Capacity calculations in "Increased reproducibility and comparability of data leak evaluations using ExOT"

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TIK Institut für Technische Informatik und Kommunikationsnetze

Capacity calculations in "Increased reproducibility and comparability of data leak evaluations using ExOT"

Authors: Philipp Miedl and Lothar Thiele[1]

This technical report is a supplement to Miedl et al. [4]. We describe the differences of the input-constrained water-filling capacity calculations used by Miedl et al. [4], in comparison with Bartolini et al. [1].

1 Symbols

Based on the notation introduced in Bartolini et al. [1] and Miedl et al. [4], following symbols are used in this technical report:

$\{\mathcal{E}_f\}$	...	Set of experiments to determine the channel spectra	(1)
$\{f\}$	...	Frequency range for the experiments $\{\mathcal{E}_f\}$	(2)
N_0	...	Constant noise power	(3)
p_0	...	Input power cap	(4)
S_{xx}^e	...	Input power spectrum of experiment e in $\{\mathcal{E}_f\}$	(5)
S_{xx}	...	Input power spectrum determined using $\{\mathcal{E}_f\}$	(6)
S_{qq}	...	Noise power spectrum of the channel	(7)
S_{hh}	...	Channel power spectrum of the channel	(8)
C	...	Channel capacity bound	(9)
λ	...	Water-filling parameter	(10)
$\overline{x}$	...	Mean of values in x	(11)

2 The constrained-input water-filling

Let A_λ be a set of frequencies as defined in Equation 12 below:

$$A_\lambda = \{f \quad | \quad \lambda \cdot S_{hh}(f) \geq 1 \quad \forall f \in (-\infty, \infty)\} \tag{12}$$

[1]Address: Computer Engineering and Networks Laboratory (TIK), ETZ G 76, Gloriastrasse 35, 8092 Zurich, Switerland, email: miedlp@ethz.ch, thiele@ethz.ch

Furthermore, we establish the constraint

$$\frac{1}{2}\int_{A_\lambda}\left(\lambda - \frac{1}{S_{hh}(f)}\right)df \leq \frac{p_0}{N_0} \tag{13}$$

The constraint in Equation 13 ensures that the signal-to-noise-ratio does not exceed the ratio of the power cap p_0 over the noise power N_0.

We define the channel capacity C as a function of the water-filing parameter λ and the channel power spectrum S_{hh} in Equation 14 below:

$$C = \max_{\lambda}\left\{\frac{1}{2}\int_{A_\lambda}\log_2\left(\lambda \cdot S_{hh}(f)\right)df\right\}\ [\text{bps}] \tag{14}$$

To determine the channel capacity C, we need to find the λ that maximises Equation 14 subject to the constraint in Equation 13. This is called *water-filling* procedure [2, 5]. It is important to note that the constrained-input water-filling procedure assumes that the noise is white. This means that the noise power spectrum is constant, as defined in Equation 15 below:

$$S_{qq}(f) = N_0 \quad \forall f \in A_\lambda \tag{15}$$

3 New derivation of the power cap p_0

Bartolini et al. [1] defines the power cap p_0 of input signal as

$$p_0 = \overline{S_{xx}} \tag{16}$$

In contrast to that, Miedl et al. [4] defines the power cap p_0 as

$$p_0 = \max_{e\in\{\mathcal{E}_f\}}\left(\int_f (S^e_{xx})\right) \tag{17}$$

While the definition in Equation 16 derives the input power cap from an approximated input power spectrum, Equation 17 uses measurement results. Therefore, we consider the new definition used by Miedl et al. [4] to be more accurate.

4 Compensating for coloured noise using a whitening filter

The input-constrained water-filling can only be applied on systems with white noise [3] (see Equation 15). So to apply the input-constrained water-filling, Bartolini et al. [1] use spectrum splitting. In contrast to this, Miedl et al. [4] use a whitening filter. We show how to apply such a whitening filter below.

Let $N_0 = \overline{S_{qq}}$, then we define the spectrum of the whitening filter S_{WF} as

$$S_{WF} = \frac{S_{qq}}{N_0} \tag{18}$$

We now apply this whitening filter S_{WF} to our channel to get the whitened channel spectrum $\hat{S}_{hh}$ and the whitened noise spectrum $\hat{S}_{qq}$.

$$\hat{S}_{hh} = \frac{S_{hh}}{S_{WF}} \tag{19}$$

$$\hat{S}_{qq} = \frac{S_{qq}}{S_{WF}} \tag{20}$$

Last, we can determine the white noise level $\hat{N}_0$.

$$\hat{N}_0 = \overline{\hat{S}_{qq}} \tag{21}$$

Now we adopt the Equations 13 and 14 for our whitened channel:

$$\frac{1}{2}\int_{A_\lambda}\left(\lambda - \frac{1}{\hat{S}_{hh}(f)}\right)df \leq \frac{p_0}{\hat{N}_0} \tag{22}$$

$$C = \max_{\lambda}\left\{\frac{1}{2}\int_{A_\lambda}\log_2\left(\lambda\cdot\hat{S}_{hh}(f)\right)df\right\}\ [\text{bps}] \tag{23}$$

References

[1] D. B. Bartolini, P. Miedl, and L. Thiele. On the Capacity of Thermal Covert Channels in Multicores. In *Proceedings of the Eleventh European Conference on Computer Systems*, EuroSys '16, pages 24:1–24:16, New York, NY, USA, 2016. ACM. ISBN 978-1-4503-4240-7. doi: $10.1145/2901318.2901322$. URL `http://doi.acm.org/10.1145/2901318.2901322`.

[2] T. M. Cover and J. A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006. ISBN 0471241954.

[3] C. Heegard and L. Ozarow. Bounding the capacity of saturation recording: the Lorentz model and applications. *Selected Areas in Communications, IEEE Journal on*, 10(1):145–156, Jan 1992. ISSN 0733-8716.

[4] P. Miedl, B. Klopott, and L. Thiele. Increased reproducibility and comparability of data leak evaluations using ExOT. In *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2020.

[5] P. P. Vaidyanathan, S.-M. Phoong, and Y.-P. Lin. *Signal Processing and Optimization for Transceiver Systems*. Cambridge University Press, 2010. ISBN 9781139042741. URL `http://dx.doi.org/10.1017/CBO9781139042741`. Cambridge Books Online.