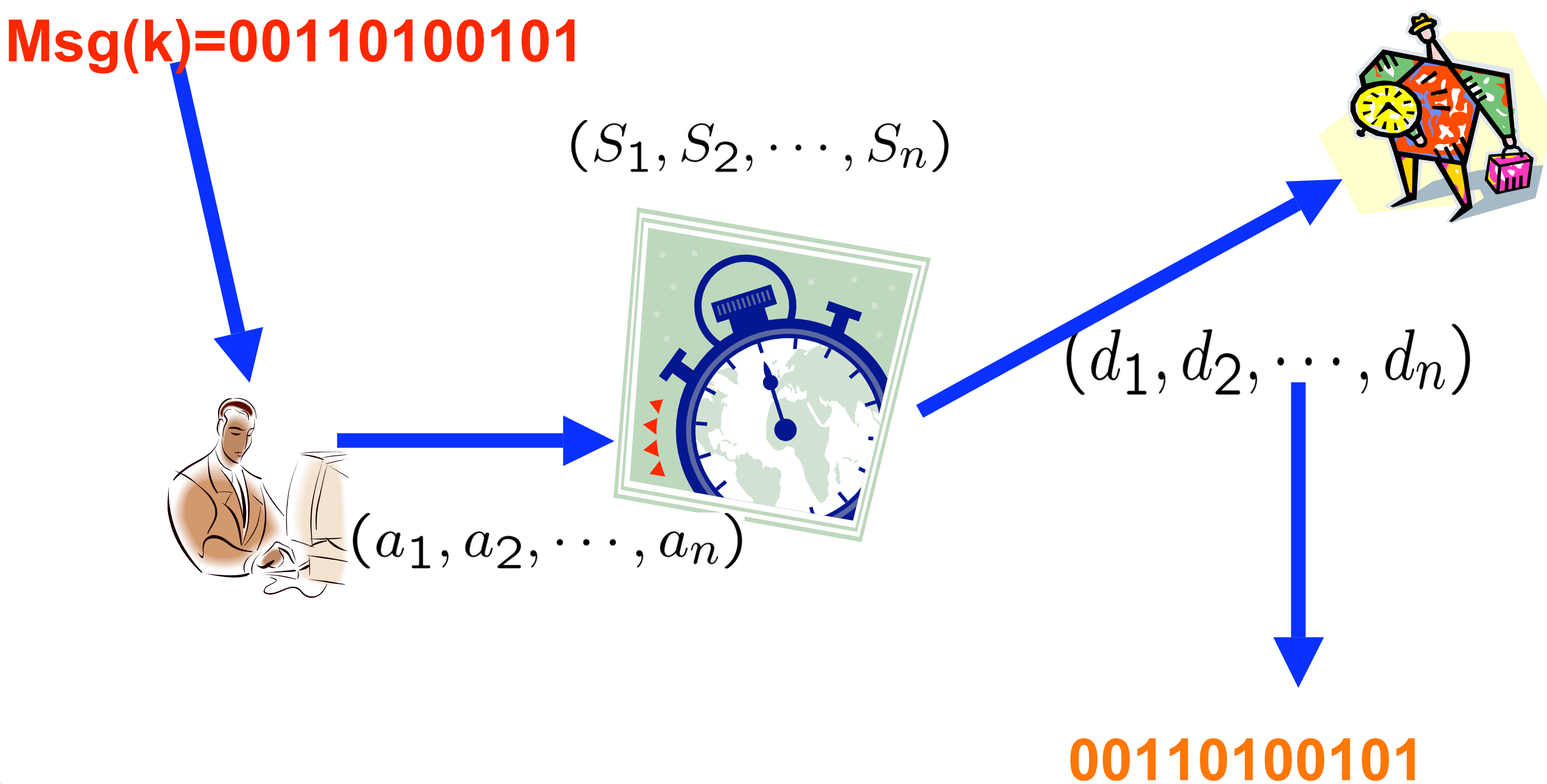
Capacity Bounds on Timing Channels with Bounded Service Times

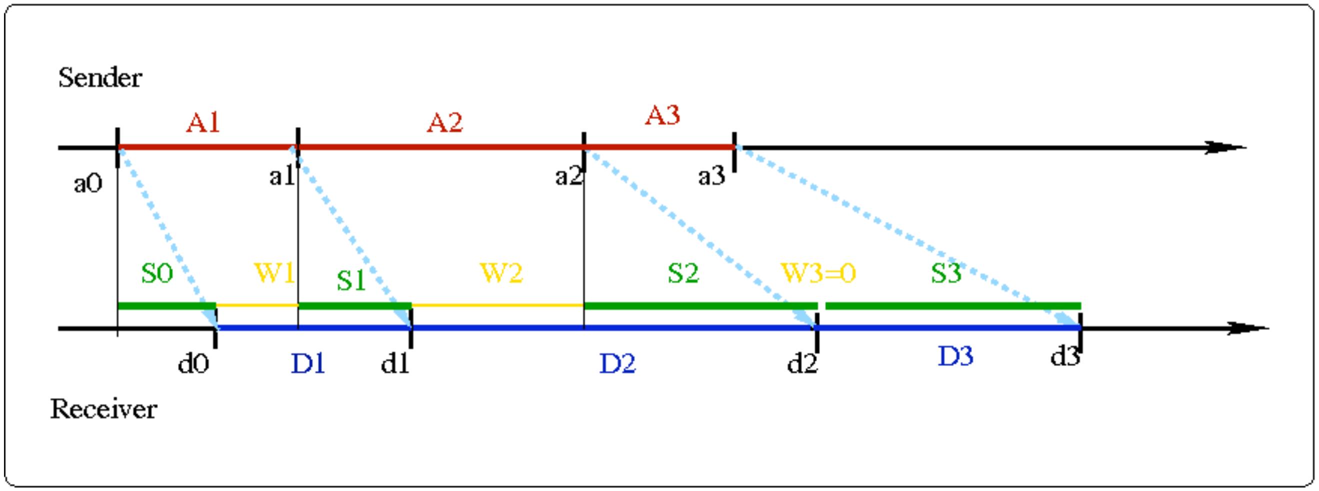
S. Sellke, C.-C. Wang, N. B. Shroff, and S. Bagchi

School of Electrical and Computer Engineering
Purdue University, West Lafayette, IN 47907
USA

What are Timing Channels?



Timing Channels



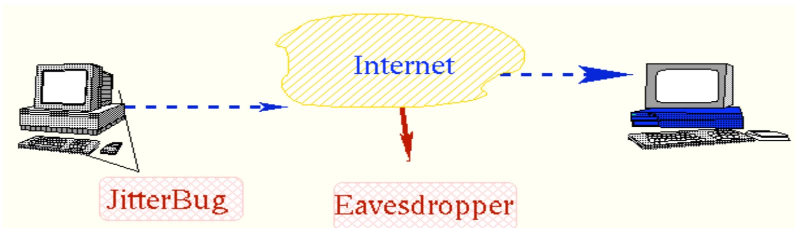
- Information is conveyed in the timing of the bits
  - Sender: $a_0, a_2, \ldots, a_{n-1.}$
  - Server: $S_0, S_2, \ldots, S_{n-1}$
  - Receiver: $d_0, d_1, \cdots, d_n$; and recovers information.

Applications of Timing Channels

- Keyboard JitterBug [1]

  [1] G. Shah *et al*, Keyboards and Covert Channels, 2006

  Best Student Paper Award, 15th USENIX Security Symposium



- Implement timing channels using on-off technique over TCP/IP networks [2]

  [2] S. Cabuk *et al*, IP Covert Timing Channels: Design and Detection, 2004

- Covert Timing Channels in Multi-Level Security (MLS) Systems [3],[4]

  [3] U. S. Department of Defense, ``The Orange Book", 1985

  [4] J. Wray, An Analysis of Covert Timing Channels, 1991

PURDUE UNIVERSITY

Exponential Service Timing Channel

- ESTC: Service times S_1, S_2, … are *iid* exponential random variables with parameter μ.

- Capacity of ESTC:

$$C_{ESTC} = e^{-1}\mu \quad nats$$

- Capacity of others: $$C \geq C_{ESTC}$$

  - Deterministic Service Timing Channels have *infinite* capacity, even if *service time is large*.

A. Anantharam and S. Verdu, “Bits through Queues,”, 1996

PURDUE UNIVERSITY

Bounded Service Timing Channels

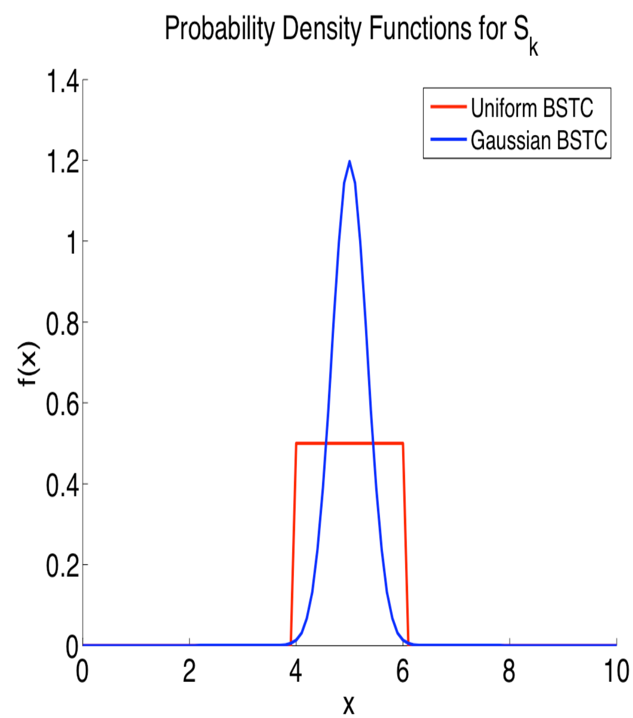
- BSTC: service times S_1, S_2, $\cdots$, S_n are *iid* with bounded support.
  - General BSTC:

$$P(a < S_k < a + \Delta) = 1$$

  - Symmetric BSTC

$$P(\frac{1}{\mu} - \epsilon < S_k < \frac{1}{\mu} + \epsilon) = 1$$

  - Examples of BSTC:
    - Uniform BSTC
    - Gaussian BSTC



Lowest capacity BSTC?

- Is there a particular BSTC that serves a role similar to that of ESTC?

  That is, it has the *lowest* capacity among all BSTC with same service rate and support interval.

Our Contributions

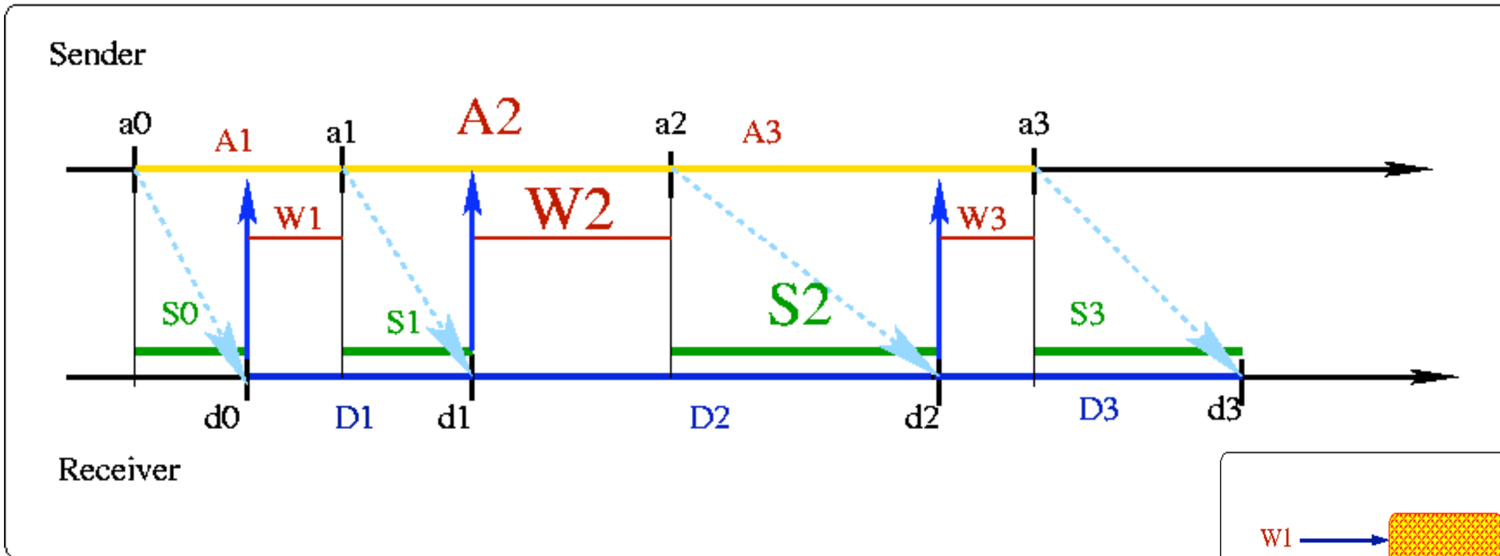
- An upper bound $C_{U,P_S} : C_{U,P_S} \geq C_{BSTC,P_S}$

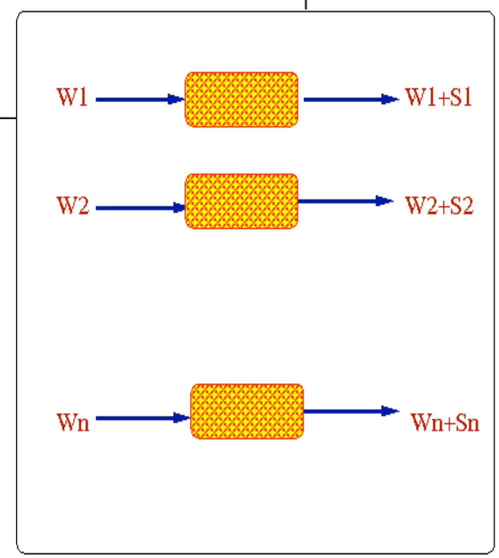
- Two lower bounds $C_{L,1}$ and $C_{L,2}$
  - $C_{L,1}$: $C_{L,1} \leq C_{BSTC,P_S}$ for all P_S.
  - $C_{L,2}$: $C_{L,2} \leq C_{BSTC,P_S}$ for all P_S.

- For the uniform BSTC,
  - $C_{U.BSTC} - C_{L,2} \rightarrow 0$ as $\epsilon \rightarrow 0$
  - $C_{U. BSTC} - C_{L,1} <$ const. for all ϵ
  - $C_{U.BSTC} < C_{BSTC}$: serves role similar to ESTC

PURDUE UNIVERSITY

Timing Channels with feedback





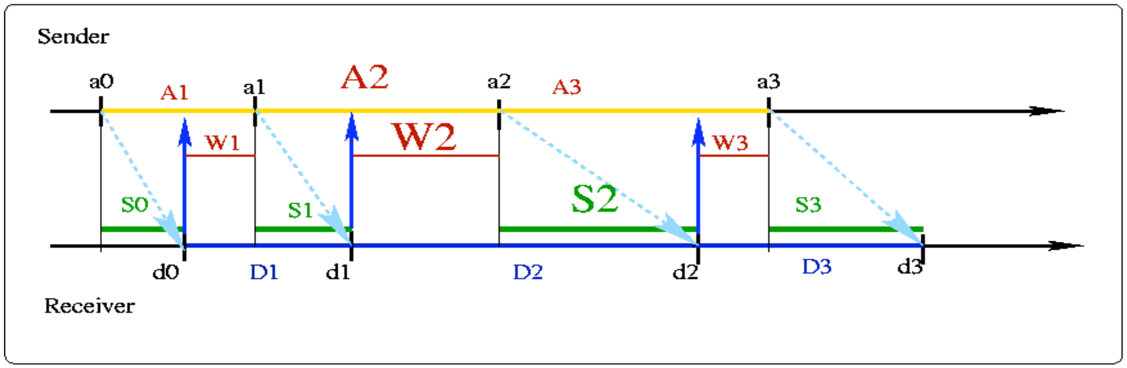
- With Feedback:
  - The sender knows d_{k-1} before deciding a_k
  - Thus, the sender has full control of W_k
  - ***FB channel is reduced to a sequentially juxtaposed iid channel:***

$$W_k \rightarrow W_k + S_k = D\_k$$

PURDUE UNIVERSITY

An Upper Bound on the Capacity

New i.i.d Channels: $W_k \rightarrow W_k + S_k$



$$C_{FB} = \sup_{W_k \geq 0,\ \text{fixed } E[D_k]} \lambda I(W_k; W_k + S_k)$$

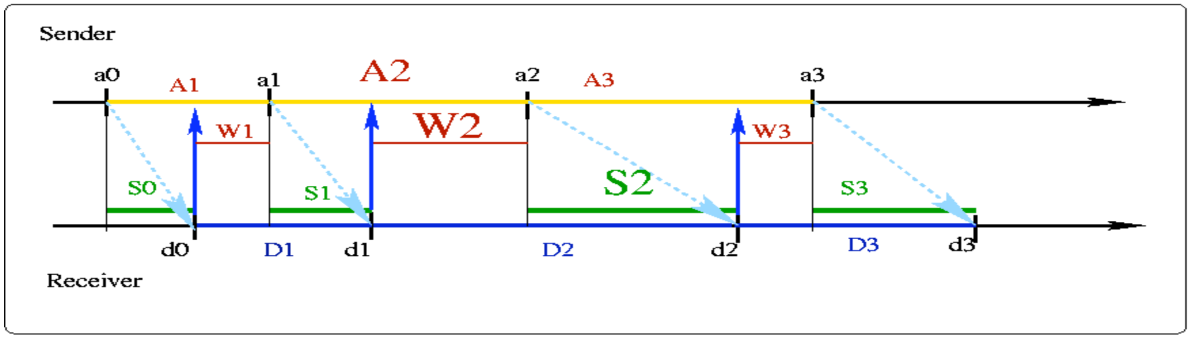
where $\lambda = \frac{1}{E[D_k]}$ (inter-departure rate)

Recall: $\mu = \frac{1}{E[S_k]}$ (service rate)

$$E[D_k] = E[W_k + S_k] = E[W_k] + 1/\mu \Rightarrow E[W_k] = 1/\mu - 1/\lambda$$

PURDUE UNIVERSITY

An Upper Bound



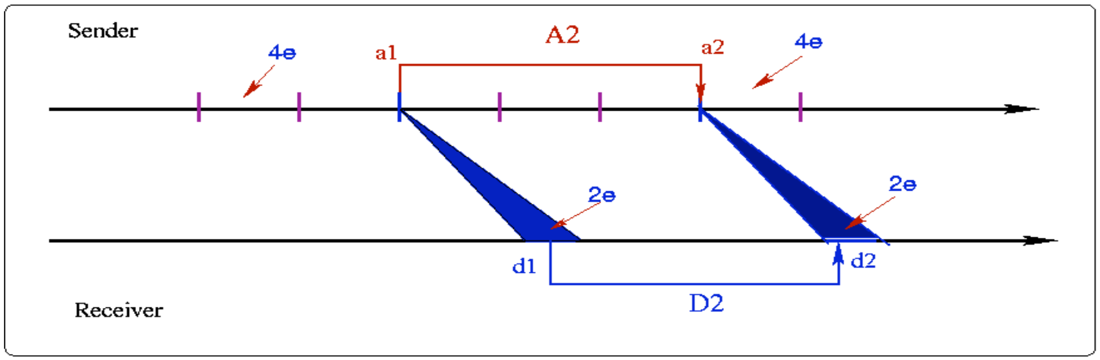
$$C_{U,P_S} = C_{FB} = \sup_{W_k \geq 0} \lambda I(W_k; W_k + S_k)$$

$C_{U,P_S}(\epsilon) = \mu \sup_{0<\gamma<1} G(\epsilon, \gamma)$ bits/sec,

where $\gamma = \lambda/\mu$ and

$$G(\epsilon,\gamma) = \gamma[\log_2(\epsilon\mu+1/\gamma-1)+\log_2(e)-\log_2(\mu)-h(S_k)]$$

Achievability: Scheme 1



- A_k : geometric r.v.
  - $A_k \geq 1/\mu + \epsilon$ to avoid queueing
  - $D_k = (a_k + 1/\mu \pm \epsilon) - (a_{k-1} + 1/\mu \pm \epsilon) = A_k \pm 2\epsilon$
    - Values for A_k are spaced 4ϵ apart for error-free decoding

$$P\{A_k = (1/\mu + \epsilon) + i(4\epsilon)\} = p_1(1-p_1)^i, \quad i = 0, 1, 2 \cdots$$

PURDUE UNIVERSITY

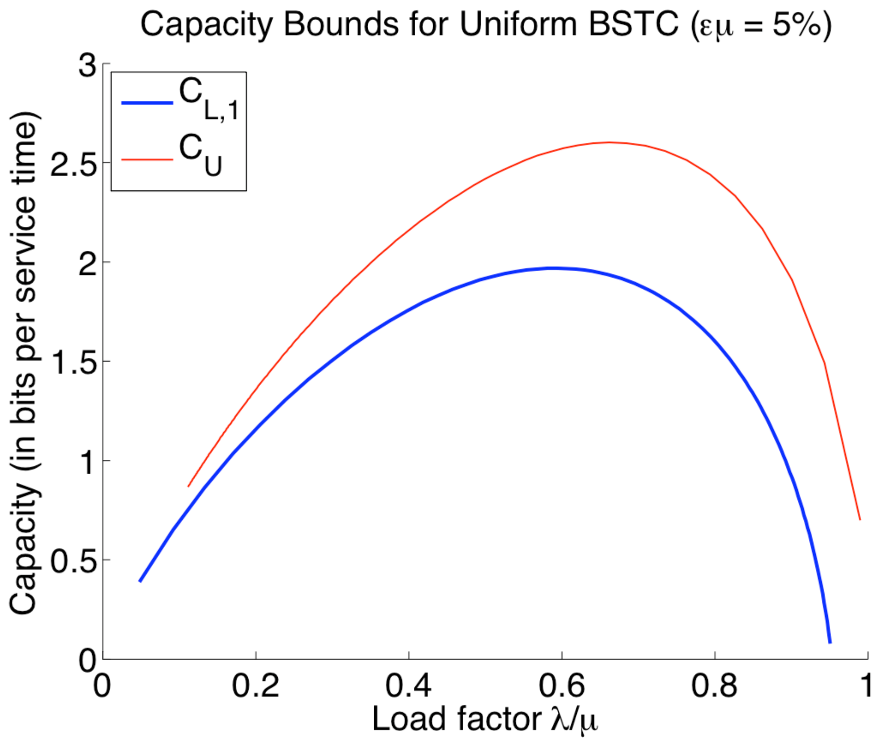
$C_{L,1}$ (ϵ): the First Lower Bound

- Error-free rate of scheme 1:
  - $C_{L,1}(\epsilon) = \mu \sup_{0<\gamma<1/(1+\epsilon\mu)} \gamma\,[H(p_1)/p_1]$ bits/sec

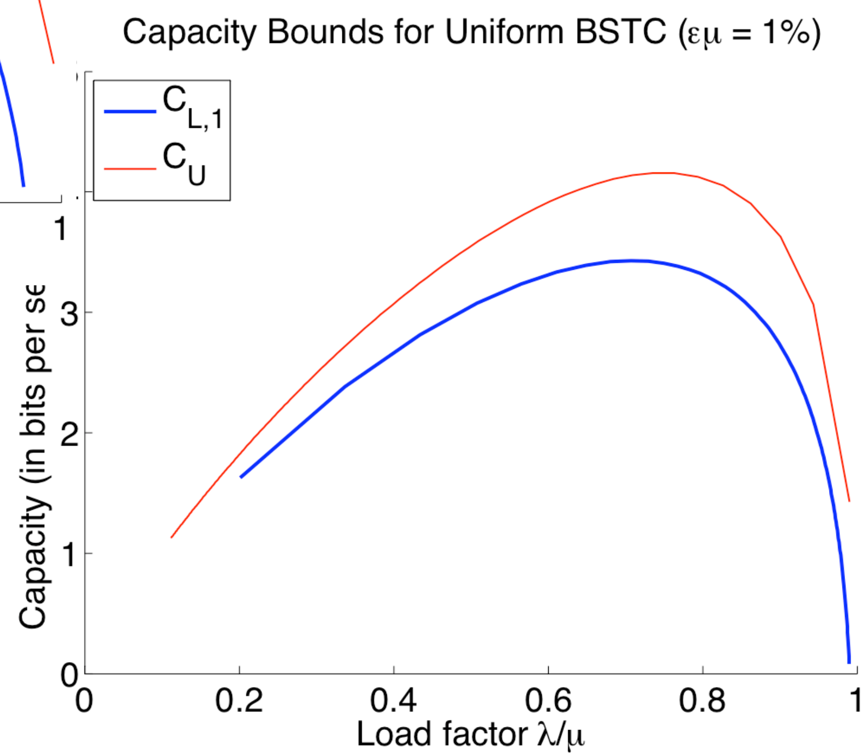
    where

    $$p_1 = (4\epsilon\mu)/(1/\gamma - 1 + 3\epsilon\mu)$$

$$C_{L,1}(\epsilon) \leq C_{BSTC,P_S} \quad \text{for all} \quad P_S.$$



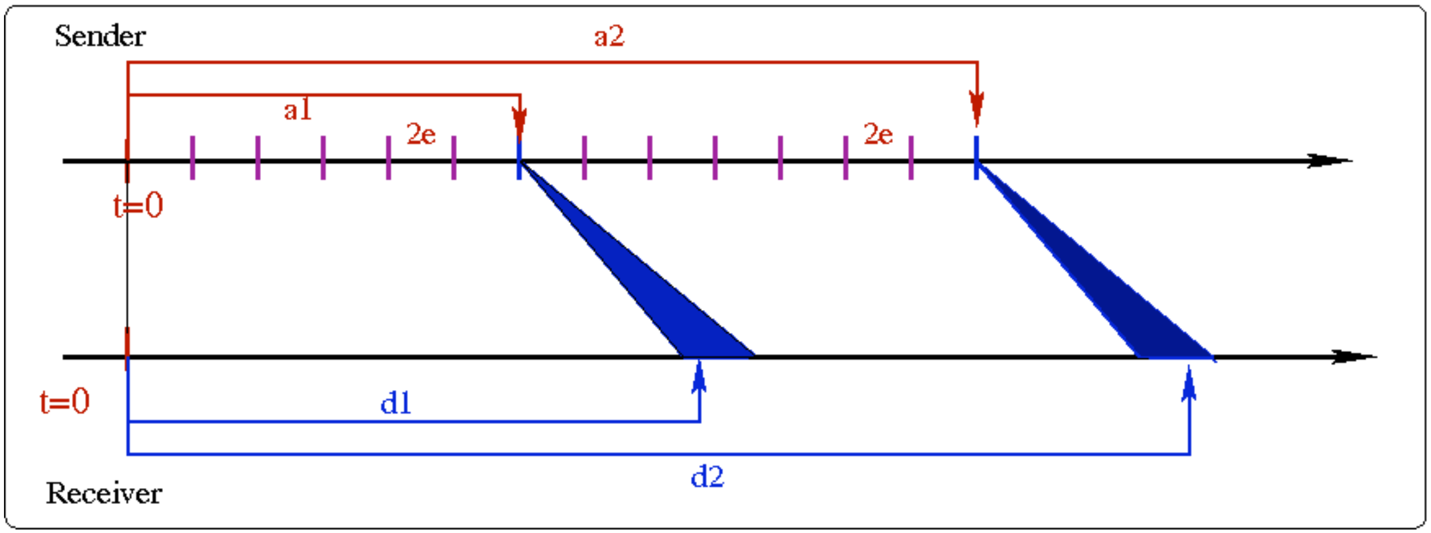
Capacity Bounds for Uniform BSTC (εμ = 5%)
Capacity (in bits per service time)
Load factor λ/μ
$C_{L,1}$
C_U
0
0.5
1
1.5
2
2.5
3
0
0.2
0.4
0.6
0.8
1



Capacity Bounds for Uniform BSTC (εμ = 1%)
Capacity (in bits per se
Load factor λ/μ
$C_{L,1}$
C_U
0
1
2
3
0
0.2
0.4
0.6
0.8
1

Achievability: Scheme 2

- If the *absolute timing* information is *available* to both sender and receiver.



- $d_k = a_k \, ^{+}/_{-} \, \epsilon$ for $k = 1, 2, \cdots \Rightarrow$ error-free decoding
- With long codeword length, the absolute timing can be obtained with arbitrary precision.

PURDUE UNIVERSITY

$C_{L,2}(\epsilon)$: The Second Lower Bound

- Error-free rate of scheme 2:
  - $C_{L,2}(\epsilon) = \mu \sup_{0<\gamma<1/(1+(1+2\alpha)\epsilon\mu)} \gamma\,[H(p_2)/p_2]$ bits/sec

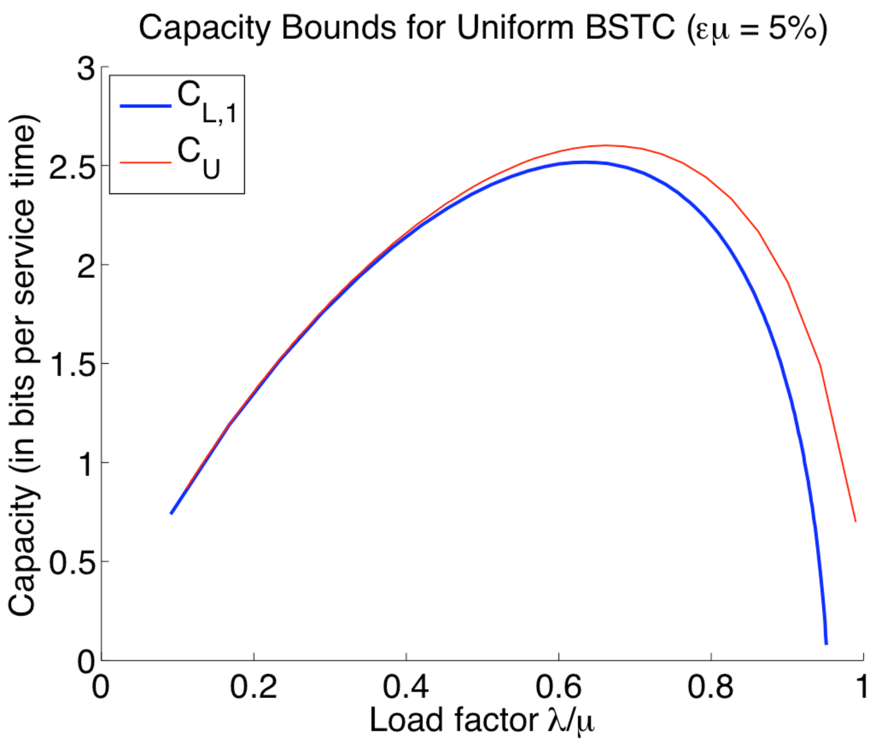
    where

    $p_2 = (2\epsilon\mu) / (1/\gamma - 1 + (1-2\alpha)\epsilon\mu)$

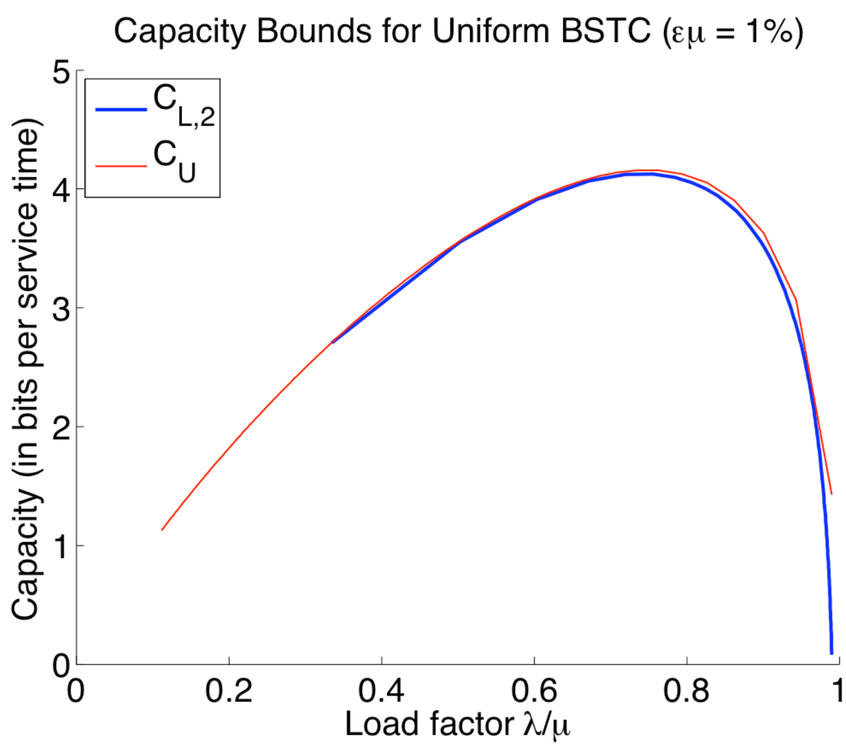
    $\alpha = [\beta] - \beta$, and $\beta = (1+\epsilon\mu)/(2\epsilon\mu)$

$$C_{L,2}(\epsilon) \leq C_{BSTC,P_S} \quad \text{for all} \quad P_S.$$

PURDUE UNIVERSITY



Capacity Bounds for Uniform BSTC (εμ = 5%)
Capacity (in bits per service time)
Load factor λ/μ
C_L,1
C_U



Capacity Bounds for Uniform BSTC (εμ = 1%)
Capacity (in bits per service time)
Load factor λ/μ
C_L,2
C_U

Optimality of Our Schemes

- Define:
  - $\Delta\, C_1(\epsilon) = C_u\,(\epsilon) - C_{L,1}\,(\epsilon)$
  - $\Delta\, C_2(\epsilon) = C_u\,(\epsilon) - C_{L,2}\,(\epsilon)$

- Results on Uniform BSTC:
  - $\Delta\, C_1(\epsilon) < \log_2(e)\, \mu$ bits/sec
  - $\Delta\, C_2(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$

Capacity of a Uniform BSTC

- For a uniform BSTC
  - $\Delta C_1(\epsilon) < \log_2(e)\,\mu$ bits/sec

$$\Rightarrow C_{U.BSTC}(\epsilon) = C_{L,1}(\epsilon) + O(1)$$

  - $\Delta C_2(\epsilon) \to 0$ as $\epsilon \to 0$

$$\Rightarrow C_{U.BSTC}(\epsilon) = C_{L,2}(\epsilon) + o(1)$$

- **Scheme 2 is optimal;**
- **When ϵ is small, the uniform BSTC has the <u>smallest</u> capacity among all BSTCs with same μ and ϵ.**

PURDUE UNIVERSITY

Gaussian BSTC

- $C = C_{L,2} + o(1)$ does not hold for G. BSTC.

	All	Uniform BSTC			Gaussian BSTC	
$\epsilon\mu$	$C_{L,2}$	C_U	ΔC_2		C_U	ΔC_2
0.1	1.9109	2.0314	0.1198		2.3927	0.4812
0.01	4.1240	4.1582	0.0342		4.5833	0.4593
0.001	6.7384	6.7469	0.0086		7.2127	0.4743

PURDUE UNIVERSITY

Summary

- Obtained one upper bound (C_U) and two error-free lower bounds ($C_{L,1}$ and $C_{L,2}$) on the capacity of BSTC.
- These bounds are asymptotically tight for the uniform BSTC:
  - C_U (U.BSTC) = $C_{L,1}$ + O(1) $\Rightarrow$ $C_{U.BSTC} = C_{L,1} + O(1)$
  - C_U (U.BSTC) = $C_{L,2}$ + o(1) $\Rightarrow$ $C_{U.BSTC} = C_{L,2} + o(1)$
  - For any distribution-independent scheme, you cannot do better than Scheme 2.
- When ϵ is small,

$$C_{BSTC}(\epsilon) \geq C_{U.BSTC}(\epsilon)$$

Implementation

- S. Sellke, C-C. Wang, N.B. Shroff, and S. Bagchi, *Covert Timing Channels over TCP/IP networks: from Theory to Practice*, 2007

  - Practical Design and Implementation of a covert timing channel over TCP/IP networks.
  - Experiments on computers at Purdue and Princeton
    - Network Delay Characteristics: Small Jitter (3-5%)
  - Rate of the TCP/IP Timing Channel:
    - Up to 80 bit/sec, 5 times improvement over the on-off channels.
  - What's more?
    - For BSTC, a non-detectable scheme mimicking the normal traffic pattern.
    - Error-control coding for timing channel.