CANS 17 @ Hong Kong

Practical Evaluation of Passive COTS Eavesdropping in 802.11b/n/ac WLAN

DANIELE ANTONIOLI (SUTD), S. SIBY (EPFL),
N. O. TIPPENHAUER (SUTD)

Our Motivations

- Some PHY features theoretically disadvantage an eavesdropper
  - Eg: reduce eavesdropping range
  - Few practical evaluations of those claims
  - Typically not focusing on a real protocol
- 802.11n/ac WLAN amendments
  - Use of MIMO and beamforming
- *Is eavesdropping affected by recent PHY features?*
  - *If yes, we get extra resilience for free*
  - *Even from COTS devices*

Our Metrics

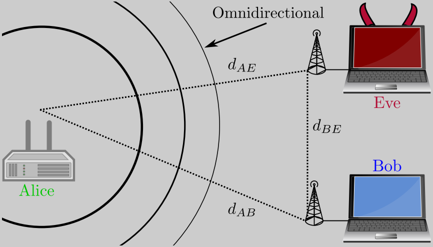
- SNR: Signal-to-Noise-Ratio
  - Power of the useful signal divided by the noise power at the receiver
  - $10 \log_{10} \mathrm{SNR} = \mathrm{SNR}_{\mathrm{dB}}$
- BER: Bit-Error-Rate
  - Probability of erroneously decoding 1-bit at the receiver
  - Not exact quantity (MCS, fading model)
  - 10^{-6} is considered a reasonable BER value
- PER: Packet-Error-Rate
  - Computed as: $\mathrm{PER} = 1 - (1 - \mathrm{BER})^N$
  - N is the average packet size in bits

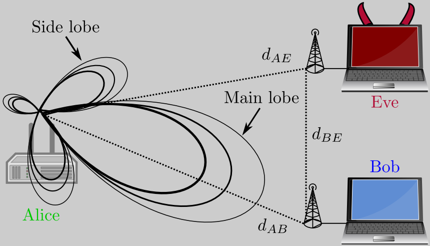
Our Evaluation of 802.11 Eavesdropping

- **802.11n/ac vs. 802.11b**
  - Passive eavesdropper (Eve)
  - Downlink channel (from Alice to Bob)
  - NLOS environment (exploit multipath)
  - 802.11b as a baseline: no MIMO
- **Predictions**
  - Eve's SNR disadvantage in b vs. n/ac
  - Eve's PER disadvantage compared to Bob in n/ac
- **Experimental evaluation**
  - With COTS devices in an indoor environment
  - Measure PER and SNR
  - Compare results with predictions

802.11 Downlink Passive Eavesdropping

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN





- **802.11b (SISO)**
  - Alice uses 1 antenna
  - No disadvantages for Eve
  - Eve success depends on: d_{AE}

- **802.11n/ac (MIMO)**
  - Alice uses L antennas
  - Transmit-beamforming towards Bob disadvantages Eve
  - Eve success depends on: d_{AE}, d_{BE}, and L

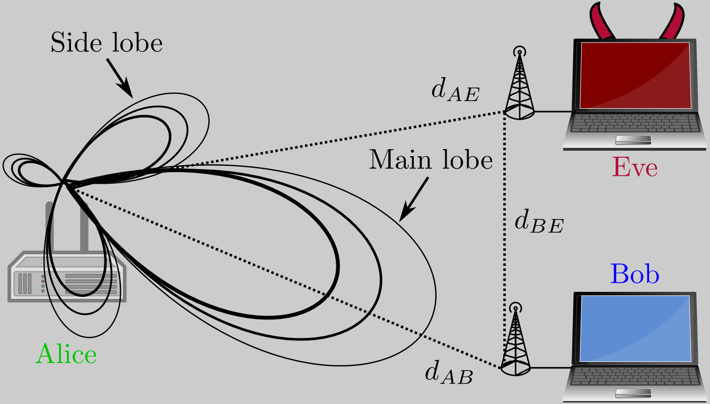
Our Attacker Model

- Eve is a *passive eavesdropper*
  - Eavesdrop the downlink
  - Outside the main lobe (if Alice uses beamforming)
- *Equipotent* to Bob
  - COTS devices
  - Same number of antennas
- Eavesdrops in monitor mode
  - No retransmissions

Theoretical Discussion Goals

- Quantify the disadvantages of Eve
  - In 802.11n/ac (MIMO) compared to 802.11b (SISO)
- Eve's SNR disadvantage
  - Upper bound from BER formula (Rayleigh fading)
  - Lower bound from transmit-beamforming gain
- Expected BER and PER of Eve vs. Bob
  - Varying their distances to Alice
  - Using 802.11n/ac different path loss models

Passive Eavesdropping 802.11n/ac



- **802.11n/ac (MISO)**
  - Alice uses L antennas
  - Transmit-beamforming towards Bob disadvantages Eve
  - Eve success depends on: d_{AE}, d_{BE}, and L

SNR Disadvantage: Upper Bound

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Number of transmitting antennas (L) is key:

$$\lambda = \sqrt{\frac{\mathrm{SNR}}{2 + \mathrm{SNR}}} \quad (1)$$

$$\mathrm{BER}_{\mathrm{SISO}} = \frac{1}{2}(1 - \lambda) \quad (2)$$

$$\mathrm{BER}_{\mathrm{MISO}} = \left(\frac{1-\lambda}{2}\right)^{L} \cdot \sum_{i=0}^{L-1} \binom{L+i-1}{i} \left(\frac{1+\lambda}{2}\right)^{i} \quad (3)$$

- If L = 4 and BER = 10^{-6}, then
  - $\mathrm{SNR}_{\mathrm{SISO}} = 57$ (no diversity)
  - $\mathrm{SNR}_{\mathrm{MISO}} = 16$ (diversity order = 4)
  - Eve's SNR disadvantage in 802.11n/ac is 41 dB (at most)

SNR Disadvantage: Lower Bound

The MISO transmission gain from Alice to Bob is (using CCD):

$$\|g\|^2 = 10 \log_{10}(L)\ dB \tag{4}$$

- Eve is not benefiting from g
- If L = 4, then
  - Eve's SNR disadvantage in 802.11n/ac is 6 dB (at least)

SNR Disadvantage: Lower Bound

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

The MISO transmission gain from Alice to Bob is (using CCD):

$$\|g\|^2 = 10\log_{10}(L)\ dB \tag{4}$$

- Eve is not benefiting from g
- If L = 4, then
  - Eve's SNR disadvantage in 802.11n/ac is 6 dB (at least)

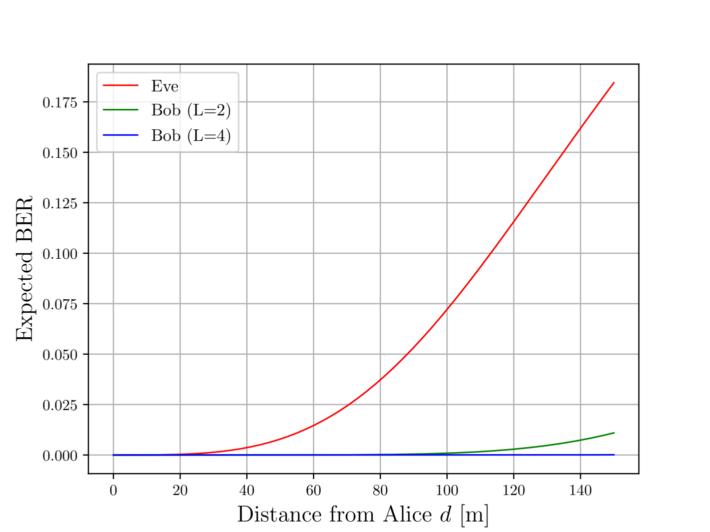
- **Eve's SNR disadvantage in 802.11n/ac form 6 to 41 dB**

BER and PER: Indoor Path Loss Models

- From: *Next Gen. Wireless LAN: 802.11n and 802.11ac*
  - d_{BP} is the breakpoint distance
  - σ_{SF} is the shadowing std dev (log-normal)
  - s_{PL} LOS and NLOS path loss slopes
- **Model B**: Residential (intra-room)
  - $d_{BP} = 5$ m
  - σ_{SF} = 3, 4 dB
  - s_{PL} = 2, 3.5
- **Model D**: Office (large conference room)
  - $d_{BP} = 10$ m
  - σ_{SF} = 3, 5 dB
  - s_{PL} = 2, 3.5

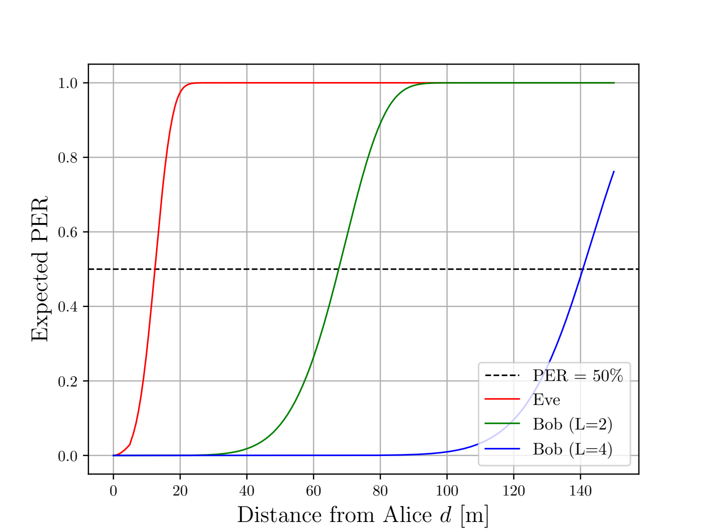
Model B (Residential) Expected BER

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN



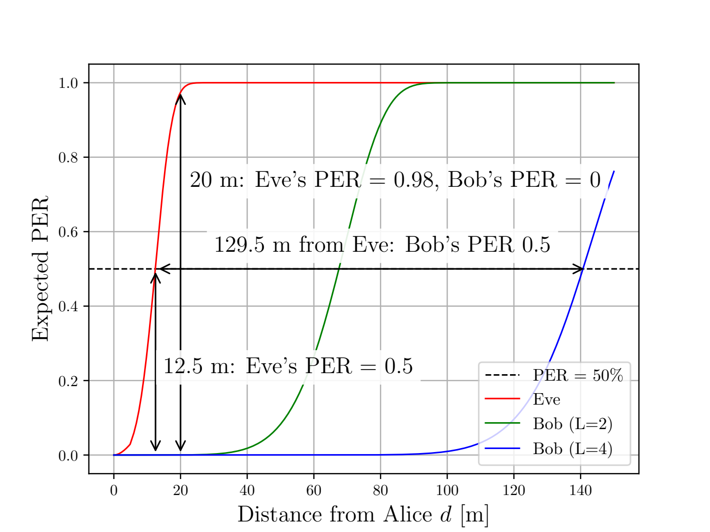
- BER of Eve, Bob(L=2) and Bob(L=4) in 802.11n (BPSK)

Model B (Residential) Expected PER



- PER of Eve, Bob(L=2) and Bob(L=4) in 802.11n (BPSK)

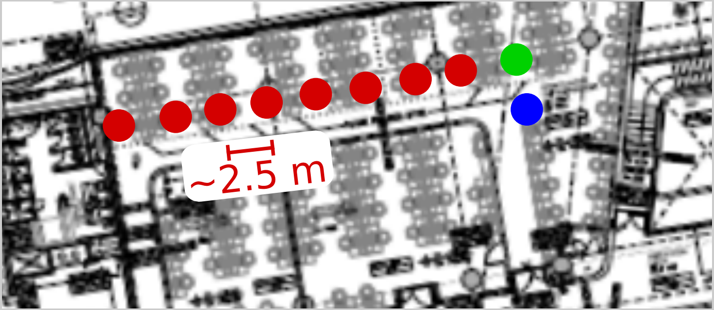
Model B (Residential) Expected PER



- PER of Eve, Bob(L=2) and Bob(L=4) in 802.11n (BPSK)

Experimental Indoor Office Layout

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN



- Alice, Bob, and Eve locations
  - $d_{AB} = 2$ m
  - $\vec{d}_{AE} = [2.5, 5.0, \ldots, 20]$ m (8 distances)
  - $\Delta d_{AE} = 2.5$ m
  - Constant angle and elevation
  - NLOS (exploit multipath)

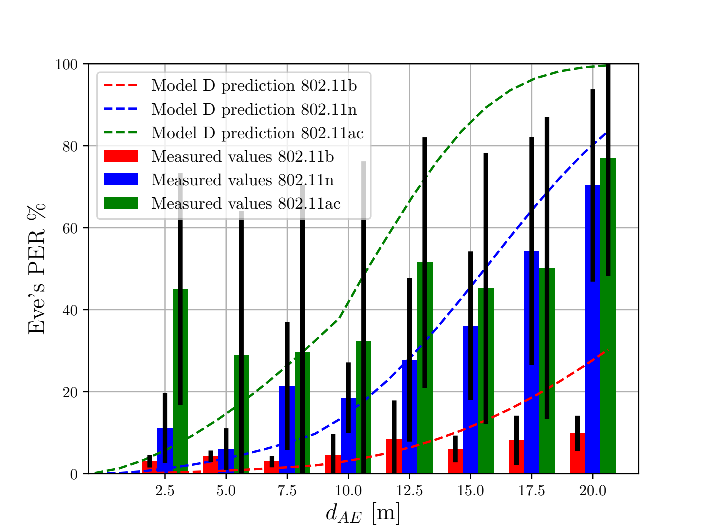
Experimental Setup: COTS and PHY

- COTS devices
  - Alice: Linksys WRT3200ACM, 4x4, OpenWrt
  - 802.11n: Bob and Eve use a TL-WN722N USB dongle
  - 802.11ac: Bob uses an USB-AC68, Eve uses a MacBook Pro
- Physical layer setup
  - $P_A = 23$ dBm (Alice's tx power)
  - $N_0 = -91$ dBm (mean noise power at receiver)
  - $Ch_{b/n/ac} = 11, 11, 36$

Experimental Setup: Traffic and Metrics

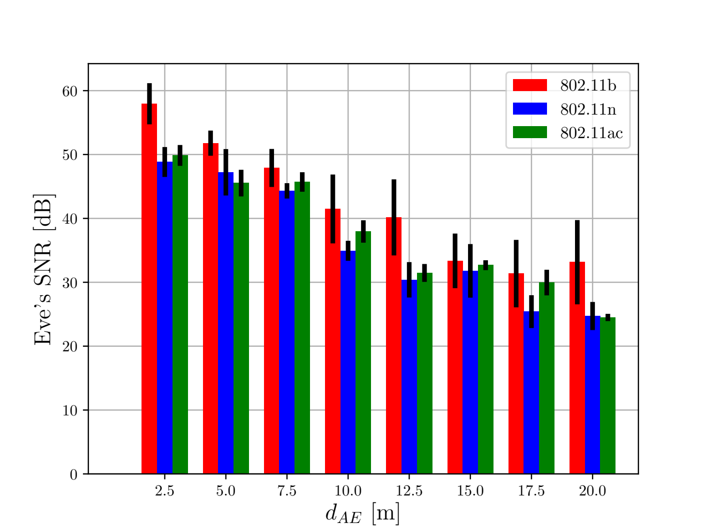
- UDP traffic from Alice to Bob
  - Using `iperf`
  - 30 repetitions per distance
- SNR
  - RSSI and noise floor from PHY radiotap headers
- PER
  - From incorrect UDP checksums
  - Over the total number of packet sent
  - Underestimate PER (no FCS)

Eve's Measured PER vs. Model D (Office)



- Eve's PER is *increasing with 802.11b/n/ac*

Eve's Measured SNR



- Eve's SNR in 802.11n/ac is *smaller* than in 802.11b

Practical Evaluation of Passive COTS Eavesdropping in 802.11b/n/ac

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Predicted 802.11n/ac disadvantages for Eve
  - SNR is bounded by 6-41 dB
  - PER increases to 98% when $d_{AE} > 20$ m
  - Eve has to be 129.5 m closer to get same performance as Bob
- Experimental results about Eve
  - PER increases significantly when $d_{AE} > 15$ m
  - PER is 20% higher in 802.11n than in 802.11b
  - PER is 30% higher in 802.11ac than in 802.11b
- We conclude that
  - *802.11n/ac PHY features disadvantage an eavesdropper*

Practical Evaluation of Passive COTS Eavesdropping in 802.11b/n/ac

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Predicted 802.11n/ac disadvantages for Eve
  - SNR is bounded by 6-41 dB
  - PER increases to 98% when $d_{AE} > 20$ m
  - Eve has to be 129.5 m closer to get same performance as Bob
- Experimental results about Eve
  - PER increases significantly when $d_{AE} > 15$ m
  - PER is 20% higher in 802.11n than in 802.11b
  - PER is 30% higher in 802.11ac than in 802.11b
- We conclude that
  - *802.11n/ac PHY features disadvantage an eavesdropper*

Thanks for your time! Questions?