Information-Theoretic Security

Iñaki Esnaola
Department of Automatic Control and Systems Engineering
University of Sheffield

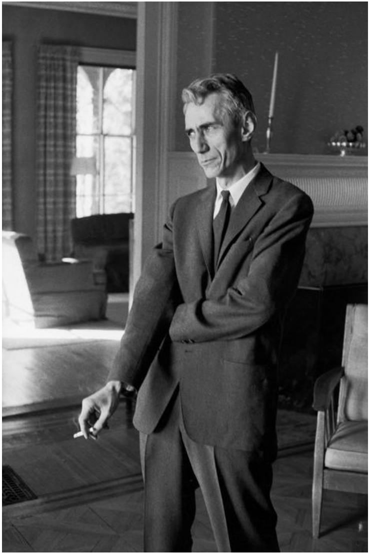
The Data Hide Meetings
Sheffield

November 17, 2015

What is information?

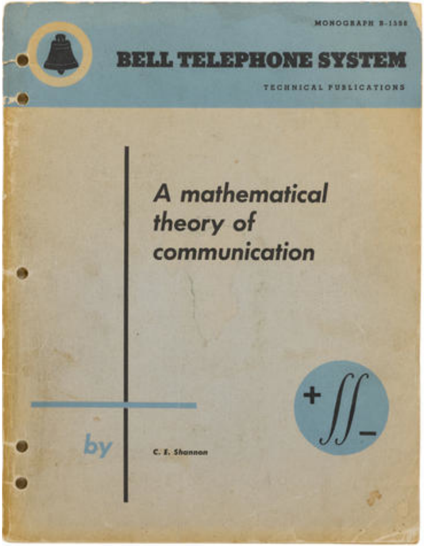
Claude E. Shannon

Henri Cartier-Bresson / Magnum Photos, 1962



A Mathematical Theory of Communication

C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379-423, Jul. 1948.



Information Source

- Alphabet: $\mathcal{X}$
- Probability distribution: P_X

Entropy

Rate at which information is produced

$$H(X) = -\sum_{x \in \mathcal{X}} P_X(x) \log_2 P_X(x)$$

Mutual Information

Information Shared by Two Random Variables

$$I(X;Y) = \sum_{x,y \in \mathcal{X} \times \mathcal{Y}} P_{XY}(x,y) \log_2 \frac{P_{XY}(x,y)}{P_X(x) P_Y(y)}$$

Motivation for Information Theoretic Security

- Cryptographic approach
  - Complexity: Limited computational power
  - Inversion of mathematical functions: Mathematical progress

Motivation for Information Theoretic Security

I am a new slide, really!

- Cryptographic approach
  - Complexity: Limited computational power
  - Inversion of mathematical functions: Mathematical progress
- Alternative approach: Information-theoretic secrecy
  - Security guarantees independent of adversary's computing power
  - Exploit intrinsic uncertainty in channel/source

Information Leakage in Written English

_ _ _ _ _ _ _ _ _ _   _ _   _ _ _ _ _ _ _ _ _   _ _ _ _ _

Information Leakage in Written English

U _ I _ _ _ _ _ _ _ Y O _ S H _ F _ _ _ _ D _ _ C K S

Information Leakage in Written English

U N I V E R S I T Y   O F   S H E F F I E L D   R O C K S

Shannon's Perfect Secrecy

One Time Pad:

- Key $\mathbf{k}$ is shared by transmitter and legitimate receiver
- Encoding: $\mathbf{y} = \mathbf{x} \oplus \mathbf{k}$

Perfect Secrecy?

Best Strategy for Eavesdropper

Guessing under complete uncertainty

$$H(\mathbf{k}) \geq H(\mathbf{x}) \iff I(\mathbf{x};\mathbf{y}) = 0$$

Shortcoming of One Time Pad

- Key must be exchanged prior to communication
- Key can only be used once

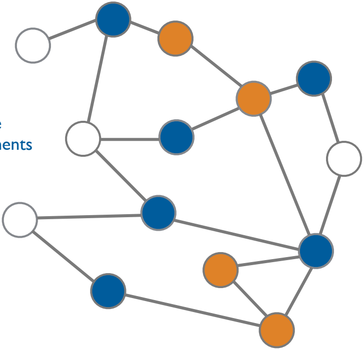
Secrecy in a Network

Operator

Eavesdropper

Legitimate Measurements

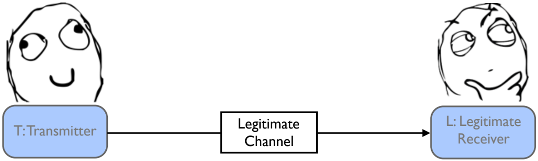
Compromised Measurements



What are the conditions for secrecy?

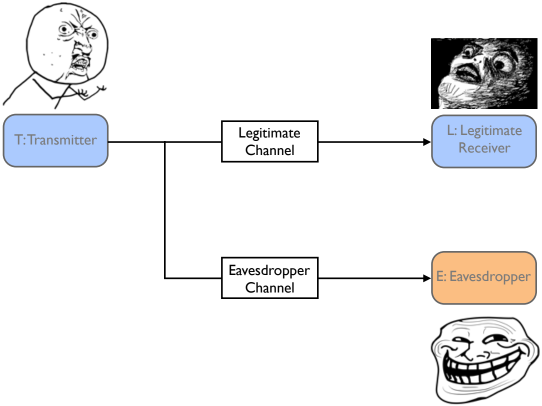
Wiretap channel

A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355-1387, Oct. 1975



Wiretap channel

A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355-1387, Oct. 1975



Secrecy types

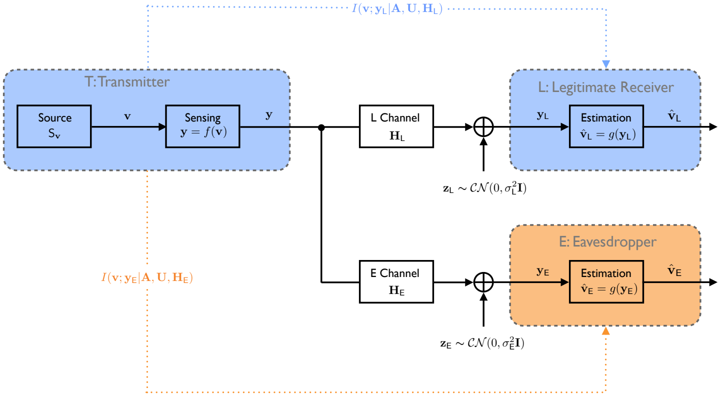
- Weak secrecy

$$\lim_{n\to\infty} \frac{1}{n} I(\mathbf{x}; \mathbf{y}_E) = 0$$

- Strong secrecy

$$\lim_{n\to\infty} I(\mathbf{x}; \mathbf{y}_E) = 0$$

MIMO Wiretap channel model



MIMO Wiretap Channel (Esnaola, Tulino, and Poor 2013)

Let V and Z be independent random variables with $\mathsf{V} \sim F_{\mathsf{V}}$ and $\mathsf{Z} \sim \mathcal{CN}(0,1)$ and $\mathbf{R}_{\mathsf{L}} = \mathbf{A}^{\dagger}\mathbf{U}^{\dagger}\mathbf{H}_{\mathsf{L}}^{\dagger}\mathbf{H}_{\mathsf{L}}\mathbf{A}\mathbf{U}$ and $\mathbf{R}_{\mathsf{E}} = \mathbf{A}^{\dagger}\mathbf{U}^{\dagger}\mathbf{H}_{\mathsf{E}}^{\dagger}\mathbf{H}_{\mathsf{E}}\mathbf{A}\mathbf{U}$, respectively. Then,

$$\begin{aligned}\mathcal{I}_S &= \Bigg(I_s(\mathsf{V},\eta_{\mathsf{L}},\eta_{\mathsf{E}}) - \log e\,(\eta_{\mathsf{L}}\chi_{\mathsf{L}} - \eta_{\mathsf{E}}\chi_{\mathsf{E}}) \\ &\qquad + \log e \left(\int_0^{\chi_{\mathsf{L}}} \mathcal{R}_{\mathbf{R}_{\mathsf{L}}}(-u)du - \int_0^{\chi_{\mathsf{E}}} \mathcal{R}_{\mathbf{R}_{\mathsf{E}}}(-u)du \right) \Bigg)^+\end{aligned}$$

where

$$I_s(\mathsf{V},\eta_{\mathsf{L}},\eta_{\mathsf{E}}) \triangleq I\left(\mathsf{V};\mathsf{V}+\frac{1}{\sqrt{\eta_{\mathsf{L}}}}\mathsf{Z}\right) - I\left(\mathsf{V};\mathsf{V}+\frac{\sigma_{\mathsf{E}}}{\sqrt{\eta_{\mathsf{E}}}}\mathsf{Z}\right)$$

and η_{L}, η_{E}, χ_{L}, χ_{E} are the non-negative solutions to the system of fixed point equations given by

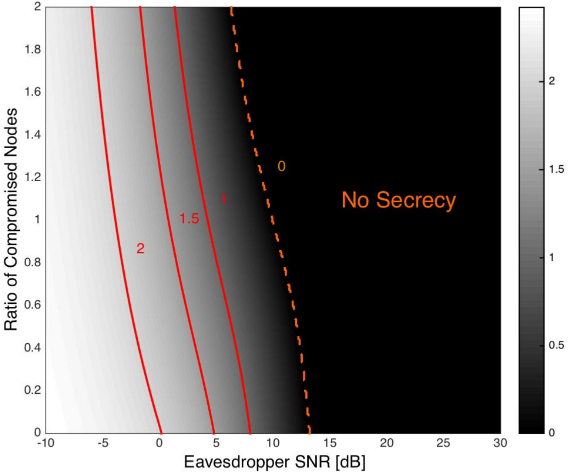
$$\begin{aligned}\eta_{\mathsf{L}} &= \mathcal{R}_{\mathbf{R}_{\mathsf{L}}}(-\chi_{\mathsf{L}}) \\ \chi_{\mathsf{L}} &= \mathrm{mmse}(\eta_{\mathsf{L}}) \\ \eta_{\mathsf{E}} &= \mathcal{R}_{\mathbf{R}_{\mathsf{E}}}(-\chi_{\mathsf{E}}) \\ \chi_{\mathsf{E}} &= \mathrm{mmse}(\eta_{\mathsf{E}})\end{aligned}$$

where we define

$$\mathrm{mmse}(\eta) \triangleq \mathbb{E}\left[|\mathsf{V} - \mathbb{E}(\mathsf{V}|\mathsf{V}+\eta^{-\frac{1}{2}}\mathsf{Z})|^2 \right]$$

Secrery region

$\mathrm{SNR_L} = 10\ dB$



Thanks!