



On Secrecy Capacity per Unit Cost

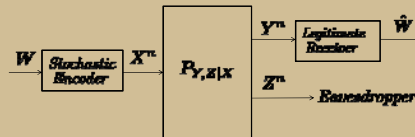
Mustafa El-Halabi, Tie Liu, and Costas Georgiades

Department of Electrical & Computer Engineering, Texas A&M University

Abstract

The concept of secrecy capacity per unit cost is introduced in the context of wideband secrecy communication. For degraded wiretap channels, we show that an orthogonal coding scheme achieves the secrecy capacity per unit cost with a zero-cost input letter, whereas for general wiretap channels, we provide upper and lower bounds on the secrecy capacity per unit cost. Also, we prove that Gaussian noise is the worst additive at the legitimate receiver for Gaussian wiretap channels.

Degraded Wiretap Channel



Theorem 1

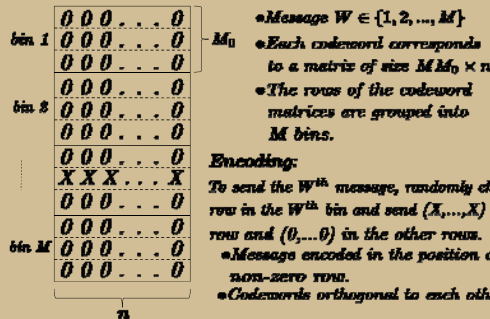
The secrecy capacity per unit cost C_s of the stationary wiretap channel, with $X \rightarrow Y \rightarrow Z$, with zero-cost input letter, is given by:

$$C_s = \sup_{x \in \mathcal{X}} \frac{D(P_{Y|X=x} \| P_{Y|X=0}) - D(P_{Z|X=x} \| P_{Z|X=0})}{b(x)}$$

proof:

Achievability:

Signalling scheme: Random binning over orthogonal codes.



Decoding: binary hypothesis testing on each of the rows to decide on the position of the non-zero row

Performance testing: using Stein's lemma, we can show that:

$$\Pr\{(0, \dots, 0) \rightarrow (x, \dots, x)\} \doteq \begin{cases} \exp[-nD(P_{Y|X=x} \| P_{Y|X=0})] & \text{at legitimate receiver} \\ \exp[-nD(P_{Z|X=x} \| P_{Z|X=0})] & \text{at eavesdropper} \end{cases}$$

• Decoding at the legitimate receiver: $M M_0 \doteq \exp[-nD(P_{Y|X=x} \| P_{Y|X=0})]$

• Secrecy at eavesdropper: $M_0 \doteq \exp[-nD(P_{Z|X=x} \| P_{Z|X=0})]$

• An achievable secrecy per unit cost:

$$R_s = \frac{\log M}{nb(x)} \doteq \frac{D(P_{Y|X=x} \| P_{Y|X=0}) - D(P_{Z|X=x} \| P_{Z|X=0})}{b(x)}$$

The converse:

Application of data processing inequality for divergence.

General Wiretap Channel

Csiszár & Körner: (Secure broadcasting)

Secrecy capacity cost function:

$$C_s(\beta) = \sup_{\substack{U \rightarrow X \rightarrow (Y, Z) \\ I(U; X) \leq \beta}} [I(U; Y) - I(U; Z)]$$

Theorem 2

The secrecy capacity per unit cost C_s of the stationary wiretap channel, with a zero-cost input letter "0" is bounded from above as:

$$C_s \leq \sup_{x \in \mathcal{X}} \frac{D(P_{Y|X=x} \| P_{Y|X=0}) - D(P_{Z|X=x} \| P_{Z|X=0})}{b(x)}$$

for any $P_{Y', Z'|X}$ such that $P_{Y'} = P_Y$ and $P_{Z'} = P_Z$.

proof:

Using a fictitious degraded wiretap channel, and using a Sato type upper bound.

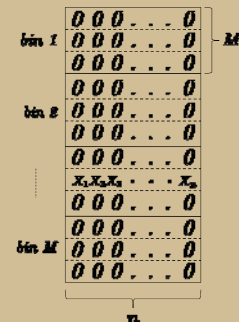
Theorem 3

The secrecy capacity per unit cost C_s of the stationary wiretap channel, with a zero-cost input letter "0" is bounded from below as:

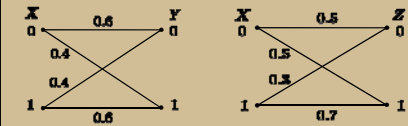
$$C_s \geq \sup_P \frac{D(P_Y \| P_{Y|X=0}) - D(P_Z \| P_{Z|X=0})}{E[b(x)]}$$

proof:

Using same footsteps as those for the achievability in theorem 1, but with further randomization of pulse shape, not only pulse position.



Example

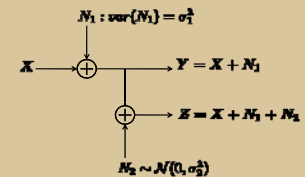


General wiretap channel $(X, (Y, Z), P_{Y, Z|X})$

- Cost function: $b(0) = 0, b(1) = 1$
 - Using randomization of position: $D(P_{Y|X=1} \| P_{Y|X=0}) - D(P_{Z|X=1} \| P_{Z|X=0}) \approx -0.0012$
 - Using randomization of position and shape, with $(\frac{1}{2}, \frac{1}{2})$ distribution: $D(P_Y \| P_{Y|X=0}) - D(P_Z \| P_{Z|X=0}) \approx 0.9003$
- Conclusion: Position randomization is suboptimal.

Worst Noise Result

Additive Gaussian wiretap channel



- N_1 and N_2 are independent
- If $N_1 \sim \mathcal{N}(0, \sigma_1^2)$ the secrecy capacity per unit cost is: $C_s = \frac{1}{2} \frac{\sigma_2^2}{\sigma_1^2(\sigma_1^2 + \sigma_2^2)}$
- If N_1 is non Gaussian, then using Fisher information inequality $C_s \geq \frac{1}{2} \frac{\sigma_2^2}{\sigma_1^2(\sigma_1^2 + \sigma_2^2)}$

Conclusion: Gaussian is the worst additive noise for legitimate receiver.

Conclusion

The maximum number of secured bits per unit energy was abstracted by introducing the concept of secrecy capacity per unit cost. It was shown that random orthogonal signalling with a constant pulse shape achieves the secrecy capacity per unit cost for the degraded case, while in the general case, a further randomization of the pulse shape can improve the achievable secrecy rate per unit cost.

Shannon, Wyner & Verdú

Shannon: (Classical model)

$$\text{rate} = (\# \text{reliable bits}) / (\# \text{channel uses})$$

$$\text{subject to: } \sum_{i=1}^n b(x_i) \leq \beta$$

$$\text{For a DMC: } C(\beta) = \sup_{\substack{P_{\mathcal{X}} \\ E[b(X)] \leq \beta}} I(X; Y)$$

Wyner: (Bandlimited secrecy)

Secrecy capacity cost function for a DMC:

$$C_s(\beta) = \sup_{\substack{P_{\mathcal{X}} \\ E[b(X)] \leq \beta}} [I(X; Y) - I(X; Z)]$$

Verdú: (Wideband communication)

Energy is the most important resource.

$$\text{Rate per unit cost} = \frac{\# \text{reliable bits}}{\text{cost of transmission}}$$

Capacity per unit cost for a DMC:

$$C = \sup_{\beta > 0} \frac{C(\beta)}{\beta}$$

In the case of a "zero-cost" input letter;

$$b(0) = 0, C = \sup_{x \in \mathcal{X}} \frac{D(P_{Y|X=x} \| P_{Y|X=0}) - D(P_{Z|X=x} \| P_{Z|X=0})}{b(x)}$$