Practical Implementations of Physical Layer Authentication

WINLAB

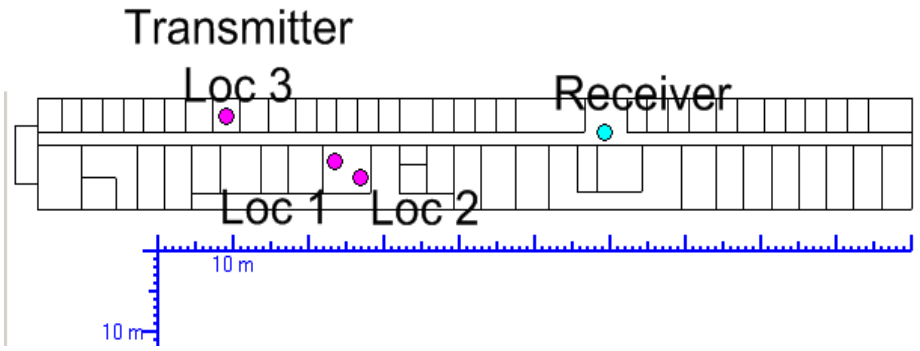
Contact: Liang Xiao

lxiao@winlab.rutgers.edu

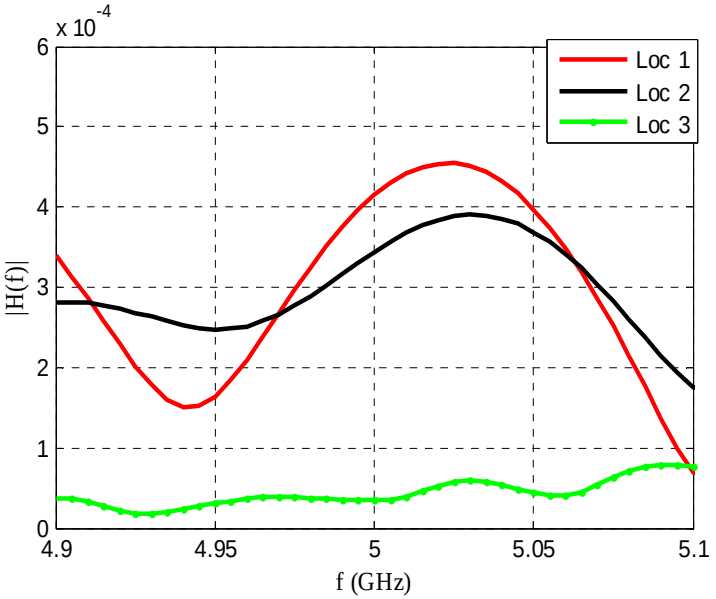
With Profs. Larry Greenstein, Wade Trappe, Narayan Mandayam, and Dr. Alex Reznik at InterDigital

Fingerprints in the Ether (FP) uses channel responses to detect spoofing attacks

- In typical indoor environments, the wireless channel decorrelates rapidly in space
- The channel response is hard to predict and to spoof
- Utilize channel estimation to detect spoofing attacks for wireless networks



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

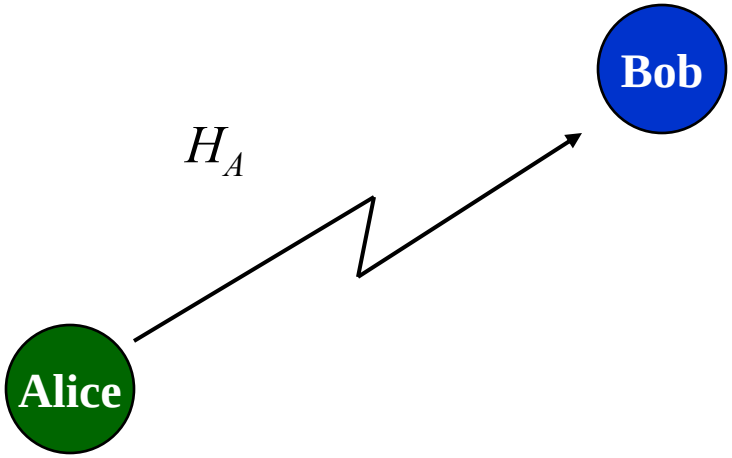


Frequency Response over a 200-MHz Bandwidth

Alice, Bob and Eve: A Simplified Spoofing Detection Scenario

TIME: k

Alice transmits to Bob



Bob estimates channel response H_A from Alice at time k

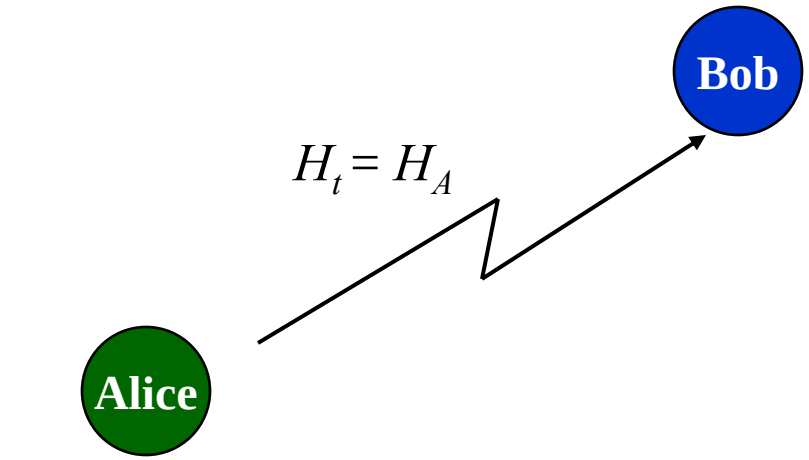
Probe Signal

- Preambles or pilots
- Assume static channel response

Spoofing Detection Scenario (cont.)

TIME: k+1

Case 1: Alice is still transmitting



Bob estimates H_t at time k+1, and compares with H_A

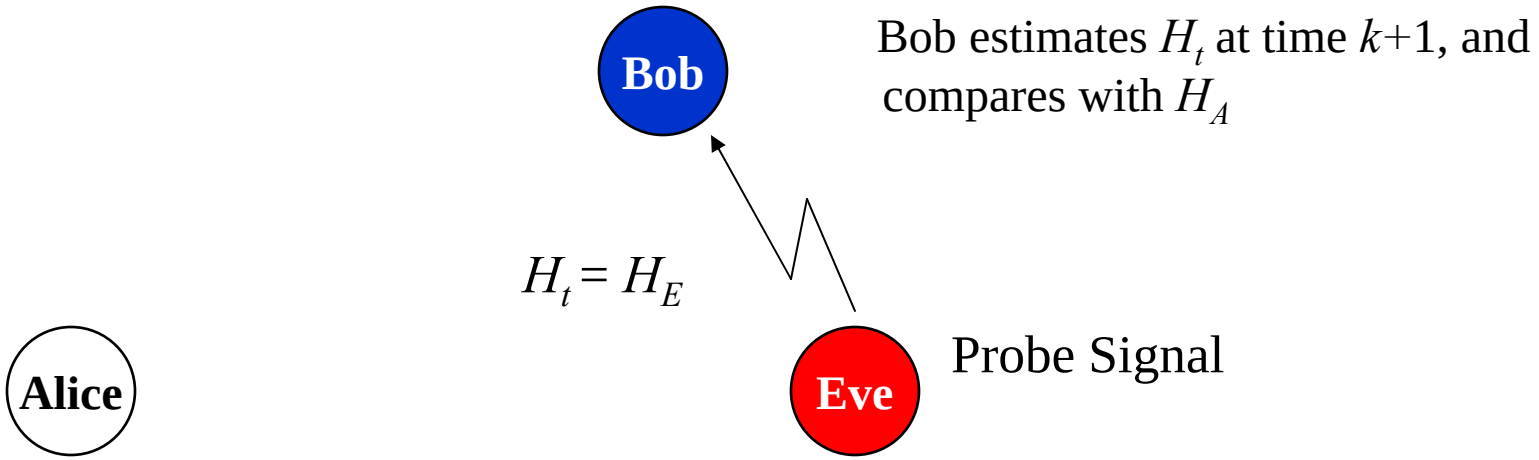
Probe Signal

Desired result: Bob accepts the transmission.

Spoofing Detection Scenario (cont.)

TIME: k+1

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



Desired result: Bob rejects the transmission.

Extensive theoretical studies for FP have been conducted

- We have theoretically analyzed the performance of FP in the detection of spoofing and Sybil attacks
  - L. Xiao, L. J. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the Ether: using the physical layer for wireless authentication," ICC'07.
  - --, "MIMO-assisted channel-based authentication in wireless networks," CISS'08.
  - --, "A physical-layer technique to enhance authentication for mobile terminals," ICC'08.
  - --, "Using the physical layer for wireless authentication under time-variant channels," Trans. Wireless Comm., Jul, 2008.
  - --, "Channel-based detection of Sybil attacks in wireless networks," Tran. Information Forensics & Security, in review.
  - --, "Generalized channel-based spoofing detection in frequency-selective Rayleigh channels," Trans. Wireless Comm., in review.
- However, in this talk we will only briefly review some important results and focus on the real implementation of FP

A simple hypothesis test has been built in FP for spoofing detection

- Observations:
  - $\underline{\hat{H}}(k+1)$ (channel response to be tested)
  - $\underline{\hat{H}}_A(k)$ (reference channel response)
- Hypothesis test:

$\mathcal{H}_0$: $\underline{H}(k+1) = \underline{H}_A(k+1)$ ← *No Spoofing*

$\mathcal{H}_1$: $\underline{H}(k+1) \neq \underline{H}_A(k+1)$ ← *Spoofing!!!*

To cope with oscillator drifting

- Test statistics: $L = \left\| \underline{\hat{H}}(k+1) - \underline{\hat{H}}_A(k) e^{jArg\left(\underline{\hat{H}}(k+1)\underline{\hat{H}}_A{}^H(k)\right)} \right\|^2$
  - Simplified version of the generalized likelihood ratio test
- Rejection region of $\mathcal{H}_0$: Test statistic >Threshold, η

Performance of FP in Snapshot Scenario

- Detection metrics for FP in snapshot scenario:
  - *False Alarm Rate*: The probability of falsely rejecting Alice,
    $$\alpha = P(L > \eta \mid \text{No spoofing})$$
  - *Miss Rate*: The probability of missing the detection of Eve,
    $$\beta = P(L \leq \eta \mid \text{Spoofing})$$
- Given maximum false alarm rate, the test threshold of FP can be derived by using Neyman-Pearson test
- "Snapshot" scenario:
  - Two moments (time k and k+1)
  - A *reliable* reference channel record always exists ("Bob knows")

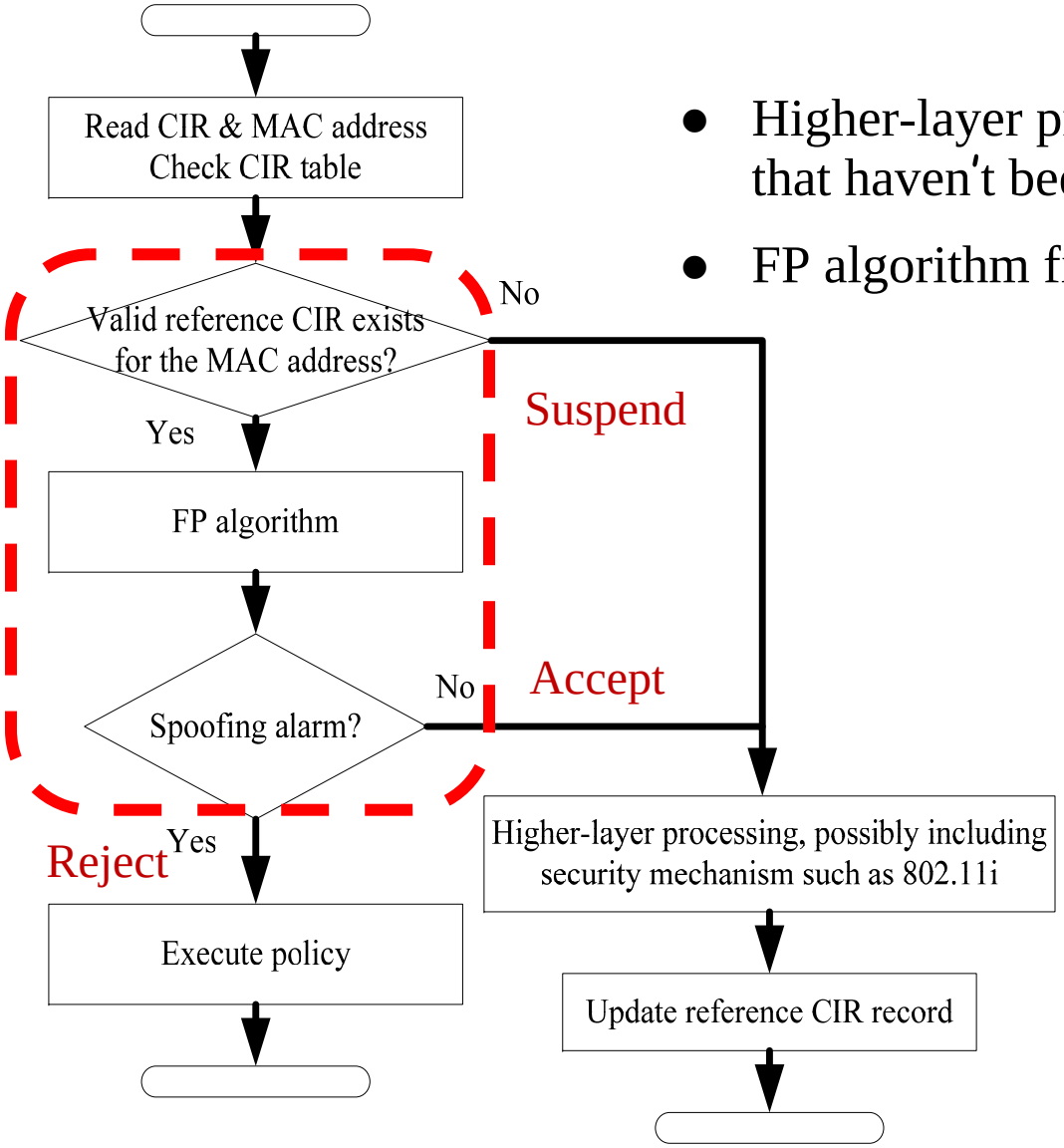
A double-layer authentication protocol is used to integrate FP in real systems

- Reliable reference channel response may not always exist because -
  - Message is the first sent by a user
  - Channel response decorrelates (elapsed channel coherence time)
  - Previous spoofing message accepted by FP
- Double-layer authentication
  - FP maintains a reference channel record for each active user
    - Each reference CIR record expires after N_T
    - Design goal: N_T <channel coherence time

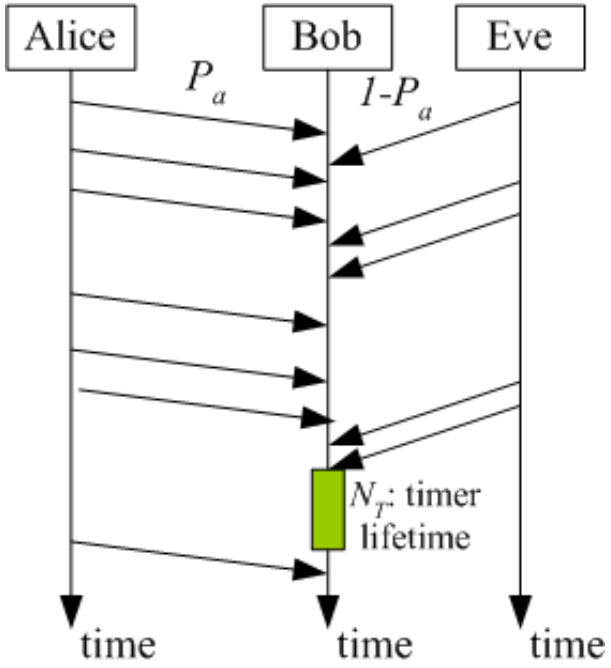
N_T is an important parameter

  - Higher-layer processing may include some security mechanism
    - May be sophisticated (e.g., 802.11i), or very simple (even nominal in some simple systems)
  - Embed the snapshot performance of FP (α, β) into a more realistic context, where we *cannot* assume that Bob knows true Alice-Bob channel

Flowchart of Double-Layer Authentication Protocol



- Higher-layer process only deals with messages that haven't been filtered out by FP
- FP algorithm filters out most spoofing messages



Performance of FP

- The generalized performance of FP, (false alarm rate P_{FA} and miss rate P_M), depends on attack pattern, snapshot FP performance, and channel coherence time (N_T)
- We upper bound its performance by assuming ideal higher-layer process:

$$\boldsymbol{P_{FA}} = \alpha - \alpha\left(1 - \boldsymbol{P_a}\left(1 - \boldsymbol{P_{FA}}\right)\right)^{\boldsymbol{N_T}}$$

$$\boldsymbol{P_M} = \beta + \left(1-\beta\right)\left(1 - \boldsymbol{P_a}\left(1 - \boldsymbol{P_{FA}}\right)\right)^{\boldsymbol{N_T}}$$

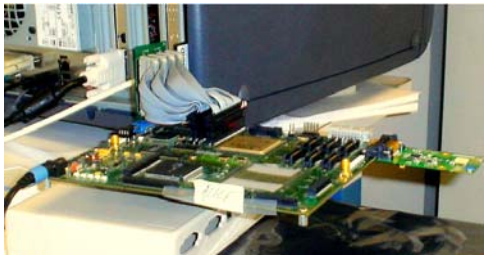
  - Fraction P_a of messages sent by Alice

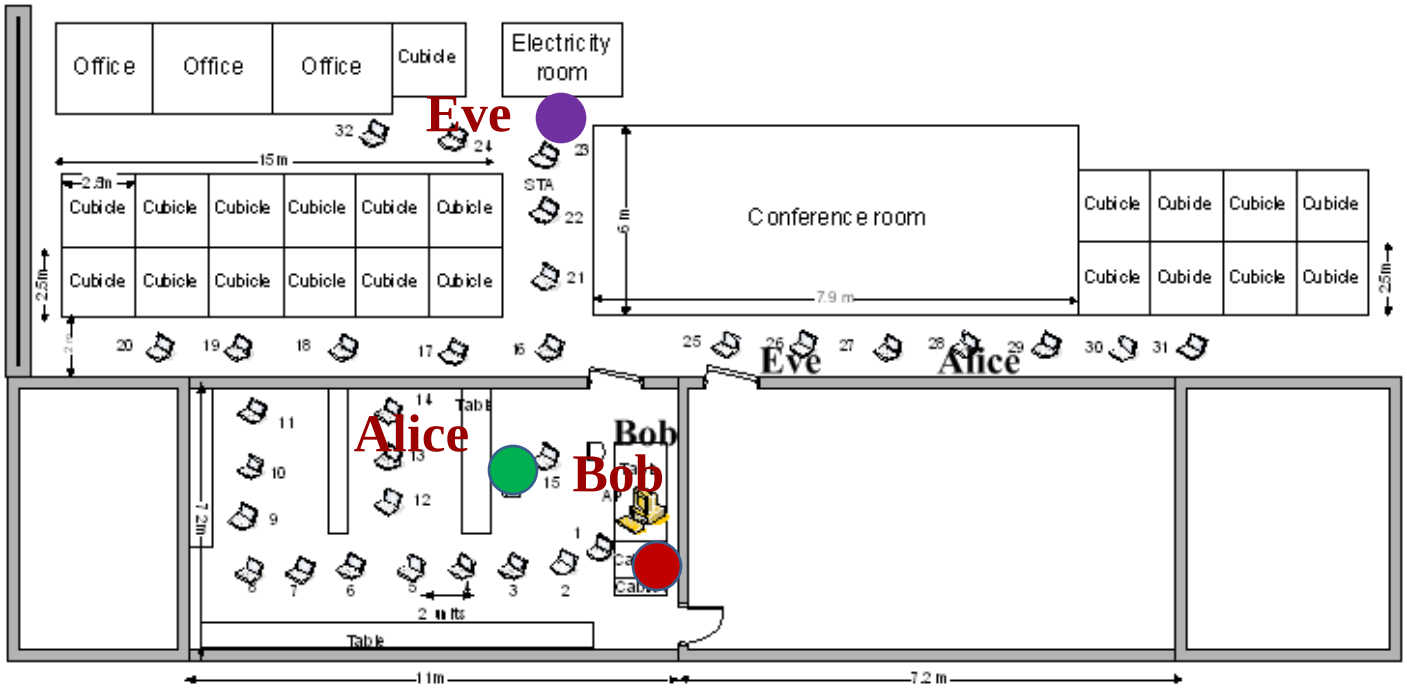
- Benefits of FP techniques
  - Significantly reduce the workload of the higher-layer functions from C to $C((1\text{-}P_a)\,P_M + P_a(1\text{-}P_{FA}))$, which is $0.74C$ with P_a = .8 and P_{FA}=P_M=.1
  - Slightly increase the overall system false alarm rate while dramatically decrease the overall miss rate, for some “naked” wireless sensor systems

Implementation Challenges of FP in 802.11

- The WiFi system bandwidth is not always wide enough to provide a very high resolution for the multipath phenomenon inside an office building
  - Want better performance? Answer: MIMO techniques (802.11n)
- The CIR data provided by an 802.11 device are scaled and corrupted by many factors
  - Receiver thermal noise & phase drifting: addressed by FP
  - Timing or frequency estimation error
- Knowledge of some channel parameters, such as the channel coherence time, may be not available.

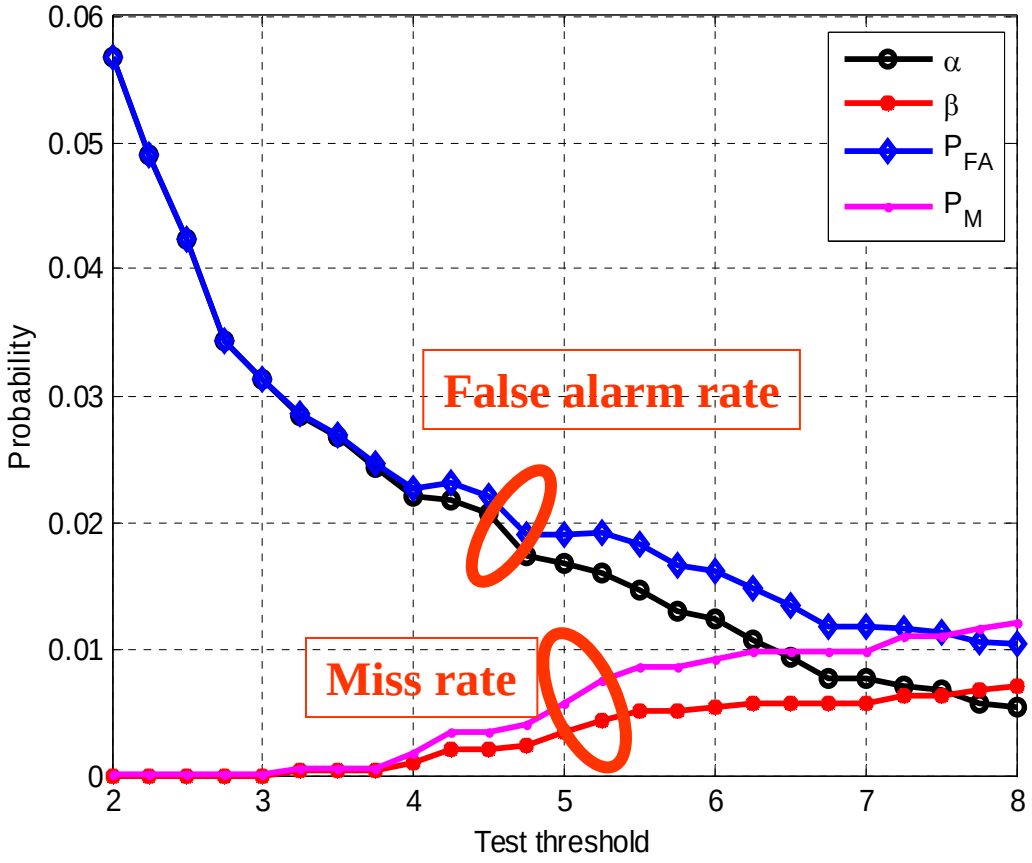
Verification of the performance of FP in 802.11 systems was done by field tests on a WiFi testbed





KOP site, InterDigital

Some Results: Its false alarm rate and miss rate in spoofing detection are mostly below 5%.



Workload of higher-layer functions reduced by ~30%

FP performance (P_{FA} and P_m), and the snapshot performance (α and β), obtained by three-board field test, with N_T=2, P_a=70% of the received messages sent by Alice.

Conclusion & Future Work

- We propose a double-layer authentication protocol to integrate the fingerprinting (FP) algorithm into real wireless systems, which either provides some degree of spoofing detection for a “naked” wireless system, or reduces the workload of the higher-layer processing
  - Performance analysis in a generalized scenario
  - Implementation in 802.11 systems
  - Field test results
- Future work:
  - How to further quantify the performance gain of FP, in terms of computation time or complexity?
  - Further performance evaluation using more offline/online field tests