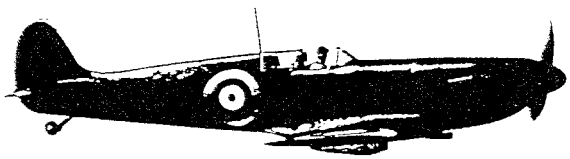

Fig. 13. A British WWII Supermarine Spitfire fighter plane featuring a dangerous fiducial.

A set of C concentric circles with $r_1 = \frac{1+1/2C}{2}$ and $\Delta r = 1+1/2C$ is expected to be a very good (although suboptimal) location shape. Experimental tests in [13] and further theoretical developments recently published in [14], led to the conclusion that the "bull's-eye" fiducial is indeed a very good, robust and practical location mark.

Hence the Royal Air Force chose, rather poorly, a deadly targeting shape to be painted on its planes during World War II (see Fig. 13).

REFERENCES

[1] C. A. Berenstein, L. N. Kanal, D. Lavine, and E. C. Olson, "A geometric approach to subpixel accuracy," *CVGIP*, vol. 40, no. 3, pp. 334–360, 1987.

[2] J. Hill, "Dimensional measurements from quantized images," in D. Nitzan, S. Bavnard, R. Bolles, R. Cain, J. Hill, W. Park, and R. Smith, Eds., *Machine Intelligence Research Applied to Industrial Automation*, SRI Report prepared for the NSF, Nov. 1980.

[3] I. Amir, "An algorithm for finding the center of circular fiducials," *CVGIP*, vol. 49, pp. 398–406, 1990.

[4] C. Bose and I. Amir, "Design of fiducials for accurate registration using machine vision," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 12, pp. 1196–1200, Dec. 1990.

[5] H. K. Nishihara and P. A. Crossley, "Measuring photolithographic overlay accuracy and critical dimensions by correlating binarized Laplacian of Gaussian convolutions," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 10, pp. 17–30, Jan. 1988.

[6] J. Sanz, Special Issue of PAMI I/II on Machine Vision. vol. 10, 1988.

[7] R. T. Chin, "Automated visual inspection 1981–1987," *CVGIP*, vol. 41, pp. 346–381, 1988.

[8] Gi Tian and M. N. Huhns, "Algorithms for subpixel registration," *CVGIP*, vol. 35, no. 2, pp. 220–233, 1986.

[9] V. N. Dvornichenko, "Bounds on the deterministic correlation functions with application to registration," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. PAMI-5, pp. 206–213, Mar. 1983.

[10] A. M. Bruckstein, L. O'Gorman, and A. Orlitsky, "Design of shapes for precise image registration," AT&T Bell Lab. Tech. Memo, Murray Hill, NJ, Oct. 1989.

[11] D. I. Havelock, "Geometric precision in noise-free digital images," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 11, pp. 1065–1075, Oct. 1989.

[12] ——, "The topology of locales and its effects on position uncertainty," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 13, pp. 380–386, Apr. 1991.

[13] L. O'Gorman, A. M. Bruckstein, C. B. Bose, and I. Amir, "Subpixel registration using a concentric ring fiducial," in *Proc. 10th ICPR Conf.* (Atlantic City, NJ, June 1990).

[14] A. Efrat and C. Gotsman, "Subpixel image registration using circular fiducials," *Int. J. Comp. Geom. and Appl.*, vol. 4, no. 4, pp. 403–422, 1994.

[15] M. Tichem and M. S. Cohen, "Sub-μm registration of fiducial marks using machine vision," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 16, pp. 791–794, Aug. 1994.

[16] G. Chiorboli and G. P. Vecchi, "Comments on 'Design of fiducials for accurate registration using machine vision'," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 15, pp. 1330–1332, Dec. 1993.

[17] N. Kiryati and A. M. Bruckstein, "Gray levels can improve the performance of binary image digitizers," *CVGIP*, vol. 53, no. 1, pp. 31–39, 1991.

[18] S. Karlin and H. Taylor, *A First Course in Stochastic Processes.* New York: Academic, 1975.

An Analysis of the Timed Z-Channel

Ira S. Moskowitz, *Member, IEEE*, Steven J. Greenwald, and Myong H. Kang

***Abstract*—Golomb analyzed the Z-channel, a memoryless channel with two input symbols and two output symbols, where one of the input symbols is transmitted with noise while the other is transmitted without noise, and the output symbol transmission times are equal. We generalize to the *timed Z-channel*, where the output symbol transmission times are not equal. The timed Z-channel appears as the basis for a large class of covert (communication) channels appearing in multilevel secure computer systems. We give a detailed mathematical analysis of the timed Z-channel and report a result expressing the capacity of the timed Z-channel as the log of the root of a characteristic equation. This generalizes Shannon's work on noiseless channels for this special case. We also report a new result bounding the timed Z-channel's capacity from below. We show how an interesting observation that Golomb reported for the Z-channel also holds for the timed Z-channel.**

***Index Terms*—Channel capacity, computer network, computer security, covert channel, CPU scheduling, timing channel, Z-channel.**

I. INTRODUCTION

In Shannon's seminal paper, he expressed the capacity of a discrete noiseless channel with variable symbol time durations as the logarithm of the zero of an associated "polynomial," see [26], [6] (in this correspondence we abuse the term polynomial since technically they are polynomials in the inverse of the variable). The nontrivial exponents of this polynomial are the negatives of the symbol time durations. Our main theoretical result is to extend this algebraic solution to a particular type of noisy binary input channel which has two output times.

Discrete noiseless channel with variable symbol time durations and their "noisy" generalizations are of great interest to designers of multilevel secure (MLS) computer systems [22]. We discuss an application of our analysis to such a system. In this correspondence we will restrict ourselves to a two-level system, consisting of the (security/sensitivity) levels Low and High. The Bell–LaPadula (BLP) [2] requirements are that a lower level user/process (Low) may not read from a higher user/process (High) and that High may not write to Low. However, due to the exigencies of realistic system design, it may be possible for High to *covertly* pass information to Low in violation of the BLP requirements. Such a violation is called a *covert channel* [14]. Mathematically, a covert channel is simply a communication channel with High acting as the transmitter and Low being the receiver. In this correspondence, as in [22], we are interested in covert channels where time values comprise the output alphabet. Such a covert channel is called a covert timing channel, or more simply, a *timing channel*. In the literature, timing channels often include the class of channels that use the notion of a "clock" to count the number of symbols sent in a certain time period [29].

Manuscript received November 10, 1996; revised February 27, 1998. The work of I. S. Moskowitz and S. J. Greenwald was supported by the Office of Naval Research. The material in this correspondence appeared in part, under the same title, in *Proc. IEEE Symp. Security and Privacy* (Oakland, CA, May 1996), pp. 2–11.

The authors are with the Center for High Assurance Computer Systems, Information Technology Division, Mail Code 5540, Naval Research Laboratory, Washington, DC 20375 USA.

Publisher Item Identifier S 0018-9448(98)07364-7.

U.S. Government work not protected by U.S. copyright

In general, timing channels arise from resource sharing in MLS systems. High can pass information to Low, by either interfering with, or refraining from interfering with, the timing of Low's activities. In most of these systems this activity is noisy. The simplest model for such interference (where the output alphabet consists of time values) is what we call the *timed Z-channel*. The timed Z-channel is a discrete memoryless communication channel with two inputs, and the output set consists of two time values. The first input can result in either output time, whereas the second input is always output as the greater time value.

Note that in [22, Strategy 2] we studied a two-input, two-output channel where the arrival times of the output values span a continuous range, not as in this correspondence, a two-input, two-ouput channel with two arrival times. Thus that channel [22] is not a generalization of the Z-channel. Furthermore, the results from our present work are not a special case of [22] due to the very different behavior of the arrival times.

We show how the well-known CPU scheduling covert channel [15], [25], as discussed in a mathematical sense by Huskamp [9, Sec. IV], is a timed Z-channel. Many researchers are currently investigating countermeasures to this scenario and its variants (e.g., [8], [7], [27], [10]). Note that McCullough's [18] "half-bit [sic] channels" are, in fact, timed Z-channels.

Theorem 1 and Corollary 1 (the main results of this correspondence) show how channel capacity can be easily expressed[1] as the log of a zero of a trinomial (recall we are using the terms polynomial/trinomial loosely). Thus we have extended Shannon's earlier algebraic approach. This lets us transform a complicated optimization problem into an algebraic problem. This, in turn, gives us a simple method for calculating capacity and seeing the interplay between the noise and timing factors. The best defense to covert channel threats is a thorough understanding and analysis of covert channel behavior. Knowledge of the interplay between these various terms leads us to a better understanding of how to lessen capacity without degrading performance. This has been seen in papers such as [3] and [4], where noise is introduced in the system to lessen capacity. Knowledge of similar system behavior was of great significance during the design and implementation of the NRL Pump [11]–[13], [21].

II. Example—The CPU Scheduler Type Channel

Most modern computers are based on an operating system that performs multiprogramming. In multiprogramming, a number of jobs (programs) are located in memory (job queue) at the same time and share one or more CPU's among them. The idea is that sharing can increase CPU utilization and total job throughput [1].

MLS computers have separate memory spaces for jobs at different security levels. However, many MLS computers are also based on a multilevel operating system that performs multiprogramming with only one CPU. Thus the CPU is shared not only among jobs within the same security level but also among jobs from different security levels.

The above is what our scenario is based upon—the multilevel CPU scheduling of jobs in a multilevel operating system. This CPU scheduling causes contention which leads to a covert channel. This effect has been well-noted in the literature [15], [25], [9].

Note that we can observe the same situation on a multilevel message server system where a High server receives messages from Low and Medium (or High) levels in a round-robin fashion. We also note that studies of this type of covert channel have been useful in other areas, such as the planned extension of the NRL network Pump

[1] All logarithms are base 2.

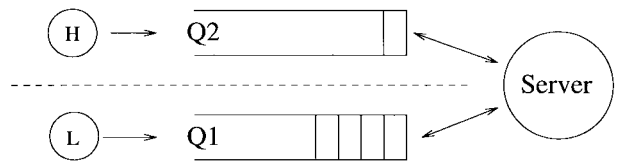

Fig. 1. A queuing diagram.

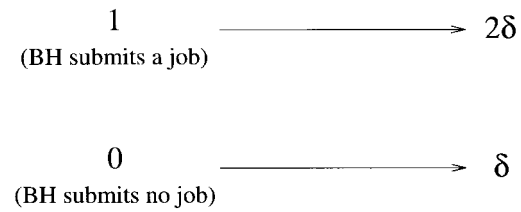

Fig. 2. A noiseless timing channel.

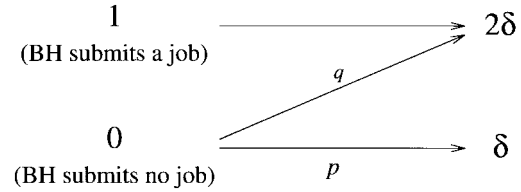

Fig. 3. A timed Z-channel.

(a secure message passer from Low to High) to a more generalized scenario. We will refer to the class of such covert channels as CPU scheduling channels. The detailed model is as follows:

There are two queues (i.e., Q2 and Q1), such that High processes put their jobs/messages into Q2 and Low processes put their jobs/messages into Q1. A server, which is a shared resource, provides service in a round-robin fashion. A server may be a CPU which processes jobs from two different levels. This is illustrated in Fig. 1.

This scenario results in the well-known covert timing channel from High to Low, which we have called the CPU scheduling channel [15], [25], [9]. For simplicity, let us assume that each job takes time δ. Assume that a Low process (e.g., BL—Bad Low) submits jobs and observes the time between job completions. If a High process (e.g., BH) does not submit any job, each job in Q1 takes time δ to complete. If BH submits a job, BL observes time 2δ between job completions (i.e., time δ for the BH job and an additional time δ for the BL job). Therefore, we have the noiseless timing channel illustrated in Fig. 2. The capacity of this noiseless timing channel is known to be $\delta^{-1}\log\frac{1+\sqrt{5}}{2}$ bits per time unit [26], [19] because $\frac{1+\sqrt{5}}{2}$ is the positive zero of $1-(x^{-1}+x^{-2})$. BH may decide to communicate with BL even in the presence of noise. The noise can be introduced by another High process (e.g., GH—Good High) that does not have any intention of communicating with BL. If GH submits a job and BH does not submit a job (i.e., BH attempts to send a binary 0), BL still observes time 2δ which will be interpreted as a binary 1 from BH. Therefore, we have a covert *timed Z*-channel (see Section IV for a formal definition) where $p+q=1$ as illustrated in Fig. 3. This type of channel, where capacity (bits per time unit) is not known, is the focus of this correspondence.

In the preliminary conference [24] version of this correspondence we examined a situation where a timed Z-channel could arise in a token ring network. This scenario is interesting because it has *three* levels, is in a network environment, and is previously unknown. We will not discuss this scenario further.

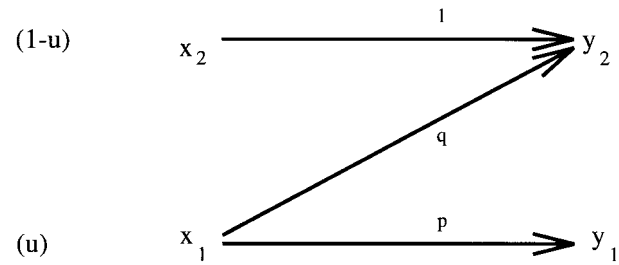

Fig. 4. The Z-channel.

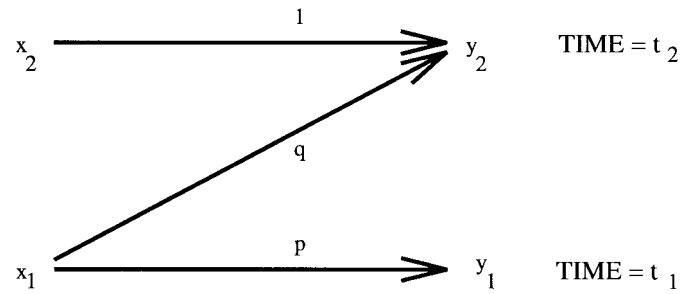

Fig. 5. The $Z(\epsilon)$-channel, $\epsilon = t_2 - t_1$.

III. Mathematical Background: Golomb's Z-Channel

In [5] Golomb succinctly analyzed the mutual information and channel capacity of the Z-channel (see Fig. 4). The Z-channel is a discrete memoryless channel with two input symbols. One symbol, x_2, is transmitted without noise and received as y_2, while the other input symbol x_1 is transmitted with noise and received as either y_1 or y_2. We denote the probability that x_i (y_j) is the input (output) by $P(x_i)$ $(P(y_j))$. Letting u represent the probability $P(x_1)$ that x_1 is the input we have $P(x_2) = 1 - u$. The amount of noise (constant with each transmission) is given by the following channel matrix $(q = 1 - p)$ which describes the conditional probabilities:

$$\begin{pmatrix} P(y_1|x_1) & P(y_2|x_1) \\ P(y_1|x_2) & P(y_2|x_2) \end{pmatrix} = \begin{pmatrix} p & q \\ 0 & 1 \end{pmatrix}.$$

Let us now calculate the mutual information I (in units of bits per symbol). I is the difference in entropies $H(Y) - H(Y|X)$. The output entropy $H(Y) = H(y_1, y_2)$, where we are using the shorthand notation of $H(a, b) = -\{a \log a + b \log b\}$. By conditioning we see that $P(y_1) = up$ and $P(y_2) = 1 - up$. So $H(Y) = H(up, 1 - up)$. The conditional entropy is

$$\begin{aligned} H(Y|X) &= P(x_1)H(Y|x_1) + P(x_2)H(Y|x_2) \\ &= P(x_1)H(p, q) + P(x_2)H(0, 1) \\ &= uH(p, q). \end{aligned}$$

Thus we see that [5, eq. (1)]

$$I = H(up, 1 - up) - uH(p, q).$$

In brief, a timed Z-channel is identical to Golomb's Z-channel except that the output symbol y_2 has a greater transmission time than y_1. Implicit in discussion of Golomb's Z-channel is that the symbols take the same amount of time to be transmitted. Therefore, units are in bits per symbol when we are dealing with the Z-channel. To avoid confusion, I (I_t) will be mutual information in bits per symbol (tick, the time unit), and C (C_t) will be capacity in bits per symbol (tick). In general, for discrete memoryless channels, if all symbols take the same time τ to be transmitted, we have $I_t = \tau^{-1} I$ and $C_t = \tau^{-1} C$. However, for the timed Z-channel, transmission times of the two symbols are different, so C_t is not a multiple of C. In the next section we analyze the timed Z-channel. Note that in [22] we get the same result for I. However, I_t and thus C_t are quite different.

IV. The Timed Z-Channel

We see from our above discussions that we may abstract our covert timing channel scenario to a memoryless channel with two input symbols, x_1 and x_2, u as before. Input symbol x_2 is transmitted without noise and is interpreted as the output symbol y_2, taking time t_2. Input symbol x_1 either arrives with probability p taking time t_1 and is interpreted as the output symbol y_1, or it arrives with probability $q = 1 - p$ taking time t_2 and is interpreted as the output symbol y_2 (the t_i are integers since by definition they are multiples of a tick). Note that the output symbols are distinguished by the differing time values in the timed Z-channel, whereas in the Z-channel it is not the time that distinguishes them, but the fact that $y_1 \neq y_2$. We will use the notation "$Z(\epsilon)$-channel," where ϵ is the difference in time $t_2 - t_1 \geq 0$, for the timed Z-channel (see Fig. 5). Of course, the channel matrix of the $Z(\epsilon)$-channel is identical to that of the Z-channel. Therefore, I for the $Z(\epsilon)$-channel is the same as I for the Z-channel. Note that the Z-channel is just a $Z(0)$-channel.

Let T represent the Bernoulli random variable that describes the time at which an output symbol arrives. The probability $P(T = t_j)$, or written more simply as $P(t_j)$, is the probability $P(y_j)$. Hence, the expected value of T is

$$E(T) = t_1(up) + t_2(1 - up).$$

Since $\epsilon = t_2 - t_1$ we have

$$E(T) = t_1 + \epsilon(1 - up).$$

We see that if the channel is noiseless $E(T)|_{q=0} = t_1 + \epsilon(1 - u)$. If the channel is totally noisy (useless) then $E(T)|_{q=1} = t_1 + \epsilon$.

We now wish to analyze the mutual information, in bits per tick, $I_t = (I/E(T))$. From our above equations we see that

$$I_t = \frac{H(up, 1 - up) - uH(p, q)}{t_1 + \epsilon(1 - up)}.$$

We wish to calculate the capacity, in units of bits per tick, C_t for the $Z(\epsilon)$-channel. Verdú [28] has rigorously shown that $C_t = \max_u I_t$, and that this is the proper measure of maximal asymptotically error-free information flow. We can find C_t by setting $(dI_t/du) = 0$ and solving for u. We denote the value of u that solves $(dI_t/du) = 0$, and therefore maximizes I_t, by u_c (see the expression on the bottom of this page). Setting the derivative to zero gives us

$$\begin{aligned} 0 = {} & t_1 p \log\left(\frac{1 - up}{up}\right) - t_1 H(p, q) + \epsilon p \log\left(\frac{1 - up}{up}\right) \\ & - \epsilon H(p, q) - \epsilon up^2 \log\left(\frac{1 - up}{up}\right) + \epsilon up H(p, q) \\ & - \epsilon up^2 \log(up) - \epsilon p(1 - up)\log(1 - up) - \epsilon up H(p, q) \end{aligned}$$

$$\frac{dI_t}{du} = \frac{[t_1 + \epsilon(1 - up)]\left[p \log\left(\frac{1-up}{up}\right) - H(p, q)\right] + \epsilon p[H(up, 1 - up) - uH(p, q)]}{[t_1 + \epsilon(1 - up)]^2}.$$

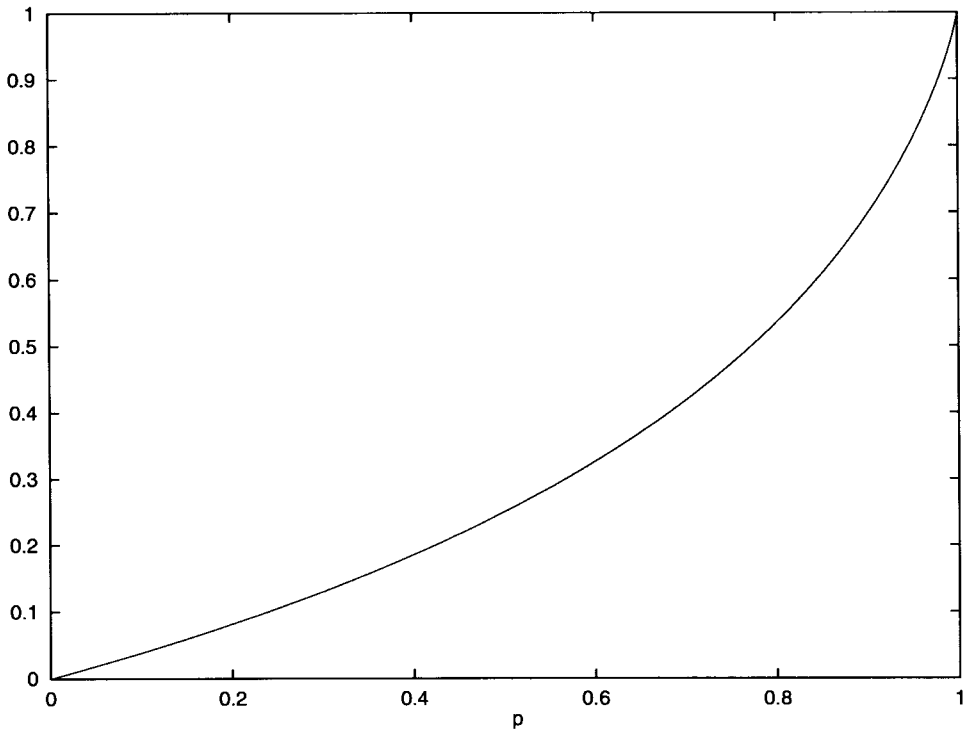

Fig. 6. $pq^{q/p}$.

which simplifies to

$$\left(\frac{t_1+\epsilon}{p}\right)H(p,q) = t_1 \log\left(\frac{1-up}{up}\right) + \epsilon \log\left(\frac{1-up}{up}\right) - \epsilon up \log\left(\frac{1-up}{up}\right) - \epsilon up \log(up) - \epsilon \log(1-up) + \epsilon up \log(1-up)$$

which further reduces to

$$\left(\frac{t_1+\epsilon}{p}\right)H(p,q) = t_1 \log\left(\frac{1-up}{up}\right) - \epsilon \log(up).$$

This simplifies to

$$\log(1-up)^{t_1}(up)^{-(t_1+\epsilon)} = \log(p^p q^q)^{-\left(\frac{t_1+\epsilon}{p}\right)}$$
$$(1-up)^{t_1} = (p^p q^q)^{-\left(\frac{t_1+\epsilon}{p}\right)}(up)^{(t_1+\epsilon)}$$
$$1-up = (p^p q^q)^{-\left(\frac{t_1+\epsilon}{t_1 p}\right)}(up)^{\frac{t_1+\epsilon}{t_1}}.$$

Letting $\kappa = (pq^{q/p})^{1/t_1}$ and $\gamma^{-t_1} = up$ we have the trinomial equation

$$1 - [(\kappa\gamma)^{-(t_1+\epsilon)} + \gamma^{-t_1}] = 0 \tag{1}$$

which we refer to as the characteristic equation of the $Z(\epsilon)$-channel. Equation (1) gives us the following useful identities:

$$(\kappa\gamma)^{-(t_1+\epsilon)} + \gamma^{-t_1} = 1$$
$$1 - \gamma^{-t_1} = (\kappa\gamma)^{-(t_1+\epsilon)}.$$

We obtained a similar expression for the channel in [22]. However, in [22] the nontrivial exponents of the equation are not, up to sign, the output time values. This contrasts with the results in this correspondence where the nontrivial exponents are the negatives of the output time values. Thus our current results generalize Shannon's polynomial representation for the simple scenario we have put forth.

Since the term $pq^{q/p}$ is so important we will include a plot of it (see Fig. 6). Keep in mind that $pq^{q/p}$ is defined by its limiting values of 0 and 1 at $p = 0$ and $p = 1$, respectively.

Of course, the variable γ in (1) is functionally dependent upon p, but (1) is very appealing because if $p = 1$, (1) reduces to

$$1 - [\gamma^{-(t_1+\epsilon)} + \gamma^{-t_1}] = 0 \tag{2}$$

and $u_c = r_1^{-t_1}$, where r_1 is the unique positive root of (2). This is of interest because Shannon has shown that $C_t = \log r_1$ [26], [23], [20] (for this noiseless channel).

Now let us attempt to find a general closed form for the capacity of the $Z(\epsilon)$-channel. Using the identity $u_c p = r_p^{-t_1}$, where r_p, for fixed p, is the positive γ value that solves (1), we see that

$$H(u_c p, 1-u_c p) = H(r_p^{-t}, (\kappa r_p)^{-(t_1+\epsilon)}) = [t_1 + \epsilon(\kappa r_p)^{-(t_1+\epsilon)}]\log r_p + (t_1+\epsilon) \cdot (\kappa r_p)^{-(t_1+\epsilon)} \log\kappa.$$

Since $H(p,q) = -\log(p^p q^q)$ we see that

$$u_c H(p,q) = -t_1 r_p^{-t_1} \log\kappa.$$

This gives us

$$\begin{aligned} H(u_c p, 1-u_c p) &- u_c H(p,q) \\ &= [t_1 + \epsilon(\kappa r_p)^{-(t_1+\epsilon)}]\log r_p + (t_1+\epsilon)(\kappa r_p)^{-(t_1+\epsilon)} \\ &\quad \cdot \log\kappa + t_1 r_p^{-t_1}\log\kappa \\ &= [t_1 + \epsilon(\kappa r_p)^{-(t_1+\epsilon)}]\log r_p \\ &\quad + [t_1(r_p^{-t_1} + (\kappa r_p)^{-(t_1+\epsilon)}) + \epsilon(\kappa r_p)^{-(t_1+\epsilon)}]\log\kappa \\ &= [t_1 + \epsilon(\kappa r_p)^{-(t_1+\epsilon)}](\log r_p + \log\kappa) \\ &= [t_1 + \epsilon(\kappa r_p)^{-(t_1+\epsilon)}]\log\kappa r_p. \end{aligned}$$

The mean time to receive a symbol, with respect to the maximizing value of u, is

$$E(T)|_{u=u_c} = t_1 + \epsilon(1-u_c p) = t_1 + \epsilon(\kappa r_p)^{-(t_1+\epsilon)}.$$

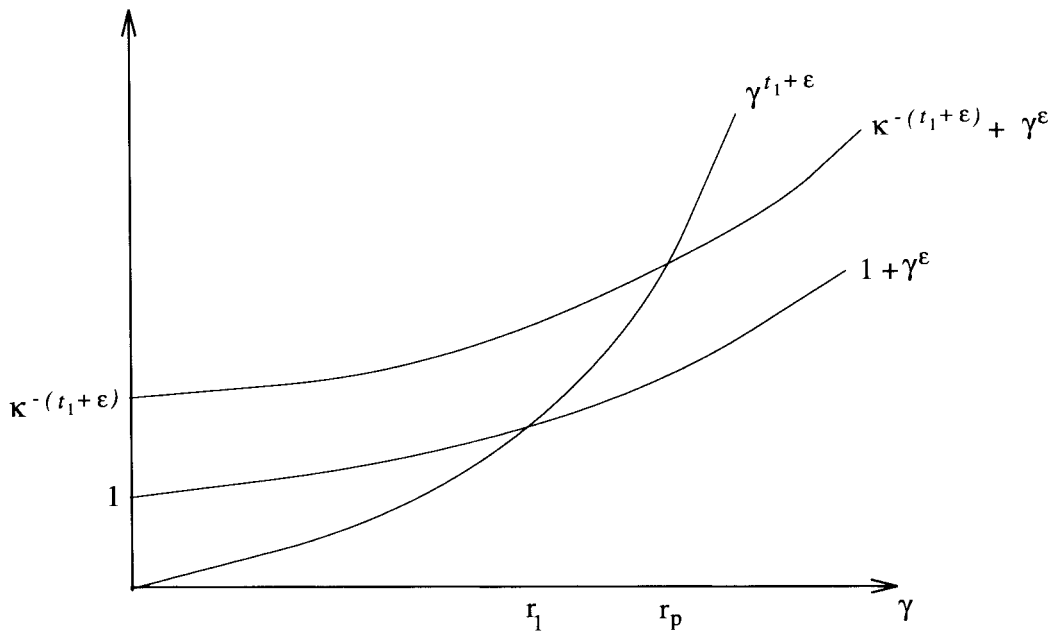

Fig. 7. Comparison of the roots.

Since

$$C_t = I_t(u_c) = \frac{H(u_c p, 1-u_c p) - u_c H(p,q)}{E(T)|_{u=u_c}}$$

we see that

Theorem 1: $C_t = \log \kappa r_p$, where r_p, for fixed p, is the positive γ value that solves

$$1 - [(\kappa\gamma)^{-(t_1+\epsilon)} + \gamma^{-t_1}] = 0.$$

Changing variables in (1) by letting $w = \kappa\gamma$, we see that κr_p, for fixed p, is the positive value of w that solves

$$1 - [w^{-(t_1+\epsilon)} + (pq^{q/p})w^{-t_1}] = 0.$$

Therefore, we have the following corollary to Theorem 1.

Corollary 1: $C_t = \log x_p$, where x_p, for fixed p, is the positive w value that solves

$$1 - [w^{-(t_1+\epsilon)} + (pq^{q/p})w^{-t_1}] = 0.$$

Theorem 1 and Corollary 1 collapse to Shannon's result [26] for $p = 1$. (We will study the case of $p \to 0^+$ in Section V.) Corollary 1 mimics the form of Shannon's result by expressing C_t as the logarithm of a zero of a polynomial. However, our polynomial has nontrivial coefficients. Note that for the $Z(0)$-channel, our result gives us $C_t|_{\epsilon=0} = (1/t_1)\log(1 + pq^{q/p})$, which can be easily obtained from Golomb's paper. This is an intriguing generalization of Shannon's result on capacity. Our results are part of a greater research plan to understand how to generalize Shannon's original definition of capacity as an asymptotic limit [26], [6, p. 106] when noise is present.

We also note that our results turn the capacity calculation from an optimization problem into a much simpler algebraic problem. The algorithm necessary to calculate the capacity is nothing more than a simple root finder.

Let us see what else we can glean from the above results. We will use the notation $C_t(p)$ for the capacity of the $Z(\epsilon)$-channel with noise $q = 1 - p$. We are interested in the behavior of $C_t(p)$ as p varies from 1 to 0 (i.e., from noiseless to useless) for t_1 and ϵ fixed. By Theorem 1 we have

$$C_t(p) = \log \kappa r_p = \log r_p + \log \kappa.$$

Since $\kappa = (pq^{q/p})^{1/t_1}$ we see that we have

$$C_t(p) = \log r_p + \frac{\log(pq^{q/p})}{t_1}.$$

We are adding a negative (we are not including the trivial comparison where $p = 1$) term to $\log r_p$. We will use this expression to bound $C_t(p)$ from below. Consider the equation

$$1 - [(\kappa\gamma)^{-(t_1+\epsilon)} + \gamma^{-t_1}] = 0.$$

This is equivalent to the equation

$$\gamma^{t_1+\epsilon} = \kappa^{-(t_1+\epsilon)} + \gamma^{\epsilon}.$$

r_p is the value of γ where the plot of $\gamma^{t_1+\epsilon}$ intersects the plot of $\kappa^{-(t_1+\epsilon)} + \gamma^{\epsilon}$, and r_1 is the value of γ where the plot of $\gamma^{t_1+\epsilon}$ intersects the plot of $1 + \gamma^{\epsilon}$ (see Fig. 7). Since $\kappa^{-(t_1+\epsilon)} > 1$ we see that $r_p > r_1$. Hence

$$\log r_1 < \log r_p$$
$$\log r_1 + \log \kappa < \log r_p + \log \kappa$$
$$C_t(1) + \log \kappa < C_t(p).$$

Therefore, the capacity $C_t(p)$ is never less than $C_t(1) + \log \kappa$. Since $C_t(p) < C_t(1)$ we have

Theorem 2: For the $Z(\epsilon)$-channel the capacity $C_t(p)$ is always bounded as

$$\max(0, C_t(1) + \log \kappa) \le C_t(p) \le C_t(1).$$

We may interpret this as a feasibility region where $C_t(p)$ must lie (see Fig. 8).

Note that if we used Corollary 1 instead of Theorem 1, we would only obtain the known and obvious bound that $C_t(p) \le C_t(1)$.

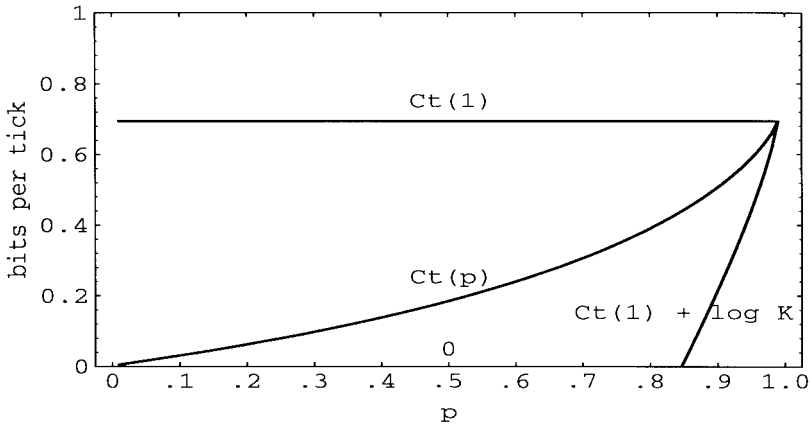

Fig. 8. Illustration of Theorem 2 for $t_1 = \epsilon = 1$.

V. Comments on the Very Noisy $Z(\epsilon)$-Channel

Majani [16] has done a systematic study of "very noisy" channels in his dissertation. We are only concerned with examining the $Z(\epsilon)$-channel as $p \to 0^+$ (which is a very noisy channel). Golomb looked at the Z-channel under the same conditions and noted some interesting behavior. We will show that the $Z(\epsilon)$-channel behaves similarly.

Golomb [5] showed that

Theorem 3 (Golomb): For the Z-channel,

$$\lim_{p \to 0^+} u_c = 1/e.$$

This result is remarkable because it implies that even though the transmission of x_1 becomes noiser and noiser, a large percentage of the inputs must still be x_1 in order for the mutual information function to approach capacity. Further, Golomb showed that u_c varies only from $1/2$ to $1/e$, as p varies from 1 to 0. This is of interest in light of the following result of Majani and Rumsey (they are concerned with units of bits per symbol, not time) [16], [17].

Theorem 4 (Majani and Rumsey): For a binary-input discrete memoryless channel with $C > 0$, I achieves C when the the probability of the first symbol being input is in the interval $(1/e, 1 - 1/e)$.

Of course, the probability for the second symbol is then also in the same interval. Therefore, Golomb's example when $p \to 0^+$ represents the limiting case of Majani and Rumsey's result, and shows that the bounds in Theorem 4 are tight. Majani and Rumsey have noted that this does not hold, in general, for more than two input symbols. Note, as the following counterexample shows, that Majani and Rumsey's result does not hold for timing channels, and in particular the $Z(\epsilon)$-channel.

Counterexample: Take the noiseless $(q = 0)$ $Z(\epsilon)$-channel with $t_1 = 1$ and $\epsilon = 29$, then $u_c \approx 0.919 > 1 - 1/e$.

However, let us see if Golomb's result generalizes to the timed Z-channel by studying it when it is very noisy, i.e., $p \to 0^+$. As we remarked above, Golomb showed for the Z-channel that $u_c \to 1/e$. Therefore, we must study the root of (1) when $p \to 0^+$. This is a little tricky because both κ and γ are functions of p. Recalling that $\gamma^{-t_1} = up$, so $\gamma^{-\epsilon} = (up)^{\epsilon/t_1}$, we may express (1) as

$$up[(pq^{q/p})^{-1} q^{-(\epsilon q)/(t_1 p)} p^{-\epsilon/t_1} u^{\epsilon/t_1} p^{\epsilon/t_1} + 1] = 1$$

which, by letting $\delta = q^{q/p}$, simplifies to

$$p\delta u + (1/\delta)^{\epsilon/t_1} u^{1+\epsilon/t_1} = \delta. \tag{3}$$

By using L'Hôpital's rule we see that $\lim_{p \to 0^+} \ln \delta = -1$, hence $\delta \to e^{-1}$. Hence as $p \to 0^+$, (3) collapses to $e^{\epsilon/t_1} u^{1+\epsilon/t_1} = e^{-1}$, so we have

Theorem 5: For the $Z(\epsilon)$-channel,

$$\lim_{p \to 0^+} u_c = 1/e.$$

Of course the rate of approach is dependent upon ϵ. We find this result to be of interest. It is worth noting that even though Majani and Rumsey's result on u_c values does not generalize to the timed Z-channel, Golomb's result on the boundary behavior of u_c does. Theorem 5 might be of use in the design of a code to exploit a very noisy timed Z-channel.

VI. Conclusion

We examined in detail a scenario where the timed Z-channel appears. This scenario is of importance to secure system designers because it models a well-known family of covert channels dating back to work on the CPU scheduling channel.

In addition to the fact that the timed Z-channel is present in real situations, it is also, in general, a good basis for an analytical study of noisy timing channels. We gave background on Golomb's classic work on the Z-channel. We then defined the timed Z-channel formally, and presented results on its capacity. These results showed the relationship between the noise and timing factors. The results also gave a theorem bounding the capacity in terms of other well-known results. In particular, we showed how to generalize Shannon's algebraic result when a simple discrete channel with variable-time outputs is noisy. We also noted that an interesting mathematical artifact, the limiting behavior of the critical probability for the Z-channel, generalizes to the timed Z-channel.

We believe that our results will be of use to the designers of MLS systems. We feel that describing and thoroughly analyzing this threat is the first step in managing it. We also feel that the serious threat of our timed Z-channel may not be restricted to just our example scenarios. We plan on investigating other scenarios, as well as systems having output alphabets with more than two timed symbols.

Acknowledgment

The authors appreciate discussion and correspondence with Solomon Golomb, Jason Martin, John McLean, Bruce Montrose, and Richard E. "Nemo" Newman. We also thank the anonymous referees and the associate editor for their useful comments.

REFERENCES

[1] M. J. Bach, *The Design of the Unix Operating System*. Englewood Cliffs, NJ: Prentice-Hall, 1986.

[2] D. E. Bell and L. J. LaPadula, "Secure computer system: Unified exposition and multics interpretation," Tech. Rep. MTR-2997, MITRE Corp., Bedford, MA, Mar. 1976. Available from the National Technical Information Service as report AD A023 588.

[3] O. L. Costich and I. S. Moskowitz, "Analysis of a storage channel in the two phase commit protocol," in *Proc. Computer Security Foundations Workshop IV* (Franconia, NH, June 1991), pp. 201–208.

[4] R. David, S. Song, and R. Mukkamala, "Supporting security requirements in multilevel real-time databases," in *Proc. IEEE Symp. Security and Privacy* (Oakland, CA, May 1995), pp. 199–210.

[5] S. W. Golomb, "The limiting behavior of the Z-Channel," in *IEEE Trans. Inform. Theory*, vol. IT-26, p. 372, May 1980.

[6] S. W. Golomb, R. E. Peile, and R. A. Scholtz, *Basic Concepts in Information Theory and Coding*. New York: Plenum, 1994.

[7] J. W. Gray, III, "On introducing noise into the bus-contention channel," in *Proc. IEEE Symp. Research in Security and Privacy* (Oakland, CA, May 1993), pp. 90–98.

[8] W. Hu, "Reducing timing channels with fuzzy time," in *Proc. IEEE Symp. Research in Security and Privacy* (Oakland, CA, May 1991), pp. 8–20.

[9] J. C. Huskamp, "Covert communication channels in timesharing systems," Ph.D. dissertation, Univ. Calif. Berkeley, May 1978. Available as UCB-CS-78-02 and also as Electronics Research Lab. Memo ERL-M78/37, Univ. Calif. Berkeley.

[10] J. V. Janeri, D. B. Darby, and D. D. Schnackenberg, "Building higher resolution clocks in covert timing channels," in *Proc. Computer Security Foundations Workshop VIII* (Kenmare, County Kerry, Ireland, June 1995), pp. 85–95.

[11] M. H. Kang and I. S. Moskowitz, "A Pump for rapid, reliable, secure communication," in *Proc. ACM Conf. Computer & Communications Security '93* (Fairfax, VA, 1993), pp. 119–129.

[12] ——, *A Data Pump for Communication*, Naval Res. Lab. Memo. Rep. 5540-95-7771, 1995.

[13] M. H. Kang, I. S. Moskowitz, and D. C. Lee, "A network Pump," *IEEE Trans. Software Eng.*, vol. 22, pp. 329–338, May 1996.

[14] B. W. Lampson, "A note on the confinement problem," *Commun. Assoc. Comput. Mach.*, vol. 16, no. 10, pp. 613–615, Oct. 1973.

[15] S. B. Lipner, "A comment on the confinement problem," in *Proc. 5th Symp. Operating System Principles* (Univ. Texas, Austin, Nov. 1975), pp. 192–196.

[16] E. E. Majani, "A model for the study of very noisy channels, and applications," Ph.D. dissertation, Calif. Inst. Technol., Pasadena, CA, 1988.

[17] E. E. Majani and H. Rumsey, "Two results on binary-input discrete memoryless channels," in *Proc. IEEE Int. Symp. Information Theory* (Budapest, Hungary, June 1991), p. 104.

[18] D. McCullogh, "Covert channels and degrees of insecurity," in *Proc. Computer Security Foundations Workshop I* (Franconia, NH, June 1988), pp. 1–33.

[19] J. K. Millen, "Finite-state noiseless covert channels," in *Proc. Computer Security Foundations Workshop II* (Franconia, NH, June 1989), pp. 81–86.

[20] A. R. Miller and I. S. Moskowitz, "Reduction of a class of Fox-Wright Psi functions for certain rational parameters," *Comput. Math. with Applic.*, vol. 30, no. 11, pp. 73–82, Nov. 1995.

[21] B. E. Montrose and M. H. Kang, "An implementation of the Pump: Event driven Pump," Naval Res. Lab. Memo. Rep. 5540-95-7782, 1995.

[22] I. S. Moskowitz and A. R. Miller, "The channel capacity of a certain noisy timing channel," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1339–1344, July 1992.

[23] ——, "Simple timing channels," in *Proc. IEEE Symp. in Security and Privacy* (Oakland, CA, May 1994), pp. 56–64.

[24] I. S. Moskowitz, S. J. Greenwald, and M. H. Kang, "An analysis of the timed Z-channel," in *Proc. IEEE Symp. in Security and Privacy* (Oakland, CA, May 1996), pp. 2–11 (preliminary version of this correspondence).

[25] M. Schaefer, B. Gold, R. Linde., and J. Scheid, "Program confinement in KVM/370," in *Proc. Annu. Conf., ACM* (Seattle, WA, Oct. 1977), pp. 404–410.

[26] C. Shannon and W. Weaver, *The Mathematical Theory of Communication*. Chicago, IL: Univ. Illinois Press, 1949. Also appeared as a series of papers by C. Shannon, *Bell Syst. Tech. J.*, July 1948, Oct. 1948 ("A mathematical theory of communication"), Jan. 1949 ("Communication in the presence of noise").

[27] J. T. Trostle, "Modeling a fuzzy time system," in *Proc. IEEE Symp. Research in Security and Privacy* (Oakland, CA, May 1993), pp. 82–89.

[28] S. Verdú, "On channel capacity per unit cost," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1019–1030, Sept. 1990.

[29] J. C. Wray, "An analysis of covert timing channels," in *Proc. IEEE Symp. Research in Security and Privacy* (Oakland, CA, May 1991), pp. 2–7.

A Lower Bound on the Error Probability for Signals in White Gaussian Noise

Gérald E. Séguin

***Abstract*— In this correpondence we apply a recent inequality by de Caen to derive a lower bound on the probability of error for M-ary signals derived from a binary linear code and used on the additive white Gaussian noise channel with a maximum-likelihood decoder. This bound depends only on the weight enumerator of the code and the signal-to-noise ratio E_b/N_o. We show that this bound converges to the union upper bound as E_b/N_o goes to infinity. Finally, by means of examples, we compare our lower bound with those of Shannon and Swaszek and with Poltyrev's upper bound.**

***Index Terms*— Additive Gaussian noise, linear code, lower bound, signaling, upper bound.**

I. INTRODUCTION

In this correspondence we study the problem of communicating one of M equally likely signals $\boldsymbol{s}_0, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_{M-1}$, of dimension N, over the additive white Gaussian noise (AWGN) channel. For this situation, if $\boldsymbol{s}_u$ is transmitted, then the received vector $\boldsymbol{R}$ is

$$\boldsymbol{R} = \boldsymbol{s}_u + \boldsymbol{n} \tag{1}$$

where $\boldsymbol{n}$ is an N-dimensional vector whose coordinates are 0-mean, independent Gaussian random variables each with variance $N_0/2$. A maximum-likelihood receiver decodes $\boldsymbol{R}$ into the nearest signal in the Euclidean sense. Consequently, the probability or error, given that $\boldsymbol{s}_u$ was transmitted, is given by

$$P(\mathcal{E}|\boldsymbol{s}_u) = Pr\left[\bigcup_{i \neq u} \mathcal{E}_{ui}|\boldsymbol{s}_u\right] \tag{2}$$

where

$$\mathcal{E}_{ui} = \{\|\boldsymbol{R} - \boldsymbol{s}_i\| \leq \|\boldsymbol{R} - \boldsymbol{s}_u\|\} \tag{3}$$

and where $\| \ \|$ is the Euclidean norm.

Manuscript received December 9, 1996; revised May 8, 1998. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant OGP0006288 held by the author at L Ecole Polytechnique de Montréal. The material in this correspondence was presented in part at the International Conference on Combinatorics, Information Theory and Statistics, Portland, ME, July 18–20, 1992.

The author is with the Department of Electrical and Computer Engineering, Royal Military College of Canada, Kingston, Ont., Canada K7K 5L0.

Publisher Item Identifier S 0018-9448(98)06902-8.

0018–9448/98$10.00 © 1998 IEEE