The Timing Capacity of Single-Server Queues with Multiple Flows

Xin Liu and R. Srikant

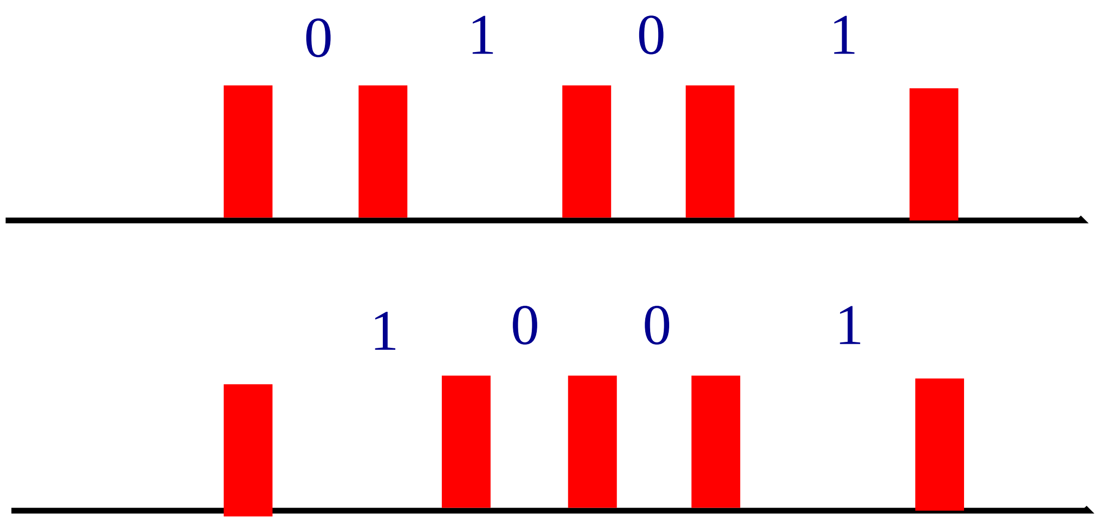
Coordinated Science Laboratory

University of Illinois at Urbana Champaign

March 14, 2003

Timing Channel

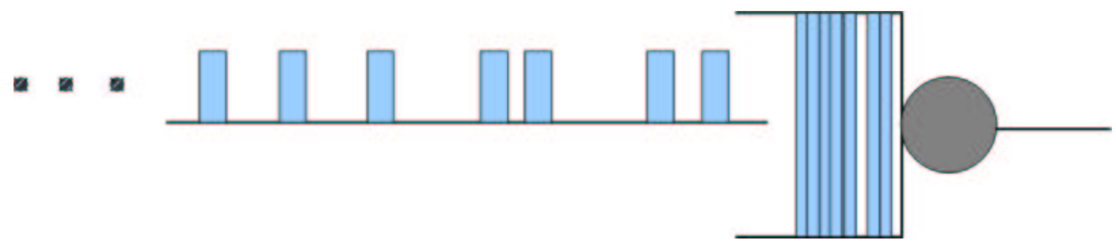
- Information can be transmitted through the timing-intervals between messages/events



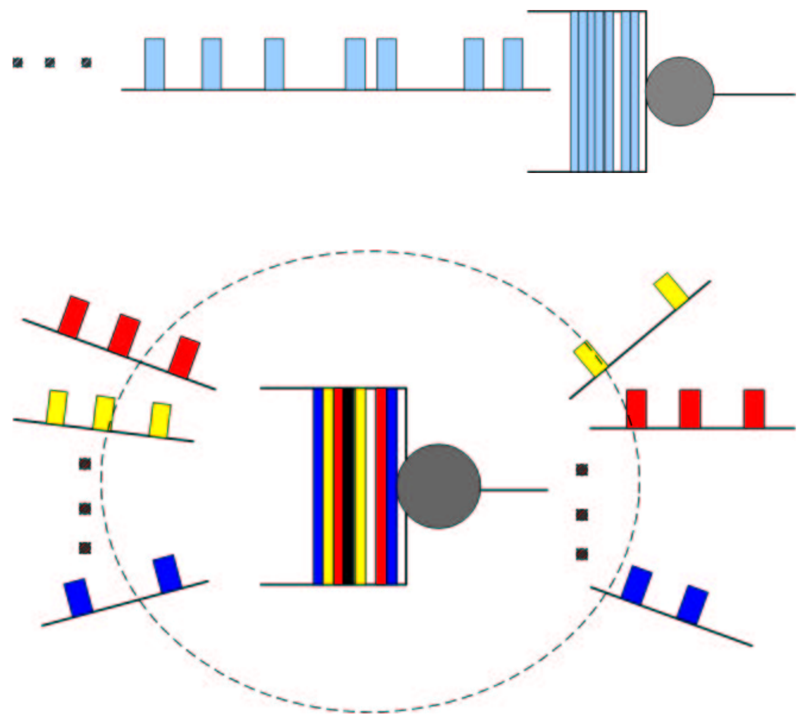
Distortion

- Distortion of timing information

- Queueing is a mechanism that naturally blurs the timing information



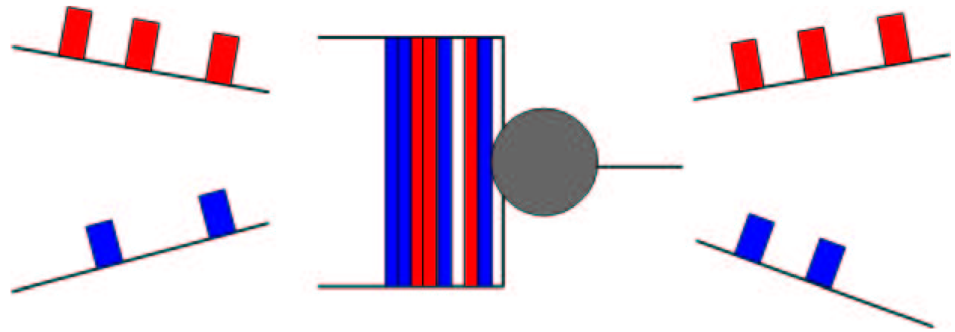
Multiple Flows



What is the sum timing capacity?

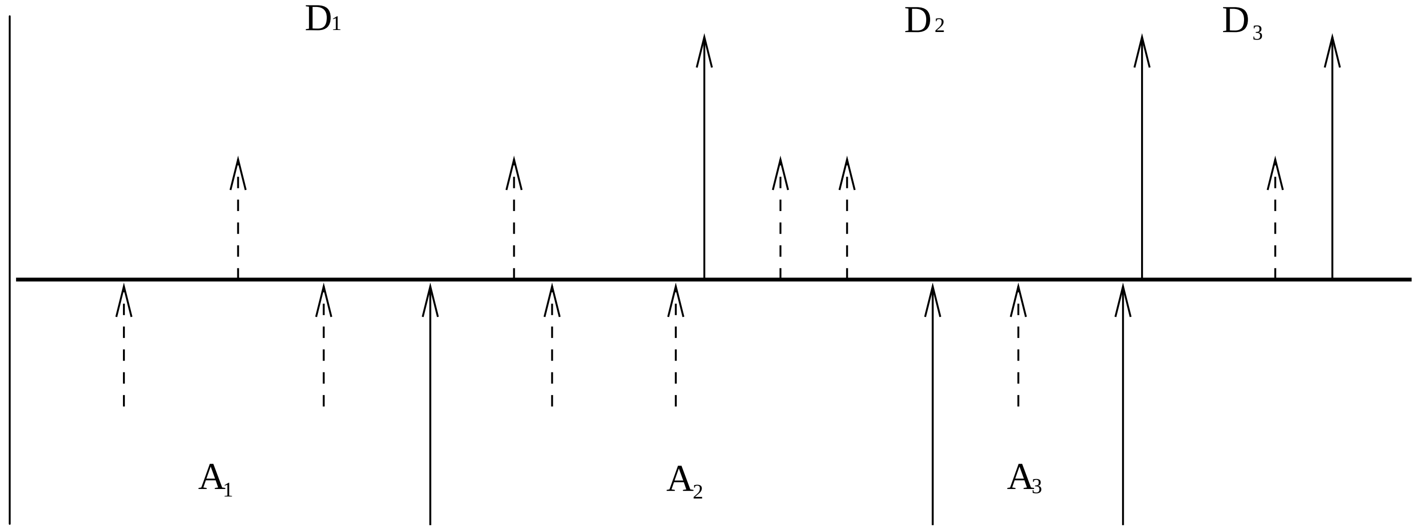
Interference Flow

- What is the timing capacity of a flow when there exists uncontrollable and undetectable cross traffic?



An Exponential Server Queue

- Interference flow: Poisson arrival with rate λ_I
- Service time distribution for all packets: i.i.d. exponentially distributed with mean $1/\mu$



A Lower Bound on Capacity

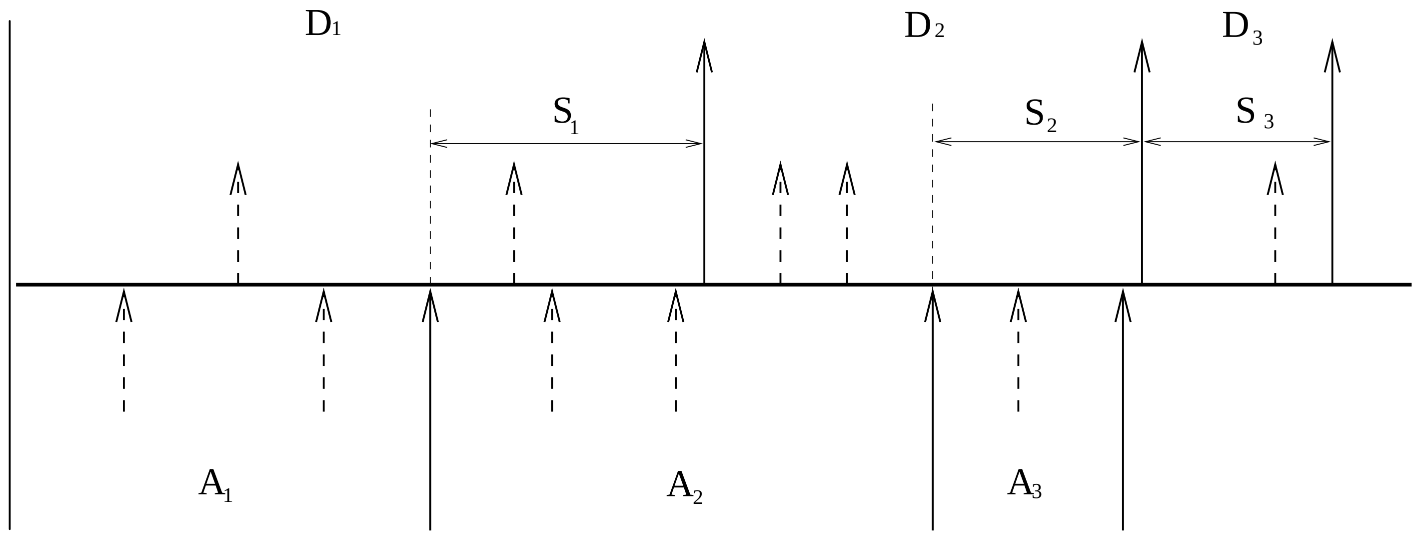
- Service discipline: FIFO
- A lower bound on the timing capacity is

$$C_L(\lambda_0) = \lambda_0 \log\left(\frac{\mu - \lambda_I}{\lambda_0}\right),$$

  where $\lambda_0 + \lambda_I \leq \mu$.
- Input process: Poisson with rate λ_0.
- Special case: $\lambda_I = 0$

$$C(\lambda_0) = \lambda_0 \log \frac{\mu}{\lambda_0}.$$

Intuition



- Randomness is caused by queue and service time
- Effective service time is exponentially distributed with mean $1/(\mu - \lambda_I)$.

Proof

$$
\begin{aligned}
I(A^n; D^n) &= h(D^n) + h(A^n) - h(D^n, A^n) \\
&\overset{(1)}{=} h(D^n) + h(A^n) - h(S^n, A^n) \\
&= h(D^n) - h(S^n|A^n) \\
&\geq h(D^n) - h(S^n) \\
&\geq h(D^n) - \sum_{i=1}^{n} h(S_i) \\
&\overset{(2)}{=} \sum_{i=1}^{n} \left(\log \frac{1}{\lambda_0} + 1\right) - \sum_{i=1}^{n} \left(\log \frac{1}{\mu - \lambda_I} + 1\right) \\
&= \sum_{i=1}^{n} \log \frac{\mu - \lambda_I}{\lambda_0},
\end{aligned}
$$

Number of Effective Interfering Packets

- n_i: number of effective interfering packets

$$
\begin{aligned}
P(n_i = k) &= \sum_{j=k}^{\infty} \pi(j) p(k|j) \\
&= p(k|k)\pi(k) + \sum_{j=k+1}^{\infty} p(k|j)\pi(k) \\
&= (1-\rho)\rho^k (1-q_0)^k + \sum_{j=k+1}^{\infty} (1-\rho)\rho^j (1-q_0)^k q_0 \\
&= \left(\frac{\lambda_I}{\mu}\right)^k \left(1 - \frac{\lambda_I}{\mu}\right), \quad k = 0, 1, 2, \cdots
\end{aligned}
$$

$q_0 = \frac{\lambda_0}{\lambda_0 + \lambda_I}$: probability a packet belongs to flow 0

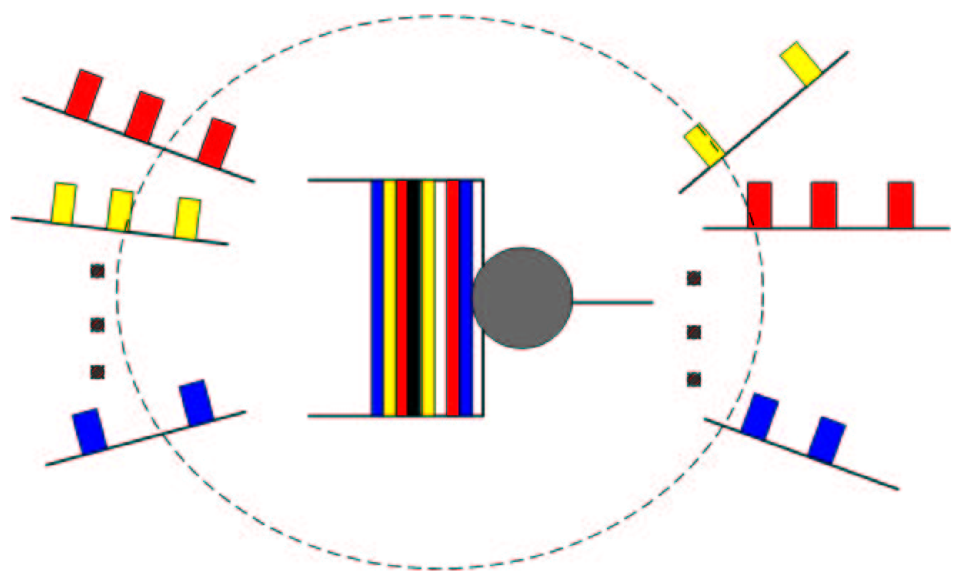
Effective Service Time

- $n_i + 1$: geometrically distributed with mean $\mu/(\mu - \lambda_I)$
- Effective service time: sum of $n_i + 1$ independent and exponentially distributed random variable is exponential with mean

$$E(S_i) = \frac{1}{\mu} E(n_i + 1) = \frac{1}{\mu - \lambda_I}.$$

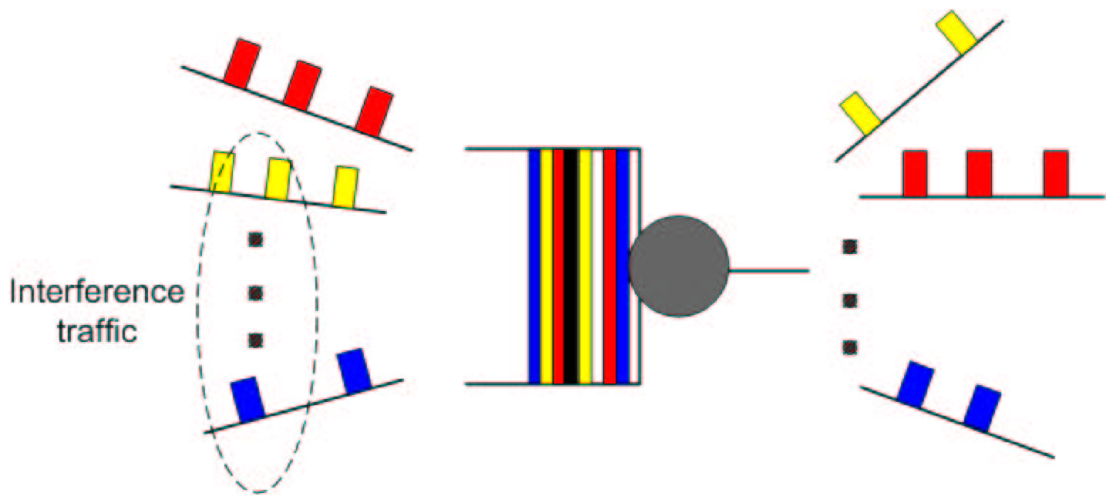
Multiple Flows

- N: number of flows
- $B = \log N$ bits for address
- Service times are i.i.d. exponentially distributed.



A Lower Bound

- The arrival process of each flow is an independent Poisson process with rate λ_i, $\sum \lambda_i \le \mu$.
- Consider all other flows as interference.



A Lower Bound Cont'd

- We have
$$C \geq \sum_i \lambda_i \log\left(\frac{\mu - \sum_{j\neq i}\lambda_j}{\lambda_i}\right).$$

- Lower bound is maximized when all users have the same arrival rate.

- Maximize over λ
$$C \geq (B - 1 - \log B)\mu.$$

Theorem

- Theorem: The timing capacity of the N flows satisfies

$$(B - 1 - \log B)\mu \leq C \leq B\mu.$$

- Upper bound holds because the overall information capacity cannot exceed $B\mu$ for $B \geq 2$ bits.

The Upper Bound

- X^n: information sent through the packets

$$
\begin{aligned}
& I(X^n, D^n; X^n, A^n) \\
= \quad & I(D^n; X^n, A^n) + I(X^n; X^n, A^n | D^n) \\
\overset{(1)}{=} \quad & I(D^n; A^n) + I(X^n; X^n) \\
\overset{(2)}{\leq} \quad & \mu B,
\end{aligned}
$$

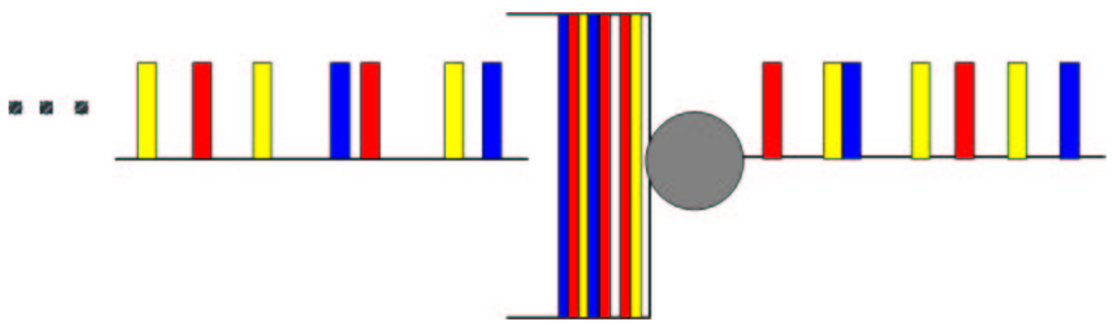
- (1): X^n contains no additional information regarding D^n other than that in A^n.
- (2): if $B > 1$ bit, the system capacity is μB.

Timing Capacity of Multiple Flows

- The arrival process of each flow is an independent Poisson process with rate λ, $N\lambda \leq \mu$.
- The lower bound is asymptotically tight.
- Timing capacity increases as the number of flows increases.

A Single Flow

- Each packet has B bits
- All B bits are used to distinguish sub-flows; i.e. there are $N = 2^B$ sub-flows

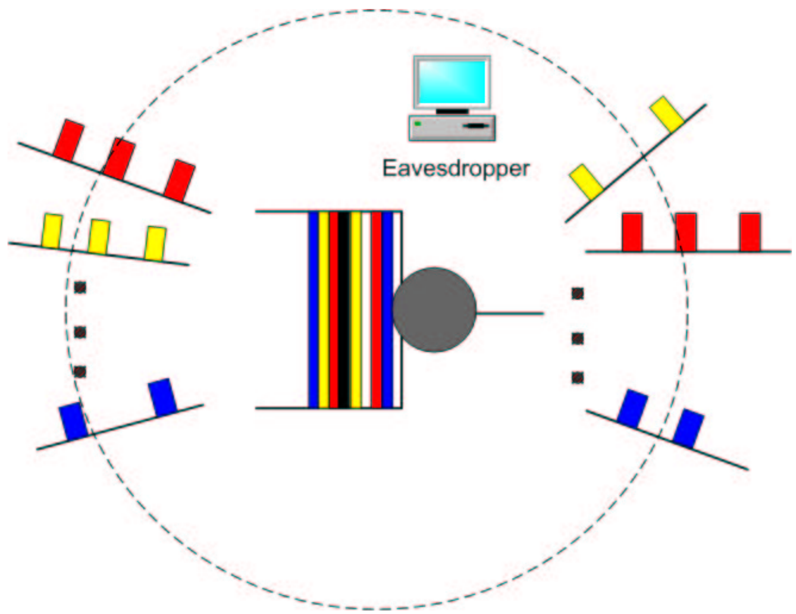


Timing Capacity of A Single Flow

- We have
$$(B - 1 - \log B)\mu \leq C_T \leq B\mu.$$
- The timing capacity is close to the server capacity $B\mu$ bits/sec
- Without splitting, it is 0.5309μ bits/sec
- A large amount of information can be conveyed through timing.
- When λ is small, the distortion caused by queueing delay is relatively small.

Covert Information

- Eavesdropper monitors the server, records packets in sequence



Covert Information

- Covert information C_c:

$$C_c = C_T - C_E,$$

  - C_T: information rate at the receiver
  - C_E: information rate at the eavesdropper

- Covert information: secrets that cannot be heard by the eavesdropper.

Two Flows

$$
\begin{aligned}
& I(A^n, B^m; N^{n+m}, D^{n+m}) \\
= \quad & h(A^n, B^m) + h(N^{n+m}, D^{n+m}) \\
& -h(A^n, B^m, N^{n+m}, D^{n+m}) \\
\leq \quad & h(A^n, B^m) + h(N^{n+m}, D^{n+m}) - h(A^n, B^m, D^{n+m}) \\
= \quad & h(A^n, B^m) + h(N^{n+m}, D^{n+m}) - h(A^n, B^m, S^{n+m}) \\
= \quad & h(N^{n+m}, D^{n+m}) - h(S^{n+m}) \\
\leq \quad & h(D^{n+m}) - h(S^{n+m}) + H(N^{n+m}).
\end{aligned}
$$

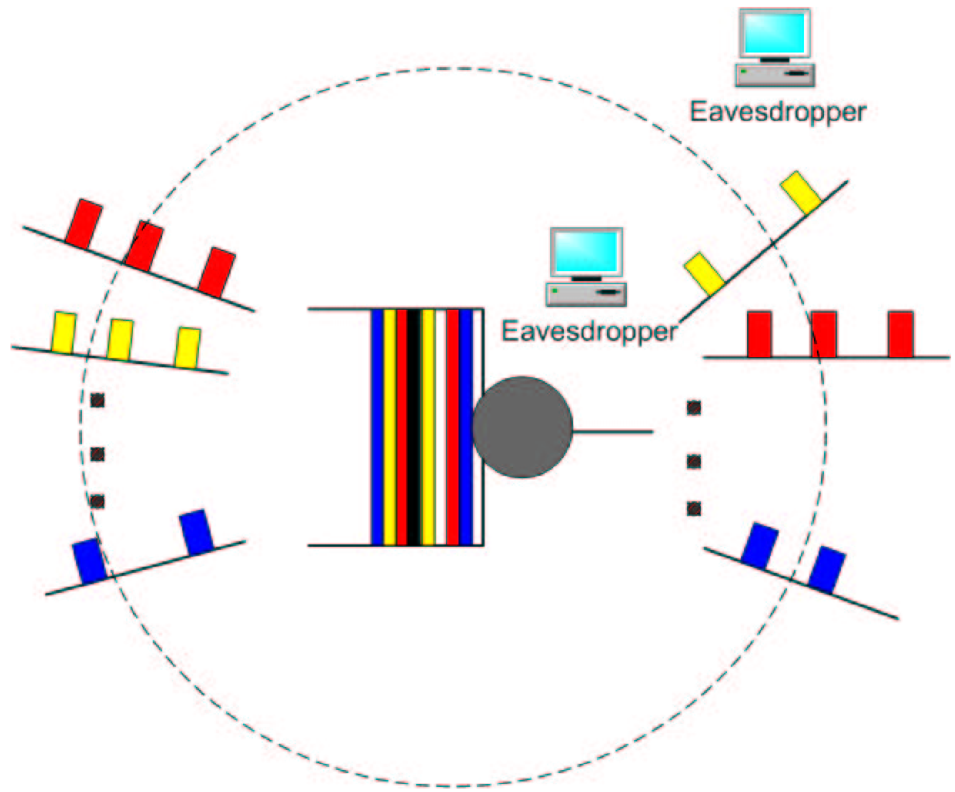
Covert Information Cont'd

- $I(A^n, B^m; N^{n+m}) = H(N^{n+m})$
  - FIFO
  - Eavesdropper located at the input of server.
- Covert information

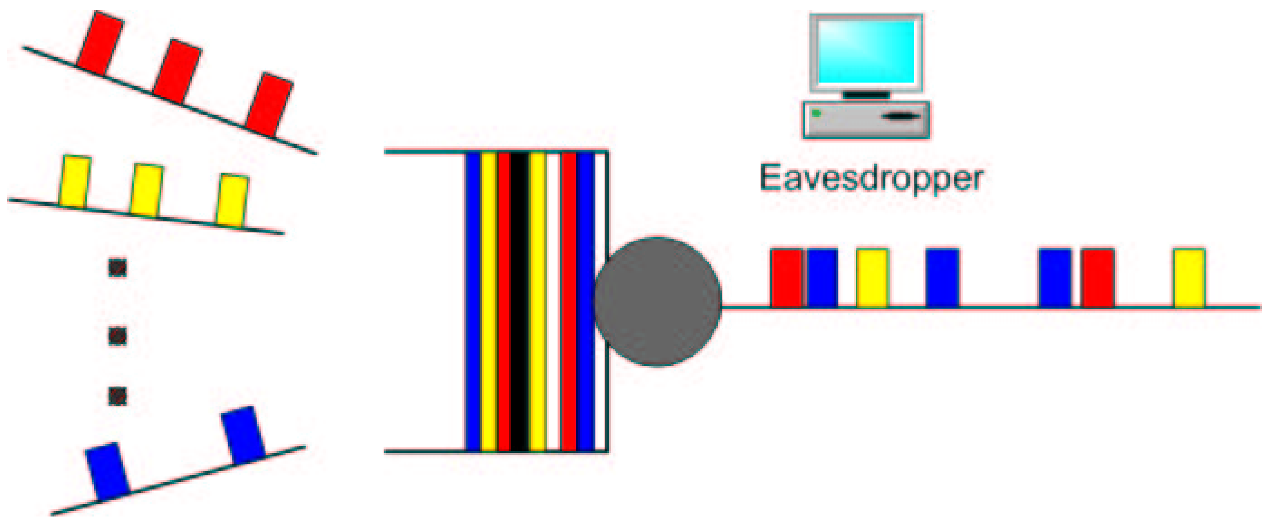
$$\begin{aligned} C_c &= C_T - C_E \\ &\leq \frac{\lambda_1 + \lambda_2}{n+m} \left(h(D^{n+m}) - h(S^{n+m}) \right), \end{aligned}$$

which is the covert information of a single flow with rate $\lambda_1 + \lambda_2$.

Location of the Eavesdropper



A Special Case



Service Disciplines

- First come first serve: covert information rate cannot be larger than that of a single flow.
- Random service discipline: covert information rate is larger than that of a single flow.
  - Intuition: timing information reduces randomness introduced by the service discipline.
  - Implementation: each packet randomly picks a diffserv class in its header.

Service Disciplines Cont'd

$$
\begin{aligned}
& I(A^n, B^m; N^{n+m}, D^{n+m}) \\
= \; & h(A^n, B^m) + h(N^{n+m}, D^{n+m}) - h(A^n, B^m, N^{n+m}, D^{n+m}) \\
= \; & h(A^n, B^m) + h(N^{n+m}, D^{n+m}) - h(A^n, B^m, S^{n+m}, N^{n+m}) \\
= \; & h(A^n, B^m) + h(N^{n+m}, D^{n+m}) - h(A^n, B^m, S^{n+m}) \\
= \; & h(N^{n+m}, D^{n+m}) - h(S^{n+m}) \\
= \; & h(D^{n+m}) - h(S^{n+m}) + h(N^{n+m}).
\end{aligned}
$$

Random Service Discipline

Total information:

$$
\begin{aligned}
& I(A^n, B^m; N^{n+m}, D^{n+m}) \\
= \quad & h(D^{n+m}) - h(S^{n+m}) + h(N^{n+m}) - h(N^{n+m}|A^n, B^m, S^{n+m})
\end{aligned}
$$

Eavesdropper:

$$I(N^{n+m}; A^n, B^m) = h(N^{n+m}) - h(N^{n+m}|A^n, B^m).$$

Covert information:

$$h(D^{n+m}) - h(S^{n+m}) + h(N^{n+m}|A^n, B^m) - h(N^{n+m}|A^n, B^m, S^{n+m}).$$

Random Service Discipline Cont'd

- $h(D^{n+m}) - h(S^{n+m})$ is maximized when the input is Poisson.
- $h(N^{n+m}|A^n, B^m) - h(N^{n+m}|A^n, B^m, S^{n+m})$ is positive because N^{n+m} is not independent of S^{n+m} conditioned on (A^n, B^m).

Discrete-Time Case

- $N = 2^B$: number of flows
- Geometric service time with mean $1/\mu$:

$$\mu(B-1) - \mu \log(B-1) \leq C \leq \mu B + 1$$

- Deterministic service time (one packet/slot):

$$(B-1) - \log(B-1) \leq C \leq B + 1$$

General Case

- General service-time distribution:

$$\frac{B-1}{B}\mu\left(B-\log\left(1+\frac{B\mu^2E(S^2)}{2}\right)\right)\le C\le B\mu+1,$$

  where $E(S^2)$ is the second moment of the service-time

- Queueing statistics of a general server queue is unknown.

- Basic idea: use waiting time + service time as an upper bound for the effective service time.

- Good approximation for small λ.

Conclusion

- An asymptotically tight lower bound on the timing capacity in the presence of interference traffic
- Timing information for multiple flows
  - Continuous case
  - Discrete case
- Coloring increases the timing information conveyed by a single flow.
- The location of the eavesdropper is important. It can significantly decrease the amount of covert information.

Note

$$
\begin{aligned}
& h(N^{n+m}|A^n, B^m) - h(N^{n+m}|A^n, B^m, S^{n+m}) \\
= \quad & \sum_{i=1}^{n+m} I(N_i; D^{n+m}|A^n, B^m, N^{i-1}).
\end{aligned}
$$

$$
\begin{aligned}
& I(N_i; D^{n+m}|A^n, B^m, N^{i-1}) \\
= \quad & \sum_{j=1}^{n+m} I(N_i; D_j|A^n, B^m, D^{j-1}, N^{i-1}) \\
\geq \quad & I(N_i; D_{i-1}|A^n, B^m, D^{i-2}, N^{i-1}) \\
= \quad & \int f(A^n, B^m, D^{i-2}) E\left(\log \frac{p(N_i|D_{i-1}, A^n, B^m, D^{i-2})}{p(N_i|A^n, B^m, D^{i-2})}\right).
\end{aligned}
$$

- To show $I(N_i; D^{n+m}|A^n, B^m, N^{i-1})$ is positive, we only need to show that with a positive probability $p(N_i = m|D_{i-1}, A^n, B^m, D^{i-2}, N^{i-1}) \neq p(N_i = m|A^n, B^m, D^{i-2}, N^{i-1})$, $m = 1, 2$. Consider the case where after the departure of $(i-2)$th packet, there is more than 1 packet in the queue. This event happens with a positive probability. Consider two events with positive probabilities: 1) during the service time of the

$(i-1)$th packet, no new packet arrives. 2) during the service time of the $(i-1)$th packet, one new packet arrives. Apparently, in these two cases, $p(N_i = m | D_{i-1}, A^n, B^m, D^{i-2}, N^{i-1})$ is different. Thus, $p(N_i = m | D_{i-1}, A^n, B^m, D^{i-2}, N^{i-1}) \neq p(N_i = m | A^n, B^m, D^{i-2}, N^{i-1})$ with a positive probability.