Secret Communications with a Helping Interferer

Xiaojun Tang  and Predrag Spasojevic

WINLAB, Rutgers University

joint with Ruoheng Liu  and  H. Vincent Poor (Princeton University)
Outline

• **Introduction**
  - Physical Layer (information-theoretic) secrecy
  - Interference

• **System Model**
  - The Gaussian wiretap channel with a helping interferer

• **Results**
  - An achievable secrecy rate
  - A computable upper bound
  - Numerical examples

• **Summary**
Secret Wireless Communication

Secret Message $W$

- can be successfully decoded by the desired receiver (user 1)
- can NOT be understood by anyone else (e.g. user 2)
Crypto-Systems v.s. Physical Layer Secrecy?

**Crypto-Systems**

- Difficult to distribute *initial key* in a large wireless network.
- Perfect secrecy cannot be ensured, unless the key is infinitely long.

**Physical Layer Secrecy**

- Perfect secrecy is possible without a key.
- Can be used to distribute keys!
How Physical-Layer Secrecy Works

Alice

Bob

Eve

Bob has a “better” channel than Eve
**Wiretap Channel Model**

- **Reliability**
  \[ P_e = \Pr(\hat{W} \neq W) \to 0 \]

- **Secrecy**
  \[ \frac{1}{n} H(W \mid Z^n) \to \frac{1}{n} H(W) \]

**Secrecy capacity** (maximal reliable rate with perfect secrecy) [Wyner-75, Csiszar&Korner-78]:

\[
C_s = \max_{U \to X \to YZ} \left\{ I(U;Y) - I(U;Z) \right\}
\]

**Gaussian channel** [Leung-Yan-Cheong&Hellman-78]:

\[
C_s = \max_X \left\{ I(X;Y) - I(X;Z) \right\}^+
\]

Rate loss (to confuse the eavesdropper)

and Gaussian input distribution is optimal.

**Can we increase the secrecy capacity with the assistance from an interferer?**
Interference can be exploited to keep secrecy

• Interference is created through scheduling transmissions.

Interference (to Eve) carries information to David, NO power is wasted (unlike generating artificial noise).
Gaussian wiretap channel with a helping interferer

- Gaussian channel (standard form)

- Average power constraints: (\(P_1, P_2\))

- Alice transmits at the rate \(R_1\), which is higher than the secrecy rate \(R_S\).

- Chris transmits at the rate \(R_2\):

Q: What is the rate \(R_S\) under the reliability and secrecy constraints?
Achievable Rate

• What is the rate \( R_1 \) the receiver can decode reliably?

• How many bits can the eavesdropper deduce from \( R_1 \)?
Achievable Rate

- The following secrecy rate \((R_S)\) is achievable:

\[
R_s = R_1 - R_{1E}
\]

An interferer can increase the secrecy rate!
Symmetric Gaussian channels

- To illustrate the results, we focus on a symmetric Gaussian channel in which $a=b$.

**Q1:** What is the achievable rate for this channel? *(answered)*

**Q2:** Should the transmitters use full power $(\bar{P}_1, \bar{P}_2)$?

**Power Control!**
Power control for the symmetric channel

• When $a < 1$, the receiver has advantage over the eavesdropper. Hence, do not introduce too much interference.

\[
(P_1, P_2) = \left( \overline{P}_1, \min \{ \overline{P}_2, P_2^* \} \right)
\]

where $P_2^* = \frac{\sqrt{1 + (1 + a)\overline{P}_1} - 1}{1 + a}$.

• When $a \geq 1$, the eavesdropper has advantage over the receiver. Hence, introduce the maximum interference.

\[
(P_1, P_2) = \begin{cases} 
  \left( \min \{ \overline{P}_1, P_1^* \}, \overline{P}_2 \right) & \text{if } \overline{P}_2 > a - 1, \\
  (0, 0) & \text{otherwise}
\end{cases}
\]

where $P_1^* = a - 1$.

Let the receiver decode the interference first!
How power control benefits the secrecy rate?

Fix $\overrightarrow{P}_1 = 2$ and vary $\overrightarrow{P}_2$ from 0 to 8.

Power control can effectively increase the secrecy rate.

\[ P_1^* = a - 1 = 1 \quad \text{when } a = 2 \]
\[ P_2^* = \sqrt{\frac{1 + (1 + a)\overrightarrow{P}_1 - 1}{1 + a}} = \frac{2}{3} \quad \text{when } a = \frac{1}{2} \]
How the secrecy rate varies with $a$?

Assume $\bar{P}_1 = \bar{P}_2 = 2$ and vary $a$.

1. $a < 1$: the eavesdropper gets more information with the increase of $a$.
2. $a = 1$: the receiver and eavesdropper get the same signal.
3. $1 < a < 1.73$: the receiver can decode and cancel interference; only the eavesdropper is interfered with.
4. $a > 1.73$: interference does not hurt the eavesdropper much when $a$ is large.

**Interference is particularly helpful in the strong interference regime ($a > 1$)**
An Upper bound on the secrecy capacity

- An upper bound assumes that a genie gives the eavesdropper’s signal $\tilde{Y}_2$ to the intended receiver as the side information for decoding.
Assume $\overline{P}_1 = \overline{P}_2 = 2$ and vary $a$

Achievable rate and upper bound

For the symmetric channels $a=b$

The upper bound and the achievable rate are close when $a<1$ (weak interference)

Not good for the case of strong interference
Achievable rate and upper bound

For the general Gaussian channels

Assume $P_1 = P_2 = 2$. Fix $b$ and vary $a$.

Assume $P_1 = P_2 = 2$. Fix $a$ and vary $b$.

The upper bound and the achievable rate are close when $ab \leq 1$.

Need to develop a new upper bound for other cases.
Summary

• Considered the use of interference to alleviate the eavesdropping issues.

• Studied the wiretap channel with a helping interferer.

• Given an achievable secrecy rate, which shows that interference can be exploited to assist secret communication.

• Given an outer bound, which shows the achievable rate is close to the capacity in some cases.
Thank you!