CSIsnoop: Attacker Inference of Channel State Information in Multi-User WLANs

Xu Zhang and Edward W. Knightly

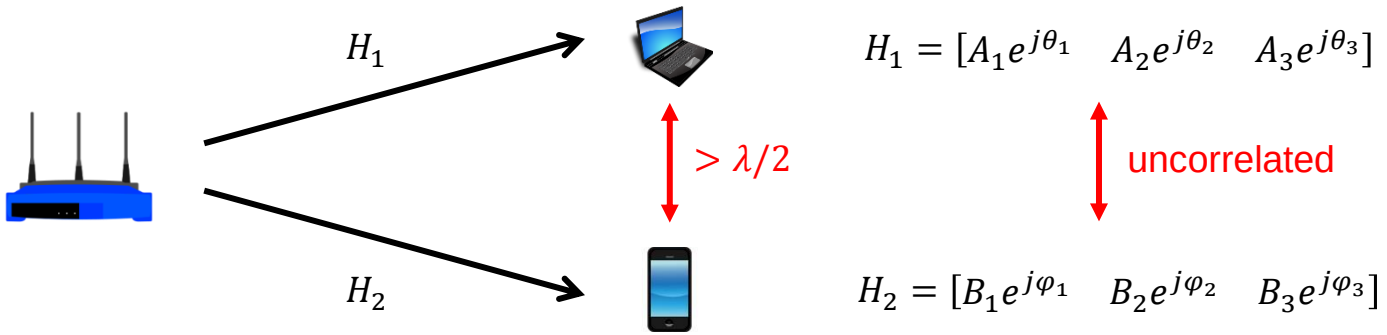
ECE Department, Rice University

Channel State Information (CSI)

- CSI plays a key role in wireless networks

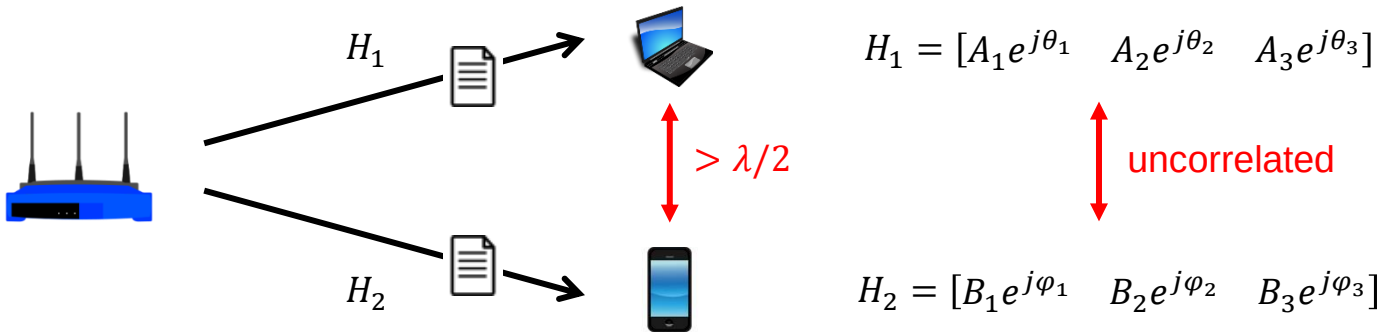
Channel State Information (CSI)

- CSI plays a key role in wireless networks



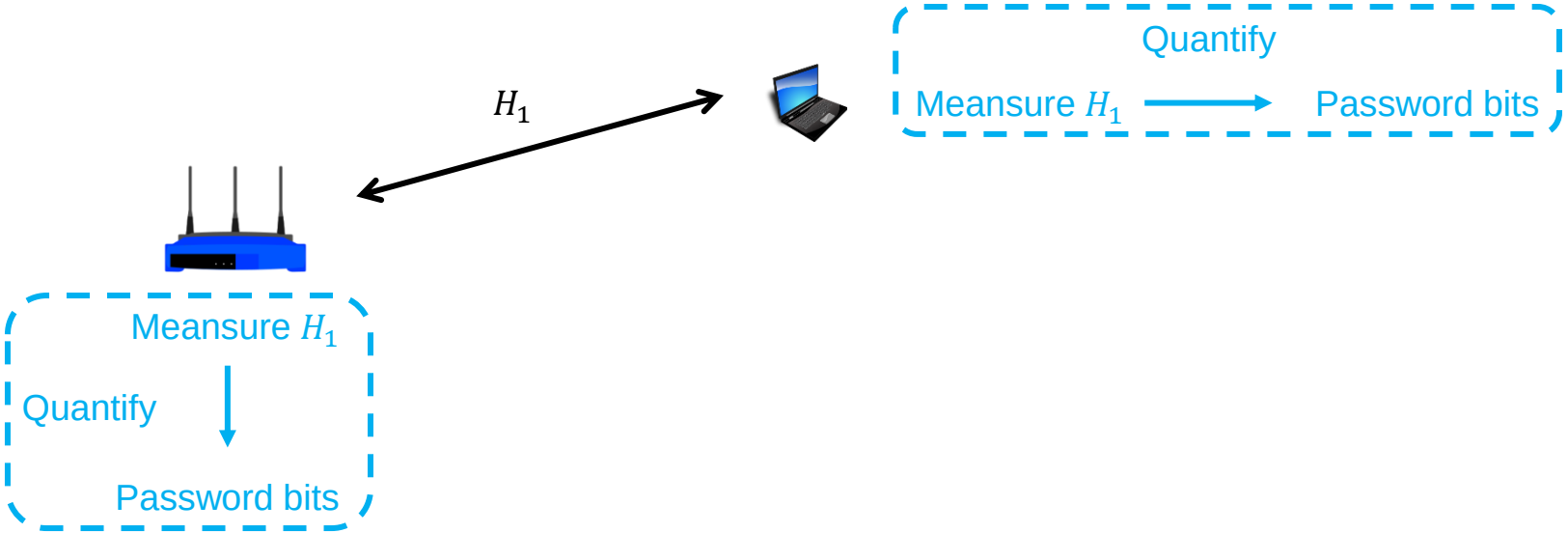
Channel State Information (CSI)

- CSI plays a key role in wireless networks
  - Increase throughput – e.g., IEEE 802.11ac



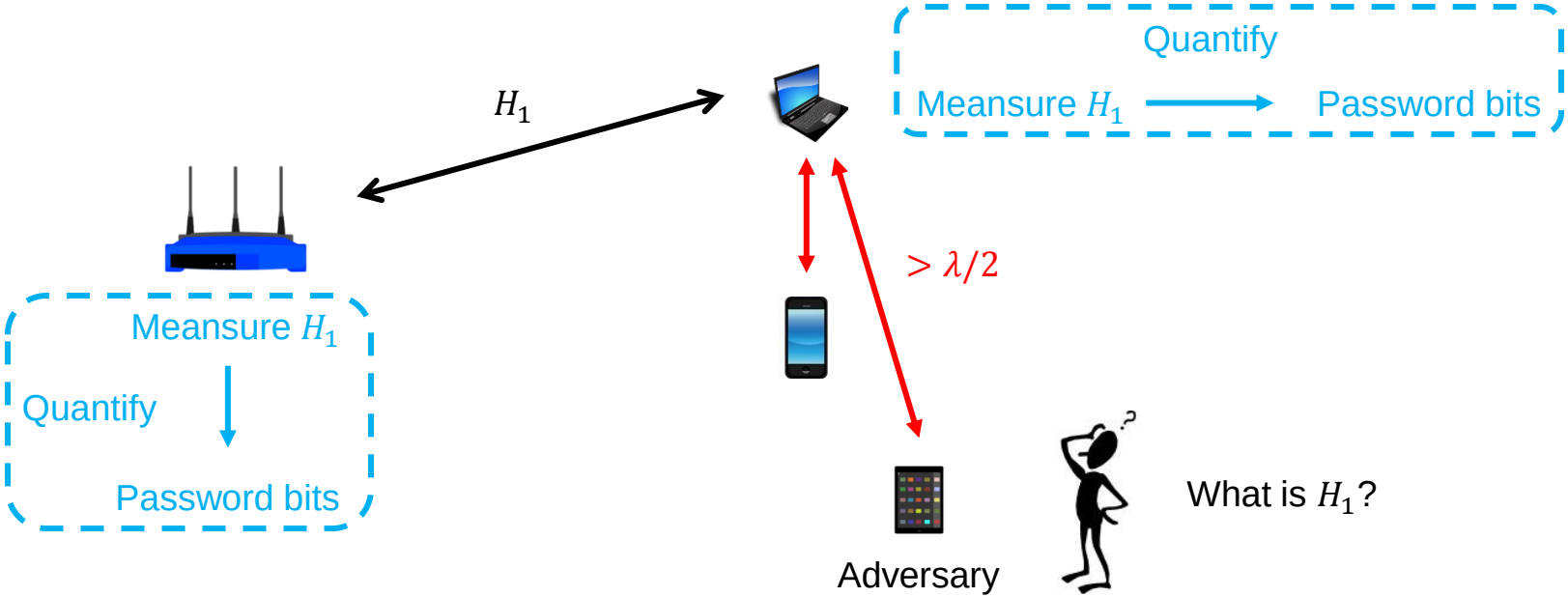
Channel State Information (CSI)

- CSI plays a key role in wireless networks
  - Increase throughput – e.g., IEEE 802.11ac
  - Enhance security – e.g., CSI-based password



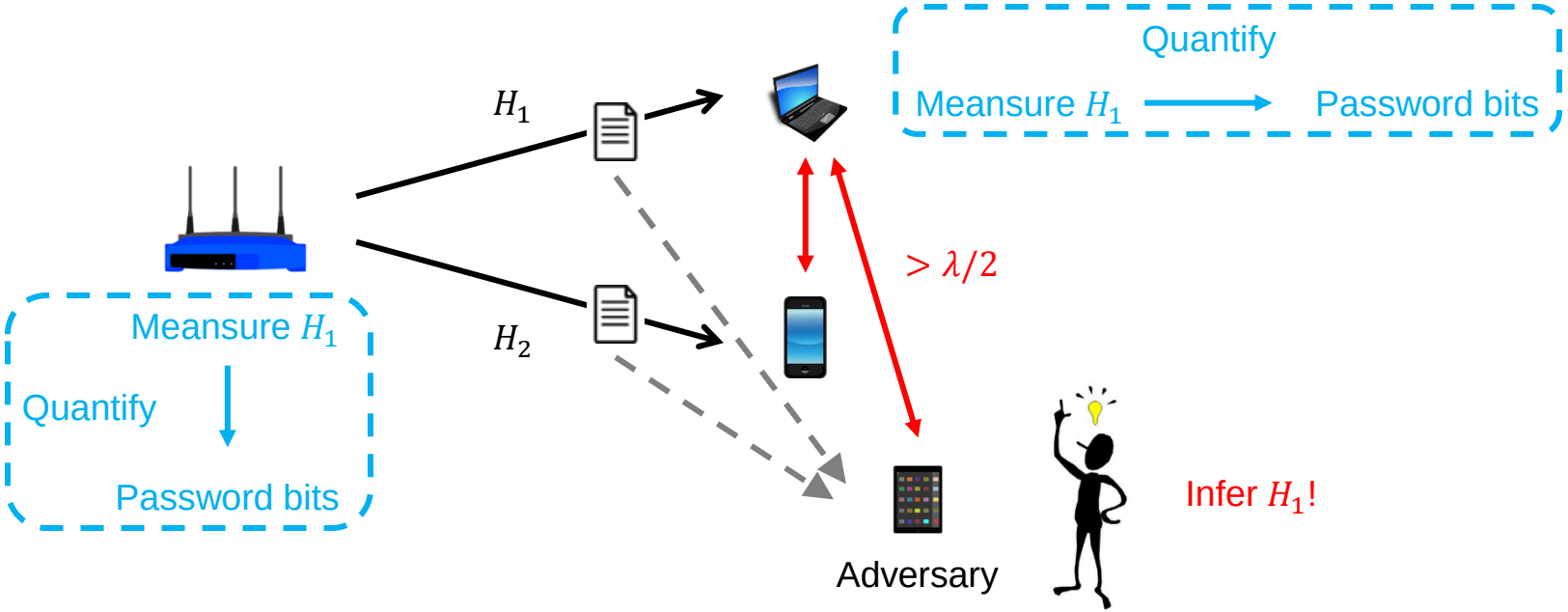
Channel State Information (CSI)

- Conventionally, any nodes half-a-wavelength away cannot guess the laptop's CSI



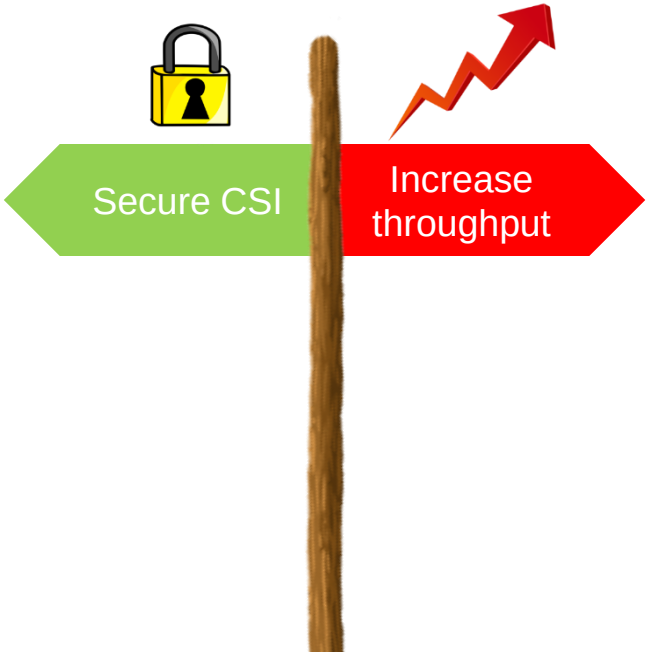
Channel State Information (CSI)

- Conventionally, any nodes half-a-wavelength away cannot guess the laptop's CSI
- However, we show that even a *passive* adversary can actually infer the laptop's CSI



CSIsnoop

- A fundamental conflict between using CSI to optimize PHY and hiding CSI from adversaries

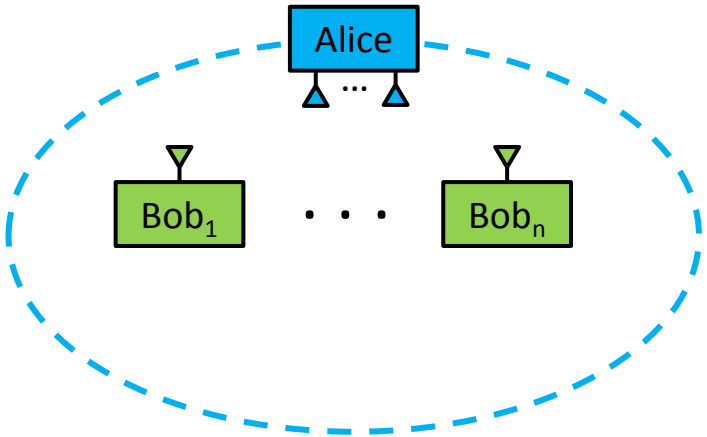


Roadmap

- Threat Model
- CSIsnoop Framework
- Implementation on WARP and Experimental Evaluation

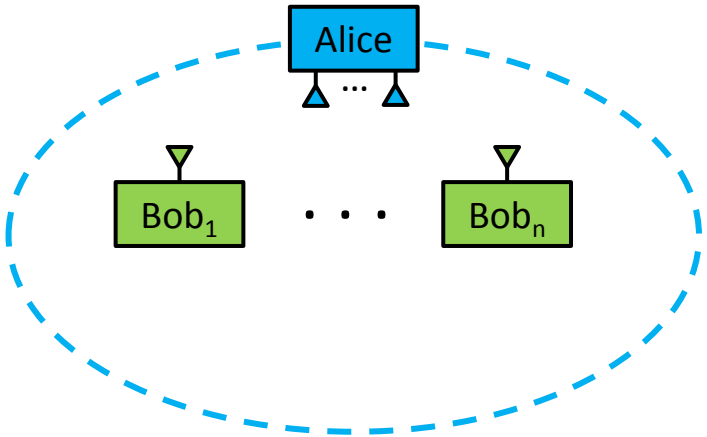
Threat Model – Legitimate Clients

- A typical multi-user WLAN with OFDM transmission
  - Multi-antenna AP Alice
  - Single-antenna clients Bob_1 to Bob_n
  - Alice always uses all her antennas to boost the throughput



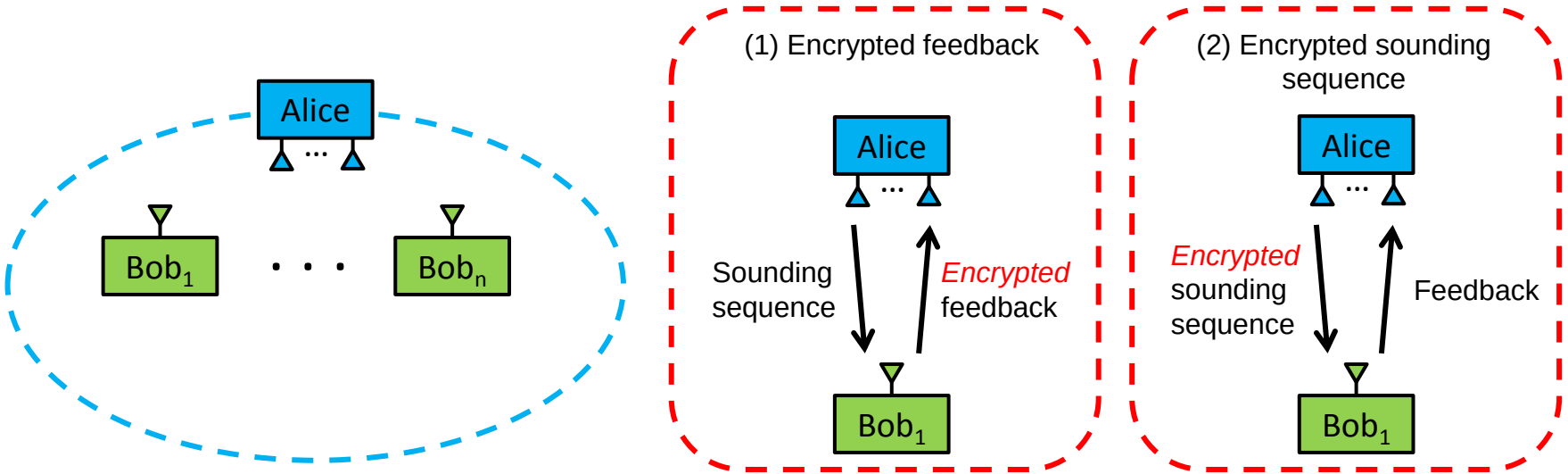
Threat Model – Legitimate Clients

- A typical multi-user WLAN with OFDM transmission
  - Explicit channel sounding like IEEE 802.11ac



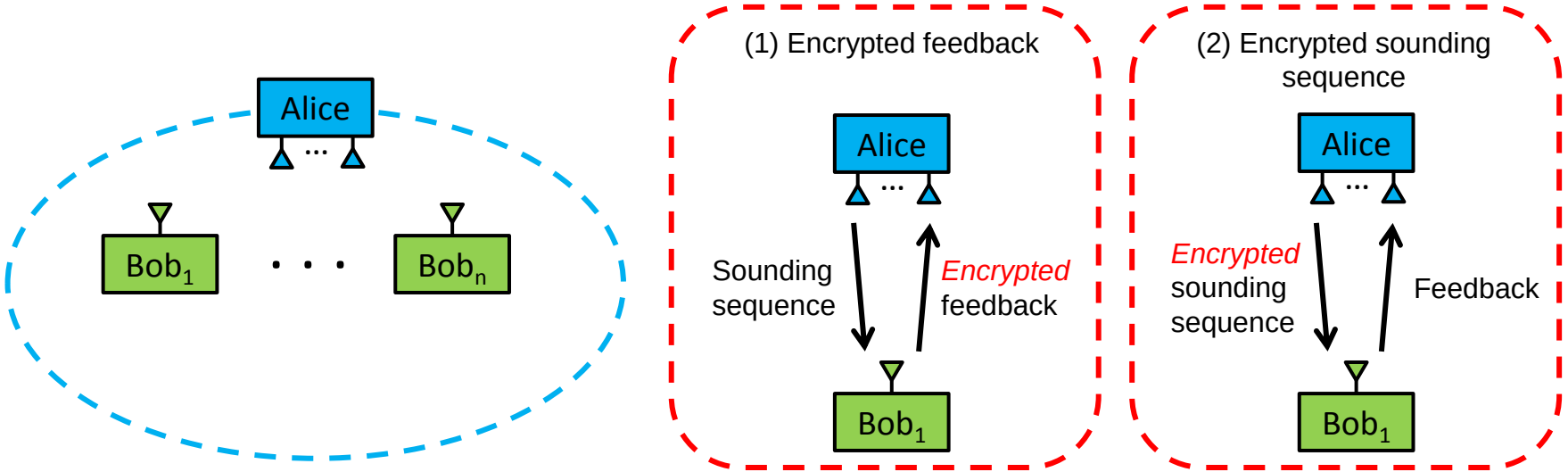
Threat Model – Legitimate Clients

- A typical multi-user WLAN with OFDM transmission
  - Explicit channel sounding like IEEE 802.11ac
  - Encrypted feedback or sounding sequence



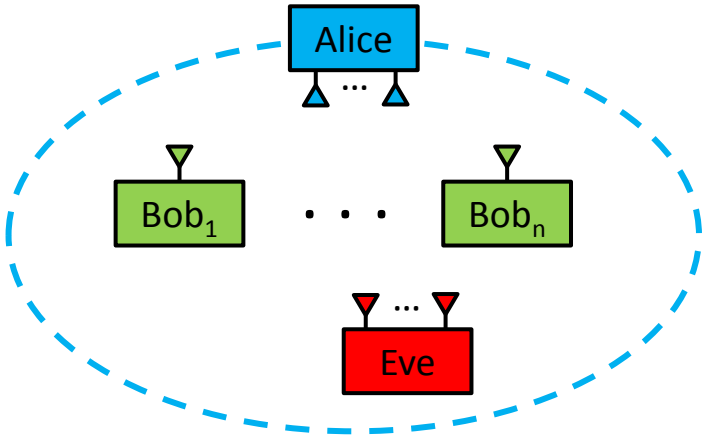
Threat Model – Legitimate Clients

- A typical multi-user WLAN with OFDM transmission
  - Explicit channel sounding like IEEE 802.11ac
  - Encrypted feedback or sounding sequence
  - Zero-force beamforming, but CSIsnoop can be generalized to other beamforming algorithms



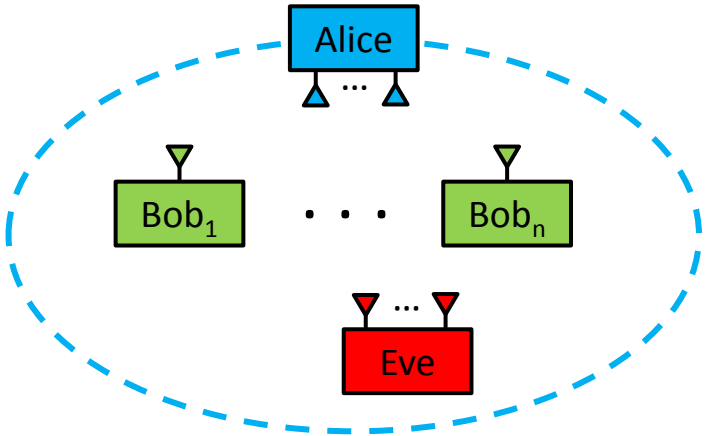
Threat Model – Adversary

- Eve is a multi-antenna adversary
  - Same number of antennas as the AP Alice



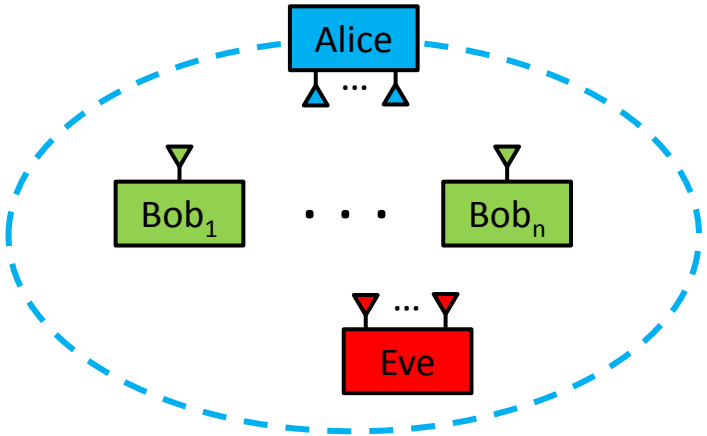
Threat Model – Adversary

- Eve is a multi-antenna adversary
  - Same number of antennas as the AP Alice
  - In range of Alice
  - Knows which Bobs are included in multi-user beamforming transmission
  - Knows part of the symbols in each Bob's downlink data packets



Threat Model – Adversary

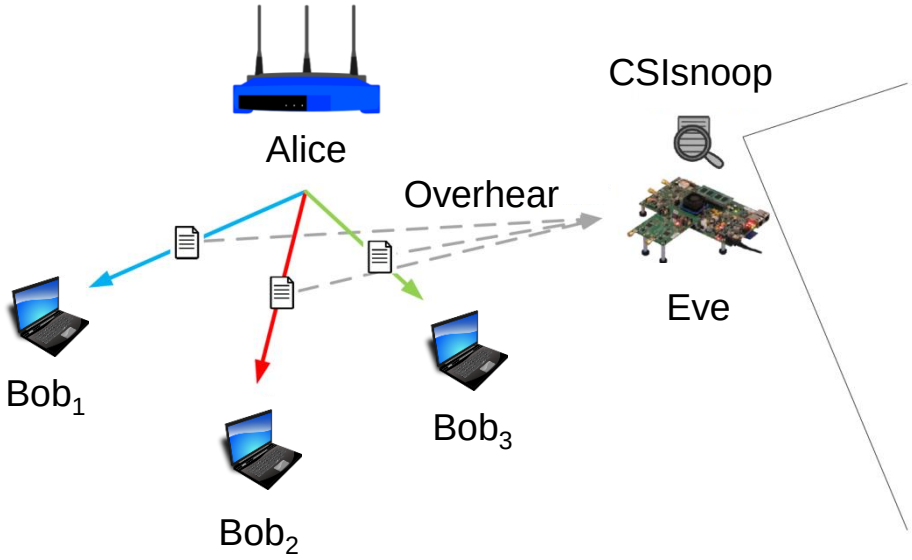
- Eve is a multi-antenna adversary
  - Same number of antennas as the AP Alice
  - In range of Alice
  - Knows which Bobs are included in multi-user beamforming transmission
  - Knows part of the symbols in each Bob's downlink data packets



Packet from Alice to Bob:

Eve knows these symbols before overhearing them

CSIsnoop Framework



Known symbols at Eve

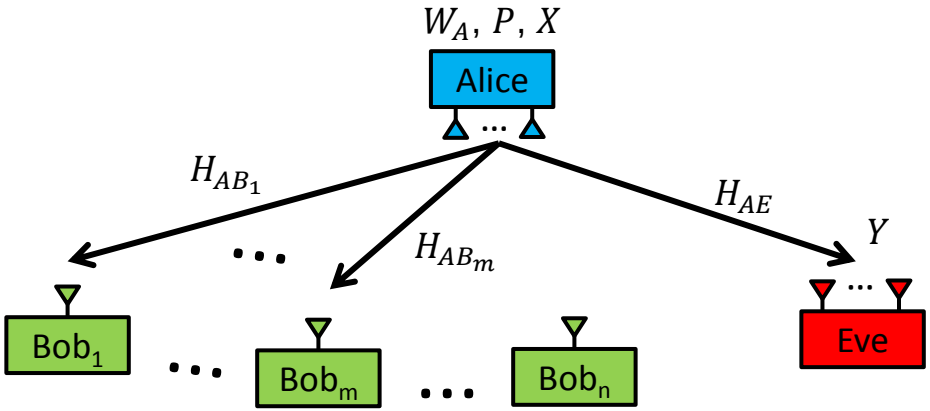
↓

Alice's transmit beamforming weights

↓

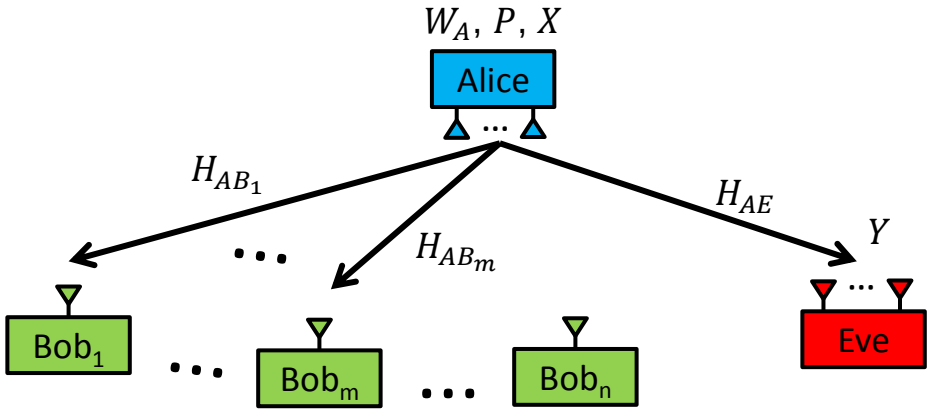
CSI between Alice and each Bob

CSIsnoop Framework



$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N$$

CSIsnoop Framework



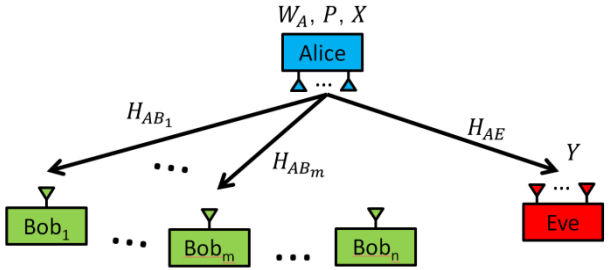
Data to selected Bobs

Signals at Eve $Y = H_{AE} \cdot W_A \cdot P \cdot X + N$

Diagonal transmit power scaling matrix

Transmit beamforming weights

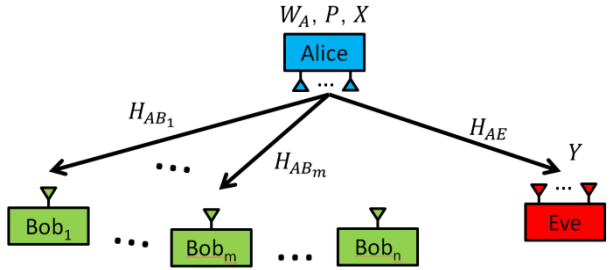
CSIsnoop Framework



$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N \qquad (1)$$

$$H_{AB} \cdot W_A = I \qquad (2)$$

CSIsnoop Framework

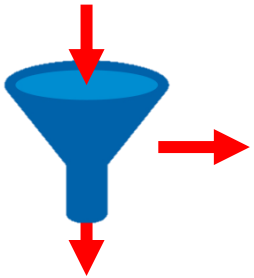


$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N \qquad (1)$$

$$H_{AB} \cdot W_A = I \qquad (2)$$

- Known-transmitted-symbol attack

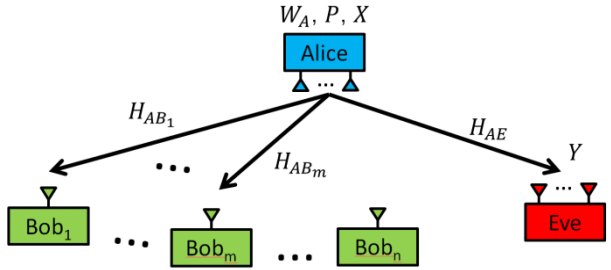
X: known symbols at Eve



$$W_E = \arg\min \|Y - W_E X\|$$

Y: overheard signals at Eve

CSIsnoop Framework



$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N \quad (1)$$

$$H_{AB} \cdot W_A = I \quad (2)$$

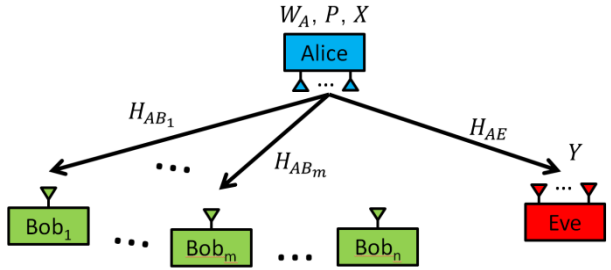
- Known-transmitted-symbol attack

X: known symbols at Eve

$$W_E = \arg\min \|Y - W_E X\| \rightarrow H_{AE} \cdot W_A \cdot P \approx W_E$$

Y: overheard signals at Eve

CSIsnoop Framework



$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N \qquad (1)$$

$$H_{AB} \cdot W_A = I \qquad (2)$$

- Known-transmitted-symbol attack

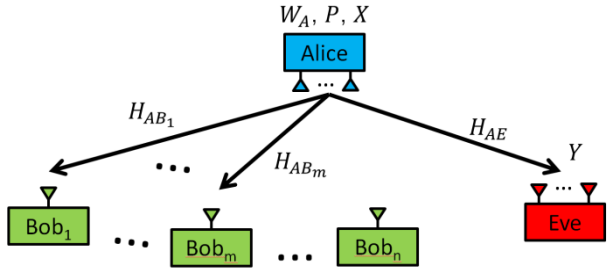
X: known symbols at Eve

Y: overheard signals at Eve

First assume that Eve knows H_{AE}

$$W_E = \arg\min \|Y - W_E X\| \rightarrow H_{AE} \cdot W_A \cdot P \approx W_E \rightarrow W_A \cdot P \approx H_{AE}^{-1} \cdot W_E$$

CSIsnoop Framework

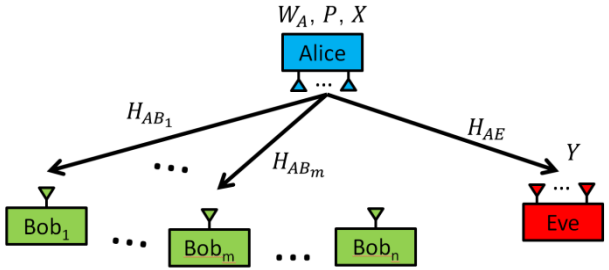


$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N \qquad (1)$$

$$H_{AB} \cdot W_A = I \qquad (2)$$

- Known-transmitted-symbol attack
  - Eve computes $W_A \cdot P$
  - Eve does not know P and cannot solve W_A

CSIsnoop Framework

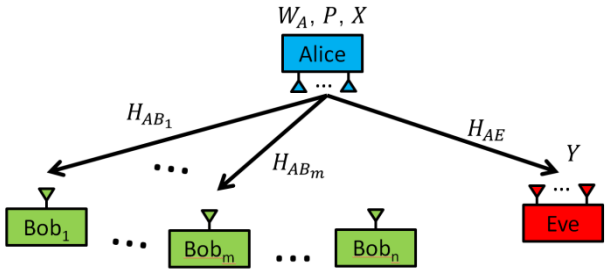


$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N \qquad (1)$$

$$H_{AB} \cdot W_A = I \qquad (2)$$

- Known-transmitted-symbol attack
  - Eve computes $W_A \cdot P$
  - Eve does not know P and cannot solve W_A
- Alice and Bob use $span(H_{AB_j})$ instead of H_{AB_j}
  - Remove inter-user interference
    - ✓ Alice transmits signals of $Bob_{i \neq j}$ into $null(H_{AB_j})$
  - CSI-based password
    - ✓ Normalize H_{AB_j} as Alice and Bob_j may use different transmit power

CSIsnoop Framework



$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N \qquad (1)$$

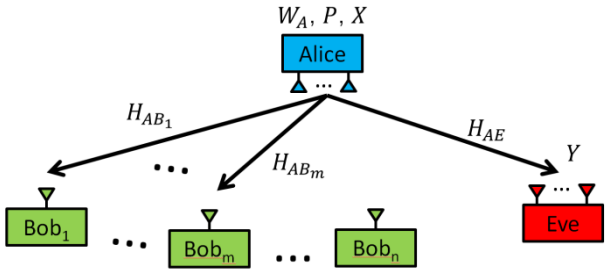
$$H_{AB} \cdot W_A = I \qquad (2)$$

$$\begin{bmatrix} -H_{AB_1} - \\ -H_{AB_2} - \\ \vdots \\ -H_{AB_m} - \end{bmatrix} \cdot \begin{bmatrix} | & | & & | \\ W_{A1} & W_{A2} & \cdots & W_{Am} \\ | & | & & | \end{bmatrix} = I$$

- To compute $span(H_{AB_j})$, Eve only needs to know the direction of each column of W_A
- $W_A \cdot P$ preserves the direction of each column of W_A

$$W_A \cdot P = [W_{A1}, \dots, W_{Am}] \cdot \begin{bmatrix} \sqrt{p_1} & & \\ & \ddots & \\ & & \sqrt{p_m} \end{bmatrix} = [W_{A1}\sqrt{p_1}, \dots, W_{Am}\sqrt{p_m}]$$

CSIsnoop Framework



$$Y = H_{AE} \cdot W_A \cdot P \cdot X + N \qquad (1)$$

$$H_{AB} \cdot W_A = I \qquad (2)$$

$$\begin{bmatrix} -H_{AB_1} - \\ -H_{AB_2} - \\ \vdots \\ -H_{AB_m} - \end{bmatrix} \cdot \begin{bmatrix} | & | & & | \\ W_{A1} & W_{A2} & \cdots & W_{Am} \\ | & | & & | \end{bmatrix} = I$$

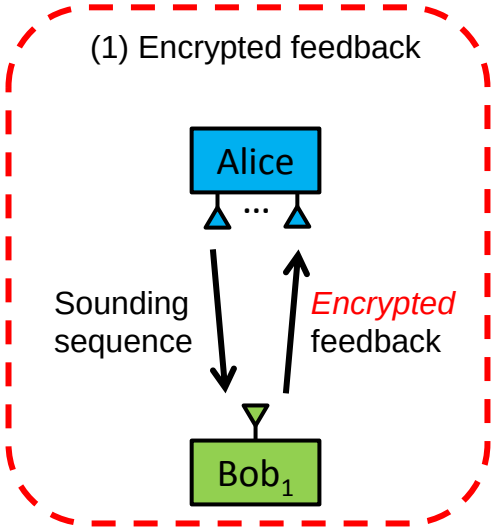
- Known-transmitted-symbol attack
- Estimate $span(H_{AB_j})$
  - If the number of selected Bobs = Alice's antenna number
    - ✓ $span(H_{AB_j})$ can be determined
  - If the number of selected Bobs < Alice's antenna number
    - ✓ Eve overhears > 1 beamforming transmissions to compute $span(H_{AB_j})$

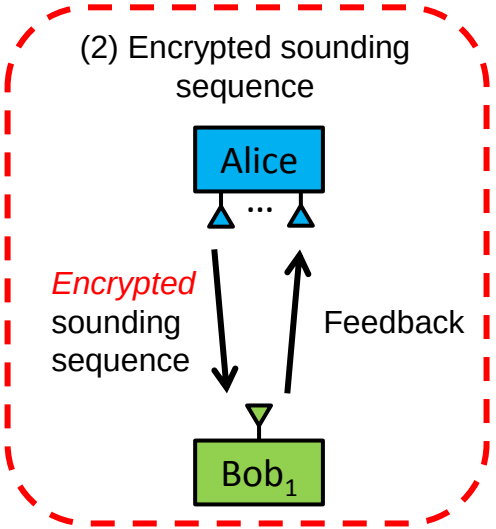
Eve Estimates Her Channel H_{AE}

- Eve needs to estimate her channel H_{AE}

Eve Estimates Her Channel H_{AE}

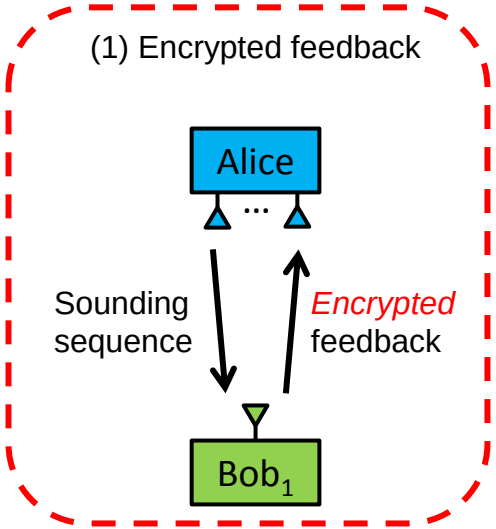
- Eve needs to estimate her channel H_{AE}

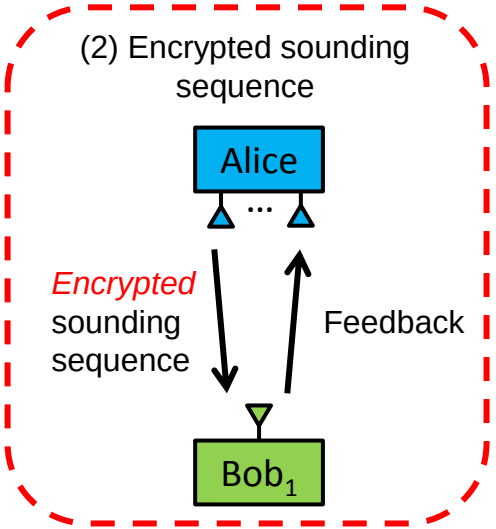




Eve Estimates Her Channel H_{AE}

- Eve needs to estimate her channel H_{AE}

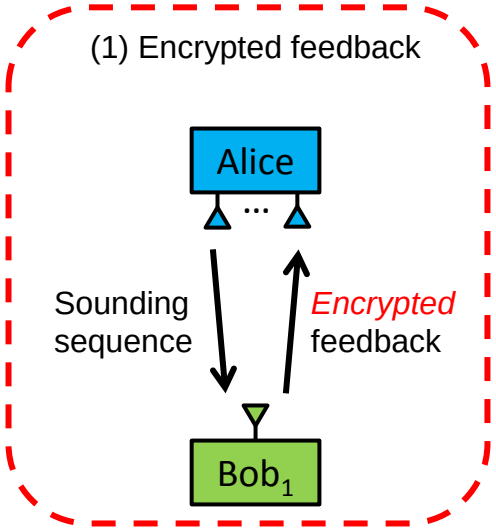




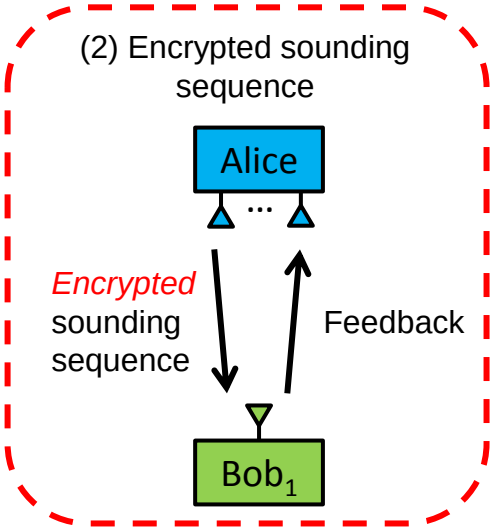
Eve estimates H_{AE} through the unencrypted channel sounding sequence

Eve Estimates Her Channel H_{AE}

- Eve needs to estimate her channel H_{AE}



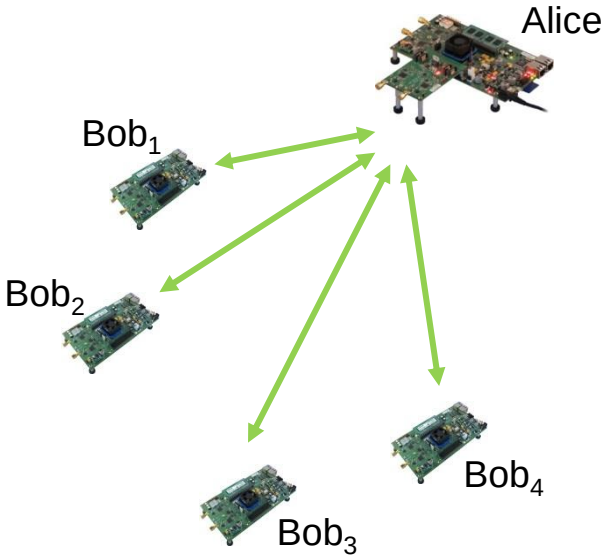
Eve estimates H_{AE} through the unencrypted channel sounding sequence



Eve can still estimate H_{AE} by using the dynamic cyclic shift

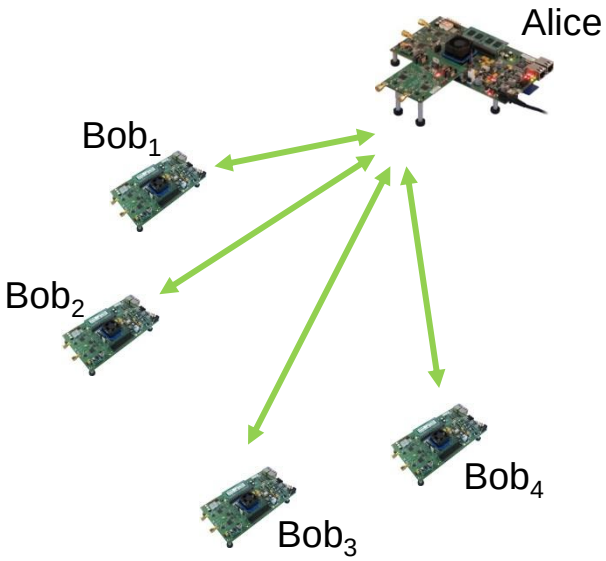
Implementation on WARP

- A multi-user MIMO WLAN in the 5 GHz band
  - A 4-antenna WARP as Alice
  - 4 single-antenna WARPs as the Bobs
  - 802.11ac packet format
  - 802.11ac-like multi-user beamforming



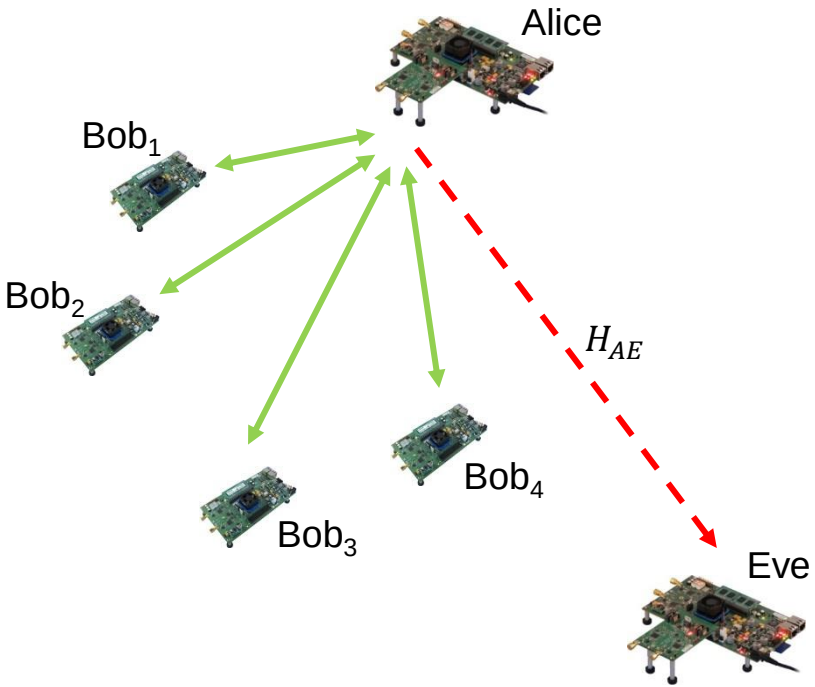
Implementation on WARP

- A multi-user MIMO WLAN in the 5 GHz band
  - A 4-antenna WARP as Alice
  - 4 single-antenna WARPs as the Bobs
  - 802.11ac packet format
  - 802.11ac-like multi-user beamforming
- Encrypted channel sounding [CSIsec, CCS 2014]



Implementation on WARP

- A multi-user MIMO WLAN in the 5 GHz band
  - A 4-antenna WARP as Alice
  - 4 single-antenna WARPs as the Bobs
  - 802.11ac packet format
  - 802.11ac-like multi-user beamforming
- Encrypted channel sounding [CSIsec, CCS 2014]
- CSIsnoop at Eve
  - Same number of antennas as Alice
  - Correct timing offset/carrier frequency offset
  - Estimate H_{AE}
  - Use CSIsnoop to compute Bobs' CSI

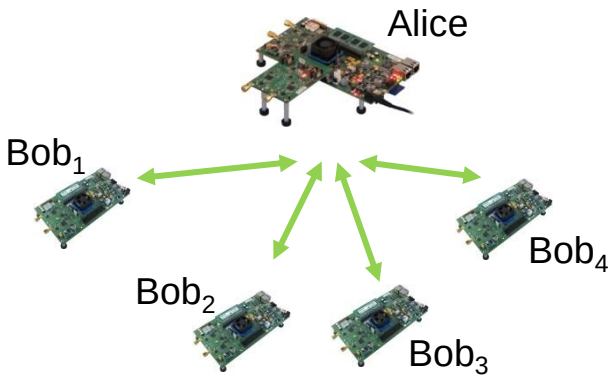


Experimental Evaluation

- Setup
  - Configure Alice and Eve to have 2, 3, or 4 antennas
  - Collect >100,000 rounds of over-the-air transmissions in different indoor environments

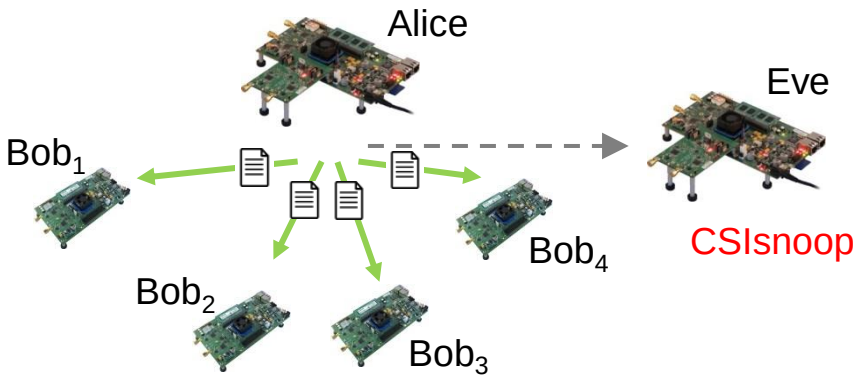
Experimental Evaluation

- Setup
  - Configure Alice and Eve to have 2, 3, or 4 antennas
  - Collect >100,000 rounds of over-the-air transmissions in different indoor environments



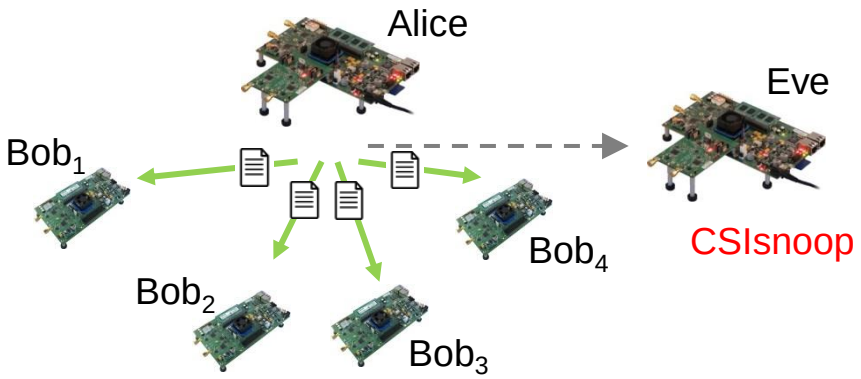
Experimental Evaluation

- Setup
  - Configure Alice and Eve to have 2, 3, or 4 antennas
  - Collect >100,000 rounds of over-the-air transmissions in different indoor environments



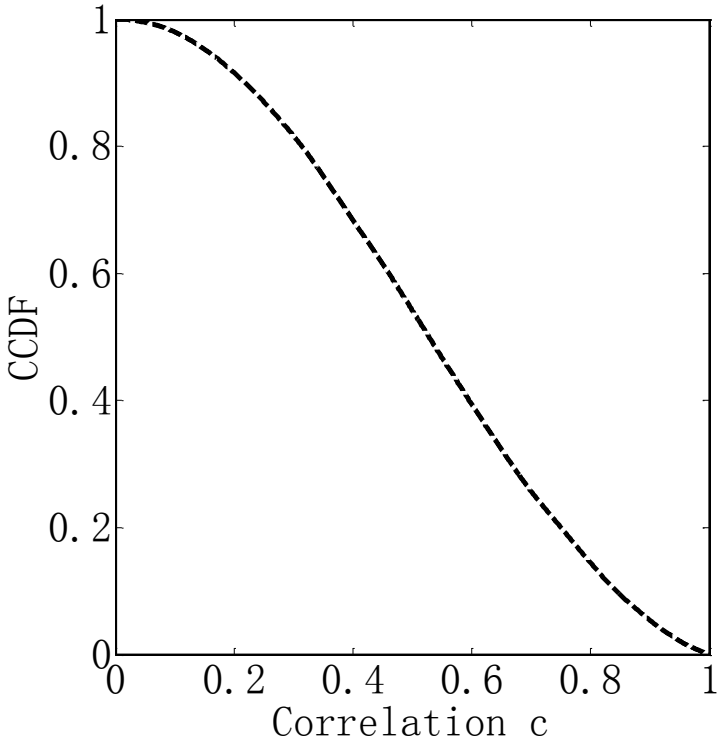
Experimental Evaluation

- Setup
  - Configure Alice and Eve to have 2, 3, or 4 antennas
  - Collect >100,000 rounds of over-the-air transmissions in different indoor environments



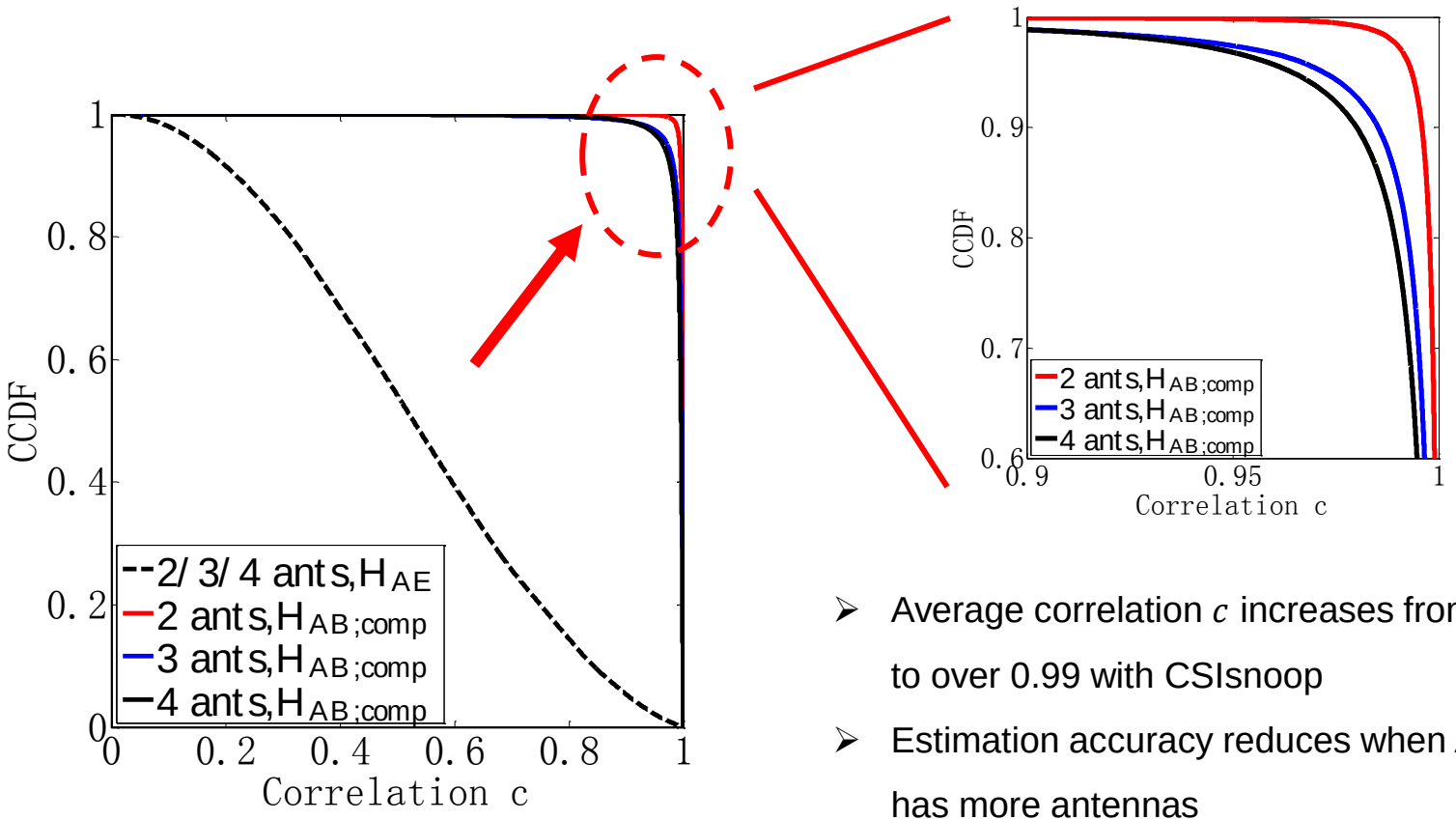
- Metric
  - Normalized correlation c between Bob's measured CSI and Eve's computed CSI
  - $c = 1$ indicates that the measured CSI and the computed CSI are perfectly correlated

Estimation Accuracy of CSIsnoop



- Eve does not use CSIsnoop
- Eve cannot estimate Bob's CSI by directly using her own CSI

Estimation Accuracy of CSIsnoop



- Average correlation c increases from 0.46 to over 0.99 with CSIsnoop
- Estimation accuracy reduces when Alice has more antennas

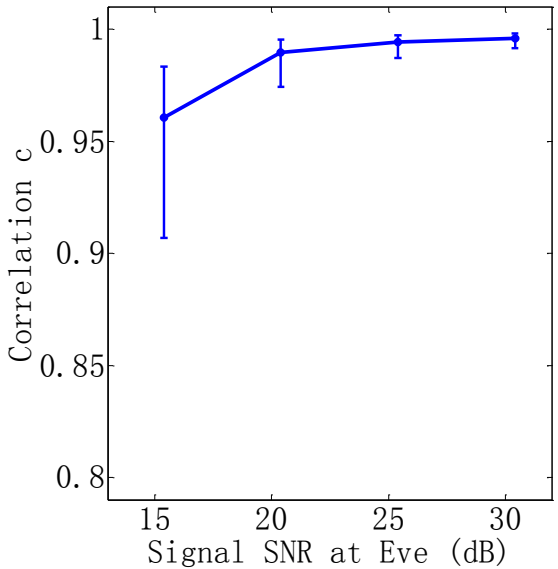
Impact of Eve's Channel H_{AE}

- Estimation accuracy is closely related to Eve's SNR and $cond(H_{AE})$
  - $cond(H_{AE})$ is the ratio between the largest and smallest singular value of H_{AE}
  - In the previous slide, average SNR is 30 dB and $cond(H_{AE}) = 5$

Impact of Eve's Channel H_{AE}

- Estimation accuracy is closely related to Eve's SNR and $cond(H_{AE})$
  - $cond(H_{AE})$ is the ratio between the largest and smallest singular value of H_{AE}
  - In the previous slide, average SNR is 30 dB and $cond(H_{AE}) = 5$

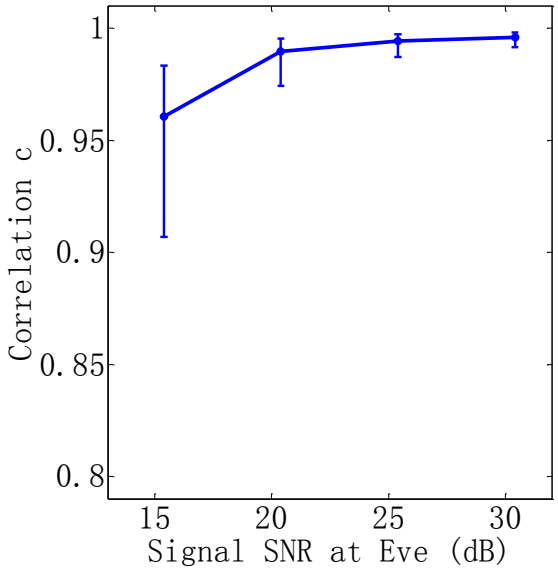
Reducing SNR



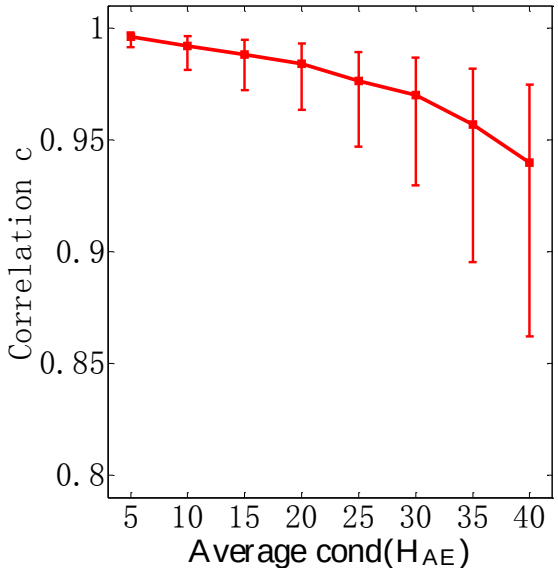
Impact of Eve's Channel H_{AE}

- Estimation accuracy is closely related to Eve's SNR and $cond(H_{AE})$
  - $cond(H_{AE})$ is the ratio between the largest and smallest singular value of H_{AE}
  - In the previous slide, average SNR is 30 dB and $cond(H_{AE}) = 5$

Reducing SNR



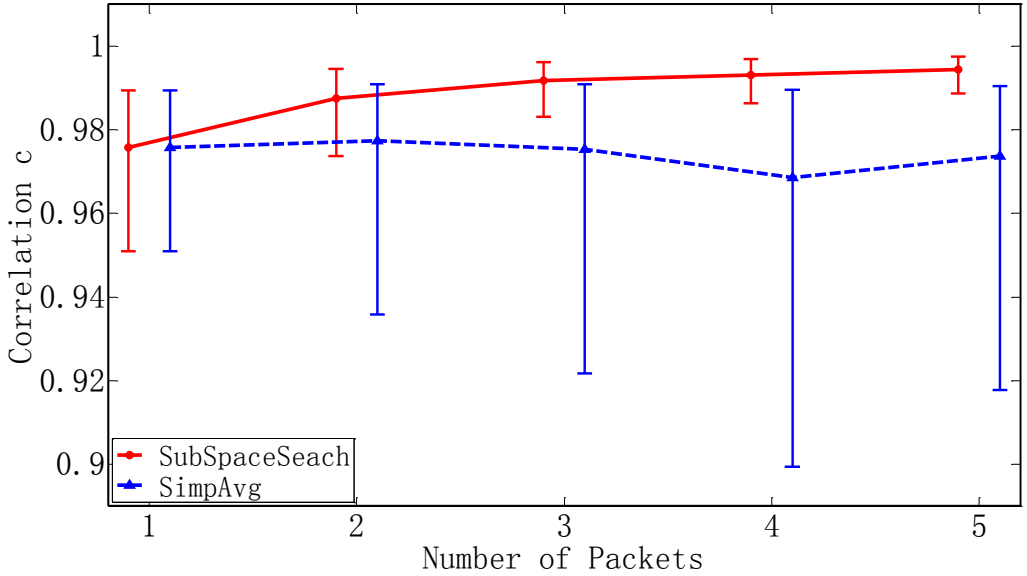
Increasing $cond(H_{AE})$



More Overheard Packets

- When Eve's SNR is small and $cond(H_{AE})$ is large
  - Eve can overhear more packets to increase her estimation accuracy
  - *SimpAvg*
    - ✓ Compute the average of the several computed CSI
  - *SubSpaceSearch*
    - ✓ Compute the most likely 1-dimensional sub-space spanned by the several computed CSI

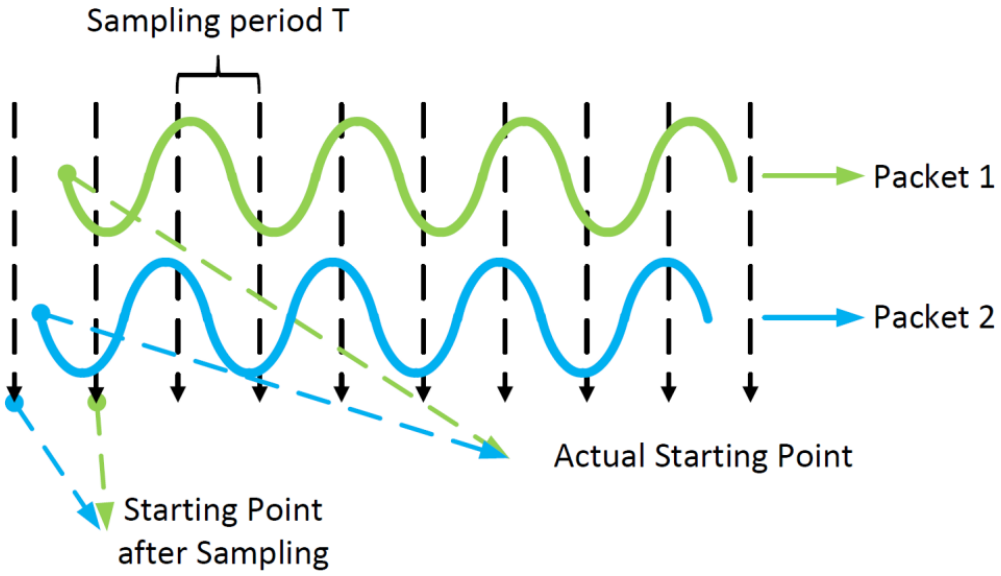
More Overheard Packets



- Eve's SNR is 20 dB and $cond(H_{AE}) = 30$
- *SubSpaceSearch* increases estimation accuracy while *SimpAvg* may even reduce it

More Overheard Packets

- Fractional timing offset due to ADC sampling at Eve
  - A maximum error of $T/2$ in determining the start of each overheard packet
  - Unknown phase rotation for Eve's computed CSI for each overheard packet
  - *SubSpaceSearch* will not be influenced by the unknown phase rotation



CSI-Based Attacks

- After Eve infers Bob's CSI
  - Eve can compute over 85% of the CSI-based password between Alice and Bob
  - Eve can selectively jam and thus only reduce the uplink throughput of a target Bob

Summary

- A fundamental conflict between using CSI to boost throughput and hiding CSI
- Describe the CSIsnoop framework
- Experimental results show high estimation accuracy of CSIsnoop
- A more careful examination of using CSI as a shared secret
- Design schemes to detect and prevent attacks based on CSI