# Vulnerability of MRD-Code-Based Universal Secure Error-Correcting Network Codes under Time-Varying Jamming Links

Jun Kurihara*†
*KDDI R&D Laboratories, Inc.
2–1–15 Ohara, Fujimino,
Saitama, 356–8502 Japan.
Email: kurihara@kddilabs.jp

Tomohiko Uyematsu†
†Tokyo Institute of Technology
2–12–1 Ookayama, Meguro,
Tokyo, 152–8550 Japan.
Email: uyematsu@ieee.org

***Abstract*—In order to provide reliable and secure communication against eavesdroppers and jammers over networks, Universal Secure Error-Correcting Network Codes (USECNC) based on Maximum-Rank-Distance (MRD) codes have been introduced. This code can be applied to any underlying network codes. However, Shioji et al. introduced a reasonable network model against the code. In their model, an attacker eavesdrops information symbols from some links, where the set of eavesdropping links is re-selected during one packet transmission. The MRD-code-based USECNC cannot guarantee the security against eavesdroppers under this model. Inspired by Shioji et al.'s result, this paper considers the model such that the set of links that jamming (error) symbols are injected into is re-selected for each time slot. We show that the MRD-code-based USECNC cannot guarantee the error-correcting capability under the model of time-varying jamming links, even if the number of jamming links is limited to only one. Furthermore, by introducing a restriction on the field of local coding vectors in the network coding, we propose a simple solution to the problem of time-varying jamming links for MRD-code-based USECNC.**

***Keywords*-Network Coding; Secure Network Coding; Network Error-Correction; Jamming**

## I. Introduction

Network coding [1] has been attracting much attentions since it can achieve better performance than ordinary networks with routing methods in terms of throughput, energy consumption, etc [2][3].

In reality, network coding may suffer from two kinds of adversaries: eavesdropping and jamming. Silva et al.'s presented Universal Secure Error-Correcting Network Codes (USECNC) [4][5] based on Maximum-Rank-Distance (MRD) codes [6][7] to provide secure and reliable communication against eavesdroppers and jammers over the network. Their code can be applied to any underlying network codes and hence it is called 'universal'. In the construction of Silva et al.'s USECNC, packets are split into $m$ segments and transmitted to sink nodes through the network over $m$ time slots. It has been assumed that packets are tapped by eavesdroppers and corrupted by jammers on several links that are fixed during one transmission of packets, i.e. $m$ time slots.

Shioji et al. introduced the time-varying eavesdropping-link model in which attacker can re-select the set of eavesdropping links at each time slot of one packet transmission [8]. They showed that Silva et al.'s USECNC is insecure under this model, that is, information is leaked to eavesdroppers [8]. When the network coding is implemented on an overlay network of the Internet, the assumption of time-varying eavesdropping links is reasonable. Although a packet is not split from the perspective of the overlay network and they are transmitted through fixed 'logical' paths, a packet is split into multiple fragments and they are routed over different 'physical' paths at an intermediate router. Hence, from the point of view of the overlay network, the set of tapped logical links may be re-selected if physical links are eavesdropped. Such attackers against the network might be active, i.e. jammers who inject jamming packets into links to corrupt the network. Thus, this paper considers the model such that the attacker injects jamming (error) symbols into some links (called 'jamming links') in the network, and the set of jamming links is re-selected during one transmission of packets. We show that the MRD-code-based USECNC cannot guarantee the error-correcting capability under the model of time-varying jamming links, even if the number of jamming links is limited to only one. Furthermore, by introducing a restriction on the field of local coding vectors (LCV's) in the network coding, we propose a simple solution to the problem of time-varying jamming links for MRD-code-based USECNC.

The rest of this paper is organized as follows: Section II gives several definitions, the basic model of network coding and a brief review of MRD-code-based USECNC presented by Silva et al. In Section III, we introduce the time-varying jamming-link model, and show the vulnerability of MRD-code-based USECNC under this model. In Section IV, we propose a simple countermeasure against this model. Finally, we conclude this paper in Section V.

## II. Preliminaries

In this section, we give definitions about the representation of finite field extensions, the basic model of network coding

 ISBN: 978-1-61208-126-7

and a brief review of MRD-code-based USECNC presented by Silva et al.

### A. Field Extensions

Let $\mathbb{F}_q$ be a finite field containing $q$ elements, and let $\mathbb{F}_{q^m}$ be an $m$-degree field extension of a base field $\mathbb{F}_q$. Then, $\mathbb{F}_{q^m}$ can be viewed as a vector space over $\mathbb{F}_q$. When the basis of the space is fixed, i.e., an irreducible polynomial generating the field extension is determined, an element of $\mathbb{F}_{q^m}$ can be represented by an $m$-dimensional vector over $\mathbb{F}_q$. We suppose that the vector representation of $x \in \mathbb{F}_{q^m}$ is written by $[x^{(1)}, x^{(2)}, \ldots, x^{(m)}] \in \mathbb{F}_q^m$.

### B. Network Coding

Let $\mathcal{G} = (\mathcal{E}, \mathcal{V})$ be a delay-free acyclic directed network, where $\mathcal{E}$ and $\mathcal{V}$ denote a set of links (edge, channel) and a set of nodes, respectively. Let $s \in \mathcal{V}$ and $\mathcal{R} \subset \mathcal{V}$ respectively denote a source node and a set of sink nodes, where $s \notin \mathcal{R}$. In this network model, we suppose that each link can carry an element of $\mathbb{F}_q$ per one time slot. The source node wishes to multicast the sequence $\vec{x} = [x_1, x_2, \ldots, x_n]^{\mathrm{T}} \in \mathbb{F}_q^n$ to all sink nodes at rate $n$, where the rate is defined as the number of elements in $\mathbb{F}_q$ transmitted from $s$ per one time slot. Suppose that

$$n \leq \min\{\mathsf{maxflow}(s, r) \ : \ r \in \mathcal{R}\}$$

holds, where $\mathsf{maxflow}(s, r)$ $(i, j \in \mathcal{V})$ denotes the max-flow from $i$ to $j$. Then, there exists a network coding method in which $s$ can multicast $\vec{x}$ to all nodes in $\mathcal{R}$ at rate equal to $n$ [1].

We assume that linear network coding [9] is employed over $\mathcal{G}$, i.e., the type of data processing performed on the packets at each node is limited to linear combination. This implies that the data flow on any link over $\mathcal{G}$ can be represented as an $\mathbb{F}_q$-linear combination of the sequence $x_1, x_2, \ldots, x_n$. Thus, the information flow on link $e \in \mathcal{E}$ can be denoted as $y_e = \vec{b_e}^{\mathrm{T}} \cdot \vec{x}$ using a global coding vector (GCV), $\vec{b_e} = [b_1, b_2, \ldots, b_n]^{\mathrm{T}} \in \mathbb{F}_q^n$. When one has access to, say, $l$ links $e_1, e_2, \ldots, e_l$, then the information obtained from these links is denoted as $M\vec{x} \in \mathbb{F}_q^l$, where $M = [\vec{b}_{e_1}, \vec{b}_{e_2}, \ldots, \vec{b}_{e_n}]^{\mathrm{T}}$. Constructing a network code is equivalent to determining the GCV of each link by setting the coefficients of the linear combination performed at each node.

### C. The MRD-Code-Based USECNC

Here we introduce the fixed jamming-link model and the construction of Silva et al's USECNC employed over this model [4][5].

*1) Fixed Jamming-Link Model:* Suppose that one packet is composed of an element of $\mathbb{F}_{q^m}$ that is an $m$-degree field extension of $\mathbb{F}_q$, and is represented by an $m$-dimensional vector over $\mathbb{F}_q$. We define $n$ packets transmitted from the source node $s$ by $X = [X_1, X_2, \ldots, X_n]^{\mathrm{T}} \in \mathbb{F}_{q^m}^n (= \mathbb{F}_q^{n \times m})$. Then, the duration of one transmission of $X$ is composed of $m$ time slots. The source node $s$ splits $X$ and sends them over $m$ time slots using a linear network code though $\mathcal{G}$, i.e., transmits $[X_1^{(i)}, X_2^{(i)}, \ldots, X_n^{(i)}]^{\mathrm{T}} \in \mathbb{F}_q^n$ at each time slot $i = 1, \ldots, m$.

Here we suppose that there exist $t (< n)$ jamming links in $\mathcal{E}$ and they inject error packets into $\mathcal{G}$. Silva et al. [4][5] assumed that these links are fixed during one transmission, i.e., $m$ time slots. At a specific sink node, the received packets though $\mathcal{G}$ with injection of jamming (error) packets is represented by

$$Y = AX + DZ \in \mathbb{F}_q^{n \times m}, \tag{1}$$

where $A \in \mathbb{F}_q^{n \times n}$ is a transition matrix corresponding to GCV's. A linear network code employed over $\mathcal{G}$ is called feasible [10] if $\mathsf{rank}\ A = n$ for all sink nodes, otherwise it is rank-deficient. The rank deficiency is defined as $\rho = n - \mathsf{rank}\ A$. On the other hand, $Z \in \mathbb{F}_q^{t \times m}$ denotes $t$ jamming (error) packets. $D \in \mathbb{F}_q^{n \times t}$ is a transition matrix corresponding to jamming links. $D$ and $Z$ are unknown random variables with unknown distributions. Then $\mathsf{rank}\ D \leq t$ holds since $t < n$ must hold.

Throughout this paper, we focus our attention only on injection of jamming packets, and omit eavesdropping on links (cf., Shioji et al.'s analysis in [8]).

*2) Silva et al.'s Scheme:* For the construction against the jamming(error)-packet injection, Silva et al.'s Universal Secure Error-Correcting Network Codes (USECNC) [4][5] is equivalent to $[n, k]$ Maximum Rank Distance (MRD) code $\mathcal{C} \subset \mathbb{F}_q^{n \times m}$ satisfying $m \geq n$ and $0 < k \leq n - 2t - \rho$, where $\rho$ $(= n - \mathsf{rank}\ A)$ is the rank deficiency of $A$. Namely, the transmitted packet $X$ in Eq.(1) is a codeword of $\mathcal{C}$. MRD code is a class of linear codes over $\mathbb{F}_{q^m}$, which is optimal in the rank-distance sense. For the $[n, k]$ MRD code $\mathcal{C}$, we have $d_R(C) \geq 2t + \rho + 1$, where $d_R(C)$ denotes the minimum rank-distance [6][7] between all pairs of distinct codewords of $\mathcal{C}$. We also have

$$\begin{aligned} d_R(AX, Y) &= \mathsf{rank}\ (Y - AX) \\ &= \mathsf{rank}\ DZ \\ &\leq \mathsf{rank}\ Z \\ &\leq t, \end{aligned} \tag{2}$$

where $d_R(P, Q)$ denotes the rank-distance between matrices $P, Q \in \mathbb{F}_q^{n \times m}$. Hence, the minimum rank-distance decoder of $\mathcal{C}$ can correct $t$ jamming packets (and $\rho$ rank deficiency of $A$) under the fixed jamming-link model $(n - k \geq 2t + \rho)$ [10].

## III. Time-Varying Jamming Links over the Network

In this section, we introduce the model of time-varying jamming links, and show that MRD-code-based USECNC cannot guarantee the error-correcting capability under this model.

 ISBN: 978-1-61208-126-7

### A. The Model

Suppose that the source node $s$ multicast $n$ packets, i.e., $n$ vectors in $\mathbb{F}_q^m$, over time slots $i = 1, 2, \ldots, m$. We consider a model such that the jammer(s) can re-select the set of $t$ jamming links at each time slot $i$.

Denote the $t$ error packets injected into $\mathcal{G}$ by a $t \times m$ matrix

$$Z = [\vec{z}_1, \vec{z}_2, \ldots, \vec{z}_m] \in \mathbb{F}_q^{t \times m},$$

where $\vec{z}_i \in \mathbb{F}_q^t$ $(i = 1, 2, \ldots, m)$ is a $t$-dimensional column vector chosen according to arbitrary distribution. At a specific sink node, let $D_i \in \mathbb{F}_q^{n \times t}$ $(i = 1, 2, \ldots, m)$ be a $n \times t$ matrix representing the linear combination of jamming-packet segments at time $i$. Jammer(s) specify the set of jamming-links arbitrarily, and hence we assume that $D_i$ is chosen arbitrarily by jammer(s). The received matrix $Y \in \mathbb{F}_q^{n \times m}$ at the specific sink node is written as

$$Y = AX + V \in \mathbb{F}_q^{n \times m}, \tag{3}$$

where the matrix $V$ denotes jamming packets conveyed over the time-varying jamming links, given by

$$V = [D_1\vec{z}_1, D_2\vec{z}_2, \ldots, D_m\vec{z}_m] \in \mathbb{F}_q^{n \times m}.$$

When $D_1 = D_2 = \cdots = D_m$, Eq.(3) is equivalent to Silva et al.'s fixed jamming-link model [4][5].

### B. MRD-Code-Based USECNC under the Time-Varying Jamming Link Model

On the time-varying jamming-link model presented in the previous subsection, we first have the following lemma.

**Lemma 1.** *Suppose that the jammer(s) can arbitrarily select non-zero matrices $D_1, D_2, \ldots, D_m$ from $\mathbb{F}_q^{n \times t}$ and can generate non-zero vectors $\vec{z}_1, \vec{z}_2, \ldots, \vec{z}_m \in \mathbb{F}_q^t$. Then the maximum possible rank of $V$ is $n$.*

*Proof:* It is only necessary to show an example having $\mathsf{rank}\ V = n$. Choose $D_i$ for $i = 1, 2, \ldots, n$ $(n \leq m)$ as follows:

$$\begin{aligned} D_1 &= \left[\vec{u}_1, \vec{0}, \ldots, \vec{0}\right], \\ D_2 &= \left[\vec{u}_2, \vec{0}, \ldots, \vec{0}\right], \\ &\vdots \\ D_n &= \left[\vec{u}_n, \vec{0}, \ldots, \vec{0}\right], \end{aligned}$$

where $\vec{u}_j$ denotes the $j$-th column vector of an $n \times n$ identity matrix and $\vec{0}$ is a column zero vector. Let $\vec{z}_i$ be represented as $\vec{z}_i = [z_i^{(1)}, 0, \ldots, 0]^{\mathrm{T}} \in \mathbb{F}_q^t$. We assume that $z_i^{(1)}$ is chosen from $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ for $i = 1, \ldots, n$. Then, we denote $V$ by

$$\begin{aligned} V &= [D_1\vec{z}_1, D_2\vec{z}_2, \ldots, D_n\vec{z}_n \mid D_{n+1}\vec{z}_{n+1}, \ldots, D_{m+1}\vec{z}_{m+1}] \\ &= [V_1 \mid V_2], \end{aligned}$$

where $V_1$ can be represented as

$$\begin{aligned} V_1 &= [D_1\vec{z}_1, D_2\vec{z}_2, \ldots, D_n\vec{z}_n] \\ &= \begin{bmatrix} z_1^{(1)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & z_n^{(1)} \end{bmatrix}. \end{aligned}$$

We thus have $\mathsf{rank}\ V_1 = n$ and hence $\mathsf{rank}\ V = n$ holds. This completes the lemma. ■

Denote $\mathsf{rank}\ V = v$. We then have $v \leq n$ from Lemma 1. Let $X$ in Eq.(3) be a codeword of Silva et al.'s USECNC, that is, $[n, k]$ MRD code $\mathcal{C}$ with $m \geq n$ and $0 < k \leq n - 2t - \rho$. From Lemma 1, jammers may select $D_i$ and $\vec{z}_i$ to satisfy $v > t$ even if $\mathsf{rank}\ D_i \leq t$ holds for all $i = 1, \ldots, m$. We then have

$$\begin{aligned} t < v &= \mathsf{rank}\ V \\ &= \mathsf{rank}\ (Y - AX) \\ &= d_R(Y, AX). \end{aligned}$$

Thus, the decoder of $\mathcal{C}$ cannot correct $t$ jamming (error) packets under the time-varying jamming-link model.

Moreover, we give the following lemma that shows the number of jamming packets is independent of $\mathsf{rank}\ V$.

**Lemma 2.** *Suppose that jammer(s) can arbitrarily choose $D_i$'s in Eq.(3) from $\mathbb{F}_q^{n \times t}$. Then, the maximum possible rank of $V$ is $n$, which is independent of the value $t > 0$.*

*Proof:* Since the supposition $m \geq n$ is required in Silva et al.'s USECNC, the example presented in the proof of Lemma 1 always satisfy $\mathsf{rank}\ V = n$. Moreover, in the example in the proof of Lemma 1, we have assumed $\mathsf{rank}\ D_i = 1$ for $i = 1, 2, \ldots, n$ independently from the value $t > 0$. Thus the lemma is completed. ■

The above analysis proves the following result.

**Theorem 1.** *Suppose that there are $t'$ jamming links in $\mathcal{E}$ under the time-varying jamming-link model. Let the transmitted packet over the network is a codeword of Silva et al.'s USECNC, i.e., $[n, k]$ MRD code $\mathcal{C}$ with $0 < k \leq n - 2t - \rho$ and $m \geq n$. Then, for any $t' > 0$, the decoder of $\mathcal{C}$ cannot correct $t'$ jamming (error) packets injected from time-varying jamming links.*

This theorem implies that, under the time-varying jamming-link model, Silva et al.'s USECNC cannot guarantee the error-correction capability even if $t' = 1$.

### C. An Example

Assume $q = 2$, $m = n = 3$ and $t = 1$. We do not consider the rank deficiency and the existence of eavesdroppers, and set $\rho = \mu = 0$. From these parameters, the USECNC is defined as a $[3, 1]$ MRD code $\mathcal{C} \subset \mathbb{F}_2^{3 \times 3}$. A codeword of $\mathcal{C}$ is defined as a $3 \times 3$ matrix $X = [X_1, X_2, X_3]^{\mathrm{T}} \in \mathcal{C}$, where $X_i \in \mathbb{F}_2^3$.

 ISBN: 978-1-61208-126-7

Under the time-varying jamming-link model, a specific sink node receives the following packet.

$$\begin{aligned} Y &= AX + V \\ &= A \begin{bmatrix} X_1 \\ X_2 \\ X_3 \end{bmatrix} + [D_1\vec{z}_1, D_2\vec{z}_2, D_3\vec{z}_3], \end{aligned}$$

where $A \in \mathbb{F}_2^{3\times 3}$, $D_i \in \mathbb{F}_2^{3\times 1}$ and $\vec{z}_i \in \mathbb{F}_2^1$ for $i = 1, 2, 3$. Here we assume $\mathsf{rank}\ A = 3$ and $\mathsf{rank}\ D_i \leq t = 1$ for $i = 1, 2, 3$. For example, we suppose $A$ is a $3 \times 3$ identity matrix $I$ and $D_i$'s are

$$\begin{aligned} D_1 &= [1, 0, 0]^{\mathrm{T}}, \\ D_2 &= [0, 1, 0]^{\mathrm{T}}, \\ D_3 &= [0, 0, 1]^{\mathrm{T}}. \end{aligned}$$

We note that $\mathsf{rank}\ D_i = t = 1$ for each of $i = 1, 2, 3$ similar to the fixed jamming-link model. We also represent $X_i = [X_i^{(1)}, X_i^{(2)}, X_i^{(3)}] \in \mathbb{F}_2^3$ and $\vec{z}_i = [z_i] \in \mathbb{F}_2^1$ for $i = 1, 2, 3$. We then receive

$$Y = \begin{bmatrix} X_1^{(1)} & X_1^{(2)} & X_1^{(3)} \\ X_2^{(1)} & X_2^{(2)} & X_2^{(3)} \\ X_3^{(1)} & X_3^{(2)} & X_3^{(3)} \end{bmatrix} + \begin{bmatrix} z_1 & 0 & 0 \\ 0 & z_2 & 0 \\ 0 & 0 & z_3 \end{bmatrix}.$$

In this case, we have $\mathsf{rank}\ V = 3$ if all $z_1, z_2, z_3$ are nonzero and hence $X$ cannot be uniquely reconstructed. This can be viewed as the worst case of Silva et al.'s USECNC under the fixed jamming-link model, that is, $3(> t)$ error packets are injected into the network.

## IV. A Simple Way to Prevent the Jammers

The simplest way to prevent time-varying jamming links is to construct the network in which no packet is split into segments. Namely, packets are transmitted not as $m$-dimensional vectors using $m$ time slots but as elements of an $m$-degree field extension itself at one time slot in Silva et al.'s USECNC. We thus consider how to transmit codewords of $[n, k]$ MRD code at one time slot over a linear network code and how to decode the received codeword by the minimum rank-distance decoder.

Let $p$ be a prime and the number of elements in a base field $\mathbb{F}_p$. And let $p^m (\sim q)$ be the number of elements in an extended field $\mathbb{F}_{p^m}$. We redefine that each link can carry an element of $\mathbb{F}_{p^m}$ per one time slot. The source node $s$ wishes to transmit $\vec{x} = [x_1, x_2, \ldots, x_n]^{\mathrm{T}} \in \mathbb{F}_{p^m}^n$ to all sink nodes in $\mathcal{R}$ at one time slot using a linear network code. Then, the received packet at a specific sink node is represented as

$$\begin{aligned} \vec{y} &= [y_1, y_2, \ldots, y_n]^{\mathrm{T}} \\ &= A\vec{x} + D\vec{z} \in \mathbb{F}_{p^m}^n, \end{aligned} \tag{4}$$

where $A \in \mathbb{F}_{p^m}^{n\times n}$ is a transition matrix according to a linear network code over $\mathbb{F}_{p^m}$. $\vec{z} \in \mathbb{F}_{p^m}^t$ denotes $t$ jamming packets and $D \in \mathbb{F}_{p^m}^{t\times t}$ is a transition matrix corresponding to jamming links.

Assume $\vec{x} \in \mathbb{F}_{p^m}^n (= \mathbb{F}_p^{n\times m})$ in Eq.(4) is a codeword of $[n, k]$ MRD code defined over $\mathbb{F}_{p^m}$, where $m \geq n$ and $0 < k \leq n - 2t + \rho$. Let $\mathcal{M}(\cdot)$ denote the matrix representation of a vector in $\mathbb{F}_{p^m}^n$ to measure the rank distance between vectors. For example, the matrix representation of $\vec{x}$ is

$$\mathcal{M}(\vec{x}) = \begin{bmatrix} x_1^{(1)} & x_1^{(2)} & \cdots & x_1^{(m)} \\ x_2^{(1)} & x_2^{(2)} & \cdots & x_2^{(m)} \\ \vdots & \vdots & \ddots & \vdots \\ x_n^{(1)} & x_n^{(2)} & \cdots & x_n^{(m)} \end{bmatrix} \in \mathbb{F}_p^{n\times m},$$

where $[x_i^{(1)}, x_i^{(2)}, \ldots, x_i^{(m)}] \in \mathbb{F}_p^m$ is the vector representation of $x_i \in \mathbb{F}_{p^m}$ $(i = 1, \ldots, n)$. Then, according to Eq.(4), we have

$$\begin{aligned} d_R(\mathcal{M}(A\vec{x}), \mathcal{M}(\vec{y})) &= \mathsf{rank}\ (\mathcal{M}(\vec{y}) - \mathcal{M}(A\vec{x})) \\ &= \mathsf{rank}\ (\mathcal{M}(\vec{y} - A\vec{x})) \\ &= \mathsf{rank}\ \mathcal{M}(D\vec{z}), \end{aligned} \tag{5}$$

from the properties of the additive operation over a field extension $\mathbb{F}_{p^m}$. However, unlike Eq.(2), $\mathsf{rank}\ \mathcal{M}(D\vec{z}) \leq t$ does not always hold from the property of the multiplicative operation over $\mathbb{F}_{p^m}$. Hence, the minimum rank-distance decoder of the $[n, k]$ MRD code cannot be simply applied to Eq.(4). Hence, we add the following condition to the construction of the underlying network coding such that $\mathsf{rank}\ \mathcal{M}(D\vec{z}) \leq t$ always holds.

**Condition 1.** *For all nodes, elements of local coding vectors (LCV's) are chosen from the subfield (base field) $\mathbb{F}_p$ of the field extension $\mathbb{F}_{p^m}$.*

Note that elements of LCV's are coefficients of linear combination of incoming symbols at each node and they define elements of GCV's [2]. Thus, this condition also yields that the transition matrices $A$ and $D$ are defined over the subfield, i.e., $A \in \mathbb{F}_p^{n\times n} \subset \mathbb{F}_{p^m}^{n\times n}$ and $D \in \mathbb{F}_p^{t\times t} \subset \mathbb{F}_{p^m}^{t\times t}$.

For any $a \in \mathbb{F}_p$ and $b \in \mathbb{F}_{p^m}$, their vector representations are $[0, \ldots, 0, a] \in \mathbb{F}_p^m$ and $[b^{(1)}, b^{(2)}, \ldots, b^{(m)}] \in \mathbb{F}_p^m$, respectively. Then, the multiplication $ab$ over $\mathbb{F}_{p^m}$ is given by

$$ab := [ab^{(1)}, ab^{(2)}, \ldots, ab^{(m)}],$$

from the fact of finite fields. That is, all operations can be executed over the base field $\mathbb{F}_p$. Thus, under Condition 1,

 ISBN: 978-1-61208-126-7

we have

$$\begin{aligned}
\mathcal{M}(D\vec{z}) &= \mathcal{M}\left(\begin{bmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,t} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ d_{t,1} & d_{t,2} & \cdots & d_{t,t} \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_t \end{bmatrix}\right) \\
&= \mathcal{M}\left(\begin{bmatrix} \sum_{w=1}^{t} d_{1,w} z_w \\ \sum_{w=1}^{t} d_{2,w} z_w \\ \vdots \\ \sum_{w=1}^{t} d_{t,w} z_w \end{bmatrix}\right) \\
&= \begin{bmatrix} \sum_{w=1}^{t} [d_{1,w} z_w^{(1)}, d_{1,w} z_w^{(2)}, \ldots, d_{1,w} z_w^{(m)}] \\ \sum_{w=1}^{t} [d_{2,w} z_w^{(1)}, d_{2,w} z_w^{(2)}, \ldots, d_{2,w} z_w^{(m)}] \\ \vdots \\ \sum_{w=1}^{t} [d_{t,w} z_w^{(1)}, d_{t,w} z_w^{(2)}, \ldots, d_{t,w} z_w^{(m)}] \end{bmatrix} \\
&= D \begin{bmatrix} z_1^{(1)} & \cdots & z_1^{(m)} \\ \vdots & \ddots & \vdots \\ z_t^{(1)} & \cdots & z_t^{(m)} \end{bmatrix} \\
&= D\mathcal{M}(\vec{z}),
\end{aligned}$$

where $d_{u,v} \in \mathbb{F}_p$ $(u, v = 1, \ldots, t)$ and $[z_w^{(1)}, z_w^{(2)}, \ldots, z_w^{(m)}] \in \mathbb{F}_p^m$ is the vector representation of $z_w \in \mathbb{F}_{p^m}$ $(w = 1, \ldots, t)$. Since $\mathsf{rank}\ \mathcal{M}(\vec{z}) \leq t$, we have

$$\mathsf{rank}\ \mathcal{M}(D\vec{z}) = \mathsf{rank}\ D\mathcal{M}(\vec{Z}) \leq t.$$

Combining Eq.(5) and this, the minimum rank-distance decoder of the $[n, k]$ MRD code can decode the received packets $\vec{y}$ as with the Silva et al.'s USECNC for the fixed jamming-link model.

However, this solution contains the following problems; a) The scheme is not universal since the condition of LCV's is introduced. b) Since the field for LCV's is changed from $\mathbb{F}_q$ to $\mathbb{F}_p$ with $p < q$, the probability of rank deficiency becomes high when random network coding [11] is employed, or the size of $\mathbb{F}_p$ might be insufficient for the deterministic construction of network coding depending on the network structure [12]. We believe the completely different technique from MRD codes must be required to realize universal secure error-correcting codes against the time-varying jamming links.

## V. Conclusion

This paper considered the reasonable network model such that the set of links that jamming (error) symbols are injected into is re-selected for each time slot. We revealed that the MRD-code-based USECNC cannot guarantee the error-correcting capability under the model of time-varying jamming links, even if the number of jamming links is limited to only one. Further, by introducing a severe restriction to the field of LCV's, we presented a simple way to avoid jamming with the time-varying jamming links for MRD-code-based USECNC.

## References


[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[2] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*. Now Publishers, 2007.

[3] C. Fragouli and E. Soljanin, *Network Coding Applications*. Now Publishers, 2007.

[4] D. Silva and F. R. Kschischang, "Universal secure error-correcting schemes for network coding." arXiv:1001.3387v1, Jan. 2010. Appeared in IEEE International Symposium on Information Theory (ISIT) 2010. Available at http://arxiv.org/abs/1001.3387v1.

[5] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes." arXiv:0809.3546v2, Apr. 2010. Available at http://arxiv.org/abs/0809.3546v2.

[6] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, no. 1, pp. 1–12, 1985.

[7] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[8] E. Shioji, R. Matsumoto, and T. Uyematsu, "Vulnerability of MRD-code-based universal secure network coding against stronger eavesdroppers," *IEICE Transactions on Fundamentals*, vol. E93-A, no. 11, pp. 2026–2033, 2010.

[9] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003.

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

[11] 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 Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[12] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, 2005.


 ISBN: 978-1-61208-126-7