Physical Layer Security for Wireless Networks

Şennur Ulukuş
Department of ECE
University of Maryland
ulukus@umd.edu

Joint work with Shabnam Shafiee, Nan Liu, Ersen Ekrem, Jianwei Xie and Pritam Mukherjee.

LTS, August 22, 2013.
Security in Wireless Systems

- Inherent openness in wireless communications channel: eavesdropping and jamming attacks
Countering Security Threats in Wireless Systems

- **Cryptography**
  - at higher layers of the protocol stack
  - based on the assumption of **limited computational power** at Eve
  - vulnerable to large-scale implementation of quantum computers

- **Techniques like frequency hopping, CDMA**
  - at the physical layer
  - based on the assumption of **limited knowledge** at Eve
  - vulnerable to rogue or captured node events

- **Physical layer security**
  - at the physical layer
  - no assumption on Eve’s computational power
  - no assumption on Eve’s available information
  - **unbreakable, provable, and quantifiable** (in bits/sec/hertz)
  - implementable by signal processing, communications, and coding techniques
Beginnings of Security Research: Shannon 1949

- Noiseless bit pipes to Bob and Eve.

- Eve gets whatever Bob gets.

- **Secure communications is not possible.**
Shannon’s 1949 Security Paper

- Noiseless bit pipes to Bob and Eve.

![Diagram of key exchange]

- **One-time pad:** $X = W \oplus K$
- If $K$ is uniform, then $X$ is independent of $W$. If we know $K$, then $W = X \oplus K$.
- For perfect secrecy, length of $K$ (key rate) must be as large as length of $W$ (message rate).
Beginnings of Cryptography

- **Private key cryptography**
  - Based on one-time pad
  - There are separate secure communication links for key exchange
  - Encryption and decryption are done using these keys

- **Public key cryptography**
  - Encryption is based on publicly known key (or method)
  - Decryption can be performed only by the desired destination
  - Security based on computational advantage
  - **Security against computationally limited adversaries**
  - Certain operations are easy in one direction, difficult in the other direction
    - Multiplication is easy, factoring is difficult (**RSA**)
    - Exponentiation is easy, discrete logarithm is difficult (**Diffie-Hellman**)}
Cryptography versus Physical Layer Security

- **Applications**
  - Secure Message
  - Keys
  - Bits
  - Signals
  - Cryptography

- **Physical Layer**
  - Signals

- **Applications**
  - Secure Bits
  - Signals

- **Physical Layer**
  - Signals

- **Transmitter**
  - Physical Layer Approach
Wyner’s Wiretap Channel

- Wyner introduced the **wiretap** channel in 1975.
- Major departure from Shannon’s model: **noisy channels**.
- Eve’s channel is **degraded** with respect to Bob’s channel: $X \rightarrow Y \rightarrow Z$

![Diagram](attachment:image.png)

- Secrecy is measured by **equivocation**, $R_e$, at Eve, i.e., the **confusion** at Eve:
  \[
  R_e = \lim_{n \to \infty} \frac{1}{n} H(W|Z^n)
  \]
Notions of Perfect Secrecy

• **Perfect secrecy** is achieved if \( R_e = R \)

• This is perfect **weak secrecy**:

\[
\lim_{n \to \infty} \frac{1}{n} I(W; Z^n) = 0
\]

• Also, there is perfect **strong secrecy**:

\[
\lim_{n \to \infty} I(W; Z^n) = 0
\]

• All capacity results obtained for **weak secrecy** have been extended for **strong secrecy**.

• However, there is still no proof of equivalence or strict containment.
Wyner characterized the optimal \((R,R_e)\) region:

\[
R \leq I(X;Y) \\
R_e \leq I(X;Y) - I(X;Z)
\]

Main idea is to split the message \(W\) into two coordinates, secret and public: \((W_s,W_p)\).

\(W_s\) needs to be transmitted in perfect secrecy.

\(W_p\) has two roles:

- Carries some information on which there is no secrecy constraint
- Provides protection for \(W_s\) by creating confusion for the eavesdropper
Wyner characterized the optimal \((R, R_e)\) region:

\[
R \leq I(X;Y) \\
R_e \leq I(X;Y) - I(X;Z)
\]

A typical \((R, R_e)\) region:

There might be a tradeoff between rate and its equivocation:

- Capacity and secrecy capacity might not be simultaneously achievable
A Typical Capacity-Equivocation Region

- Wyner characterized the optimal \( (R, R_e) \) region:

\[
R \leq I(X;Y) \\
R_e \leq I(X;Y) - I(X;Z)
\]

- A typical \( (R, R_e) \) region:

There might be a tradeoff between rate and its equivocation:
- Capacity and secrecy capacity might not be simultaneously achievable
Secrecy Capacity

- Perfect secrecy when $R = R_e$.
- The maximum perfect secrecy rate is the secrecy capacity:

$$C_s = \max_{X \to Y \to Z} I(X;Y) - I(X;Z)$$

- Main idea is to replace $W_p$ with dummy indices, $\tilde{W}_s$, which carry no information.
- In particular, each $W_s$ is mapped to many codewords:
  - Stochastic encoding (a.k.a. random binning)
- To send message $W_s$ securely, we send $X^n(W_s, \tilde{W}_s)$ where $\tilde{W}_s$ is random.
- This one-to-many mapping aims to confuse the eavesdropper.
**Main Tool: Stochastic Encoding**

- Each message $W_s$ is associated with many codewords: $X^n(W_s, \tilde{W}_s)$.

<table>
<thead>
<tr>
<th></th>
<th>$(1, 1)$</th>
<th>$\cdots$</th>
<th>$(1, j)$</th>
<th>$\cdots$</th>
<th>$(1, 2n\tilde{R}_s)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(i, 1)$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$(i, j)$</td>
<td></td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$(2n\tilde{R}_s, 1)$</td>
<td>$\vdots$</td>
<td>$\cdots$</td>
<td>$(2\tilde{R}_s, j)$</td>
<td>$\cdots$</td>
<td>$(2n\tilde{R}_s, 2n\tilde{R}_s)$</td>
</tr>
</tbody>
</table>

Eve’s decoding capability

Stochastic encoding

Message $i$
Stochastic Encoding: 64-QAM Example

Bob’s Noise

Eve’s Noise

Bob’s Constellation

Eve’s Constellation

$C_B = \log_2 64 = 6 \text{ b/s}$

$C_E = \log_2 16 = 4 \text{ b/s}$

$C_s = C_B - C_E = 2 \text{ b/s}$
Stochastic Encoding: 64-QAM Example

Divide Bob’s constellation into 4 subsets.
StochasticEncoding: 64-QAM Example

All red stars denote the same message. Pick one randomly.
Bob can decode the message reliably.
For Eve, all 4 messages look equally likely.
Csiszar and Korner considered the general wiretap channel in 1978.

Eve’s signal is not necessarily a degraded version of Bob’s signal.
General Capacity-Equivocation Region

- General \((R, R_e)\) region:

\[
R \leq I(V; Y)
\]
\[
R_e \leq I(V; Y|U) - I(V; Z|U)
\]

for some \((U, V)\) such that \(U \rightarrow V \rightarrow X \rightarrow Y, Z\).

- Two new ingredients in the achievable scheme
  - \(V\): channel prefixing
  - \(U\): rate splitting
• Contrast with the degraded case

\[ R \leq I(V;Y) \quad R \leq I(X;Y) \]
\[ R_e \leq I(V;Y|U) - I(V;Z|U) \quad R_e \leq I(X;Y) - I(X;Z) \]

for some \((U, V)\) such that \(U \rightarrow V \rightarrow X \rightarrow Y, Z\).

• Two new ingredients in the achievable scheme
  – \(V\): channel prefixing
  – \(U\): rate splitting
General Secrecy Capacity

- Contrast with the degraded case

\[
R \leq I(V;Y) \quad R \leq I(X;Y)
\]

\[
R_e \leq I(V;Y|U) - I(V;Z|U) \quad R_e \leq I(X;Y) - I(X;Z)
\]

for some \((U,V)\) such that \(U \to V \to X \to Y,Z\).

- Two new ingredients in the achievable scheme
  - \(V\): channel prefixing
  - \(U\): rate splitting

- General secrecy capacity expression:

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

i.e., rate splitting is not needed.
Main Tool: Channel Prefixing

- A virtual channel from $V$ to $X$.
- Additional stochastic mapping from the message to the channel input: $W \rightarrow V \rightarrow X$.
- Real channel: $X \rightarrow Y$ and $X \rightarrow Z$. Constructed channel: $V \rightarrow Y$ and $V \rightarrow Z$.

With channel prefixing: $V \rightarrow X \rightarrow Y, Z$.

From DPI, both mutual informations decrease, but the difference may increase.

The secrecy capacity:

$$C_s = \max_{V \rightarrow X \rightarrow YZ} I(V; Y) - I(V; Z)$$
Leung-Yang-Cheong and Hellman considered the Gaussian wire-tap channel in 1978.

\[ Y = X + N_1 \quad \text{and} \quad Z = X + N_2 \]

- **Degraded:** No channel prefixing is necessary and Gaussian signalling is optimal.
- The **secrecy capacity:**

\[ C_s = \max_{X \rightarrow Y \rightarrow Z} I(X;Y) - I(X;Z) = [C_B - C_E]^+ \]

i.e., the difference of two capacities.
Caveat: Need Channel Advantage

The secrecy capacity: \( C_s = [C_B - C_E]^+ \)

Bob’s channel is better

\[
\begin{align*}
W &\xrightarrow{X} Y \xrightarrow{\hat{W}} \text{Bob} \\
&\xrightarrow{\text{Alice}} X \xrightarrow{Z} H(W|Z^n) \xrightarrow{\text{Eve}} \hat{W}
\end{align*}
\]

positive secrecy

\[ C_s = C_B - C_E \]

Eve’s channel is better

\[
\begin{align*}
W &\xrightarrow{X} Y \xrightarrow{\hat{W}} \text{Bob} \\
&\xrightarrow{\text{Alice}} X \xrightarrow{Z} H(W|Z^n) \xrightarrow{\text{Eve}} \hat{W}
\end{align*}
\]

no secrecy

\[ C_s = 0 \]
Two Recurring Themes

- **Creating advantage for the legitimate users:**
  - computational advantage (cryptography)
  - knowledge advantage (spread spectrum)
  - channel advantage (physical layer security)

- **Exhausting capabilities of the illegitimate entities:**
  - exhausting computational power (cryptography)
  - exhausting searching power (spread spectrum)
  - exhausting decoding capability (physical layer security)
Outlook at the End of 1970s and Transition into 2000s

• Information theoretic secrecy is extremely powerful:
  – no limitation on Eve’s computational power
  – no limitation on Eve’s available information
  – yet, we are able to provide secrecy to the legitimate user
  – unbreakable, provable, and quantifiable (in bits/sec/hertz) secrecy

• We seem to be at the mercy of the nature:
  – if Bob’s channel is stronger, positive perfect secrecy rate
  – if Eve’s channel is stronger, no secrecy

• We need channel advantage. Can we create channel advantage?

• Wireless channel provides many options:
  – time, frequency, multi-user diversity via fading
  – cooperation via overheard signals
  – multi-dimensional signalling via multiple antennas
  – signal alignment
In the Gaussian wiretap channel, secrecy is not possible if

\[ C_B \leq C_E \]

Fading provides time-diversity: Can it be used to obtain/improve secrecy?
In SISO Gaussian wiretap channel, secrecy is not possible if
\[ C_B \leq C_E \]

Multiple antennas improve reliability and rates. How about secrecy?
Broadcast (Downlink) Channel

- In cellular communications: base station to end-users channel can be eavesdropped.
- This channel can be modelled as a broadcast channel with an external eavesdropper.
Internal Security within a System

- Legitimate users may have **different security clearances**.
- Some legitimate users may have **paid for some content**, some may not have.
- Broadcast channel with two confidential messages.
- Alice and Charles want to have secure communication with Bob in the presence of Eve.
- Simultaneous multi-message secrecy. Opportunities for deaf cooperation.
Interference Channel with Confidential Messages

- Interference results in performance degradation, requires sophisticated transceiver design.
- From a secrecy point of view, interference (overheard signal) results in loss of confidentiality.
Cooperative Channels

- **Overheard information** at communicating parties:
  - Forms the basis for cooperation; results in loss of confidentiality
- How do cooperation and secrecy interact?
- Can Charles help without learning the messages going to Bob?
Both users want secrecy against each other.

In a non-fading setting, only one user can have a positive secure rate.

With full CSIT and CSIR: Gaussian signalling with power control is optimal.

Ekrem et. al., Ergodic Secrecy Capacity Region of the Fading Broadcast Channel, ICC 2009.
• (Squared) channel gains are exponential random variables with means $\sigma_1, \sigma_2$, respectively.

• Fading (channel variation over time) is beneficial for secrecy.

• Both users can have positive secrecy rates in fading (even if they have the same average quality). **This is not possible without fading.**
Fading Wiretap Channel without CSI

- Fast fading channel: no CSI anywhere.
- Discrete signalling is optimal.

Mukherjee et. al., Fading Wiretap Channel with No CSI Anywhere, ISIT 2013.
• Multiple antennas improve reliability and rates. They improve secrecy as well.

\[
W \xrightarrow{X} Y \xrightarrow{Z} \hat{W} \text{ | } \mathbf{H} \text{ } \mathbf{W} \text{ } \mathbf{Z}.
\]

\[\cdot\]

Bob

Alice

\[Eve\]

Bob

Alice

\[Eve\]

\[H(W \mid Z^e)\]

• No channel prefixing is necessary and Gaussian signalling is optimal. The secrecy capacity:

\[
C_s = \max_{\mathbf{K}: \text{tr}(\mathbf{K}) \leq P} \frac{1}{2} \log |\mathbf{H}_M \mathbf{K} \mathbf{H}_M^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_E \mathbf{K} \mathbf{H}_E^\top + \mathbf{I}|
\]

• As opposed to the SISO case, \( C_S \neq C_B - C_E \). Tradeoff between the rate and its equivocation.

Cooperative Channels and Secrecy

- How do cooperation and secrecy interact?
- Is there a trade-off or a synergy?

Interactions of Cooperation and Secrecy

- Existing cooperation strategies:
  - Decode-and-forward (DAF)
  - Compress-and-forward (CAF)

- Decode-and-forward:
  - Relay decodes (learns) the message.
  - No secrecy is possible.

- Compress-and-forward:
  - Relay does not need to decode the message.
  - Can it be useful for secrecy?

- Achievable secrecy rate when relay uses CAF:

\[
I(X_1; Y_1, \hat{Y}_1 | X_2) - I(X_1; Y_2 | X_2) = I(X_1; Y_1 | X_2) - I(X_1; Y_2 | X_2) + I(X_1; \hat{Y}_1 | X_2, Y_1) \\
\]

- Secrecy rate of the wiretap channel
- Additional term due to CAF
Bob cannot have any positive secrecy rate without cooperation.

Cooperation is beneficial for secrecy if CAF based relaying (cooperation) is employed.

Charles can further improve his own secrecy by joint relaying and jamming.
Secure Degrees of Freedom: Motivation

- For most multi-user wiretap channels, secrecy capacity is unknown.
- Partial characterization in the high power, $P$, regime.
- Secure degrees of freedom (d.o.f.) is defined as:

$$D_s \triangleq \lim_{P \to \infty} \frac{C_s}{\frac{1}{2} \log P}$$

- Rest of this talk:
  - Secrecy penalty paid in d.o.f
  - Role of a helper for security
  - D.o.f. optimal deaf cooperation
  - Secure d.o.f. of some multi-user channels
• Canonical Gaussian wiretap channel with power $P$,

$$C_s = \frac{1}{2} \log (1 + h^2 P) - \frac{1}{2} \log (1 + g^2 P)$$

• In this case, $C_s$ does not scale with $\log P$, and $D_s = 0$.

• Severe penalty for secrecy. D.o.f. goes from 1 to 0 due to secrecy.
Cooperative Jamming

- Cooperative jamming from helpers improves secure rates [Tekin, Yener, 2008].

- Secure d.o.f. with i.i.d. Gaussian cooperative jamming is still zero.

- Positive secure d.o.f. by using nested lattice codes [He, Yener, 2009].

- **Question**: What is the exact secure d.o.f.?
Gaussian Wiretap Channel with $M$ Helpers

- The exact secure d.o.f. with $M$ helpers is $\frac{M}{M+1}$.
- Even though they are independent, more helpers is better.

Tools: Real interference alignment and structured coding.

Secure Signal Alignment with $M$ Helpers

- Alignment for the $M = 2$ case:

  + The transmitter sends $M$ independent sub-messages.
  + $M$ helpers send an independent cooperative jamming signal each.
  + Each cooperative jamming signal is aligned with one sub-message at the eavesdropper.
  + All cooperative jamming signals are aligned together at the legitimate receiver.
The previous achievable scheme required **perfect knowledge** of eavesdropper CSI.

- Generally, it is **difficult or impossible** to obtain the eavesdropper’s CSI.

- **Question**: What is the **exact** secure d.o.f. **without** eavesdropper CSI?

- The **exact secure d.o.f. is still** $\frac{M}{M+1}$.  

Secure Signal Alignment with $M$ Helpers without Eavesdropper CSI

- Alignment for $M = 2$ helpers without eavesdropper CSI:

- The transmitter sends $M$ independent sub-messages and also a cooperative jamming signal.
- $M$ helpers send an independent cooperative jamming signal each.
- All $M + 1$ cooperative jamming signals are blue aligned together at the legitimate receiver.
- All cooperative jamming signals span the entire space at the eavesdropper.
Each user has its own message to be kept secret from the external eavesdropper.

The exact sum secure d.o.f. is \( \frac{K(K-1)}{K(K-1)+1} \).

Secure Signal Alignment for the Multiple Access Channel

- Alignment for the $K = 3$ case:

- Each transmitter divides its own message into $K - 1$ sub-messages.
- The total $K$ jamming signals from the $K$ users span the whole space at the eavesdropper.
- The jamming signals are aligned in the same dimension at the legitimate receiver.
Secure Signal Alignment for the Multiple Access Channel

- Alignment for the $K = 3$ case:

  Each transmitter divides its own message into $K - 1$ sub-messages.

  The total $K$ jamming signals from the $K$ users span the whole space at the eavesdropper.

  The jamming signals are aligned in the same dimension at the legitimate receiver.
Interference Channel with an External Eavesdropper

- External eavesdropper model (IC-EE).

- Secure all messages against the external eavesdropper.
Interference Channel with Confidential Messages

- Confidential message model (IC-CM).

- Secure all messages against all unintended receivers.
Unified Model: Internal and External Security

- Interference channel with confidential messages and one external eavesdropper (IC-CM-EE):

- Secure all messages against the internal unintended receivers and the external eavesdropper.
Secure Signal Alignment for the Unified $K$-User IC-CM-EE

- The exact sum secure dof is $\frac{K(K-1)}{2K-1}$.
- Added challenge: simultaneous alignment at multiple receivers.

Going Back to where We have Started

- **Cryptography**
  - at higher layers of the protocol stack
  - based on the assumption of **limited computational power** at Eve
  - vulnerable to large-scale implementation of quantum computers

- **Techniques like frequency hopping, CDMA**
  - at the physical layer
  - based on the assumption of **limited knowledge** at Eve
  - vulnerable to rogue or captured node events

- **Physical layer security**
  - at the physical layer
  - no assumption on Eve’s computational power
  - no assumption on Eve’s available information
  - **unbreakable, provable, and quantifiable** (in bits/sec/hertz)
  - implementable by **signal processing, communications, and coding** techniques
• Cryptography
  – at higher layers of the protocol stack
  – based on the assumption of **limited computational power** at Eve
  – vulnerable to large-scale implementation of quantum computers

• Techniques like frequency hopping, CDMA
  – at the physical layer
  – based on the assumption of **limited knowledge** at Eve
  – vulnerable to rogue or captured node events

• Physical layer security
  – at the physical layer
  – no assumption on Eve’s computational power
  – no assumption on Eve’s available information
  – **unbreakable, provable, and quantifiable** (in bits/sec/hertz)
  – implementable by **signal processing, communications, and coding** techniques
Going Back to where We have Started

• **Cryptography**
  – at higher layers of the protocol stack
  – based on the assumption of **limited computational power** at Eve
  – vulnerable to large-scale implementation of quantum computers

• **Techniques like frequency hopping, CDMA**
  – at the physical layer
  – based on the assumption of **limited knowledge** at Eve
  – vulnerable to rogue or captured node events

• **Physical layer security**
  – at the physical layer
  – no assumption on Eve’s computational power
  – no assumption on Eve’s available information
  – based on the assumption of **limited ???????** at Eve
  – **unbreakable, provable, and quantifiable** (in bits/sec/hertz)
  – implementable by **signal processing, communications, and coding** techniques
Two Recurring Themes

- **Creating advantage for the legitimate users:**
  - computational advantage (cryptography)
  - knowledge advantage (spread spectrum)
  - channel advantage (physical layer security)

- **Exhausting capabilities of the illegitimate entities:**
  - exhausting computational power (cryptography)
  - exhausting searching power (spread spectrum)
  - exhausting decoding capability (physical layer security)
Three Dimensions of Advantage

- Three known dimensions of advantage: knowledge, computational, channel advantage.

- Each method uses only one possible dimension of advantage.
Hybrid Schemes

- Hybrid schemes: move to another dimension when an advantage is lost.

- Still a single dimension is used.
Hybrid Schemes

- Hybrid schemes: move to another dimension when an advantage is lost.

- Still a single dimension is used.
Combined Schemes

- Combine and utilize multiple dimensions of advantage

- Multi-dimensional, multi-faceted, cross-layer security.
Conclusions

- Wireless communication is susceptible to eavesdropping and jamming attacks.

- Wireless medium also offers ways to neutralize the loss of confidentiality:
  - time, frequency, multi-user diversity via fading
  - cooperation via overheard signals
  - multi-dimensional signalling via multiple antennas
  - secure signal alignment

- Information theory directs us to methods that can be used to achieve:
  - unbreakable, provable, and quantifiable (in bits/sec/hertz) security
  - irrespective of the adversary’s computation power or inside knowledge

- Resulting schemes implementable by signal processing, communications and coding tech.

- Many open problems...