Timing Codes with Causal Side Information

Ibtissam Ezzeddine

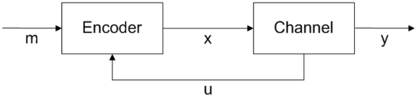
Department of Electrical and Computer Engineering
University of Illinois at Urbana Champaign

Introduction

- **Objective:** Embed hidden messages in time intervals between packets while preserving the characteristics of the underlying timing channel (undetectability).
- **Approach:** Look at a queue based model (for undetectability) and at a family of encoding functions (for embedding the messages).
- **Outline:**
  - A Brief Background about queues and CSI
  - The link between these two and timing codes
  - The algorithm and preliminary results

Channels with Side Information at TX (C.E. Shannon)

- Consider a DMC K with:
  - h independent finite states s $\in$ S $\sim P_s$
  - Causal state information available at TX
  - $p_{ti}(j)$ in state s_t, where $t = 1, \ldots, |S|$, $i = 1, \ldots, |X|$, and $j = 1, \ldots, |Y|$



- Consider an n-length block code with M messages:

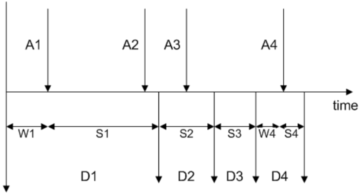
$$x_i = f_i(m; u_1, \ldots, u_i), i = 1, \ldots, n$$

- **Theorem:** Capacity of K= Capacity of K' (without side information) with same output alphabet and an input alphabet with $|X|^{|S|}$ input letters $\Omega = (x_1, \ldots, x_h)$ where $x_i = 1, \ldots, |X|$ and $r_\Omega(y) = r_{x_1,\ldots,x_n}(y) = \sum_{t=1}^{h} p(s_t) p_{tx_t}(y)$

Notation and Queuing Theory Basics

- **Queue:** Nonlinear system with memory
- Lindley equations for a queue:

$$D_i = W_i + S_i,\; W_i = \left|\sum_{j=1}^{i} A_j - \sum_{j=1}^{i-1} D_j\right|^{+},\; i = 1, 2, \ldots$$



- M/M/1 Queue: Geometric interarrival and service times

$$\mu > \lambda, \qquad p(s) = (1-\mu)^s \mu, \qquad s = 0, 1, 2, \ldots$$
$$p(a) = p(d) = (1-\mu)^{d-1}\lambda, \qquad d = 1, 2, 3, \ldots$$

Queue-Based Mappings - Steganographic Codes

- P_{WD} joint distribution of (W,D) over ($\mathcal{W} x \mathcal{D}$) for M/M/1 queue
- u is a mapping: W $\rightarrow$ D
  W$\leftrightarrow$ S and D$\leftrightarrow$X in Shannon's formulation such that

$$P_{WD}(w,d) = P_W(w) \sum_{u \in U} P_U(u) P_{D|UW}(d|u,w) \qquad \forall d, w$$

- Let $\mathcal{P}_U(P_{WD})$ be the set of feasible probability distributions over U. Find P_u that maximizes I(U;D) over $\mathcal{P}_U(P_{WD})$
- COMPUTATIONALLY HARD!!!! (Continuum of mappings)

Algorithm

- Consider a set of N mappings $u_1, \ldots, u_N \in$ a certain family of mappings (Ex: mappings of even/odd w are symmetric)
- Find p_u supporting N points such that $A_{|W||D|xN} P_u = P_{WD}$ where $A = [u_1, \ldots, u_N]$
- Compute I(U;D)
- Iterate to get a better mutual information

Preliminary Results

- A: Interarrival time
  S: Service time
  $P_S(s)$: Truncated (at t) geometric service time distribution with μ=0.5
  $P_A(a)$: Truncated (at t) geometric interarrival time distribution with λ=0.3
  N=t^2
-

t	H(A)	Maximum Achieved I(U;D)
5	2.1524	1.3050
6	2.3454	1.3095
7	2.4904	1.2959
8	2.6001	1.2782
9	2.6835	1.2665

Conclusion

- **Happiness Condition:** Find a "Good" set of encoding functions (mappings) while ensuring a certain level of undetectability.
- Thank You!!!