A BIT OF SECRECY FOR GAUSSIAN SOURCE COMPRESSION

Eva C. Song, Paul Cuff, H. Vincent Poor
{CSONG, CUFF, POOR}@PRINCETON.EDU

PROBLEM

The compression of an i.i.d. Gaussian source sequence is studied in an unsecured network. Within a game theoretic setting for a three-party noiseless communication network (sender Alice, legitimate receiver Bob, and eavesdropper Eve), the problem of how to efficiently compress a Gaussian source with limited secret key in order to guarantee that Bob can reconstruct with high fidelity while preventing Eve from estimating an accurate reconstruction is investigated.

THREE CASES

1. Weak eavesdropper $s^E = \{z^{-1}\}$
2. Causal Source Awareness $s^E = \{x^{-1}, z^{-1}\}$
3. Causal General Awareness $s^E = \{x^{-1}, y^{-1}, z^{-1}\}$

In all three cases, the SI of Bob is given by $k$ and $c_i = \{x^{-1}, y^{-1}, z^{-1}\}$. It is sufficient to consider only $s^E = \{k\}$ which is independent of Bob’s awareness of the eavesdropper.

PROBLEM SETUP

- $K \sim Unif[1 : 2^{R_s}]$
- Encoder $f_s : A^n \times K \mapsto M$
- Bob’s decoder \( \{g : M \times S^E \mapsto Y\} \)
- Eve’s decoder \( \{t : M \times S^E \mapsto Z\} \)
- Payoff $\pi(x, y, z) \triangleq \frac{1}{n} \sum_{i=1}^{n} \pi(x_i, y_i, z_i)$
- Payoff achievable:

$Y = nU$ and $U \triangleq n \mod N$, we greedily obtain an achievable lower bound by sequentially solving for the optimal $T$ that satisfies $R \geq I(X; U; Y)$ and the optimal $N$ that satisfies $R_s \geq I(X; Y | U)$.

Scalar quantization upper bound:

The quantization upper bound is numerically obtained by solving a linear programming problem

\[
\Pi_{\text{quant}}(R, R_s) = \max_{p(y, z | x)} \min_{U, Y} \mathbb{E}[X | \text{Quantization bin of } X_i]
\]

NUMERICAL COMPUTATION

We numerically compare the payoffs under different schemes for the scenario of causal source awareness.

RESULTS

Theorem 1 The secrecy rate-payoff triple $(R, R_s, \Pi)$ for a weak eavesdropper is achievable for an i.i.d. Gaussian source if and only if

\[
R_s > 0, \text{ and } \Pi \leq 1 - \exp(-2R).
\]

With causal source awareness, the general optimal payoff function

\[
\Pi_{\text{causal}}(R, R_s) = \max_{p(y, z | x)} \min_{U, Y} \mathbb{E}[X | \text{Quantization bin of } X_i]
\]

SCONCLUSION

For an eavesdropper that has causal information of Alice (and Bob), at most 1 bit of secret key is needed for each Gaussian source symbol to force maximum distortion to Eve while keeping the rate-distortion tradeoff at the same level as in point-to-point communication. Counter-intuitively, choosing the auxiliary random variable to be jointly Gaussian is not optimal.

REFERENCES


ACKNOWLEDGEMENT

This work was supported by NSF Grants CCF-1116013 and CNS-09-05086, and AFOSR Grant FA9550-12-1-0196