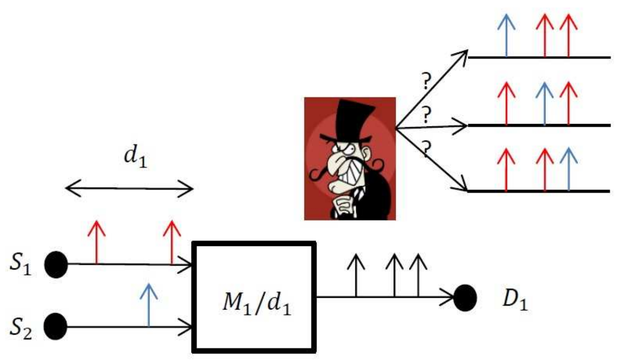
Optimizing the Delay Anonymity Trade-off in Data Networks

{ Omid Javidbakht and Parv Venkitasubramaniam}

LEHIGH UNIVERSITY

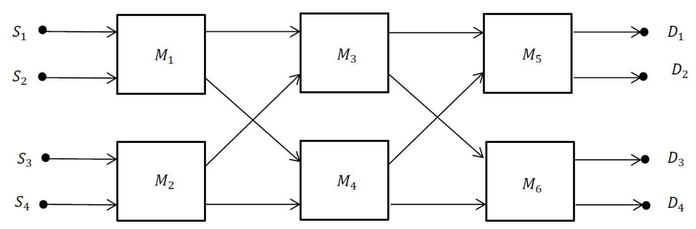
Introduction

Mix can provide anonymity by delaying, shuffling and reordering the incoming packets.(Chaum Mix(1981)).



Problem

1. In TOR, each source chooses 3 intermediate nodes and transmits packets through this route.



How to allocate the rate between the possible routes to get more anonymity?

System Model

1. Each source S_i transmits packets to each destination D_j according to an independent Poisson process of rate Λ_{ij} through different routes.
2. Eavesdropper (Eve) knows the mixing strategy but does not know realization of the router's randomness.
3. Anonymity is defined as

$$\mathcal{A} = \lim_{n\to\infty} \frac{\mathbb{E}(H(X_1,\ldots,X_n|\Phi))}{n}$$

where Φ denotes Eve's complete observation.

Main Results

1. In **heavy traffic regime**, the maximum anonymity in a multipath multiple destination mix network is achieved for any set of allocated rates.
2. In **light traffic regime**, there exists a unique single route for each pair of source and destination such that overall anonymity in the network is maximized.

Heavy Traffic

Anonymity of any arbitrary network in the heavy traffic rate regime is lower bounded by:

$$\mathcal{A}_M(\lambda) \geq \sum_{i=1}^{|\mathcal{M}|}\sum_{j=1}^{\xi_i} \frac{w^j_{M_i}}{w}(\mathcal{A}^j_{M_i} - \sum_{k=1}^{|\mathcal{S}|} \frac{\sum_{u=1}^{\zeta_i} w^{jk}_{M_i u}}{w^j_{M_i}} H(\frac{w^{jk}_{M_i 1}}{\sum_{u=1}^{\zeta_i} w^{jk}_{M_i u}},\cdots,\frac{w^{jk}_{M_i \zeta_i}}{\sum_{u=1}^{\zeta_i} w^{jk}_{M_i u}}))$$

Theorem 1 *If each mix utilizes an asymptotically optimal mixing strategy, then the maximum anonymity in a multiple destination mix network is achieved for any set of allocated rates.*

Light Traffic

Theorem 2 *The solutions $\lambda^*_{P_k^{(i,j)}}$ which maximizes the total light traffic anonymity of any mix network must necessarily be of the form:*

$$\forall i,j \exists k_{ij} \text{ s.t. } \lambda^*_{P^{(i,j)}_{k_{ij}}} = \frac{\lambda}{M}, \lambda^*_{P^{(i,j)}_{l}} = 0, l \neq k_{ij}$$

Proof hints:

1. Our goal is optimizing anonymity function under some linear constraints.

$$\max_{\lambda_{P_k^{(i,j)}}} sd_{max} \sum_{i,j,k,u\neq i,v,l} \frac{\lambda_{P_k^{(i,j)}}}{\lambda_T}\frac{\lambda_{P_l^{(u,v)}}}{\lambda_T}\Upsilon(i,j,k,u,v,l)$$

2. All the elements on the diagonal of the Hessian matrix are zero which means all the valid solutions are saddle points.
3. Considering the boundary, all the feasible solutions will be saddle points.

Delay-Anonmity Tradeoff

What is the cost of getting higher anonymity?

1. End to end delay is a linear function of rate allocation parameters.
2. Our goal is optimizing a weighted reward including both anonymity and delay.

$$\max_{\lambda_{P_k^{(i,j)}}} \alpha\mathcal{A} + (1-\alpha)\mathcal{D}$$

3. The result of Theorem 2 is also valid for delay anonymity tradeoff.

Conclusion

1. In high enough rates, changes in rate allocation makes negligible difference. Thus, sources can optimize their multipath route selection based on other desired QoS metrics.
2. Although the optimal rate allocation for medium traffic rates is theoretically an open problem, the light traffic optimal scheme performs quite well for medium traffic rates.
3. Our result can be utilized by an efficient algorithm to determine the optimal single path routes given end-to-end delay constraints.

Numerical Result