Redundancy Minimizing Techniques for Robust Transmission in Wireless Networks

Anna Kacewicz and Stephen B. Wicker

Department of Electrical and Computer Engineering
Cornell University

TRUST Fall Conference
November 11, 2008

MOTIVATION

- Wireless networks vulnerable to attacks
  - Passive listening
  - Denial of service
- Necessary for wireless network to be resilient to malicious nodes
  - Reliability in data transmission
  - Security in communication
- Topology of Mobile Ad Hoc Networks constantly changing
  - Pre-determined routing schemes inadequate
  - Important to dynamically determine message dispersion

APPROACH

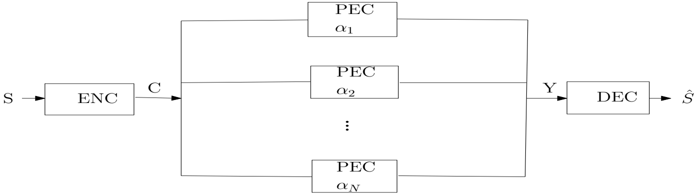
- Information/Coding theory for robustness against compromised pathways
  - Forward error correction coding: MDS codes
- Devise routing scheme based on channel conditions
  - Develop exponential and polynomial time algorithms

PROBLEM STATEMENT

- **Assumption:** There are N paths each with an assigned probability of success
- **Goal:** Transmit message across these paths to attain desired probability of success
- **Question:** What is the minimum redundancy needed and optimal symbol allocation to each path to achieve target success probability?

BASIC ASSUMPTIONS AND DEFINITIONS

- N paths and transmit f_i symbols down path i, which has probability of success $1 - \alpha_i$, all independent from one another.
- Each path is like an erasure channel, either the transmitted symbols are received or they are not.



BASIC ASSUMPTIONS AND DEFINITIONS CONT...

- k symbol message which is to be encoded using an MDS code into n symbols using a systematic representation
- WLOG assume $1 - \alpha_1 \geq 1 - \alpha_2 \geq \ldots \geq 1 - \alpha_N$, implying $f_1 \geq f_2 \geq \ldots \geq f_N$

BASIC ASSUMPTIONS AND DEFINITIONS CONT...

$$P_{success}(\mathbf{f}) = \sum_{s \in S} \prod_{i=1}^{N} (1 - \alpha_i)^{s_i} \alpha_i^{1-s_i} u(s \cdot \mathbf{f} - k) \qquad (1)$$

where $u(\cdot)$ represents the unit step function, and S is the set containing all possible length N combinations of 0's and 1's .

- Running through all possible combinations of $s \in S$ would result in exponential time algorithm $\Rightarrow$ inefficient.

PROBABILITY OF SUCCESS APPROXIMATION

- Each f_i represents the average amount of transmissions attempts to transmit over path i, and in fact follows binomial distribution.
- If we consider all the paths and use the Gaussian approximation, we obtain $\sim \mathcal{N}\left(\sum_{i=1}^{N} f_i(1-\alpha_i), \sum_{i=1}^{N} f_i^2\alpha_i(1-\alpha_i)\right)$

$$P_{success} \approx \frac{1}{2} + \frac{1}{2} erf\left(\frac{\sum_{i=1}^{N} f_i(1-\alpha_i) - k + \frac{1}{2}}{\sqrt{2\sum_{i=1}^{N} f_i^2\alpha_i(1-\alpha_i)}}\right) \triangleq \hat{P}_{success} \quad (2)$$

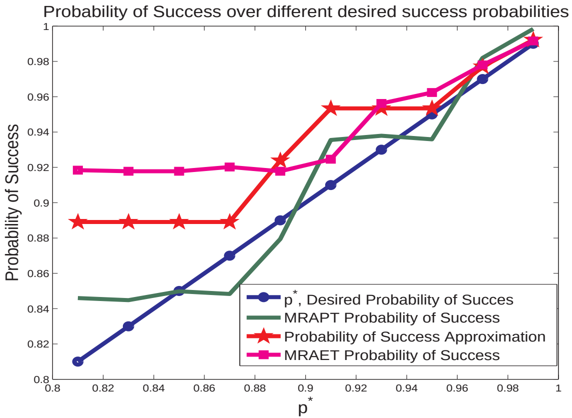
Redundancy and Symbol Allocation Algorithms

- Two algorithms, MRAET and MRAPT (exponential and polynomial time), to make wireless network robust
  - Determine minimum redundancy using MDS codes to achieve desired success probability
  - Allocate symbols to paths based on path success probabilities

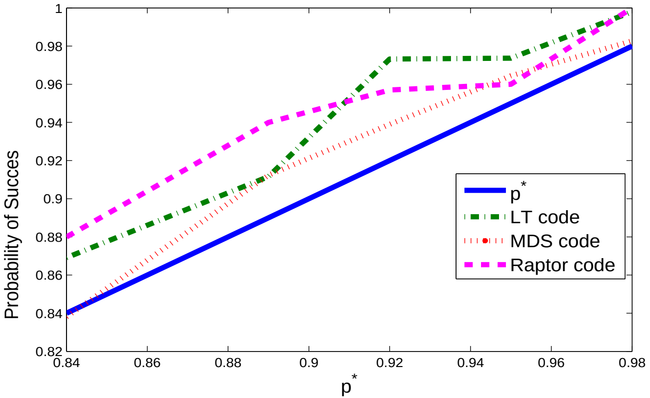
Applications of different codes

- Reed-Solomon codes are MDS codes but have quadratic decoding time
- Fountain codes have an advantage in that they are rateless
  - Well constructed fountain codes are almost MDS
  - LT codes have decoding running time $O(k \log k)$, where k is number of input symbols
  - Raptor codes have running time linear in the message size

SIMULATION RESULTS



SIMULATION RESULTS CONT...



SIMULATION RESULTS CONT...

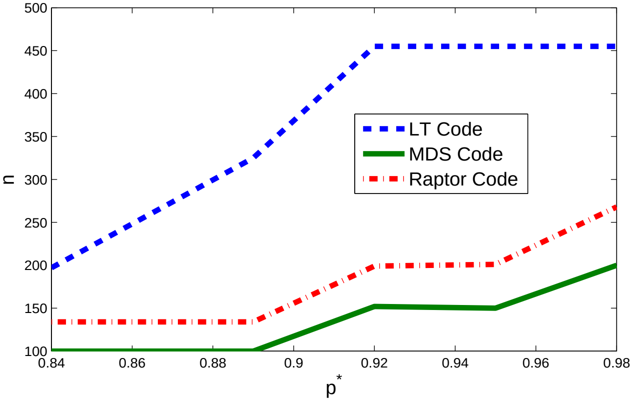


Figure: Total Codeword size for Different Codes using MRAET

SIMULATION RESULTS CONT...

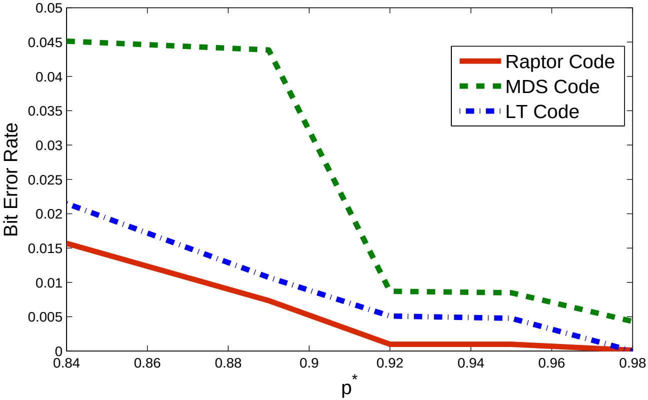


Figure: Bit Error Rate over Different Codes using MRAET

CONCLUSION

- LT codes have greatest robustness but largest overhead
- MDS codes have lowest overhead but highest bit error rate
- Raptor codes have lowest bit error probability

QUESTIONS

THANKS!

MRAET

$$P^A_{success} = \sum_{\mathbf{s} \in A} \prod_{i=1}^{N} p_i^{s_i}(1-p_i)^{1-s_i}$$

Where A is some subset of S. Let,

$$Z_{(i,s)} = \{z \in \{1,\ldots,2^{N-(j-2)}\} \mid \sum_{l=j-1}^{j-2+i} S_{z,l} \geq s\}$$

for some integers s, i. Where $S_{z,l}$ represents the element of S in the z^{th} row and l^{th} column.
Part 1:

Step 1: Assign $j = 1$ and go to step 2.
Step 2: Let $A = S_{\left((2^j+1,\ldots,2^N),(1,\ldots,N)\right)}$ and go to step 3.
Step 3: Calculate $P^A_{success}$.
If $P^A_{success}(\mathbf{f}) \geq p^*$ then save j, let

$$f_1,\ldots,f_j = k, f_{j+1},\ldots,f_N = 0$$

and $\gamma_{\min} = j$, $P_{temp} = P^A_{success}$.
Then go to part 2 of the algorithm.
Otherwise let $j = j+1$ and if $j > N$ move on to Part 2, else if $j \leq N$ return to Step 2.

MRAET CONT...

If $j < 2$ then we have an optimal allocation and we are done. Otherwise:
Part 2:
Let $i = 2$

Step 1: Let $i = i + 1$ and if either $i > N$ or $j - 2 + i > N$ then terminate Part 2, otherwise go to step 2.

Step 2: Let $s = 2$

Step 3: If $j - 2 + \frac{i}{s} \leq \gamma_{\min}$ then
let A denote the subset of matrix S composed of rows whose indices are in $Z_{(i,s)}$ and go to step 4. Otherwise, go to step 6.

Step 4: Calculate $P^A_{success}$
If $P^A_{success} \geq p^*$ with $j - 2 + \frac{i}{s} < \gamma_{\min}$
or
$j - 2 + \frac{i}{s} = \gamma_{\min}$ and $P_{temp} < P^A_{success}$
then go to step 5, otherwise go to step 6.

Step 5: Let $P_{temp} = P^A_{success}$, $\gamma_{\min} = j - 2 + \frac{i}{s}$, and

$f_1, \ldots, f_{j-2} = k$,
$f_{j-1}, \ldots f_{j-2+i} = \frac{k}{s}$,
$f_{j-1+i}, \ldots, f_N = 0$.
Go to step 6.

Step 6: Let $s = s + 1$. If $s > i$ then go to step 1, else go to step 3.