Vulnerability of MRD-Code-based Universal Secure Network Coding against Stronger Eavesdroppers**

Eitaro SHIOJI[†*a)], *Nonmember*, **Ryutaroh MATSUMOTO**[†b)], *Member*, and **Tomohiko UYEMATSU**[†c)], *Senior Member*

SUMMARY   Silva et al. proposed a universal secure network coding scheme based on MRD codes, which can be applied to any underlying network code. This paper considers a stronger eavesdropping model where the eavesdroppers possess the ability to re-select the tapping links during the transmission. We give a proof for the impossibility of attaining universal security against such adversaries using Silva et al.'s code for all choices of code parameters, even with a restricted number of tapped links. We also consider the cases with restricted tapping duration and derive some conditions for this code to be secure.

key words: *network coding, secure network coding, linear network coding, universal security, MRD code*

1.   Introduction

The notion of network coding, proposed by Ahlswede et al. [1], has been attracting much attention. On a conventional routing network, each node is only allowed to relay the received packets to the next node, while on a network with network coding support, each node is allowed to perform some data processing using the received packets and send the result to the next node. It is known that the use of network coding offers many advantages over the use of conventional network, such as achievement of higher rate in multicast communications or better energy efficiency in wireless communications [2].

Secrecy of communication, or more specifically, information-theoretically secure communication in the presence of an adversary capable of tapping a fixed number of links of its choice, is considered as one of such advantages of network coding. Such a scheme, referred to as secure network coding, consists of the following two components: the network code which determines how packets are coded at intermediate nodes, and the outer code which is a pre-coding done at the source before transmission. Several secure network codes have been proposed, such as the one by Cai et al. [3]. However, these codes require the reconstruction of

the network code, or the reconstruction of the outer code in order to attain security for a given set of tapped links. Such a property causes problems, such as difficulty when securing random network codes [4], where network codes are constructed randomly.

Silva et al. proposed a universal secure network coding method [5] based on MRD codes [6] and coset coding scheme [7]. This code can be applied on top of any already-constructed network code to attain security. However, due to its use of vector outer code which requires that each symbol be transmitted over multiple time slots, it must assume that the tapped links are fixed during the transmission period.

We consider a stronger eavesdropping model where the eavesdroppers possess the ability to re-select the tapping links during the transmission. Such a model is worth consideration because the conventional non-universal secure network codes (e.g. [3], [8]) are guaranteed to be secure against it. Moreover, this model corresponds to some practical situations where random network coding is used and the coding vectors are time-varying, such as the robust random network coding scheme proposed by Chou et al. [9]. Also, the current standard of the IP protocol allows the network to split a packet into multiple fragments and carry them through multiple distinct routes, as explained in [10, Section 11.5]. Thus, the stronger eavesdropping model considered here has practical importance when Silva et al.'s method is used over the current Internet.

This paper aims to clarify the security of Silva et al.'s universal code against this eavesdropping model, and is organized as follows. In Section 2 we define some notations and briefly review some of the existing results of secure network coding, and describe Silva et al.'s universal secure network code. In Section 3 we introduce our stronger eavesdropping model. In Section 4 we prove the vulnerability of this universal code against our model for all code parameters. We also prove that the code is vulnerable even with a limited number of tapped links. Moreover, the cases with shorter tapping duration are considered, and sufficient conditions and necessary conditions for the code to be secure are given. In Section 5 we state our conclusion and the future tasks.

2.   Preliminaries

In this section we define our basic notations and review some of the existing results of secure network coding.

2.1 Extension Field

The extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ can be regarded as a vector space over $\mathbb{F}_q$. Thus, when the basis of this space is fixed, an element of $\mathbb{F}_{q^m}$ can be represented as an m-dimensional vector over $\mathbb{F}_q$. For $y \in \mathbb{F}_{q^m}$, denote the i-th element of its vector representation as $y^{(i)}$. Accordingly, the vector representation of $x \in \mathbb{F}_{q^m}$ is written as $(x^{(1)}, x^{(2)}, \cdots, x^{(m)}) \in \mathbb{F}_q^m$.

2.2 Network Coding

Data communication over a network is considered. We use a network model defined by an acyclic and directed graph $G = (V, E)$, where V and E denote the set of nodes and the set of links, respectively. In this model we assume that, each link can carry an element of $\mathbb{F}_q$ per unit time, and data flowing on the network is not affected by delays, erasures or errors.

Let $s \in V$ and $\mathcal{R} \subset V$ denote the source node and the set of sink nodes, respectively. The source node wishes to multicast the sequence $X = (X_1, X_2, \cdots, X_n)^T \in \mathbb{F}_q^n$ to all sink nodes at rate n. The rate is defined as the number of elements of $\mathbb{F}_q$ transmitted at the source node per unit time. Assume $n \leq \min\{\text{maxflow}(s, r) \mid r \in \mathcal{R}\}$ holds, where $\text{maxflow}(i, j)$ denotes the maximum flow from node i and j. We assume that linear network coding [11] is employed on the network, i.e. the type of data processing performed on the packets at each node is limited to linear combination. This implies that the data flowing on any link on the network can be represented as an $\mathbb{F}_q$-linear combination of the sequence $X_1, X_2, \cdots, X_n$. Thus, the information flowing on a link e can be denoted as $Y_e = \vec{b}_e \cdot X$ using a global coding vector (GCV), $\vec{b}_e = (b_1, b_2, \cdots, b_n)^T \in \mathbb{F}_q^n$, where "·" denotes the inner product operator for vectors. When one has access to, say, the l links $e_1, e_2, \cdots, e_l$, then the information obtained from these links is denoted as $MX \in \mathbb{F}_q^l$, where $M = (\vec{b}_{e_1}, \vec{b}_{e_2}, \cdots, \vec{b}_{e_l})^T$.

Constructing a network code is equivalent to fixing the GCV of each link by setting the coefficients of the linear combination performed at each node. A network code is called feasible if every sink is able to decode X. When q is sufficiently large, a feasible network code for rate n multicast can always be constructed [2].

2.3 Secure Network Coding

The wiretap network model used in the works [3] and [5] on which secure network coding is employed is described below. For simplification, only one receiver is assumed. Let F be some extension field of $\mathbb{F}_q$.

- **Sender:** The sender wishes to send the secret information sequence represented by a random variable $S = (S_1, S_2, \cdots, S_k)^T$ distributed uniformly over F^k. S is first coded into the sequence $X = (X_1, X_2, \cdots, X_n)^T \in$ F^n using an outer code and then X is sent over the network with a feasible network code.
- **Receiver:** The receiver receives the information sequence $Y = AX = (Y_1, Y_2, \cdots, Y_n)^T \in F^n$, where A is the matrix constructed by appending the GCVs of the input links to the receiver node.
- **Eavesdropper:** The eavesdropper is able to wiretap any μ links on the network. Let the set of tapped links be $\mathcal{I} = \{e_1, e_2, \cdots, e_\mu\} \subseteq E$. Then the wire-tapped information sequence is represented as $W = BX = (W_1, W_2, \cdots, W_\mu)^T \in F^\mu$ using the matrix $B = (\vec{b}_{e_1}, \vec{b}_{e_2}, \cdots, \vec{b}_{e_\mu})^T \in \mathbb{F}_q^{\mu \times n}$.

The security which guarantees that no information about S leaks out to the wiretapper even when μ arbitrary links are wiretapped, is defined as follows.

Definition 1 (strong security [3]).

$$H(S|Y) = 0, \tag{1}$$
$$I(S; W = BX) = 0, \forall \mathcal{I} \subseteq E, |\mathcal{I}| = \mu.$$

Condition (1) is satisfied if the outer code used is uniquely decodable and the network code used is feasible. Cai et al. showed a construction method [3] for secure network codes that satisfies the conditions in Definition 1 for $\mu = n - k$, using $F = \mathbb{F}_q$.

2.4 Universal Secure Network Code

The definition of strong security depends on the GCVs of the set of tapped links $\mathcal{I}$, implying that it is dependent on the underlying network code. Silva et al. proposed a coding scheme that attains strong security that is independent of the network code, as defined below.

Definition 2 (universal strong security [5]).

$$H(S|Y) = 0, \tag{2}$$
$$I(S; W = BX) = 0, \forall B \in \mathbb{F}_q^{\mu \times n}. \tag{3}$$

The universal code is based on MRD codes[6] and coset coding scheme[7]. MRD codes are a class of linear code over $\mathbb{F}_{q^m}$ which is optimal in the rank-distance sense. Coset coding scheme is a type of randomized coding described as follows. Let H be the parity check matrix of a $[n, n - k]$ linear code C over F. To code $S = (S_1, \cdots, S_k) \in F^k$ into $X = (X_1, \cdots, X_n) \in F^n$, regard S as a syndrome of C, and choose X uniformly random from the corresponding coset. Using these tools, the communication procedure of the universal network code is briefly described as follows:

The procedures of secret communication using the universal secure network code is briefly described as follows:

1. Choose an integer $m \geq n$.
2. Construct an $[n, \mu = n - k]$ MRD code over $\mathbb{F}_{q^m}$.
3. Encode $S \in \mathbb{F}_{q^m}^k \to X \in \mathbb{F}_{q^m}^n$ by coset coding scheme based on the MRD code.
4. Split X and send them over m time slots using a feasible

network code, i.e. transmit $(X_1^{(t)}, X_2^{(t)}, \cdots, X_n^{(t)})^T \in \mathbb{F}_q^n$ at time $1 \le t \le m$.

3. Stronger Eavesdropping Model

In this section, we propose a stronger eavesdropping model than the one presented in Section 2.3.

3.1 Model Definition

In the conventional non-universal secure network coding scheme, $F = \mathbb{F}_q$ is used, but note that in the universal scheme, due to the use of MRD code over $\mathbb{F}_{q^m}$, $F = \mathbb{F}_{q^m}$ is used. Since the network can only transmit up to n elements of $\mathbb{F}_q$ per unit time, the universal code requires that a secret message S be transmitted over multiple time slots, while the conventional codes require only one. The definition of the wiretap network model implies that the universal code assumes the selection of tapped links to be fixed during the transmission. Hence, we replace the eavesdropper model presented in Section 2.3 with the following stronger model.

Stronger Eavesdropper: At each time slot of the transmission over m time slots, the wiretapper can re-select the set of μ tapping links. Let $e_{i,t} \in E$ denote the i-th link tapped at time t. The wiretapped links are then, $e_{1,1}, e_{2,1}, \cdots, e_{\mu,1}, \cdots \cdots, e_{1,m}, e_{2,m}, \cdots, e_{\mu,m}$. For $x = (x_1, x_2, \cdots, x_n)^T \in \mathbb{F}_{q^m}^n$, define $\bar{x} \in \mathbb{F}_q^{mn}$ as

$$\bar{x} \triangleq (x_1^{(1)}, x_2^{(1)}, \cdots, x_n^{(1)}, \cdots \cdots, x_1^{(m)}, x_2^{(m)}, \cdots, x_n^{(m)})^T.$$

Note that there is a one-to-one correspondence between x and $\bar{x}$. For simplification, let $\vec{b}_{i,t} \triangleq \vec{b}_{e_{i,t}}$. The GCVs of the μ links tapped at time t are $\vec{b}_{1,t}, \cdots, \vec{b}_{\mu,t} \in \mathbb{F}_q^n$. Also, define $\tilde{B} \in \mathbb{F}_q^{m\mu \times mn}$ and $B_t \in \mathbb{F}_q^{\mu \times n}$ as follows:

$$\tilde{B} \triangleq \begin{bmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_m \end{bmatrix}, \quad B_t \triangleq \begin{bmatrix} \vec{b}_{1,t}^T \\ \vec{b}_{2,t}^T \\ \vdots \\ \vec{b}_{\mu,t}^T \end{bmatrix}.$$

Then, the information obtained by the wiretapper is represented by the random variable $\tilde{W}$ distributed over $\mathbb{F}_q^{m\mu}$, defined by

$$\tilde{W} \triangleq \tilde{B}\bar{X}.$$

We now define the following security conditions that assure security against our eavesdropping model.

Definition 3 (universal m-strong security)**.**

$$H(S|Y) = 0,$$
$$I(S; \tilde{W} = \tilde{B}\bar{X}) = 0, \forall B_t \in \mathbb{F}_q^{\mu \times n}, t = 1, \cdots, m.$$

Note that, the conventional eavesdropping model defined in Section 2.3 corresponds to the special case of our model

Table 1 The elements of $\mathbb{F}_{2^2}$

Power	Polynomial	Vector
Zero	0	$(0,0)$
α^0	1	$(0,1)$
α^1	α^1	$(1,0)$
α^2	$\alpha^1 + 1$	$(1,1)$

with $\vec{b}_{i,t_1} = \vec{b}_{i,t_2}, \forall t_1, t_2, i$. Also note that the security of the non-universal conventional secure network codes such as the one by Cai [3], is not affected by such a strengthening of the eavesdropper because a secret message is transmitted over only one time slot. To be fair with the universal code, we also mention that even when m secret messages are regarded as one message and are sent over m time period, the conventional non-universal codes remain secure. To avoid confusion, we mention that universal m-strong security and k-strong security[12] are distinct notions.

3.2 Code Example

We present an example of Silva et al.'s universal secure network code and show that it is insecure against our eavesdropping model. The example code is constructed using the following parameters.

- $q = 2, k = 1, n = 2, m = 2, \mu = n - k = 1$.
- $\mathbb{F}_{2^2}$ constructed with the root α of primitive polynomial $f(x) = x^2 + x + 1$. (Table 1 shows the elements of this field in power, polynomial, and vector representation)
- A parity check matrix $H = [1, \alpha]$ of a $[2, 1]$MRD code over $\mathbb{F}_{2^2}$.

Note that between $X = (X_1, X_2)^T$ and S, we have the relation

$$S = HX = X_1 + \alpha X_2. \quad (4)$$

This code uses a network code over $\mathbb{F}_2$ at rate 2, so it is sufficient to consider only the links e_1, e_2, e_3 with GCVs $\vec{b}_{e_1} = (0,1)^T$, $\vec{b}_{e_2} = (1,0)^T$, $\vec{b}_{e_3} = (1,1)^T$. This implies that the information flowing on an arbitrary link is one of $X \cdot \vec{b}_{e_1} = X_1, X \cdot \vec{b}_{e_2} = X_2$, or $X \cdot \vec{b}_{e_3} = X_1 + X_2$. Table 2 shows the value, represented in power and vector form, on each link with all distinct GCVs for each X sent. The value of S is also shown.

An eavesdropper capable of re-selecting the tapping links at each time is able to wiretap an element of $\{(P^{(1)}, Q^{(2)}) \mid P, Q \in \{X_1, X_2, (X_1 + X_2)\}\}$. Recall that $P^{(i)}$ represents the i-th element of the vector representation of $P \in \mathbb{F}_{q^m}$. When the sequence $(X_1^{(1)}, (X_1 + X_2)^{(2)}) = (0, 1)$ (underlined on the table) is wiretapped, the candidates for S are narrowed down to α^0, α^1, implying

$$H(S|X_1^{(1)}, (X_1 + X_2)^{(2)}) \ne H(S)$$
$$\Rightarrow I(S; X_1^{(1)}, (X_1 + X_2)^{(2)}) \ne 0$$
$$\Rightarrow I(S; \tilde{W} = \tilde{B}\bar{X}) \ne 0, \text{ for some } \tilde{B}, \text{rank}\tilde{B} = 2.$$

Therefore, we can conclude that this code does not attain universal m-strong security.

Table 2 The value flowing on each link and S, for each X

X_1	X_2	$X_1 + X_2$	S
$0 = (\underline{0}, 0)$	$0 = (0, 0)$	$0 = (0, 0)$	0
$0 = (\underline{0}, 0)$	$\alpha^0 = (0, 1)$	$\alpha^0 = (0, \underline{1})$	α^1
$0 = (\underline{0}, 0)$	$\alpha^1 = (1, 0)$	$\alpha^1 = (1, \underline{0})$	α^2
$0 = (\underline{0}, 0)$	$\alpha^2 = (1, 1)$	$\alpha^2 = (1, \underline{1})$	α^0
$\alpha^0 = (\underline{0}, 1)$	$0 = (0, 0)$	$\alpha^0 = (0, \underline{1})$	α^0
$\alpha^0 = (\underline{0}, 1)$	$\alpha^0 = (0, 1)$	$0 = (0, 0)$	α^2
$\alpha^0 = (\underline{0}, 1)$	$\alpha^1 = (1, 0)$	$\alpha^2 = (1, \underline{1})$	α^1
$\alpha^0 = (\underline{0}, 1)$	$\alpha^2 = (1, 1)$	$\alpha^1 = (1, \underline{0})$	0
$\alpha^1 = (1, 0)$	$0 = (0, 0)$	$\alpha^1 = (1, 0)$	α^1
$\alpha^1 = (1, 0)$	$\alpha^0 = (0, 1)$	$\alpha^2 = (1, \underline{1})$	0
$\alpha^1 = (1, 0)$	$\alpha^1 = (1, 0)$	$0 = (0, 0)$	α^0
$\alpha^1 = (1, 0)$	$\alpha^2 = (1, 1)$	$\alpha^0 = (0, \underline{1})$	α^2
$\alpha^2 = (1, 1)$	$0 = (0, 0)$	$\alpha^2 = (1, \underline{1})$	α^2
$\alpha^2 = (1, 1)$	$\alpha^0 = (0, 1)$	$\alpha^1 = (1, 0)$	α^0
$\alpha^2 = (1, 1)$	$\alpha^1 = (1, 0)$	$\alpha^0 = (0, \underline{1})$	0
$\alpha^2 = (1, 1)$	$\alpha^2 = (1, 1)$	$0 = (0, 0)$	α^1

4. Security Analysis

In this section, we analyze the security of the universal secure network code against our stronger eavesdropping model. The example presented in the previous section shows that the universal code is not universal m-strongly secure *in general*. Construction of the universal code involves the choice of parameters n, k, q, m, a parity check matrix H, and a basis of $\mathbb{F}_{q^m}$. A natural question to ask at this point is, if it is possible to secure this code by restricting these parameters. We show that universal m-strong security cannot be attained no matter how they are chosen. We also analyze the cases with a restricted number of tapping links and tapping duration.

4.1 Proof of Vulnerability for $\mu = n - k$

As a preparation, we first derive the necessary and sufficient condition for the universal code to be universal m-strongly secure. Let

$$N_{s,w}^{\tilde{B}} \triangleq |\{x \in \mathbb{F}_{q^m}^n \mid s = Hx, w = \tilde{B}\bar{x}\}|.$$

Lemma 1. *The necessary and sufficient condition for the universal coding scheme with parameters n, k, q, m, H and a fixed basis of $\mathbb{F}_{q^m}$ to attain universal m-strong security for $\mu \geq 1$ is, for $\forall w \in \mathbb{F}_q^{m\mu}, \forall B_t \in \mathbb{F}_q^{\mu \times n}, \text{rank} B_t = \mu, 1 \leq t \leq m$ the following holds:*

$$N_{s,w}^{\tilde{B}} = N_{s',w}^{\tilde{B}}, \forall s, s' \in \mathbb{F}_{q^m}^k.$$

Proof. By the definition of universal m-strong security, for $\forall w \in \mathbb{F}_q^{m\mu}$,

$$I(S; \tilde{W}) = 0$$
$$\Leftrightarrow \Pr(S = s | \tilde{W} = w) = \Pr(S = s), \forall s \in \mathbb{F}_{q^m}^k$$
$$\Leftrightarrow \frac{|\{x \in \mathbb{F}_{q^m}^n \mid s = Hx, w = \tilde{B}\bar{x}\}|}{|\{x \in \mathbb{F}_{q^m}^n \mid w = \tilde{B}\bar{x}\}|} = \frac{1}{q^{mk}}, \forall s \quad (5)$$
$$\Leftrightarrow N_{s,w}^{\tilde{B}} = \frac{|\{x \in \mathbb{F}_{q^m}^n \mid w = \tilde{B}\bar{x}\}|}{q^{mk}}, \forall s.$$

Equation (5) holds because X is distributed uniformly over $\mathbb{F}_{q^m}^n$ and S is distributed uniformly over $\mathbb{F}_{q^m}^k$. Note that to attain universal m-strong security, it is sufficient to satisfy the security condition for all full-rank $B_t, 1 \leq t \leq m$. □

We prove the vulnerability for the special case $\mu = n - k$, which corresponds to the case considered in the work by Silva et al.

Lemma 2. *The necessary and sufficient condition for the universal coding scheme with parameters n, k, q, m, H and a fixed basis of $\mathbb{F}_{q^m}$ to attain universal m-strong security for $\mu = n - k$ is, for $\forall w \in \mathbb{F}_q^{m\mu}, \forall B_t \in \mathbb{F}_q^{\mu \times n}, \text{rank} B_t = \mu, 1 \leq t \leq m, \mathcal{X}_w = \{x \in \mathbb{F}_{q^m}^n \mid w = \tilde{B}\bar{x}\}$, the following holds:*

$$x \neq x' \Rightarrow Hx \neq Hx', \forall x, x' \in \mathcal{X}_w.$$

Proof. By Lemma 1, $\forall w \in \mathbb{F}_q^{m\mu}$,

$$N_{s,w}^{\tilde{B}} = \frac{|\{x \in \mathbb{F}_{q^m}^n \mid w = \tilde{B}\bar{x}\}|}{q^{mk}}, \forall s$$
$$\Leftrightarrow |\{x \in \mathcal{X}_w \mid s = Hx\}| = 1, \forall s \quad (6)$$
$$\Leftrightarrow x \neq x' \Rightarrow Hx \neq Hx', \forall x, x' \in \mathcal{X}_w.$$

Equation (6) holds since

$$|\{x \in \mathbb{F}_{q^m}^n \mid w = \tilde{B}\bar{x}\}| = q^{\dim \ker \tilde{B}}$$
$$= q^{(mn - \text{rank}\tilde{B})}$$
$$= q^{(mn - m(n-k))} = q^{mk}.$$

□

Note that if Lemma 2 holds for set $\mathcal{X}_w$ then the lemma holds for any of its subsets. Let $w_{i,t} \in \mathbb{F}_q$ be the information tapped at time t on the i-th link. Then, by representing w as

$$w = (w_{1,1}, w_{2,1}, \cdots, w_{\mu,1}, \cdots\cdots, w_{1,m}, w_{2,m}, \cdots w_{\mu,m})^T,$$

Lemma 2 yields the following corollary.

Corollary 1. *The necessary and sufficient condition for the universal coding scheme with parameters n, k, q, m, H and a fixed basis of $\mathbb{F}_{q^m}$ to satisfy universal m-strong security for $\mu = n - k$ is that*

$$x \neq x' \Rightarrow Hx \neq Hx', \forall x, x' \in \mathcal{X}$$

holds for an arbitrary set $\mathcal{X} \subseteq \mathbb{F}_{q^m}^n$ such that $\forall x \in \mathcal{X}$ satisfies

$$\begin{cases} (\vec{b}_{1,1} \cdot x)^{(1)} = w_{1,1}, \cdots, (\vec{b}_{1,m} \cdot x)^{(m)} = w_{1,m}, \\ (\vec{b}_{2,1} \cdot x)^{(1)} = w_{2,1}, \cdots, (\vec{b}_{2,m} \cdot x)^{(m)} = w_{2,m}, \\ \quad\vdots \\ (\vec{b}_{\mu,1} \cdot x)^{(1)} = w_{\mu,1}, \cdots, (\vec{b}_{\mu,m} \cdot x)^{(m)} = w_{\mu,m}, \end{cases}$$

for $\forall w \in \mathbb{F}_q^{m\mu}$.

Proof. By denoting the l-th element of $\vec{b}_{i,t}$ as $b_{i,t}^{[l]} \in \mathbb{F}_q$,

$$(\vec{b}_{i,t} \cdot x)^{(t)} = (b_{i,t}^{[1]} x_1 + b_{i,t}^{[2]} x_2 + \cdots + b_{i,t}^{[n]} x_n)^{(t)}$$

$$= (b^{[1]}_{i,t} x^{(t)}_1 + b^{[2]}_{i,t} x^{(t)}_2 + \cdots + b^{[n]}_{i,t} x^{(t)}_n) \qquad (7)$$

$$= \vec{b}_{i,t} \cdot (x^{(t)}_1, x^{(t)}_2, \cdots, x^{(t)}_n)^T$$

holds. Note that since $\mathbb{F}_{q^m}$ is a linear space on $\mathbb{F}_q$,

$$b^{[l]}_{i,t} x_l = b^{[l]}_{i,t} (x^{(1)}_l, x^{(2)}_l, \cdots, x^{(m)}_l)^T$$
$$= (b^{[l]}_{i,t} x^{(1)}_l, b^{[l]}_{i,t} x^{(2)}_l, \cdots, b^{[l]}_{i,t} x^{(m)}_l)^T$$

holds for every $1 \leq l \leq n$, and adding the t-th element of each of $b^{[1]}_{i,t} x_1, \cdots, b^{[n]}_{i,t} x_n$ yields Eq. (7). Therefore, we have the relation,

$$w_{i,t} = \vec{b}_{i,t} \cdot (x^{(t)}_1, x^{(t)}_2, \cdots, x^{(t)}_n)^T = (\vec{b}_{i,t} \cdot x)^{(t)}. \qquad (8)$$

The corollary holds immediately from Eq. (8) and Lemma 2. $\qquad \square$

Using this corollary, we prove the following theorem.

Theorem 1. *For any choice of parameters n, k, q, m, H and the basis for $\mathbb{F}_{q^m}$, the universal secure network coding scheme cannot satisfy the universal m-strong security condition for $\mu = n - k$.*

Proof. Assume the existence of the universal code which satisfies the universal m-strong security condition. Let X denote the set of all $x \in \mathbb{F}^n_{q^m}$ satisfying the relation,

$$\begin{cases} x^{(1)}_1 = x^{(2)}_1 = \cdots = x^{(m)}_1 = 0, \\ x^{(1)}_2 = x^{(2)}_2 = \cdots = x^{(m)}_2 = 0, \\ \quad \vdots \\ x^{(1)}_\mu = x^{(2)}_\mu = \cdots = x^{(m)}_\mu = 0. \end{cases} \qquad (9)$$

Note that, $|X| = q^{mn}/q^{m\mu} = q^{mk}$. Let α be an element of $\mathbb{F}_q$, and choose $\hat{x} \in \mathbb{F}^n_{q^m}$ that satisfies the following:

$$\begin{cases} \hat{x}^{(1)}_1 = \hat{x}^{(2)}_1 = \cdots = \hat{x}^{(m)}_1 = 0, \\ \hat{x}^{(1)}_2 = \hat{x}^{(2)}_2 = \cdots = \hat{x}^{(m)}_2 = 0, \\ \quad \vdots \\ \hat{x}^{(1)}_\mu = \hat{x}^{(2)}_\mu = \cdots = \hat{x}^{(m-1)}_\mu = 0, \hat{x}^{(m)}_\mu = 1, \hat{x}^{(m)}_{\mu+1} = \alpha. \end{cases}$$

Such $\hat{x}$ always exists, and satisfies $\hat{x} \notin X$. For $\psi \in \mathbb{F}_q$, let $X_\psi \subseteq X$ be the set of all $x \in X$ satisfying $x^{(m)}_{\mu+1} = \psi$. In other words, $\forall x \in X_\psi$ satisfies Eq. (10).

$$\begin{cases} x^{(1)}_1 = x^{(2)}_1 = \cdots = x^{(m)}_1 = 0, \\ x^{(1)}_2 = x^{(2)}_2 = \cdots = x^{(m)}_2 = 0, \\ \quad \vdots \\ x^{(1)}_\mu = x^{(2)}_\mu = \cdots = x^{(m)}_\mu = 0, x^{(m)}_{\mu+1} = \psi. \end{cases} \qquad (10)$$

Note that,

$$\bigcup_{\psi \in \mathbb{F}_q} X_\psi = X \qquad (11)$$

holds. We see that,

$$\begin{cases} x^{(1)}_1 = x^{(2)}_1 = \cdots = x^{(m)}_1 = 0, \\ x^{(1)}_2 = x^{(2)}_2 = \cdots = x^{(m)}_2 = 0, \\ \quad \vdots \\ x^{(1)}_\mu = x^{(2)}_\mu = \cdots = x^{(m-1)}_\mu = 0, (\gamma x_\mu + x_{\mu+1})^{(m)} = \psi, \end{cases} \qquad (12)$$

holds for $\forall x \in \{\hat{x}\} \cup X_\psi$ by the definition of $\hat{x}$ and X_ψ, where $\gamma = \psi - \alpha$. Note that, Corollary 1 can be applied to the set $\{\hat{x}\} \cup X_\psi$ because relation (12) can be represented as

$$\begin{cases} ((1, 0, \cdots \cdots \cdots, 0) \cdot x)^{(1)} = 0, \cdots, ((1, 0, \cdots \cdots \cdots, 0) \cdot x)^{(m)} = 0, \\ ((0, 1, 0, \cdots \cdots \cdots, 0) \cdot x)^{(1)} = 0, \cdots, ((0, 1, 0, \cdots \cdots \cdots, 0) \cdot x)^{(m)} = 0, \\ \quad \vdots \\ ((0, \cdots, 0, \underbrace{1}_{\mu\text{-th}}, 0, \cdots, 0) \cdot x)^{(1)} = 0, \cdots, ((0, \cdots, 0, \underbrace{\gamma}_{\mu\text{-th}}, 1, 0, \cdots, 0) \cdot x)^{(m)} = \psi, \end{cases}$$

and because it can be confirmed that the corresponding matrices B_t in Corollary 1 satisfy $\text{rank} B_t = \mu$, $1 \leq t \leq m$. Applying Corollary 1 to the set $\{\hat{x}\} \cup X_\psi$ we have

$$x \neq x' \Rightarrow Hx \neq Hx', \forall x, x' \in \{\hat{x}\} \cup X_\psi, \forall \psi \in \mathbb{F}_q.$$

This result, combined with Eq. (11), yields

$$H\hat{x} \neq Hx, \forall x \in X. \qquad (13)$$

Corollary 1 can be applied to the set X as well by relation (9), hence

$$x \neq x' \Rightarrow Hx \neq Hx', \forall x, x' \in X \qquad (14)$$

holds. Therefore, Eqs. (13) and (14) yield

$$x \neq x' \Rightarrow Hx \neq Hx', \forall x, x' \in \{\hat{x}\} \cup X. \qquad (15)$$

However, by $\hat{x} \notin X$ and $|X| = q^{mk}$, for Eq. (15) to hold, it is necessary that

$$|\{Hx \mid x \in \mathbb{F}^n_{q^m}\}| \geq |\{\hat{x}\} \cup X| = q^{mk} + 1$$

holds, which contradicts with

$$|\{Hx \mid x \in \mathbb{F}^n_{q^m}\}| = (q^m)^{\text{rank} H} = q^{mk},$$

Therefore, a code constructed by the universal coding scheme that attains universal m-strong security does not exist. $\qquad \square$

4.2 Proof of Vulnerability for $1 \leq \mu \leq n - k$

We now consider the more general case, $1 \leq \mu \leq n - k$, and prove that the code still cannot be secure for any μ. First, we define the following to simplify the notations:

- $\mathcal{H}_s \triangleq \{x \in \mathbb{F}^n_{q^m} \mid s = Hx\}$,
- $X^{\tilde{B}}_w \triangleq \{x \in \mathbb{F}^n_{q^m} \mid w = \tilde{B}\bar{x}\}$.

Now we prove the following lemma.

Lemma 3. *If the universal coding scheme is universal m-strongly secure for $\mu = 1$, then it is universal m-strongly*

secure for $\mu = n - k$.

Proof. When universal m-strong security for $\mu = 1$ is attained for some code, by Lemma 1, for $\forall w \in \mathbb{F}_q^m$, $\forall B_t \in \mathbb{F}_q^{1 \times n}$, rank$B_t = 1$, $1 \le t \le m$, the following must hold for this code:

$$N_{s,w}^{\tilde{B}} = N_{s',w}^{\tilde{B}}, \forall s, s' \in \mathbb{F}_{q^m}^k.$$

We will show that, then, such a code attains universal m-strongly security for $\mu = n-k$, which implies that by Lemma 1, for $\forall w^* \in \mathbb{F}_q^{m(n-k)}$, $\forall B_t^* \in \mathbb{F}_q^{(n-k) \times n}$, rank$B_t^* = n - k$, $1 \le t \le m$,

$$B^* = \begin{bmatrix} B_1^* & & & \\ & B_2^* & & \\ & & \ddots & \\ & & & B_m^* \end{bmatrix},$$

the following holds:

$$N_{s,w^*}^{B^*} = N_{s',w^*}^{B^*}, \forall s, s' \in \mathbb{F}_{q^m}^k.$$

Let $B_{t,i}^* \in \mathbb{F}_q^{1 \times n}$ denote the i-th row of B_t^*, and let B' denote the matrix defined as below, using the matrices $B^{[i]} \in \mathbb{F}_q^{m \times mn}$, $1 \le i \le n - k$:

$$B' = \begin{bmatrix} B^{[1]} \\ B^{[2]} \\ \vdots \\ B^{[n-k]} \end{bmatrix}, B^{[i]} = \begin{bmatrix} B_{1,i}^* & & & \\ & B_{2,i}^* & & \\ & & \ddots & \\ & & & B_{m,i}^* \end{bmatrix}.$$

Note that B' is obtained by permuting the rows of B^*. Let w' be the column vector obtained by permuting the rows of w^* in the same order as B', and let $w^{[i]} \in \mathbb{F}_q^m$, $1 \le i \le n - k$, denote each m rows of w' as shown below:

$$w' = \begin{bmatrix} w^{[1]} \\ w^{[2]} \\ \vdots \\ w^{[n-k]} \end{bmatrix}. \tag{16}$$

Using the notations above, we have

$$\begin{aligned} N_{s,w^*}^{B^*} &= |\{x \in \mathbb{F}_{q^m}^n \mid s = Hx, w^* = B^* \bar{x}\}| \\ &= |\{x \in \mathbb{F}_{q^m}^n \mid s = Hx, w' = B' \bar{x}\}| \\ &= \left| \left\{ x \in F_{q^m} \mid s = Hx, \begin{bmatrix} w^{[1]} \\ w^{[2]} \\ \vdots \\ w^{[n-k]} \end{bmatrix} = \begin{bmatrix} B^{[1]} \\ B^{[2]} \\ \vdots \\ B^{[n-k]} \end{bmatrix} \bar{x} \right\} \right| \\ &= \left| \bigcap_{i=1}^{n-k} \left\{ x \in \mathcal{X}_{w^{[i]}}^{B^{[i]}} \mid s = Hx \right\} \right| \\ &= \left| \left(\bigcap_{i=1}^{n-k} \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \bigcap \mathcal{H}_s \right|. \end{aligned}$$

Noting that

$$\left| \cap_{i=1}^{n-k} \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right| = |\{w^* = B^* \bar{x}\}| = q^{mk}, \tag{17}$$

we prove $N_{s_1,w^*}^{B^*} = N_{s_2,w^*}^{B^*}$, $\forall s_1, s_2 \in \mathbb{F}_{q^m}^k$ for each of the following three cases of the set $\left(\bigcap_{i=1}^{n-k} \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \bigcap \mathcal{H}_s$.

Case 1 $\left(\bigcap_{i=1}^{n-k} \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \bigcap \mathcal{H}_s = \phi, \forall s$: By $\bigcup_s \mathcal{H}_s = \mathbb{F}_{q^m}^n$, we have

$$\left(\bigcap_{i=1}^{n-k} \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \bigcap \mathcal{H}_s = \phi, \forall s \Leftrightarrow \bigcap_{i=1}^{n-k} \mathcal{X}_{w^{[i]}}^{B^{[i]}} = \phi,$$

which contradicts with Eq. (17). Thus, this case does not exist.

Case 2 $\left(\bigcap_{i=1}^{n-k} \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \bigcap \mathcal{H}_s \ne \phi, \forall s$: Clearly,

$$\left| \left(\bigcap_i \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \cap \mathcal{H}_s \right| \ge 1, \forall s \tag{18}$$

holds. By Eq. (17), we have

$$\begin{aligned} & \left| \left(\bigcap_i \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \cap \bigcup_{s \in \mathbb{F}_{q^m}^k} \mathcal{H}_s \right| \le q^{mk} \\ \Leftrightarrow & \left| \bigcup_{s \in \mathbb{F}_{q^m}^k} \left(\left(\bigcap_i \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \cap \mathcal{H}_s \right) \right| \le q^{mk} \\ \Leftrightarrow & \left| \left(\bigcap_i \mathcal{X}_{w^{[i]}}^{B^{[i]}} \right) \cap \mathcal{H}_s \right| = 1, \forall s. \end{aligned}$$

The last line yields from Eq. (18), $|\mathbb{F}_{q^m}^k| = q^{mk}$, and

$$\mathcal{H}_{s_1} \cap \mathcal{H}_{s_2} = \phi, \forall s_1, s_2 \in \mathbb{F}_{q^m}^k, s_1 \ne s_2.$$

Thus, the lemma holds for this case.

Case 3 Otherwise: There exist $s_1, s_2 \in \mathbb{F}_{q^m}^k$ and $1 \le l \le n - k$ that satisfy the following:

$$\begin{cases} \mathcal{X}_{w^{[l]}}^{B^{[l]}} \cap \mathcal{H}_{s_1} = \phi \\ \mathcal{X}_{w^{[l]}}^{B^{[l]}} \cap \mathcal{H}_{s_2} \ne \phi \end{cases} \Leftrightarrow \begin{cases} N_{s_1,w^{[l]}}^{B^{[l]}} = 0 \\ N_{s_2,w^{[l]}}^{B^{[l]}} \ne 0 \end{cases}.$$

However, $N_{s_1,w^{[l]}}^{B^{[l]}} \ne N_{s_2,w^{[l]}}^{B^{[l]}}$ contradicts with the assumption that universal m-strong security for $\mu = 1$ is satisfied. Thus, Case 3 does not exist.

We considered all three cases, which cover all possible cases and are disjoint, and conclude that the lemma holds since it holds for Case 2 which is the only existing case. □

Assume the existence of a secure network code that satisfies the universal m-strong security condition for some $1 \le \mu \le n - k$. Then this code must satisfy the security condition for $\mu = 1$ because in this case, the amount of information that can be wiretapped is obviously no more than the case for $1 \le \mu \le n - k$. Then by Lemma 3, this code satisfies the security condition for $\mu = n - k$, which contradicts with Theorem 1 stating that universal m-strong security for $\mu = n - k$ cannot be attained. Hence, we have the following result.

Theorem 2. *For any choice of parameters n, k, q, m, H*

and the basis for $\mathbb{F}_{q^m}$, *the universal secure network coding scheme cannot attain universal m-strong security for* $1 \leq \mu \leq n - k$.

4.3 Restricted Tapping Time

Now we consider the case when the tapping duration is generalized to $1 \leq m' \leq m$ in addition to the generalized μ considered in the previous part. Since the tapping duration is restricted, we do not restrict μ to $1 \leq \mu \leq n - k$, and assume $1 \leq \mu$ instead. This imposes an additional condition, $B_t = O, \forall t \in M$ for any choice of $M \subseteq \{1, 2, \cdots, m\}, |M| = m - m'$, on Definition 3. Note that the set M represents the set of time slot indices at which wiretapping does not occur. We are interested in, with which pairs of μ and m' the universal code becomes secure. From the discussions up to this point and the result of Silva et al., the following is clear:

- $\mu = 1$ and $1 \leq m' \leq n - k$: secure
- $1 \leq \mu \leq n$ and $m' = m$: insecure
- $1 \leq \mu \leq n - k$ and $m' = 1$: secure

Additionally, by the necessary and sufficient condition of universal m-strong security in Lemma 2 we have,

$$N_{s,w}^{\tilde{B}} = \frac{|\{x \in \mathbb{F}_{q^m}^n \mid w = \tilde{B}\bar{x}\}|}{q^{mk}}, \forall s$$

$$\Leftrightarrow N_{s,w}^{\tilde{B}} = \frac{q^{mn-m'\mu}}{q^{mk}}, \forall s \qquad (19)$$

Since the RHS takes a positive value, and by the definition of $N_{s,w}^{\tilde{B}}$ the LHS must be a non-negative integer, a necessary condition for satisfying Eq. (19), or the necessary condition for the code to be universal m-strongly secure, is as follows:

$$\frac{q^{mn-m'\mu}}{q^{mk}} \geq 1$$

$$\Leftrightarrow q^{mn-m'\mu} \geq q^{mk}$$

$$\Leftrightarrow m' \leq \frac{m(n-k)}{\mu}. \qquad (20)$$

For any fixed m', m, n, and k, Eq. (20) is unsatisfied for $\mu \geq m(n-k) + 1$ because of the restriction $m' \geq 1$. Note that being able to wiretap n arbitrary links allows the wiretapper to obtain the maximum amount of information that can possibly be wiretapped over the m' time slots, by continuously tapping the n links with GCVs that form a basis of $\mathbb{F}_q^n$. Thus, the amount of information obtained by the wiretapper with $\mu \geq n$ is at least as much as what is obtained by the wiretapper with $\mu \geq m(n-k) + 1$, which implies that the code is insecure with $\mu \geq n$. Thus, we have another necessary condition,

$$\mu \leq n - 1. \qquad (21)$$

Combining Eqs. (20) and (21) yields the necessary condition,

$$\mu \leq \min\left\{\frac{m}{m'}(n-k), n-1\right\}.$$

5. Conclusion

We proposed an eavesdropping model where the adversary is able to re-select the tapping wires at each time slot during the communication. We proved the impossibility of securing against this model using the universal secure network code proposed by Silva et al. for all choices of code parameters, even with a restricted number of tapped links. Moreover, we considered the case with shorter tapping duration, and derived a necessary condition for this code to be secure. The future tasks include improving this condition to a necessary and sufficient one.

Acknowledgment

References

[1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.
[2] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*, Foundations and Trends in Networking, vol. 2, No. 1, now Publishers Inc., 2007.
[3] N. Cai and R. W. Yeung, "Secure Network Coding," in *Proc. 2002 IEEE International Symposium on Information Theory(ISIT'02)*, p. 323, Jun. 2002.
[4] 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 Transaction on Information Theory*, vol. 52, pp. 4413–4430, Oct. 2006.
[5] D. Silva and F. R. Kschischang, "Universal Secure Network Coding via Rank-Metric Codes," arXiv:0809.3546v1 [cs.IT], Sep. 2008 (revised Apr. 2010).
[6] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inform. Transm*, vol. 21, no. 1, pp. 1–12, 1985.
[7] A. D. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, Oct. 1975.
[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] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2003.
[10] W. R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols*, Addison-Wesley, 1994.
[11] S. Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, vol.49, no.2, pp.371–381, Feb. 2003.
[12] K. Harada and H. Yamamoto, "Strongly Secure Linear Network Coding," *IEICE Trans. Fundamentals*, vol. E91-A, no. 10, pp. 2720-2728, Oct. 2008.