Protection against link errors and failures using network coding

Shizheng Li and Aditya Ramamoorthy
Iowa State University

Introduction

We want to protect the network against:

1) Failures: packet loss; easy to detect

2) Adversarial errors: The adversary knows communications protocol; No secrecy hidden from him; Controls certain links in the network

The multiple bidirectional unicast connections to be protected are over primary paths. The protection paths pass through the end nodes of all the connections

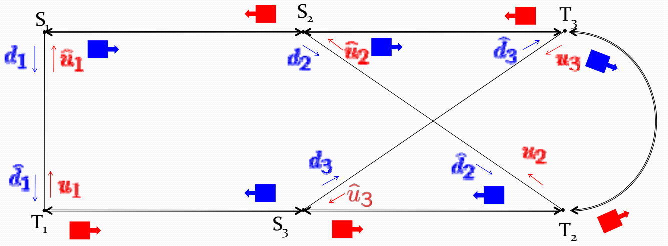
Main Results

1) n_e paths (protection or primary) in error: need $4n_e$ protection paths
2) n_e paths (protection or primary) in error and n_f paths (protection or primary) fail: need $4n_e + 2n_f$ protection paths

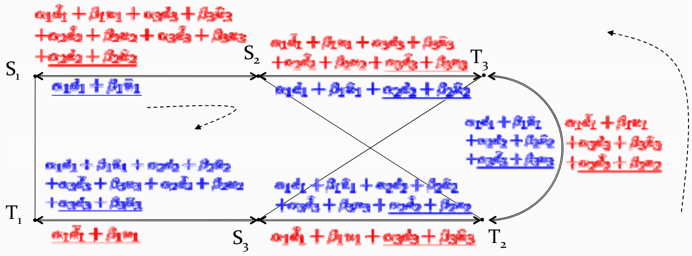
- Number of protection paths only depends on the number of errors and failures
- Multiple unicast connections can share the same set of protection paths, save resource

Network Model and Encoding

- n connections (primary paths), M protection paths
- The i^th^ primary path S_i-T_i
- Paths are bidirectional, with same capacity
- Transmission in rounds; each data unit has a round number
- en(de)coding applies to data units belonging to the same round



Encoding on each protection path:



Data units to the downstream =
Data units from the upstream + a linear combination of available data units
Each node sum the data units from two directions together

Errors on primary path $\hat{d}_i = d_i + e_{d_i}, \hat{u}_i = u_i + e_{u_i}$
Errors on the kth protection path e_{p_k}

Equation obtained by T_i from a protection path k

$$\sum_{l=1}^{n}(\alpha_l^{(k)}e_{d_l}+\beta_l^{(k)}e_{u_l})+e_{p_k}=\alpha_i^{(k)}P_m+P^{(k)}-\beta_i^{(k)}u_i=P_{syn}^{(k)}$$

The system of equations obtained by each node:

$$\underbrace{\overbrace{H=[\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_{2n}]}\quad \overbrace{I_{M\times M}=\{\mathbf{v}_1^p,\ldots,\mathbf{v}_M^p\}}}_{H_{ext}}$$

$$\begin{bmatrix} \alpha_1^{(1)} & \beta_1^{(1)} & \cdots & \alpha_n^{(1)} & \beta_n^{(1)} & 1 & 0 & \cdots & 0 \\ \alpha_1^{(2)} & \beta_1^{(2)} & \cdots & \alpha_n^{(2)} & \beta_n^{(2)} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{(M)} & \beta_1^{(M)} & \cdots & \alpha_n^{(M)} & \beta_n^{(M)} & 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} e_{d_1} \\ e_{u_1} \\ \cdots \\ e_{d_n} \\ e_{u_n} \\ e_{p_1} \\ \cdots \\ e_{p_M} \end{bmatrix} = P_{syn} \qquad (1)$$

Find it

Available at each node

"Syndrome": available but different at each node

Recovery from single error

Each node only wants to recover the data unit sent to it.

Decoding algorithm (At S_i or T_i)

1) Try to solve the system of equations for (e_{d_i}, e_{u_i})

$$HE_i = P_{syn} \Rightarrow [\mathbf{v}_{2i-1}\mathbf{v}_{2i}]\begin{bmatrix} e_{d_i} \\ e_{u_i} \end{bmatrix} = P_{syn}$$

2) If it has a solution, (e_{d_i}, e_{u_i}) is the error; otherwise, no error on S_i-T_i

"iff" Condition: vectors in the sets

$$\{\mathbf{v}_{2i-1}, \mathbf{v}_{2i}, \mathbf{v}_{2j-1}, \mathbf{v}_{2j}\}, \forall i,j = 1,\ldots,n, i \neq j$$
$$\{\mathbf{v}_{2i-1}, \mathbf{v}_{2i}, \mathbf{v}_l^p\}, i = 1,\ldots,n, l = 1,\ldots,M$$

are linearly independent.

- Four protection paths needed
- Coefficient assignments: 1) Simple scheme 2) Vandermonde matrix 3) Random from large field
- Remark: In classical coding theory, to correct two errors, need min distance five; to transmit one symbol, need code length at least five. In our case: one error, two directions, five paths in total (one primary + four protection). We conjecture that we are using near optimal number of protection paths.

Multiple (n_e) errors

Decoding at S_i, T_i

Try to solve the system of linear equations $HE = P_{syn}$ for all possible error value vector E that contain at most n_e errors and an error on S_i-T_i

- ➢ If a solution exists for one of these systems of equations, get the error value
- ➢ If no solution, no error on S_i-T_i

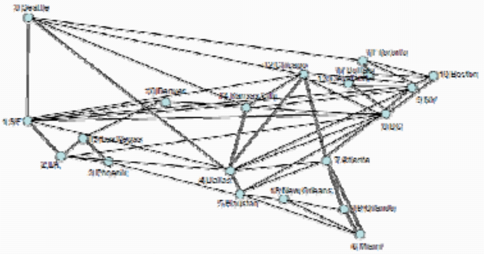
Need $4n_e$ protection paths; Coefficients: randomly from large field

If the errors only happen on primary paths, we can choose H to be the parity check matrix of a $(2n, 2n-4n_e)$ Reed-Solomon code. It satisfies the decodability condition and the decoding becomes RS hard decision decoding problem when the number of errors is up to $2n_e$. Berlekamp-Massey algorithm can be applied and it is more efficient than the previous algorithm.

Combination of errors and failures

Failures on primary paths can be viewed as errors with known locations. And we discard failed protection paths. The decoding algorithm and condition are similar and it requires $M = 4n_e + 2n_f$. Coefficient can be randomly chosen from a large field. If error/failure only happen on primary paths, we can apply(2n, 2n-4ne-2nf) RS code here.

Experimental comparisons

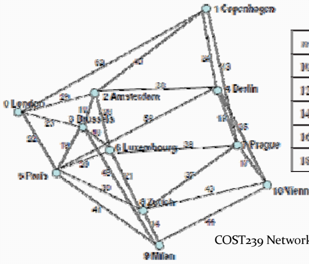


Labo3 Network

Compare our scheme (called 4+n) to 2+1 naïve scheme, in which three paths are provisioned for one connection. The costs for both cases are optimized by integer linear programming.

COMPARISON OF THE AVERAGE COSTS FOR LARNET03 NETWORK

n	Average cost for 4+n (upper bound)	Average cost for 2+1	Percentage gain
10	1826	1916.4	4.72%
12	2106.4	2295.6	8.24%
14	2339.6	2598.8	9.97%
16	2677.6	3049.2	12.19%
18	3105.2	3660	15.16%



COST239 Network

COMPARISON OF THE AVERAGE COSTS FOR COST239 NETWORK

n	Average cost for 4+n (upper bound)	Average cost for 2+1	Percentage gain
10	1226	1245	1.53%
12	1548	1628.4	4.94%
14	1742.4	1854	6.02%
16	1810.8	1958.4	7.54%
18	1883.2	2114.4	10.93%

This work was in part presented in 2009 IEEE International Symposium on Information Theory.
This work is supported by NSF grant CNS-0721453