RC24634 (W0809-038) September 10, 2008
Electrical Engineering

IBM Research Report[1]

Maximum Throughput of Clandestine Relay: Proof of Selected Theorems

Ting He
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

[1] Research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

I. INTRODUCTION

In this technical report, we provide a detailed proof for some of the theorems on the clandestine throughput in [1]. In the paper, we define the clandestine throughput as the maximum (asymptotic) fraction of matched packets in a given pair of stochastic transmission schedules. If each transmission has a fixed duration (called fixed "packet length"), then the schedules can be modeled as point processes, and i.i.d. renewal processes are considered in the analysis. Under the strict delay constraint, we have proposed an optimal flow-embedding algorithm "Strict Greedy Match" (SGM) to compute the clandestine throughput. Analysis is performed through modeling the packet delay in each iteration of SGM by a Markov process $\mathbf{Y}\stackrel{\Delta}{=}(Y_j)_{j=0}^{\infty}$ ($Y_0 \equiv 0$), where

$$Y_j = \begin{cases} Y_{j-1} + V_j & \text{if } Y_{j-1} < l \\ Y_{j-1} - U_j & \text{if } Y_{j-1} > \Delta \\ Y_{j-1} + V_j - U_j & \text{o.w.} \end{cases} \tag{1}$$

with U_j, V_j being the interarrival times in the incoming process $\mathbf{S}_1$ and the outgoing process $\mathbf{S}_2$, respectively. In the sequel, we will analyze the asymptotic properties of $\mathbf{Y}$ in detail to support the claims in the paper.

II. CLANDESTINE THROUGHPUT UNDER THE STRICT DELAY CONSTRAINT

We have the following exact expression for the clandestine throughput under the strict delay constraint (l is the packet length and Δ the maximum delay).

Theorem 2.1 ([1]): If $\mathbf{S}_1$ and $\mathbf{S}_2$ are i.i.d. renewal processes with interarrival *probability density function (pdf)* $f(x)$ ($f(x) \equiv 0$ for $x < l$), then the fraction of packets matched by SGM converges a.s., and the limit (i.e., the clandestine throughput under the strict delay constraint) is

$$C_d(\Delta)\stackrel{\Delta}{=}C(\mathbf{S}_1,\, \mathbf{S}_2;\, \Delta) = \frac{2-2q}{2-q}, \tag{2}$$

where $q\stackrel{\Delta}{=}\lim_{j\to\infty} \Pr\{Y_j \notin [l,\, \Delta]\}$ can be computed by $1 + H(l) - H(\Delta)$, where $H(x)$ ($x \in \mathbb{R}$) is the invariant *cumulative distribution function (cdf)* of $\mathbf{Y}$. Furthermore, $H(x)$ is the solution to

$$H(x) = L(x) + \int_{-\infty}^{l} H(y)f(x-y)dy + \int_{l}^{\Delta} H(y)g(x-y)dy + \int_{\Delta}^{\infty} H(y)f(y-x)dy, \tag{3}$$

where $g(x)$ is the convolution of $f(x)$ and $f(-x)$, defined as $g(x)\stackrel{\Delta}{=}\int_0^{\infty} f(y)f(y-x)dy$, and

$$L(x)\stackrel{\Delta}{=}\left[F(x-l) - G(x-l)\right] H(l) + \left[G(x-\Delta) + F(\Delta-x) - 1\right] H(\Delta) \tag{4}$$

with $F(x),\ G(x)$ being the cdf's of $f(x),\ g(x)$, respectively.

Proof: We first justify the covert capacity formula (2). Assume $\mathbf{Y}$ has the property that the frequency for Y_j to fall outside the interval $[l,\ \Delta]$ converges a.s. to a constant, defined as q. Then since each Y_j outside $[l,\ \Delta]$ represents a chaff packet whereas each Y_j inside the interval represents a pair of information packets, we see that SGM converges a.s., and the covert capacity, which is the limiting fraction of information packets, is given by $2(1-q)/(2-q)$.

Next, we show the calculation of q. If $H(x)$ is the limiting cdf of $\mathbf{Y}$, then by definition, $q = \lim_{j\to\infty}(\Pr\{Y_j < l\} + 1 - \Pr\{Y_j \leq \Delta\}) = H(l) + 1 - H(\Delta)$. Now that $H(x)$ should be invariant under the transition in (1), we have the recursion

$$H(x) = \int_{-\infty}^{l} F(x-y)dH(y) + \int_{l}^{\Delta} G(x-y)dH(y) + \int_{\Delta}^{\infty}[1-F(y-x)]dH(y), \qquad (5)$$

where $F(x)$, $G(x)$, and $1-F(-x)$ are the cdf's of the steps of $\mathbf{Y}$ when the chain starts from $(-\infty,\ l),\ [l,\ \Delta]$, and $(\Delta,\ \infty)$, respectively. Integrating (5) by parts yields (3).

The remaining proof is to show the convergence of $\mathbf{Y}$. Let a set $X \subseteq \mathbb{R}$ denote the states reachable from 0. Without loss of generality, assume that $[l,\ \Delta] \subset X$ and $[l,\ \Delta]$ is a.s. accessible from all $x \in X$ (otherwise, the clandestine throughput is trivially 1 or 0). By Theorem 17.1.7 in [2], if $\mathbf{Y}$ is positive Harris with invariant cdf $H(x)$, then for the indicator function[2] $I_{[l,\ \Delta]^c}(x)$, $\lim_{n\to\infty}\frac{1}{n}\sum_{j=0}^{n} I_{[l,\ \Delta]^c}(Y_j)$ exists a.s., i.e., the asymptotic frequency for Y_j's to fall outside $[l,\ \Delta]$ converges a.s. to a constant, which we have defined as q. It remains to prove the property of positive Harris recurrence.

First, we show that $\mathbf{Y}$ is ψ-irreducible (all the sets mentioned in the sequel are Borel). Let φ be the Lebesgue measure constrained to $[l,\ \Delta]$, i.e., $\varphi(A) = \mu(A \cap [l,\ \Delta])$, where μ is the Lebesgue measure, and U, V i.i.d. random variables with pdf $f(x)$. There must exist $\epsilon_0 > 0$ such that $f(x) > 0$ for all x within some interval $[t,\ t+\epsilon_0]$, and thus

$$\Pr\{|U-V| \in [\epsilon_1,\ \epsilon_2]\} > 0, \quad \forall 0 \leq \epsilon_1 < \epsilon_2 \leq \epsilon_0.$$

Thus, for any $A \subseteq [l,\ \Delta]$ with $\mu(A) > 0$, $\exists m \geq 1$ such that A is uniformly accessible from $[l,\ \Delta]$ using sampling distribution δ_m, i.e., $\exists \delta > 0$ such that $\inf_{x\in[l,\ \Delta]} P^m(x,\ A) > \delta$, where $P^m(x,\ A)$ is the m-step transition kernel of $\mathbf{Y}$. Since by assumption, $[l,\ \Delta]$ is accessible from all $x \in X$,

[2]An indicator function $I_A(x)$ is defined as 1 if $x \in A$ and 0 otherwise.

any nontrivial subset of $[l,\,\Delta]$ is accessible from all $x \in X$, implying that $\mathbf{Y}$ is φ-irreducible and hence ψ-irreducible for a maximal irreducibility measure ψ.

Second, we show that $\mathbf{Y}$ is Harris recurrent. Since $\mathbf{Y}$ is ψ-irreducible and $[l,\,\Delta]$ is accessible from X, by Theorem 5.2.2 in [2], there exists a nontrivial measure ν_n and a nontrivial set $C_1 \subseteq [l,\,\Delta]$ such that C_1 is ν_n-petite. Since we have shown that C_1 is uniformly accessible from $[l,\,\Delta]$, by Proposition 5.5.4 in [2], $[l,\,\Delta]$ is $\delta\nu_n$-petite for some $\delta > 0$. By Proposition 9.1.7 in [2], the fact that petite set $[l,\,\Delta]$ is a.s. accessible from X implies Harris recurrence. Note that $\mathbf{Y}$ is also aperiodic.

Finally, we show its positivity by drift analysis. Define function $V(x) \overset{\Delta}{=} 2\lambda \inf\{|x-y| : y \in [l,\,\Delta]\}$, where $1/\lambda$ is the mean interarrival time, and set $C_2 \overset{\Delta}{=} [l-x_0,\,\Delta+x_0]$ for x_0 sufficiently large such that $\int_l^{x_0} f(y)ydy - \int_{2x_0+\Delta-l}^{\infty} f(y)ydy \geq 1/(2\lambda)$. Then for any $x > \Delta + x_0$, the mean drift satisfies

$$\begin{aligned}\Delta V(x) &= -2\lambda\left[\int_l^{x-\Delta} f(y)ydy + \int_{x-\Delta}^{x-l} f(y)(x-\Delta)dy + \int_{x-l}^{\infty} f(y)(2x-l-\Delta-y)dy\right] \\ &\leq -2\lambda\left[\int_l^{x_0} f(y)ydy - \int_{2x_0+\Delta-l}^{\infty} f(y)ydy\right] \\ &\leq -1. \end{aligned} \tag{6}$$

The same holds for $x < l - x_0$. It is easy to see that $\Delta V(x)$ is bounded for $x \in C_2$. Furthermore, since petite set $[l,\,\Delta]$ is uniformly accessible from C_2, C_2 is also petite. The drift condition holds. Therefore, by Theorem 13.0.1 in [2], we conclude that $\mathbf{Y}$ is positive Harris. ■

References

[1] T. He, L. Tong, and A. Swami, "Relative Capacity of Covert Information Flows." submitted to the 28th IEEE Conference on Computer Communications (INFOCOM'09), Auguest 2008.

[2] S. Meyn and R. Tweedie, *Markov Chains and Stochastic Stability*. London, UK: Springer-Verlag, 1993.