Information Theoretic Paths Forward in the Wireless Physical Layer

H. Vincent Poor
(poor@princeton.edu)

Thanks to the U.S. NSF under Grants CNS-1702808 and ECCS-1647198.
Outline of Today’s Talk

- **State of the Art and Emerging Challenges in the Wireless PHY**
  - Key Enablers of the State of the Art: 4G
  - Challenges for the Emerging Generation: 5G & Beyond
  - Open Problems & Potential Solutions

- **Two Fundamental Approaches**
  - Physical Layer Security
  - Finite-Blocklength Fundamentals
State of the Art and Emerging Challenges in the Wireless PHY
Wireless Networks: Layers

Application (APP)

Web Browsing, Voice, etc.

Network (NET)

Routing, Flow Control, etc.

Medium Access Control (MAC)

Scheduling, Access Control, etc.

Physical (PHY)

Data Transmission
Key Enablers of the State-of-the-Art

- **Exploiting spatial diversity:**
  - MIMO, cooperation & relaying

- **Exploiting frequency diversity:**
  - OFDMA

- **Approaching the Shannon limit:**
  - Iterative decoding (Turbo, LDPC)
Challenges for the Emerging Generation

• **Always** capacity, reliability, and now, **energy efficiency**

• In the **emerging generation**, supporting:
  
  – **Internet of Things (IoT):**
    
    • 100’s of billions of terminals, densification, low complexity
  
  – **Autonomy & telecontrol:**
    
    • low latency and very high reliability
  
  – **Immersive experiences:**
    
    • very high bandwidth streaming
Open Problems & Potential Solutions

• **Densification & interference management:**
  - C-RAN, massive MIMO, mmWave, energy harvesting

• **Capacity enhancement:**
  - Full duplex, NOMA, caching

• **Security in IoT:**
  - Physical layer security

• **Short packet transmission:**
  - Finite-blocklength fundamentals
Physical Layer Security
The PHY: From Foe to Friend

- **Key Techniques for Improving Capacity & Reliability:**
  - MIMO (Multiple-Antenna Systems)
  - Cooperation & Relaying
  - Cognitive Radio
The PHY: From Foe to Friend

- **Key Techniques for Improving Capacity & Reliability:**
  - MIMO (Multiple-Antenna Systems)
  - Cooperation & Relaying
  - Cognitive Radio

- **What About Security?**
  - Traditionally a higher-layer issue (e.g., APP)
  - Encryption can be complex and difficult without infrastructure
  - Information theoretic security examines the fundamental ability of the PHY to provide security (primarily secrecy – i.e., data confidentiality)
Shannon [1949]: For cipher, perfect secrecy requires a one-time pad.

[I.e., the entropy of the key must be at least the entropy of the source: $H(K) \geq H(M)$]
Information Theoretic Secrecy: Wyner’s Model

“The Wiretap Channel”

- Tradeoff: reliable rate $R$ to Bob vs. the “equivocation” $H(M|Z)$ at Eve
- Secrecy capacity = maximum $R$ such that $R = H(M|Z)$
- Wyner [1975]: Secrecy capacity $> 0$ iff. $Z$ is degraded relative to $Y$
Physical Layer Security in Wireless Networks

- There has been a resurgence of interest in these ideas, as standard encryption is impractical for emerging wireless networking paradigms.
Physical Layer Security in Wireless Networks

- There has been a resurgence of interest in these ideas, as standard encryption is impractical for emerging wireless networking paradigms.

- In general, the legitimate receiver needs an advantage over the eavesdropper — either a secret shared with the transmitter, or a better channel.
Physical Layer Security in Wireless Networks

• There has been a resurgence of interest in these ideas, as standard encryption is impractical for emerging wireless networking paradigms.

  • In general, the legitimate receiver needs an advantage over the eavesdropper – either a secret shared with the transmitter, or a better channel.

• The physical properties of radio propagation (diffusion & superposition) provide opportunities for this, via
  
  – fading: provides natural degradedness over time
  – interference: allows active countermeasures to eavesdropping
  – spatial diversity (MIMO, relays): creates “secrecy degrees of freedom”
  – random channels: sources of common randomness for key generation

Secrecy in Fundamental Channel Models

- **Broadcast Channels:**

- **Multiple-Access Channels:**

- **Interference Channels:**

- **Relay Channels:** Relay cooperates to improve security; or relay is untrusted.

- **MIMO Channels:** Allows simultaneous secure transmission without rate penalty.
Key Generation from Common Randomness

• **Passive Eavesdropper:**
  – Public discussion (Ahlswede & Cziszár [1993], Mauer [1993])
  – Channel reciprocity: joint source-channel model
  – Relay assisted: trusted or oblivious

• **Active Eavesdropper:**
  – Channel reciprocity: joint source-channel model

A Rich Area

Physical Layer Security

- Coding Theory
  - code design
- Cryptography
  - key generation & management
- Networking
  - cross-layer design
- Game Theory
  - adversarial model
Augmentation of Traditional Encryption
Broadcast with Secret Keys

Augmentation of Traditional Encryption

Example: AWGN Channel

Augmentation of Traditional Encryption

Example: AWGN Channel

Augmentation of Traditional Encryption

Example: AWGN Channel

PHY Security in Massive MIMO Systems

[PHYSecurity.png]

Finite-Blocklength Fundamentals
A Fundamental Problem

- **(n,M,ε) code**: $P(W \neq \hat{W}) \leq \varepsilon$
- **Fundamental limit**: $M^*(n,\varepsilon) = \max\{M: \exists \text{ an (n,M,ε) code}\}$
- **Shannon**: As $n \to \infty$, $\varepsilon \to 0$
  \[
  \frac{\log M^*(n,\varepsilon)}{n} \to C \quad \text{(capacity)}
  \]
- In many situations (e.g., short packets) $n$ and $\varepsilon$ are noticeably finite.
Finite $n$ and $\varepsilon$

• Bounds:
  • Shannon-Feinstein (1954/57); Gallager (1965)
  • Random coding union; dependence testing

• Approximation:
  • Strassen (1962) – discrete memoryless channels
  • New bounds yield – sharper for DMCs; Gaussian; fading

\[
\log M^*(n,\varepsilon) = n C - \sqrt{nV} Q^{-1}(\varepsilon) + O(\log n)
\]

\[V = \text{Var}[i(X^*,Y*)] \quad ("\text{dispersion}\")\]

Example: **AWGN** \((\text{SNR} = 0 \text{ dB}; \; \varepsilon = 10^{-3})\)
Applications

Analysis of Codes
(normalized to the approx.; $\varepsilon = 10^{-4}$)

ARQ: Optimal $\varepsilon$ vs. $n$
(AWGN; SNR = 0 dB)
Short-Packet Energy/Spectral-Efficiency Tradeoff

[Shannon limit]

\[ \varepsilon = 0.1 \]

\[ \varepsilon = 0.01 \]

\[ \varepsilon = 0.001 \]

\[ \varepsilon = 0.0001 \]

Short-Packet Security
Semi-deterministic Wiretap Channel

Short-Packet Security
Gaussian Wiretap Channel

$C_S \equiv 0.5$

[Secrecy rate, bit/(ch. use)]

[Converse Approximation]
[Hayashi et al.]
[Achievability]
[Watanabe-Hayashi]

Blocklength, $n$

Summary

• **State of the Art and Emerging Challenges in the Wireless PHY**
  
  – **Key Enablers of 4G**: spatial diversity, OFDMA, iterative decoding, etc.
  
  – **Challenges for 5G & Beyond**: densification, low latency/high reliability, high data bandwidths, etc.
  
  – **Potential Solutions**: C-RAN, massive MIMO, mmWave, energy harvesting, full duplex, NOMA, caching, etc.

• **Two Fundamental Approaches**
  
  – **Physical Layer Security** (e.g., the Internet of Things)
  
  – **Finite-Blocklength Fundamentals** (e.g., optimal short-packet transmission)
Thank You!