Secure-broadcast codes over linear-deterministic channels

Ashish Khisti
ECE Dept.
University of Toronto
Toronto, ON,
akhisti@comm.utoronto.ca

Danilo Silva
School of Electrical and Computer Engineering
State University of Campinas - UNICAMP
Campinas, SP, Brazil
danilo@decom.fee.unicamp.br

Frank Kschischang
ECE Dept.
University of Toronto
Toronto, ON,
frank@comm.utoronto.ca

***Abstract*—We study a non-multicast secure network coding problem with two receivers. First we study a linear-deterministic channel model with two receivers and a collection of eavesdroppers, which generalizes the Ozarow-Wyner wiretap channel II. The secrecy capacity region for independent and common messages is characterized and is achieved by concatenating a coset-coding scheme based on maximum rank distance codes with a repetition code. By applying our coding scheme at the source node of a network that uses an underlying generic network code we also establish the secrecy capacity region of a network coding problem with two sinks and one sender node.**

I. Introduction

The wiretap channel, introduced by Wyner [10], characterizes the maximum rate of reliable information transfer under a secrecy constraint. Ozarow and Wyner [4] develop a coset coding approach for the erasure wiretap channel and characterize its secrecy capacity under a stronger model for the eavesdropper. More recently connections between the Ozarow-Wyner model and secure network coding [1] have been identified [6]. In [9] the authors observe that a linear maximum-rank-distance (MRD) code in the coset coding scheme is universal. Its construction neither imposes any constraints nor requires any knowledge of the underlying network code. Thus the problem of secure network coding can be reduced to that of communicating over linear and deterministic channels.

The present paper studies the problem of broadcasting information to two receivers over linear and deterministic channels. The eavesdropper's channel transfer matrix can be arbitrary but satisfies a rank constraint. We characterize the secrecy capacity region for transmitting independent and common messages to the two users. Our coding scheme involves (a) enlarging the dimension of common subspace between the two receivers by repeating a certain number of symbols in their orthogonal subspace and (b) applying coset coding based on a block diagonal parity check matrix of a MRD code of suitable dimension.

Applying our coding scheme to a network with one sender node and two sink nodes we characterize the secrecy capacity region for the one sender two sink multi source secure network coding problem. To the best of our knowledge this result appears to be new and compliments an analogous result without the secrecy constraint (see e.g., [5] and references therein).

II. Problem Statement and Main Result

A. Channel Model

The channels of the two legitimate receivers are linear and deterministic i.e.,

$$\mathbf{y}_1(t) = A_1\mathbf{x}(t), \quad \mathbf{y}_2(t) = A_2\mathbf{x}(t) \tag{1}$$

where the rank of transfer matrices $A_i \in \mathbb{F}_q^{r_i \times n}$ is r_i and $t = 1, 2, \ldots$ denotes the discrete time index. The channel matrices remain constant throughout the duration of transmission and are known to all terminals. Define

$$r_{12} = \text{rank}\begin{bmatrix} A_1 \\ A_2 \end{bmatrix}, \qquad \Delta = r_1 + r_2 - r_{12} \tag{2}$$

where Δ denotes the dimension of the common row-space between A_1 and A_2.

In addition to the two receivers we also consider a class of eavesdroppers whose channels are linear and deterministic and whose channel transfer matrices have a rank that does not exceed μ,

$$\mathcal{Z} = \left\{ \mathbf{z}(t) = B \cdot \mathbf{x}(t) \;\middle|\; B \in \mathbb{F}_q^{\mu \times n},\ \text{rank}(B) \le \mu \right\}. \tag{3}$$

B. Secure-Broadcast Code

The message pair (m_0, m_i) needs to be delivered to receiver i for $i \in \{1, 2\}$. A length L, rate (R_0, R_1, R_2) *secure broadcast code* for this channel consists of

1) Information sets $\mathcal{I}_k = \left\{1, 2, \ldots, 2^{LR_k \cdot \log_2 |\mathbb{F}_q|}\right\}$, for $k = 0, 1, 2$, and the message m_k is uniformly distributed over $\mathcal{I}_k$. We will further assume that the pair (R_0, R_1, R_2) is an integer tuple[1].
2) A set of possibly stochastic encoding functions $\mathcal{F}_t : \mathcal{I}_0 \times \mathcal{I}_1 \times \mathcal{I}_2 \to (\mathbb{F}_q)^n$ for $t = 1, 2, \ldots L$ that map the given messages (m_0, m_1, m_2) into channel input symbols $\mathbf{x}(1), \ldots, \mathbf{x}(L)$.
3) A pair of decoding functions $\mathcal{G}_i : \mathbb{F}_q^{n \times L} \to \mathcal{I}_0 \times \mathcal{I}_i$ that produce a message estimate $(\hat{m}_0, \hat{m}_i) = \mathcal{G}_i(\mathbf{y}_i(1), \ldots, \mathbf{y}_i(L))$, for $i = 1, 2$.

[1] As will be evident, the corner points in our capacity region are integer tuples. Hence all the remaining points can be obtained by time-sharing between these corner points.

978-1-4244-7892-7/10/$26.00 ©2010 IEEE

A rate tuple (R_0, R_1, R_2) is achievable if there exists a sequence of length L secure broadcast codes such that $\Pr((\hat{m}_0, \hat{m}_1, \hat{m}_2) \neq (m_0, m_1, m_2)) \to 0$ as $L \to \infty$ and the secrecy constraint $I(m_0, m_1, m_2; \mathbf{z}(1), \ldots, \mathbf{z}(L)) \to 0$ is satisfied. The set of all achievable rate pairs constitutes the *secure broadcast capacity* region.

C. Channel Matrix Reduction

One useful property that we use throughout this paper is that without loss of generality, A_1 and A_2 can have the following cannonical structure:

$$A_1 = \begin{array}{c} \\ r_1-\Delta \\ \Delta \end{array} \begin{array}{c} \begin{array}{cccc} r_1-\Delta & r_2-\Delta & \Delta & n-r_{12} \end{array} \\ \left[\begin{array}{cccc} I & 0 & 0 & 0 \\ 0 & 0 & I & 0 \end{array}\right] \end{array}$$
$$A_2 = \begin{array}{c} \\ r_2-\Delta \\ \Delta \end{array} \begin{array}{c} \begin{array}{cccc} r_1-\Delta & r_2-\Delta & \Delta & n-r_{12} \end{array} \\ \left[\begin{array}{cccc} 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \end{array}\right] \end{array} \tag{4}$$

where recall that $\Delta = r_1 + r_2 - r_{12}$, and let I and 0 denote identity-matrix and zero-matrix of appropriate dimensions. This equivalence can be established through a series of linear invertible transformations at the sender and the receivers (see e.g., [7]).

Without loss of generality we assume that $n = r_{12}$ i.e., the dimension of null space common to A_1 and A_2 is zero. Clearly neither receiver sees any information transmitted in this subspace. Also any eavesdropper whose channel has dimensions in this subspace can be replaced with another channel that has a smaller rank and no dimensions in this subspace.

With this choice of matrices, we can partition the input vector

$$\mathbf{x} = \begin{array}{c} r_1-\Delta \\ r_2-\Delta \\ \Delta \end{array} \left[\begin{array}{c} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_\Delta \end{array}\right]$$

and assume that the receivers' observe

$$\mathbf{y}_1 = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_\Delta \end{bmatrix}, \quad \mathbf{y}_2 = \begin{bmatrix} \mathbf{x}_2 \\ \mathbf{x}_\Delta \end{bmatrix} \tag{5}$$

respectively. We will focus on the model (5) in the remainder of this paper.

D. Main Result

The following result characterizes the secrecy capacity region.

Theorem 1: The secrecy capacity region with common message is the union of all rate tuples (R_0, R_1, R_2) that satisfy $R_i \geq 0$ for $i = 0, 1, 2$ and

$$R_0 \leq \min(r_1 - \mu, r_2 - \mu) \tag{6}$$
$$R_0 + R_1 \leq r_1 - \mu \tag{7}$$
$$R_0 + R_2 \leq r_2 - \mu \tag{8}$$
$$R_0 + R_1 + R_2 \leq n - \mu. \tag{9}$$

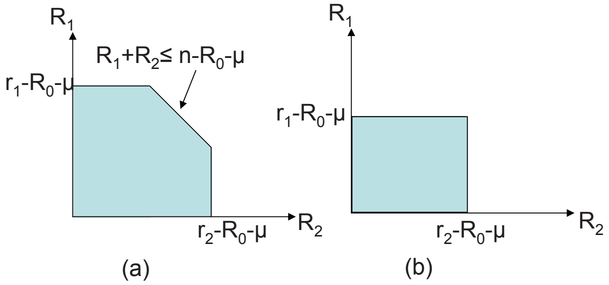

Fig. 1. Capacity region for secure broadcasting to two receivers . The common message rate is fixed to R_0 and the tradeoff between (R_1, R_2) is illustrated. The left hand plot corresponds to the case $\mu \leq \Delta$ and $R_0 \leq \Delta - \mu$. The right hand plot corresponds to the case when $\mu \leq \Delta$ and $\Delta - \mu \leq R_0 \leq \min(r_1, r_2) - \Delta$ and also when $\mu \geq \Delta$ and $0 \leq R_0 \leq \min(r_1, r_2) - \mu$. Note that in these two cases the sum-rate constraint in the capacity region is not active.

1) Structure of Capacity Region: To interpret the capacity region in Theorem 1 we fix R_0 and study the tradeoff between the independent message rate pair (R_1, R_2). As illustrated in Fig. 1 the capacity region takes one of two forms depending on whether the sum rate is active or not. When $\mu \leq \Delta$ and $R_0 \leq \Delta - \mu$ i.e., when $\mu + R_0 \leq \Delta$ the dominant boundary of the capacity region is the set of points that lie on the sum-rate constraint (9) and beyond the corner points i.e.,

$$\mathcal{D}_s = \{(R_1, R_2) \geq 0 \mid R_1 + R_2 = n - \mu - R_0,\ R_i \geq r_i - \Delta\} \tag{10}$$

whereas when $\mu + R_0 \geq \Delta$ the dominant boundary region is a single point

$$\mathcal{D}_b = \{(R_1, R_2) \mid R_1 = r_1 - \mu - R_0,\ R_2 = r_2 - \mu - R_0\}. \tag{11}$$

Our coding scheme exploits the following alternative characterization of the dominant boundary region.

Proposition 1: Let $\alpha = \max\{\mu + R_0 - \Delta, 0\}$, let $\tilde{n} = n - \alpha$ and $\tilde{\Delta} = \Delta + \alpha$. The set of rate pairs on the dominant boundary of the capacity region are characterized by

1) $R_0 + R_1 + R_2 = \tilde{n} - \mu$; and
2) $R_i \geq r_i - \tilde{\Delta}$, $i = 1, 2$.

Proof: Consider first the case $\Delta \geq \mu + R_0$. In this case $\alpha = 0$ and hence $\tilde{n} = n$ and $\tilde{\Delta} = \Delta$. The two constraints then define $\mathcal{D}_s$ in (10).

When $\Delta \leq \mu + R_0$ the rate pair in $\mathcal{D}_b$ is given by $R_i = r_i - \mu - R_0$, $i = 1, 2$. This implies that $R_i = r_i - \tilde{\Delta}$, $i = 1, 2$, since $\alpha = \mu + R_0 - \Delta$. Moreover, $R_0 + R_1 + R_2 = r_1 - \mu + r_2 - \tilde{\Delta} = \tilde{n} - \mu$. Thus, there is no loss of generality in assuming the conditions above. ■

Remark 1: The choice of α in Prop. 1 has a physical interpretation in the code construction. As illustrated in Fig. 2 α characterizes the number of symbols that get repeated in the orthogonal subspace of the two users. This increases the dimension of the common subspace from Δ to $\tilde{\Delta} = \Delta + \alpha$ while reducing the dimension of each orthogonal subspace by α units. The length of independent symbols in a codeword reduces from n to $\tilde{n} = n - \alpha$.

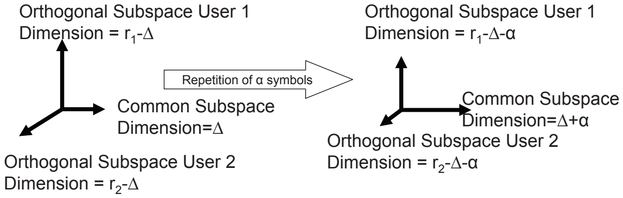

Fig. 2. Effect of repeating α symbols in each of the orthogonal subspaces of the two users. The dimension of the common subspace increases by α units whereas the dimension of each of the orthogonal subspaces decreases by α units. In the coding scheme we use $\alpha = \max(\mu + R_0 - \Delta, 0)$.

III. Converse for Theorem 1

We establish an upper bound in two steps. First we consider one possible eavesdropper and use standard information theoretic arguments to show that the capacity region lies inside a particular polyhedron. Then we show that the intersection of all such polyhedra contains the region stated in Theorem 1.

Proposition 2: Let $\mathcal{P}_x$ denote the set of all possible input distributions and let $\mathbf{z}_i = B_i \cdot \mathbf{x}$ denote one particular eavesdropper channel among the collection. Further, let $\mathcal{R}(p_x)$ denote the region consisting of rate pairs (R_0, R_1, R_2) that satisfy

$$\begin{aligned} R_0 &\leq \min(H(\mathbf{y}_1|\mathbf{z}_i), H(\mathbf{y}_2|\mathbf{z}_i)) \\ R_0 + R_1 &\leq H(\mathbf{y}_1|\mathbf{z}_i) \\ R_0 + R_2 &\leq H(\mathbf{y}_2|\mathbf{z}_i) \\ R_0 + R_1 + R_2 &\leq H(\mathbf{y}_1, \mathbf{y}_2|\mathbf{z}_i) \end{aligned} \tag{12}$$

with the entropy expressions evaluated for the joint distribution $p_{\mathbf{x},\mathbf{y}_1,\mathbf{y}_2,\mathbf{z}_i}(\cdot) = p_{\mathbf{x}}(\cdot) p_{\mathbf{y}_1,\mathbf{y}_2,\mathbf{z}_i|\mathbf{x}}(\cdot)$. The secrecy capacity region is contained in $\bigcup_{p_x \in \mathcal{P}_x} \mathcal{R}(p_x)$.

Note that the first constraint is a constraint on multicasting common message to the two receivers, the next two constraint in (12) above are single-user secrecy constraints with respect to eavesdropper $\mathbf{z}_i$, whereas the last constraint is a result of allowing both the receivers to cooperate. We omit a formal proof.

In what follows we use Prop. 2 to deduce the converse in Theorem 1. Recall that the constraint (6) on the common message rate follows from the capacity of single message multicast (e.g., [8]). To obtain the remaining constraints we separately consider the case when $\mu \leq \Delta$ and $\mu > \Delta$.

First consider the case when $\mu \leq \Delta$. Select an eavesdropper whose observations align with any μ symbols of $\mathbf{x}_\Delta$ i.e., say $\mathbf{z}_i(t) = [\mathbf{x}_{\Delta,1}(t), \ldots, \mathbf{x}_{\Delta,\mu}(t)]$, where $\mathbf{x}_{\Delta,j}(t)$ denotes the $j-$th symbol of the vector $\mathbf{x}_\Delta(t)$. Consequently for each $p_x \in \mathcal{P}_x$,

$$\begin{aligned} R_0 + R_1 &\leq H(\mathbf{y}_1|\mathbf{z}_i) \leq r_1 - \mu \\ R_0 + R_2 &\leq H(\mathbf{y}_2|\mathbf{z}_i) \leq r_2 - \mu \\ R_0 + R_1 + R_2 &\leq H(\mathbf{y}_1, \mathbf{y}_2|\mathbf{z}_i) \leq n - \mu. \end{aligned}$$

This establishes that any pair (R_0, R_1, R_2) in the capacity region satisfies the constraints in Theorem 1.

When $\mu > \Delta$ consider an eavesdropper who observes all the Δ symbols of $\mathbf{x}_\Delta$ and $\mu - \Delta$ additional symbols from $\mathbf{x}_1$. For such an eavesdropper we have that for each $p_x \in \mathcal{P}_x$,

$$R_0 + R_1 \leq H(\mathbf{y}_1|\mathbf{z}_i) \leq r_1 - \mu, \; R_0 + R_2 \leq H(\mathbf{y}_2|\mathbf{z}_i) \leq r_2 - \Delta.$$

Likewise if we consider another eavesdropper who observes Δ symbols from $\mathbf{x}_\Delta$ and $\mu - \Delta$ symbols of $\mathbf{x}_2$ we get that for each $p_x \in \mathcal{P}_x$,

$$R_0 + R_1 \leq H(\mathbf{y}_1|\mathbf{z}_i) \leq r_1 - \Delta, \; R_0 + R_2 \leq H(\mathbf{y}_2|\mathbf{z}_i) \leq r_2 - \mu.$$

An intersection of these two constraints gives $R_0 + R_i \leq r_i - \mu$. Finally as noted in section II-D1 the sum rate constraint (9) is not active in this case.

IV. Achievability for Theorem 1

We simplify the description of the coding scheme by using an extension field approach. Let $\mathbb{F}_q^{n \times L}$ denote the set of all $n \times L$ matrices over $\mathbb{F}_q$. Let the finite field $\mathbb{F}_{q^L}$ be a degree-L extension of $\mathbb{F}_q$. Since $\mathbb{F}_{q^L}$ is a vector space over $\mathbb{F}_q$, there is a vector space isomorphism $\phi : \mathbb{F}_q^{1 \times L} \leftrightarrow \mathbb{F}_{q^L}$. For all n, let $\phi_n : \mathbb{F}_q^{n \times L} \leftrightarrow \mathbb{F}_{q^L}^n$ be the vector space isomorphism defined by applying $\phi(\cdot)$ row-wise. We will omit the subscript from ϕ_n when the dimensions of the argument are clear from the context.

Let $X = \phi([\mathbf{x}(1) \quad \cdots \quad \mathbf{x}(L)]) \in \mathbb{F}_{q^L}^n$ and $Y_i = \phi([\mathbf{y}_i(1) \quad \cdots \quad \mathbf{y}_i(L)]) \in \mathbb{F}_{q^L}^{r_i}$, $i = 1, 2$. Note that, since ϕ is an $\mathbb{F}_q$-linear transformation, we have

$$Y_i = A_i X = \begin{bmatrix} X_i \\ X_\Delta \end{bmatrix} \qquad i = 1, 2$$

where $X_i = \phi([\mathbf{x}_i(1) \quad \cdots \quad \mathbf{x}_i(L)])$, $i = 1, 2, \Delta$. Similarly, we have

$$Z = BX$$

where $Z = \phi([\mathbf{z}(1) \quad \cdots \quad \mathbf{z}(L)]) \in \mathbb{F}_{q^L}^\mu$.

Now, assume that R_0, R_1, R_2 are integers, and consider a length L, rate (R_0, R_1, R_2) secure broadcast code. Without loss of generality, assume that $m_i \in \mathbb{F}_{q^L}^{R_i}$, $i = 0, 1, 2$, and let $m = \begin{bmatrix} m_1 \\ m_2 \\ m_0 \end{bmatrix}$. Then, we can view the code as consisting of a stochastic encoding that maps m to X and two decoders that map each Y_i to an estimate $(\hat{m}_0, \hat{m}_i)$ of (m_0, m_i), $i = 1, 2$.

A. Coding Scheme

Our coding scheme is a specific form of Ozarow-Wyner coset coding (over the extension field $\mathbb{F}_{q^L}$) for the combined message m. Let

$$H = \begin{array}{c} \\ R_1 \\ R_2 \\ R_0 \end{array} \begin{array}{c} \begin{array}{ccc} r_1 - \tilde{\Delta} & r_2 - \tilde{\Delta} & \tilde{\Delta} \end{array} \\ \begin{bmatrix} H_{11} & 0 & H_{1\Delta} \\ 0 & H_{22} & H_{2\Delta} \\ 0 & 0 & H_{0\Delta} \end{bmatrix} \end{array} \tag{13}$$

be a full-rank $(R_0 + R_1 + R_2) \times \tilde{n}$ matrix over $\mathbb{F}_{q^L}$. Encoding is performed by first selecting $\tilde{X} \in \mathbb{F}_{q^L}^{\tilde{n}}$ uniformly at random such that $m = H\tilde{X}$. In other words, if $\mathcal{C}$ is the $[\tilde{n}, \tilde{n} - R_0 - R_1 - R_2]$ linear code defined by the parity-check matrix H, then the combined message m can be viewed as a syndrome determining a coset of $\mathcal{C}$, and $\tilde{X}$ is selected uniformly at random among the elements of that coset.

Then, the transmitted word is computed as $X = V\tilde{X}$, where

$$V = \begin{bmatrix} I_{r_1-\tilde{\Delta}} & 0 & 0 & 0 \\ 0 & 0 & I_\alpha & 0 \\ 0 & I_{r_2-\tilde{\Delta}} & 0 & 0 \\ 0 & 0 & I_\alpha & 0 \\ 0 & 0 & 0 & I_\Delta \end{bmatrix}.$$

The transformation produced by V may be seen as a form of repetition coding and is therefore reversible. Writing

$$\tilde{X} = \begin{array}{c} r_1-\tilde{\Delta} \\ r_2-\tilde{\Delta} \\ \tilde{\Delta} \end{array} \begin{bmatrix} \tilde{X}_1 \\ \tilde{X}_2 \\ \tilde{X}_\Delta \end{bmatrix}$$

we have that $\begin{bmatrix} \tilde{X}_i \\ \tilde{X}_\Delta \end{bmatrix} = \begin{bmatrix} X_i \\ X_\Delta \end{bmatrix}, \quad i = 1, 2.$

As illustrated in Fig. 2, the transformation $X = V\tilde{X}$ is intended to increase the amount of common information transmitted, from Δ to $\tilde{\Delta}$ units. This is done by repeating the extra symbols (α units) into both X_1 and X_2. As a result, we can guarantee that $\tilde{\Delta} \geq \mu + R_0$ in all cases. Thus, we can use $\tilde{X}_\Delta$ to transport both the common message (R_0 units) and the randomness to confuse the wiretapper (μ units).

Now, let $H_i = \begin{bmatrix} H_{ii} & H_{i\Delta} \end{bmatrix}$, $i = 1, 2$. Since

$$\begin{bmatrix} m_1 \\ m_2 \\ m_0 \end{bmatrix} = \begin{bmatrix} H_{11} & 0 & H_{1\Delta} \\ 0 & H_{22} & H_{2\Delta} \\ 0 & 0 & H_{0\Delta} \end{bmatrix} \begin{bmatrix} \tilde{X}_1 \\ \tilde{X}_2 \\ \tilde{X}_\Delta \end{bmatrix} \tag{14}$$

it is clear that decoding can be performed by computing

$$\begin{bmatrix} \hat{m}_i \\ \hat{m}_0 \end{bmatrix} = H_i Y_i = \begin{bmatrix} H_{i1} & H_{i\Delta} \\ 0 & H_{0\Delta} \end{bmatrix} \begin{bmatrix} \tilde{X}_i \\ \tilde{X}_\Delta \end{bmatrix} = \begin{bmatrix} m_i \\ m_0 \end{bmatrix}.$$

Note that the probability of error is precisely zero.

B. *Secrecy Analysis*

We show with a suitable choice of H, the following condition is satisfied:

$$I(m; Z) = 0 \quad \text{for all } B \in \mathbb{F}_q^{\mu \times n}. \tag{15}$$

Note that $Z = BX = BV\tilde{X}$. As B runs through all matrices in $\mathbb{F}_q^{\mu \times n}$, also BV runs through all matrices in $\mathbb{F}_q^{\mu \times \tilde{n}}$. Thus, we need to guarantee that

$$I(m; \tilde{B}\tilde{X}) = 0 \quad \text{for all } \tilde{B} \in \mathbb{F}_q^{\mu \times \tilde{n}}. \tag{16}$$

It is shown in [9] that (16) is satisfied if

$$\operatorname{rank} \begin{bmatrix} H \\ \tilde{B} \end{bmatrix} = R_0 + R_1 + R_2 + \mu \quad \text{for all full-rank } \tilde{B}. \tag{17}$$

Our task is to construct H satisfying (13) and (17). For this purpose we rely on the properties of rank-metric codes, which are reviewed in Appendix A for the convenience of the reader.

Let $H_0 \in \mathbb{F}_{q^L}^{(\tilde{n}-\mu) \times \tilde{n}}$ be a parity-check matrix of an $[\tilde{n}, \mu]$ linear MRD code over $\mathbb{F}_{q^L}$. By converting H_0 to systematic form and permuting rows, we can obtain a matrix $H \in \mathbb{F}_{q^L}^{(\tilde{n}-\mu) \times \tilde{n}}$ of the form

$$H = \begin{array}{c} \\ r_1-\tilde{\Delta} \\ R_1-r_1+\tilde{\Delta} \\ r_2-\tilde{\Delta} \\ R_2-r_2+\tilde{\Delta} \\ R_0 \end{array} \begin{array}{c} \begin{array}{ccccc} r_1-\tilde{\Delta} & r_2-\tilde{\Delta} & R_1-r_1+\tilde{\Delta} & R_2-r_2+\tilde{\Delta} & \mu+R_0 \end{array} \\ \begin{bmatrix} I & 0 & 0 & 0 & P_1 \\ 0 & 0 & I & 0 & P_2 \\ 0 & I & 0 & 0 & P_3 \\ 0 & 0 & 0 & I & P_4 \\ 0 & 0 & 0 & 0 & P_5 \end{bmatrix} \end{array}$$

such that H_0 and H are parity-check matrices of the same code. It is easy to check that H is of the form (13). Moreover, by Theorem 3 in the appendix, we have that (17) is satisfied. Thus, the proof is complete.

V. Application to Network Coding

Consider a communication network represented by a directed multigraph with unit capacity edges. Each edge is assumed to be a noiseless channel. Suppose that the network contains one source node S and two destination nodes T_1 and T_2. The source node produces messages m_0, m_1 and m_2 such that T_i is interested in receiving (m_0, m_i), $i = 1, 2$. Additionally, suppose that there is an eavesdropper that can observe the transmissions on μ arbitrarily chosen links. We allow coding at all nodes in the network provided that causality is respected, i.e., the symbols transmitted by a node must be a function of the previously received symbols at the same node. We wish to characterize the capacity region for secret and reliable communication over the network (the precise definitions are similar to Section II-B).

For the achievability part, our approach will be to convert the network into the linear deterministic channel of section II-A by employing a suitable linear network code; then, Theorem 1 can be used. We start by reviewing a few definitions.

For any nodes A, B, let $\operatorname{mincut}(A, B)$ denote the minimum number of edges that must be removed in order to make B unreachable from A. Similarly, for a set of nodes $\mathcal{B}$, let $\operatorname{mincut}(A, \mathcal{B})$ denote the minimum number of edges that must be removed in order to make each $B \in \mathcal{B}$ unreachable from A. Let $C_i = \operatorname{mincut}(S, T_i)$, $i = 1, 2$, and $C_{12} = \operatorname{mincut}(S, \{T_1, T_2\})$.

Lemma 1: There exists a linear network code over a sufficiently large field such that $\operatorname{rank} A_i = C_i$, $i = 1, 2$, and $\operatorname{rank} \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} = C_{12}$, where A_1 and A_2 are the transfer matrices from S to T_1 and T_2, respectively.

Proof: Consider an extended network obtained by adding a new node T_3 and a number of edges from T_i to T_3 corresponding to the number of edges entering T_i, $i = 1, 2$. It is easy to see that $\operatorname{mincut}(S, T_3) = \operatorname{mincut}(S, \{T_1, T_2\})$. By applying the *generic* linear network code construction of [3] over a sufficiently large field, we can obtain a linear network code such that $\operatorname{rank} A_i = \operatorname{mincut}(S, T_i)$, where A_i is the transfer matrix seen by node T_i, $i = 1, 2, 3$. On the other hand, by construction, we have that

$$\mathsf{rank}\ A_3 \leq \mathsf{rank} \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \leq \mathrm{mincut}(S, \{T_1, T_2\}).$$

It follows that $\mathsf{rank} \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} = \mathrm{mincut}(S, \{T_1, T_2\})$, completing the proof. ∎

Note that, when a linear network code is used, the eavesdropper's observation can be characterized by a transfer matrix B with μ rows. Thus, the overall wiretap channel produced by Lemma 1 falls exactly into the linear-deterministic channel of section II-A. We can thus obtain the following result.

Theorem 2: For a network with one source and two destinations, the capacity region for communicating messages m_0, m_1, m_2 at rates R_0, R_1, R_2, respectively, while guaranteeing secrecy from an eavesdropper that observes any subset of μ links, is the union of all non-negative rate tuples (R_0, R_1, R_2) that satisfy

$$R_0 + R_1 \leq C_1 - \mu, \quad R_0 + R_2 \leq C_2 - \mu$$
$$R_0 + R_1 + R_2 \leq C_{12} - \mu, \quad R_0 \leq \min(C_1, C_2) - \mu.$$

Proof: Achievability follows from Lemma 1 together with Theorem 1. The converse follows by applying the single user secure multicast coding [1] to each individual receiver and to the two cooperating receivers. ∎

Remark 2: When $\mu = 0$ i.e., in absence of a secrecy constraint, the result in Theorem 2 shows that the cut-set bound is tight for the case of broadcasting independent and common messages from one sender to two sinks over a network. This recovers an earlier result (see e.g., [5] and references therein).

VI. Conclusion

This paper characterizes the secrecy-capacity region of transmitting independent and common messages to two legitimate receivers in the presence of a collection of eavesdroppers. All channels are linear and deterministic and the channel transfer matrices of the eavesdroppers have a bounded rank. The coding scheme combines syndrome coding based on the parity check of a rank metric code with a suitable repetition code. Using this coding scheme and a generic network code we also characterize the secrecy-capacity region for the one sender two sink secure network coding problem.

As it is already known that linear network coding is insufficient for the general multiuser case (without the secrecy constraint), we expect the a complete multiuser generalization of our results to be difficult. Nevertheless our results on the two receiver channel shed some interesting insights arising due to the secrecy constraints. Note that the capacity region behaves differently depending on the rank of the eavesdropper's channel. Hence a fruitful direction could be to pursue the extension to more than two receivers when the rank of the eavesdropper's channel is either above or below certain thresholds.

Appendix A
Review of Rank-Metric Codes

A *rank-metric code* is a block code over an extension field (or, alternatively, a matrix code) that uses the *rank distance* as a metric. The rank distance between matrices $X, Y \in \mathbb{F}_q^{n\times L}$ is defined as $d_{\mathrm{R}}(X, Y) \triangleq \mathsf{rank}\,(Y - X)$. Similarly, using the isomorphism $\phi_n : \mathbb{F}_q^{n\times L} \leftrightarrow \mathbb{F}_{q^L}^n$, the rank distance between vectors $X, Y \in \mathbb{F}_{q^L}^n$ is defined as

$$d_{\mathrm{R}}(X, Y) \triangleq \mathsf{rank}\ \phi_n^{-1}(Y - X).$$

The *minimum rank distance* of a code $\mathcal{C} \subseteq \mathbb{F}_{q^L}^n$, denoted $d_{\mathrm{R}}(\mathcal{C})$, is the minimum rank distance among all pairs of distinct codewords of $\mathcal{C}$. The size of a code $\mathcal{C} \subseteq \mathbb{F}_{q^L}^n$ with $d_{\mathrm{R}}(\mathcal{C}) = d$ is bounded by the Singleton bound for the rank metric, which is given by

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

Codes that achieve this bound are called *maximum-rank-distance* (MRD) codes.

It is useful to consider MRD codes that are *linear* $[n, k]$ codes over $\mathbb{F}_{q^L}$. In the case that $L \geq n$, the minimum rank distance of the code is given by $d = n - k + 1$. Such codes have a very useful property, which is given in the following theorem.

Theorem 3 ([8], [9]): Let $H \in \mathbb{F}_{q^L}^{(n-\mu)\times n}$ be a parity-check matrix of an $[n, \mu]$ linear MRD code over $\mathbb{F}_{q^L}$, where $L \geq n$. Then, for every full-rank matrix $B \in \mathbb{F}_q^{\mu\times n}$, we have $\mathsf{rank} \begin{bmatrix} H \\ B \end{bmatrix} = n$.

Note that linear MRD codes with $L \geq n$ can be constructed very easily using a construction by Gabidulin [2].

Acknowledgement

Aditya Ramamoorthy pointed the authors to reference [5].

References

[1] N. Cai and R. Yeung. Secure network coding. In *Proc. IEEE Int. Symp. Information Theory*, page 323, Lausanne, Switzerland, July 2002.

[2] E. M. Gabidulin. Theory of codes with maximum rank distance. *Probl. Inform. Transm.*, 21(1):1–12, 1985.

[3] S.-Y. R. Li, R. W. Yeung, and Ning Cai. Linear network coding. *IEEE Trans. Inf. Theory*, 49(2):371–381, February 2003.

[4] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. *EUROCRYPT*, pages 33—50, 1984.

[5] A. Ramamoorthy and R. D. Wesel. The single source two terminal network with network coding. In *Canadian Workshop on Information Theory*, 2005.

[6] S. Y. E. Rouayheb and E. Soljanin. On wiretap networks II. In *Proc. IEEE Int. Symp. Information Theory*, pages 551—555, Nice, France, June 2007.

[7] S. Saeedi, S. N. Diggavi, C. Fragouli, and V. Prabhakaran. On degraded two message set broadcasting. In *IEEE Information Theory Workshop (ITW)*, Taormina, Italy, October 2009.

[8] D. Silva and F. R. Kschischang. Security for wiretap networks via rank-metric codes. In *Proc. IEEE Int. Symp. Information Theory*, pages 176–180, Toronto, Canada, July 6–11, 2008.

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

[10] A. D. Wyner. The wiretap channel. *Bell Syst. Tech. J.*, 54:1355–87, 1975.