Timing Channel Capacity for Uniform and Gaussian Servers

Sarah Sellke, Ness B. Shroff, Saurabh Bagchi, and Chih-Chun Wang
School of Electrical and Computer Engineering, Purdue University
email: {ssellke, shroff, sbagchi, chihw}@ecn.purdue.edu

***Abstract*— It is well known that queues with exponentially distributed service time have the smallest Shannon capacity among all single-server queues with the same service rate. However, the capacity of other service disiplines such as Gaussian service timing channels (GSTC) remains unknown. In this paper, we outline a preliminary investigation into timing channel capacity, when the service distributions are uniform, Gaussian, and truncated Gaussian. Our study indicates that the capacity per service time increases as the ratio of the standard deviation to the mean service time of the server decreases.**

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 intervals between the departing bits and decodes the message. It has been shown in [1] that the Exponential Service Timing Channel (ESTC) has a capacity of $e^{-1}\mu$ nats/sec, where μ is the service rate. Its capacity is the lowest among all the servers with the same service rate. Most of the existing work such as [1], [2], [3], [4], [5], [6] has focused on ESTC. The discrete-time counterpart has been studied in [7], [8].

We also know that the Deterministic Service Timing Channel (DSTC) has infinite capacity. A question arises naturally from the above two extremes: if the service time distribution is just a little ”short” of being deterministic, how large is the timing capacity? We attempt to answer this question by investigating the capacities of three timing channels, in which the service time distributions are uniform (USTC), Gaussian (GSTC), and truncated Gaussian (TGSTC). In particular, we are interested in characterizing the capacities of these channels when σ/T is small, where σ is the standard deviation of the service time, and T is the mean service time. We show the capacity of these timing channels increases when σ/T decreases. The lower bound in each case tends to ∞ as $\sigma/T \to 0$, which agrees with the fact that the DSTC has infinite capacity.

This work is partially supported by the National Science Foundation grant 0335247-ANI, 0523249-CNS and an NSF Graduate Research Fellowship.

II. Bounds on Timing Channel Capacities

We will present our results for the lower bounds (denoted as C_L) and upper bounds (denoted as C_U) on the timing channel capacities for the USTC, GSTC, and TGSTC in this section. The upper bounds C_U in all cases are obtained by using Thereom 5 in [1].

We first consider the USTC in which the service times $S_1, S_2, \cdots, S_n$ are *i.i.d.* uniform random variables $U(T-\epsilon, T+\epsilon)$. The bounds are provided below:

$$C_L = \mu \max_{0<p<1} [\frac{H(p)}{p+(\epsilon/T)(4-3p)}] \quad \text{nats/sec} \quad (1)$$

$$C_U = \mu(\ln(\frac{T}{2\epsilon})+1) \quad \text{nats/sec} \quad (2)$$

where $H(p) = -p\ln(p) - (1-p)\ln(1-p)$.

We obtain C_L by choosing the inter-arrival times $A_1, A_2, \cdots$ to be *i.i.d.* geometric random variables, having discrete density function

$$P[A_i = T+\epsilon+4k\epsilon] = p(1-p)^k, \quad k = 0, 1, \cdots$$

This encoding scheme ensures no queueing and also allows the receiver to decode a message error-free.

Next, we consider the GSTC in which the service times $S_1, \cdots, S_n$ are *i.i.d.* Gaussian random variables $N(T, \sigma^2)$ and $\sigma/T \leq 1/\sqrt{2\pi e} \approx 0.24$. The bounds are estimated to be:

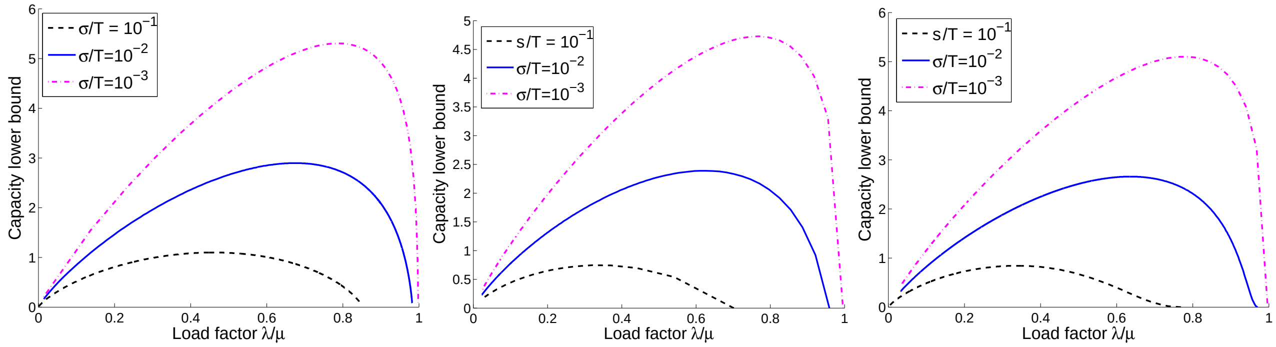
$$C_L \approx \mu \max_{Y\geq 0} [\frac{\ln\frac{T}{\sigma} + \ln Y}{1+3\sqrt{2}Y}] \quad \text{nats/sec} \quad (3)$$

$$C_U \approx \mu \ln(\sqrt{\frac{e}{2\pi}}\frac{T}{\sigma}) \quad \text{nats/sec,} \quad (4)$$

We obtain C_L for the GSTC by choosing the inter-arrival times $A_1, A_2, \cdots$ to be *i.i.d.* Gaussian $N(T_a, \sigma_a^2)$, and independent of the service times. We require

$$T_a = T + 3\sqrt{\sigma_a^2 + \sigma^2} \quad (5)$$

Condition (5) minimizes queueing effect. This is because $A_i - S_j$ is Gaussian $N(T_a - T, \sigma^2 + \sigma_a^2)$ and



(a) USTC (b) GSTC (c) TGSTC

Fig. 1. The Capacity Lower Bounds (in bits per average service time) vs the Load Factor λ/μ

$$P(\text{No Queueing}) = P(A_{k+1} - S_k \geq 0) = 0.997$$

Finally, we consider TGSTC in which the service times $S_1, S_2, \cdots$ are *i.i.d.* with density function:

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

where $T > 3\sigma$ and $K = \int_{-\infty}^{\infty} f(x)dx = 0.997$

Its upper bound C_U is estimated to be the same as that of GSTC given by (4). Its lower bound C_L is estimated to be:

$$C_L \approx \mu \max_Y [\frac{0.5\ln(1+0.5Y^2)}{1+3\frac{\sigma}{T}(Y+1)}] \quad \text{nats/sec} \qquad (6)$$

Similar to GSTC, we obtain C_L by choosing the inter-arrival times $A_1, A_2, \cdots$ to be *i.i.d.* truncated Gaussian with density function:

$$f_a(x) = \frac{1}{K\sqrt{2\pi}\sigma_a}\exp(-\frac{(x-T_a)^2}{2\sigma_a^2})\ I(T_a-3\sigma_a, T_a+3\sigma_a)$$

where $T_a > 3\sigma_a$ and $K = \int_{-\infty}^{\infty} f_a(x)dx = 0.997$
To ensures $P(\text{no queueing}) = 1$, we require

$$T_a = T + 3(\sigma_a + \sigma)$$

Figure 1 illustrates the capacity lower bounds as functions of the load factor λ/μ for the USTC, GSTC, and TGSTC; Table 1 shows the numerical values of C_L for these timing channels. When $\sigma/T = 10^{-2}$, C_L is more than twice the service rate.

We observe that in all three types of timing channels, both C_L and C_U increase when $\frac{\sigma}{T}$ decreases, and $C_L \to \infty$ as $\frac{\sigma}{T} \to 0$. Moreover, the capacity C of the channels satisfies $C \sim \Theta(\ln(\frac{T}{\sigma}))$.

TABLE I

THE LOWER BOUNDS (IN BITS PER SERVICE TIME)

$\frac{\sigma}{T}$	GSTC	TGSTC	USTC
10^{-1}	0.7439	0.8417	1.0977
10^{-2}	2.3886	2.6574	2.8960
10^{-3}	4.7261	5.0997	5.3052

III. ONGOING RESEARCH

We are finding tighter bounds for GSTC and TGSTC. We are studying the capacities of covert network timing channels and implementing efficient and good coding schemes.

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] 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

[5] 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

[6] 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

[7] A. Bedekar and M. Azizoglu "The information-theoretic capacity of discrete-time queues," *IEEE Trans. Inform. Theory,* vol. 44, pp. 446 – 461, Mar. 1998

[8] J. A. Thomas "On the Shannon capacity of discrete time queues," *IEEE Int. Symp. Inform. Theory,* pp. 333, July 1997

[9] T. Cover and J. Thomas *Elements of Information Theory, New York: Wiley,* 1991