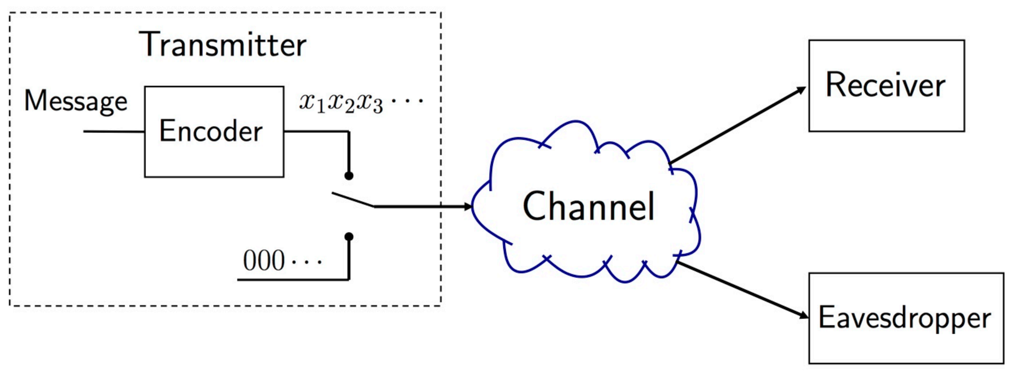
On Covert Communication Over Infinite-Bandwidth Gaussian Channels

Ligong Wang
ETIS—Université Paris Seine, Université de Cergy-Pontoise, ENSEA, CNRS
Cergy-Pontoise, France

Covert Communication and Square-Root Law



Suppose

- Both Receiver and Eavesdropper observe same AWGN channel (with same noise power);
- Covertness requirement is
$$D(P^n \| Q^n) \le \delta$$
where P^n is average output distribution when Transmitter sends a codeword;
Q^n is output distribution when Transmitter sends n zeros (pure Gaussian noise).

Then [1], [2]
$$\text{maximum number of nats over } n \text{ channel uses} = \sqrt{n\delta} + o(\sqrt{n}).$$
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.

$\Longrightarrow$ Total number of nats $\propto \sqrt{WT}$.

$\Longrightarrow$ Positive per-second rate possible if $W \gtrsim T$.

Formal Treatment in Continuous Time

Model 1: Input $X(\cdot)$ and output (at both Receiver and Eavesdropper) $Y(\cdot)$ are related by
$$Y(t) = X(t) + Z(t), \quad t \in \mathbb{R},$$
where $Z(\cdot)$ 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
$$\lim_{T\to\infty} \frac{\int_0^T |x(t)|^2 \,\mathrm{d}t}{\int_{-\infty}^{\infty} |x(t)|^2 \,\mathrm{d}t} = 1.$$
- Decoder is strictly time-limited: it maps $y(t)$, $t \in [0,T]$, to decoded message.
- Eavesdropper is not time-limited: covertness constraint is
$$\lim_{T\to\infty} D\big(P_{-\infty}^{\infty} \big\| Q_{-\infty}^{\infty}\big) = 0,$$
where $P_{-\infty}^{\infty}$ and $Q_{-\infty}^{\infty}$ are resp. distributions of $Y(t)$ and $Z(t)$, $t \in (-\infty, \infty)$.

> **Proposition 1.** *Assume, for every T, the noise process $Z(\cdot)$ has PSD $N_0/2$ over $[-W_T, W_T]$, where $W_T = T^2$. Under the above conditions and power constraint*
> $$\mathsf{E}\left[\int_{-\infty}^{\infty} |X(t)|^2 \,\mathrm{d}t\right] \le PT,$$
> *the covert communication capacity of the channel is P/N_0 nats per second.*

Prolate Spheroidal Wave Functions (PSWFs) [3], [4]:

There exist $1 > \lambda_1 > \lambda_2 > \cdots > 0$ (countably infinite) and functions $\{\boldsymbol{\psi}_i\}$ such that

1. Each $\boldsymbol{\psi}_i$ is band-limited to W Hz. Further, the functions $\{\boldsymbol{\psi}_i\}$ are orthonormal on $\mathbb{R}$, and complete in the space of functions that are band-limited to W Hz.
2. The restrictions of $\{\boldsymbol{\psi}_i\}$ to the interval $[0,T]$ are orthogonal:
$$\int_0^T \psi_i(t)\psi_j(t)\,\mathrm{d}t = \begin{cases} \lambda_i, & i = j, \\ 0, & i \ne j. \end{cases}$$
Restrictions of $\{\psi_i\}$ to $[0,T]$ are complete in the space of square integrable functions on $[0,T]$.
3. For any $\epsilon \in (0,1)$, as $WT \to \infty$,
$$\lambda_{2(1-\epsilon)WT} \to 1$$
$$\lambda_{2(1+\epsilon)WT} \to 0.$$
4. Let $Z(\cdot)$ be stationary Gaussian noise with PSD
$$N(f) = \begin{cases} \frac{N_0}{2}, & |f| \le W, \\ 0, & |f| > W \end{cases}$$
restricted to the interval $[0,T]$, then $\mathbf{Z}$ can be written in the Karhunen-Loève expansion
$$Z(t) = \sum_{i=1}^{\infty} Z_i \psi_i(t), \quad t \in [0,T],$$
where $\{Z_i\}$ are IID Gaussian random variables of mean zero and variance $N_0/2$.

Proof Sketch of Proposition 1: Fix $\epsilon \in (0,1)$. Our coding scheme is to generate $2(1-\epsilon)T^3$ IID Gaussian random variables $\{X_i\}$ each of mean zero and variance $PT^{-2}/2$, and transmit the signal
$$X(t) = \sum_{i=1}^{(1-\epsilon)T^3} X_i \psi_i(t), \quad t \in \mathbb{R},$$
where $\{\psi_i\}$ are PSWFs for the frequency band $[-T^2, T^2]$ and time interval $[0,T]$. The proof then follows classic works [5], [6]; covertness, 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
$$\lim_{T\to\infty} D\Big(P_0^T \Big\| Q_0^T\Big) = 0.$$

> **Proposition 2.** *Let $Z(\cdot)$ 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^3 IID Gaussian random variables $\{X_i\}$ of mean zero and variance k^{-2}. Let
$$X(t) = \begin{cases} \sum_i X_i \psi_i(t), & t \in [0,T], \\ 0, & \text{otherwise.} \end{cases}$$
By the orthogonality of the PSWFs on $[0,T]$, the channel can be reduced, for both Eavesdropper and Receiver, to a set of k^3 parallel, independent Gaussian channels $Y_i = X_i + Z_i$. The claim then follows from the discrete-time AWGN results, and the fact that k can be arbitrarily large. □

Lesson: Model 2 is bad. When channel has memory (e.g., noise with limited bandwidth), covertness constraint must not be restricted to communication duration.

Colored Noise

Infinite-bandwidth white noise does not exist, as it would have infinite power. Consider colored Gaussian noise $Z(\cdot)$ with PSD $N(f) > 0$ for all $f \in \mathbb{R}$, symmetric around $f = 0$, satisfying
$$\int_{-\infty}^{\infty} N(f)\,\mathrm{d}f < \infty.$$
Let us choose the input signal $X(\cdot)$ to be generated from a stationary Gaussian process with PSD
$$S(f) = \begin{cases} T^{-7/4} \cdot N(f), & f \in [-W_T, W_T] \\ 0, & \text{otherwise,} \end{cases}$$
where again $W_T = T^2$. We then have [7]
$$D(P_{\mathbf{Y}} \| P_{\mathbf{Z}}) = T \cdot \frac{1}{2} \int_{-W_T}^{W_T} \left(\frac{S(f)}{N(f)} - \log\left(1 + \frac{S(f)}{N(f)}\right)\right) \mathrm{d}f \le \frac{T^{-1/2}}{2},$$
which tends to zero as $T \to \infty$; while
$$\frac{1}{T} \cdot I(\mathbf{X};\mathbf{Y}) = \int_{-W_T}^{W_T} \frac{1}{2} \log\left(1 + \frac{S(f)}{N(f)}\right) \mathrm{d}f \approx \frac{T^{1/4}}{2}$$
which tends to infinity as $T \to \infty$. Note also $\int_{-W_T}^{W_T} S(f)\,\mathrm{d}f \to 0$ as $T \to \infty$.

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

> **Conjecture 3.** *If $Z(\cdot)$ 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

[1] B. A. Bash, D. Goekel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Select. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sept. 2013.

[2] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inform. Theory*, vol. 62, no. 6, pp. 3493–3503, June 2016.

[3] D. Slepian, H. Landau, and H. Pollak, "Prolate spheroidal wave functions, Fourier analysis and uncertainty – I & II," *Bell System Techn. J.*, vol. 40, pp. 43–84, 1961.

[4] D. Slepian, "Some asymptotic expansions of prolate spheroidal wave functions," *J. Math. and Phys.*, vol. 44, pp. 99–140, 1965.

[5] A. D. Wyner, "Capacity of the band-limited Gaussian channel," *Bell System Techn. J.*, vol. 45, pp. 359–395, 1966.

[6] R. G. Gallager, *Information Theory and Reliable Communication*. John Wiley & Sons, 1968.

[7] M. S. Pinsker, *Information and Information Stability of Random Variables and Processes*. San Francisco: Holden-Day, 1964.