

On the Secrecy Capacity of the Z-Interference Channel

Ronit Bustin, Mojtaba Vaezi, Rafael F. Schaefer and H. Vincent Poor

International Zurich Seminar on Communications

March 2-4, 2016

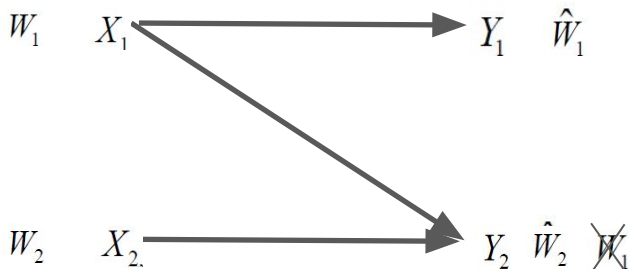
Outline

- 1 Introduction and Motivation
- 2 First Model: Allowing Stochastic Encoders
- 3 Second Model: Deterministic Encoder for the Interfered-With Transmitter
- 4 Conclusions and Future Work

Motivation

- 1 The interference channel is a central open problem in multi-user information theory. Understanding the effect of interference is critical to the understanding of the limitations of communication and essentially the interactions in any network.
- 2 An additional requirement - complete secrecy of the interfering message at the interfered-with receiver. This additional requirement is relevant to many practical settings, in which our transmission can both be received by other, unintended receivers, but still we would like it to remain secure.

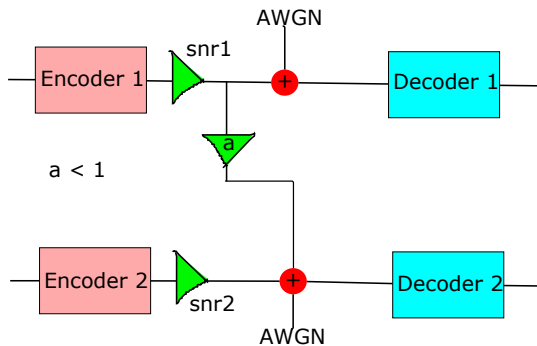
Z-Interference with a Complete Secrecy Constraint



Channel: $P_{\mathbf{Y}_1, \mathbf{Y}_2 | \mathbf{X}_1, \mathbf{X}_2} = P_{\mathbf{Y}_1 | \mathbf{X}_1} P_{\mathbf{Y}_2 | \mathbf{X}_1, \mathbf{X}_2}$.

Complete Secrecy: $\lim_{n \rightarrow \infty} \frac{1}{n} I(W_1; \mathbf{Y}_2) \rightarrow 0$

The Gaussian Z-Interference with a Complete Secrecy Constraint



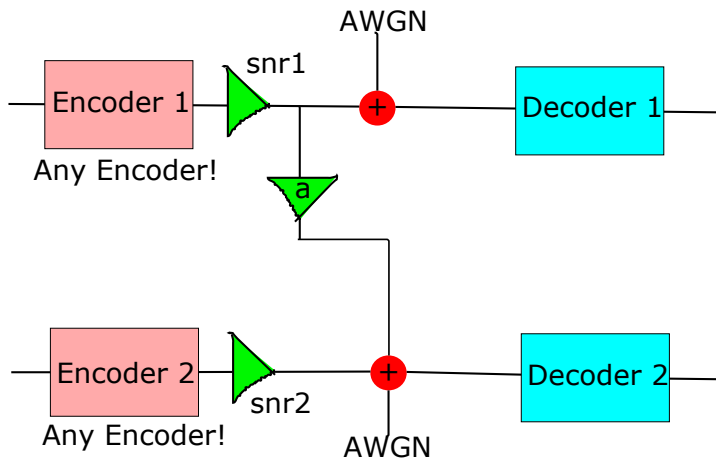
$$Y_1 = \sqrt{\text{snr}_1} X_1 + N_1$$

$$Y_2 = \sqrt{\text{snr}_2} X_2 + \sqrt{a \text{snr}_1} X_1 + N_2$$

Two Sub-Models Considered

- 1 The General Model: We place no additional constraints and allow both encoders to be stochastic.
- 2 A Deterministic Encoder for the Interfered-With Transmitter: Note that this transmitter has no secrecy constraint on its own transmitted message.

Allowing Stochastic Encoders



What is the Bounding Box of the Capacity Region?

What is the maximum rate for either W_1 or W_2 ?

- For W_2 : setting $R_1 = 0$ we trivially comply with the secrecy constraint. Since there is no interference:

$$R_2 = \frac{1}{2} \log(1 + \text{snr}_2)$$

which is the maximum possible rate.

- For W_1 : $\mathbf{X}_1 - \mathbf{Y}_1 - \mathbf{Y}_2$ is a Markov chain (for $a \in [0, 1)$) regardless of the distribution of \mathbf{X}_2 . Using Wyner's result for *degraded* wiretap channels we have a single-letter expression

$$R_{1,\max} = \max_{P_{X_1} P_{X_2}} \{I(X_1; Y_1) - I(X_1; Y_2)\}$$

where the maximization is over both distributions, as Y_2 depends on X_2 as well.

Maximum R_1

Theorem

For any $\text{snr}_1 > 0$, $\text{snr}_2 > 0$ and any $a \in [0, 1)$, $R_{1,\max}$ is obtained by non-Gaussian distributions, meaning

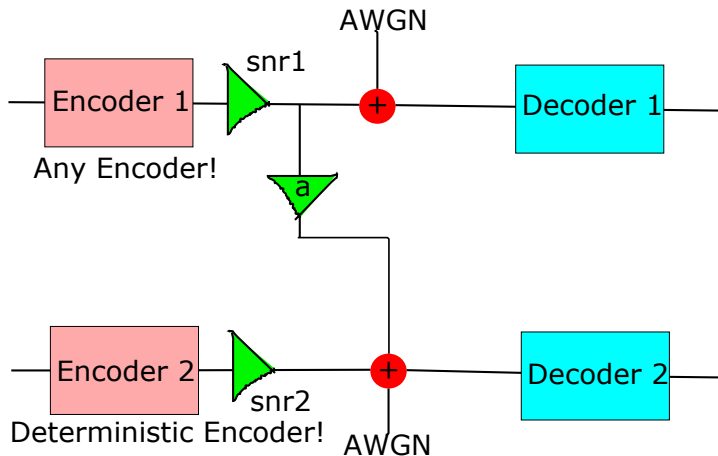
$$R_{1,\max} > \frac{1}{2} \log(1 + \text{snr}_1) - \frac{1}{2} \log \left(1 + \frac{a \text{snr}_1}{1 + \text{snr}_2} \right).$$

Proof method:

We apply the perturbation approach of Abbe and Zheng, using Hermite polynomials:

E. A. Abbe and L. Zheng, "Coding along Hermite polynomials for interference channels," in *Proc. IEEE Information Theory Workshop, (ITW 2009)*, pp. 584–588, Taormina, Sicillia, Italy, 11-16 October 2009

A Deterministic Encoder for the Interfered-With Transmitted



Capacity Region Reduces

Theorem

By restricting the encoder of the interfered-with user to a deterministic encoder we strictly reduce the capacity region.

Method of Proof:

We show that the point

$$(R_1, R_2) = \left(\frac{1}{2} \log(1 + \text{snr}_1) - \frac{1}{2} \log \left(1 + \frac{a \text{snr}_1}{1 + \text{snr}_2} \right), 0 \right)$$

which we have shown to be included in the capacity region of the general case, is not included in the capacity region given the deterministic encoder constraint.

Sato-Type Outer Bound - Equivalence

Lemma

The Gaussian Z-Interference channel with secrecy constraint and a deterministic encoder for the message W_2 , meaning $H(\mathbf{X}_2|W_2) = 0$, is equivalent, in the sense that they have the same capacity region, to the degraded Gaussian interference channel:

$$\mathbf{Y}'_1 = \sqrt{\text{snr}_1} \mathbf{X}_1 + \sqrt{\frac{\text{snr}_2}{a}} \mathbf{X}_2 + \mathbf{N}_1$$

$$\mathbf{Y}'_2 = \sqrt{\text{snr}_1} \mathbf{X}_1 + \sqrt{\frac{\text{snr}_2}{a}} \mathbf{X}_2 + \mathbf{N}_1 + \mathbf{N}'_2$$

where \mathbf{N}_1 is as defined above, standard additive Gaussian noise, whereas \mathbf{N}'_2 is additive Gaussian noise of variance $\frac{1-a}{a}$.

Method of Proof: Follows the proof of Costa IT'85:

M. H. M. Costa, "On the Gaussian interference channel," *IEEE Transactions on Information Theory*, vol. 31, no. 5, pp. 607–615, September 1985.

Sato-Type Outer Bound - Using BCC

- Using the approach of Sato IT'77 the capacity region of the Gaussian *degraded* interference channel with a secrecy constraint can be outer bounded by the capacity region of the Gaussian broadcast channel with confidential messages.
- Due to the above equivalence this provides an outer bound to our setting as well.

Theorem

The capacity region of the Gaussian Z-interference channel with a secrecy constraint on the interfering message and a deterministic encoder at the interfered-with transmitter is contained in the following region:

$$(R_1, R_2) = \left(\frac{1}{2} \log \left(\frac{1 + \beta(\text{snr}_1 + \text{snr}_2/a)}{1 + \beta a(\text{snr}_1 + \text{snr}_2/a)} \right), \frac{1}{2} \log \left(\frac{1 + a(\text{snr}_1 + \text{snr}_2/a)}{1 + \beta a(\text{snr}_1 + \text{snr}_2/a)} \right) \right)$$

$$R_1 \leq \frac{1}{2} \log(1 + \text{snr}_1) - \frac{1}{2} \log(1 + a\text{snr}_1)$$

$$R_2 \leq \frac{1}{2} \log(1 + \text{snr}_2)$$

for some $\beta \in [0, 1]$.

Some Inner Bounds

We depict three basic bounds. The first is a simple time-sharing. The second is a time/frequency division multiplexing scheme:

Lemma (TDM/FDM)

The set of non-negative rate pairs (R_1, R_2) satisfying

$$R_1 \leq \frac{\lambda}{2} \log\left(1 + \frac{\text{snr}_1}{\lambda}\right) - \frac{\lambda}{2} \log\left(1 + \frac{a\text{snr}_1}{\lambda}\right),$$
$$R_2 \leq \frac{\bar{\lambda}}{2} \log\left(1 + \frac{\text{snr}_2}{\bar{\lambda}}\right),$$

in which $0 \leq \lambda \leq 1$ and $\bar{\lambda} = 1 - \lambda$, is achievable for the Gaussian Z-Interference channel with secrecy constraint and a deterministic encoder.

Some Inner Bounds

We can improve the above TDM/FDM bound by allowing the interfered-with transmitter to split its power over both subbands.

Lemma

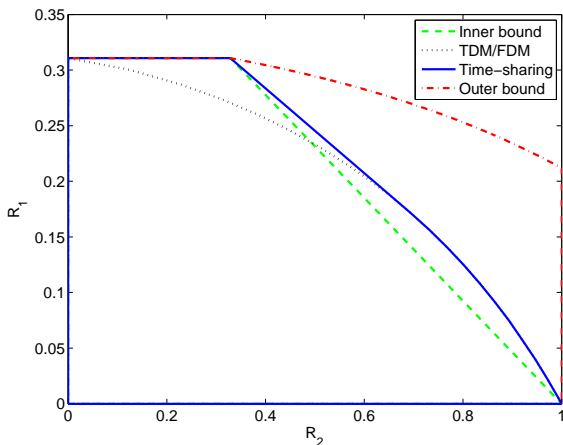
The set of non-negative rate pairs (R_1, R_2) satisfying

$$R_1 \leq \frac{\lambda}{2} \log \left(1 + \frac{\text{snr}_1}{\lambda} \right) - \frac{\lambda}{2} \log \left(1 + \frac{a \text{snr}_1}{\lambda} \right),$$

$$R_2 \leq \frac{\lambda}{2} \log \left(1 + \frac{\text{snr}_{21}}{1 + a \frac{\text{snr}_1}{\lambda}} \right) + \frac{\bar{\lambda}}{2} \log \left(1 + \text{snr}_{22} \right),$$

in which $0 \leq \lambda \leq 1$, $\bar{\lambda} = 1 - \lambda$, and $\lambda \text{snr}_{21} + \bar{\lambda} \text{snr}_{22} = \text{snr}_2$ is achievable for the Gaussian Z-Interference channel with secrecy constraint and a deterministic encoder.

Inner and Outer Bounds



The Sato-type outer bound (red dash-dot line), the basic time-sharing inner bound (green dashed), the TDM/FDM inner bound (black dotted) and the improved TDM/FDM inner bound (blue solid).

Corner Points

We can identify one corner point where the inner and outer bound coincide:

$$(R_1, R_2) = \left(\frac{1}{2} \log(1 + \text{snr}_1) - \frac{1}{2} \log(1 + a \text{snr}_1), \frac{1}{2} \log \left(1 + \frac{\text{snr}_2}{1 + a \text{snr}_1} \right) \right)$$

We also have that:

$$(R_1, R_2) = \left(0, \frac{1}{2} \log(1 + \text{snr}_2) \right)$$

is a corner point, **given a variance constraint on the inputs**. This is due to the result in [Bustin-Poor-Shamai,'15] which shows that the minimum mean-square error of the interference must be zero to allow reliable communication at the maximum rate. Thus, no level of secrecy can be obtained!

Conclusions and Future Work

- Enhancing the achievability schemes to obtain tighter inner bounds.
- Investigating the gap, specifically at the high-SNR regime.
- The Discrete Memoryless Channel model: Can the additional secrecy constraint provide additional insights into the interference channel?



Thank You!

Ronit Bustin^{*}, Mojtaba Vaezi[†], Rafael F. Schaefer[‡] and H. Vincent Poor[†]

^{*}Dept. EE, TAU, [†]Dept. EE, Princeton University, [‡]Information Theory and Applications Group, Technische Universität Berlin

“On the Secrecy Capacity of the Z-Interference Channel”

The two-user Z-interference channel with an additional secrecy constraint is considered. The two transmitter-receiver pairs wish to reliably transmit their messages; however the transmission of the first pair both interferes with the transmission of the second pair and is also required to be completely secure from the second receiver. The focus here is on the capacity region of the above Z-interference channel in the Gaussian case under the standard power constraints. The maximum rates of the two users in this setting are described, and although the maximum rate of the transmission of the first pair has a single-letter expression, due to Wyner's secrecy capacity expression, its maximization is non-trivial. The significance of a stochastic encoder for the second transmitter, encoding a message which is not required to comply with any secrecy constraints, is noted. It is shown explicitly that constraining this encoder to be deterministic reduces the capacity region. Finally, a Sato-type outer bound on the capacity region is obtained under this additional deterministic encoder constraint.

-  E. A. Abbe and L. Zheng, “Coding along Hermite polynomials for interference channels,” in *Proc. IEEE Information Theory Workshop, (ITW 2009)*, pp. 584–588, Taormina, Sicillia, Italy, 11-16 October 2009.
-  M. H. M. Costa, “On the Gaussian interference channel,” *IEEE Transactions on Information Theory*, vol. 31, no. 5, pp. 607–615, September 1985.