A General Security Condition for Multi-Source Linear Network Coding

Zhixue Zhang*
School of Information and Communication Engineering
Beijing University of Posts and Telcommunications
Beijing, China
Email: zxzhang@ie.cuhk.edu.hk

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

***Abstract*—In this paper, we study the linear multi-source network coding security problem in [4], without the assumption that all source messages have positive distributions. We obtain a necessary and sufficient security condition, which can be regarded as a generalization of the one in [4].**

I. Introduction

The problem of secure network coding was first studied by Cai and Yeung in [1]. They introduced a communication system on a wiretap network (CSWN) and proposed a secure network coding scheme. A CSWN consists of a single-source network and a collection $\mathcal{W}$ of subsets of channels, whose members are called wiretap subsets of channels. An eavesdropper can arbitrarily choose one but only one wiretap subset $W \in \mathcal{W}$ and fully access all the channels in the wiretap subset W. The sender over a CSWN knows the collection $\mathcal{W}$ of wiretap subsets but does not know which subset W is chosen by the eavesdropper. Cai and Yeung proposed in [1] a secure network coding scheme based on a given decodable linear network code over a sufficiently large field. Recently, they proved in [2], [3] that the coding scheme can achieve the required security while multicasting the maximum possible amount of information and using the minimum amount of randomness.

In [4], Cai and Yeung continued their original work with a more general model in which there can be more than one source node and randomness can be generated at an arbitrarily given subset of nodes, and they obtained a necessary and sufficient condition for the security of a linear network code. Their condition is based on the assumption that all the source messages and randomness have positive probability. In this work, we obtain a generalization of their condition with this assumption removed.

The rest of the paper is organized as follows. Section II gives the problem formulation. In Section III, we present and prove the general security condition. In Section IV, we reduce our general condition to the condition in [4] by making the assumption that all the source messages have positive probability. The paper is concluded in Section V.

II. Problem Formulation

Consider network transmission in a directed multi-source acyclic communication network denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of edges in the network. Let $\mathcal{S} = \{s_1, s_2, \cdots, s_{|\mathcal{S}|}\}$ be a subset of nodes, whose members are called source nodes at each of which a message is generated independently over $\mathbb{F}_q$, where q is a power of prime number p. Denote the messages generated by the source node s_i by a λ_i-dimensional row vector m_i over $\mathbb{F}_q$. Let $\mathcal{T}$ be a set of sink nodes, each of which has to recover the messages generated by a given subset of sources. An edge from node a to b, denoted by (a, b), represents a communication channel from node a to node b. Each edge can transmit one symbol in a finite field $\mathbb{F}_q$. Let $\mathcal{W}$ be a collection of subsets of edges, whose members are called wiretap subsets. In the network, there is a wiretapper who can fully access one and only one wiretap subset to his knowledge.

In order to protect the messages from the wiretapper, randomness has to be generated somewhere in the network. Let $\mathcal{U} = \{u_1, u_2, \cdots, u_{|\mathcal{U}|}\} \subset \mathcal{V}$ be a subset of nodes such that at most r_i symbols of randomness can be generated at node u_i per unit time independent of the source messages. Denote the outcome of randomness generated at the source node u_i by a k_i-dimensional row vector k_i over $\mathbb{F}_q$. Let $m = (m_1, m_2, \cdots, m_{|\mathcal{S}|})$, $k = (k_1, k_2, \cdots, k_{|\mathcal{U}|})$, $x = (m, k)$, $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_{|\mathcal{S}|}$, $\gamma = \gamma_1 + \gamma_2 + \cdots + \gamma_{|\mathcal{U}|}$ and $n = \lambda + \gamma$.

Like [4], we also separate the issue of security from the issue of decodablility of a linear network code. Thus $u_i \in \mathcal{U}$ can be treated as source node. Then a linear network code for a network $\mathcal{G}$ can be specified by either a set of local encoding kernels $\{k_{e'e} : e', e \in \mathcal{E}\}$ or set of global encoding kernels $\{f_e : e \in \mathcal{E}\}$ [5], where f_e is an n-dimensional column vector over $\mathbb{F}_q$.

Let λ-dimensional random row vector M be the random messages, k-dimensional random row vector K be the randomness, and $X := (M, K)$. For all $e \in E$, $Y_e = Xf_e$ is the symbol transmitted on channel e. Denote by $Y_A = \{Y_e : e \in A\}$ for $A \subset E$. Let $F(A)$ be the matrix formed by the juxtaposition of the global encoding kernels $f_e, e \in A$. Then the random output accessed by a wiretapper from a wiretap

[*] This work was done when Z. Zhang was on leave at The Chinese University of Hong Kong.

subset $W \in \mathcal{W}$ of edges is

$$\begin{aligned} Y_W &= XF(W) && (1)\\ &= (M,K)\begin{pmatrix} F_1(W)\\ F_2(W)\end{pmatrix} && (2)\\ &= MF_1(W) + KF_2(W), && (3)\end{aligned}$$

where $F_1(W)$ and $F_2(W)$ are submatrices of $F(W)$ consisting of its first λ rows and last γ rows, respectively. Let w-dimensional row vector $M_W = MF_1(W)$ and w-dimensional row vector $K_W = KF_2(W)$. Thus

$$Y_W = M_W + K_W.$$

A code is secure if and only if for all wiretap subsets $W \in \mathcal{W}$,

$$H(M|Y_W) = H(M). \qquad (4)$$

We do not assume that all the source messages m have positive probability. Therefore, M can have arbitrary distributions. We will obtain a necessary and sufficient condition for security in the next section.

III. A General Security Condition

Lemma 3.1: $H(M|Y_W) = H(M)$ if and only if $H(M_W|Y_W) = H(M_W)$.

Proof: Since $M_W = MF_1(W)$, $I(M;M_W) = H(M_W)$ and $I(M;Y_W) \geq I(M_W;Y_W)$. By Observing that $M \to M_W \to Y_W$ forms a Markov chain, we have $I(M;Y_W) \leq I(M_W;Y_W)$. Thus $I(M;Y_W) = I(M_W;Y_W)$. So if $H(M_W|Y_W) = H(M_W)$, then $I(M;Y_W) = I(M_W;Y_W) = 0$. And if $H(M|Y_W) = H(M)$, then $I(M_W;Y_W) = I(M;Y_W) = 0$. The lemma is proved. ■

In the following, we will obtain a necessary and sufficient condition for $H(M_W|Y_W) = H(M_W)$. Let m, k and y_W be the outcomes of M, K and Y_W, respectively. We respectively define the support of M_W, K_W and Y_W as:

$$\begin{aligned} \mathcal{S}_{M_W} &= \{\mu = mF_1(W) : P(m) > 0\}, && (5)\\ \mathcal{S}_{K_W} &= \{\kappa = kF_2(W) : P(k) > 0\}, && (6)\\ \mathcal{S}_{Y_W} &= \{y_W = \mu + \kappa : \mu \in \mathcal{S}_{M_W}, \\ &\qquad \kappa \in \mathcal{S}_{K_W}\}. && (7)\end{aligned}$$

For $\nu \in \mathbb{F}_q^w$ and $z \in \mathbb{F}_p$, we define

$$z\nu = \underbrace{\nu + \nu + \cdots + \nu}_{z},$$

with the convention that $0\nu = \mathbf{0}$. Since the *characteristic* of $\mathbb{F}_q$ is p, $p\nu = \mathbf{0}$ for all $\nu \in \mathbb{F}_q^w$. Let

$$\mathcal{C}_{M_W} = \left\{ \sum_{\mu,\mu' \in \mathcal{S}_{M_W}} z_{\mu\mu'}(\mu - \mu') : z_{\mu\mu'} \in \mathbb{F}_p \right\}.$$

$\mathcal{C}_{M_W}$ is a subgroup of $\mathbb{F}_q^w$. Denote the cosets of $\mathcal{C}_{M_W}$ by $\kappa + \mathcal{C}_{M_W} = \{\kappa + \nu : \nu \in \mathcal{C}_{M_W}\}$, where $\kappa \in \mathbb{F}_q^w$. In fact, $\mathcal{C}_{M_W}$ forms a vector space over $\mathbb{F}_p$, which will be shown as follows. First, $\mathcal{C}_{M_W}$ is a commutative group under addition. Second, for any element $\alpha \in \mathbb{F}_p$, $\alpha = 1+1+\cdots+1$ for α summands, where 1 is the multiplicative identity of $\mathbb{F}_p$. Thus for all elements $\nu \in \mathcal{C}_{M_W}$, $\alpha\nu = (1+1+\cdots+1)\nu = \nu+\nu+\cdots+\nu$, which is also in $\mathcal{C}_{M_W}$. Finally the distributive law and associative law also hold.

Proposition 3.2: For any $\mu, \mu' \in \mathcal{S}_{M_W}$ and $\kappa \in \mathbb{F}_q^w$.

$$\mu + \kappa + \mathcal{C}_{M_W} = \mu' + \kappa + \mathcal{C}_{M_W}. \qquad (8)$$

Proof: The equation (8) is equivalent to $\mu + \mathcal{C}_{M_W} = \mu' + \mathcal{C}_{M_W}$. When $\mu = \mu'$, the lemma is trivial. When $\mu \neq \mu'$, $\mu + \nu = \mu' + [(\mu - \mu') + \nu] \in \mu' + \mathcal{C}_{M_W}$, for all $\nu \in \mathcal{C}_{M_W}$. By the same method, $\mu' + \nu \in \mu + \mathcal{C}_{M_W}$, for all $\nu \in \mathcal{C}_{M_W}$. Hence $\mu + \mathcal{C}_{M_W} = \mu' + \mathcal{C}_{M_W}$. The proof is completed. ■

Next we will derive the algebraic structure of $\mathcal{S}_{K_W}$ and a property of probability distribution of $\mathcal{S}_{K_W}$ when $H(M_W|Y_W) = H(M_W)$.

Theorem 3.3: If $H(M_W|Y_W) = H(M_W)$, then $\mathcal{S}_{K_W}$ can be partitioned into cosets of $\mathcal{C}_{M_W}$, and for any $\kappa, \tilde{\kappa} \in \mathcal{S}_{K_W}$ in the same coset of $\mathcal{C}_{M_W}$, $\Pr(K_W = \tilde{\kappa}) = \Pr(K_W = \kappa)$.

Proof: $H(M_W|Y_W) = H(M_W)$ is equivalent to that for all $y_W \in \mathcal{S}_{Y_W}$ and $\mu \in \mathcal{S}_{M_W}$, $\Pr(Y_W = y_W|M_W = \mu) = \Pr(Y_W = y_W) > 0$. This implies that for all $\mu \in \mathcal{S}_{M_W}$,

$$\mathcal{S}_{Y_W} = \mu + \mathcal{S}_{K_W}. \qquad (9)$$

Since $\Pr(Y_W = y_W|M_W = \mu) = \Pr(K_W = y_W - \mu|M_W = \mu) = \Pr(K_W = y_W - \mu)$,

$$\Pr(Y_W = y_W) = \Pr(K_W = y_W - \mu). \qquad (10)$$

Now fix a $\kappa \in \mathcal{S}_{K_W}$ and consider any $\mu, \mu' \in \mathcal{S}_{M_W}$. Then by (9) there exists $\kappa_1 \in \mathcal{S}_{K_W}$ such that $\mu + \kappa = \mu' + \kappa_1$. Thus

$$\begin{aligned} \Pr(K_W = \kappa_1) &= \Pr(K_W = (\mu + \kappa) - \mu') && (11)\\ &= \Pr(Y_W = \mu + \kappa) && (12)\\ &= \Pr(K_W = \kappa), && (13)\end{aligned}$$

where (12) and (13) follow from application of (10). Again by (9), given κ_1, μ' and μ, there exists $\kappa_2 \in \mathcal{S}_{K_W}$, such that $\mu + \kappa_1 = \mu' + \kappa_2$. Then we have $\kappa_2 = \kappa + 2(\mu - \mu')$ and $\Pr(K_W = \kappa_2) = \Pr(K_W = \kappa_1) = \Pr(K_W = \kappa)$. By repeating this argument, we can see that for $z \in \mathbb{F}_p$, $\kappa_z = \kappa + z(\mu - \mu')$ are elements of $\mathcal{S}_{K_W}$, and $\Pr(K_W = \kappa_z) = \Pr(K_W = \kappa)$. Note that when $z = 0$, $\kappa_0 = \kappa + z(\mu - \mu') = \kappa$, which is an element of $\mathcal{S}_{K_W}$ according to our assumption.

Since the above argument works for any $\kappa \in \mathcal{S}_{K_W}$ and any $\mu, \mu' \in \mathcal{S}_{M_W}$, by replacing κ by $\kappa + z_{\mu\mu'}(\mu - \mu')$ where $z_{\mu\mu'} \in \mathbb{F}_q$, for any $\mu'', \mu''' \in \mathcal{S}_{M_W}$ where $(\mu, \mu') \neq (\mu'', \mu''')$, we can show that

$$\kappa + z_{\mu\mu'}(\mu - \mu') + z_{\mu''\mu'''}(\mu'' - \mu''') \in \mathcal{S}_{K_W} \qquad (14)$$

and

$$\begin{aligned} &\Pr\left(K_W = \kappa + z_{\mu\mu'}(\mu - \mu') + z_{\mu''\mu'''}(\mu'' - \mu''')\right)\\ &= \Pr(K_W = \kappa). && (15)\end{aligned}$$

Applying this argument repeatedly, we can see that for any $z_{\mu,\mu'} \in \mathbb{F}_q$ where $\mu, \mu' \in \mathcal{S}_{M_W}$,

$$\kappa + \sum_{\mu,\mu' \in \mathcal{S}_{M_W}} z_{\mu\mu'}(\mu - \mu') \in \mathcal{S}_{M_W}.$$

In other words, if $\kappa \in \mathcal{S}_{M_W}$, then $\kappa + \mathcal{C}_{M_W} \subset \mathcal{S}_{M_W}$. We also see that

$$\Pr\left(K_W = \kappa + \sum_{\mu,\mu' \in \mathcal{S}_{M_W}} z_{\mu\mu'}(\mu - \mu')\right)$$
$$= \Pr(K_W = \kappa), \tag{16}$$

i.e., if $\kappa, \tilde{\kappa} \in \mathcal{S}_{K_W}$ in the same coset of $\mathcal{C}_{M_W}$, $\Pr(K_W = \tilde{\kappa}) = \Pr(K_W = \kappa)$.

Finally, from the foregoing, we can write $\mathcal{S}_{K_W} = \bigcup_{\kappa \in \mathcal{S}_{K_W}} (\kappa + \mathcal{C}_{M_W})$. Since for $\kappa, \tilde{\kappa} \in \mathcal{S}_{M_W}$, $\kappa + \mathcal{S}_{M_W}$ and $\tilde{\kappa} + \mathcal{S}_{M_W}$ are either identical or disjoint, we have shown that $\mathcal{S}_{K_W}$ can be partitioned into cosets of $\mathcal{C}_{M_W}$. The proof is completed. ■

The next theorem is the converse of Theorem 3.3.

Theorem 3.4: If $\mathcal{S}_{K_W}$ can be partitioned into cosets of $\mathcal{C}_{M_W}$, and for any $\kappa, \tilde{\kappa} \in \mathcal{S}_{K_W}$ in the same coset of $\mathcal{C}_{M_W}$, $\Pr(K_W = \tilde{\kappa}) = \Pr(K_W = \kappa)$, then $H(M_W|Y_W) = H(M_W)$.

Proof: For all $y_W \in \mathcal{S}_{Y_W}$ and all $\mu \in \mathcal{S}_{M_W}$, we have

$$\Pr(Y_W = y_W | M_W = \mu) \tag{17}$$
$$= \Pr(K_W = y_W - \mu | M_W = \mu) \tag{18}$$
$$= \Pr(K_W = y_W - \mu). \tag{19}$$

Let $y_W \in \mathcal{S}_{Y_W}$ be fixed. then for all $\mu \in \mathcal{S}_{M_W}$, $y_W - \mu$ are in the same coset of $\mathcal{C}_{M_W}$, say J, because for $\mu, \mu' \in \mathcal{S}_{M_W}$, $(y_W - \mu) - (y_W - \mu') = \mu - \mu' \in \mathcal{C}_{M_W}$. Therefore,

$$\Pr(Y_W = y_W | M_W = \mu) = \frac{1}{r'} \Pr(K_W \in J), \tag{20}$$

where $r' = |\mathcal{C}_{M_W}| = |J|$. Hence, $\Pr(Y_W = y_W | M_W = \mu)$ does not depend on μ, i.e., Y_W and M_W are independent, or $H(M_W|Y_W) = H(M_W)$. The proof is completed. ■

Combing Theorem 3.3 and 3.4, we have

Theorem 3.5: For any $W \in \mathcal{W}$, $H(M_W|Y_W) = H(M_W)$, if and only if $\mathcal{S}_{K_W}$ can be partitioned into cosets of $\mathcal{C}_{M_W}$, and for any $\kappa, \tilde{\kappa} \in \mathcal{S}_{K_W}$ in the same coset of $\mathcal{C}_{M_W}$, $\Pr(K_W = \tilde{\kappa}) = \Pr(K_W = \kappa)$.

IV. Reduction To Cai and Yeung's Security Condition

In this section, we make the same assumption as in [4], that all $m \in \mathbb{F}_q^\lambda$ and $k \in \mathbb{F}_q^\gamma$ have positive probability. The following is a corollary of Theorem 3.3.

Corollary 4.1: If $\mathcal{S}_{M_W}$ is a vector space over $\mathbb{F}_q$ and $H(M_W|Y_W) = H(M_W)$, then $\mathcal{S}_{K_W}$ can be partitioned into some cosets of $\mathcal{S}_{M_W}$.

Proof: If $\mathcal{S}_{M_W}$ is a vector space, then $\mathbf{0} \in \mathcal{S}_{M_W}$. For any $\mu \in \mathcal{S}_{M_W}$, we can write

$$\mu = 1 \cdot \mu \tag{21}$$
$$= \sum_{\mu' \in \mathcal{S}_{M_W}} 1(\mu' = \mu) \cdot (\mu - \mathbf{0}), \tag{22}$$

where

$$1(\mu' = \mu) = \begin{cases} 1 & \text{if } \mu' = \mu, \\ 0 & \text{if } \mu' \neq \mu. \end{cases} \tag{23}$$

Thus we see that $\mu \in \mathcal{C}_{M_W}$, and hence $\mathcal{S}_{M_W} \subset \mathcal{C}_{M_W}$. On the other hand, since $\mathcal{S}_{M_W}$ is a vector space, it is readily seen that $\mathcal{C}_{M_W} \subset \mathcal{S}_{M_W}$, and $\mathcal{C}_{M_W} = \mathcal{S}_{M_W}$. Then by Theorem 3.3, $\mathcal{S}_{K_W}$ can be partitioned into some cosets of $\mathcal{S}_{M_W}$. ■

By Corrollary 4.1, when $\mathcal{S}_{K_W}$ is a vector space over $\mathbb{F}_q$, we have $\mathcal{S}_{M_W} \subset \mathcal{S}_{K_W}$. Then Theorem 3.5 is reduced to the following theorem which is equivalent to Theorem 3.3 in [4].

Theorem 4.2: $H(M_W|Y_W) = H(M_W)$ if and only if $\mathcal{S}_{M_W}$ is a subspace of $\mathcal{S}_{K_W}$ and for any $\kappa, \tilde{\kappa} \in \mathcal{S}_{K_W}$ in the same coset of $\mathcal{S}_{M_W}$, $\Pr(K_W = \tilde{\kappa}) = \Pr(K_W = \kappa)$.

When K has uniform distribution over $\mathbb{F}_q^\gamma$, the security condition $rank(F_2(W)) = rank(F(W))$ is also derived in [4]. The next corollary is a generalization of this condition without the assumption that all the source messages have positive distributions.

Corollary 4.3: Assume that M has arbitrary distributions over $\mathbb{F}_q^\lambda$ and K has uniform distributions over $\mathbb{F}_q^\gamma$. If $rank(F_2(W)) = rank(F(W))$, then $H(M_W|Y_W) = H(M_W)$.

Proof: Let $\langle F \rangle$ denotes the space spanned by the row vectors of matrix F. If K is distributed uniformly over $\mathbb{F}_q^\gamma$ and $rank(F_2(W)) = rank(F(W))$, then $\mathcal{S}_{K_W} = \langle F_2(W) \rangle = \langle F(W) \rangle$. Since $\mathcal{C}_{M_W}$ is a vector space over $\mathbb{F}_p$ and $\mathcal{C}_{M_W} \subset \mathcal{S}_{K_W}$, also a vector space over $\mathbb{F}_p$. Therefore, $\mathcal{S}_{K_W}$ can be partitioned into cosets of $\mathcal{C}_{M_W}$. The proof is completed by Theorem 3.4.

■

V. Conclusion

In this paper, we have studied the security problem of a multi-source linear network code. A necessary and sufficient condition for the security of such a code is obtained. Our security condition is a generalization of the security condition in [4], which is based on the assumption that all source messages have positive probability.

Acknowledgment

The authors would like to thank Dr. Bojin Zhuang and Dr. Kenneth W. Shum for their useful discussions. This work was partially supported by a grant from the Research Grant Committee of the Hong Kong Special Administrative Region, China (RGC Ref. No. CUHK 2/06C) and a grant from the European Community (FP7-INFSO-ICT-215252, N-Crave Project), a research grant from Qualcomm China, and a gift from Cisco, Inc.

References

[1] N. Cai and R. W. Yeung, "Secure network coding," ISIT02, June 2002.

[2] N. Cai and R. W. Yeung, "On the optimality of a construction of secure network codes," ISIT08, June 2008.

[3] N. Cai and R. W. Yeung, "Secure network coding," submitted to *IEEE Trans. Inform. Theory*.

[4] N. Cai and R. W. Yeung, “A secure condition for multi-source linear network coding,” ISIT07, June 2007.

[5] R. W. Yeung, *Information Theory and Network Coding*, Springer 2008.