Capacity Bounds on Timing Channels with Bounded Service Times

Sarah H. Sellke, Chih-Chun Wang, Ness Shroff, and Saurabh Bagchi
Center for Wireless Systems and Applications
School of Electrical and Computer Engineering
Purdue University, West Lafayette, IN 47907
{ssellke, chihw, shroff, sbagchi}@purdue.edu

***Abstract*— It is well known that queues with exponentially distributed service times have the smallest Shannon capacity among all single-server queues with the same service rate. In this paper, we study the capacity of timing channels in which the service time distributions have bounded support, i.e., Bounded Service Timing Channels (BSTC). We derive an upper bound and two lower bounds on the capacity of such timing channels. The tightness of these bounds is investigated analytically as well as via simulations. We find that the uniform BSTC serves a role for BSTCs that is similar to what the exponential service timing channel does for the case of timing channels with unbounded service time distributions. That is, when the length of the support interval is small, the uniform BSTC has the smallest capacity among all BSTCs.**

I. Introduction

A timing channel is a non-conventional communication channel, in which a message is encoded in terms of the arrival times of bits. The receiver observes the time of the departing bits and decodes the message. It has been shown in [1] that when the service time of the queue is exponentially distributed, the channel capacity, $e^{-1}\mu$ nats/sec, is the lowest among all the servers with the same service rate μ. Most of the existing work such as in [1], [2], [3], [4], [5], [6], [7], [8] has been focused on Exponential Service Timing Channels (ESTC). The discrete-time counterpart has been studied in [9], [10].

While ESTC has the lowest capacity among all servers with the same service rate, deterministic service timing channels have infinite capacity. In [11], we estimated the lower bounds on the capacities of single-server timing channels in which the service time distributions are uniform (uniform BSTC), Gaussian (GSTC), and truncated Gaussian (Gaussian BSTC). The capacities of these channels are on the order of $\mu \log_2(\mu\sigma)^{-1}$ bits/sec as $\sigma \to 0$, where μ is the service rate and σ is the standard deviation of the service time.

In many real world applications, the service time distributions have *bounded support*. By bounded support, we mean that there exist some constants $a, \Delta > 0$, such that the *i.i.d.* service times $S_1, S_2, \cdots$ satisfy $P(a < S_k < a + \Delta) = 1$. Such timing channels are called Bounded Service Timing Channels (BSTC), and $(a, a+\Delta)$ is called a support interval of the BSTC. We are especially interested in BSTC with small relative fluctuation of the service time, i.e. $\Delta/a \ll 1$.

In this paper, we focus on the capacity of BSTCs with support intervals symmetric about the mean service time $\frac{1}{\mu}$, i.e. support intervals of the form $(\frac{1}{\mu} - \epsilon, \frac{1}{\mu} + \epsilon)$. The service time distribution does not need to be symmetric about $1/\mu$. We derive an upper bound $C_U(\epsilon)$ on the capacity of BSTC using a feedback argument, and two *zero-error* capacity lower bounds, $C_{L,1}(\epsilon)$ and $C_{L,2}(\epsilon)$, using geometrically distributed inter-arrival times. While $C_U(\epsilon)$ is dependent on the service time distribution, both $C_{L,1}(\epsilon)$ and $C_{L,2}(\epsilon)$ are independent of the distribution of the service time, given the support interval. All these results can easily be extended to BSTCs that have support intervals asymmetric about $\frac{1}{\mu}$, i.e. of the form $(\frac{1}{\mu} - \epsilon_L, \frac{1}{\mu} + \epsilon_R)$.

We further show that these bounds are asymptotically tight for the uniform BSTC. By the tightness, we mean, when ϵ is small, the *capacity* of the uniform BSTC is $C_{L,2}(\epsilon) + o(1)$ (or $C_{L,1}(\epsilon) + O(1)$). Since our lower bound $C_{L,2}(\epsilon)$ is universal for all BSTC, the uniform BSTC serves a role similar to that of the ESTC in the paper by Anantharam and Verdu [1]. Namely, when ϵ is small, the uniform BSTC has the smallest capacity among all BSTCs, just as the exponential service time has the smallest capacity when considering unbounded service time distributions.

The rest of the paper is organized as follows: In Section II we provide an upper bound $C_U(\epsilon)$ on the capacity of BSTC using a feedback argument. In Section III, we provide two lower bounds $C_{L,1}(\epsilon)$ and $C_{L,2}(\epsilon)$, both of which are asymptotically tight but in different senses. Furthermore, we show that the second lower bound, exploiting the absolute timing information, is extremely close to the capacity of the uniform BSTC when small ϵ is considered and is hence asymptotically optimal. We conclude our paper in Section IV.

II. An Upper Bound on the Capacity of BSTCs

Bounded Service Timing Channels (BSTC) are single-server queue based timing channels in which the service times $S_1, S_2, \cdots$ are *i.i.d.* with bounded support. In this paper, we consider servers with support intervals symmetric about the mean service time $E[S_k] = \frac{1}{\mu}$, i.e. $\exists \epsilon, 0 < \epsilon < \frac{1}{\mu}$ such that $P(\frac{1}{\mu} - \epsilon < S_k < \frac{1}{\mu} + \epsilon) = 1$. The service times $S_1, S_2, \cdots$ of the uniform BSTC are *i.i.d.* $U(\frac{1}{\mu} - \epsilon, \frac{1}{\mu} + \epsilon)$ uniform random variables. The service times $S_1, S_2, \cdots$ of the Gaussian BSTC are *i.i.d.* truncated Gaussian random variables with density function:

$$f(x) = \frac{1}{K\sqrt{2\pi}\sigma}\exp(-\frac{(x-1/\mu)^2}{2\sigma^2})\ I(\frac{1}{\mu}-3\sigma, \frac{1}{\mu}+3\sigma)$$

where $\epsilon = 3\sigma < \frac{1}{\mu}$, and $K = \int_{-\infty}^{\infty} f(x)dx = 0.997$.

We will first provide an upper bound on the capacity of the BSTC by using a feedback argument of these channels.

Proposition 1: Consider a BSTC with service rate μ and support interval $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$.
(a) An upper bound $C_U(\epsilon)$ on the capacity of the BSTC is $C_U(\epsilon) = \mu \sup_{0<\gamma<1} G(\epsilon, \gamma)$ bits/sec, where
$G(\epsilon,\gamma) = \gamma[\log_2(\epsilon\mu + \frac{1}{\gamma} - 1) + \log_2(e) - \log_2(\mu) - h(S_i)]$
(b) $C_U(\epsilon)$ for the uniform BSTC with service rate μ and support interval $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$ is the smallest among all BSTC with the same service rate and support interval.

[Proof] (a) Let S_i be the service time of the i^{th} bit, and let a_i and d_i be the arrival and the departure time of the i^{th} bit, respectively. Further, let A_i and D_i be the inter-arrival time and the inter-departure time between the $(i-1)^{st}$ bit and the i^{th} bit, respectively, and let W_i be the queue's idle time before the arrival of the i^{th} bit.

An upper bound C_U is the capacity C_{FB} of the timing channel in which there is an additional feedback channel providing the queue size information on the server back to the transmitter, so that the sender has the knowledge of d_{i-1} before deciding a_i. With the feedback information, the sender has full control over W_i and can completely avoid any queueing. Thus, the timing channel is reduced to a sequentially juxtaposed *i.i.d.* channel: $W_i \to W_i + S_i$. The capacity of this new channel with feedback information is simply

$$C_{FB} = \sup_{\lambda<\mu} \lambda I(W_i; W_i + S_i),$$

where λ is the inter-departure rate ($\lambda = 1/E[D_i]$) and $I(W_i, W_i + S_i) = h(W_i + S_i) - h(S_i)$.

Since $W_i + S_i - (\frac{1}{\mu}-\epsilon) > 0$ and $E[W_i + S_i - (\frac{1}{\mu}-\epsilon)] = \frac{1}{\lambda} - \frac{1}{\mu} + \epsilon$, We have

$$\sup_{W_i>0}[h(W_i+S_i)] \le 1 + \ln(\frac{1}{\lambda} - \frac{1}{\mu} + \epsilon) \text{ nats.} \quad \text{Thus,}$$

$$\begin{aligned} C_{FB} &= \sup_{\lambda<\mu}\{\lambda[1+\ln(\frac{1}{\lambda}-\frac{1}{\mu}+\epsilon) - h(S_i)]\} \\ &= \mu \sup_{\lambda<\mu}\{\frac{\lambda}{\mu}[\ln(\frac{\mu}{\lambda} - 1 + \epsilon\mu) + 1 - \ln(\mu) - h(S_i)] \end{aligned}$$

Let $\gamma = \lambda/\mu$. Define

$$G(\epsilon,\gamma) = \gamma[\log_2(\epsilon\mu + \frac{1}{\gamma} - 1) + \log_2(e) - \log_2(\mu) - h(S_i)]$$

We have an upper bound on the capacity of BSTCs:

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

(b) Since the uniform $U(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$ random variable has the maximum entropy among all random variables with the support interval $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$, $G(\epsilon,\gamma)$ in part (a) for the uniform BSTC is the smallest among all BSTC for each γ. Therefore, $C_U(\epsilon)$ for the uniform BSTC is the smallest among all BSTCs with the same service rate and support interval. ■

It is apparent that the value of $C_U(\epsilon)$ is dependent on the service time distribution. Next, we will provide two zero-error lower bounds $C_{L,1}(\epsilon)$ and $C_{L,2}(\epsilon)$ on the capacity for BSTCs. Both lower bounds are *independent* of the service time distributions given the support interval.

III. Two Lower Bounds on the Capacity of BSTCs

A. The First Lower Bound

In this section, we will provide a sub-optimal lower bound $C_{L,1}$ on the capacity of BSTC. This lower bound is obtained by using a coding scheme in which the inter-arrival times $A_1, A_2, \cdots$ are *i.i.d.* geometric random variables. We require $A_i \ge \frac{1}{\mu} + \epsilon$ to avoid queuing. Further, the possible values of A_i are spaced 4ϵ apart to allow error-free decoding. More precisely, $A_1, A_2, \cdots$ are *i.i.d.* random variables with the following probability mass function:

$$P\{A_i = (\frac{1}{\mu}+\epsilon) + k(4\epsilon)\} = p_1(1-p_1)^k, \quad k = 0, 1, \cdots$$

Since this encoding scheme does not require prior knowledge of the service time distribution, given the support interval $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$, it yields a *universal* lower bound $C_{L,1}(\epsilon)$ on the capacity of BSTC.

We now state our first lower bound Lemma without proof. The proof is provided in our online technical report [12].

Lemma 1: Consider a BSTC where the service times $S_1, S_2, \cdots$, are *i.i.d.* random variables with service rate μ and $P[S_i \in (\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)] = 1$. A zero-error lower bound $C_{L,1}(\epsilon)$ on the capacity of the timing channel is:

$$C_{L,1}(\epsilon) = \mu \sup_{0<\gamma<(1+\epsilon\mu)^{-1}} \gamma[H(p_1)/p_1] \text{ bits/sec}$$

where $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ and

$$p_1 = \frac{4\epsilon\mu}{1/\gamma - 1 + 3\epsilon\mu}.$$

Figure 1 shows $C_{L,1}(\epsilon)$ as a function of the load factor $\gamma = \lambda/\mu$ when $\epsilon\mu = 0.01$, along with the upper bounds $C_U(\epsilon)$ for *uniform BSTC* and *Gaussian BSTC*. As shown in this figure, $C_{L,1} = 3.4\mu$ bits/sec, and C_U for the uniform BSTC (4.16μ bits/sec) is smaller than that of the Gaussian BSTC (4.58μ bits/sec). This is expected by Proposition 1(b).

Now, we compare the performance of $C_{L,1}(\epsilon)$ with our upper bound $C_U(\epsilon)$. Denote $\Delta C_1(\epsilon) = C_U(\epsilon) - C_{L,1}(\epsilon)$. We will show that $\Delta C_1(\epsilon)$ for the uniform BSTC is the smallest among all BSTC and $\Delta C_1(\epsilon) = O(1)$ for the uniform and Gaussian BSTC.

Proposition 2: For BSTC with service rate μ and support interval, $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$, $\Delta C_1(\epsilon)$ satisfies:
(a) $\Delta C_1(\epsilon) < \mu(\log_2(e) + D(S_n||U_{\mu,\epsilon}))$ bits/sec, where $D(\cdot||\cdot)$ is the Kullback-Leibler distance and $U_{\mu,\epsilon}$ is the uniform distribution on $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$.
(b) $\Delta C_1(\epsilon)$ for the uniform BSTC is the smallest such

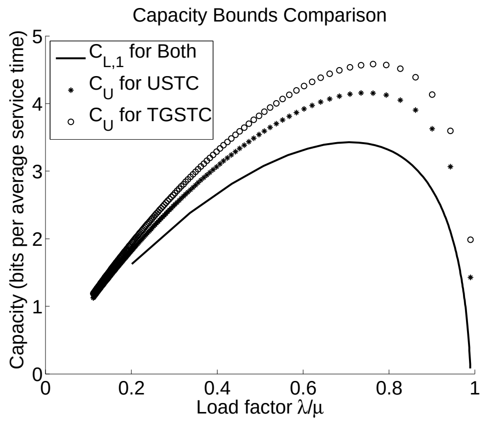

Fig. 1. Capacity Lower Bound $C_{L,1}$ compared with C_U for the uniform and Gaussian BSTC when $\epsilon\mu = 0.01$ (in bits per average service time).

difference between our $C_U(\epsilon)$ and $C_{L,2}(\epsilon)$ among all BSTCs with the same service rate μ and support interval $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$. **[Proof]** See Appendix.

TABLE I

THE UPPER AND LOWER BOUNDS ON THE CAPACITY OF UNIFORM BSTC AND GAUSSIAN BSTC (IN BITS PER AVERAGE SERVICE TIME).

	ALL	Uniform	Uniform	Gaussian	Gaussian
$\epsilon\mu$	$C_{L,1}$	C_U	ΔC_1	C_U	ΔC_1
10^{-1}	1.4500	2.0314	0.5814	2.3927	0.9428
10^{-2}	3.4287	4.1582	0.7295	4.5833	1.1547
10^{-3}	5.9081	6.7469	0.8388	7.2127	1.3045

We obtain $\Delta C_1(\epsilon) < \log_2(e)\mu$ bits/sec $\approx 1.447\mu$ bits/sec for uniform BSTCs, and $\Delta C_1(\epsilon) < 2.004\mu$ bits/sec for Gaussian BSTCs by Proposition 2(a).

In Table I, we show the values of $C_{L,1}(\epsilon)$ for BSTCs, and the values of $C_U(\epsilon)$ and $\Delta C_1(\epsilon)$ for the uniform BSTC and the Gaussian BSTC when $\epsilon\mu = 10^{-1}, 10^{-2},$ and 10^{-3}. We can see that $\Delta C_1 < 2\mu$ bits/sec for all ϵ in this Table.

Our first lower bound $C_{L,1}(\epsilon)$ is sub-optimal by using a naive coding scheme with a large (4ϵ) spacing. Nevertheless, it is a good lower bound because it is tight in the sense that for the uniform BSTC, $\Delta C_1(\epsilon) < 1.447$ bits/sec for all ϵ. That is, the *capacity* of the uniform BSTC is $C_{L,1}(\epsilon) + O(1)$. Moreover, it is universal for all BSTC in a given support interval.

We now present our optimal lower bound $C_{L,2}(\epsilon)$ for BSTCs, which is also independent of the service time distribution given the support interval. However, it requires knowledge of absolute timing information at both sender and receiver.

B. The Second Lower Bound

To derive our second zero-error lower bound $C_{L,2}$, the receiver is required to use more computational power to recover the absolute time. When the absolute time is available to the receiver, we use a *slotted-arrival-time* coding scheme to obtain our lower bound $C_{L,2}(\epsilon)$.

Lemma 2: Assuming that absolute time information is available to both the sender and the receiver, a zero-error lower bound $C_{L,2}(\epsilon)$ on the capacity of BSTCsde with service rate μ and support interval $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$ is:

$$C_{L,2}(\epsilon) = \mu \sup_{0<\gamma<(1+(1+2\alpha)\epsilon\mu)^{-1}} \gamma[H(p_2)/p_2] \text{ bits/sec}$$

where $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$,

$$p_2 = \frac{2\epsilon\mu}{\frac{1}{\gamma} - 1 + (1-2\alpha)\epsilon\mu}, \quad \text{and } \alpha = \lceil \frac{1+\epsilon\mu}{2\epsilon\mu} \rceil - \frac{1+\epsilon\mu}{2\epsilon\mu}.$$

Proof. When the absolute time information is available, we use *slotted* arrival times with slot size 2ϵ. That is, the arrival time of the i^{th} bit, a_i, is restricted to be on the grid $t = (2\epsilon)k_i, k_i = 0, 1, 2\cdots$.

To see why our scheme works, we start with a simple example of encoding messages by sending only one bit at time a_1. Let d_1 be the departure time of that bit. Assuming the queue is initially empty, we have $d_1 = a_1 + S_1$. In our scheme, the only possible values of a_1 are $(2k)\epsilon, k = 0, 1, 2, \cdots$. Since $S_1 \in (\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$, we have $a_1 = (2k)\epsilon$ if and only if $d_1 \in I_k = (\mu + (2k-1)\epsilon, \mu + (2k+1)\epsilon)$. Moreover, I_k and $I_{k'}$ do not overlap if $k \neq k'$.

To decode a message, the receiver uses slotted departure times with slot size 2ϵ, and the k^{th} slot corresponds to the time interval $I_k = (\frac{1}{\mu} + (2k-1)\epsilon, \frac{1}{\mu} + (2k+1)\epsilon)$. Upon observing a bit departing at time d_1^* in slot k^*, i.e. $d_1^* \in I_{k^*}$, the receiver can recover the arrival time correctly as $a_1^* = (2k^*)\epsilon$.

When we encode messages by transmitting more than one bit, the receiver can decode the message error-free in exactly the same way as transmitting only one bit, as long as there is no queueing at the server. To avoid queueing, simply choose k_i so that $k_i \geq k_{i-1} + \frac{1+\epsilon\mu}{2\epsilon\mu}$ for $i \geq 2$. This condition is equivalent to $a_i - a_{i-1} \geq \frac{1}{\mu} + \epsilon$.

Thus, in our coding scheme, the inter-arrival times $A_1, A_2, \cdots$ must satisfy (1) $A_i = 2k'\epsilon$ and (2) $A_i \geq \frac{1}{\mu} + \epsilon$.

$$\text{Let } K_0 = \lceil \frac{1+\epsilon\mu}{2\epsilon\mu} \rceil, \text{ and } \alpha = K_0 - \frac{1+\epsilon\mu}{2\epsilon\mu}, \quad 0 \leq \alpha < 1.$$

Choose $A_1, A_2, \cdots$ to be *i.i.d.* geometric random variables that satisfy (1) and (2), with probability mass function:

$$P[A_i = K_0(2\epsilon) + k(2\epsilon)] = p_2(1-p_2)^k, \quad k = 0, 1, \cdots$$

Let λ be the departure rate and $\gamma = \lambda/\mu$. We have $1/\lambda = E[D_i] = E[A_i] = K_0(2\epsilon) + 2\epsilon(\frac{1}{p_2} - 1)$. Thus,

$$p_2 = \frac{2\epsilon\mu}{\frac{1}{\gamma} - 1 + \epsilon\mu - 2\alpha(\epsilon\mu)}$$

Since $I(A_i; D_i) = h(A_i) = H(p_2)/p_2$, we have

$$C \geq \frac{I(A_i; D_i)}{E[D_i]} = \mu[\gamma H(p_2)/p_2]$$

$$\text{for all } \gamma, \text{ such that } 0 < \gamma < (1 + (1+2\alpha)(\epsilon\mu))^{-1}.$$

Therefore,

$$C_{L,2}(\epsilon) = \mu \sup_{0<\gamma<(1+(1+2\alpha)\epsilon\mu)^{-1}} \gamma[H(p_2)/p_2] \text{ bits/sec}$$

■

The major difference between the first scheme in Section III-A and the second scheme is that the timing information is now embedded in the *absolute* timing of each arrival rather than the traditional inter-arrival time. Or equivalently, the timing information is in the inter-arrival time between the i-th bit and the timing origin, rather than in the lapse between the i-th and the $(i-1)$-th bits, so that the noisy component of the service time is kept at 2ϵ rather than 4ϵ, the superposition of the noises from both the i-th and the $(i-1)$-th bits.

The absolute timing (or the timing origin), on the other hand, is generally not available at the receiver end. Nonetheless, by slightly increasing the size of the slots, from 2ϵ to $2\epsilon+\delta$, where δ serves as a guard band, the absolute timing information recovery problem is reduced to a grid realigning problem. The goal of this problem is to find a realignment such that no departure time falls into the guard band δ. With a sufficiently long observation period, the recovery is always possible in probability. By further reducing the size of the guard band δ, we obtain the same lower bound in Lemma 2 as if we have the absolute timing information.

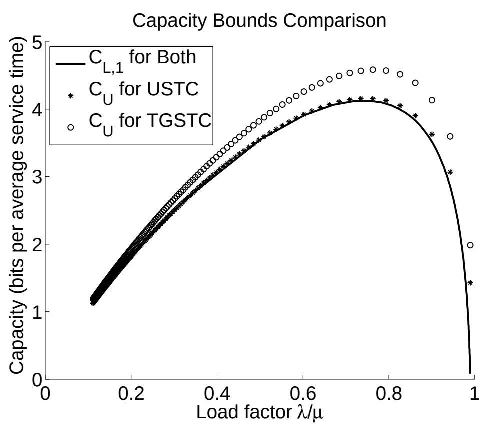

Fig. 2. Capacity Lower Bound $C_{L,2}$ compared with C_U for the uniform and Gaussian BSTC when $\epsilon\mu = 0.01$ (in bits per average service time).

Figure 2 shows the universal lower bound $C_{L,2}(\epsilon)$ for BSTCs as a function of the load factor $\gamma = \lambda/\mu$ for $\mu\epsilon = 0.01$, along with upper bounds $C_U(\epsilon)$ for *uniform* BSTCs and *Gaussian* BSTCs. As shown in Figure 2, $C_U(\epsilon)$ for uniform BSTCs is extremely close to $C_{L,2}(\epsilon)$.

In the next Proposition, we will show that $C_{L,2}(\epsilon)$ is asymptotically optimal in the sense that, $C_U(\epsilon)-C_{L,2}(\epsilon) \to 0$ as $\epsilon \to 0$ for uniform BSTCs.

Proposition 3: Denote $\Delta C_2(\epsilon) = C_U(\epsilon) - C_{L,2}(\epsilon)$.
(a) ΔC_2 for a uniform BSTC is the smallest such difference between our $C_U(\epsilon)$ and $C_{L,2}(\epsilon)$ among all BSTCs with same service rate μ and support interval $(\frac{1}{\mu}-\epsilon, \frac{1}{\mu}+\epsilon)$.
(b)$\Delta C_2(\epsilon) \to 0$ as $\epsilon \to 0$ for uniform BSTC.

Proof See Appendix.

Proposition 3 shows that $C_{L,2}(\epsilon)$ is asymptotically tight for the uniform BSTC. By tightness, we mean that when ϵ is small, the *capacity* of the uniform BSTC is $C_{L,2} + o(1)$. Since our lower bound $C_{L,2}(\epsilon)$ is universal for all BSTCs, the uniform BSTC serves a role similar to that of the ESTC in [1]. Namely, when ϵ is small, the uniform BSTC has the smallest capacity among all BSTCs, while the exponential service time has the smallest capacity when considering unbounded service time distribution. Further, Proposition 3(b) does not hold for Gaussian BSTC. We can show that $\Delta C_2(\epsilon) > 0$ as $\epsilon \to 0$ for Gaussian BSTC.

Table II shows the values of the universal lower bound $C_{L,2}(\epsilon)$ of BSTCs, C_U and ΔC_2 for uniform BSTCs and Gaussian BSTCs, for various values of $\epsilon\mu$. When $\epsilon\mu = 10^{-3}$, $C_{L,2} = 6.7384\mu$; and for the uniform BSTC, $C_U = 6.7469\mu$ and $\Delta C_2 = 0.0086\mu$. Using the two tight bounds, we can infer that the *capacity* of this uniform BSTC is 6.7μ bits/sec.

TABLE II
THE UPPER AND LOWER BOUNDS ON THE CAPACITY OF UNIFORM BSTC AND GAUSSIAN BSTC (IN BITS PER AVERAGE SERVICE TIME).

$\epsilon\mu$	ALL $C_{L,2}$	Uniform C_U	Uniform ΔC_2	Gaussian C_U	Gaussian ΔC_2
10^{-1}	1.9106	2.0314	0.1198	2.3927	0.4812
10^{-2}	4.1240	4.1582	0.0342	4.5833	0.4593
10^{-3}	6.7384	6.7469	0.0086	7.2127	0.4743

IV. Conclusion

We have studied the capacity of timing channels with bounded service times. We have obtained an upper bound, and two universal lower bounds on the capacity of BSTCs. These bounds are shown to be asymptotically tight for uniform BSTCs. An interesting observation that comes about as a by-product of this work is that the uniform BSTC serves a role similar to that of the ESTC in [1], i.e., when ϵ is small, the uniform BSTC has the smallest capacity among all BSTCs.

References

[1] N. Anantharam and S. Verdu, "Bits through queues," *IEEE Trans. Inform. Theory,* vol. 42, pp. 4 – 18, Jan. 1996
[2] R. Sundaresan and S. Verdu "Robust decoding for timing channels," *IEEE Trans. Inform. Theory,* vol. 46, pp. 405 – 419, Mar. 2000
[3] R. Sundaresan and S. Verdu "Sequential decoding for the exponential server timing channel," *IEEE Trans. Inform. Theory,* vol. 46, pp. 405 – 419, Mar. 2000
[4] R. Sundaresan and S. Verdu "Capacity of Queues Via Point-Process Channels," *IEEE Trans. Inform. Theory,* vol. 52, pp. 2697 – 2709, June 2006
[5] J. Giles and B. Hajek "An Information-theoretic and game-theoretic study of timing channels," *IEEE Trans. on Inform. Theory,* VOL. 48, pp. 2455 – 2477, Mar. 2002
[6] X. Liu and R. Srikant "The timing capacity of single-server queues with multiple flows," *DIMACS Series in Discrete Mathematics and Theoretical Computer Science,* 2004
[7] A. B. Wagner and V. Anantharam "Zero-reate reliability of the exponetial-server timing channel," *IEEE Trans. on Inform. Theory,* VOL 52, No 2, pp. 447 – 465, Feb. 2005
[8] P. Mimčilović "Mismatch Decoding of a Compound Timing Channel," *Forty-Fourth Annual Allerton Conference on Communication, Control, and Computing,* Sep. 2006
[9] A. Bedekar and M. Azizoglu "The information-theoretic capacity of discrete-time queues," *IEEE Trans. Inform. Theory,* vol. 44, pp. 446 – 461, Mar. 1998

[10] J. A. Thomas “On the Shannon capacity of discrete time queues,” *IEEE Int. Symp. Inform. Theory*, pp. 333, July 1997
[11] S. H. Sellke, N. B. Shroff, S. Bagchi, and C. C. Wang “Timing Channel Capacity for Uniform and Gaussian Servers,” *Forty-Fourth Annual Allerton Conference on Communication, Control, and Computing*, 2006
[12] S. H. Sellke, C. C. Wang, N. B. Shroff, and S. Bagchi “Capacity Bounds on Timing Channels with Bounded Service Times,” http://www.stat.purdue.edu/∼ssellke/TimingChannels.pdf
[13] T. Cover and J. Thomas *Elements of Information Theory, New York: Wiley*, 1991

APPENDIX

[Proof of Proposition 2]

(1) We wish to show $\Delta C_1(\epsilon) \le \mu[\log_2(e) - h(S_n) + \log_2(2\epsilon)]$ bit/sec. By *Proposition 1*,
$C_U(\epsilon) = \mu \sup_{0<\gamma<1} G(\epsilon,\gamma)$ bits/sec, where
$G(\epsilon,\gamma) = \gamma[\log_2(\epsilon\mu + \frac{1}{\gamma} - 1) + \log_2(e) - \log_2(\mu) - h(S_i)]$.

By *Lemma 1*,

$$C_{L,1}(\epsilon) = \mu \sup_{0<\gamma<(1+\epsilon\mu)^{-1}} \gamma[H(p_1)/p_1] \text{ bits/sec},$$

where $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ and $p_1 = (4\epsilon\mu)(1/\gamma - 1 + 3\epsilon\mu)^{-1}$. Thus,

$$\begin{aligned} \Delta C_1 &= C_U(\epsilon) - C_{L,1}(\epsilon) \\ &< \mu \sup_{0<\gamma<(1+\epsilon\mu)^{-1}} [G(\epsilon,\gamma) - \gamma H(p_1)/p_1] \end{aligned} \quad (1)$$

First, express the first term of $G(\epsilon,\gamma)$, $\log_2(\epsilon\mu + 1/\gamma - 1)$, in terms of p_1.

$$p_1 = \frac{4\epsilon\mu}{1/\gamma - 1 + 3\epsilon\mu} \qquad \Rightarrow \epsilon\mu = \frac{(1/\gamma - 1)p_1}{4 - 3p_1}$$

Thus, $\epsilon\mu + 1/\gamma - 1 = (\epsilon\mu)(\frac{4-2p_1}{p_1})$, so that

$$\begin{aligned} & G(\epsilon,\gamma) \\ =\ & \gamma[\log_2(\epsilon\mu + \frac{1}{\gamma} - 1) + \log_2(e) - \log_2(\mu) - h(S_i)] \\ =\ & \gamma\{\log_2[(\epsilon\mu)(\frac{4-2p_1}{p_1})] + \log_2(e) - \log_2(\mu) - h(S_i)\} \\ =\ & \gamma\{\log_2[(\epsilon)(\frac{4-2p_1}{p_1})] + \log_2(e) - h(S_i)\} \end{aligned}$$

Thus,

$$\begin{aligned} & G(\epsilon,\gamma) - \gamma H(p_1)/p_1 \\ =\ & \gamma\{\log_2[(\epsilon)(\frac{4-2p_1}{p_1})] + \log_2(e) - h(S_i)\} - \gamma H(p_1)/p_1 \\ =\ & \gamma[\log_2(2\epsilon(2-p_1)/p_1) + \log_2(e) - h(S_i) \\ & +(\log_2(p_1) + (1-p_1)/p_1 \log_2(1-p_1))] \\ =\ & \gamma[\log_2(e) - h(S_n) + \log_2(2\epsilon)] \\ & +\gamma[\log_2(2-p_1) + (\frac{1-p_1}{p_1})\log_2(1-p_1))] \\ =\ & \gamma[\log_2(e) + D(S_n||U_{\mu,\epsilon})] \\ & +\gamma[\log_2(2-p_1) + (\frac{1-p_1}{p_1})\log_2(1-p_1))] \end{aligned}$$

Since $\log_2(2-p) + \frac{1-p}{p}\log_2(1-p) < 0$ and $0 < \gamma < 1$, we have $G(\epsilon,\gamma) - \gamma H(p_1)/p_1$

$$< \gamma[\log_2(e) + D(S_n||U_{\mu,\epsilon})] \ < \log_2(e) + D(S_n||U_{\mu,\epsilon})$$

By equation (1), $\Delta C_1(\epsilon) \le \mu[\log_2(e)) + D(S_n||U_{\mu,\epsilon})]$ bits/sec.

(2) By *Proposition 1* part (b), $C_U(\epsilon)$ the uniform BSTC with service rate μ and support interval $(\frac{1}{\mu} - \epsilon, \frac{1}{\mu} + \epsilon)$ is the smallest among all BSTCs with the same service rate and support interval, and by Lemma 1, $C_{L,1}(\epsilon)$ is independent of the service distribution. Therefore, ΔC_1 for the uniform BSTC is the smallest among all BSTCs with service rate μ and support interval $(\frac{1}{\mu} - \epsilon, \frac{1}{\mu} + \epsilon)$

■

[Proof of Proposition 3]

(a) Same argument as in the proof of Proposition (2)(b).
(b)We wish to show $\Delta C_2(\epsilon) \to 0$ as $\epsilon \to 0$ for uniform BSTC.

As in the proof of Proposition 2,

$$\begin{aligned} \Delta C_2(\epsilon) &= C_U(\epsilon) - C_{L,2}(\epsilon) \\ &= \mu \sup_{0<\gamma<1} G(\epsilon,\gamma) - \sup_{0<\gamma<(1+\epsilon\mu)^{-1}} [\gamma H(p_2)/p_2] \end{aligned}$$

First, express the first term of $G(\epsilon,\gamma)$, $\log_2(\epsilon\mu + 1/\gamma - 1)$, in terms of p_2. Since

$$p_2 = \frac{2\epsilon\mu}{\frac{1}{\gamma} - 1 + (1-2\alpha)\epsilon\mu} \quad \Rightarrow \epsilon\mu = \frac{(\frac{1}{\gamma} - 1)p_2}{2 - (1-2\alpha)p_2},$$

we have $\epsilon\mu + \dfrac{1}{\gamma} - 1 = (\dfrac{1}{\gamma} - 1)(\dfrac{2 + 2\alpha p_2}{2 - (1-2\alpha)p_2}) = (\epsilon\mu)(\dfrac{2}{p_2} + 2\alpha)$.

Since $h(S_i) = \log_2(2\epsilon)$ for uniform BSTC, we have

$$\begin{aligned} & G(\epsilon,\gamma) = \gamma[\log_2(\epsilon\mu + \frac{1}{\gamma} - 1) + \log_2(e) - \log_2(\mu) - h(S_i)] \\ =\ & \gamma\{\log_2[(\epsilon\mu)(\frac{2}{p_2} + 2\alpha)] + \log_2(e) - \log_2(\mu) - \log_2(2\epsilon))\} \\ =\ & \gamma\{\log_2(\frac{1}{p_2} + \alpha) + \log_2(e)\} \end{aligned}$$

Thus,

$$\begin{aligned} & G(\epsilon,\gamma) - \gamma H(p_2)/p_2 \\ =\ & \gamma[\log_2(\frac{1}{p_2} + \alpha) + \log_2(e)] - \gamma H(p_2)/p_2 \\ =\ & \gamma[\log_2(\frac{1}{p_2} + \alpha) + \log_2(e) \\ & +(\log_2(p_2) + \frac{1-p_2}{p_2}\log_2(1-p_2)] \\ =\ & \gamma[\log_2(e) + (\frac{1-p_2}{p_2})\log_2(1-p_2))] + \gamma\log_2(1+\alpha p_2) \end{aligned}$$

Let $\gamma^* = \gamma^*(\epsilon)$ be the value where $G(\epsilon,\gamma)$ achieves its maximum, i.e. $C_U(\epsilon) = G(\epsilon,\gamma^*)$. The corresponding value of p_2^* sastifies $p_2^* \to 0$ as $\epsilon \to 0$. Thus,

$$\log_2(e) + (\frac{1-p_2^*}{p_2^*})\log_2(1-p_2^*) \to 0 \quad \text{as} \quad \epsilon \to 0,$$

and $\log_2(1+\alpha p_2^*) \to 0$ as $\epsilon \to 0$.

Thus for uniform BSTCs,

$$(G(\epsilon,\gamma^*) - \gamma^* H(p_2^*)/p_2^*) \longrightarrow 0 \quad \text{as} \quad \epsilon \to 0.$$

Therefore, $\Delta C_2(\epsilon) \to 0$ as $\epsilon \to 0$ for uniform BSTCs.

■