Encoding of Network Protection Codes Against Link and Node Failures Over Finite Fields

Salah A. Aly and Ahmed E. Kamal
Department of Electrical and Computer Engineering
Iowa State University, Ames, IA 50011, USA
Email: {salah,kamal}@iastate.edu

Abstract—Link and node failures are common two fundamental problems that affect operational networks. Hence, protection of communication networks is essential to increase their reliability, performance, and operations. Much research work has been done to protect against link and node failures, and to provide reliable solutions based on pre-defined provision or dynamic restoration of the domain. In this paper we develop network protection strategies against multiple link failures using network coding and joint capacities. In these strategies, the source nodes apply network coding for their transmitted data to provide backup copies for recovery at the receivers’ nodes. Such techniques can be applied to optical, IP, and mesh networks. The encoding operations of protection codes are defined over finite fields. Furthermore, the normalized capacity of the communication network is given by \((n - t)/n\) in case of \(t\) link failures. In addition, a bound on the minimum required field size is derived.

I. INTRODUCTION

With the increase in the capacity of backbone networks, the failure of a single link or node can result in the loss of enormous amounts of information, which may lead to catastrophes, or at least loss of revenue. Network connections are therefore provisioned with the property that they can survive such failures, and hence several techniques have been introduced in the literature. Such techniques either add extra resources, or reserve some of the available network resources as backup circuits, just for the sake of recovery from failures. Recovery from failures is also required to be agile in order to minimize the network outage time. This recovery usually involves two steps: fault diagnosis and location, and rerouting connections. Hence, the optimal network survivability problem is a multi-objective problem in terms of resource efficiency, operation cost, and agility [9].

In network survivability, the four different types of failures that might affect network operations are [7], [10]: 1) link failure, 2) node failure, 3) shared risk link group (SRLG) failure, and 4) network control system failure. Henceforth, one needs to design network protection strategies against these types of failures. Although the common frequent failures are link failures, node failures sometimes happen due to burned switch/router, fire, or any other hardware damage. In addition, the failure might be due to network maintenance.

Network coding allows the intermediate nodes not only to forward packets using network scheduling algorithms, but also encode/decode them using algebraic primitive operations, see [1], [3], [4], [8] and the references therein. As an application of network coding, data loss because of failures in communication links can be detected and recovered if the sources are allowed to perform network coding operations.

Recently, network protection strategies against multiple link failures using network coding and reduced capacities are proposed in [2], [5]. In this paper, we provide a new technique for protecting network failures using protection codes and reduced capacity in which the encoding operations are defined over finite fields. This technique can be deployed at an overlay layer in optical mesh networks, in which detecting failure is an essential task. The benefits of this approach are that:

i) It allows receivers to recover the lost data without contacting a third parity or main domain server.

ii) It has less computational complexity and does not require adding extra paths.

iii) All \(n\) disjoint paths have full capacity except at \(t\) paths in case of protecting against \(t\) link failures.

This paper is organized as follows. In Sections II and III we present the network model and problem definition. In Section IV we provide network protections against \(t\) link failures. We present differentiated distributed capacities in Section V and demonstrate analysis of protection codes in Section VII. Finally, Bounds on the finite field size is proved in Section VI and the paper is concluded in Section VIII.

II. NETWORK MODEL AND ASSUMPTIONS

In this section we introduce the network model and provide the needed assumptions. The main hypothesis of this network model can be stated as follows.

i) Let \(\mathcal{N}\) be a network represented by an abstract graph \(G = (\mathcal{V}, \mathcal{E})\), where \(\mathcal{V}\) is the set of nodes and \(\mathcal{E}\) be set of undirected edges. Let \(\mathcal{S}\) and \(\mathcal{R}\) are sets of independent sources and destinations, respectively. The set \(\mathcal{V} = \mathcal{V} \cup \mathcal{S} \cup \mathcal{R}\) contains the relay nodes, sources, and destinations. Assume for simplicity that \(|\mathcal{S}| = |\mathcal{R}| = n\), hence the set of sources is equal to the set of receivers.

ii) The node can be a router, switch, or an end terminal depending on the network model \(\mathcal{N}\) and the transmission layer.

iii) \(L\) is a set of links \(L = \{L_1, L_2, \ldots, L_n\}\) carrying the data from the sources to the receivers as shown in Fig. I. All connections have the same bandwidth, otherwise a connection with high bandwidth can be divided into multiple
connections, each of which has a unit capacity. There are exactly \( n \) connections. For simplicity, we assume that the number of sources is less than or equal to the number of links. A sender with a high capacity can divide its capacity into multiple unit capacity, each of which has its own link. Put differently,

\[
\{(s_i, w_{1i}), (w_{1i}, w_{2i}), \ldots, (w_{\lambda i}), r_i)\},
\]

where \( 1 \leq i \leq n \) and \((w_{(j-1)i}, w_{ji}) \in E \), for some integer \( \lambda \geq 1 \). Hence we have \(|S| = |R| = |L| = n\). The \( n \) connection paths are pairwise link disjoint.

iv) The data from all sources are sent in cycles. Each cycle has a number of time slots \( n \). Hence \( t_j^i \) is a value at round time slot \( j \) in cycle \( \delta \).

v) The failure on a link \( L_i \) may happen due to the network circumstance such as a link replacement, overhead, etc. We assume that the receiver is able to detect a failure and our protection strategy is able to recover it.

vi) In this model \( \mathcal{N} \), consider only a single link failure, it is sufficient to apply the encoding and decoding operation over a finite field with two elements, we denote it \( F_2 = \{0, 1\} \).

### III. Problem Setup and Terminology

We assume that there is a set of \( n \) connections that need to be protected with \%100 guaranteed against single and multiple link failures. We assume that all connections have the same bandwidth, and each link (one hop or circuit) has the same bandwidth as a path.

Every sender \( s_i \) prepares a packet \( \text{packet}_{s_i \rightarrow r_j} \) to send to a receiver \( r_j \). The packet contains the sender’s ID, data \( x_i^j \), and a round time for every cycle \( t_\ell^i \) for some integers \( \delta \) and \( \ell \). There are two types of packets:

i) **Plain Packets**: Packets sent without coding, in which the sender does not need to perform any coding operations. For example, in case of packets sent without coding, the sender \( s_i \) sends the following packet to the receiver \( r_j \).

\[
\text{packet}_{s_i \rightarrow r_j} := (ID_{s_i}, x_i^j, t_\ell^i) \tag{2}
\]

ii) **Encoding Packets**: Packets sent with encoded data, in which the sender \( s_j \) sends other sender’s data. In this case, the sender \( s_j \) sends the following packet to receiver \( r_j \):

\[
\text{packet}_{s_j \rightarrow r_j} := (ID_{s_j}, \sum_{i=1}^{n} \alpha_i x_i^\ell, t_\ell^j),
\]

where \( \alpha_i \in F_q \).

In either case the sender has a full capacity in the connection link \( L_i \).

**Definition 1**: The capacity of a connecting link \( L_i \) between \( s_i \) and \( r_i \) is defined by

\[
c_i = \begin{cases} 
1, & L_i \text{ has active signals;} \\
0, & \text{otherwise.}
\end{cases}
\]

And the total capacity is given by the summation of all link capacities. What we mean by an active link is that the receiver is able to receive un-encoded signals/messages throughout this link and process them.

Clearly, if all links are active then the total capacity is \( n \) and normalized capacity is 1. In general the normalized capacity of the network for the active and failed links is computed by

\[
C_N = \frac{1}{n} \sum_{i=1}^{n} c_i.
\]

The following definition describes the **working and protection** paths between two network switches as shown in Fig. [1]

**Definition 2**: The **working paths** on a network with \( n \) connection paths carry un-encoded traffic under normal operations. The **Protection paths** provide an alternate backup path to carry encoded traffic. A protection scheme ensures that data sent from the sources will reach the receivers in case of failure incidences on the working paths.

### IV. NPS-T: Protecting Against t Path Failures

In this section we present a network protection strategy against \( t \) failures in optical networks. Assume the same notations as shown in the previous sections hold. Assume also that the total number of failures are \( t \) and they happen at arbitrary \( t \) links.

Let \( m = \lceil n/t \rceil \), hence we have \( m \) rounds per cycle. The encoding operations of NPS-T against \( t \) failures are shown in Scheme (6). We can see that \( y_t \) in general is given by

\[
y_t = \sum_{i=1}^{(j-1)\ell} a_i x_i^j - 1 + \sum_{i=j\ell+1}^{n} a_i x_i^j
\]

for \( (j-1)\ell + 1 \leq \ell \leq j\ell, 1 \leq j \leq n \). \tag{7}

The advantages of NPS-T approach is that

- The data is encoded and decoded online, and it will be sent and received in different rounds. Once the receivers detect failures, they are able to obtain a copy of the lost data immediately without delay by querying the neighboring nodes with unbroken working paths.
- The recovery is assured with \%100. Since \( t \) paths will carry encoded data, up to \( t \) failures can be recovered.
Using this strategy, no extra paths are needed. This will make this approach more suitable for applications, in which adding extra paths is not allowed.

- Since in real case scenarios, the number of failures is very small in comparison to the number of working paths, the NPS-T performs well.
- The encoding operations are linear, and the coefficients of the variables $x_i^j$ are taken from a finite field with $q \geq n - t + 1$ elements.

**Theorem 3:** Let $n$ be the total number of connections from sources to receivers. The capacity of NPS-T strategy shown in Scheme 6 against $t$ path failures is given by

$$C_N = (n - t)/(n)$$  

**Lemma 4:** The encoding Scheme 6 is optimal in terms of max capacity.

One cannot find a better encoding scheme against $t$ link failures rather than providing one protection path against one failure. Indeed $t$ protection paths are used to protect $t$ link failures and this is shown in Scheme (6).

### A. Encoding Operations

Assume that each connection path $L_i$ (L) has a unit capacity from a source $s_i$ (S) to a receiver $r_i$ (R). The data sent from the sources S to the receivers R is transmitted in rounds. Under NPS-T, in every round $n - t$ paths are used to carry new data ($x_i^j$), and $t$ paths are used to carry protected data units, $y_1, y_2, \ldots, y_t$, and in the second round, the next $t$ sources transmit $y_{t+1}, y_{t+2}, \ldots, y_{2t}$, and so on. All sources S and receivers R must keep track of the round numbers. Let $ID_{s_i}$ and $x_{s_i}$ be the ID and data initiated by the source $s_i$. Assume the round time $j$ in cycle $\delta$ is given by $t_{\delta}^{j}$. Then the source $s_i$ will send $packet_{s_i}$ on the working path which includes

$$Packet_{s_i} = (ID_{s_i}, x_{i}^{\ell}, t_{\delta}^{j})$$

Also, the source $s_j$, that transmits on a protection path, will send a packet $packet_{s_j}$:

$$Packet_{s_j} = (ID_{s_j}, y_{j}, t_{\delta}^{j})$$

where $y_k$ is defined in (7). Hence the protection paths are used to protect the data transmitted in round $\ell$, which are included in the $x_{i}^{j}$ data units. So, we have a system of $t$ independent equations at each round time that will be used to recover at most $t$ unknown variables.

The strategy NPS-T is a generalization of protecting against a single path failure shown in the previous section in which $t$ protection paths are used instead of one protection path in case of one failure. We also notice that most of the network operations suffer from one and two path failures [7], [10].

### B. Proper Coefficients Selection

One way to select the coefficients $a_{i}^{\ell}$’s in each round such that we have a system of $t$ linearly independent equations is by using the matrix $H$ shown in (11). Let $q$ be the order of a finite field, and $\alpha$ be the root of unity. Then we can use this
matrix to define the coefficients of the senders as:

\[
H = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\
1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{t-1} & \alpha^{2(t-1)} & \cdots & \alpha^{(t-1)(n-1)}
\end{bmatrix}.
\] (11)

We have the following assumptions about the encoding operations.

1) Clearly if we have one failure \( t = 1 \), then all coefficients will be one. The first sender will always choose the unit value.

2) If we assume \( t \) failures, then the \( y_1, y_2, \ldots, y_t \) equations are written as:

\[
y_1 = \sum_{i=t+1}^{n} x_i^1, \quad y_2 = \sum_{i=t+1}^{n} \alpha^{(i-1)} x_i^2, \quad \cdots \quad y_t = \sum_{i=t+1}^{n} \alpha^{(t-1)} \quad \text{mod} \quad (q-1) x_i^t,
\] (12)

This equation gives the general theme to choose the coefficients at any particular round in any cycle. However, the encoded data \( y_i \)'s are defined as shown in Equation (13). In other words, for the first round in cycle one, the coefficients of the plain data \( x_1, x_2, \ldots, x_t \) are set to zero.

**C. Decoding Operations**

We know that the coefficients \( \alpha_1, \alpha_2, \ldots, \alpha_n \) are elements of a finite field, hence the inverses of these elements exist and are unique. Once a node fails which causes \( t \) data units to be lost, and once the receivers receive \( t \) linearly independent equations, they can linearly solve these equations to obtain the unknown \( t \) data units. At one particular cycle \( j \), we have three cases for the failures

i) All \( t \) link failures happened in the working paths, i.e. the working paths have failed to convey the messages \( x_i^j \) in round \( \ell \). In this case, \( n-t \) equations will be received, \( t \) of which are linear combinations of \( n-t \) data units, and the remaining \( n-2t \) are explicit \( x_i \) data units, for a total of \( n-t \) equations in \( n-t \) data units. In this case any \( t \) equations (packets) of the \( t \) encoded packets can be used to recover the lost data.

ii) All \( t \) link failures happened in the protection paths. In this case, the exact remaining \( n-t \) packets are working paths and they do not experience any failures. Therefore, no recovery operations are needed.

iii) The third case is that the failure might happen in some working and protection paths simultaneously in one particular round in a cycle. The recovery can be done using any \( t \) protection paths as shown in case i.

**V. Bounds on the Finite Field Size, \( F_q \)**

In this section we derive lower and upper bound on the alphabet size required for the encoding and decoding operations. In the proposed schemes we assume that direction connections exist between the senders and receivers, which the information can be exchanged with neglected cost.

The first result shows that the alphabet size required must be greater than the number of connections that carry unencoded data.

**Theorem 5:** Let \( n \) be the number of connections in the network model \( \mathcal{N} \), then the receivers are able to decode the encoded messages over \( F_q \) and will recover from \( t \geq 2 \) path failures if

\[
q \geq n - t + 1.
\] (14)

Also, if \( q = p^r \), then \( r \leq \lceil \log_p(n+1) \rceil \). The binary field is sufficient in case of a single path failure.

**Proof:** We will prove the lower bound by construction. Assume a NPS-T at one particular time \( t_j \) in the round \( \ell \) in a certain cycle \( \delta \). The protection code of NPS-T against \( t \) path failures is given in [1].

Without loss of generality, the interpretation of Scheme (11) is as follows:

i) The columns correspond to the senders \( S \) and rows correspond to \( t \) encoded data \( y_1, y_2, \ldots, y_t \).

ii) The first row corresponds to \( y_1 \) if we assume the first round in cycle one. Furthermore, every row represents the coefficients of every senders at a particular round.

iii) The column \( i \) represents the coefficients of the sender \( s_i \) through all protection paths \( L_1, L_2, \ldots, L_t \).

iv) Any element \( \alpha \) is \( F_q \) appears once in a column and row, except in the follow column and first row, where all elements are one’s.

v) All columns (rows) are linearly independent.

Due to the fact that the \( t \) failures might occur at any \( t \) working paths of \( L = \{L_1, L_2, \ldots, L_t\} \), then we can not predict the \( t \) protection paths as well. This means that \( t \) out of the \( n \) columns do not participate in the encoding coefficients, because \( t \) paths will carry encoded data. We notice that removing any \( t \) out of the \( n \) columns in Scheme (11) will result to \( n-t \) linearly independent columns. Therefore the smallest finite field that satisfies this condition must have \( n-t+1 \) elements.

The upper bound comes from the case of no failures, hence \( q \geq (n+1) \). Assume \( q \) is a prime power, then the result follows.

If \( q = 2^r \), then in general the previous bound can be stated as

\[
n - t + 1 \leq q \leq 2^{\lceil \log_2(n+1) \rceil}.
\] (15)

The following result shows the maximum admissible paths, which can suffer from failures, and the decoding operations can be achieved successfully.

**Lemma 6:** Let \( n \) and \( t \) be the number of connections and failures in the network model \( \mathcal{N} \), then we have \( t \leq \lfloor n/2 \rfloor \).

**Proof:** The proof is a direct consequence and from the fact that the protection paths must be less than or equal to the number of working paths.

This lemma shows that one can not provide protection paths better than duplicating the number of working paths.

**VI. Network Protection Using Distributed Capacities and Network Coding**

In this section we develop network protection strategy where some connection paths have high priorities (less bandwidth,
high demand). Let \( n \) be the set of available connections (disjoint paths from sources to receivers). Let \( m \) be the set of rounds in every cycle. In the previous strategies (NPS-T) we assumed that all connection paths have the same priority demand and working capacities. This might be the real case scenario, connections that carry applications with multimedia traffic have high priority than applications that carry data traffic. Therefore, it is required to design network protection strategies based on the traffic and sender priorities.

Consider that available working connections \( n \) may use their bandwidth assignments in asymmetric ways. Some connections are less demanding in terms of bandwidth requirements than other connections that require full capacity frequently. Therefore connections with less demanding can transmit more protection packets, while other connections demand more bandwidth, and can therefore transmit fewer protection packets throughout transmission rounds. Let \( m \) be the number of rounds and \( \ell_i \) be the time of transmission in a cycle \( \delta \) at round \( i \). For a particular cycle \( i \), let \( t \) be the number of protection paths against \( t \) failures that might affect the working paths. We will design network protection strategy against \( t \) arbitrary link failures (NPS-T2) as follows. Let the source \( s_j \) sends \( d_i \) data packets and \( p_i \) protection packets such that \( d_i + p_i = m \). Put differently:

\[
\sum_{i=1}^{n} (d_i + p_i) = nm \tag{16}
\]

In general we do not assume that \( d_i = d_i \) and \( p_i = p_i \). NPS-T2 is described as shown in Scheme [17]

The encoded data \( y^f_i \) is given by

\[
y^f_i = \sum_{k=1}^{n} x^f_k \tag{18}
\]

We assume that the maximum number of failures that might occur in a particular cycle is \( t \). Hence the number of protection paths (paths that carry encoded data) is \( t \). The selection of the working and protection paths in every round is done using a priority demanding function at the senders’s side. It will also depend on the traffic type and service provided on these protection and working connections.

In Scheme [17] every connection \( i \) is used to carry \( d_i \) un-encoded data \( x^f_i, x^d_i \) (working paths) and \( p_i \) encoded data \( y^f_i, y^p_i \) (protection paths) such that \( d_i + p_i = m \).

**Lemma 7:** Let \( t \) be the number of connection paths carrying encoded data in every round in NPS-T2, then the normalized network capacity \( C_N \) is given by

\[
(n - t)/n \tag{19}
\]

**Proof:** The proof is straight forward from the fact that \( t \) protection paths exist in every round, hence \( n - t \) working paths are available throughout all \( m \) rounds.

VII. ANALYSIS OF THE PROTECTION CODES OVER \( \mathbb{F}_q \)

We will prove correctness of the protection codes over \( \mathbb{F}_q \). Let \( \mathbb{F}_q \) be a finite field with \( q \) elements such that \( q = p^r \) for some nonzero integer \( r \) and prime \( p \). We will drive a scheme to recover from any \( m \) failures in the \( n + m \) primary and protection paths. Assume \( t \) be the number of failures in the primary paths. We have three cases

i) All failures occur in the primary paths, \( t = m \). In this case we need to establish a system of \( t \) linearly independent equations in \( t \) variables.

ii) \( t \) failures occur in the primary paths and \( m - t \) failures occur in the protection paths. In this case we need to establish a system of equations to recover the failures in the primary paths only.

iii) All failures occur in the protection paths. No recovery process is needed in this case.

We will show the encoding operation in case of directional connections from the senders to receivers. consider the worst case scenario in which \( m = t \). We can describe the encoding scheme for multiple link failures as shown in [11].

All \( \alpha \)'s powers are taken module the field size, i.e. \( \alpha^j \mod q = n+1 \). In other words, if \( q \geq n + 1 \), then we have the encoding matrix

\[
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
\alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^n \\
\alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(n)} \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\alpha^{t-1} & \alpha^{2(t-1)} & \alpha^{3(t-1)} & \cdots & \alpha^{(t-1)(n)}
\end{bmatrix} \tag{20}
\]

In this case we have \( \alpha^{q-1} = 1 \), \( q \) is a prime power.

The first column represents the coefficients of the encoding data at the first sender. Also, the first row represents the binary coefficients of all senders in case of a single link failure. Hence \( \alpha^{i-1} \) column represents the coefficients of the encoding data at the \( i \) sender for all \( 1 \leq i \leq n - 1 \).

In general for multiple \( m = t \) failures, the encoding data in the \( j \)-th protection is given by

\[
y_{n+j} = \sum_{i=1}^{n} \alpha^{j(i-1)} \mod q x_i, \tag{21}
\]

for \( 1 \leq j \leq m \).

As a matter of fact, the square sub-matrix of \( t \) columns of the encoding scheme [20] is invertable (has a full rank) if and only if its determinant is not equal to zero [6]. We will show

| Round time cycle 1 | 1   | 2   | 3   | 4   | 5   |
|-------------------|-----|-----|-----|-----|-----|
| \( s_1 \rightarrow r_1 \) | \( y^f_1 \) | \( x^f_1 \) | \( x^d_1 \) | \( y^f_1 \) | \( x^d_1 \) |
| \( s_2 \rightarrow r_2 \) | \( x^f_2 \) | \( y^f_2 \) | \( x^d_2 \) | \( y^f_2 \) | \( x^d_2 \) |
| \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) |
| \( s_i \rightarrow r_i \) | \( y^f_i \) | \( x^f_i \) | \( x^d_i \) | \( y^f_i \) | \( x^d_i \) |
| \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) |
| \( s_j \rightarrow r_j \) | \( x^f_j \) | \( y^f_j \) | \( x^d_j \) | \( y^f_j \) | \( x^d_j \) |
| \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) |
| \( s_n \rightarrow r_n \) | \( y^f_n \) | \( x^f_n \) | \( x^d_n \) | \( y^f_n \) | \( x^d_n \) |
that for any $t$ arbitrary link failures, the receivers are able to form a system of $t$ linearly independent equations and recover the lost data.

**Lemma 8:** If there are $t$ link failures in the primary paths, then the receivers are successfully able to recover from those failures using $t$ protection paths.

**Proof:** Let $\begin{bmatrix} 1 & \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{(t-1)j_1} \end{bmatrix}$ represent the any arbitrary column in the encoding scheme $\alpha_j$ indexed by the second element $\alpha^{i_j}$. Choosing any $t$ arbitrary columns $\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_t}$ yield

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_t} \\ \alpha^{j_2} & \alpha^{j_2} & \cdots & \alpha^{j_t} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(t-1)j_1} & \alpha^{(t-1)j_2} & \cdots & \alpha^{(t-1)j_t} \end{bmatrix}$$

(22)

Hence we have a system of $t$ equations in $t$ variables. Clearly, all elements in each row are different. Indeed this system has determinant given by the form [6, Theorem 6.5.5]

$$\alpha^{j_1+j_2+j_3+\cdots+j_t} \prod_{h>\ell} (\alpha^{j_h} - \alpha^{j_\ell}) \neq 0,$$

(23)

which proves the result.

Now, we shall prove the general case that any $\mu \times \mu$ square sub-matrix of the matrix $B$ has a full rank. Assume the square matrix is represented by

$$B = \begin{bmatrix} \alpha^{i_1j_1} & \alpha^{i_1j_2} & \cdots & \alpha^{i_1j_\mu} \\ \alpha^{i_2j_1} & \alpha^{i_2j_2} & \cdots & \alpha^{i_2j_\mu} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{i_\mu j_1} & \alpha^{i_\mu j_2} & \cdots & \alpha^{i_\mu j_\mu} \end{bmatrix}$$

(24)

where $1 \leq \mu \leq n$ and $\alpha^{i_jj_i}/F_q$.

**Lemma 9:** The sub-matrix $B$ described in (24) has a full rank.

**Proof:** We proceed the proof by mathematical induction.

i) We first prove that any $2 \times 2$ sub-matrix of $B$ has a full rank. It means that for any four elements lie in the corner are not alike (do not share a common factor). Put differently, $i \neq j$ and $\ell \neq 1$,

$$\begin{bmatrix} \alpha^i & \alpha^j \\ \alpha^{i_1} & \alpha^{j_1} \end{bmatrix}$$

(25)

If we divide the second row by $\alpha^{(1-\ell)i}$, we obtain $\alpha^i$. Now assume by contradiction that $\alpha^{(1-\ell)i}, \alpha^{j_1} = \alpha^i$. Or $\alpha^{(1-\ell)i} = \alpha^{(1-\ell)j} \mod q$. Obviously, this contradicts the fact that $\ell \neq 1$ and $i \neq j$. In addition $(l-1)(j-i) = 0 \mod q$ contradicts the fact about the field order. Hence, the result is a consequence.

ii) Now, assume the matrix

$$B_{\mu-1} = \begin{bmatrix} \alpha^{i_1j_1} & \alpha^{i_1j_2} & \cdots & \alpha^{i_1j_{\mu-1}} \\ \alpha^{i_2j_1} & \alpha^{i_2j_2} & \cdots & \alpha^{i_2j_{\mu-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{i_{\mu-1}j_1} & \alpha^{i_{\mu-1}j_2} & \cdots & \alpha^{i_{\mu-1}j_{\mu-1}} \end{bmatrix}$$

(26)

has a full rank.

iii) We will add any arbitrary row and column to the matrix $B_{\mu-1}$ to construct the matrix $B$.

$$B = \begin{bmatrix} \alpha^{i_1j_1} & \alpha^{i_1j_2} & \cdots & \alpha^{i_1j_{\mu-1}} & 1 \\ \alpha^{i_2j_1} & \alpha^{i_2j_2} & \cdots & \alpha^{i_2j_{\mu-1}} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha^{i_{\mu-1}j_1} & \alpha^{i_{\mu-1}j_2} & \cdots & \alpha^{i_{\mu-1}j_{\mu-1}} & 1 \end{bmatrix}$$

(27)

All elements in the last columns are different, also all elements in the last row are different. Since $\alpha^{i_jj_i}$ is an element in $F_q$, it has a unique inverse. Therefore, we can divide every row in the matrix $B$ by the element in the last column. Hence, we have

$$B' = \begin{bmatrix} \alpha^{i_1j_1} & \alpha^{i_1j_2} & \cdots & \alpha^{i_1j_{\mu-1}} & 1 \\ \alpha^{i_2j_1} & \alpha^{i_2j_2} & \cdots & \alpha^{i_2j_{\mu-1}} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha^{i_{\mu-1}j_1} & \alpha^{i_{\mu-1}j_2} & \cdots & \alpha^{i_{\mu-1}j_{\mu-1}} & 1 \end{bmatrix}$$

(28)

All powers of $\alpha$’s are taken modulo $q$. Furthermore, all elements in each row (or column) are pairwise disjoint. The matrix $B'$ is similar to the matrix shown in (22). Using lemma 8 the matrix $B'$ has a full rank given by $\mu$. ■

**VIII. CONCLUSION**

In this paper we demonstrated the encoding operations of network protection codes defined over finite fields. We derived a bound on the minimum field size required for choosing unique coefficients of data sent on the working paths. In addition we presented a scheme for differentiated services in cases of some working paths have high priorities in terms of bandwidth and capacity assignments.

**REFERENCES**

[1] R. Ahlsvede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. IEEE Trans. Inform. Theory, 46:1204–1216, 2000.

[2] S. A. Aly and A. E. Kamal. Network protection codes against link failures using network coding. In Proc. IEEE Globecom '08, New Orleans, LA, December 1-4 2008. [arXiv:0809.1258v1 [cs.IT].

[3] C. Fragouli, J. Le Boudec, and J. Widmer. Network coding: An instant primer. ACM SIGCOMM Computer Communication Review, 36(1):63–68, 2006.

[4] C. Fragouli and E. Soljanin. Network coding applications, foundations and trends in networking. Hanover, MA, Publishers Inc.

[5] A. E. Kamal. 1+N protection against multiple faults in mesh networks. In Proc. of the IEEE International Conference on Communications (ICC), 2007.

[6] V. Lint. Introduction to coding theory. 3rd edition, 1999.

[7] A. K. Somani. Survivability and traffic grooming in Optical Networks. Cambridge Press, 2006.

[8] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang. Network Coding Theory. Now Publishers Inc., 2006.

[9] H. Zeng and A. Vukovic. The variant cycle-cover problem in fault detection and localization for mesh all-optical networks. Photo Network Communication, 14:111–122, 2007.

[10] D. Zhou and S. Subramaniam. Survivability in optical networks. IEEE network, 14:16–23, Nov./Dec. 2000.