A Security Condition for Multi-Source Linear Network Coding

Ning Cai
State Key Lab. of ISN
Xidian University
Xi'an, Shaanxi, China
Email: caining@mail.xidian.edu.cn

Raymond W. Yeung
Department of Information Engineering
The Chinese University of Hong Kong
Hong Kong, China
Email:whyeung@ie.cuhk.edu.hk

***Abstract*— We obtain a necessary and sufficient condition for the security of multi-source linear network codes by studying the algebraic structure of such codes. This condition is useful for analyzing the security of such linear network codes, and it applies in cases when the random keys do not necessarily have uniform distributions. This condition also shows that the security of a linear network code does not depend on the source distribution.**

I. Introduction

A network is specified by a directed graph $G = (V, E)$ whose nodes stand for communication units and whose edges stand for channels in a point-to-point communication network. In this paper, we assume that all the channels in the network are noiseless and have unit capacity. Messages are generated at nodes referred to as the source nodes, while subsets of these messages are decoded perfectly at nodes referred to as the sink nodes. Linear network coding introduced by Li *et al* [1] are provably optimal for single-source networks in the sense of achieving the maximum flow upper bound. Owing to their simple structures and other desirable properties, linear network codes have been widely studied and are regarded as the most important class of network codes. In this paper, we confine our discussion to linear network codes.

Motivated by security considerations in network communications, we introduced the communication system on a wiretap network (CSWN) in [2]. A CSWN consists of a network and a collection $\mathcal{W}$ of subsets of channels, whose members are called wiretap subsets of channels. A wiretapper can arbitrarily choose one but only one wiretap subset $W \in \mathcal{W}$ and fully access (the output of) all the channels in the wiretap subset W. The communicators over a CSWN know the collection $\mathcal{W}$ of wiretap subsets but do not know which subset W is chosen by the wiretapper. The goal of the communicators is that the wiretapper can obtain absolutely no information about the messages transmitted through the network. Obviously, the transmission in the network has to be randomized because otherwise the output of a channel would be either a function depending on the messages or simply a constant. In the former case the wiretapper would be able to obtain useful information about the messages by accessing the channel, and in the latter case the channel would be completely useless and can be deleted. We assume that the wiretapper knows the coding scheme and may choose a wiretap subset according to his/her knowledge. A code for CSWN is said to be secure if the wiretapper can obtain no information about the transmitted messages no matter how the wiretap subset is chosen. To randomize the transmission, randomness (also referred to as *random key(s)*) has to be generated at some node(s) within the network. We studied in [2] the model in which the randomness is generated at the unique source node. This model contains Shannon's cipher system [3] and the secrete sharing schemes introduced independently by Blakley [4] and Shamir [5] as special cases.

For this model, we proposed in [2] a secure network coding scheme based on a given decodable linear network code over a sufficiently large field. Specifically, we first construct a matrix with certain properties according to a given linear network code and the collection of wiretap subsets. Then we treat the random key as "part of the message" and pre-encode the whole message by the above matrix at the source node. This is equivalent to linearly transforming the given linear network code to a new linear network code. It was proved that under suitable condition, one can find a matrix such that the new code is secure. This coding scheme works when both the message and the randomness are generated at source node. Such secure network codes have been further studied in [6].

In this paper, we consider the more general model in which randomness can be generated at an arbitrarily given subset of nodes, and there can be more than one source nodes in the network. In the next section, we present necessary definitions and notation. In Section III, we formulate the problem and obtain a necessary and sufficient condition for the security of a linear network code. This condition shows that the security of a network code does not depend on the source distributions. To illustrate the applications of the condition, we present an example in Section IV. The paper is concluded in Section V.

II. Definitions and Notation

In this paper we follow the notation and terminology in [7]. A communication network, or in short a network, consists of the following components:

(a) a finite directed graph $G = (V, E)$ with multiple edges, whose vertices $v \in V$ are called nodes and whose edges $e = (u, v) \in E$ are called channels, where we assume that

each channel transmits one unit of information per unit time noiselessly;
(b) a subset $S := \{s_1, s_2, \ldots, s_{|S|}\}$ of nodes, whose members are called source nodes at each of which a message is generated independently and uniformly over a given finite alphabet;
(c) a subset $\mathcal{T}$ of nodes whose members are called sinks, each of which has to recover the messages generated by a given subset of sources.

A communication system on a wiretap network (CSWN) consists of a communication network specified by the components (a)-(c) together with

(d) a collection $\mathcal{W}$ of subsets of channels, whose members are called wiretap subsets (of channels), each of which may be fully accessed by a wiretapper but no wiretapper may access more than one wiretap subset.

As we pointed out in the previous section, in order to protect the messages from the wiretapper, randomness has to be generated somewhere in the network. Let $U := \{u_1, u_2, \ldots, u_{|U|}\} \subset V$ be a subset of nodes such that at most r_i units of randomness can be generated at node u_i per unit time independent of the source messages.

For simplicity, we assume the network is acyclic or there exits a well-defined encoding order for the channels. A code is decodable if it is uniquely decodable at all the sinks. For a given network code, let $\mathbf{Z}$ be the messages generated by the information sources and $Y(e)$ be the symbol transmitted on a channel e. Thus for all $e \in E$, $Y(e)$ is a function of $\mathbf{Z}$ and the randomness. Denote by $\mathbf{Y}(A) = \{Y(e) : e \in A\}$ for $A \subset E$. Then a code is secure if and only if for all wiretap subsets $W \in \mathcal{W}$

$$H(Z|\mathbf{Y}(W)) = H(Z). \tag{1}$$

A network code is linear if the symbols transmitted in the network are linear in the source messages and the randomness. The secure condition (1) implies that the wiretapper knows the topological structure of the network and the coding scheme so that he/she may choose the wiretap subset he/she wants. Throughout this paper, we separate the issue of security from the issue of decodability of a linear network code. This way, we can treat $u_i \in U$ as a source node and the randomness generated there as a message. Then we can define the global and local encoding kernels of a linear network code over a ground field as in [7].

III. A Necessary and Sufficient Condition for Security

Let the unit of information be a symbol in a given finite field F. Consider a CSWN in which the message generated at source node s_j consists of m_j units, and $n_i \le r_i$ units of randomness are generated at node $u_i \in U$. We will study the condition for a linear code to satisfy (1). Denote the messages generated by source node s_j by an m_j-dimensional row vector $\mathbf{z}_j$ over F and the outcome of the randomness generated at node $u_i \in U$ by an n_i-dimensional row vector $\mathbf{k}_i$ over the same field. Write $\mathbf{z} := (\mathbf{z}_1, \mathbf{z_2}, \ldots, \mathbf{z}_{|S|})$, $\mathbf{k} := (\mathbf{k}_1, \mathbf{k}_2, \ldots, \mathbf{k}_{|U|})$, $\mathbf{x} := (\mathbf{z}, \mathbf{k})$, $m := m_1 + m_2 + \ldots + m_{|S|}$, $n := n_1 + n_2 + \ldots + n_{|U|}$, and $\omega := m + n$. To simplify our discussion, throughout the paper we assume that all the sources messages (randomness) $\mathbf{z}$ ($\mathbf{k}$) have positive probability. Therefore, all $\mathbf{x}$ have positive probability. The output of channel $e \in E$ is a linear function of $\mathbf{x}$ if the code is linear. Thus for a linear network code, we may define its local encoding kernels $k_{d,e}, d, e \in E$, where $d \in In(v)$ and $e \in Out(v)$ for some $v \in V$, and global encoding kernels $\mathbf{f}_e, e \in E$ (where $\mathbf{f}_e$ is an ω-dimensional column vector for all channels $e \in E$) as in [7] such that channel e outputs $\mathbf{x}\mathbf{f}_e$ if $\mathbf{z}$ and $\mathbf{k}$ are the message and randomness generated, respectively. For a subset $A \subset E$ of channels, denote by $F(A)$ the matrix whose columns are the global encoding kernels of channels $e \in A$ (according to an arbitrary but fixed indexing). Let m-dimensional random row vector $\mathbf{Z}$ be the random messages, n-dimensional random row vector $\mathbf{K}$ be the randomness, and $\mathbf{X} := (\mathbf{Z}, \mathbf{K})$. Then the random output accessed by a wiretapper from a wiretap subset $W \in \mathcal{W}$ of channels is $\mathbf{Y}(W) := \mathbf{X}F(W)$. Thus by (1) a linear network code is secure if and only if $\mathbf{Y}(W)$ is statistically independent of $\mathbf{Z}$ for all $W \in \mathcal{W}$.

It was proved in [2] that when $S = U = \{s\}$ i.e., the CSWN has a single source node where all the randomness is generated, a linear network code can be linearly transformed into a linear secure network code by a properly chosen full rank matrix, and the matrix can always be found under suitable conditions. The secure network code, namely the image of the linear transformation, has the following property: If $\{\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_w\}$ is a maximal subset of linearly independent vectors in $\{\mathbf{f}_d : d \in W\}$, where $\mathbf{f}_e$ is the global encoding kernel of channel e in the image code, W is a wiretap subset of channels in $\mathcal{W}$, and ϵ_j is the ω-dimensional column vector whose jth component is 1 and all other components are 0, then

$$\epsilon_1, \epsilon_2, \ldots, \epsilon_m, \mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_w, \text{ are linearly independent.} \tag{2}$$

It can readily be seen by invoking Theorem 7.3 in [7] that (2) is the necessary and sufficient condition for the network code to be secure when both the source messages and the randomness have uniform distributions. By the assumption in (2), $rank(F(W)) = w$. Let $F^*(W)$ be the submatrix of matrix $F(W)$ consisting of the maximal linearly independent set $\{\mathbf{f}_j, j = 1, 2, \ldots w\}$ in (2). Then condition (2) is equivalent to that $G := (\epsilon_1, \epsilon_2, \ldots, \epsilon_m, F^*(W))$ has rank $m + w$. Write

$$G = \begin{pmatrix} I & F_1^*(W) \\ 0 & F_2^*(W) \end{pmatrix},$$

where $F_1^*(W)$ and $F_2^*(W)$ are submatrices of $F^*(W)$ consisting of its first m rows and last n rows, respectively, and I is the $m \times m$ identity matrix. By multiplying suitable values to the first m columns of G and adding them to the last n columns, we can obtain

$$G' = \begin{pmatrix} I & 0 \\ 0 & F_2^*(W) \end{pmatrix}$$

with the same rank as G. Thus we have

$$rank(F_2^*(W)) = w = rank(F^*(W)) = rank(F(W)).$$

Let $F_1(W)$ and $F_2(W)$ be the submatrices of $F(W)$ consisting of its first m rows and last n rows, respectively. Following the above discussion, the next lemma gives a necessary and sufficient condition for the security of a linear network code. Note that this condition does not depend on the assumption that the sources messages have uniform distribution.

Lemma 3.1: (*Security Lemma*) Suppose $\mathbf{X} := (\mathbf{Z}, \mathbf{K})$ is the input to the CSWN so that channel $e \in E$ outputs $\mathbf{xf}_e$.
i) The wiretapper can obtain no information about $\mathbf{z}$ from the outputs of W if $rank(F_2(W)) = rank(F(W))$ and $\mathbf{K}$ has uniform distribution on the n-dimensional row space.
ii) The wiretapper can obtain information about $\mathbf{z}$ from the outputs of W if $rank(F_2(W)) < rank(F(W))$.

Proof: Let $\mathbf{Y} := \mathbf{X}F(W)$, $\mathbf{Y}_1 := \mathbf{Z}F_1(W)$, and $\mathbf{Y}_2 := \mathbf{K}F_2(W)$. Then

$$\mathbf{Y} = \mathbf{Y}_1 + \mathbf{Y}_2. \tag{3}$$

Let T, T_1 and T_2 be the linear transformations sending an ω-dimensional row vector $\mathbf{x}$ to $\mathbf{x}F(W)$, sending an m-dimensional row vector $\mathbf{z}$ to $\mathbf{z}F_1(W)$, and sending an-n dimensional row vector $\mathbf{k}$ to $\mathbf{k}F_2(W)$, and denote their image spaces by L, L_1, and L_2, respectively. Obviously, $L_1 \subset L$ and $L_2 \subset L$. We now prove i) and ii).
i) Suppose $rank(F_2(W)) = rank(F(W)) := r$ and $\mathbf{K}$ has uniform distribution. Then $L_2 = L$ and the common image space $L_2 = L$ of T_2 and T has dimension r. Therefore, for all $\mathbf{y}_2 \in L$, $Pr(\mathbf{Y}_2 = \mathbf{y}_2) = q^{-n+(n-r)} = q^{-r}$, where $q := |F|$ is the order of the ground field, because T_2 sends exactly q^{n-r} n-dimensional column vectors to each vector in the r-dimensional linear subspace L. Moreover, for all $\mathbf{y}_1 \in L_1$ and $\mathbf{y} \in L$, $\mathbf{y} - \mathbf{y}_1 \in L$ because $L_1 \subset L$. Thus by (3), for all $\mathbf{y}_1$ with $Pr(\mathbf{Y}_1 = \mathbf{y}_1) \neq 0$, we have

$$\begin{aligned} Pr(\mathbf{Y} = \mathbf{y}|\mathbf{Y}_1 = \mathbf{y}_1) &= Pr(\mathbf{Y}_2 = \mathbf{y} - \mathbf{y}_1|\mathbf{Y}_1 = \mathbf{y}_1) \\ &= Pr(\mathbf{Y}_2 = \mathbf{y} - \mathbf{y}_1) \\ &= q^{-r} \end{aligned}$$

for all $\mathbf{y} \in L$, where the second equality above holds because $\mathbf{Y}_1$ and $\mathbf{Y}_2$ are respectively functions of $\mathbf{Z}$ and $\mathbf{K}$, which are independent of each other. This shows that $\mathbf{Y}$ and $\mathbf{Y}_1$ are independent. Finally, by observing that $\mathbf{Z} \to \mathbf{Y}_1 \to \mathbf{Y}$ forms a Markov chain, we see that $\mathbf{Z}$ and $\mathbf{Y}$ are independent, proving part i).
ii) Suppose $rank(F_2(W)) < rank(F(W))$. Then there exists a $\mathbf{y} \in L \setminus L_2$. By our assumption that all $\mathbf{z}$ and $\mathbf{k}$ have positive probabilities, we have $Pr(\mathbf{Z} = \mathbf{0}) \neq 0$ and $Pr(\mathbf{Y} = \mathbf{y}) \neq 0$, whereas $Pr(\mathbf{Y} = \mathbf{y}|\mathbf{Z} = \mathbf{0}) = Pr(\mathbf{Y}_2 = \mathbf{y}) = 0$. Thus $Pr(\mathbf{Y} = \mathbf{y}|\mathbf{Z} = \mathbf{0}) \neq Pr(\mathbf{Y} = \mathbf{y})$. Consequently, $\mathbf{Z}$ and $\mathbf{Y}$ are dependent, proving part ii).

Corollary 3.2: Suppose $\mathbf{K}$ has uniform distribution. Then the following are equivalent necessary and sufficient conditions for the wiretapper not being able to obtain any information about $\mathbf{z}$ from the outputs of W:
i) the condition in (2) is satisfied;
ii) $rank(F_2(W)) = rank(F(W))$.

Proof: By Lemma 3.1, ii) implies that the wiretapper can obtain no information about $\mathbf{z}$ from the outputs of W for any source distributions, in particular for the uniform source distributions. The latter is equivalent to i) from the discussion following (2). Therefore, the wiretapper not being able to obtain any information about $\mathbf{z}$ from the outputs of W implies i). Finally, the condition in (2) holds if and only if $rank(F_2^*(W)) = rank(F(W))$. Since

$$rank(F_2^*(W)) \leq rank(F_2(W)) \leq rank(F(W)),$$

this implies $rank(F_2(W)) = rank(F(W))$. Thus i) implies ii), completing the proof.

Next we seek a necessary and sufficient condition for the general case where $\mathbf{K}$ may not have uniform distribution. It is sufficient for us to study the condition for an arbitrarily chosen wiretap subset W of channels. To this end, let us consider the subspaces L and L_1 in the proof of Lemma 3.1 for a fixed wiretap subset W of channels, i.e., $L := \{\mathbf{x}F(W) : \mathbf{x} \in F^\omega\}$ and $L_1 := \{\mathbf{z}F_1(W) : \mathbf{z} \in F^m\}$. As we have seen in the proof of Lemma 3.1, L_1 is a linear subspace of L. Let $dim(L) = r$ and $dim(L_1) = r_1$. Then $r_1 \leq r$, and L is partitioned into q^{r-r_1} cosets of L_1 say, $J_0, J_1, J_2, \ldots, J_{q^{r-r_1}-1}$ with $|J_i| = q^{r_1}, i = 0, 1, 2, \ldots, q^{r-r_1} - 1$, where $J_0 = L_1$.

Theorem 3.3: For $W \in \mathcal{W}$, let $\mathbf{Y}_2 := \mathbf{K}F_2(W)$. Then the wiretapper can obtain no information about $\mathbf{z}$ from the outputs of W if and only if for $i = 0, 1, 2, \ldots, q^{r-r_1} - 1$ and all $\mathbf{y_2} \in J_i$,

$$Pr(\mathbf{Y}_2 = \mathbf{y}_2) = q^{-r_1} Pr(\mathbf{Y}_2 \in J_i), \tag{4}$$

or equivalently

$$Pr(\mathbf{Y}_2 = y_2|\mathbf{Y_2} \in J_i) = q^{-r_1} \tag{5}$$

provided that $\mathbf{K}$ has a strictly positive distribution.

Proof: The wiretapper can obtain no information about $\mathbf{z}$ from the outputs of W if and only if

$$Pr(\mathbf{Y} = \mathbf{y}|\mathbf{Z} = \mathbf{z}) = Pr(\mathbf{Y} = \mathbf{y}),$$

for all $\mathbf{y} \in L$ and all m-dimensional row vectors $\mathbf{z}$. On the other hand, it follows from (3) and the independence of $\mathbf{Z}$ and $\mathbf{K}$ that

$$Pr(\mathbf{Y} = \mathbf{y}|\mathbf{Z} = \mathbf{z}) = Pr(\mathbf{Y}_2 = \mathbf{y} - \mathbf{z}F_1(W)).$$

Therefore, the wiretapper can obtain no information about $\mathbf{z}$ from the outputs of W if and only if

$$Pr(\mathbf{Y}_2 = \mathbf{y} - \mathbf{z}F_1(W)) = Pr(\mathbf{Y} = \mathbf{y}). \tag{6}$$

Let $\mathbf{y}$ be fixed. Then $Pr(\mathbf{Y} = \mathbf{y})$ is a constant that does not depend on $\mathbf{z}$. Now observe that $\{\mathbf{y} - \mathbf{z}'F_1(W) : \mathbf{z}' \in F^m\}$ is precisely the coset of L_1 in L, say J_i, that contains $\mathbf{y}$. So we see from (6) that for all $\mathbf{y}_2 \in J_i$, $Pr(\mathbf{Y}_2 = \mathbf{y}_2)$ does not depend on $\mathbf{y}_2$. Then (4) follows because $|J_i| = q^{r_1}$.

Conversely, if (4) holds, then for all $\mathbf{y} \in L$ and all m-dimensional row vectors $\mathbf{z}$, we have

$$\begin{aligned} Pr(\mathbf{Y} = \mathbf{y}|\mathbf{Z} = \mathbf{z}) &= Pr(\mathbf{Y}_2 = \mathbf{y} - \mathbf{z}F_1(W)) \\ &= q^{-r_1} Pr(\mathbf{Y}_2 \in J_i) \end{aligned}$$

which does not depend on $\mathbf{z}$, showing that $\mathbf{Y}$ and $\mathbf{Z}$ are independent, or the wiretapper can obtain no information about $\mathbf{z}$ from the outputs of W.

We now prove that if $\mathbf{K}$ has a strictly positive distribution, then $Pr(\mathbf{Y}_2 \in J_i) > 0$, so that $Pr(\mathbf{Y}_2 = y_2|\mathbf{Y_2} \in J_i)$ in (5) is properly defined. Toward this end, consider any $\mathbf{y} \in J_i$. Since $\mathbf{y} \in L$, $\mathbf{y} = \mathbf{z}F_1(W) + \mathbf{k}F_2(W)$ for some $\mathbf{z} \in F^m$ and $\mathbf{k} \in F^n$. Then $\mathbf{k}F_2(W) = \mathbf{y} - \mathbf{z}F_1(W) \in \{\mathbf{y} - \mathbf{z}'F_1(W) : \mathbf{z}' \in F^m\} = J_i$. Since we assume that each $\mathbf{k}$ has positive probability, it follows that

$$Pr(\mathbf{Y}_2 \in J_i) \geq Pr(\mathbf{K} = \mathbf{k}) > 0. \tag{7}$$

Then (5) are (4) equivalent, completing the proof.

Remark: It is easy to see the condition in (5) yields $rank(F_2(W)) = rank(F(W))$. Since $Pr(\mathbf{Y}_2 \in J_i) > 0$ for all i from (7), we see from (4) that $Pr(\mathbf{Y}_2 = \mathbf{y}) > 0$ for all $\mathbf{y} \in L$. It then follows immediately that $L_2 = L$ (because $L_2 \subset L$), or $rank(F_2(W)) = rank(F(W))$.

An immediately consequence of Theorem 3.3 is that the security of a linear network code is independent of the source distributions provided they are strictly positive.

Corollary 3.4: Let $\mathbf{Z}$ and $\mathbf{Z}'$ be two arbitrary random sources for the same CSWN with strictly positive probability distributions over the m-dimensional space F^m. Then a linear network code with randomness $\mathbf{K}$ for the CSWN is secure for source $\mathbf{Z}$ if and only if it is secure for source $\mathbf{Z}'$.

Proof: This corollary follows immediately because the security condition for a linear network code in Theorem 3.3 does not dependent the source distributions.

With Corollary 3.4, in studying the security of a linear network code, we may always assume without loss of generality that the sources have uniform distributions.

IV. An Example

In this section, we present an example to illustrate the applications of Corollary 3.2. Consider the CSWN shown in Figure 1. There are two source nodes s_1 and s_2, and random messages Z_1 and Z_2 are generated uniformly and independently at unit rate at s_1 and s_2, respectively. We want to send the messages Z_1 and Z_2 to the sinks t_1 and t_2, respectively. Assume that all channels have unit capacity, and let $GF(5)$ be the ground field. Then Z_1 and Z_2 are uniformly distributed over $GF(5)$ and each channel can carry a symbol in $GF(5)$. Let $E_0 = \{(u_1, t_2), (w_1, v_1), (u_2, v_0), (w_2, v_2), (w_3, t_1)\}$ and $\mathcal{W} = \binom{E_0}{2}$, the collection of all 2-subsets of E_0. That is, a wiretapper can arbitrarily choose two channels in E_0 to access. From Figure 1, we see that both source nodes have out-degree one. Thus we may not send any randomness from the source nodes even in the case that they are qualified to generate randomness. In the other words, the randomness has to be generated somewhere else in the network. Let $\mathcal{U} = \{u_1, u_2\}$, and let a unit of uniform randomness K_i be generated at node u_i for $i = 1, 2$.

Denote the output of channel e by $y(e)$ and the realizations of random variables Z_i and K_j by z_i and k_j, respectively for $i, j = 1, 2$. The encoding functions are defined as follows.

$$\begin{aligned} y((s_1, u_1)) &= z_1 \\ y((s_2, w_3)) &= z_2 \\ y((u_1, t_2)) &= y((s_1, u_1)) + k_1 \\ y((u_1, u_2)) &= y((s_1, u_1)) + k_1 \\ y((u_2, w_3)) &= k_2 \\ y((u_2, v_0)) &= y((u_1, u_2)) + 2k_2 \\ y((u_1, w_1)) &= 2y((s_1, u_1)) + k_1 \\ y((w_3, w_1)) &= y((u_2, w_3)) \\ y((w_1, v_1)) &= y((u_1, w_1)) + y((w_3, w_1)) \\ y((u_1, w_2)) &= y((s_1, u_1)) + 2k_1 \\ y((w_3, w_2)) &= y((s_2, w_3)) + y((u_2, w_3)) \\ y((w_2, v_2)) &= y((u_1, w_2)) + y((w_3, w_2)) \\ y((w_3, t_1)) &= 2y((s_2, w_3)) + y((u_2, w_3)) \\ y((v_1, t_2)) &= y((w_1, v_1)) \\ y((v_1, t_1)) &= y((w_1, v_1)) \\ y((v_2, t_2)) &= y((w_2, v_2)) \\ y((v_2, t_1)) &= y((w_2, v_2)) \\ y((v_0, t_2)) &= y((u_2, v_0)) \\ y((v_0, t_1)) &= y((u_2, v_0)). \end{aligned}$$

These encoding functions yield

$$\begin{gathered} y((u_1, t_2)) = z_1 + k_1 \\ y((v_1, t_2)) = y((v_1, t_1)) = y((w_1, v_1)) = 2z_1 + k_1 + k_2 \\ y((v_0, t_2)) = y((v_0, t_1)) = y((u_2, v_0)) = z_1 + k_1 + 2k_2 \\ y((v_2, t_2)) = y((v_2, t_1)) = y((w_2, v_2)) = z_1 + z_2 + 2k_1 + k_2 \\ y((w_3, t_1)) = 2z_2 + k_2. \end{gathered}$$

In other words, the global encoding kernels of the channels in set E_0 are

$$\mathbf{f}_{(u_1,t_2)} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ \mathbf{f}_{(w_1,v_1)} = \begin{pmatrix} 2 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \ \mathbf{f}_{(u_2,v_0)} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}$$

$$\mathbf{f}_{(w_2,v_2)} = \begin{pmatrix} 1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \ \mathbf{f}_{(w_3,t_1)} = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix},$$

and the matrices formed by the global encoding kernels of

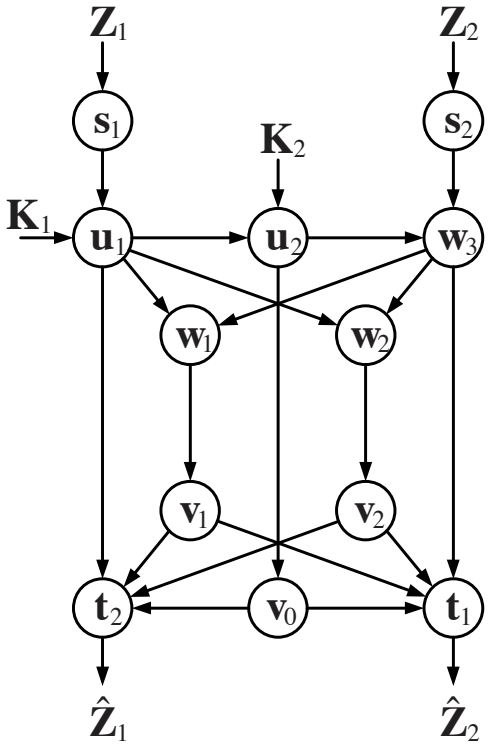

Fig. 1. An example of a secure code for a CSWN.

channels in $In(t_1)$ and $In(t_2)$ are

$$M_1 = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 1 & 1 \end{pmatrix}$$

and

$$M_2 = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

Since any pair of vectors taken from

$$\left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

are linearly independent, for all $W \in \mathcal{W}$, we have $rank(F_2(W)) = 2$. Thus the security of the network code follows from Corollary 3.2. Finally, we can easily verify that M_1 and M_2 are full rank, and therefore the network code is decodable.

V. Conclusion

In this paper, we obtain a necessary and sufficient condition for a linear network code to be secure. Our results apply to networks in which there can be more than one source nodes, and randomness can be generated at more than one node in the network. Shannon's cipher system and secret-sharing schemes are special cases of such networks. We also show that the security of a linear network code does not depend on the source distributions. This finding greatly simply the design of secure linear network codes.

Acknowledgment

The work of Ning Cai was partially supported by a grant from the National Natural Science Foundation of China (Ref. No. 60672119). The work of Raymond W. Yeung was partially supported by a grant from the Research Grant Council of the Hong Kong Special Administrative Region, China (RGC Ref. No. 418006).

References

[1] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. on Information Theory*, vol. IT-49, pp. 371-381, 2003.

[2] N. Cai and R. W. Yeung, "Secure network coding," 2002 IEEE International Symposium on Information Theory, Lausanne, Switzerland, Jun 30-Jul 5, 2002.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. Journal*, 28, pp. 656-715, 1949.

[4] G. R. Blakley, "Safeguarding cryptographic keys," AFIPS Conference Proceeding 48, pp. 313-317, 1979.

[5] A. Shamir, "How to share a secret," *Commun. of the ACM*, 22, pp. 612-613, 1979.

[6] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the Capacity of Secure Network Coding," Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing, September 2004.

[7] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Network Coding Theory*, now Publishers, 2005.