Technical Report TSC/SO/24082016: Filter design for delay-based anonymous communications

Simon Oya Fernando Pérez-González Carmela Troncoso

In this report, we provide an expression for the overall MSE ξ_T of the best linear estimator of $\mathbf{P}$, described in [1], under the following conditions:

1. The number of rounds observed by the adversary goes to infinity ($\rho \to \infty$) and it is much larger than the number of users in the system ($\rho \gg N$).
2. The input processes are i.i.d. as a Poisson distribution, i.e., $X_i^r \sim P(\mu(i))$.
3. The average number of messages sent each round by all the users is much larger than one, i.e., $\sum_{i=1}^N \mu(i) \gg 1$.

The expression we obtain only depends on the delay characteristic $\mathbf{d} \doteq [d_0, d_1, \cdots, d_{\rho-1}]^T$ through the following parameters:

$$\gamma_1 \doteq \sum_k d_k^2 \tag{1}$$

$$\gamma_2 \doteq \sum_r \left(\sum_k d_r d_{r+k}\right)^2 \tag{2}$$

$$\gamma_3 \doteq \sum_k d_k^3. \tag{3}$$

After obtaining an expression for ξ_T, we prove that the MSE grows with $1/\gamma_1$ when the "sharpness" of each sender, defined as $\nu_i \doteq \sum_{j=1}^M p_{j,i}^2$ for sender i, is almost zero, i.e., $\nu_i \approx 0$, for all $i \in \{1, \cdots, N\}$. We also prove that the overall MSE grows with $(\gamma_1 - \gamma_2)/\gamma_1^2$ when $\nu_i \approx 1$ for all i.

1 Theoretical expression for ξ_T.

From [1], we get that

$$\xi_T = \mathrm{E}\left\{\mathrm{Tr}\left\{\mathbf{M}(\mathbf{X}^T\mathbf{D}^T\mathbf{D}\mathbf{X})^{-1}\mathbf{X}^T\mathbf{D}^T\mathbf{\Sigma}_{\mathbf{N}|\mathbf{X}}\mathbf{D}\mathbf{X}(\mathbf{X}^T\mathbf{D}^T\mathbf{D}\mathbf{X})^{-1}\mathbf{M}\right\}\right\}, \tag{4}$$

where

$$\mathbf{\Sigma}_{\mathbf{N}|\mathbf{X}} = \mathrm{diag}\left\{\mathbf{D}\mathbf{X}\mathbf{1}_N\right\} - \mathbf{D}\cdot\mathrm{diag}\left\{\mathbf{X}\boldsymbol{\nu}\right\}\cdot\mathbf{D}^T. \tag{5}$$

We define $\mathbf{R}_{xx} \doteq \frac{1}{\rho}\mathbf{X}^T\mathbf{D}^T\mathbf{D}\mathbf{X}$ and $\mathbf{R}_{xyx} \doteq \frac{1}{\rho}\mathbf{X}^T\mathbf{D}^T\mathbf{\Sigma}_{\mathbf{N}|\mathbf{X}}\mathbf{D}\mathbf{X}$, and note that (4) can be written as $\xi_T = \mathrm{E}\left\{\mathrm{Tr}\left\{\mathbf{M}\mathbf{R}_{xx}^{-1}\mathbf{R}_{xyx}\mathbf{R}_{xx}^{-1}\mathbf{M}\right\}\right\}$. The entries of $\mathbf{R}_{xx}$ and $\mathbf{R}_{xyx}$ are sample averages over ρ, and therefore as ρ grows they get closer to their expected value. Using that the the input samples in $\mathbf{X}$ are i.i.d. Poissonian with rates $\boldsymbol{\mu} \doteq [\mu(1), \cdots, \mu(N)]^T$, we can compute

$$\mathbf{R}_{xx} = \boldsymbol{\mu}\boldsymbol{\mu}^T + \gamma_1 \cdot \mathrm{diag}\left\{\boldsymbol{\mu}\right\} . \tag{6}$$

On the other hand, we can expand $\mathbf{R}_{xyx}$ as

$$\mathbf{R}_{xyx} = \frac{1}{\rho}\mathbf{X}^T\mathbf{D}^T\mathrm{diag}\left\{\mathbf{D}\mathbf{X}\mathbf{1}_N\right\}\mathbf{D}\mathbf{X} - \frac{1}{\rho}\mathbf{X}^T\mathbf{D}^T\mathbf{D}\mathrm{diag}\left\{\mathbf{X}\boldsymbol{\nu}\right\}\mathbf{D}^T\mathbf{D}\mathbf{X} . \tag{7}$$

Let $\mathbf{R}'_{xyx}$ and $\mathbf{R}''_{xyx}$ be the first and second summands of this expression, respectively. These summands can be written, when $\rho \to \infty$, as

$$\mathbf{R}'_{xyx} = \boldsymbol{\mu}\boldsymbol{\mu}^T\left(2\gamma_1 + \sum_{i=1}^{N}\mu(i)\right) + \mathrm{diag}\left\{\boldsymbol{\mu}\right\}\left(\gamma_3 + \gamma_1 \cdot \sum_{i=1}^{N}\mu(i)\right) , \tag{8}$$

and

$$\begin{aligned} \mathbf{R}''_{xyx} \quad &= \quad \boldsymbol{\mu}\boldsymbol{\mu}^T \cdot \sum_{i=1}^{N}\mu(i)\nu_i + \gamma_1 \cdot \left[(\boldsymbol{\mu}\circ\boldsymbol{\nu})\boldsymbol{\mu}^T + \boldsymbol{\mu}(\boldsymbol{\mu}\circ\boldsymbol{\nu})^T\right] \\ &+ \quad \gamma_2 \cdot \mathrm{diag}\left\{\boldsymbol{\mu}\right\} \cdot \sum_{i=1}^{N}\mu(i)\nu_i + \gamma_1^2 \cdot \mathrm{diag}\left\{\boldsymbol{\mu}\circ\boldsymbol{\nu}\right\} . \end{aligned} \tag{9}$$

where $\circ$ is the entry-wise or Hadamard product.

In order to compute ξ_T, we need an expression for $\mathbf{R}_{xx}^{-1}$. Using the Sherman-Morrison formula in (6), we can write

$$\mathbf{R}_{xx}^{-1} = \frac{1}{\gamma_1}\left(\mathrm{diag}\left\{\boldsymbol{\mu}\right\}^{-1} - \frac{\mathbf{1}_N\mathbf{1}_N^T}{\gamma_1 + \sum_{i=1}^{N}\mu(i)}\right) . \tag{10}$$

We then use our assumption $\sum_{i=1}^{N}\mu(i) \gg 1$ and the fact that $1 \geq \gamma_1$ to approximate $\gamma_1 + \sum_{i=1}^{N}\mu(i) \approx \sum_{i=1}^{N}\mu(i)$ in this expression.

Finally, we perform the matrix multiplications to obtain $\mathbf{M}\mathbf{R}_{xx}^{-1}\mathbf{R}_{xyx}\mathbf{R}_{xx}^{-1}\mathbf{M}$ and compute its trace to obtain a closed-form expression for ξ_T:

$$\begin{aligned} \xi_T \quad &\approx \quad \frac{1}{\rho}\cdot\frac{1}{\gamma_1^2}\cdot\left(\gamma_1\cdot\sum_{i=1}^{N}\mu(i) - \gamma_2\cdot\sum_{i=1}^{N}\mu(i)\nu_i + \gamma_3\right)\cdot\left[\sum_{i=1}^{N}\mu(i) - \frac{\sum_{i=1}^{N}\mu(i)^2}{\sum_{i=1}^{N}\mu(i)}\right] \\ &+ \quad \frac{1}{\rho}\cdot\left[\left(\frac{\sum_{i=1}^{N}\mu(i)^2}{(\sum_{i=1}^{N}\mu(i))^2} + 1\right)\cdot\sum_{i=1}^{N}\mu(i)\nu_i - \frac{\sum_{i=1}^{N}\mu(i)^2\nu_i}{\sum_{i=1}^{N}\mu(i)}\right] . \end{aligned} \tag{11}$$

We study now the dependence of ξ_T on the delay characteristic when $\nu_i \approx 0$ and $\nu_i \approx 1$. Note that, regardless of the value of ν_i, the second term in (11) does not depend on the delay characteristic, so we can disregard it when studying how to design the delay characteristic to increase the MSE.

2 Dependence of ξ_T on the delay characteristic

2.1 First scenario ($\nu_i \approx 0$).

In this case, we can write

$$\gamma_1 \cdot \sum_{i=1}^{N} \mu(i) - \gamma_2 \cdot \sum_{i=1}^{N} \mu(i)\nu_i + \gamma_3 \approx \gamma_1 \cdot \sum_{i=1}^{N} \mu(i) + \gamma_3 \approx \gamma_1 \cdot \sum_{i=1}^{N} \mu(i) \,, \tag{12}$$

where the first step comes from $\nu_i \approx 0$ and the second one from $\gamma_3 \leq \gamma_1$ and $\sum_{i=1}^{N} \mu(i) \gg 1$. Since the second term of (11) can be disregarded when $\nu_i \approx 0$, we have

$$\xi_T \approx \frac{1}{\rho} \cdot \frac{1}{\gamma_1} \cdot \sum_{i=1}^{N} \mu(i) \cdot \left[\sum_{i=1}^{N} \mu(i) - \frac{\sum_{i=1}^{N} \mu(i)^2}{\sum_{i=1}^{N} \mu(i)} \right] . \tag{13}$$

Then, the overall MSE of the adversary is proportional to $1/\gamma_1$, and therefore in order to increase ξ_T we must increase $1/\gamma_1$.

2.2 Second scenario ($\nu_i \approx 1$).

Here, by evaluating $\nu_i \approx 1$ and using the same approximations above, we get

$$\xi_T \approx \frac{1}{\rho} \cdot \sum_{i=1}^{N} \mu(i) \cdot \left[\frac{\gamma_1 - \gamma_2}{\gamma_1^2} \cdot \left(\sum_{i=1}^{N} \mu(i) - \frac{\sum_{i=1}^{N} \mu(i)^2}{\sum_{i=1}^{N} \mu(i)} \right) + 1 \right] . \tag{14}$$

We can see that, in order to increase ξ_T, we must increase $(\gamma_1 - \gamma_2)/\gamma_1^2$.

This concludes the proof.

References

[1] Simon Oya, Fernando Pérez-González, and Carmela Troncoso, "Filter design for delay-based anonymous communications," Under submission.