WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

Fingerprints in the Ether: Physical Layer Authentication

Liang Xiao

Advisors: Prof. L. Greenstein, Prof. N. Mandayam and Prof. W. Trappe

IAB 2007

WIRELESS INFORMATION NETWORK LABORATORY

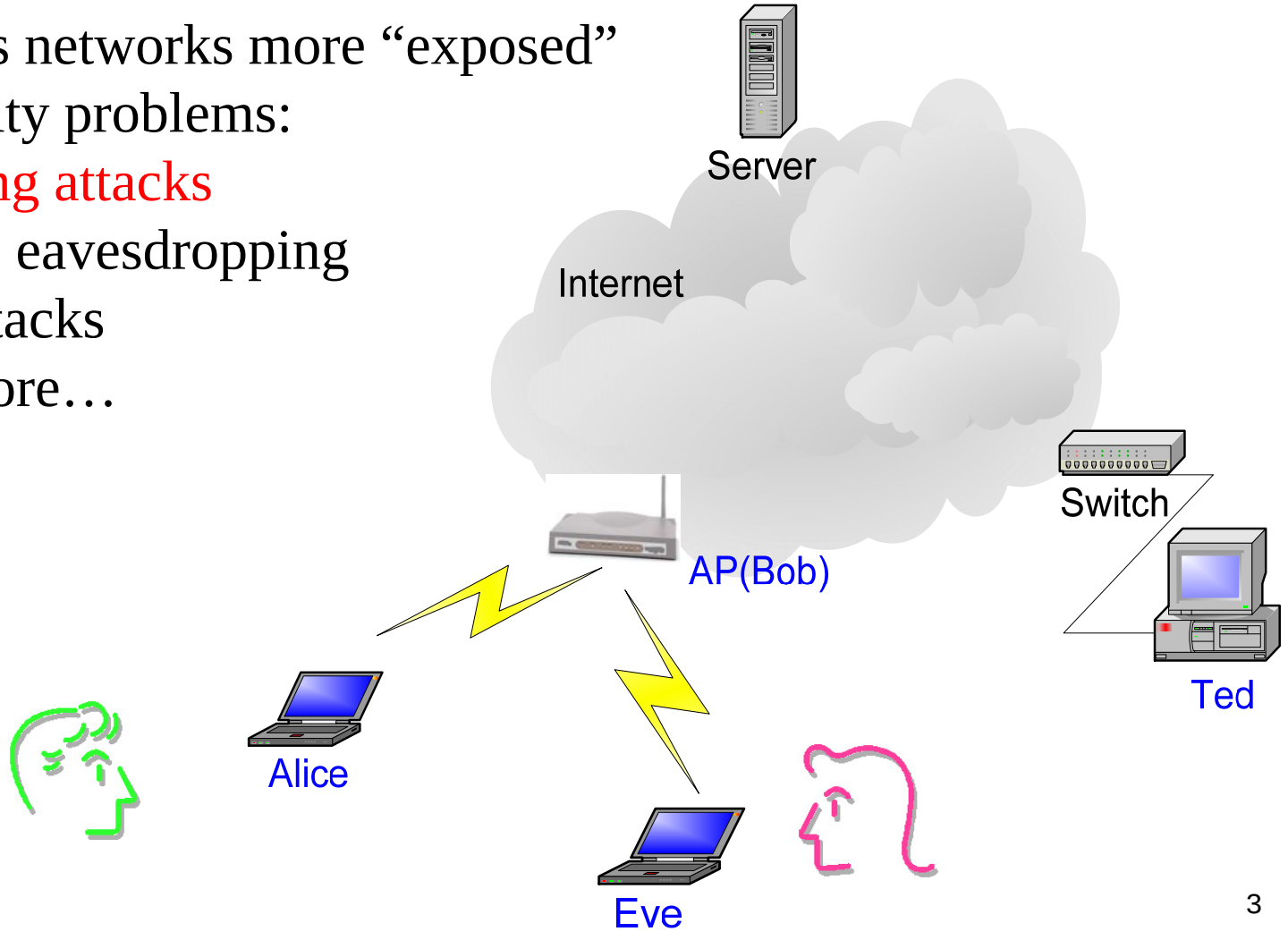
Outline

- Motivation & Main Idea
- System Model & Hypothesis Test
- Simulation & Results
  - Time-Invariant Channel with Receiver Thermal Noise
  - Time-Variant Channel with Background Changes
- Conclusion & Future Work

Motivation

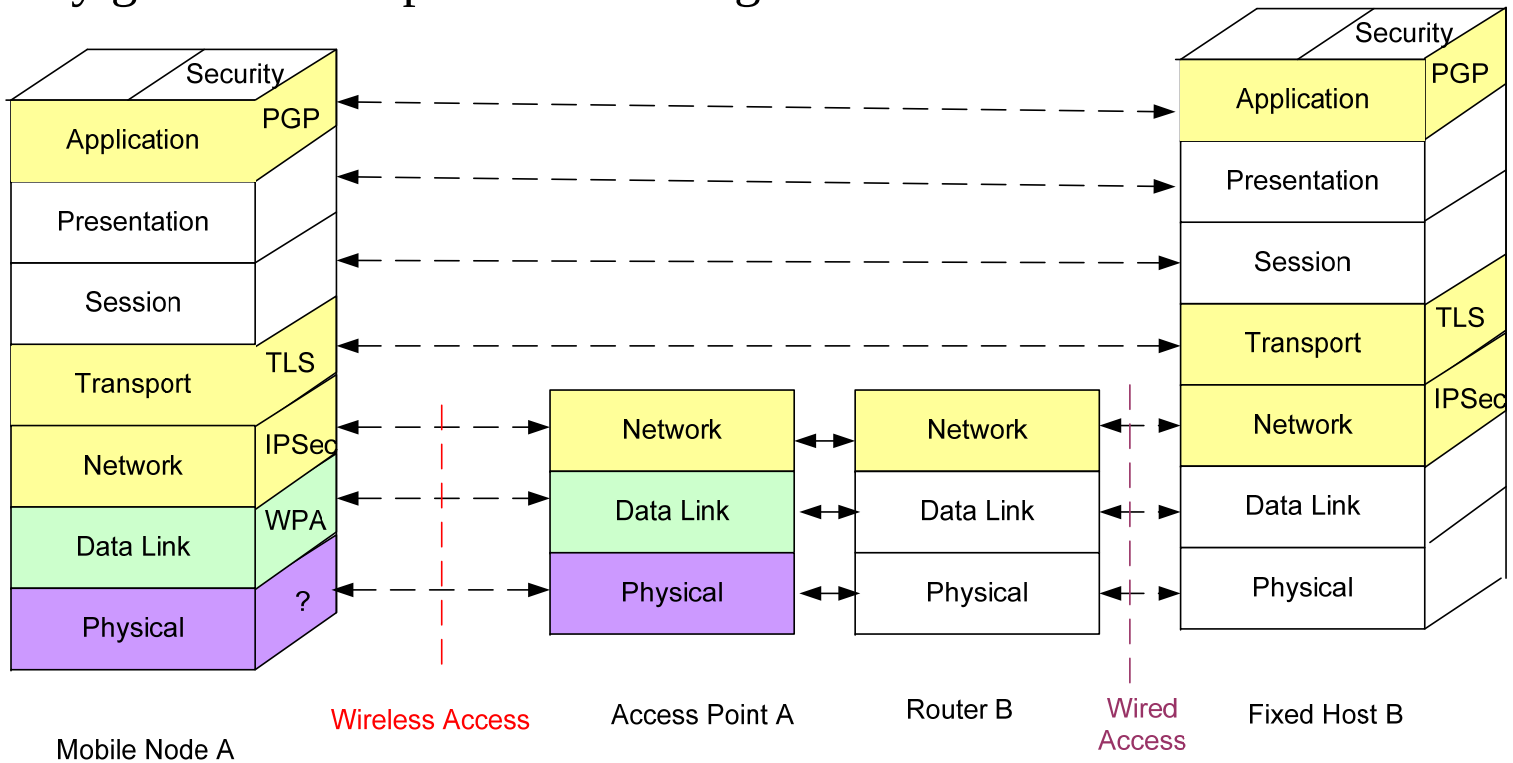
Wireless networks more “exposed” to security problems:

- Spoofing attacks
- Passive eavesdropping
- DoS attacks
- And more…



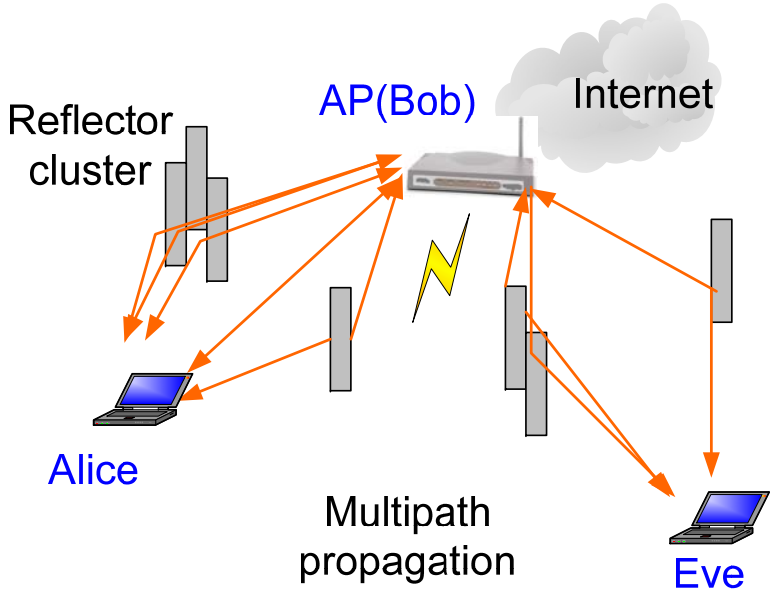
Security Protocols

Q1: Can we use the physical layer information to enhance security?
A1: Yes, as we will see
Q2: What is the value added?
A2: My graduation depends on finding out …



Main Idea: Fingerprints in the Ether

- **"Fingerprints"**: Distinguishes channel responses of different paths to enhance authentication

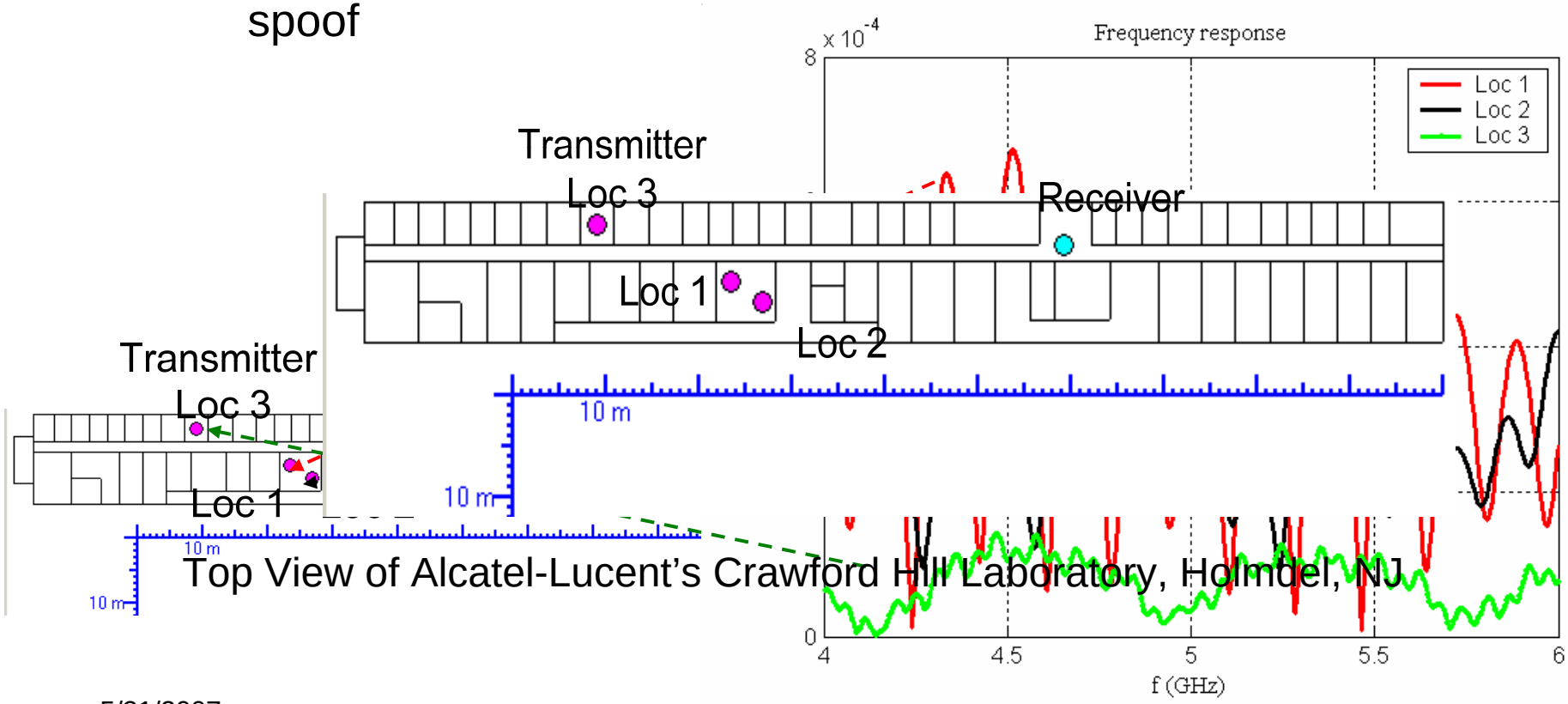


- **Other examples that benefit from multipath fading:**
  - **CDMA**: Rake processing that transforms multipath into a diversity-enhancing benefit
  - **MIMO**: Transforms scatter-induced Rayleigh fading into a capacity-enhancing benefit

Fingerprints in the Ether (Cont.)

The channel frequency response in the indoor environments

- Frequency selective with spatial variability
- Rapidly decorrelates with distance: hard to predict and to spoof

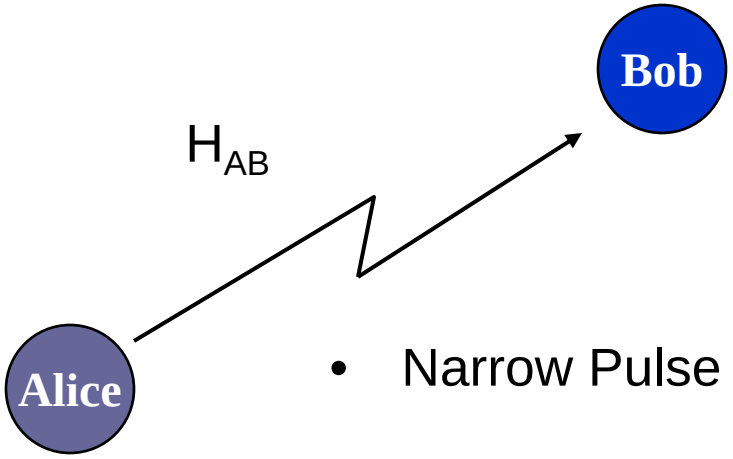


Top View of Alcatel-Lucent's Crawford Hill Laboratory, Holmdel, NJ

PHY-Authentication Scenario

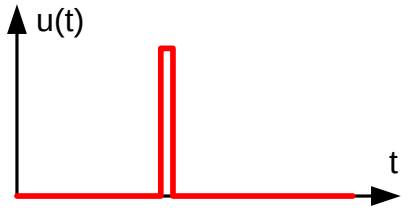
TIME: 0

Bob estimates channel response H_{AB} from Alice at time 0

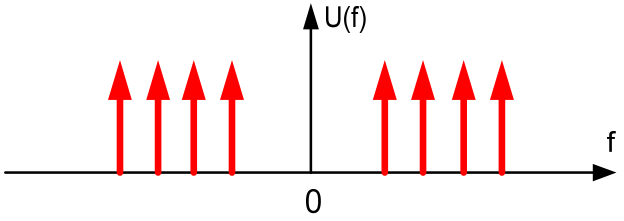


Probe Signal u(.)

- Narrow Pulse



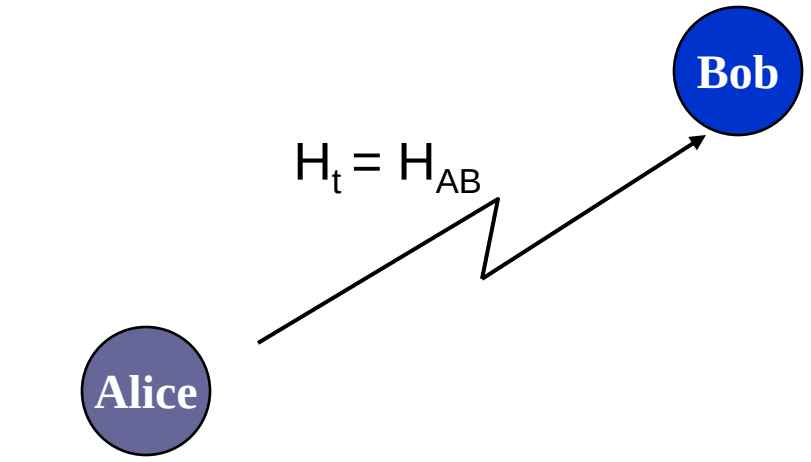
- Pilot Tones



PHY-Authentication Scenario (Cont.)

TIME: t

Case 1: Alice is still transmitting.



Bob estimates H_t at time t, and compares with H_{AB}

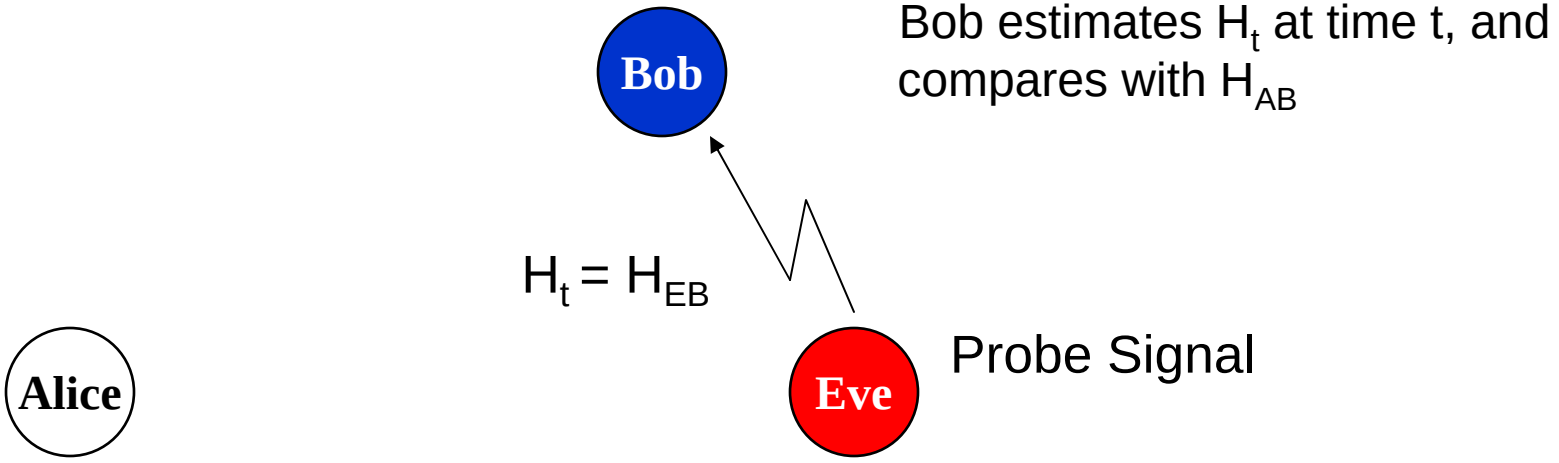
Probe Signal

Desired result: Bob accepts the transmission.

PHY-Authentication Scenario (Cont.)

TIME: t

Case 2: Eve is transmitting, pretending to be Alice.



Desired result: Bob rejects the transmission.

PHY-Authentication Via Hypothesis Test

- Sample frequency response at M frequencies
- Two complex frequency response vectors

$$\underline{\hat{H}}_{AB} = [\hat{H}_{AB}(0, f_1), \hat{H}_{AB}(0, f_2), ..., \hat{H}_{AB}(0, f_M)]^T$$

$$\underline{\hat{H}}_{t} = [\hat{H}_{?}(t, f_1), \hat{H}_{?}(t, f_2), ..., \hat{H}_{?}(t, f_M)]^T$$

- Simple Hypothesis:

$$\mathcal{H}_0: \ \underline{H}_t = \underline{H}_{AB}$$

$$\mathcal{H}_1: \ \underline{H}_t \neq \underline{H}_{AB}$$

- Test Statistic: $Z = \min_{\theta} \frac{1}{\sigma^2} \| \underline{\hat{H}}_A - \underline{\hat{H}}_t e^{j\theta} \|^2$
  - Phase measurement error due to changes of receiver local oscillator
- Channel measurement assumed to be noisy

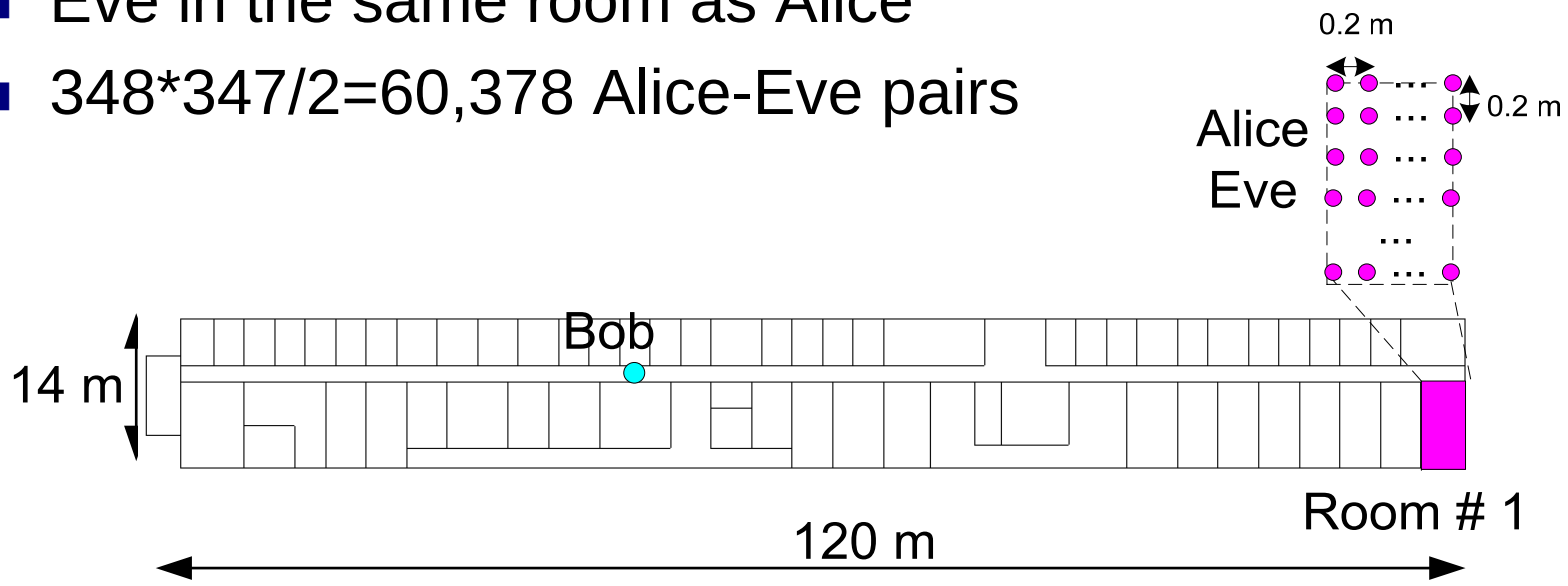
Hypothesis Test (Cont.)

- Rejection region of $\mathcal{H}_0$: $Z > \Gamma$
- Detection Metrics
  - False Alarm Rate, $\alpha = P_{H_0}(Z > \Gamma)$
  - Miss Rate, $\beta = P_{H_1}(Z \leq \Gamma)$
- Threshold Γ is chosen to satisfy

$$P_{H_0}(Z > \Gamma) = \alpha$$

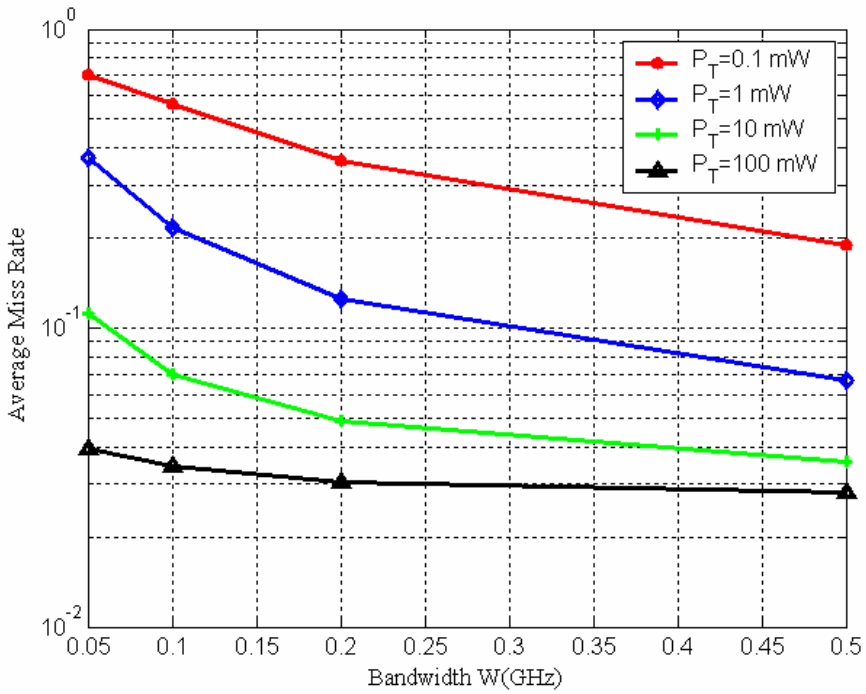
Simulation

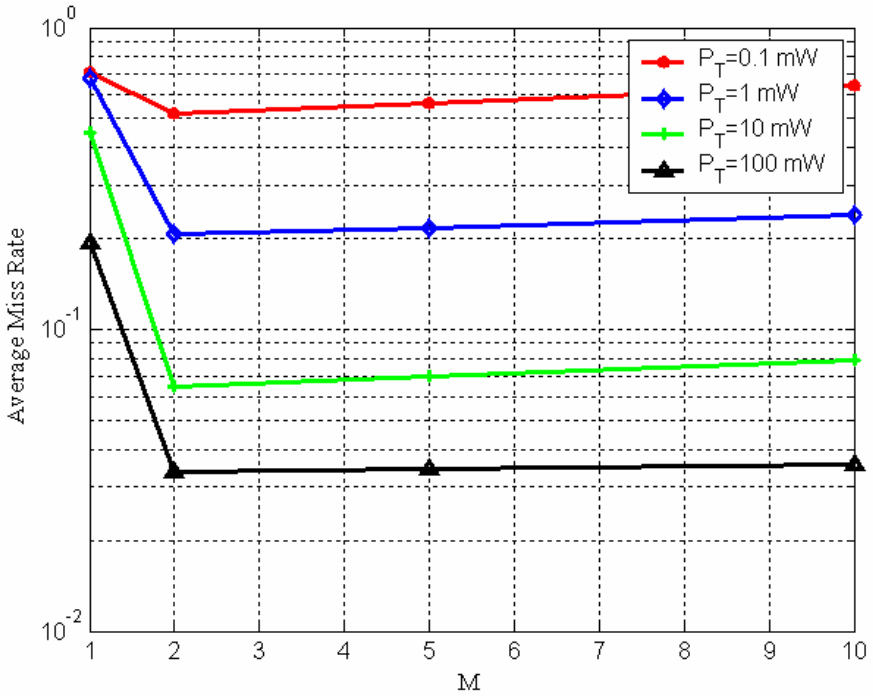
- Use ray-tracing tool WiSE (Wireless System Engineering) to generate channel responses for specified real environments
- Eve in the same room as Alice
- 348*347/2=60,378 Alice-Eve pairs



Case 1: Time-Invariant Channel

Average miss rate β, for required false alarm rate $\alpha = 0.01$

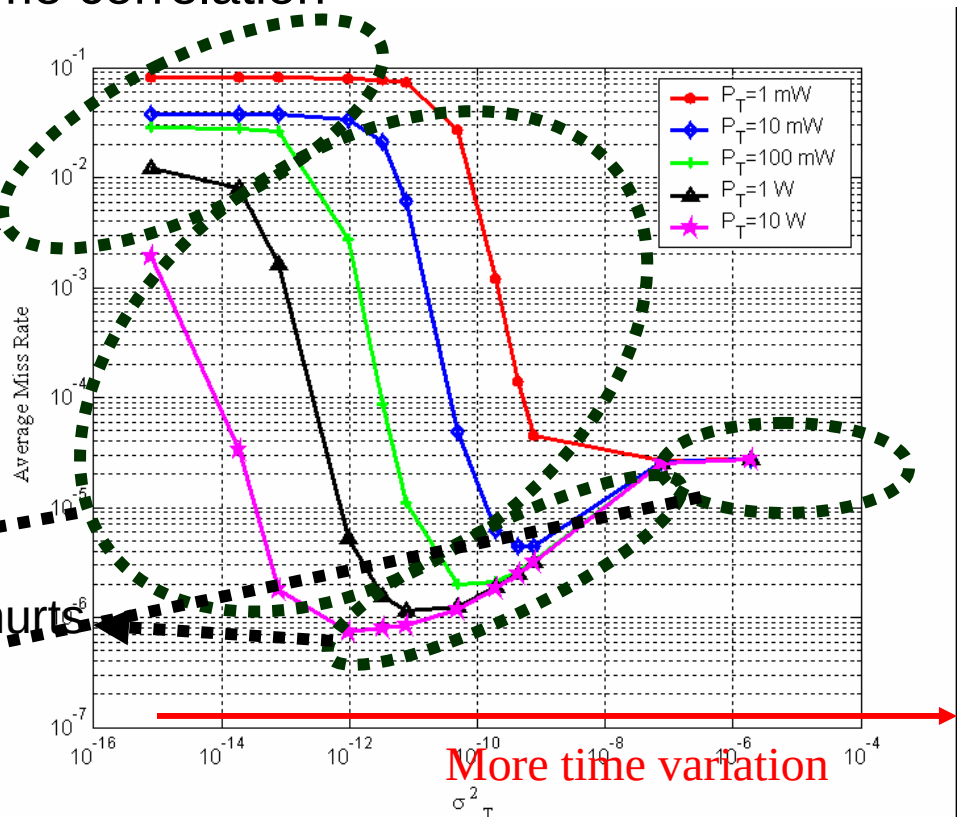




Sample Size (M)=5 *Room # 1* *Bandwidth (W)* = 100 MHz

Case 2: Time-Variant Channel

- Channel response $H_{AB}(t, f) = \bar{H}_{AB}(f) + \varepsilon_{AB}(t, f)$
  - Tap-delay model for the inverse Fourier transform of $\varepsilon_{AB}(t, f)$
  - Single-sided exponential model as power delay profile
  - AR-1 Model for the time correlation
- W=10 MHz, M=10



Time variation is negligible
Time variation helps
Time variation is so big that it hurts
Thermal noise is negligible

Conclusion & Future Work

- We proposed a PHY-layer authentication scheme
  - Channel frequency response measurement and hypothesis testing are used to discriminate between a legitimate user and a would-be intruder
  - Verified using a ray-tracing tool (WiSE) for indoor environment
  - Works well, requiring reasonable values of the measurement bandwidth (e.g., $W > 10$ MHz), number of response samples (e.g., $M \leq 5$) and transmit power (e.g., $P_T \sim 100$ mW)
  - Channel time-variations can improve the performance
- Ongoing work:
  - Cross-layer framework for security: protocol design
  - Terminal mobility
  - Measurements

Thank you!

Questions?

References

[1] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, “Fingerprints in the either: using the physical layer for wireless authentication,” IEEE ICC’ 2007, to appear.

[2] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, “ Using the physical layer for wireless authentication in time-invariant channels,” submitted to *IEEE Trans. On Wireless Communications*, 2007.