Network Protection Codes Against Link Failures Using Network Coding

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

***Abstract*—Protecting against link failures in communication networks is essential to increase robustness, accessibility, and reliability of data transmission. Recently, network coding has been proposed as a solution to provide agile and cost efficient network protection against link failures, which does not require data rerouting, or packet retransmission. To achieve this, separate paths have to be provisioned to carry encoded packets, hence requiring either the addition of extra links, or reserving some of the resources for this purpose. In this paper, we propose network protection codes against a single link failure using network coding, where a separate path using reserved links is not needed. In this case portions of the link capacities are used to carry the encoded packets.**

The scheme is extended to protect against multiple link failures and can be implemented at an overlay layer. Although this leads to reducing the network capacity, the network capacity reduction is asymptotically small in most cases of practical interest. We demonstrate that such network protection codes are equivalent to error correcting codes for erasure channels. Finally, we study the encoding and decoding operations of such codes over the binary field.

I. Introduction

Network coding is a powerful tool that has been used to increase the throughput, capacity, and performance of communication networks [14], [17]. It offers benefits in terms of energy efficiency, additional security, and reduced delay. 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], [14], [17] and references therein).

One application of network coding that has been proposed recently is to provide protection against link failures in overlay networks [8], [11]. This is achieved by transmitting combinations of data units from multiple connections on a backup path in a manner that enables each receiver node to recover a copy of the data transmitted on the working path in case the working path fails. This can result in recovery from failures without data rerouting, hence achieving agile protection. Moreover, the sharing of protection resources between multiple connections through the transmission of linear combinations of data units results in efficient use of protection resources. This, however, requires the establishment of extra paths over which the combined data units are transmitted. Such paths may require the addition of links to the network under the Separate Capacity Provisioning strategy (SCP), or that paths be provisioned using existing links if using the Joint Capacity Provisioning strategy (JCP), hence reducing the network traffic carrying capacity.

Certain networks can allow extra transmissions and the addition of bandwidth, but they do not allow the addition of new paths. In this scenario, one needs to design efficient data recovery schemes. Several previous approaches focused on solving this problem using additional extra paths at an overlay network level, or deploying ARQ protocols for the recovery of lost packets. In order to provide recovery from link failures in such networks, approaches other than using dedicated paths, or adding extra links must be used. In this paper, we propose such an approach in which we use network coding to provide agile, and resource efficient protection against link failures, and without adding extra paths. The approach is based on combining data units from a number of sources, and then transmitting the encoded data units using a small fraction of the bandwidth allocated to the connections, hence disposing of the requirement of having extra paths. In this scenario, once a path fails, the receiver can recover the lost packets easily from the neighbors by initiating simple queries.

Previous solutions in network survivability approaches using network coding focused on providing backup paths to recover the data affected by the failures [8], [9], [10]. Such approaches include 1+N, and M+N protections. In 1+N protection, an extra secondary path is used to carry combinations of data units from N different connections, and is therefore used to protect N primary paths from any single link failure. The M+N is an extension of 1+N protection where M extra secondary paths are needed to protect multiple link failures.

In this paper, we apply network coding for network protection against link failures and packet loss. We define the concept of protection codes similar to error-correcting codes that are widely used in channel coding [7], [13]. Protection codes are a new class of error monitoring codes that we propose in Section V. Such codes aim to provide better provisioning and data recovery mechanisms. A protection code is defined by a matrix G known at a set of senders S and receivers R. Every column vector in the generator matrix of a protection code defines the set of operations, in which every sender (receiver) needs to perform.

The new contributions in this paper are stated as follows:

i) We introduce link protection network coding-based using reduced capacity instead of adding extra paths as shown

This research was supported in part by grants CNS-0626741 and CNS-0721453 from the National Science Foundation, and a gift from Cisco Systems.

in the previous work [8], [9], [10].

ii) We develop a theoretical foundation of protection codes, in which the receivers are able to recover data sent over t failed links out of n primary links.

This paper is organized as follows. In Section II we briefly state the related work and previous solutions to the network protection problem using network coding. In Section III we present the network model and problem definition. Sections IV and V discuss single and multiple link failures and how to protect these link failures using reduced capacity and network coding. In Section VI we give analysis of the general case of $t \ll n$ link failures, and the paper is concluded in Section VII.

II. Related Work

In [8], the author introduced a 1+N protection model in optical mesh networks using network coding over p-cycles. The author suggested a model for protecting N connections from a set of sources to a set of receivers in a network with n connections, where one connection might fail. The suggested model can protect against a single link failure in any arbitrary path connecting a source and destination.

In [9], the author extended the previous model to protect multiple link failures. It is shown that protecting against m failures, at least m p-cycles are needed. An illustrative example in case of two link failures was given. The idea was to derive m linearly independent equations to recover the data sent from m sources.

In [10], the author extended the protection model in [8] and provided a GMPLS-based implementation of a link protection strategy that is a hybrid of 1+N and 1:N. It is claimed that the hybrid 1+N link protection provides protection at higher layers and with a speed that is comparable to the speed achieved by the physical layer implementations. In addition, it has less cost and much flexibility.

Monitoring network information flow using network coding was introduced in [6], [5]. In [4], it was shown how to use network coding techniques to improve network monitoring in overlay networks. Practical aspects of network coding has been shown in [2].

In this paper, we provide a new technique for protecting network failures using *protection codes* and *reduced capacity*. This technique can be deployed at an overlay layer in optical mesh networks, in which detecting failure is an essential task. The benefits of the proposed approach are that:

i) It allows receivers to recover the lost data without data rerouting or data retransmission.

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

iii) At any point in time, all n connection paths have full capacity except at one path in case of protecting against a single link failure and $m < n$ paths in case of protecting against m link failures.

We will analyze the proposed *protection codes* and error correcting codes that are used for erasure channels.

III. Network Model

Let $\mathcal{G} = (V, E)$ be a graph which represents an abstraction of a set of connections. V is a set of network nodes and E is a set of edges. Let there be n unicast connections, and let $S \subset V$ be the set of sources $\{s_1, ..., s_n\}$ and $R \subset V \backslash S$ be the set of receiver nodes $\{r_1, ..., r_n\}$ of the n connections in $\mathcal{G}$. The case of $S \cap R \neq \phi$ can be easily incorporated in our model. Two nodes u and v in $V \backslash \{S \cup R\}$ are connected by an edge (u, v) in E if there is a direct connection between them. We assume that the sources are independent of each other, meaning they can only send messages and there is no correlation between them. For simplicity, we will assume that a direct disjoint path exists between s_i and r_i, and it is disjoint from the path between s_j and r_j, for $j \neq i$.

The graph $\mathcal{G}$ represents an abstraction of our network model $\mathcal{N}$ with the following assumptions.

i) Let $\mathcal{N}$ be a network with a set of sources $S = \{s_1, s_2, \ldots, s_n\}$ and a set of receivers $R = \{r_1, r_2, \ldots, r_n\}$, where $S \cup R \subset V$.

ii) Let L be a set of links $L_1, L_2, \ldots, L_n$ such that there is a link L_i if and only if there is a connection path between the sender s_i and receiver r_i, i.e.,

$$L_i = \{(s_i, w_{1i}), (w_{1i}, w_{2i}), \ldots, (w_{(m)i}, r_i)\}, \qquad (1)$$

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

iii) Every source s_ℓ sends a packet with its own ID_{s_ℓ} and data x_ℓ to the receiver r_ℓ, so

$$packet_{s_\ell} = (ID_{s_\ell}, x_\ell, t_\ell^\delta), \qquad (2)$$

where t_ℓ^δ is the round time at step δ of the source packet $packet_{s_\ell}$.

iv) All links carry uni-directional messages from sources to receivers.

v) We consider the scenario where the cost of adding a new path is higher than just combining messages in an existing path, or there is not enough resources to provision extra paths in the network. These two cases correspond to separate and joint capacity provisioning, respectively [18].

We can define the unit capacity c_i of a link L_i as follows.

***Definition** 1:* Let $\mathcal{N}$ be a network model defined by a tuple (S, R, L). The unit capacity of a link L_i is given by

$$c_i = \begin{cases} 1, & L_i \text{ is active;} \\ 0, & \text{otherwise .} \end{cases} \qquad (3)$$

Also, the average normalized capacity of $\mathcal{N}$ is defined by the total number of active links divided by the total number of links n

$$C_{\mathcal{N}} = \frac{1}{n} \sum_{i=1}^{n} c_i. \qquad (4)$$

This means that each source s_i can send one packet per unit time on a link L_i. Assume that all links have the same capacity. In fact, we measure the capacity of $\mathcal{N}$ in the sense of the max-flow min-cut theorem, see [12]. One can always assume that a source with a large rate can be divided into a set of sources, each of which has a unit link capacity.

We can also define the set of sources that are connected to a source s_i in $\mathcal{N}$ as the degree of this source.

***Definition** 2:* The number of neighbors with a direct connection to a node u (i.e., a source s_i in S in the network $\mathcal{N}$) is called the *node degree* of $u \in V$, and is denoted by $d_n(u)$, i.e.,

$$1 \leq |\mathcal{N}(u)| = d_n(u) \leq n. \tag{5}$$

The following definition describes the *working* and *protection* paths between two network switches.

***Definition** 3:* The *working paths* on a network with n connection paths carry traffic under normal operations. The *Protection paths* provide alternate backup paths to carry the traffic in case of failures. A protection scheme ensures that data sent from the sources will reach the receivers in case of failure incidences on the working paths.

In this work the goal is to provide a reliable method for data protection sent over a link L_i without adding extra paths to the existing ones, but by possibly reducing the source rates slightly. In fact there are network scenarios where adding extra path is not applicable [15], [16], [18]. We propose a model to protect link failures using network coding where some senders are able to encode other sender's packets. We will study the network protection against link failures at an overlay layer in two cases: Single link failures and multiple link failures.

IV. Protecting Networks Against A Single Link Failure

In this section we study the problem of protecting a set of connections against a single link failure in a network $\mathcal{N}$ with a set of sources S and a set of receivers R. This problem has been studied in [8], [9] by provisioning a path that is link disjoint from all connection paths, and passes through all sources and destinations. All source packets are encoded in one single packet and transmitted over this path. The encoding is dynamic in the sense that packets are added and removed at each source and destination.

Assume that the assumptions about the proposed network model $\mathcal{N}$, and the abstraction graph $\mathcal{G}$ presented in Section III hold. We know that if there is an active link L_i between s_i and r_i, then the capacity c_i is the unit capacity. Let us consider the case where every source s_i sends its own data x_i and the encoded data y_i. The encoded message y_i is defined as

$$y_i = x_1 \oplus \ldots \oplus x_{i \neq j} \oplus \ldots \oplus x_n \tag{6}$$

from all other sources $S \backslash \{s_i\}$ over the finite field $\mathbf{F}_2 = \{0, 1\}$, where the symbol $\oplus$ is the XOR operation.

Assume that among the set of links L, there is a link L_i for $1 \leq i \leq n$ such that the sources s_i sends a packet to the receivers r_i as follows

$$packet_{s_i} = (ID_{s_i}, x_i, t_i^{\delta}). \tag{7}$$

Assume for now that link L_j has the unit capacity. The source s_j sends a packet that will carry the encoded data y_j to the receiver r_j over the link L_j,

$$packet_{s_j} = (ID_{s_j}, y_j, t_j^{\delta}). \tag{8}$$

We assume that the summation operations are performed over $\mathbf{F}_2$.

Now we consider the case where there is a single failure in a link L_k. Therefore, we have two cases:

i) If $k \neq j$, then the receiver r_k needs to query $(n-1)$ nodes in order to recover the lost data x_k over the failed link L_k. x_k can be recovered by adding all other $n-1$ data units.

ii) If the link L_j has a failure, then the receiver r_j does not need to query any other node. In this case the link L_j carries encoded data that is used for protection.

This shows that only one single receiver needs to perform $(n-1)$ operations in order to recover its data if its link fails. In other words, all other receivers will receive the transmitted data from the senders of their own connections with a constant operation $O(1)$.

A. Network Protection Codes (NPC) for a Single Link Failure

We can define the set of sources that will send encoded packets by using constraint matrices. We assume that there is a network protection code $\mathcal{C} \subseteq \mathbf{F}_2^n$ defined by the constraint systematic matrix

$$G = \begin{bmatrix} 1 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 1 \end{bmatrix}, \tag{9}$$

Without loss of generality, in Equation (9), the column vector $(\ g_{1j} \ \ g_{2j} \ \ \ldots \ \ g_{(n-1)j} \ )^T$ in $\mathbf{F}_2^{n-1}$ corresponds to (n-1) sources, say for example the sources $s_1, s_2, \ldots, s_{n-1}$, that will send (update) their values to (n-1) receivers, say i.e., $r_1, r_2, \ldots, r_{n-1}$. Also, there exists one source that will send encoded data. Also, the row vector $(\ g_{i1} \ \ g_{i2} \ \ \ldots \ \ g_{in} \ )$ in $\mathbf{F}_2^n$ determines the channels $L_1, L_2, \ldots, L_n$. The column vector $g_{i(n)}$ corresponds to the source s_i that will carry encoded data on the connection path L_i, see Fig. 1.

We can define the *protection codes* that will protect a single path failure as follows:

***Definition** 4:* An $[n, n-1]$ network protection code $\mathcal{C}$ is a 2^{n-1} dimensional subspace of the space $\mathbf{F}_2^n$ defined by the systematic generator matrix G and is able to protect a single network failure of an arbitrary path L_i.

We note that the *protection codes* are also error correcting codes that can be used for channel detection. Recall that an $[n, n-1, 2]$ code over $\mathbf{F}_2$ is a code that encodes (n-1) symbols into n symbols and detects (correct from) a single path failure.

In general, we will assume that the code $\mathcal{C}$ defined by the systematic generator matrix G is known for every source s_i

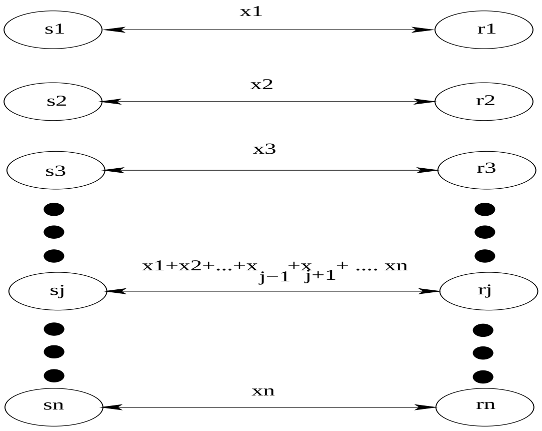

Fig. 1. Network protection against a single link failure using reduced capacity and network coding. One link out of n primary links carries encoded data.

and every receiver r_i. This means that every receiver will be able to recover the data x_i if the link L_i is corrupted. We assume that the positions of the failures are known. Furthermore, every source node has a copy of the code $\mathcal{C}$. Without loss of generality, the protection matrix among all sources is given by:

$$\begin{array}{c||ccccc} & L_1 & L_2 & \cdots & L_{n-1} & L_n \\ \hline\hline s_1 & x_1 & 0 & \cdots & 0 & x_1 \\ s_2 & 0 & x_2 & \cdots & 0 & x_2 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ s_{n-1} & 0 & 0 & \cdots & x_{n-1} & x_{n-1} \\ \hline\hline total & x_1 & x_2 & \dots & x_n & y_1 \end{array} \tag{10}$$

where y_1 is the protection value from every source s_ℓ that will be encoded at source s_i, for all $1 \leq \ell \leq n-1$. Put differently, we have

$$y_1 = \sum_{\ell=1}^{n-1} x_\ell \tag{11}$$

The summation operation is defined by the XOR operation. We note that the any source s_i can carry the encoded data.

Hence from the matrix (10), we have

$$y_{s_i} = \sum_{\ell=1,\ell\neq i}^{n} x_i \tag{12}$$

We assume that every source s_i has a buffer that stores its value x_i and the protection value y_{s_i}. Hence s_i prepares a packet $packet_{s_i}$ that contains the values

$$packet_{s_i} = (ID_{s_i}, y_{s_i}, t_i^\delta), \tag{13}$$

where y_{s_i} is defined in Equation (12).

***Example** 5:* Consider five sources $\{s_1, s_2, s_3, s_4, s_5\}$ and five receivers $\{r_1, r_2, r_3, r_4, r_5\}$. Without loss of generality, let us assume that the source s_i sends its message x_i to the receiver r_i for $i = \{1, 2, 3, 4\}$. Furthermore, the source s_5 sends the message $x_1 \oplus x_2 \oplus x_3 \oplus x_4$ to the receiver r_5. This is an example where a single path failure can be recovered from using network coding and the protection code shown above.

Hence, the source s_5 prepares the message $y_1 = x_1 \oplus x_2 \oplus x_3 \oplus x_4$, and sends the packet

$$packet_{s_5} = (ID_{s_5}, y_1, t_5^\delta).$$

Also, for $i = \{1, 2, 3, 4\}$, the source s_i sends the packet

$$packet_{s_i} = (ID_{s_i}, x_i, t_i^\delta).$$

So, every receiver r_ℓ will obtain a packet at a round time t_ℓ^δ in a connection path L_ℓ. If we assume that there is one failed path, then four receivers will receive their packets correctly. Assuming a receiver, with a failure in its path, knows the matrix G, in this case it is able to query other receivers to obtain its data.

We notice that it is enough to allow only one source node to perform the encoding operations for protecting against a single path failure. This fact can be stated in the following lemma.

***Lemma** 6:* Encoding the data from sources $S \backslash \{s_i\}$ at a source s_i in the network $\mathcal{N}$ is enough to protect against a single path failure.

***Lemma** 7:* The total number of encoding operations needed to recover from a single link failure in a network $\mathcal{N}$ with n sources is given by $(n-1)$ and the total number of transmissions is n.

The previous lemma guarantees the recovery from a single arbitrary link failure. The reason is that the link that carries encoded data might fail itself and one needs to protect its data.

***Lemma** 8:* In the network model $\mathcal{N}$, the average network capacity of protecting against a single link failure using reduced capacity and network coding is given by $(n-1)/n$.

Proof: (Sketch)

i) We know that every source s_ℓ that sends the data x_ℓ has capacity $c_\ell = 1$. ii) Also, the source s_i that sends x_i and the encoded data y_{s_i} at different slots, has a full capacity. iii) The source s_i is not fixed among all nodes S, however, it is rotated periodically over all sources for fairness. On average one source of the n nodes will reduce its capacity. This shows the capacity of $\mathcal{N}$ as stated. ■

V. Protecting Networks Against Multiple Link Failures

In the previous section we introduced a strategy for a single link failure in optical mesh networks, where the chance of a single link failure is much higher than multiple link failures. However, it was shown in [15], [18] through an experimental study that about $\%30$ of the failures of the Sprint backbone network are multiple link failures. Hence, one needs to design a general strategy against multiple link failures.

In this section we will generalize the above strategy to protect against t path failures using network protection codes

(NPC) and the reduced capacity. We have the following assumptions about the channel model:

i) We assume that any t arbitrary paths may fail and they are independent of each other.

ii) Location of the failures are known, but they are arbitrary among n connections.

iii) Protecting n working paths, k connection must carry plain data, and $m = n-k$ connections must carry encoded data.

iv) We do not add extra link paths, and every source node is able to encode the incoming packets.

v) We consider the encoding and decoding operations are performed over $\mathbf{F}_2$.

We will show the connection between error correcting codes and protection codes [7], [13].

We have n working paths from the senders to receivers. We will assume that a path L_i can have a full capacity or it can manage a buffer that maintains the full capacity where the encoded data is sent.

Assume that the notations in the previous sections hold. Let us assume a network model $\mathcal{N}$ with $t > 1$ path failures. One can define a protection code $\mathcal{C}$ which protects n links as shown in the systematic matrix G in (14). In general, the systematic generator matrix G defines the source nodes that will send encoded messages and source nodes that will send only plain messages. In order to protect n working paths, k connection must carry plain data, and $m = n - k$ connections must carry encoded data. The systematic generator matrix of the NPC for multiple link failures is given by:

$$G = \left[\begin{array}{cccccccc} 1 & 0 & \ldots & 0 & | & p_{11} & \ldots & p_{1m} \\ 0 & 1 & \ldots & 0 & | & p_{22} & \ldots & p_{2m} \\ \vdots & \vdots & \vdots & & | & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & | & p_{k1} & \ldots & p_{km} \\ & & & & & & & \\ \multicolumn{4}{c}{\underbrace{\text{identity matrix } k \times k}} & & \multicolumn{3}{c}{\underbrace{\text{Submatrix } P_{k \times m}}} \end{array} \right], \quad (14)$$

where $p_{ij} \in \mathbf{F}_2$ goodbreak

The matrix G can be rewritten as

$$G = \left[\; I_k \;\; | \;\; \mathbf{P} \; \right], \quad (15)$$

where $\mathbf{P}$ is the sub-matrix that defines the redundant data $\sum_{i=1}^{k} p_{ij}$ to be sent to a set of sources for the purpose of data protection against data loss and link protection against link failures. Based on the above matrix, every source s_i sends its own message x_i to the receiver r_i via the link L_i. In addition m links out of the n links will carry encoded data.

***Definition** 9:* An [n,k,d] protection code $\mathcal{C}$ is a 2^k dimensional subspace of the space $\mathbf{F}_2^n$ that is able to protect all network failures up to $d-1$.

In general the network protection code (NPC), which protects against multiple path failures, can be defined by a generator matrix G known for every sender and receiver. Also, there exists a parity check matrix H corresponds to G such that $GH^T = 0$. We will restrict ourselves in this work for NPC that are generated by a given systematic generator matrix G over $\mathbf{F}_2$.

Without loss of generality, the protection matrix among all sources is given by

$$\begin{array}{c||cccccccc} & L_1 & L_2 & \cdots & L_k & L_{k+1} & L_{k+2} & \ldots & L_n \\ \hline s_1 & x_1 & 0 & \cdots & 0 & x_1 & x_1 & \ldots & x_1 \\ s_2 & 0 & x_2 & \cdots & 0 & x_2 & x_2 & \ldots & x_2 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \\ s_k & 0 & 0 & \cdots & x_k & x_k & x_k & \ldots & x_k \\ \hline\hline & x_1 & x_2 & \ldots & x_k & y_1 & y_2 & \ldots & y_m \end{array} \quad (16)$$

We ensure that $k = n - m$ paths have full capacity and they carry the plain data $x_1, x_2, \ldots, x_k$. Also, all other m paths have full capacity, in which they carry the encoded data $y_1, y_2, \ldots, y_m$. In addition, the m links are not fixed, and they are chosen alternatively between the n links.

Encoding Process. The network encoding processes at the set of senders are performed in a similar manner as in Section IV. Every source s_i has a copy of the systematic matrix G and it will prepare a packet along with its ID in two different cases. First, if the source s_i will send only its own data x_i with a full link capacity, then

$$packet_{s_i} = (ID_{s_i}, x_i, t_i^{\delta}). \quad (17)$$

Second, if the source s_j will send an encoded data in its packet, then

$$packet_{s_j} = (ID_{s_j}, \sum_{\ell=1,\ell\neq j}^{k} p_{\ell j} x_{\ell}, t_j^{\delta}), \quad (18)$$

where $p_{\ell j} \in \mathbf{F}_2$.

Recovery Process. The recovery process is done as follows. The $packet_{s_i}$ arrives at a receiver r_i in time slots, hence every packet from a source s_i has a round time t_i^{δ}. In this case, time synchronization is needed to guarantee the reception of the correct data. The receiver r_i at time slot n will detect the signal in the link L_i. If the link L_i failed, then r_i will send a query to other receivers in $R \backslash \{r_i\}$ asking for their received data. Assume there are t path failures. Then we have three cases:

1) All t link failures have occurred in links that do not carry encoded packets, i.e., $packet_{s_i} = (ID_{s_i}, x_i, t_i^{\delta})$. In this case, one receiver that carries an encoded packet, e.g., r_j, can send $n-t-1$ queries to the other receivers with active links asking for their received data. After this process, the receiver r_j is able to decode all messages and will send individual messages to all receivers with link failures to pass their correct data.

2) All t link failures have occurred in links that carry encoded packets, i.e., $packet_{s_j} = (ID_{s_j}, \sum_{\ell=1,\ell\neq j}^{k} x_\ell, t_j^\delta)$. In this case no recovery operations are needed.
3) All t link failures have occurred in arbitrary links. This case is a combination of the previous two cases and the recover process is done in a similar way. Only the lost data on the working paths needs to be recovered.

Our future work will include practical implementation aspects of the proposed model as shown in the case of adding extra paths [10]. The proposed network protection scheme using distributed capacity and coding is able to recover up to $t \leq d-1$ link failures (as defined in Definition 9) among n paths and it has the following advantages:

i) $k = n-m$ links have full capacity and their sender nodes have the same transmission rate.
ii) The m links that carry encoded data are dynamic (distributed) among all n links. Therefore, no single link L_i will suffer from usage of reduced capacity.
iii) The encoding process is simple once every sender s_i knows the NPC. Hence s_i maintains a round time t_i^δ for each sent $packet_{s_i}$.
iv) The recovery from link failures is done in a dynamic and simple way. Only one receiver node needs to perform the decoding process and it passes the data to other receivers that suffer from link failures.

VI. Analysis

We shall provide theoretical analysis regarding the proposed network protection codes. One can easily compute the number of paths needed to carry encoded messages to protect against t link failures, and will obtain the average network capacity. The main idea behind NPC is to simplify the encoding operations at the sources and the decoding operations at the receivers. The following lemma demonstrates the average capacity of the proposed network model $\mathcal{N}$.

***Lemma** 10:* Let $\mathcal{C}$ be a protection code with parameters $[n, n-m, d_{min}]$ over $\mathbf{F}_2$. Assume n and m be the number of sources (receivers) and number of connections carrying encoded packets, respectively, the average capacity of the network $\mathcal{N}$ is given by

$$(n-m)/n. \tag{19}$$

Proof: We have m protection paths that carry encoded data. Hence there are $n-m$ working paths that carry plain data. The result is a direct consequence by applying the normalized capacity definition. ■

***Lemma** 11:* In the network protection model $\mathcal{N}$, in order to protect t network disjoint link failures, the minimum distance of the protection code must be at least $t+1$.

Proof: We can assume that the network link failures can occur at any arbitrary paths. The proof comes from the fact that the protection code can detect t failures. ■

The previous lemma ensures that the maximum number of failures that can be recovered by $\mathcal{C}$ is $d_{min} - 1$.

For example one can use the Hamming codes with parameters $[2^m - 1, 2^m - m - 1, 3]_2$ to recover from two failures, see [7], [13] for notation. One can also puncture these codes to reach the required length, i.e., number of connections. $[7,4,3]_2$, $[15,11,3]_2$, and $[63,57,3]_2$ are examples of Hamming codes that protect against two link failures. Another example is the BCH codes with arbitrary design distance. $[15,11,3]_2$, $[31,26,3]_2$ and $[63,56,3]_2$ are examples of BCH codes that protect one and two link failures. Also, $[15,8,5]_2$, $[31,21,5]_2$ and $[48,36,5]_2$ are examples of BCH codes that protect against four link failures [7], [13]. Our future work will include tables of the best known network protection codes.

VII. Conclusion

We studied a model for recovering from network link failures using network coding and reduced capacity. We defined the concept of network protection codes to protect against arbitrary t link failures. We showed that the encoding and decoding processes of the proposed scheme are simple and can be done in a dynamic way at any arbitrary senders and receivers in an overlay layer on optical mesh networks. Our future work will include tables of best known protection codes and a comparison between protection against link failures using reduced capacity and using extra paths.

References

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

[2] P. A. Chou, Y. Wu, and K. Jain. Practical network coding. *41st Allerton Conf. Comm., Ctrl. and Comp.*, Monticello, IL, Oct. 2003.

[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 A. Markopoulou. A network coding approach to overlay network monitoring. In *44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, September 2005.

[5] T. Ho, R. Koetter, M. Medard, D. Karger, and M. Effros. The benefits of coding over routing in a randomized setting. In *Proc. of the IEEE International Symposium on Information Theory (ISIT03)*, page 442, Yokohama, Japan, June 2003.

[6] T. Ho, B. Leong, Y. Chang, Y. Wen, and R. Koetter. Network monitoring in multicast networks using network coding. In *Proc. of International Symposium on Information Theory (ISIT05)*, 2005.

[7] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[8] A. E. Kamal. 1+N protection in optical mesh networks using network coding on p-cycles. In *Proc. of the IEEE Globecom*, 2006.

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

[10] A. E. Kamal. Gmpls-based hybrid 1+N link protection over *p*-cycles: Design and performance. In *Proc. of IEEE Globecom*, 2007.

[11] A. E. Kamal. A generalized strategy for 1+N protection. In *Proc. of the IEEE International Conference on Communications (ICC)*, 2008.

[12] D. R. Karger. Random sampling in cut, flow and network design problems. *Math. of Oper. Res.*, 24(2):0383 0413, 1999.

[13] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[14] E. Soljanin and C. Fragouli. Network codinginformation flow perspective. 2007.

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

[16] J. Vasseur, M. Pickavet, and P. Demeester. *Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*. Morgan Kaufmann Publishers Inc. San Francisco, CA, 2004.

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

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