NETWORK CODING TUTORIAL

Emina Soljanin

Comm. & Stat. Research, Bell Labs

Murray Hill, June 2007

WIRELESS NETWORKS

- The medium is shared and networks change in time.
- How does connectivity depend on power?
- State of the art:
  - Simplicity and scalability are the main focus of design.
  - Broadcast nature of wireless medium is not exploited.
- Information theory
  - predicts gains from broadcast and relaying
  - assumes complex non-scalable coding schemes
- Network coding could provide and intermediate solution.
- The first practical applications of network coding could be in ad-hoc wireless networks because of their less rigid protocols.

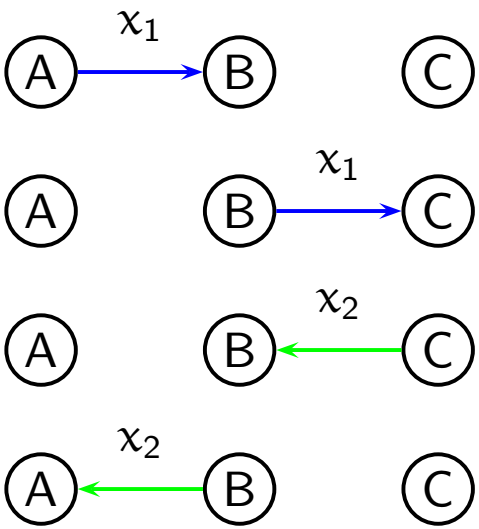
WIRELESS NETWORKS

- Coding reduces delay and energy & bandwidth requirements.
- Example:

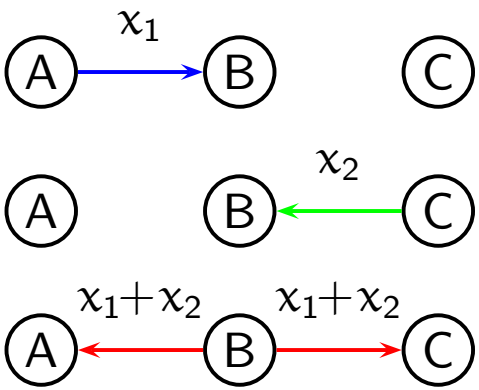


A has x_1 and C has x_2; all three nodes want both x_1 and x_2.

Without Coding



With Coding



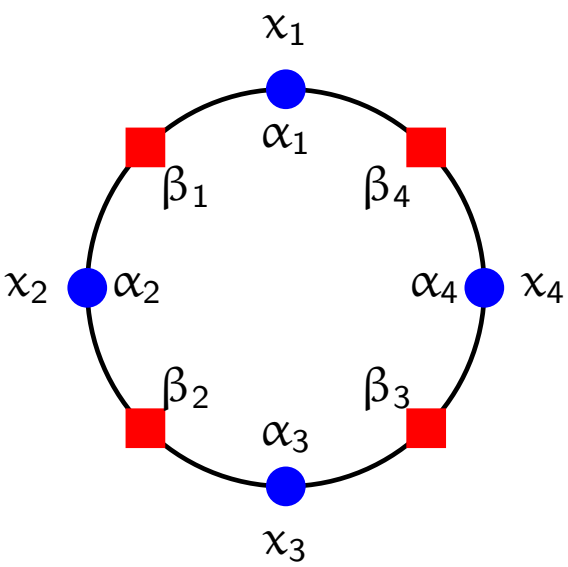
A WIRELESS NETWORK MODEL

- All nodes act as both sources and receivers.
- Each node wants the information from all other nodes.
- Each node can broadcast information to its closest neighbors.
- The total number of transmissions per information unit is
  - N_c with network coding
  - N_r with routing.
- How large are network coding benefits N_r/N_c?

INFORMATION DISSEMINATION IN WIRELESS NETWORKS

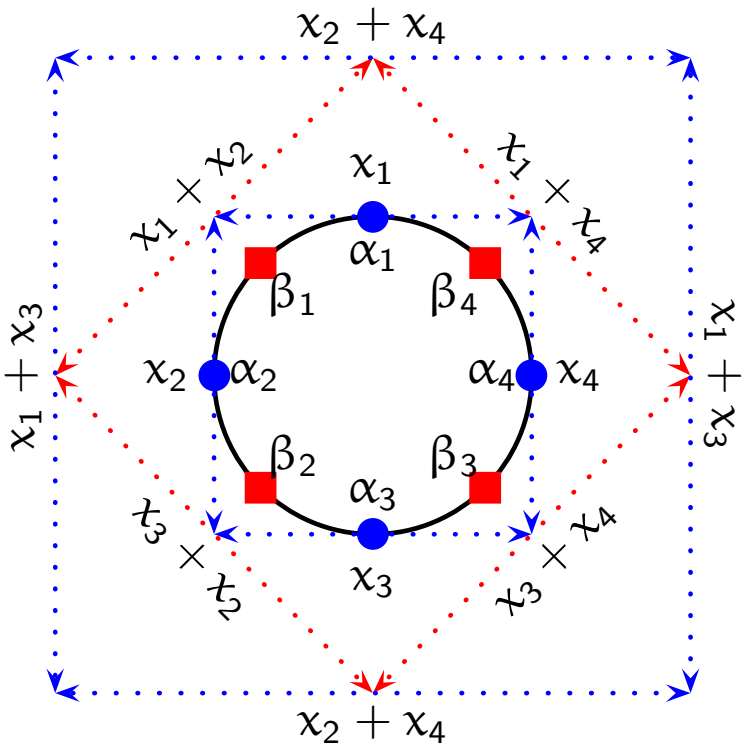
- Think about the coupon collectors's problem.
- Each node can broadcast information to its closest neighbors.
- Topology is often assumed to be fixed and known.
- Topology is often assumed to have some regularity:
  - equidistant nodes on a circle
  - notes on a regular lattice points
  - constant number of neighbors
- More general scenarios are studied by simulation.

Circular Wireless Network



- There are $2n$ nodes (e.g., $n = 4$).
- Nodes can reach the nearest neighbors.
- Claim:
  - $N_r \geqslant 2n - 2$
  - $N_c \geqslant n - 1$

Coding for Circular Wireless Network



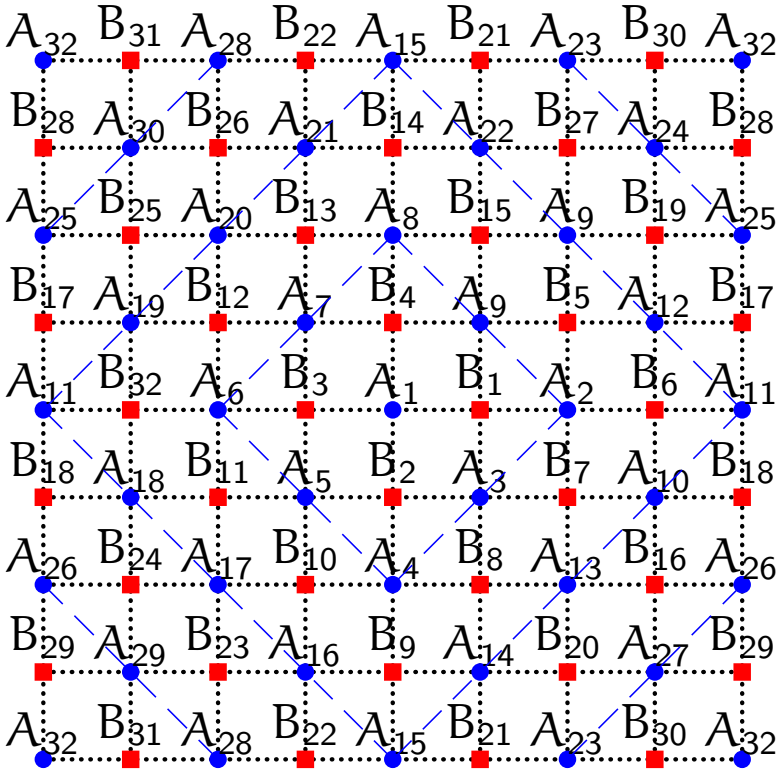
Step $k = 1$

- each α_i broadcasts its x_i.

Step $k > 1$:

- Phase 1 (β's transmit):
  each β_i transmits the sum of the symbols it received in step $k - 1$.
- Phase 2 (α's transmit):
  each α_i transmits the sum of the symbols it received in phase 1.

A Grid Wireless Network



$$N_r \geqslant \frac{4}{3} N_c$$

DECENTRALIZED ALGORITHMS

Square Grid:

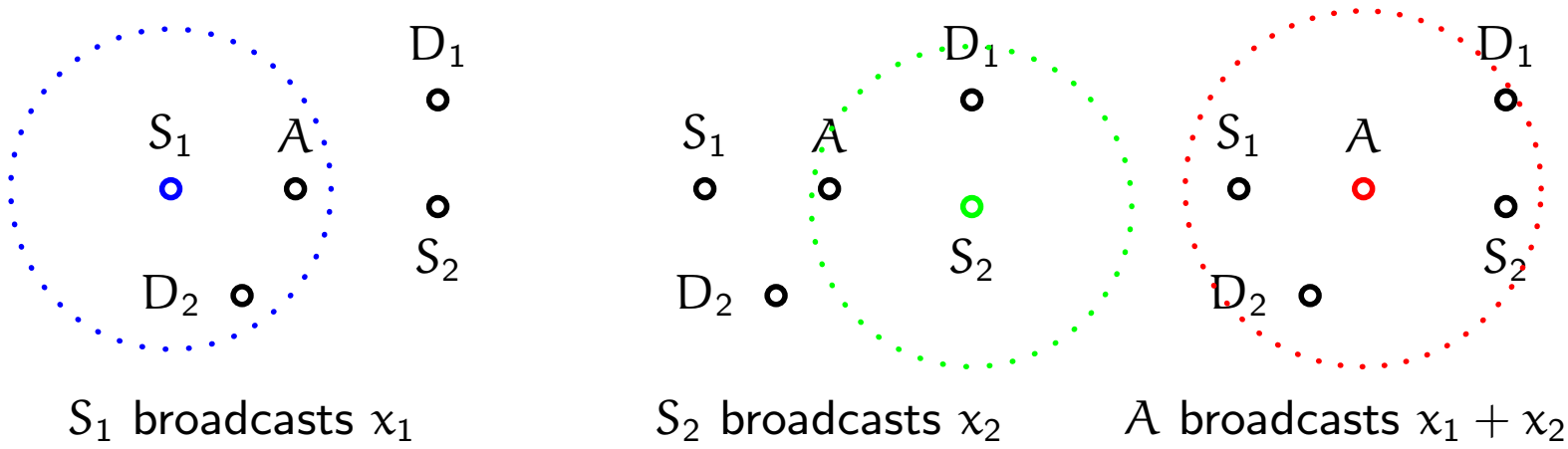
- Each broadcast brings information to c neighbors.
- A node broadcast a random linear combination of all of its packets as soon as it receives c new packets.

Random Network:

- Number of neighbors not constant.
- Nodes keep track of the number of
  - the innovative packet they have accumulated
  - the broadcasts they have performed
- Decision to broadcast is made based on this information, and it also has a random component.

COPE – Example

- Two unicasts (S_1, D_1) and (S_2, D_2), and a common relay A.



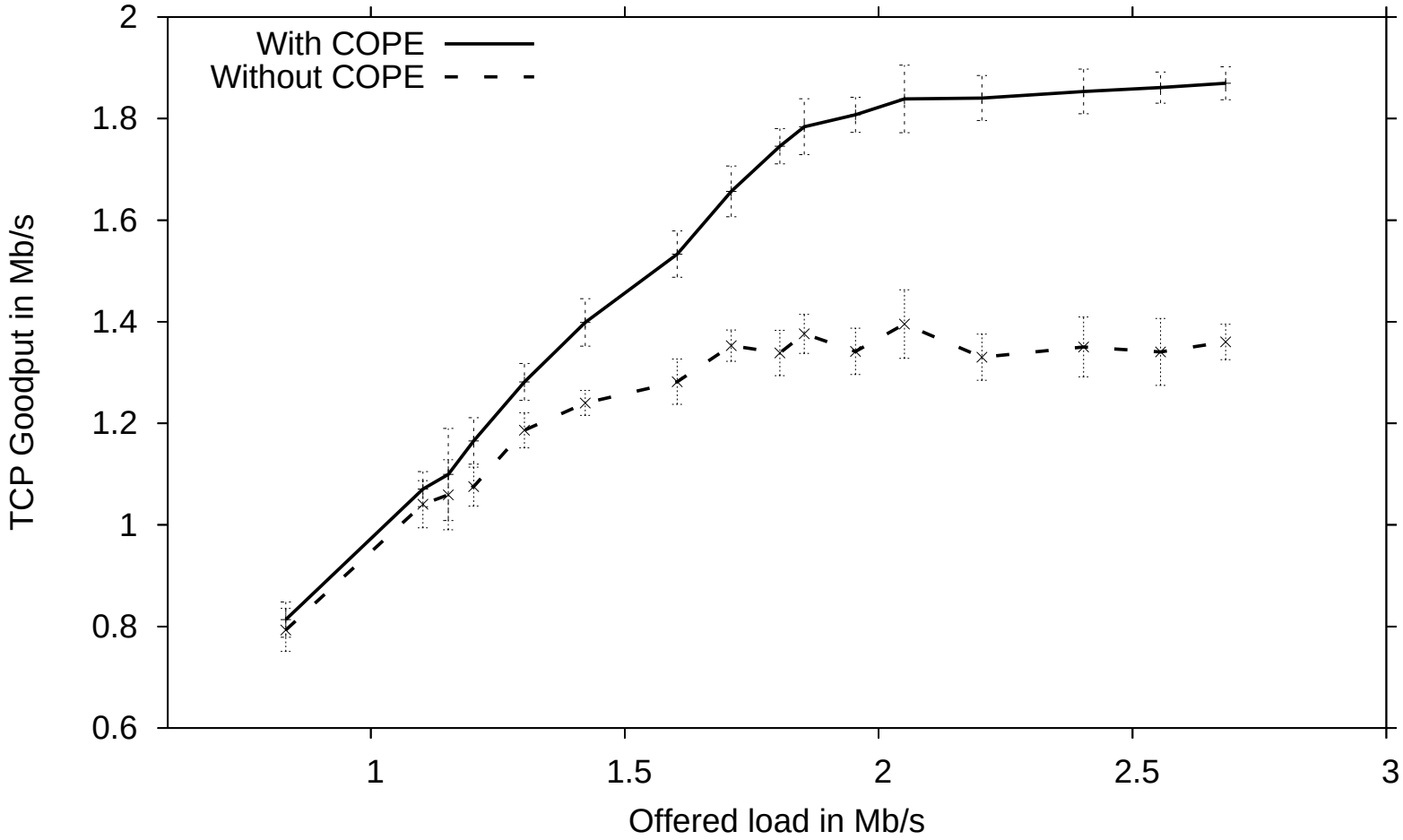
S_1 broadcasts x_1 S_2 broadcasts x_2 A broadcasts $x_1 + x_2$

- Without coding, A becomes a bottleneck, unless it transmits twice as fast as the other nodes, which MAC does not allow.

COPE

- Multiple unicasts and no centralized network knowledge.
- Nodes announce the packets they have successfully received.
- A relay
  - keeps track of each neighbor's a list of received symbols.
  - broadcasts a linear combination of his symbols that
    - may not be innovative for all his neighbors, BUT
    - all the neighbors will be able to immediately decode
- Network coding equalizes requirements on transmission rates.
- MAC layer protocols do not have to deal with bottlenecks.

COPE – Performance



SENSOR NETWORKS – Data Collection

Sensing model and collecting goal:

- n^2 static sensors are placed on an $n \times n$ grid.
- Each sensor node has 4 nearest neighbors.
- Sensors make independent observations x_i, $1 \leqslant i \leqslant n^2$.
- A mobile collector is looking for all observations.

A transmission scheme:

- Phase 1: Each sensor node broadcasts m times.
- Phase 2: The collector queries k sensors uniformly at random.

What can be said about k in terms of n and m if the requirement is that the collected information be sufficient to retrieve all x_i.

Data Collection: Forwarding vs Network Coding

Forwarding:

- In phase 1,

  sensors randomly select and broadcast one of their symbols.
- At the beginning of phase 2,

  each sensor will have at most $4m + 1$ different observations.
- Therefore, $k \geqslant \frac{n^2}{4m+1}$.

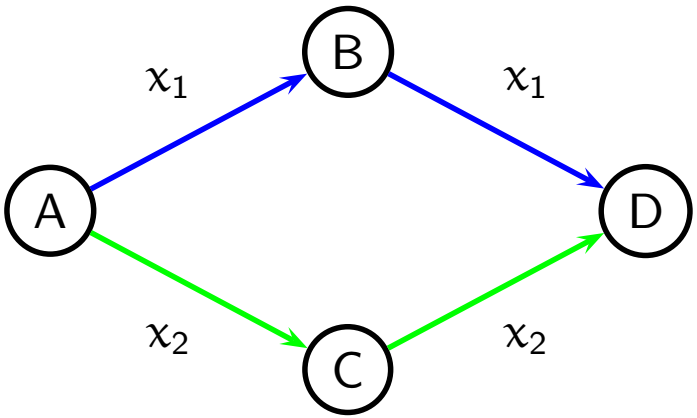
Coding:

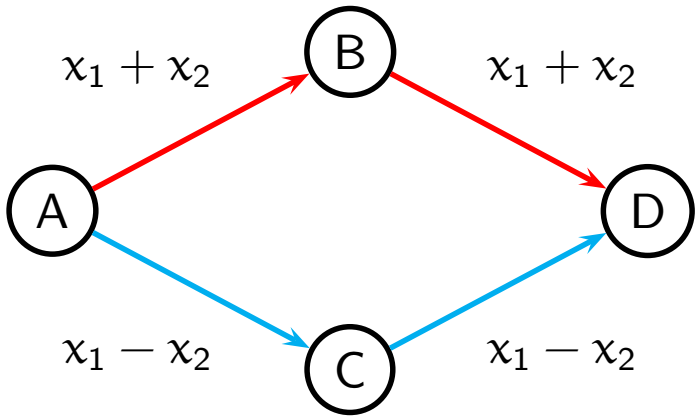
- In phase 1,

  sensors broadcast random linear combinations their packets.
- At the beginning of phase 2 each sensor will have
  - at most $4m + 1$ different packets with
  - $\mathcal{O}(m^2)$ unknown observations
- What can be said about k?

NETWORK CODING AND SECURITY

Q: How does network coding affect security?





A: Network coding affects security both favorably and adversely.

WIRETAP NETWORK II

- Network is represented as a directed, acyclic graph G.
- G has unit-capacity edges and parallel edges are allowed.
- There is a single source node and N receiver nodes, and h edge-disjoint paths between the source and each receiver.
- The network implements a network multicast code.
- The adversary is an eavesdropper who knows the code and can access any μ edges in G.
- How many bits can the source multicast securely?

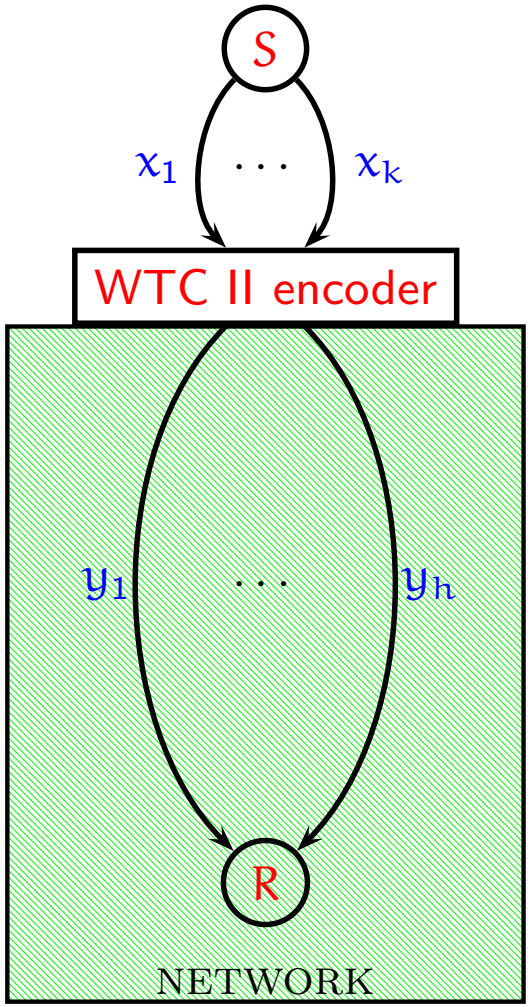
THE SECURITY REQUIREMENT

- Let $W \subset E$ be the set of edges observed by the wiretapper.
- $|W| \leqslant \mu$.
- Random variables of interest:
  - $X = (x_1, x_2, \ldots, x_k)$ denotes the secret information symbols.
  - $Z_W = (z_1, z_2, \ldots, z_\mu)$ denotes the observed symbols.
- Perfect secrecy means

$$H(X|Z_W) = H(X) \quad \text{for all} \quad W \subset E$$

- What is the maximum value that k can take?

WIRETAP CHANNEL II – Unicast



The Ozarow-Wyner soulution:

- $k = h - \mu$ symbols can be transmitted securely.
- Coding scheme is based on an $[h, \mu]$ MDS code.
- k information symbols X specify a coset $\mathcal{V}$.
- Y is chosen uniformly at random from $\mathcal{V}$.

Coding for Wiretap Channel II – Example

- Let $h = 2$, $\mu = 1$, and thus $k = 1$.
- Encode as follows:

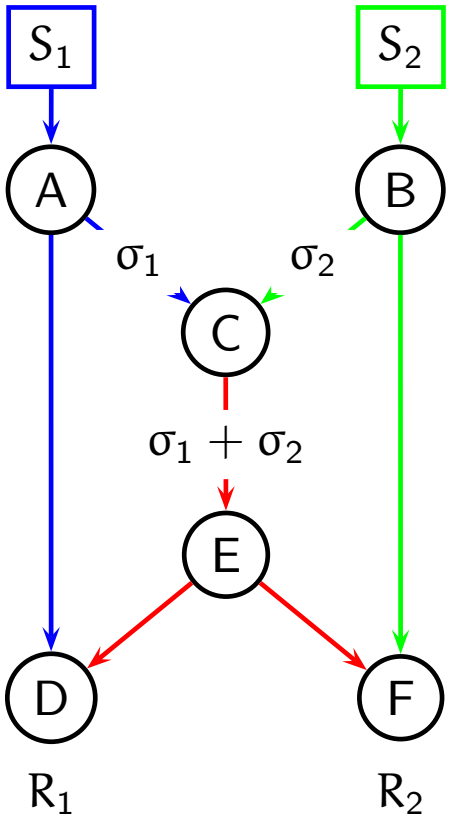
source bit x_1:	0	1
$y_1 y_2$ chosen randomly from:	$\{00, 11\}$	$\{01, 10\}$

- Decode as follows: $x_1 = y_1 + y_2$.
- This scheme is based on the $[2, 1]$ code with the parity check matrix

$$\mathbf{H} = \begin{bmatrix} 1 & 1 \end{bmatrix}$$

- Can such codes be used in wiretap networks?

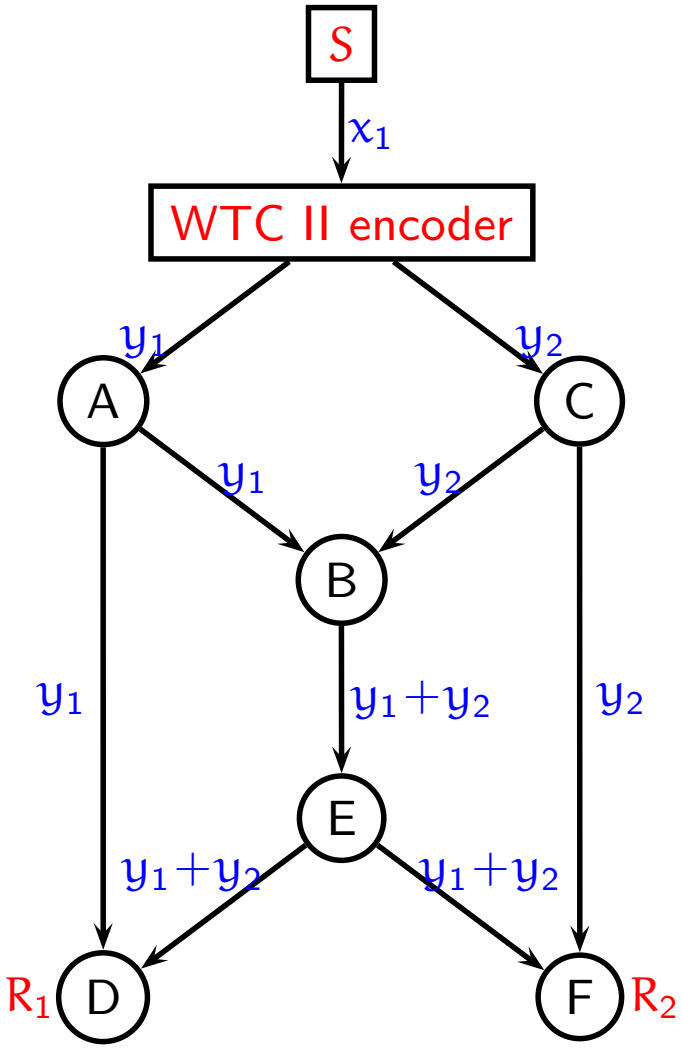
NETWORK MULTICAST – The Butterfly

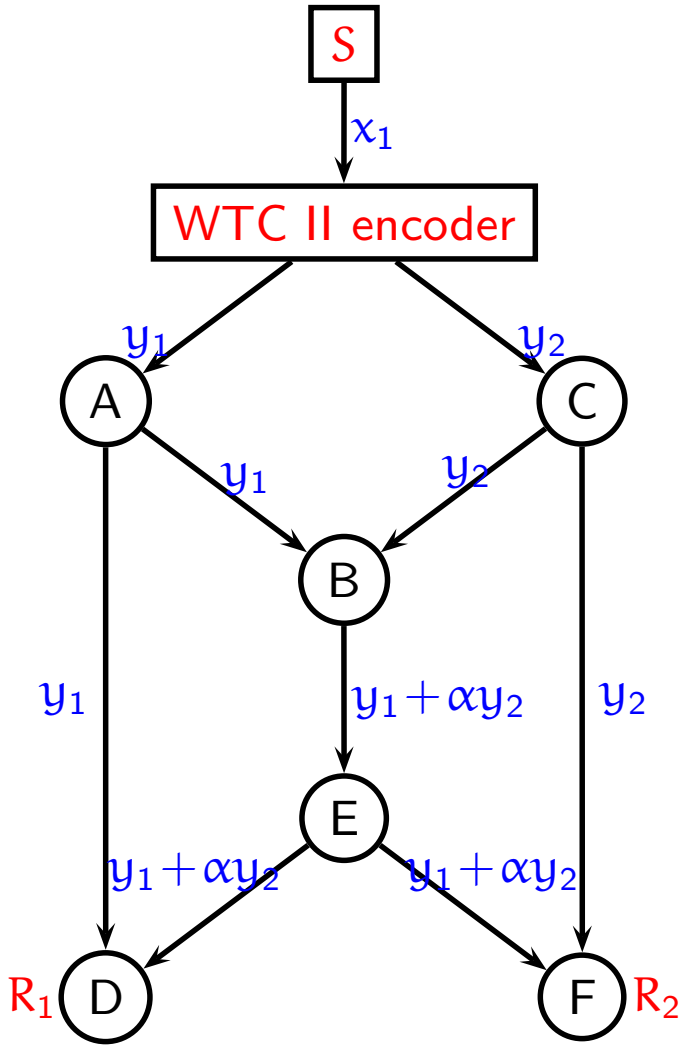


- The edges have unit capacity.
- There are 2 edge-disjoint paths to each receiver.
- Multicast rate of 2 is achievable by coding.

Can 1 bit be transmitted securely by WTC II coding at the source?

WIRETAPPED BUTTERFLY





NETWORK MULTICAST – Linear Combining

- Source S_i emits σ_i which is an element of some finite field.
- Edges carry linear combinations of their parent node inputs.
- Consequently,
  edges carry linear combinations of source symbols σ_i.
- Network Multicast Problem:

  How should nodes combine their inputs to ensure that any h edges observed by a receiver carry h independent linear combinations of source symbols?

THE SECURITY REQUIREMENT

- Let $W \subset E$ be the set of μ edges the wiretapper observes.
- Random variables of interest:
  - $X = (x_1, x_2, \ldots, x_k)$ denotes the secret information symbols.
  - $Y = (y_1, y_2, \ldots, y_h)$ denotes wiretap channel code symbols
  - $Z_W = (z_1, z_2, \ldots, z_\mu)$ denotes denotes the observed symbols.
- Perfect secrecy means $H(X|Z_W) = H(X)$ for all $W \subset E$.
- What is the maximum value that k can take?
- Note:
  - Each edge e carries a linear combination of $y_1, y_2, \ldots, y_h$.
    This linear combination is specified by the coding vector of e.
  - Each x_i is a linear combination of $y_1, y_2, \ldots, y_h$.
    This linear combination is specified by the i-th row of H.

UPPER BOUND ON THE SECURE MULTICAST RATE

- Consider $H(X, Y, Z_W)$:

$$\underbrace{H(X|Z_W)}_{=H(X)} + H(Y|XZ_W) = H(Y|Z_W) + \underbrace{H(X|YZ_W)}_{=0}$$

$$\Rightarrow \underbrace{H(X)}_{=k} = H(Y|Z_W) - \underbrace{H(Y|XZ_W)}_{\geqslant 0}$$

- $H(Y|Z_W) = h - \text{rank}(\mathbf{C}_W)$ giving $k \leqslant h - \text{rank}(\mathbf{C}_W)$
  where the rows of $\mathbf{C}_W$ are the coding vectors of the edges in W.
- Since there is a set of edges W such that
  $\text{rank}(C_W) = |W| = \mu$, we have

$$k \leqslant h - \mu.$$

SECURITY CONDITION ON THE NETWORK CODE

- The bound $k \leqslant h - \mu$ is achieved with equality iff $H(Y|XZ_W) = 0$.
- Equivalently, the system of equations

$$\begin{bmatrix} X \\ Z_w \end{bmatrix} = \begin{bmatrix} \mathbf{H} \\ \mathbf{C}_W \end{bmatrix} \cdot Y$$

  has to have unique solution for all W for which $\text{rank}(\mathbf{C}_W) = \mu$.
- In other words,

$$\text{rank} \begin{bmatrix} \mathbf{H} \\ \mathbf{C}_W \end{bmatrix} = h \text{ for all } \mathbf{C}_W \text{ s.t. } \text{rank}(\mathbf{C}_W) = \mu.$$

CODES FOR WIRETAP NETWORKS

- A secure network code can be designed over $\mathbb{F}_q$

$$q > \binom{|E| - 1}{\mu - 1} + N$$

by using the LIF algorithm.

- A network code can be designed such that not more than

$$O(h^3 N^2 + \delta)$$

edges carry different information (coding points).

- For any configuration with N receivers, the code alphabet $\mathbb{F}_q$ of size

$$q > \binom{h^3 N^2 + \delta}{\mu - 1} + N$$

is sufficient for a secure network code.

FIELD SIZE FOR $h = 2$

- Coding is equivalent to vertex coloring of certain graphs.
- Available colors are the points on the projective line $\mathbb{PG}(1, q)$:

$$[0\,1],\ [1\,0],\ \text{and } [1\,\alpha^i] \text{ for } 0 \leqslant i \leqslant q-2,$$

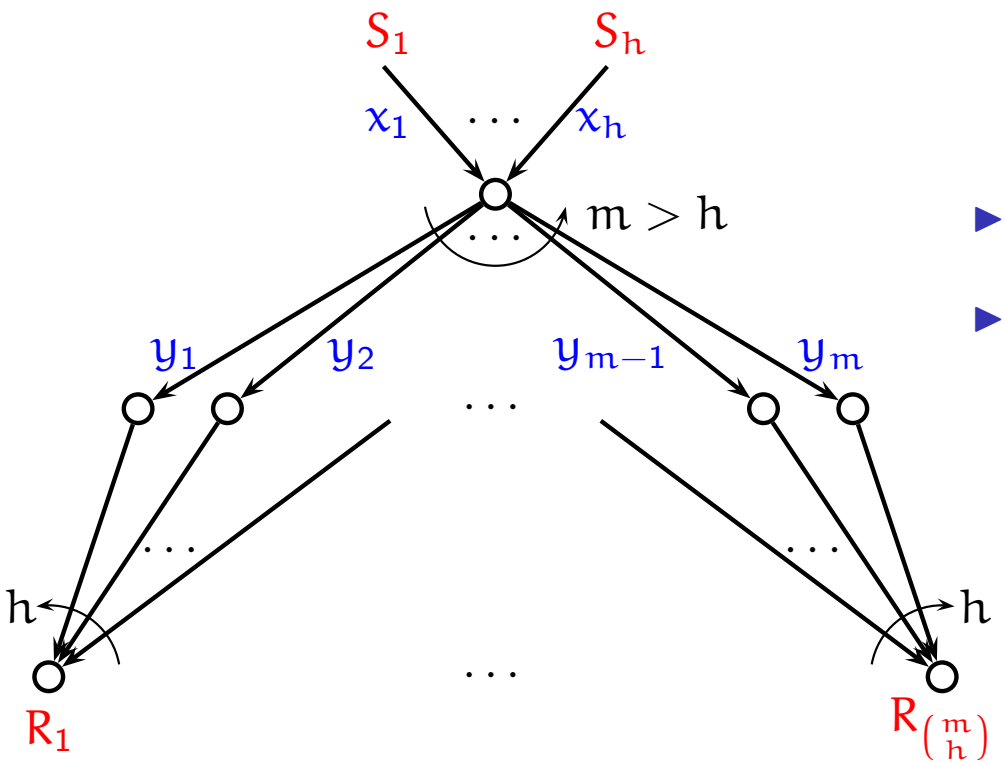
  where α is a primitive element of $\mathbb{F}_q$.
- The field size depends on the chromatic number of the graph.
- WTC II coding takes away one color.
- For any configuration with N receivers, the code alphabet $\mathbb{F}_q$

$$q = \lfloor \sqrt{2N - 7/4} + 1/2 \rfloor + 1$$

  is sufficient for a secure network code.

  There exist configurations for which it is necessary.

Combination Network



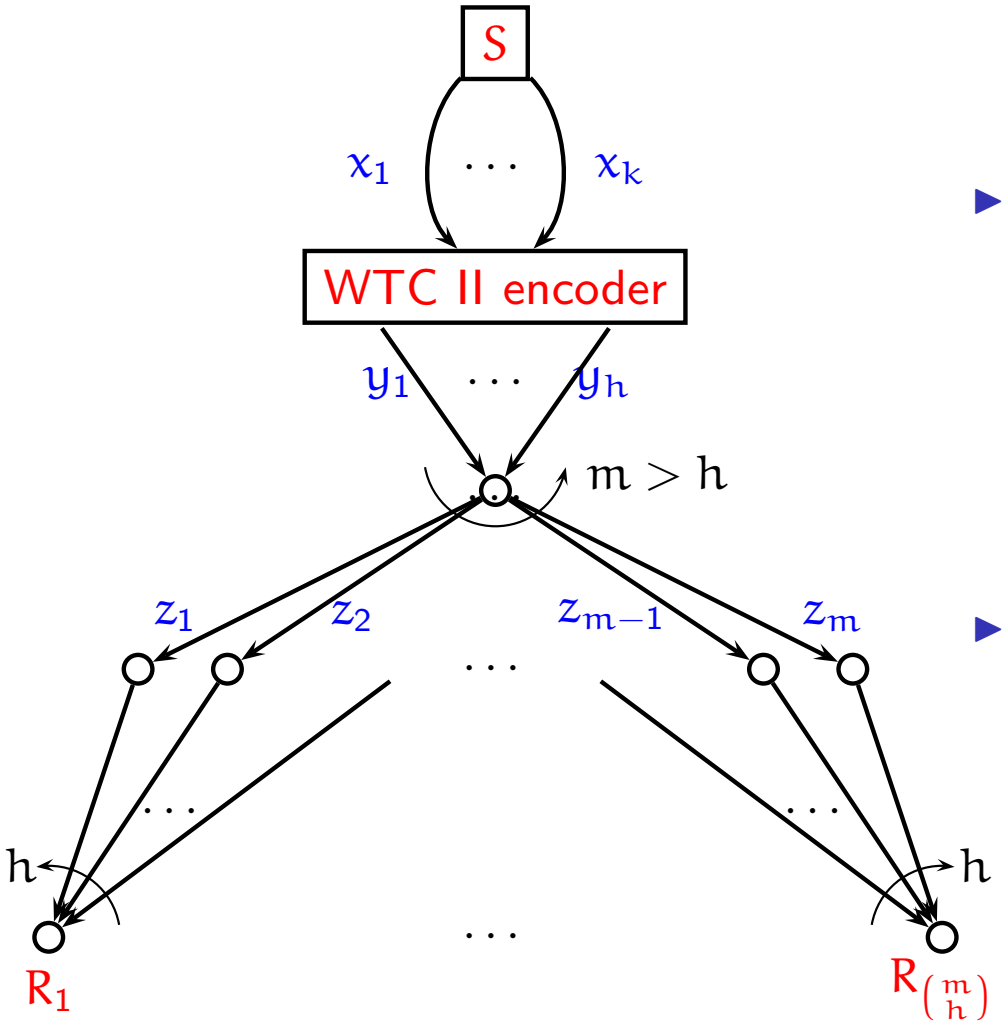
- Assume $x_j \in \mathbb{C}$, $j = 1, \ldots, h$.
- Apply an overcomplete FT to $\{x_j\}$:

$$z_i = \frac{1}{\sqrt{h}} \sum_{j=1}^{h} x_j W_m^{(j-1)(i-1)}$$

where $i = 1, \ldots, m$ and $W_m = e^{\imath \frac{2\pi}{m}}$.

Each receiver has access to h of the m numbers $\{z_i\}$ and can recover $\{x_j\}$.

Secure Combination Network



- Apply an overcomplete FT to $\{y_j\}$:

$$z_i = \frac{1}{\sqrt{h}} \sum_{j=1}^{h} y_j W_{m+k}^{(j-1)(i-1)}$$

where $i = 1, \ldots, m$ and $W_{m+k} = e^{\imath \frac{2\pi}{m+k}}$.

- For $i = m+1, \ldots m+k$, take vectors

$$[1, W_{m+k}^{(i-1)}, \ldots, W_{m+k}^{(h-1)(i-1)}]$$

as rows of matrix $\mathbf{H}$.

When $x_i \in \mathbb{F}_q$, we take an $[m+k, h]$ RS code.