + 1 \geq 2t + 1$. Thus, the scheme is universally t-error-correcting.

In particular, decoding can be performed in two steps: first, applying a decoder for $\mathcal{C}$ in order to find $U \in \mathbb{F}_{q^m}^{k+\mu}$; then, extracting the message S as the first k rows of U.

In order to prove the secrecy of the scheme, consider first an alternative interpretation. Let $T \in \mathbb{F}_{q^m}^{n \times n}$ be an invertible matrix such that the last $k + \mu$ rows of T^T correspond to the matrix G. Then, we have

$$X = G^T U = T \begin{bmatrix} 0 \\ U \end{bmatrix} = T \begin{bmatrix} S' \\ V \end{bmatrix}, \quad \text{where} \quad S' = \begin{bmatrix} 0 \\ S \end{bmatrix}.$$

In other words, the encoder is identical to the encoder described in Section IV-B if S' is taken as the message. Furthermore, we have that the last μ rows of T^T correspond to G_{sec}, which is the generator matrix of an $[n, \mu]$ linear MRD code over $\mathbb{F}_{q^m}$. Thus, by Proposition 3 (which holds regardless of the message distribution), we have that the scheme is universally secret under μ observations.

The above analysis proves the following result.

Theorem 4: The scheme described above is universally t-error-correcting and universally secret under μ observations.

Our proposed scheme relies on the assumption that a generator matrix G for an $[n, k + \mu]$ linear MRD code $\mathcal{C}$ exists such that its last μ rows form a generator matrix for another $[n, \mu]$ linear MRD code. It is easy to see that, if G is taken as a generator matrix of a Gabidulin code given in the form (2), then any μ consecutive rows of G (in particular the last ones) indeed form a generator matrix of an MRD sub-code. In this case, decoding of $\mathcal{C}$ can be efficiently performed using the methods in [10], [12], [16].

VI. CONVERSE RESULTS

In this section, we prove that our proposed scheme is optimal, both in the sense of achieving the maximum possible rate and in the sense of requiring the minimum possible packet length among all schemes that achieve this maximum rate.

Theorem 5: Consider an $(n \times m)_q$ linear coded network. Assume that the source message has entropy of k packets. There exists a scheme that is universally t-error-correcting and universally secure under μ observations only if $k \leq n - 2t - \mu$. Moreover, this maximum rate can be attained only if $m \geq n$.

Proof: Let $n' = n - 2t$. Let $B \in \mathbb{F}_q^{\mu \times n}$ be a full-rank matrix and let $A \in \mathbb{F}_q^{n' \times n}$ be a full-rank matrix such that $B = PA$ for some (necessarily full-rank) $P \in \mathbb{F}_q^{\mu \times n'}$. Let $Y_A = AX$ and $W_B = BX = PY_A$. If the encoder admits a scheme that is universally t-error-correcting then, by Theorem 2, it also admits a scheme that is zero-error for the coherent channel $Y_A = AX$. Thus, there is a function $f_A \colon \mathbb{F}_q^{n' \times m} \to \mathcal{S}$ such that $S = f_A(Y_A)$. In particular, there is also a function $f \colon \mathbb{F}_q^{n \times m} \to \mathcal{S}$ such that $S = f(X)$. Thus, we may write $\mathcal{X}_s = \{x \in \mathbb{F}_q^{n \times m} : f(x) = s\}$. Now,

$$\begin{aligned}
k &= H(S) \\
&= H(S|Y_A, W_B) + I(S; Y_A, W_B) \\
&= I(S; Y_A, W_B) \\
&= I(S; W_B) + I(S; Y_A|W_B) \\
&= I(S; Y_A|W_B) \\
&= H(Y_A|W_B) - H(Y_A|S, W_B)
\end{aligned} \quad \begin{aligned} \\ \\ (5) \\ \\ (6) \\ \end{aligned}$$

$$\leq H(Y_A|W_B) \tag{7}$$
$$\leq n' - \text{rank } P = n' - \mu \tag{8}$$

where (5) follows since S is a function of Y_A and (6) follows since $I(S;W_B) = 0$. This proves the first statement. Now consider the second statement. Since (8) holds with equality, we must have $H(Y_A|S,W_B) = 0$ and $H(Y_A|W_B) = n' - \mu$. Note that these conditions hold for all full-rank B and all $A \in \mathcal{A}_B$, where

$$\mathcal{A}_B = \{A \in \mathbb{F}_q^{n' \times n} : \text{rank } A = n', \langle B \rangle \subseteq \langle A \rangle\}$$

and $\langle \cdot \rangle$ denotes the row space of a matrix. This implies that $H(\{Y_A : A \in \mathcal{A}_B\}|S,W_B) = 0$ and therefore $H(\bar{Y}_B|S,W_B) = 0$, where $\bar{Y}_B = \bar{A}_B X$ and $\bar{A}_B$ is the matrix consisting of the vertical stacking of all matrices in $\mathcal{A}_B$. It is not hard to see that, as long as $n' > \mu$, $\text{rank } \bar{A}_B = n$. (In fact, $\bar{A}_B$ contains every nonzero vector of $\mathbb{F}_q^{1 \times n}$ as one of its rows.) It follows that $H(X|S,W_B) = 0$, for all full-rank B. Thus, X must be uniquely determined given $W_B = BX$ and the indication that $X \in \mathcal{X}_S$. From Theorem 1, this implies that each $\mathcal{X}_s$ must be a rank-metric code with $d_R(\mathcal{X}_s) \geq n - \mu + 1$.

On the other hand, we have seen that, for each full-rank $A \in \mathbb{F}_q^{n' \times n}$, it holds that $H(Y_A|W_B) = n' - \mu$ for *all* full-rank $P \in \mathbb{F}_q^{\mu \times n'}$, where $W_B = PY_A$ and $B = PA$. By the chain rule of entropy, it is not hard to see that this implies that Y_A is uniform (for instance, by choosing some P's that are submatrices of an identity matrix, as in the wiretap channel II). Thus, $H(Y_A) = n'$, which implies that $H(X) \geq n'$. Since $H(X) = H(X,S) = H(S) + H(X|S)$, we have that $H(X|S) \geq n' - k = \mu$. Thus, there must be some $s \in \mathcal{S}$ such that $H(X|S = s) \geq \mu$, which implies that $|\mathcal{X}_s| \geq q^{m\mu}$. Together with the fact that $d_R(\mathcal{X}_s) \geq n - \mu + 1$, we can see, from the Singleton bound (1), that this can only happen if $m \geq n$. ∎

VII. EXTENSION TO NONCOHERENT NETWORK CODING

The scheme described in the paper is suitable for coherent network coding and is indeed optimal. In the case of noncoherent network coding, the scheme can be adapted by including appropriate packet headers. More precisely, the transmission matrix should be $\begin{bmatrix} I & X \end{bmatrix}$, where X is the transmission matrix of the original scheme. Clearly, including packet headers does not affect security, but it allows the scheme to be decoded when the transfer matrix A is unknown. It is shown in [10] that such adaptation preserves the error-correcting capability of the code, so the universally t-error-correcting property is maintained. Although the rate achieved in this case is no longer optimal, it is very close to optimal for all practical packet lengths [10].

VIII. CONCLUSION

In this paper, we have proposed a *universal* end-to-end coding scheme that can guarantee *perfectly secure* and *perfectly reliable* communication over a linear coded network subject to malicious interference and eavesdropping. The scheme is *optimal* both in the sense of achieving the maximum possible rate as well as requiring the smallest possible packet length. The scheme is based on rank-metric codes and admit efficient encoding and decoding algorithms.

REFERENCES

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

[2] 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.

[3] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds; part II: Lower bounds," *Commun. Inform. Syst.*, vol. 6, no. 1, pp. 19–54, 2006.

[4] Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 209–218, 2008.

[5] S. Yang, R. W. Yeung, and Z. Zhang, "Weight properties of network codes," *European Transactions on Telecommunications*, vol. 19, no. 4, pp. 371–383, 2008.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inform. Transm.*, vol. 21, no. 1, pp. 1–12, 1985.

[16] D. Silva and F. R. Kschischang, "Fast encoding and decoding of Gabidulin codes," in *Proc. IEEE Int. Symp. Information Theory*, Seoul, Korea, Jun. 28–Jul. 3, 2009, pp. 2858–2862.

[17] 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.

[18] 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.

[19] H. Yao, D. Silva, S. Jaggi, and M. Langberg, "Network codes resilient to jamming and eavesdropping," in *IEEE Int. Symp. Network Coding*, 2010, to be published. [Online]. Available: http://arxiv.org/abs/1001.3714

[20] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inf. Theory*, 2010, submitted for publication (revised version). [Online]. Available: http://arxiv.org/abs/0809.3546

[21] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Proc. EUROCRYPT 84 workshop on Advances in cryptology: theory and applicationof cryptographic techniques*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 33–51.

[22] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.