Network Coding-Based Protection Strategy Against Node Failures

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—**With the enormous increase in the usage of communication networks, protection against node and link failures became essential in the deployment of reliable networks. To manage loss of data due to node failures, we design a network protection strategy that aims to withstand such failures. In this paper we propose a protection strategy against any single node failure in the network. We deploy network coding and reduced capacity in this strategy without adding extra working paths to the readily available connection paths. The strategy is based on representing node failures by the failure of multiple links, and hence is transformed into a protection against multiple link failures. Consequently, the protection strategies proposed in [2], [8] can also be applied for protection against node failures. In addition, we demonstrate the implementation aspects of the premeditated protection strategies.**

Index Terms—

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. Several techniques to provide network survivability 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 [13].

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], [5], [6], [12] 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.

In network survivability, the four different types of failures that might affect network operations are [10], [14]: 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

swritch/router, fire, or any other hardware damage. In addition, the failure might be due to network maintenance. However, node failure is more damaging than link or system failures since multiple connections may be affected by the failure of a single node.

Recently, the authors have proposed employing the network coding technique in order to protect against single and multiple link failures [2], [4], [8], in a manner that achieves both agility and resource efficiency. The idea is to form linear combinations of data packets transmitted on the working circuits, and transmit these combinations simultaneously on a shared protection circuit. The protection circuit can take the form of an additional p-cycle [7], [8], a path or a general tree network [9]. In the case of failures, the linear combinations can be used by the end nodes of the connection(s) affected by the failure(s) to recover the lost data packets. These network protection strategies against link failures using network coding have been extended to use reduced capacities instead of reserving, or even adding separate protection circuits [2], [4]. The advantages of using network coding-based protection are twofold: first, one set of protection circuits is shared between a number of connections, hence leading to reduced protection cost; and second, copies of data packets are transmitted on the shared protection circuit after being linearly combined, hence leading to fast recovery of lost data since failure detection and data rerouting are not needed.

In this paper we consider the problem of providing protection against node failures using network coding, and using the reduced capacity technique. As a byproduct of this protection strategy, protection against any single link failure is also guaranteed. This is based on representing the node failure by the failure of multiple links. However, the failed links are not any arbitrary links. Since working paths used by the connections that are protected together are link disjoint, the links that need to be protected are used by different connections.

II. NETWORK MODEL

The following points highlight the network model and main considerations.

- Let $\mathcal{N}$ be a network represented by an abstract graph $G = (\mathbf{V}, E)$, where $\mathbf{V}$ is the set of nodes and E be set of undirected edges. Let S and R be sets of independent sources and destinations, respectively. The set $\mathbf{V} = V \cup S \cup R$ contains the relay nodes which are in the set V,
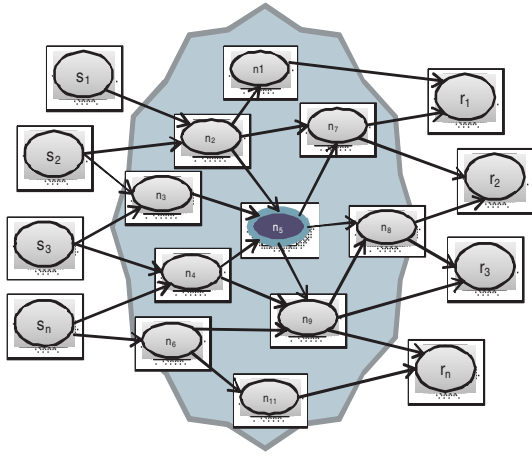
Fig. 1. A Network $\mathcal{N}$ with a set of nodes $\mathbf{V}$ and a set of edges E. The nodes $\mathbf{V}$ consist of sources S, receivers R, and relay nodes V. The node n_5 represents a failed node with 3 working connections that must be protected at the failure incidence.

sources, and destinations as show in Fig. 1. Assume for simplicity that $|S| = |R| = n$, hence the set of sources is equal to the set of receivers.

- A path (connection) is a set of edges connected together with a starting node (sender) and an ending node (receiver).

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

where $1 \leq i \leq n$, $(w_{(j-1)i}, w_{ji}) \in E$, and +ve integer m.

- The node can be a router, switch, or an end terminal depending on the network model $\mathcal{N}$ and the transmission layer, see Fig. 2.
- L is a set of paths $L = \{L_1, L_2, \ldots, L_n\}$ carrying the data from the sources to receivers. Connection paths are link disjoint and provisioned in the network between senders and receivers. All connections have the same bandwidth, otherwise a connection with high bandwidth can be divided into multiple connections, each of which has the unit capacity. There are exactly n connections. A sender with a high capacity can divide its capacity into multiple unit capacities.
- We consider the case that the failures happen in the relay nodes. The failures in the relay nodes might happen due to a failed switch, router, or any connecting point as shown in fig. 1. We assume that the failures are independent of each other.

Definition 1 (Node Relay Degree): Let u be an arbitrary node in $V = \mathbf{V} \backslash \{S \cup R\}$, which relays the traffic between source and terminal nodes. The number of connections passing through this node is called the *node relay degree*, and is referred to as $d(u)$. Put differently:

$$d(u) = \left| \{L_i : (u, w) \in L_i, \forall w \in \mathbf{V}, 1 \leq i \leq n\} \right|. \quad (2)$$

Note that the above definition is different from the graph theoretic definition of the node degrees; input and output

degrees. However, the node degree must not be less than the node relay degree. Furthermore, the node relay degree of a node u is $d(u) \leq \lfloor \mu(u)/2 \rfloor$, where $\mu(u)$ is the degree of a node u in an undirected graph.

We can define the network capacity from the min-cut max-flow information theoretic view [1]. It can be described as follows.

Definition 2: The unit capacity of a connecting path L_i between s_i and r_i is defined by

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

The total capacity of $\mathcal{N}$ is given by the summation of all path capacities. What we mean by an *active* path is that the receiver is able to receive and process signals/packets throughout this path, see for further details [3].

Clearly, if all paths are active then the total capacity of all connections is n and the normalized capacity is 1. If we assume there are n disjoint paths, then, in general, the normalized capacity of the network for the active and failed paths is computed by

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

The *working paths* on a network with n connection paths carry traffic under normal operations, see Fig. 2. The *Protection paths* provide an alternate backup path 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 [2], [4].

III. PROTECTING AGAINST A SINGLE NODE FAILURE

In this section we demonstrate a model for network protection against a single node failure (SNF) using network coding. Previous work focused on network protection against single and multiple link failures using rerouting and sending packets throughout different links. We use network coding and reduced capacity on the paths carrying data from the sources to destinations. The idea has been developed for the purpose of link and path failures in [2], [7]. We present a protection strategy against a single node failure denoted by NPS-T. Under NPS-T, the normalized network capacity, based on the max-flow between sources and destinations, is given by $(n-t)/n$, where t is the maximum number of connections traversing any node in the network. We develop the design methodology of this strategy. In addition we derive bounds on the field size and encoding operations.

Assume we have the same definitions as shown in the previous section. Let $d(u)$ be the relay node degree of a node u in V. We define d_0 to be the max over all node's relay degrees in the network $\mathcal{N}$.

$$d_0 = \max_{u \in V} d(u) \quad (5)$$

Note that d_o is the degree representing the max links that can fail, in other words it is the number of working paths that
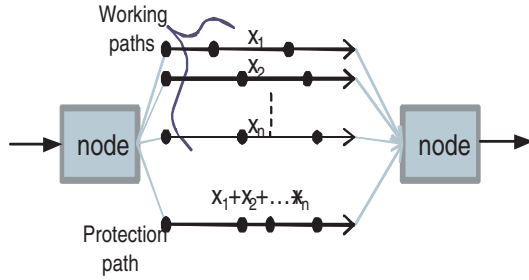
Fig. 2. Network protection against a single path failure using reduced capacity and network coding. One path out of n primary paths carries encoded data. The black points represent various other relay nodes

$$
\begin{array}{c|cccccc}
 & 1 & 2 & 3 & 4 & \ldots & \lfloor n/t \rfloor \\
\hline
s_1 \to r_1 & y_1 & x_1^1 & x_1^2 & x_1^3 & \ldots & x_1^{n-1} \\
s_2 \to r_2 & y_2 & x_2^1 & x_2^2 & x_2^3 & \ldots & x_2^{n-1} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
s_t \to r_t & y_t & x_t^1 & x_t^2 & x_t^3 & \ldots & x_t^{n-1} \\
s_{t+1} \to r_{t+1} & x_{t+1}^1 & y_{t+1} & x_{t+1}^2 & x_{2t+1}^3 & \ldots & x_{2t+1}^{n-1} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
s_{2t} \to r_{2t} & x_{2t}^1 & y_{2t} & x_{2t}^2 & x_{2t}^3 & \ldots & x_{2t}^{n-1} \\
s_{2t+1} \to r_{2t+1} & x_{2t+1}^1 & x_{2t+1}^2 & y_{2t+1} & x_{2t+1}^3 & \ldots & x_{2t+1}^{n-1} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
s_n \to r_n & x_n^1 & x_n^2 & x_n^3 & x_n^4 & \ldots & y_n
\end{array}
\tag{6}
$$

might fail due to the failure of a relay node. Let v be the node with relay degree d_0, and assume v to be the failed node. Our goal is to protect the network $\mathcal{N}$ against this node failure. In fact d_0 represents a set of failed connections caused by a failure of the node v in the network $\mathcal{N}$. Although the failure of v is represented by the failure of $2d_0$ links, each incoming link at v has a corresponding outgoing link, and if either, or both of these two links fail, the effect on the connection is the same. Therefore, our protection strategy is based on representing the node failure by the failure of d_0 connections, and we therefore need to protect against d_0 failed connections.

Notice that in this case, t must not exceed d_0. We therefore consider the worst case, i.e., protecting against d_0 failures.

A. NPS-T Protecting SNF with $d_0 = t$ and Achieving $(n-t)/n$ Normalized Capacity

Assume the sender s_i sends a message to the receiver r_i via the path L_i. Assume without loss of generality that t disjoint working paths have failed due to the failure of a single node. Then, the protection code can be described as in Scheme (6). Under this protection scheme, $n - t$ of the working paths will be carrying new data units, which are denoted by x_j^i, which is the data unit transmitted on working path j in round i. The remaining t paths will be carrying linear combinations, which are denoted by y_i, which will be used to recover from data unit losses due to the failure.

In general, y_ℓ is given by

$$
y_\ell = \sum_{i=1}^{(j-1)t} \alpha_i^\ell x_i^j + \sum_{i=jt+1}^{n} a_i^\ell x_i^j
$$

$$
\text{for } (j-1)t+1 \leq \ell \leq jt, 1 \leq j \leq \frac{n}{t}. \tag{7}
$$

We consider the coefficients α_i^l to be taken from a finite field with $q > 2$ alphabets. Later in this section, we will show how to perform the encoding and decoding operations for the purpose of recovery from failures. The following Theorem gives the normalized capacity of NPS-T strategy.

Theorem 3: Let n be the total number of connections from sources to receivers. The capacity of NPS-T strategy against t path failures as a result of a single node failure is given by

$$
\mathcal{C}_\mathcal{N} = (n-t)/(n) \tag{8}
$$

Proof: In NPS-T, there are t paths that will carry encoded data in each round time in particular session. Without loss of generality, consider the case in which n/t is an integer[1]. Therefore, there exists (n/t) rounds, in which the capacity is (n-t) in each round. Also, the capacity in the first round is n-t. Hence, we have

$$
\begin{aligned}
\mathcal{C}_\mathcal{N} &= \frac{\sum_{i=1}^{n/t}(n-t)}{(n/t)n} \\
&= \frac{n-t}{n}
\end{aligned}
\tag{9}
$$

∎

The advantages of NPS-T approach are 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 approach is suitable for applications that do not tolerate packet delay such as real-time applications, e.g., voice and TV transmissions.
- %100 recovery against any single node failure. In addition, up to t disjoint path failures can be recovered from.
- Using this strategy, no extra paths are needed. This will make this approach more suitable for applications, in which adding extra paths, or reserving links or paths just for protection, may not be feasible.
- The encoding and decoding operations are linear, and the coefficients of the variables x_i^j are taken from a finite field with $q > 2$ elements.

B. 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

---

[1]The general case in which n/t is not an integer can be accommodated by running the strategy for $m\lfloor(n/t)\rfloor$ rounds, where m is the smallest integer such that $mn \bmod t = 0$.

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. there are t protection paths. Therefore, to treat all connections fairly, there will be n/t rounds, and in each round the capacity is given by n-t.

We consider the case in which all symbols x_i^j belong to the same round. The first t sources transmit the first encoded 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 receiver 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 session δ is given by t_δ^j. Then the source s_i will send $packet_{s_i}$ on the working path which includes

$$Packet_{s_i} = (ID_{s_i}, x_i^\ell, t_\delta^\ell) \qquad (10)$$

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

$$Packet_{s_j} = (ID_{s_j}, y_k, t_\delta^\ell), \qquad (11)$$

where y_k is defined in (7). Hence the protection paths are used to protect the data transmitted in round ℓ, which are included in the x_i^l data units. The encoded data y_k is computed in a simple way where source s_j, for example, will collect all sources' data units, and using proper coefficients, will compute the y_k data units defined in Scheme (7). In this case every data unit x_i^ℓ is multiplied by a unique coefficient $\alpha_i \in \mathbf{F}_q$. This will differentiate the encoded data $y_i's$. Also, the sender s_k will send a $packet_{s_k}$ in the protection path as follows

$$Packet_{s_k} = (ID_{s_k}, \sum_{i=1}^{n} \alpha_i^l x_i^\ell, t_\delta^\ell) \qquad (12)$$

s_k chooses different coefficients in the finite field $\mathbf{F}_q$. So, we have a system of t independent equations at each round time that will be used to recover at most t unknown variables.

C. Proper Coefficients Selection

One way to select the coefficients a_j^ℓ's in each round such that we have a system of t linearly independent equations is by adapting the parity check matrix of a nonprimitive narrow-sense BCH code of length n and designed distance t. Let α be a primitive element in $\mathbf{F}_q$. Let q be the order of a finite field, and α be the root of unity. Then we modify and use the parity check matrix of a BCH code to define the coefficients of the senders as:

$$H_{bch} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{t-1} & \alpha^{2(t-1)} & \cdots & \alpha^{(t-1)(n-1)} \end{bmatrix}. \qquad (13)$$

We have the following assumptions about the encoding operations as shown in Scheme (16).

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 $d_0 = t$, then the $y_1, y_2, \ldots, y_t$ equations are written as:

$$y_1 = \sum_{i=t+1}^{n} x_i^1, \; y_2 = \sum_{i=t+1}^{n} \alpha^{(i-1)} x_i^2, \qquad (14)$$

$$y_j = \sum_{i=t+1}^{n} \alpha^{i(j-1) \mod (q-1)} x_i^\ell, \qquad (15)$$

Therefore, the scheme that describes the encoding operations in the first round for t link failures can be described as

		round one, t failures			
	y_1	y_2	y_3	$\cdots$	y_t
$s_1 \to r_1$	1	1	1	$\cdots$	1
$s_2 \to r_2$	1	α	α^2	$\cdots$	α^{t-1}
$s_3 \to r_3$	1	α^2	α^4	$\cdots$	$\alpha^{2(t-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$s_i \to r_i$	1	α^{i-1}	$\cdots$	$\cdots$	$\alpha^{(i-1)(t-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$s_n \to r_n$	1	α^{n-1}	$\alpha^{2(n-1)}$	$\cdots$	$\alpha^{(t-1)(n-1)}$

$$(16)$$

This Scheme gives the general theme to choose the coefficients at any particular round in any session. However, the encoded data y_i's are defined as shown in Equation (15). In other words, for the first round in session one, the coefficients of the plain data $x_1, x_2, \ldots, x_t$ are set to zero.

D. Decoding Operations

We know that the coefficients $a_1^\ell, a_2^\ell, \ldots, a_n^\ell$ are elements of a finite field, $\mathbf{F}_q$, hence the inverses of these elements exist and they 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 t unknown data units. At one particular session 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^ℓ in round ℓ. 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 session. The recover can be done using any t protection paths as shown in case i.

IV. BOUNDS ON THE FINITE FIELD SIZE, $\mathbf{F}_q$

In this section we derive lower and upper bounds on the alphabet size required for the encoding and decoding operations. In the proposed schemes we assume that unidirectional connections exist between the senders and receivers, which the information can be exchanged with little cost. The first result shows that the alphabet size required must be greater than the number of connections that carry unencoded data.

Theorem 4: Let n be the number of connections in the network model $\mathcal{N}$. Then the receivers are able to decode the encoded messages over $\mathbf{F}_q$ and will recover from $t \geq 2$ path failures if

$$q \geq n - t + 1. \tag{17}$$

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_δ^ℓ in the round ℓ in a certain session δ. The protection code of NPS-T against t path failures is given as

$$C_t = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{t-1} & \alpha^{2(t-1)} & \cdots & \alpha^{(t-1)(n-1)} \end{bmatrix} \tag{18}$$

Without loss of generality, the interpretation of Equation (18) 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 session 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 $\alpha^i \in F_q$ appears once in a column and row, except in the first 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 $L = \{l_1, L_2, \ldots, l_n\}$, 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 Equation (18) will result in $n - t$ 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, then the result follows. ∎

if $q = 2^r$, then in general the previous bound can be stated as

$$n - t + 1 \leq q \leq 2^{\lceil \log_2(n+1) \rceil}. \tag{19}$$

We defined the feasible solution for the encoding and decoding operations of NPS-T as the solution that has integer reachable upper bounds.

Corollary 5: The protection code (18) always gives a feasible solution.

V. CONCLUSIONS

In this paper we presented a model for network protection against a single node failure, which is equivalent to protecting against t link failures, and can therefore be used also to protect against t link failures. We demonstrated an implementation strategy for the proposed network protection schemes. The network capacity is computed, and bounds on the network resources are established.

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

[3] S. A. Aly and A. E. Kamal. Network protection codes: Providing self-healing in autonomic networks using network coding. *IEEE Journal on Selected Areas in Communciation (JSAC), special issue on Autonomic Communications, submitted*, 2008. arXiv:0812.0972v1 [cs.NI].

[4] S. A. Aly and A. E. Kamal. Network coding-based protection strategies against a single link failure in optical networks. In *Proc. IEEE International Conference on Computer Engineering & Systems (ICCES'08), Cairo, EG*, November 25-27, 2008. arXiv:0810.4059v1 [cs.IT].

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

[6] C. Fragouli and E. Soljanin. Network coding applications, foundations and trends in networking. *Hanover, MA, Publishers Inc.*, vol. 2, no. 2, pp. 135-269, 2007.

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

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

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

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

[11] A. Sprintson, S. Y. El-Rouayheb, and C. N. Georghiades. Robust network coding for bidirected networks. In *Proc. IEEE Information theory workshop, UCSD, CA*, pages 378–383, 2007.

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

[13] 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.

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