Technical Report TSC/SO/02052014: Derivation of the Mean Squared Error of the Least Squares Estimator in a Timed Pool Mix with Dummy Traffic

Simon Oya   Carmela Troncoso   Fernando Pérez-González

May 2, 2014

In this report, we derive an expression for the Mean Squared Error (MSE) per transition probability $p_{j,i}$ of the least-squares estimator presented in [1], defined as $\texttt{MSE}_{j,i} \doteq |\hat{p}_{j,i} - p_{j,i}|^2$. Please refer to [1] for the thorough description of the system and adversary model considered, as well as the notation used in this document.

We start by showing that this estimator is unbiased: using the law of total expectation together with $\mathrm{E}\{\mathbf{Y}_j|\,\mathbf{U}\} = \hat{\mathbf{U}}_s \cdot \mathbf{p}_j$,

$$\mathrm{E}\{\hat{\mathbf{p}}_j\} = \mathrm{E}\{\mathrm{E}\{\hat{\mathbf{p}}_j|\mathbf{U}\}\} = \mathrm{E}\left\{(\hat{\mathbf{U}}_s^T\hat{\mathbf{U}}_s)^{-1}\hat{\mathbf{U}}_s^T\mathrm{E}\{\mathbf{Y}_j|\mathbf{U}\}\right\} = \mathbf{p}_j \tag{1}$$

Therefore, computing the MSE per transition probability is equivalent to computing the variance of the estimator, $\mathrm{Var}\{\hat{p}_{j,i}\}$. In order to do so, we look for the i-th element in the diagonal of the covariance matrix of $\hat{\mathbf{p}}_j$, denoted $\mathbf{\Sigma}_{\mathbf{p}_j}$. Using the law of total variance and $\mathrm{Var}\{\mathrm{E}\{\hat{p}_{j,i}|\mathbf{U}\}\} = 0$ (which is straightforward from (1)), we can write the covariance matrix as

$$\begin{aligned}\mathbf{\Sigma}_{\mathbf{p}_j} &= \mathrm{E}\left\{\mathbf{\Sigma}_{\mathbf{p}_j|\mathbf{U}}\right\} = \mathrm{E}\left\{(\hat{\mathbf{U}}_s^T\hat{\mathbf{U}}_s)^{-1}\hat{\mathbf{U}}_s^T\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}\hat{\mathbf{U}}_s(\hat{\mathbf{U}}_s^T\hat{\mathbf{U}}_s)^{-1}\right\} \\ &= \mathbf{P}_\lambda^{-1}\mathrm{E}\left\{(\mathbf{U}^T\mathbf{B}^T\mathbf{B}\mathbf{U})^{-1}\mathbf{U}^T\mathbf{B}^T\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}\mathbf{B}\mathbf{U}(\mathbf{U}^T\mathbf{B}^T\mathbf{B}\mathbf{U})^{-1}\right\}\mathbf{P}_\lambda^{-1}\end{aligned} \tag{2}$$

In order to develop this expression, we need to assume that $\rho \to \infty$ and use the Law of Large Numbers to make $(\mathbf{U}^T\mathbf{B}^T\mathbf{B}\mathbf{U})$ approximately independent from the observed inputs $\mathbf{U}$. This is, given that the input process X_i^r is stationary and memoryless, we can write

$$\lim_{\rho\to\infty}(\mathbf{U}^T\mathbf{B}^T\mathbf{B}\mathbf{U})/\rho \to \hat{\mathbf{R}}_{xs} \tag{3}$$

where the (m,n)-th element of $\hat{\mathbf{R}}_{xs}$ is

$$(\hat{\mathbf{R}}_{xs})_{m,n} = \frac{1}{\rho}\sum_{k=1}^{\rho}\sum_{r=1}^{k}\sum_{s=1}^{k}\mathrm{E}\{X_m^r X_n^s\}\,\alpha^2(1-\alpha)^{2k-r-s} \tag{4}$$

We can easily find a matricial expression for $\hat{\mathbf{R}}_{xs}$. First, using the hypotheses described in Sect. 4 of [1],

$$\mathrm{E}\{X_m^r X_n^s\} = \begin{cases}(\lambda_m+\delta_m)^2 + \lambda_m + \delta_m, & \text{if } m=n,\ r=s \\ (\lambda_m+\delta_m)(\lambda_n+\delta_n), & \text{otherwise.}\end{cases} \tag{5}$$

Then, if we assume that $\rho \gg 1/\alpha$ and define $\alpha_q = \alpha/(2-\alpha)$, we can approximate this autocorrelation matrix by

$$\hat{\mathbf{R}}_{xs} \approx (\mathbf{F}_\lambda + \mathbf{F}_\delta)[\mathbf{1}_{N\times N} + \alpha_q(\mathbf{F}_\lambda + \mathbf{F}_\delta)^{-1}](\mathbf{F}_\lambda + \mathbf{F}_\delta) \tag{6}$$

where $\mathbf{F}_\lambda \doteq \mathrm{diag}\{\lambda_1, \cdots, \lambda_N\}$ and $\mathbf{F}_\delta \doteq \mathrm{diag}\{\delta_1, \cdots, \delta_N\}$. Its inverse, computed by applying the Sherman-Morrison formula, is

$$\hat{\mathbf{R}}_{xs}^{-1} \approx \frac{1}{\alpha_q}\left((\mathbf{F}_\lambda + \mathbf{F}_\delta)^{-1} - \frac{1}{\alpha_q + \mathrm{tr}(\mathbf{F}_\lambda + \mathbf{F}_\delta)}\mathbf{1}_{N\times N}\right) \tag{7}$$

where $\mathrm{tr}(\cdot)$ denotes the trace operation. Going back to (2), our problem is to compute the i-th element of the diagonal of

$$\mathbf{\Sigma}_{\mathbf{P}_j} = \mathrm{E}\left\{\mathbf{\Sigma}_{\mathbf{P}_j|\mathbf{U}}\right\} \approx \frac{1}{\rho^2}\mathbf{P}_\lambda^{-1}\hat{\mathbf{R}}_{xs}^{-1}\mathrm{E}\left\{(\mathbf{BU})^T\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}\mathbf{BU}\right\}\hat{\mathbf{R}}_{xs}^{-1}\mathbf{P}_\lambda^{-1} \tag{8}$$

We follow three steps:

1. Compute $\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}$.
2. Compute $\frac{1}{\rho}\mathrm{E}\left\{(\mathbf{BU})^T\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}\mathbf{BU}\right\}$.
3. Get the i-th element of the diagonal of $\mathbf{\Sigma}_{\mathbf{P}_j}$.

Computation of $\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}$.

Our aim to compute $\mathrm{E}\left\{(\mathbf{Y}_j - \mathrm{E}\{\mathbf{Y}_j|\mathbf{U}\})(\mathbf{Y}_j - \mathrm{E}\{\mathbf{Y}_j|\mathbf{U}\})^T|\mathbf{U}\right\}$. Since the variables $Y_{\lambda,j}^r$ and $Y_{\delta,j}^r$ are independent, we can split this computation into two subproblems:

1. Using the law of total variance, it can be shown that

$$\begin{aligned} \mathrm{Var}\left\{Y_{\lambda,j}^r|\mathbf{U}\right\} &= \sum_{m=1}^{r}\sum_{i=1}^{N} x_i^m\left(P_{\lambda_i}p_{j,i}\alpha(1-\alpha)^{r-m} - P_{\lambda_i}^2 p_{j,i}^2\alpha^2(1-\alpha)^{2(r-m)}\right) \\ \mathrm{Cov}\left\{Y_{\lambda,j}^r, Y_{\lambda,j}^s|\mathbf{U}\right\} &= -\alpha^2(1-\alpha)^{r-s}\sum_{m=1}^{s}\left((1-\alpha)^{2(s-m)}\sum_{i=1}^{N} x_i^m P_{\lambda_i}^2 p_{j,i}^2\right) \quad r \geq s \end{aligned} \tag{9}$$

2. On the other hand, since the variables $Y_{\delta,j}^r$ and $Y_{\delta,j}^s$ are independent for $r \neq s$, we get

$$\begin{aligned} \mathrm{Var}\left\{Y_{\delta,j}^r|\mathbf{U}\right\} &= \delta_{\mathtt{MIX}}p_{j,\mathtt{MIX}} \\ \mathrm{Cov}\left\{Y_{\delta,j}^r, Y_{\delta,j}^s|\mathbf{U}\right\} &= 0 \end{aligned} \tag{10}$$

We can therefore write $\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}$ in matricial form as:

$$\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}} = \mathrm{diag}\{\mathbf{BUP}_\lambda\mathbf{P}_j\mathbf{1}_N\} - \mathbf{B}\cdot\mathrm{diag}\{\mathbf{UP}_\lambda^2\mathbf{P}_j^2\mathbf{1}_N\}\cdot\mathbf{B}^T + \delta_{\mathtt{MIX}}p_{j,\mathtt{MIX}}\mathbf{I}_\rho \tag{11}$$

where $\mathbf{P}_j \doteq \mathrm{diag}\{p_{j,1}, \cdots, p_{j,N}\}$.

Computation of $\frac{1}{\rho}\mathrm{E}\left\{(\mathbf{BU})^T\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}\mathbf{BU}\right\}$.

Using (11), we can obtain $\frac{1}{\rho}\mathrm{E}\left\{(\mathbf{BU})^T\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}\mathbf{BU}\right\}$ by performing matrix multiplications. We omit the full description of these steps for practicality issues and indicate that the result is:

$$\begin{aligned} &\tfrac{1}{\rho}\mathrm{E}\left\{(\mathbf{BU})^T\mathbf{\Sigma}_{\mathbf{Y}_j|\mathbf{U}}\mathbf{BU}\right\} \approx \\ &(\mathbf{F}_\lambda + \mathbf{F}_\delta)\left\{(\lambda_j' - \lambda_j'' + \delta_{\mathtt{MIX}}p_{j,\mathtt{MIX}})\mathbf{1}_{N\times N} + \alpha_q\left(\mathbf{1}_{N\times N}(\mathbf{P}_j\mathbf{P}_\lambda - \mathbf{P}_j^2\mathbf{P}_\lambda^2) + (\mathbf{P}_j\mathbf{P}_\lambda - \mathbf{P}_j^2\mathbf{P}_\lambda^2)\mathbf{1}_{N\times N}\right)\right\}(\mathbf{F}_\lambda + \mathbf{F}_\delta) \\ &+(\mathbf{F}_\lambda + \mathbf{F}_\delta)\left\{\alpha_q(\lambda_j' - \lambda_j'' + \delta_{\mathtt{MIX}}p_{j,\mathtt{MIX}})\mathbf{I}_N + \alpha_s\mathbf{P}_j\mathbf{P}_\lambda - \alpha_q^2\mathbf{P}_j^2\mathbf{P}_\lambda^2 - \left(\frac{\alpha_q}{\alpha_r} - 1\right)\alpha_q\lambda_j'\mathbf{I}_N\right\} \end{aligned} \tag{12}$$

where $\lambda_j' \doteq \sum_{i=1}^N \lambda_i p_{j,i}$, $\lambda_j'' \doteq \sum_{i=1}^N \lambda_i P_{\lambda_i} p_{j,i}^2$, $\alpha_r \doteq \dfrac{\alpha(2-\alpha)}{2-\alpha(2-\alpha)}$ and $\alpha_s \doteq \dfrac{\alpha^3}{1-(1-\alpha)^3}$.

Computation of a single element in the diagonal of $\mathbf{\Sigma}_{\mathbf{p}_j}$.

The next step is plugging (12) and (7) into (8) and performing laborious matrix multiplications. We omit writing the whole expression that is obtained after this process and point out that the i-th element in the diagonal of $\mathbf{\Sigma}_{\mathbf{p}_j}$, which is $\mathrm{Var}\left\{\hat{p}_{j,i}\right\}$ or, equivalently, $\mathtt{MSE}_{j,i}$, is:

$$\begin{aligned} \mathtt{MSE}_{j,i} \quad & \approx \frac{1}{\rho} \cdot \frac{1}{\lambda_i} \cdot \left(1 + \frac{\delta_i}{\lambda_i}\right) \cdot \left(1 - \frac{\lambda_i + \delta_i}{\sum_{k=1}^{N}(\lambda_k + \delta_k)}\right) \cdot \\ & \left(\frac{1}{\alpha_q}\left(\sum_{k=1}^{N} \lambda_k p_{j,k} + \delta_{\mathtt{MIX}} p_{j,\mathtt{MIX}}\right) - \frac{1}{\alpha_r}\sum_{k=1}^{N} \lambda_k P_{\lambda_k} p_{j,k}^2\right) \\ & + \frac{1}{\rho} \cdot \frac{1}{\lambda_i}\left(p_{j,i} - P_{\lambda_i} p_{j,i}^2\right) \end{aligned} \tag{13}$$

where we have assumed that $\lambda_i + \delta_i \ll \left(\sum_{k=1}^{N}(\lambda_k + \delta_k)\right)$. Finally, since we can assume $p_{j,i} \ll \sum_{k=1}^{N} \lambda_k p_{j,k}$, we get the expression

$$\begin{aligned} \mathtt{MSE}_{j,i} \approx \frac{1}{\rho} \cdot \frac{1}{\alpha_q} \cdot \quad & \frac{1}{\lambda_i} \cdot \left(1 + \frac{\delta_i}{\lambda_i}\right) \cdot \left(1 - \frac{\lambda_i + \delta_i}{\sum_{k=1}^{N}(\lambda_k + \delta_k)}\right) \cdot \\ & \left(\sum_{k=1}^{N} \lambda_k p_{j,k} + \delta_{\mathtt{MIX}} p_{j,\mathtt{MIX}} - \frac{\alpha_q}{\alpha_r}\sum_{k=1}^{N} \lambda_k P_{\lambda_k} p_{j,k}^2\right) \end{aligned} \tag{14}$$

References

[1] Oya, S., Troncoso, C., Pérez-González, F.: Do dummies pay off? limits of dummy traffic protection in anonymous communications. In: 14th Symposium on Privacy Enhancing Technologies. (2014)