Making Physical Inferences to Enhance Wireless Security

PI: Yingying Chen†, Co-PI: Jie Yang‡
†Stevens Institute of Technology, ‡ Oakland University

This project aims to utilize physical layer information to enhance wireless security. In particular, the fine-grained channel state information is exploited to make secret key generation faster and more practical in wireless networks.

Motivation

- Securing wireless communication remains challenging
  - Overhead in key distribution and management
  - High dynamics of mobile devices
  - The key establishment vulnerable to eavesdropping
- Secret key generation using physical layer information is promising
  - Without requiring a fixed key management infrastructure
  - Utilize temporal and spatial variation of radio channel
  - Existing RSS based method only use coarse-grained channel information, with low key generation rate

Objective

- Exploit fine-grained physical layer information for secret key generation
  - Multiple subcarriers of OFDM provide detailed Channel State Information (CSI)
  - Resilient to malicious attacks
- Improve secret key generation rate while reducing bit mismatch rate
  - Fine-grained CSI can provide fast secret key generation rate
  - Mitigate the non-reciprocity component embedded in the CSI to reduce the bit mismatch rate

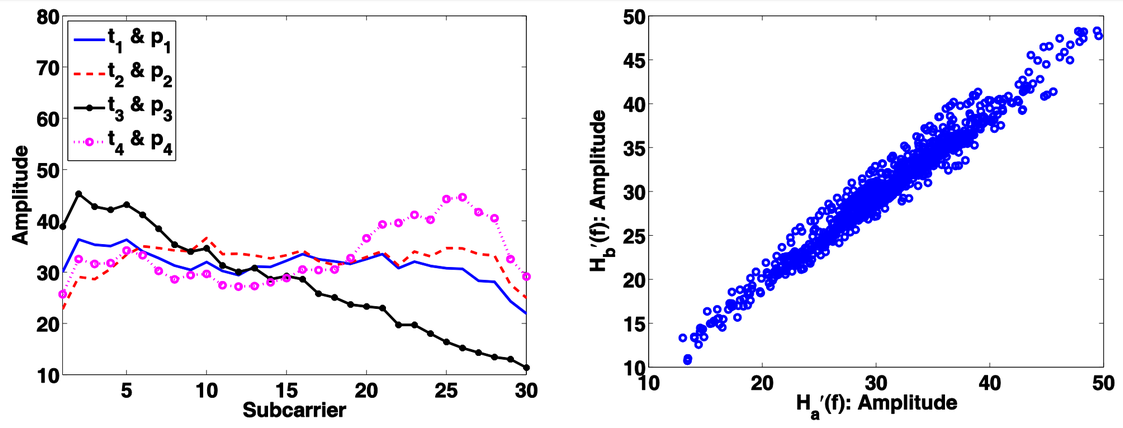
Challenges

- Reciprocity of CSI cannot be assumed due to different electrical characteristics in practice
- Traditional RSS based methods are vulnerable to some active attacks, such as predictable channel attack and stalking attack

Attack Model

- Predictable channel attack
  - Adversary uses planned movements to cause desired and predictable changes in the channel measurements
- Stalking attack
  - Adversary/stalker follows the trajectory of either party during the key establishment and eavesdrops legitimate communication

Feasibility



(a) amplitude of channel response across 30 subcarriers of OFDM (b) Illustration of channel reciprocity

Fig. 1. Channel randomness and reciprocity

- Channel response with multiple subcarriers of OFDM provides more randomness
- CSI of the same channel observed by two parties should be highly correlated (within coherence time)

Channel Gain Complement (CGC) Assisted Secret Key Extraction

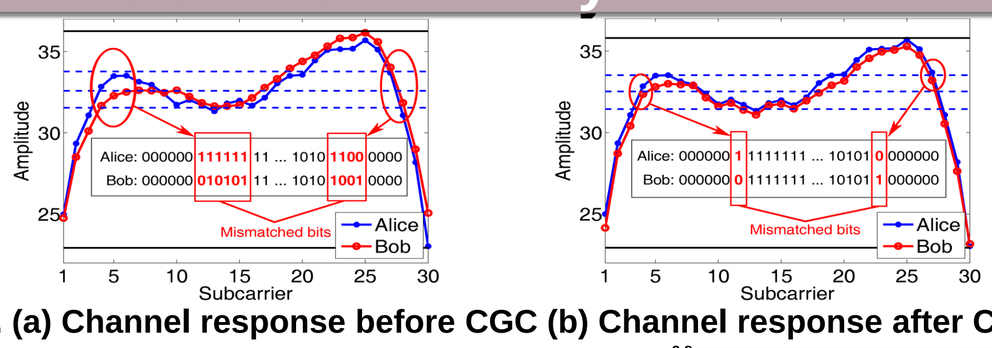


Fig. 2. (a) Channel response before CGC (b) Channel response after CGC

- Non-reciprocity learning
  - Averaging a number of the difference of CSI between Alice and Bob over time
- Channel gain complement
  - Subtract the learned non-reciprocity component from the CSI of Alice or Bob
- Quantization
  - Quantize the amplitude of CSI across different subcarriers

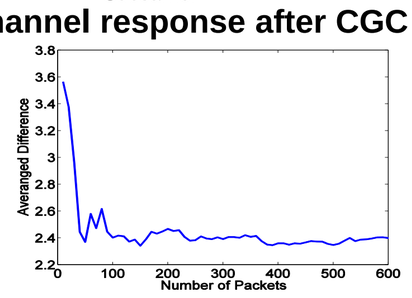


Fig. 3. Averaged differences along the time

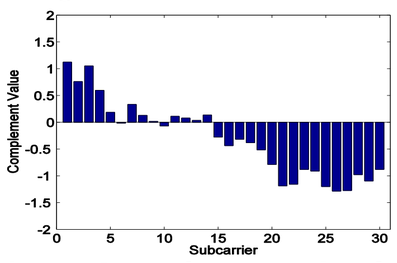
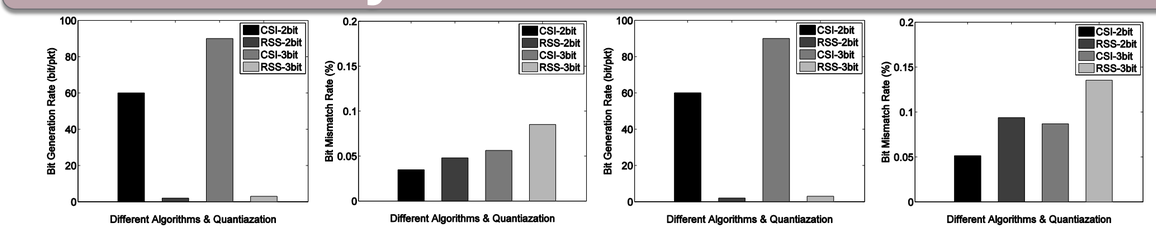


Fig. 4. Complemented value across 30 subcarriers

Experimental Setup

- Two laptops equipped with Intel WiFi Link 5300 wireless card extract CSI for 30 subcarrier groups
- Mobile and static scenarios in both indoor and out door environments
- Multiple bits quantization and MIMO

Preliminary Results and Future Work



(a) Indoor BGR (b) Indoor BMR (c) Outdoor BGR (d) Outdoor BMR

Fig. 5. Indoor and outdoor performance evaluation

- Bit generation rate (BGR) and bit mismatch rate (BMR) both out-perform the RSS based method
- MIMO can significantly improve the performance
- **More aspects**
  - Develop new learning based method to accurately capture channel non-reciprocity in reality
  - Utilize amplitude and phase information of CSI to model radio channel

2012 Science of Security Community Meeting
Nov. 29-30, 2012
National Harbor, MD
http://cps-vo.org/group/sosmtg

Vote Here

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

Oakland UNIVERSITY