Physical Layer Security Overview

Yao Zheng

Outline

• Research Problem Statement
• Introduction to Achievable Rate and Capacity
• Physical Layer (PHY) Security
• Some Research Results
• Conclusions and Future work

Research Problem Statement

Wireless Environment

• Open-access medium

Wiretap Channel Modeling

• The received signals are modeled as

\[ Y = HX + W \]
\[ Z = GX + W' \]

where \( H, G \) are channel coefficients and \( W, W' \) are Gaussian noises

Channel State Information

• In convention, the channel state information (CSI) \( H, G \) are assumed to be known to all the nodes

• However, letting the eavesdropper know the CSI can be problematic by increasing her ability in eavesdropping
Reference Signaling

- In wireless communications, we use reference signals to help estimate channel information

Conventional Channel Estimation

- Uplink and downlink channel estimation

Channel Estimation for Secrecy

- Q: Is uplink reference signaling enough?

Introduction to Achievable Rate and Capacity

Rate without Noises and Channel Uncertainty

- Let’s take a look at the point-to-point channel

Random Property

- We often model the $X, Y, H, Z$ as random variables

• For example, let $X$ be a Bernoulli random variable

<table>
<thead>
<tr>
<th>Degenerate case</th>
<th>Randomized case</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P(X = 1) = 1$</td>
<td>$P(X = 0) = 1/2$</td>
</tr>
<tr>
<td>$P(X = 0) = 0$</td>
<td>$P(X = 1/2) = 1$</td>
</tr>
<tr>
<td>Message: 11111111...</td>
<td>Message: 01011100101...</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Channel Uncertainty and Noises
• However, channel uncertainty and noises make it impossible to deliver messages at an infinite rate

\[ X \xrightarrow{channel} Y \xrightarrow{noise} X = Y \]

• That is, \( Y = HX + W \) where \( H \) is the channel coefficient and \( |W| \) is the additive noise
• Reference signaling can help eliminate the channel uncertainty

Overcome the Noise
• Assume a Gaussian channel, i.e., \( Y = X + W \) where \( W \sim N(0, \sigma_w^2) \)
• To overcome the noise, we can quantize the transmitted symbol \( X \)

\[ X + Z = Y \]

• Since the transmit power, i.e., \( \mathbb{E}(X) \), is limited, the number of quantization levels is limited \( \Rightarrow \) rate is limited

Rate and Capacity
• With the noise, we know that the transmission rate cannot be infinite
• Q: How large can the rate be? Or is there a capacity (maximum achievable rate)?
• The notion of capacity

Channel Coding
• Channel coding is essential for achieving the capacity
• Channel coding: Ways to quantize and randomize the transmitted symbol to tolerate noises and convey as much information as possible

Some Assumptions
• We want to transmit at a rate of \( R \), i.e., each symbol represents \( R \) bits
• As the signals are sent through time, let \( Y_i = HX_i + W \) where \( i \in \{1, \ldots, n\} \) is the time index

\[ \begin{align*} X_1 & \quad X_2 & \quad \cdots & \quad X_n \\ R & + R & + \cdots & + R = nR \text{ bits} \end{align*} \]
• Therefore, we convey a message from a \( 2^R \) set, e.g., \( \{M_1, M_2, \ldots, M_{2^R}\} \)

Random Coding
• Random coding: randomly generate the quantization according to a specific distribution
• In the theoretical development, random coding saves the struggle of designing a channel coding scheme
• Random coding is generally not good in the practical use
Codebook Generation

- In random coding, we need to randomly generate a codebook

- For each message candidate, there is a randomly generated codeword associated with it

Achievable Rate

- A rate is said to be achievable if there exists a channel coding scheme (including random coding) such that the message error probability, i.e., $P(M \neq \hat{M})$, is zero as $n \to \infty$

- For example, with the CSI $H$ known to both the transmitter and the receiver, it turns out that the capacity of the channel

\[ y_i = h_i x_i + w_i \]

subject to the power constraint $\frac{1}{n} \sum x_i^2 \leq P$, is given by

\[ R = \frac{1}{2} \log(1 + P \frac{h_i^2}{w_i^2}) \]

Converse

- Capacity proofs usually consist of two parts
  - Achievability
  - Converse

- The converse part helps you identify that a certain achievable rate is in fact the maximum rate (capacity), i.e., any rate above it is not achievable

- Usually, the converse part of the proof is difficult and may not be always obtained

Physical Layer (PHY) Security

- Scenario: The transmitter wants to send secret messages to the receiver without being wiretapped by the eavesdropper

- In 1975, Wyner showed that channel coding is possible to protect the secret messages without using any cryptography methods

- The corresponding maximum rate of the secret message is referred to as the "secrecy capacity"

Gaussian Wiretap Channel

- The received signals are modeled as

\[ y = h x + w \]

subject to the power constraint $\mathbb{E}[x^2] \leq P$

where $h, w$ are the channel coefficients and $w, x \sim \mathcal{CN}(0,1)$
Secrecy Capacity

- Suppose that the CSI \( G \) are known to all the terminals. The secrecy capacity turns out to be

\[
C_s = \log_2 \left( 1 + \frac{|G|^2 P}{N_0} \right) - \log_2 \left( 1 + |G|^2 P_R \right)
\]

where \( a = \max(0, a) \).

- To have a positive secrecy capacity, the receiver should experience a better channel than the eavesdropper, i.e., \( |G|^2 P > |G|^2 P_R \).

Interpretation of Secrecy Capacity

- Information theoretic points of view

- This portion is used to overwhelm the eavesdropper

- This remaining portion is the secrecy capacity

Random Modulation

- Use 4PSK to transmit the secret message while randomly choosing the quadrants to confuse the eavesdropper

- For example, to transmit the 00 symbol, we have four candidates to select

- 2-bit degrees of freedom are used to confuse the eavesdropper

Realistic Channel Assumption

- An essential assumption for achieving the secrecy capacity is for the transmitter to know the CSI from the eavesdropper

- However, as a malicious node, the eavesdropper will not feed its channel information back

- What we are interested in is “Secrecy with CSIT only”
Some Research Results

SISO Wiretap Channel Model

- The received signals are modeled as
  \[ Y = HX + W \]
  \[ Z = GX + W' \]

where \( H \in \mathbb{C} \mathcal{N}(0, \sigma_h^2) \), \( G \in \mathbb{C} \mathcal{N}(0, \sigma_g^2) \), and \( W, W' \in \mathbb{C} \mathcal{N}(0, 1) \)

Case 1: Reversed Training without CSIRE

- Suppose that the transmitter knows \( H \) but doesn’t know \( G \).
  
- We take the strategy of channel inversion with a channel quality threshold for transmission, i.e.,
  \[ X = \begin{cases} 1 & \text{if } |H| > \gamma \\text{transmit} \\ 0 & \text{stop} \end{cases} \]
  
where \( \gamma \sim \mathbb{C} \mathcal{N}(0, \sigma_h^2) \)

- \( X \) and \( \gamma \) are first revealed to the receiver and eavesdropper

Resulting Channel and Achievable Rate

- The resulting received signals at the receiver and eavesdropper are
  \[ Y = E_{|H|>\gamma} H \begin{cases} 1 & \text{if } |H| > \gamma \\text{transmit} \\ 0 & \text{stop} \end{cases} + W \]
  \[ Z = \frac{G}{H} E_{|H|>\gamma} |H| \begin{cases} 1 & \text{if } |H| > \gamma \\text{transmit} \\ 0 & \text{stop} \end{cases} + W' \]

- We want to find an achievable secrecy rate for this scheme as
  \[ R_{secrecy} = \max_{\mathbf{G}} I(S;Y) - I(S;Z) \]
  
where the mutual information is obtained by numerical integration

Case 2: Reversed Training with Practical CSIRE

- Here, we assume that the receiver and eavesdropper know their respective received SNR, i.e., \( Y = |H|^2 E|X|^2 |H|^2 \) and \( L = |G|^2 E|X|^2 |H|^2 \)

- So the transmitter only has to null the phase to the receiver. The resulting channel is given by
  \[ Y = |H| E_{|H|>\gamma} S + W \]
  \[ Z = |G| E_{|H|>\gamma} |H| S + W' \]

where \( \gamma \) is a uniform phase random variable

Achievable Secrecy Rate

- It turns out that the achievable secrecy rate is given by
  \[ R_{secrecy} = \max_{\mathbf{G}} I(S;Y) - I(S;Z) \]
  
where
  \[ I(S;Y) = E_{|H|>\gamma} \log(1 + |H|^2 |S|^2) \]

and
  \[ I(S;Z) = E_{|H|>\gamma} \log(1 + |H|^2 |S|^2 |Z|^2) \]
Asymptotic Bounds on the Achievable Rates

- Since the achievable rates above rely on the numerical integration, explicit asymptotic bounds are also useful for performance evaluation.

- Based on the techniques in [1], we can derive the asymptotic lower bounds for the above achievable secrecy rates as

\[
\begin{align*}
\mathcal{R}_s & \approx \frac{1}{2} \log \left( 1 + \left( \frac{2}{\log(1+\gamma)} \right)^2 \right) \\
\mathcal{R} & \approx \frac{1}{2} \log \left( 1 + \left( \frac{2}{\log(1+\gamma)} \right)^2 \right)
\end{align*}
\]


\[
R_s \text{ vs. } \gamma \text{ with } P = 10 \text{ dB and } \sigma_H^2 = \sigma_G^2 = 1
\]

MISO Wiretap Channel Model

- Suppose that the transmitter has \( M \) antennas, and the legitimate receiver and the eavesdropper have respectively one antenna.

- The MISOSE wiretap channel is modeled by

\[
Y = hX + W, \quad Z = gX + W, \quad \text{and} \quad Z \sim \mathcal{CN}(0, \sigma_Z^2)
\]

where \( h \sim \mathcal{CN}(0, \sigma_H^2) \), \( g \sim \mathcal{CN}(0, \sigma_G^2) \), and \( W \sim \mathcal{CN}(0, 1) \).

\[
X \xrightarrow{H} G \xrightarrow{Z} Y
\]

Case 1: Reversed Training without CSIR

- Suppose that the transmitter knows \( h \) but doesn’t know \( g \).

- The transmitter applies the channel inversion strategy with a channel quality threshold, i.e.,

\[
x = \mathbb{E}_h [Y | H] \text{ \( \sim \mathcal{CN}(0,1) \)}
\]

where \( Y \sim \mathcal{CN}(0, \sigma_Y^2) \).

- \( \gamma = 1/N \) and \( \gamma = 1/\sigma_Y^2 \) are first revealed to the receiver and eavesdropper.

Resulting Channel and Achievable Rate

- The resulting received signals at the receiver and eavesdropper are

\[
Y = \mathbb{E}_h [Y | H] S + W, \quad Z = \mathbb{E}_h [Z | H] S + W.
\]

- The achievable secrecy rate for this scheme can still be found by

\[
\mathcal{R}_s = \max_{\mathbb{E}_h} I(S; Y) - I(S, Z).
\]
Case 2: Reversed Training with Practical CSIR

- Here, we assume that the receiver and eavesdropper know their respective received SNR, i.e., $\gamma = \frac{\beta h^T x}{\sigma_n^2}$ and $\tilde{\gamma} = \frac{\tilde{\beta} g^T x}{\sigma_n^2}$.
- So the transmitter only has to null the phase to the receiver. The resulting channel is given by $y = \beta h^T x + \tilde{\beta} \tilde{g}^T x + w$.
- It turns out that the achievable secrecy rate is also given by $R_{s,\text{ach}} = \max_{\tilde{\gamma}} I(S; Y) - I(S; Z)$.

$R_s$ vs. $\gamma$ with $P = 10$ dB and $\sigma_h^2 = \sigma_g^2 = 1$

$R_s$ vs. $P$ with Optimal $\gamma$ and $\sigma_h^2 = \sigma_g^2 = 1$

Backup Slides

Conclusions

- With CSIT only, we can achieve a higher secrecy rate than with full CSI at all the nodes.
- With multiple antennas at the transmitter, the gain on the achievable secrecy rate can be even increased.
- By setting a channel gain threshold $\gamma$, i.e., transmit only when $|h| > \gamma$, the secrecy rate can be effectively improved.

Future Work

- Design an efficient algorithm to find the optimal $\gamma$.
- Find the achievable rate for the multi-antenna receiver and eavesdropper.
- Work on the scenario with finite-precision CSIT. Will the imprecision of the CSIT affect the achievable rate a lot?