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
- Artificial fading in Wireless Channel
- Estimation of Mutual Information using different approaches
- Comparison of Results
- Conclusion
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.

$$I_K = I(\hat{h}_a; \hat{h}_a') = \mathbb{E} \left\{ \log_2 \frac{f(\hat{h}_a, \hat{h}_a')}{f(\hat{h}_a)f(\hat{h}_a')} \right\}. \quad (1)$$
Available Key bits ($I_K$)

- Mutual Information can also be computed from Entropy.
- **Entropy**: Average information gained by observing a single variable
  \[
  H(h_a) = \int f(h_a) \log f(h_a) \, dh_a. \tag{2}
  \]
- **Joint Entropy**: Average total information gained by observing two or more variables
  \[
  H(h_a, h_a') = \int f(h_a, h_a') \log f(h_a, h_a') \, dh_a \, dh_a'. \tag{3}
  \]
Available Key bits ($I_K$)

- Mutual Information in terms of entropy is

$$I_K = H(\hat{h}_a) + H(\hat{h}_{a'}) - H(\hat{h}_a, \hat{h}_{a'}).$$
Wireless Channel

- Estimated channels at Alice and Bob are

\[
\hat{h}_a = E_A(\theta', \phi') \alpha E_B(\theta, \phi) + \epsilon_a. \tag{4}
\]

\[
\hat{h}_{a'} = E_B(\theta, \phi) \alpha E_A(\theta', \phi') + \epsilon_{a'}. \tag{5}
\]

\[\alpha\text{ is varying}\]

\[\alpha\text{ is fixed}\]
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

\[ x_1 = h_a \text{ for } N_{\text{RE}} = 24, \ x_2 = h_a \text{ for } N_{\text{RE}} = 8. \]
Available Key bits Computation

Approaches

- Gaussian Approximation ($I_{K,GA}$)
- Numerical Computation ($I_{K,NC}$)
- Histogram based Approximation ($I_{K,HA}$)
- Gaussian Mixtures based Approximation ($I_{K,GM}$)

Channels

- By assuming $h_\alpha$ is Gaussian
- By computing $h_\alpha$ for $N_{RE} = 24$
- By computing $h_\alpha$ for $N_{RE} = 8$
Gaussian Approximation

- Closed form solution of entropy exists [1]

\[ I_{K,GA} = H(\hat{h}_a) + H(\hat{h}_a') - H(\hat{h}_a, \hat{h}_a'), \]
\[ = \log_2(\pi e)\sigma^2_{\hat{h}_a} + \log_2(\pi e)\sigma^2_{\hat{h}_a'} - \log_2 (\pi e)^2 |\hat{R}_{h_a h_a'}|. \]  

<table>
<thead>
<tr>
<th>Channel</th>
<th>( I_{K,GA} ) (in bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian</td>
<td>2.5266</td>
</tr>
<tr>
<td>( N_{RE} = 24 )</td>
<td>2.3074</td>
</tr>
<tr>
<td>( N_{RE} = 8 )</td>
<td>2.0643</td>
</tr>
</tbody>
</table>
Numerical Computation

- Mutual information needs to be computed numerically [2]

\[
I_{K,NC} = I(\hat{h}_a; \hat{h}_a') = \mathbb{E} \left\{ \log_2 \frac{f(\hat{h}_a, \hat{h}_a')}{f(\hat{h}_a)f(\hat{h}_a')} \right\}. \tag{7}
\]

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

\[
f(\hat{h}_a) = \int f(\hat{h}_a|h_a) \, dh_a = \mathbb{E}_{h_a} f(\hat{h}_a|h_a), \tag{8}
\]

\[= \mathbb{E}_{h_a} f_n((\hat{h}_a - h_a)/\sigma_a^2). \]

Similarly,

\[
f(\hat{h}_a') = \mathbb{E}_{h_a} f_n((\hat{h}_a' - h_a)/\sigma_a'^2). \tag{9}
\]
Numerical Computation

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

\[
f(\hat{h}_a, \hat{h}_a') = \int f(\hat{h}_a, \hat{h}_a' | h_a) dh_a
\]

\[
= E_{h_a} f(\hat{h}_a, \hat{h}_a' | h_a) = E_{h_a} \{ f(\hat{h}_a | h_a) f(\hat{h}_a' | h_a) \}
\]

\[
= E_{h_a} \{ f_n((\hat{h}_a - h_a)/\sigma_a^2) f_n((\hat{h}_a' - h_a)/\sigma_{a'}^2) \}.
\]

- 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.
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

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

- 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

$$f(\hat{h}_a, \hat{h}_{a'}) = f(h_a, h_{a'}) \ast f(\epsilon_a, \epsilon_{a'}).$$  \hspace{1cm} (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 $h_a$
A given distribution can be expressed in terms of a mixture of several Gaussian distributions:

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

(15)
Gaussian Entropy Computation

- Mutual information is computed using the entropy as
  \[ I_{K,\text{GM}} = H(\hat{h}_a) + H(\hat{h}_a') - H(\hat{h}_a, \hat{h}_a'). \] (16)
- The entropy for a random vector \( \underline{x} \) of size \( P \) with pdf \( f(\underline{x}) \) is given by
  \[ H(\underline{x}) = \int f(\underline{x}) \cdot \log f(\underline{x}) d\underline{x}. \] (17)
  where
  \[ f(\underline{x}) = \sum_{i=1}^{L} w_i \cdot \mathcal{N}(\underline{x}, \underline{\mu}_i, \underline{C}_i). \] (18)
- \( \log f(\underline{x}) \) is estimated using Taylor series [3]
  \[ \log f(\underline{x}) = \sum_{k=0}^{R} \frac{1}{k!} ((\underline{x} - \underline{\mu}_i) \odot \Delta)^k \log f(\underline{x})|_{\underline{x}=\underline{\mu}_i} + O_R. \] (19)
Gaussian Entropy Computation

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

Arbitrary distribution for $h_\alpha$
Conclusion

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

<table>
<thead>
<tr>
<th>Method Used</th>
<th>$I_K$ for Case A</th>
<th>$I_K$ for Case B</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian Approx</td>
<td>2.3074</td>
<td>2.0643</td>
<td>≤ 1</td>
</tr>
<tr>
<td>Numerical Computation</td>
<td>2.2737</td>
<td>1.9142</td>
<td>1920</td>
</tr>
<tr>
<td>Histogram based Approx</td>
<td>2.2581</td>
<td>1.8908</td>
<td>13289</td>
</tr>
<tr>
<td>Gaussian mixtures</td>
<td>2.2787</td>
<td>1.9106</td>
<td>209</td>
</tr>
</tbody>
</table>
References

