Covert Communication and Square-Root Law

Suppose
- Both Receiver and Eavesdropper observe the same AWGN channel (with same noise power).
- Covertness requirement is
\[ D(P||Q) \leq \delta \]
where \( P \) is average output distribution when Transmitter sends a codeword, and \( Q \) is output distribution when Transmitter sends noise (pure Gaussian noise).

Then [1, 2]) maximum number of nats over n channel uses \( \sqrt{n} \rightarrow \delta \) in particular, covert communication capacity (nats per channel use) is zero.

Infinite Bandwidth: Simple Heuristics

Over \( W \) Hz and \( T \) seconds with white Gaussian noise, one has 2WT independent samples.
- Total number of nats \( \propto \sqrt{WT} \)
- Positive per-second rate possible if \( W \geq 1 \).

Formal Treatment in Continuous Time

Model 1: Input \( X(t) \) and output (at both Receiver and Eavesdropper) \( Y(t) \) are related by
\[ Y(t) = X(t) + Z(t), \quad t \in \mathbb{R}, \]
where \( Z(t) \) is a stationary Gaussian process to be further specified later.
- Transmitter is "approximately time-limited": it maps a message to \( x(t), t \in \mathbb{R}, \) such that
\[ \lim_{T \to \infty} \int_{-T}^{T} |x(t)|^2 dt = 1. \]
- Decoder is strictly time-limited: it maps \( y(t), t \in [0, T], \) to decoded message.
- Eavesdropper is not time-limited: covertness constraint is
\[ \lim_{T \to \infty} D(P_{Y|X}||Q_{Y|X}) = 0, \]
where \( P_{Y|X} \) and \( Q_{Y|X} \) are respective distributions of \( Y(T) \) and \( Z(T), t \in (-\infty, \infty). \)

Proposition 1. Assume, for every \( T \), the noise process \( Z(t) \) has PSD \( N_0/2 \) over \([-W, W], \)
where \( W = \mathcal{T}^2 \). Under the above conditions and power constraint
\[ E \left[ \int_{-T}^{T} |X(t)|^2 dt \right] \leq PT, \]
the covert communication capacity of the channel is \( P/\sqrt{N_0} \) nats per second.

Prolate Spheroidal Wave Functions (PSWFs) [5, 6, 7]

There exist \( 1 > \lambda_1 > \lambda_2 > \ldots > 0 \) (countably infinite) functions \( \phi_k \) such that
1. Each \( \phi_k \) is band-limited to \( W \) Hz. Further, the functions \( \phi_k \) are orthonormal on \( \mathbb{R} \), and complete in the space of functions that are band-limited to \( W \) Hz.
2. The restrictions of \( \phi_k \) to the interval \( [0, T] \) are orthogonal:
\[ \int_{\lambda_j \mathbb{R}} \phi_k(\lambda_j \omega) d\omega = \lambda_j \delta_{kj}, \quad i \neq j. \]
3. Restrictions of \( \phi_k \) to \([0, T]\) are complete in the space of square integrable functions on \([0, T]\).
4. For any \( \epsilon > 0, W \to \infty, \)
\[ \lambda_1 \mathbb{R} \to 1, \quad \lambda_2 \mathbb{R} \to 0, \]

4. Let \( Z(t) \) be stationary Gaussian noise with PSD
\[ N(f) = \begin{cases} N_0 & |f| \leq W, \\ 0 & |f| > W. \end{cases} \]
restricted to the interval \([0, T]\), then \( Z(t) \) can be written in the Karhunen–Loève expansion
\[ Z(t) = \sum_{i} \psi_i(t), \quad t \in [0, T], \]
where \( \psi_i \) are IID Gaussian random variables of mean zero and variance \( N_0/2. \)

Proof of Proposition 1. Fix \( \epsilon < (0, 1). \) Our coding scheme is to generate \( 2(1-\epsilon)T^2 \) IID Gaussian random variables \( X_i \), each of mean zero and variance \( PT^{-1/2} \), and transmit the signal
\[ X(t) = \sum_{i=1}^{(1-\epsilon)T^2} X_i \nu_i(t), \quad t \in \mathbb{R}, \]
where \( \nu_i \) are PSWFs for the frequency band \([-T^2, T^2] \) and time interval \([0, T] \). The proof then follows classic work [5, 6] correctness, data rates, and other results all follow from the nice properties of the PSWFs.

Band-Limited Noise: Good and Bad Models

Model 2: make the following changes from Model 1.
- Transmitter is strictly time-limited: \( X(t) = 0 \) w.p. 1 for all \( t \notin [0, T] \).
- Eavesdropper is also time-limited: covertness constraint is
\[ \lim_{T \to \infty} D(P_{Y|X}||Q_{Y|X}) = 0. \]

Proposition 2: Let \( X(t) \) have PSD that equals \( N_0/2 \) on \([-W, W] \) and zero elsewhere, where \( W \) is a constant that does not grow with \( T \). Under Model 1, the covert communication capacity of the channel is zero. Under Model 2, the covert communication capacity is infinity.

Proof Sketch for Model 2: Fix interval \([0, T] \). For any positive integer \( k \), generate a sequence of \( k^2 \) IID Gaussian random variables \( X_i \) of mean zero and variance \( k^{-2} \).

Colored Noise

Infinite-bandwidth white noise does not exist, as it would have infinite power. Consider colored Gaussian noise \( Z(t) \) with PSD \( N(f) > 0 \) for all \( f \in \mathbb{R} \). Symmetric around \( f = 0 \), satisfying
\[ \int_{-\infty}^{\infty} N(f) df < \infty. \]
Let us choose the input signal \( X(t) \) to be generated from a stationary Gaussian process with PSD
\[ S(f) = \begin{cases} T^{-1/2} N(f) & f \in [-W, W], \\ 0 & \text{otherwise}, \end{cases} \]
where again \( W \rightarrow T^2 \). We then have [7]
\[ D(P_{Y|X}/P_{Z|X}) = T \int_{-W}^{W} \log \left( 1 + \frac{S(f)}{N(f)} \right) \frac{1}{T^{-1/2}} df = \frac{T}{2}, \]
which tends to zero as \( T \to \infty \); while
\[ T^{-1/2} \rho(X, Y) = \int_{-W}^{W} \log \left( 1 + \frac{S(f)}{N(f)} \right) df = \frac{T^{1/2}}{2}, \]
which tends to infinity as \( T \to \infty \). Note also \( D(P_{Y|X}/P_{Z|X}) \to 0 \) as \( T \to \infty \).

The following conjecture remains to be formulated and proven in a true continuous-time setting.

Conjecture 3. If \( Z(f) \) is Gaussian noise as above, then the covert communication capacity of the channel without bandwidth constraint on the input is infinity. Furthermore, this should hold irrespective of whether an average-power constraint is imposed on the input or not.

References