Capacity and queue-based codes for MANET timing channels

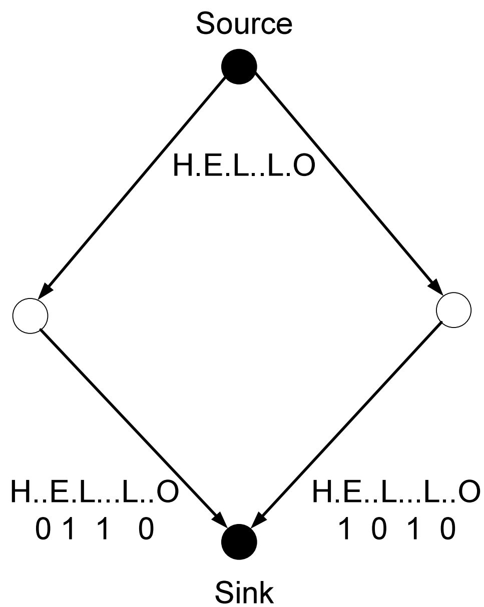
Pierre Moulin

Dept. of Electrical and Computer Engineering

University of Illinois at Urbana-Champaign

July 27, 2007

MANET Timing Channels



- Packet network
- Source and/or relays may covertly transmit information by modulating interdeparture packet times
- Such modulation should be statistically undetectable
- Context: 1) discrete communication; 2) byzantine users
- Status Quo: some IT work on point-to-point

Context: IT Work on Timing Channels

- Network pump (Moskowitz, early 1990s)
- Bits through queues (Anantharam and Verdú 1998)
- Jamming game for timing channels (Giles and Hajek 2002)
- Steganographic capacity (Moulin and Wang 2004, 2007) (maximum rate of reliable transmission for data hiding under *perfect undetectability* condition)

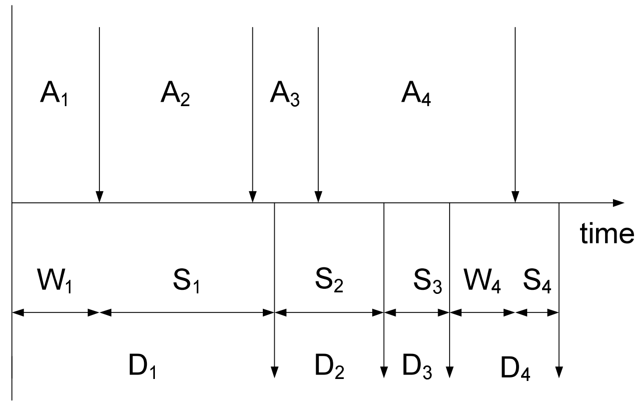
The Problem

- Assume stationary packet arrival times and an iid jitter channel
- What is covert capacity for this problem?
- What is the structure of capacity-achieving codes?
- For MANET-type dynamic environments:
  codes should be adaptive to incoming packet statistics

Achievements

- Upper bound on covert capacity
- Queue-based framework for code construction

A Queueing View of the Problem



- Queue is a nonlinear system with memory:

$$\begin{aligned} \text{Interdeparture times} \quad D_i &= W_i + S_i \\ \text{Idling times} \quad W_i &= \left| \sum_{k=1}^{i} A_k - \sum_{k=1}^{i-1} D_k \right|^+, \quad i \geq 1 \end{aligned}$$

- Inject information by modulating $\{D_i\}$ subject to $D_i \geq W_i$
- $\{A_i\}$ and $\{D_i\}$ should be statistically indistinguishable

A Simple Stochastic Queue-Based Code

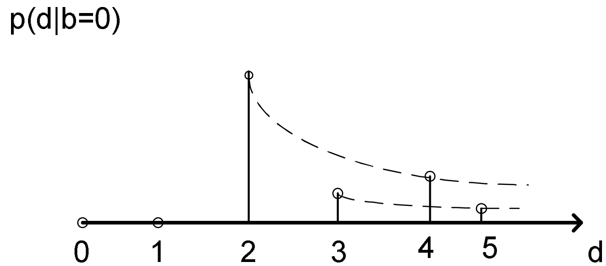
- Assume interarrival times are iid with geometric distribution

$$p(a) = (1 - \lambda\Delta)^{a-1}\lambda\Delta, \quad a = 1, 2, 3, \cdots$$

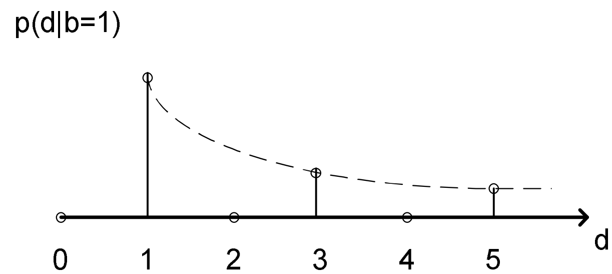
- At time i, transmit information bit b_i by generating d_i from probability distribution $p(\cdot|w_i, b_i)$
- Can design $p(d|w, b)$ such that $\{d_i\}$ are iid and

$$p(d) = (1 - \lambda\Delta)^{d-1}\lambda\Delta, \quad d = 1, 2, 3, \cdots$$

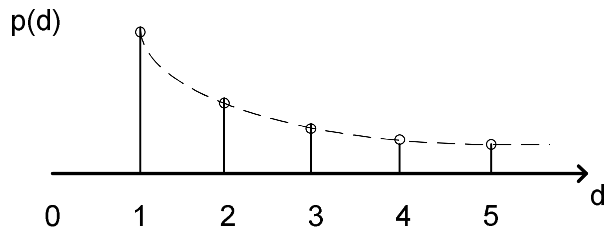
$\Rightarrow$ perfect undetectability



(a)



(b)



(c)

A *perfectly secure, stochastic*, queue-based code with rate $R = 1$. Interdeparture times are generated according to the distributions in (a) and (b), respectively. (c) The mixture distribution is the desired geometric distribution.

Covert Capacity

- Communication with side information at encoder where interarrival times $\{A_i\}$ = side information and $\{Y_i\}$ = output of jitter channel
- Causality constraint: $D_i \geq W_i$ for all $i \geq 1$
- Average-delay constraint:

$$\limsup_{n\to\infty} \mathbb{E} \underbrace{\left[\sum_{i=1}^{n} (D_i - A_i) \right]}_{\text{delay at time } n} \leq \tau$$

- Without causality & delay constraints, would have $C = H(p_A)$
- With constraints: covert capacity $C(\tau) \leq H(p_\tau)$ where p_τ = geometric pmf with rate $\lambda_S(\tau) > \lambda_A$.

Extension to MANETs

- First, are *stochastic* queue-based codes capacity-achieving at the link level?
- Evaluate MANET timing channel capacity
- Couple queue-based coding at link level with network coding at higher level
- In principle this can be done regardless of network topology