On the Estimation of Joint Mutual Information for Physical Layer Security

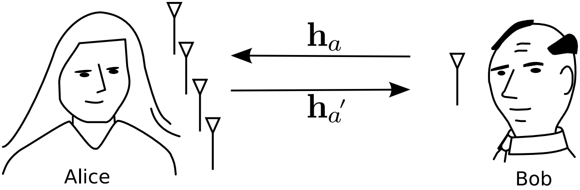
Rashid Mehmood and Attiya Mahmood
Course Project: ECEN 670

Brigham Young University

December 3, 2013

Table of Contents

Physical Layer Security



- The reciprocal channel ($h_a = h_{a'}$) can be used to generate the secret key.
- Requires channel to be changing with time (fading).

Available Key bits (I_{K})

- How many secret key bits can be generated per observation of the channel?
- Depends on the mutual information between the two channels.
- **Mutual Information**: Amount of information shared between $\hat{h}_a$ and $\hat{h}_{a'}$. How much information $\hat{h}_a$ tells us about $\hat{h}_{a'}$ and vice versa.

$$I_{\mathrm{K}} = I(\hat{h}_a; \hat{h}_{a'}) = \mathbf{E}\left\{\log_2 \frac{f(\hat{h}_a, \hat{h}_{a'})}{f(\hat{h}_a) f(\hat{h}_{a'})}\right\}. \tag{1}$$

Available Key bits (I_{K})

- Mutual Information can also be computed from Entropy.
- **Entropy**: Average information gained by observing a single variable

$$\mathrm{H}(\hat{h}_a) = \int f(\hat{h}_a) \log f(\hat{h}_a) d\hat{h}_a. \tag{2}$$

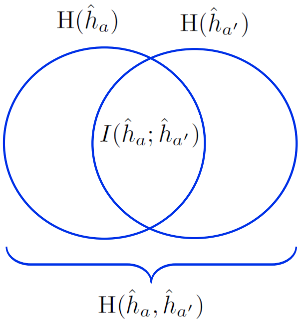
- **Joint Entropy**: Average total information gained by observing two or more variables

$$\mathrm{H}(\hat{h}_a, \hat{h}_{a'}) = \int f(\hat{h}_a, \hat{h}_{a'}) \log f(\hat{h}_a, \hat{h}_{a'}) d\hat{h}_a d\hat{h}_{a'}. \tag{3}$$

Available Key bits (I_{K})

- Mutual Information in terms of entropy is

$$I_{\mathrm{K}} = \mathrm{H}(\hat{h}_a) + \mathrm{H}(\hat{h}_{a'}) - \mathrm{H}(\hat{h}_a, \hat{h}_{a'}).$$

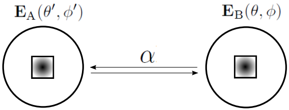


Wireless Channel

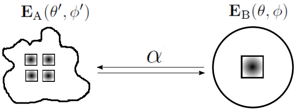
- Estimated channels at Alice and Bob are

$$\hat{h}_a = \mathbf{E}_{\mathrm{A}}(\theta', \phi')\alpha\mathbf{E}_{\mathrm{B}}(\theta, \phi) + \epsilon_a. \tag{4}$$

$$\hat{h}_{a'} = \mathbf{E}_{\mathrm{B}}(\theta, \phi)\alpha\mathbf{E}_{\mathrm{A}}(\theta', \phi') + \epsilon_{a'}. \tag{5}$$



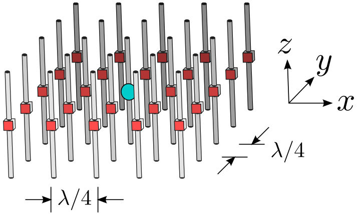
α is varying



α is fixed

Wireless Channel using Reconfigurable Antenna

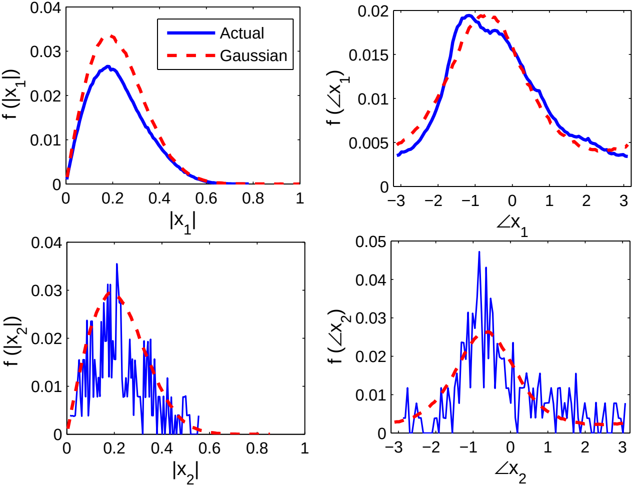
- Alice has a reconfigurable antenna.
- Each reconfigurable element (RE) is a switch.



- Channel is generated by changing the states of REs using an i.i.d uniform distribution.
- Channel distribution is unknown.

Wireless Channel using Reconfigurable Antenna

- $x_1 = h_a$ for $N_{\mathrm{RE}} = 24$, $x_2 = h_a$ for $N_{\mathrm{RE}} = 8$.



Available Key bits Computation

- Approaches
  - Gaussian Approximation ($I_{\mathrm{K,GA}}$)
  - Numerical Computation ($I_{\mathrm{K,NC}}$)
  - Histogram based Approximation ($I_{\mathrm{K,HA}}$)
  - Gaussian Mixtures based Approximation ($I_{\mathrm{K,GM}}$)
- Channels
  - By assuming h_a is Gaussian
  - By computing h_a for $N_{\mathrm{RE}} = 24$
  - By computing h_a for $N_{\mathrm{RE}} = 8$

Gaussian Approximation

- Closed form solution of entropy exists [1]

$$
\begin{aligned}
I_{\mathrm{K,GA}} &= \mathrm{H}(\hat{h}_a) + \mathrm{H}(\hat{h}_{a'}) - \mathrm{H}(\hat{h}_a, \hat{h}_{a'}), \qquad (6)\\
&= \log_2(\pi e)\sigma^2_{\hat{h}_a} + \log_2(\pi e)\sigma^2_{\hat{h}_{a'}} - \log_2(\pi e)^2|\hat{\mathbf{R}}_{h_a h_{a'}}|.
\end{aligned}
$$

Channel	$I_{\mathrm{K,GA}}$ (in bits)
Gaussian	2.5266
$N_{\mathrm{RE}} = 24$	2.3074
$N_{\mathrm{RE}} = 8$	2.0643

Numerical Computation

- Mutual information needs to be computed numerically [2]

$$I_{\mathrm{K,NC}} = I(\hat{h}_a; \hat{h}_{a'}) = \mathbf{E}\left\{\log_2 \frac{f(\hat{h}_a, \hat{h}_{a'})}{f(\hat{h}_a) f(\hat{h}_{a'})}\right\}. \qquad (7)$$

- The individual pdfs $f(\hat{h}_a)$ and $f(\hat{h}_{a'})$ can be expressed in terms of the conditional pdfs

$$\begin{aligned} f(\hat{h}_a) &= \int f(\hat{h}_a | h_a) dh_a = \mathrm{E}_{h_a} f(\hat{h}_a | h_a), \\ &= \mathrm{E}_{h_a} f_n((\hat{h}_a - h_a)/\sigma_a^2). \end{aligned} \qquad (8)$$

Similarly,

$$f(\hat{h}_{a'}) = \mathrm{E}_{h_a} f_n((\hat{h}_{a'} - h_a)/\sigma_{a'}^2). \qquad (9)$$

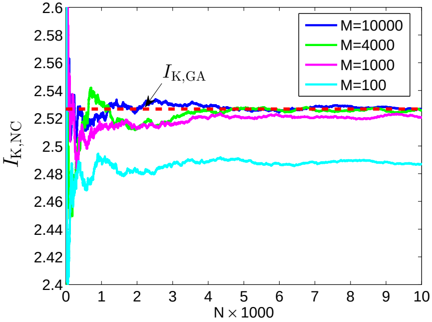
Numerical Computation

- Joint pdf $f(\hat{h}_a, \hat{h}_{a'})$ can be expressed as the product of two noise pdfs

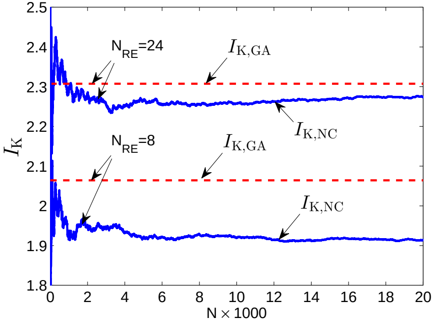
$$
\begin{aligned}
f(\hat{h}_a, \hat{h}_{a'}) &= \int f(\hat{h}_a, \hat{h}_{a'} | h_a) dh_a \qquad (10) \\
&= \mathrm{E}_{h_a} f(\hat{h}_a, \hat{h}_{a'} | h_a) = \mathrm{E}_{h_a} \{ f(\hat{h}_a | h_a) f(\hat{h}_{a'} | h_a) \} \\
&= \mathrm{E}_{h_a} \{ f_n((\hat{h}_a - h_a)/\sigma_a^2) f_n((\hat{h}_{a'} - h_a)/\sigma_{a'}^2 \}.
\end{aligned}
$$

- The convergence of the numerical computation will depend on N and M, which are the number of sample points in the outer and inner expectations.

Numerical Computation



Gaussian distribution for h_a



Arbitrary distribution for h_a

Histogram based Approximation

- Mutual information is computed by estimating the pdfs using multi-dimensional histograms

$$I_{\mathrm{K,HA}} = I(\hat{h}_a; \hat{h}_{a'}) = \mathbf{E}\left\{\log_2 \frac{f(\hat{h}_a, \hat{h}_{a'})}{f(\hat{h}_a) f(\hat{h}_{a'})}\right\}. \tag{11}$$

- Estimated channel pdfs can be expressed in terms of convolution as

$$f(\hat{h}_a) = f(h_a) * f(\epsilon_a). \tag{12}$$

$$f(\hat{h}_{a'}) = f(h_{a'}) * f(\epsilon_{a'}). \tag{13}$$

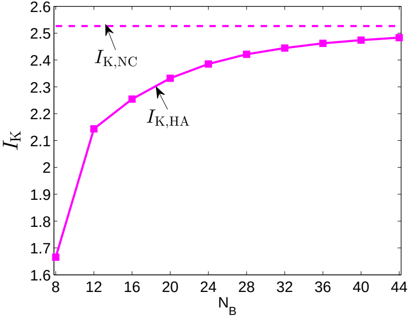
Histogram based Approximation

- The joint pdf $f(\hat{h}_a, \hat{h}_{a'})$ can be expressed as

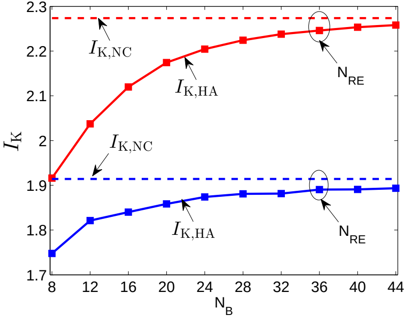
$$f(\hat{h}_a, \hat{h}_{a'}) = f(h_a, h_{a'}) * f(\epsilon_a, \epsilon_{a'}). \tag{14}$$

- 2-D and 4-D convolution and histograms are used for computing individual and joint pdfs.
- Number of bins (N_B) along each dimension is variable.

Histogram based Approximation



Gaussian distribution for h_a

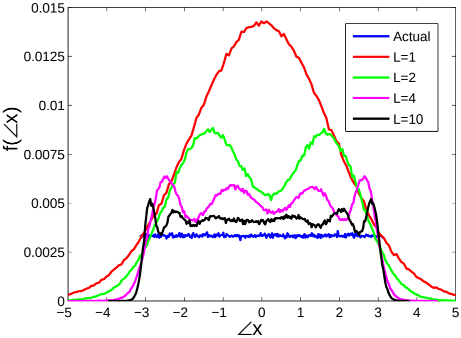


Arbitrary distribution for h_a

Gaussian Mixture based Approximation

- A given distribution can be expressed in terms of a mixture of several Gaussian distributions

$$\hat{f}(\angle x) = \sum_{i=1}^{L} w_i \cdot \mathcal{N}(\angle x, \mu_i, \sigma_i^2). \tag{15}$$



Gaussian Entropy Computation

- Mutual information is computed using the entropy as

$$I_{\mathrm{K,GM}} = \mathrm{H}(\hat{h}_a) + \mathrm{H}(\hat{h}_{a'}) - \mathrm{H}(\hat{h}_a, \hat{h}_{a'}). \quad (16)$$

- The entropy for a random vector $\underline{x}$ of size P with pdf $f(\underline{x})$ is given by

$$\mathrm{H}(\underline{x}) = \int f(\underline{x}) \cdot \log f(\underline{x}) d\underline{x}. \quad (17)$$

where

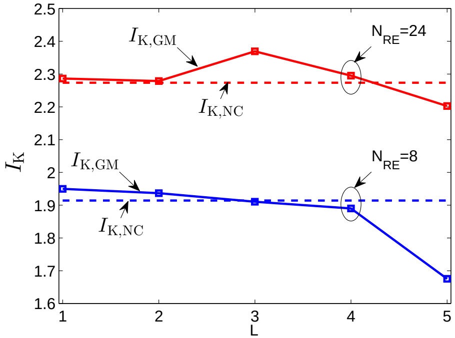
$$f(\underline{x}) = \sum_{i=1}^{L} w_i \cdot \mathcal{N}(\underline{x}, \underline{\mu}_i, \mathbf{C}_i). \quad (18)$$

- $\log f(\underline{x})$ is estimated using Taylor series [3]

$$\log f(\underline{x}) = \sum_{k=0}^{R} \frac{1}{k!} ((\underline{x} - \underline{\mu_i}) \odot \Delta)^k \log f(\underline{x})|_{\underline{x}=\underline{\mu_i}} + O_R. \quad (19)$$

Gaussian Entropy Computation

- For Gaussian distribution $I_{\mathrm{K,GM}} = 2.5216$ when $L = 1$.



Arbitrary distribution for h_a

Conclusion

- Comparison of different techniques for arbitrary channel distribution.
- Case A: h_a is generated using $N_{\mathrm{RE}} = 24$
- Case B: h_a is generated using $N_{\mathrm{RE}} = 8$

Method Used	I_{K} for Case A	I_{K} for Case B	Time
Gaussian Approx	2.3074	2.0643	≤ 1
Numerical Computation	2.2737	1.9142	1920
Histogram based Approx	2.2581	1.8908	13289
Gaussian mixtures	2.2787	1.9106	209

References

- J. Wallace, “Secure physical layer key generation schemes: performance and information theoretic limits,” in *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE, 2009, pp. 1–5.
- R. Mehmood and J. W. Wallace, “Wireless security enhancement using parasitic reconfigurable aperture antennas,” in *Antennas and Propagation (EUCAP), Proceedings of the 5th European Conference on*. IEEE, 2011, pp. 2761–2765.
- M. F. Huber, T. Bailey, H. Durrant-Whyte, and U. D. Hanebeck, “On entropy approximation for gaussian mixture random vectors,” in *Multisensor Fusion and Integration for Intelligent Systems, 2008. MFI 2008. IEEE International Conference on*. IEEE, 2008, pp. 181–188.